

# **MedMij Afsprakenstelsel, normenkader**

Release 1.2.0

Auteur Project Afsprakenstelsel

Datum 31 oktober 2020

This deliverable contains original unpublished work or work to which the author holds all rights except where clearly indicated otherwise. Acknowledgement of previously published material and of the work of others has been made through appropriate citation, quotation or both.

## Inhoudsopgave



1. _snippets	6
1.1 snippet.beoordeling.auditor	7
1.2 snippet.implementatie.niet.voorgeschreven	8
1.3 snippet.weging.laag	9
1.4 snippet.weging.midden	10
1.5 snippet.weging.hoog	11
1.6 snippet.rollen	12
1.7 snippet.evidence	13
2. MedMij Afsprakenstelsel 1.2.0	14
2.1 Introductie	17
2.1.1 Afsprakenstelsel in de praktijk	21
2.2 Afsprakenstelsel release 1.2.0	24
2.2.1 Releaseinfo	26
2.2.1.1 Release- en versiebeschrijving	27
2.2.1.2 Changelog	29
2.2.1.2.1 Changelog release 1.2	30
2.2.1.2.2 Changelog release 1.1	33
2.2.1.2.3 Changelog release 1.0	45
2.2.1.3 Engelse vertaling / English translation	55
2.2.1.3.1 Architecture and technical specifications	56
2.2.2 Grondslagen	222
2.2.2.1 Achtergrond	223
2.2.2.2 Criteria	229
2.2.2.3 Principes	233
2.2.2.4 Opzet	239
2.2.2.5 Begrippenlijst	241
2.2.3 Juridische context	245
2.2.3.1 Juridisch kader	246
2.2.3.2 Overeenkomsten en rechtsrelaties	258
2.2.3.3 Toelichting verwerkingsverantwoordelijkheid	262
2.2.3.4 Toelichting AVG-normen	266
2.2.4 Architectuur en technische specificaties	300
2.2.4.1 Coördinatie, regie en uitwisseling	306
2.2.4.2 Juridica	311
2.2.4.3 Processen en informatie	312
2.2.4.3.1 UC Verzamelen	325
2.2.4.3.2 UC Delen	332
2.2.4.3.3 UC Abonneren	339
2.2.4.3.4 UC Notificeren	346
2.2.4.3.5 UC Opvragen GNL	349
2.2.4.3.6 UC Opvragen OCL	350
2.2.4.3.7 UC Opvragen ZAL	351
2.2.4.3.8 Beschikbaarheids- en ontvankelijkheidsvoorwaarde	352
2.2.4.4 Applicatie	356
2.2.4.4.1 Interfaces	371
2.2.4.4.2 Use case-implementaties	397
2.2.4.5 Netwerk	429
2.2.4.5.1 Use case-implementatie Opvragen WHL	439
2.2.4.5.2 WHL-Interface	440
2.2.4.6 Informatiemodellen	441
2.2.4.6.1 Metamodel	442
2.2.4.6.2 Logische modellen	461
2.2.4.6.3 XML-schema's	476
2.2.4.6.4 XML-bestanden voor lijsten	483
2.2.5 Normenkader informatiebeveiliging	484
2.2.5.1 A. 5.1.1 Beleidsregels voor informatiebeveiliging	491
2.2.5.2 A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging	492
2.2.5.3 A. 7.2.2 (1) Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	494
2.2.5.4 A. 7.2.2 (2) Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	495
2.2.5.5 A. 8.2.1 Classificatie van informatie	497
2.2.5.6 A. 9.1.1 Beleid voor toegangsbeveiliging	498
2.2.5.7 A. 9.2.5 Beoordeling van toegangsrechten van gebruikers	500

2.2.5.8 A. 9.4.1 Beperking toegang tot informatie	501
2.2.5.9 A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen	504
2.2.5.10 A.12.1.2 (1) Wijzigingsbeheer	506
2.2.5.11 A.12.1.2 (2) Wijzigingsbeheer	507
2.2.5.12 A.12.1.2 (3) Wijzigingsbeheer	508
2.2.5.13 A.12.1.3 (1) Capaciteitsbeheer	509
2.2.5.14 A.12.1.3 (2) Capaciteitsbeheer	510
2.2.5.15 A.12.3.1 Back-up van informatie	511
2.2.5.16 A.12.4.1 Gebeurtenissen registreren	512
2.2.5.17 A.12.4.3 Logbestanden van beheerders en operators	513
2.2.5.18 A.12.4.4 Kloksynchronisatie	514
2.2.5.19 A.12.6.1 Beheer van technische kwetsbaarheden	515
2.2.5.20 A.14.2.1 Beleid voor beveiligd ontwikkelen	516
2.2.5.21 A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	517
2.2.5.22 A.15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers	518
2.2.5.23 A.16.1.1 Verantwoordelijkheden en procedures	519
2.2.5.24 A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging	520
2.2.5.25 A.16.1.7 Verzamelen van bewijsmateriaal	521
2.2.5.26 A.18.2.3 (1) Beoordeling van technische naleving	522
2.2.5.27 A.18.2.3 (2) Beoordeling van technische naleving	524
2.2.5.28 Aanvullende auditverklaring en onderbouwende rapportage	525
2.2.6 Beleid	533
2.2.6.1 Beleid inzake gecontroleerde livegang	534
2.2.6.2 Change- en releasebeleid	536
2.2.6.3 Dienstverleningsoverdrachtsbeleid	539
2.2.6.4 Gegevensdienstenbeleid	540
2.2.6.5 Informatieclassificatiebeleid	542
2.2.6.6 Intellectueel eigendomsbeleid	545
2.2.6.7 Klachten- en geschillenbeleid	547
2.2.6.8 Nalevingsbeleid	548
2.2.6.9 OAuthclient-namenbeleid	550
2.2.6.10 Performancebeleid	551
2.2.6.11 Privacy- en informatiebeveiligingsbeleid	552
2.2.6.11.1 Risicoanalyse	553
2.2.6.12 Samenwerkings- en escalatiebeleid	555
2.2.6.13 Testbeleid	556
2.2.6.14 Zorgaanbiedersnamenbeleid	558
2.2.7 Operationele processen	560
2.2.8 Communicatie	566
2.2.8.1 Merkgebruik	567
2.2.8.2 Gebruikersvoorlichting	569
2.2.8.3 Toestemmingsverklaring	570
2.2.8.4 Toestemmingsverklaring Abonneren	572
2.2.8.5 Bevestigingsverklaring	574
2.2.8.6 Notificatie van Zorggebruiker	576
2.2.9 Managementinformatie	577
2.2.10 Correcties op deze release	582
2.3 Catalogus	586
2.4 Deelnemersovereenkomsten	587
2.4.1 Deelnemersovereenkomst Dienstverlener persoon	588
2.4.2 Deelnemersovereenkomst Dienstverlener zorgaanbieder	597
2.5 Toetreding	605
2.5.1 Toetredingsbeleid	606
2.5.2 Toetredingsproces	607
2.5.3 Zelfverklaring integriteit	608
2.5.4 Intentieverklaringen	611
2.5.4.1 Intentieverklaring Dienstverlener persoon	612
2.5.4.2 Intentieverklaring Dienstverlener zorgaanbieder	616
2.6 Governance	620
2.6.1 Rollen	622
2.6.2 Inrichting	626

2.6.2.1 Beheerverantwoordelijkheden .....	632
2.6.3 Statuten Stichting MedMij .....	634
2.7 Modelverwerkersovereenkomst .....	635
2.8 Issues .....	643
3. pdf.images .....	644

## \_snippets

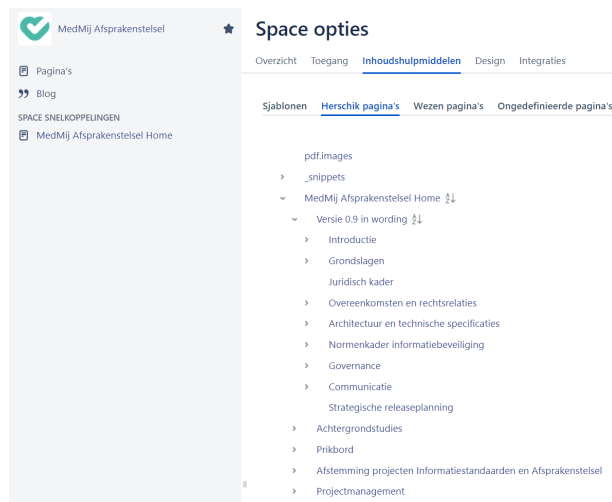
Snippets zijn kleine herbruikbare stukjes tekst die je eenvoudig op een pagina kunt inbedden middels de **Include Page**-macro.

Momenteel zijn er de volgende "snippets".

- [snippet.beoordeling.auditor](#)
- [snippet.implementatie.niet.voorgescreven](#)
- [snippet.weging.laag](#)
- [snippet.weging.midden](#)
- [snippet.weging.hoog](#)
- [snippet.rollen](#)
- [snippet.evidence](#)

Let op bij het publiceren van het afsprakenstelsel!

Om te voorkomen dat gebruikers de snippets zien, staan ze op een plek staan "buiten het zicht":



Als je het afsprakenstelsel publiceert door de boom te kopiëren naar een andere space, gaan de snippets dus niet mee. De pagina's blijven dan verwijzen naar de snippets in de oorspronkelijke locatie.

Om toch te zorgen dat de snippets mee-gekopieerd worden, en de hyperlinks correct blijven werken, volg onderstaande stappen:

1. Ga naar de menu-optie "herschik pagina's" (<https://afsprakenstelsel.medmij.nl/pages/reorderpages.action?key=MA08>)
2. Sleep de pagina "\_snippets" naar een plek **in** het afsprakenstelsel, bijvoorbeeld onder "Introductie"
3. Kopieer het afsprakenstelsel zoals je gewend was
4. Vanuit de nieuwe locatie, ga je opnieuw naar de menu-optie "herschik pagina's"
5. Sleep de pagina "\_snippets" nu weer **uit** het afsprakenstelsel, bijvoorbeeld boven de "Home"-pagina.
6. Geniet van een afsprakenstelsel met werkende snippets

## snippet.beoordeling.auditor

Het afsprakenstelsel schrijft dit niet voor. De auditor kan dit naar eigen inzicht uitvoeren.

## snippet.implementatie.niet.voorgeschreven

Deze beheersmaatregel moet zijn opgenomen op de Verklaring van Toepasselijkheid, maar het afsprakenstelsel schrijft (nog) geen nadere invulling voor. Partijen mogen deze naar eigen inzicht invullen.

## snippet.weging.laag

LAAG RISICO

MedMij geeft geen specifieke weging aan de implementatie van deze maatregel, hij mag evenwel niet uitgesloten zijn. De auditor of CI bepaalt hoe zwaar deze maatregel weegt in zijn certificatiebeslissing.

## snippet.weging.midden

MIDDEN RISICO

MedMij hecht waarde aan de correcte implementatie van deze maatregel. De maatregel moet zijn geïmplementeerd, maar er mag een *kleine non-conformiteit* aanwezig zijn. De auditor moet het verbeterplan hebben goedgekeurd.



## snippet.weging.hoog

HOOG

MedMij hecht veel waarde aan de correcte implementatie van deze maatregel. De maatregel moet zijn geïmplementeerd en mogen geen *non-conformiteiten* aanwezig zijn.

## snippet.rollen

*DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie*

## snippet.evidence

*Bij de eerste certificering volgens dit normenkader is het aantonen van de opzet voldoende.*

## MedMij Afsprakenstelsel 1.2.0

Het MedMij Afsprakenstelsel draagt eraan bij dat persoonsgebonden, gevoelige en vertrouwelijke gezondheidsgegevens op een veilige en gebruiksvriendelijke wijze uitgewisseld kunnen worden tussen persoonlijke gezondheidsomgevingen en zorgaanbieders. De uitwisseling geschiedt in twee richtingen; personen kunnen gegevens verzamelen en delen.

MedMij streeft naar het realiseren van interoperabiliteit voor deze uitwisseling. Hiertoe is een afsprakenstelsel ontwikkeld, bestaande uit afspraken op juridisch, organisatorisch, financieel, communicatief, semantisch en technisch gebied, zodat personen en zorgaanbieders op een veilige manier gegevens kunnen uitwisselen. Partijen die deelnemen aan het MedMij Afsprakenstelsel committeren zich aan de afspraken, en kunnen diensten aanbieden op basis van de reeds overeengekomen afspraken.

Het afsprakenstelsel gaat uit van *centraal vertrouwen en decentrale operatie*. Het afsprakenstelsel is een bewust gecreëerde verzameling instituties die waarborgen biedt voor een faire omgang met de belangen van de verschillende stakeholders. Bij de uitwisseling van gegevens via het MedMij-netwerk wordt echter uitgegaan van decentrale technische voorzieningen.

### Onderdelen van het afsprakenstelsel

Het MedMij Afsprakenstelsel bestaat uit een samenhangende set afspraken, voorzieningen en ingerichte ontwikkel- en beheerprocessen.

- Partijen die diensten willen bieden aan personen of zorgaanbieders kunnen als deelnemer toetreden tot het afsprakenstelsel in de rol van Dienstverlener persoon of Dienstverlener zorgaanbieder.
- Voordat partijen deelnemer worden in het afsprakenstelsel, doorlopen zij het [Toetredingsproces](#). Op dit proces is het [Toetredingsbeleid](#) van toepassing. Bij de start van het proces overlegt de potentiële deelnemer een [Zelfverklaring integriteit](#). Na een eerste controle op enkele formaliteiten maken de kandidaat-deelnemer en de MedMij-beheerorganisatie afspraken over het vervolg van het toetredingsproces door middel van een [Intentieverklaring](#).
- Als het toetredingsproces met goed gevolg is doorlopen en toetreding van de deelnemer het stelselbelang niet schaadt, sluiten de deelnemer en de beheerorganisatie een [Deelnemersovereenkomst](#) met elkaar.
- In de [Deelnemersovereenkomst](#) is onder meer opgenomen dat partijen zich houden aan de [Afsprakenstelsel](#), een uitgebreide set met rollen en verantwoordelijkheden. Partijen erkennen via de overeenkomst ook de [Grondslagen](#) en de [Juridische context](#). Zowel de afsprakenstelsel, de grondslagen als de juridische context van de afsprakenstelsel worden releasematig ontwikkeld, gepubliceerd en in productie genomen.
- De beheerorganisatie onderhoudt twee registers die relevant zijn voor de dienstverlening die via het MedMij-netwerk kan worden aangeboden. Het Register van Informatiestandaarden bevat de toegelaten informatiestandaarden. De [Catalogus](#) definieert welke Gegevensdiensten deelnemers kunnen aanbieden.
- De governance van het afsprakenstelsel is formeel vastgelegd in de [Statuten](#) van de Stichting MedMij, maar ook in een [toegankelijker vorm](#) beschreven.
- De toelating van informatiestandaarden tot het MedMij Afsprakenstelsel is onderworpen aan eisen (aan informatiestandaarden) en een uitgewerkte governance (proces en rolverdeling).
- De voor deelnemers relevante beheerprocessen zijn in groter detail uitgewerkt door de beheerorganisatie. De detailuitwerking is geen onderdeel van de afsprakenstelsel omdat die bovenal informatief is; deelnemers worden gebonden via de [Operationele processen](#) uit de afsprakenstelsel.
- Zorgaanbieders sluiten op grond van de AVG verplicht een verwerkersovereenkomst met hun dienstverlener(s) zorgaanbieder. MedMij stelt een [Modelverwerkersovereenkomst](#) beschikbaar die partijen kunnen gebruiken om passende afspraken met elkaar te maken.

### Bindingen

Onderstaande tabel geeft weer hoe partijen formeel gebonden zijn aan de verschillende componenten van het MedMij Afsprakenstelsel.

*Gebonden* betekent dat een partij een verplichting is aangegaan. *Erkend* betekent dat de partij heeft verklaard dat de component relevante context bij de uitleg van verplichtingen en het overig handelen in het kader van het afsprakenstelsel betreft.

Component	Dienstverlener persoon	Dienstverlener zorgaanbieder	Beheerorganisatie
Afsprakenstelsel	Gebonden via deelnemersovereenkomst	Gebonden via deelnemersovereenkomst	Gebonden via deelnemersovereenkomst
Grondslagen	Erkend via deelnemersovereenkomst	Erkend via deelnemersovereenkomst	Erkend via deelnemersovereenkomst
Juridische context	Erkend via deelnemersovereenkomst	Erkend via deelnemersovereenkomst	Erkend via deelnemersovereenkomst
Register van Informatiestandaarden	Gebonden via afsprakenstelsel	Gebonden via afsprakenstelsel	Gebonden via afsprakenstelsel
Catalogus	Gebonden via afsprakenstelsel	Gebonden via afsprakenstelsel	Gebonden via afsprakenstelsel
Deelnemersovereenkomst Dienstverlener persoon	Gebonden door overeenkomst	-	Gebonden door overeenkomst
Deelnemersovereenkomst Dienstverlener zorgaanbieder	-	Gebonden door overeenkomst	Gebonden door overeenkomst
Toetredingsbeleid	Gebonden via intentieverklaring	Gebonden via intentieverklaring	Gebonden via intentieverklaring
Toetredingsproces	Gebonden via intentieverklaring	Gebonden via intentieverklaring	Gebonden via intentieverklaring
Zelfverklaring integriteit	Gebonden door ondertekening	Gebonden door ondertekening	-
Intentieverklaring Dienstverlener persoon	Gebonden via overeenkomst (niet in rechte afdwingbaar)	-	Gebonden via overeenkomst (niet in rechte afdwingbaar)
Intentieverklaring Dienstverlener zorgaanbieder	-	Gebonden via overeenkomst (niet in rechte afdwingbaar)	Gebonden via overeenkomst (niet in rechte afdwingbaar)
Governance	Gebonden door statuten	Gebonden door statuten	Gebonden door statuten
Statuten Stichting MedMij	-	-	Gebonden door burgerlijk recht

Coördinatie standaarden MedMij - Eisen	-	-	-
Coördinatie standaarden MedMij - Governance	-	-	-
Uitwerking beheerprocessen	Gebonden via beleid (afsprakenet)	Gebonden via beleid (afsprakenet)	Gebonden via bel (afsprakenet)
Modelverwerkersovereenkomst Zorgaanbieder - Dienstverlener zorgaanbieder	-	Optioneel gebonden door overeenkomst met zorgaanbieder	-

## Introductie

Het MedMij Afsprakenstelsel draagt eraan bij dat persoonsgebonden, gevoelige en vertrouwelijke gezondheidsgegevens op een veilige en gebruiksvriendelijke wijze uitgewisseld kunnen worden tussen persoonlijke gezondheidsomgevingen en zorgaanbieders. De uitwisseling geschiedt in twee richtingen; personen kunnen gegevens verzamelen en delen.

MedMij streeft naar het realiseren van interoperabiliteit voor deze uitwisseling. Hiertoe is een afsprakenstelsel ontwikkeld, bestaande uit afspraken op juridisch, organisatorisch, financieel, communicatief, semantisch en technisch gebied, zodat personen en zorgaanbieders op een veilige manier gegevens kunnen uitwisselen. Partijen die deelnemen aan het MedMij Afsprakenstelsel committeren zich aan de afspraken, en kunnen diensten aanbieden op basis van de reeds overeengekomen afspraken.

Het afsprakenstelsel gaat uit van *centraal vertrouwen en decentrale operatie*. Het afsprakenstelsel is een bewust gecreëerde verzameling instituties die waarborgen biedt voor een faire omgang met de belangen van de verschillende stakeholders. Bij de uitwisseling van gegevens via het MedMij-netwerk wordt echter uitgegaan van decentrale technische voorzieningen.

## Onderdelen van het afsprakenstelsel

Het MedMij Afsprakenstelsel bestaat uit een samenhangende set afspraken, voorzieningen en ingerichte ontwikkel- en beheerprocessen.

- Partijen die diensten willen bieden aan personen of zorgaanbieders kunnen als deelnemer toetreden tot het afsprakenstelsel in de rol van Dienstverlener persoon of Dienstverlener zorgaanbieder.
- Voordat partijen deelnemer worden in het afsprakenstelsel, doorlopen zij het [Toetredingsproces](#). Op dit proces is het [Toetredingsbeleid](#) van toepassing. Bij de start van het proces overlegt de potentiële deelnemer een [Zelfverklaring integriteit](#). Na een eerste controle op enkele formaliteiten maken de kandidaat-deelnemer en de MedMij-beheerorganisatie afspraken over het vervolg van het toetredingsproces door middel van een [Intentieverklaring](#).
- Als het toetredingsproces met goed gevolg is doorlopen en toetreding van de deelnemer het stelselbelang niet schaadt, sluiten de deelnemer en de beheerorganisatie een [Deelnemersovereenkomst](#) met elkaar.
- In de [Deelnemersovereenkomst](#) is onder meer opgenomen dat partijen zich houden aan de [Afsprakenset](#), een uitgebreide set met rollen en verantwoordelijkheden. Partijen erkennen via de overeenkomst ook de [Grondslagen](#) en de [Juridische context](#). Zowel de afsprakenset, de grondslagen als de juridische context van de afsprakenset worden releasematig ontwikkeld, gepubliceerd en in productie genomen.
- De beheerorganisatie onderhoudt twee registers die relevant zijn voor de dienstverlening die via het MedMij-netwerk kan worden aangeboden. Het Register van Informatiestandaarden bevat de toegelaten informatiestandaarden. De [Catalogus](#) definieert welke Gegevensdiensten deelnemers kunnen aanbieden.
- De governance van het afsprakenstelsel is formeel vastgelegd in de [Statuten](#) van de Stichting MedMij, maar ook in een [toegankelijker vorm](#) beschreven.
- De toelating van informatiestandaarden tot het MedMij Afsprakenstelsel is onderworpen aan eisen (aan informatiestandaarden) en een uitgewerkte governance (proces en rolverdeling).
- De voor deelnemers relevante beheerprocessen zijn in groter detail uitgewerkt door de beheerorganisatie. De detailuitwerking is geen onderdeel van de afsprakenset omdat die bovenal informatief is; deelnemers worden gebonden via de [Operationele processen](#) uit de afsprakenset.
- Zorgaanbieders sluiten op grond van de AVG verplicht een verwerkersovereenkomst met hun dienstverlener(s) zorgaanbieder. MedMij stelt een [Modelverwerkersovereenkomst](#) beschikbaar die partijen kunnen gebruiken om passende afspraken met elkaar te maken.

## Bindingen

Onderstaande tabel geeft weer hoe partijen formeel gebonden zijn aan de verschillende componenten van het MedMij Afsprakenstelsel.

*Gebonden* betekent dat een partij een verplichting is aangegaan. *Erkend* betekent dat de partij heeft verklaard dat de component relevante context bij de uitleg van verplichtingen en het overig handelen in het kader van het afsprakenstelsel betreft.



Component	Dienstverlener persoon	Dienstverlener zorgaanbieder	Beheerorganisatie
Afsprakenset	Gebonden via deelnemersovereenkomst	Gebonden via deelnemersovereenkomst	Gebonden via deelnemersovereenkomst
Grondslagen	Erkend via deelnemersovereenkomst	Erkend via deelnemersovereenkomst	Erkend via deelnemersovereenkomst
Juridische context	Erkend via deelnemersovereenkomst	Erkend via deelnemersovereenkomst	Erkend via deelnemersovereenkomst
Register van Informatiestandaarden	Gebonden via afsprakenset	Gebonden via afsprakenset	Gebonden via afsprakenset
Catalogus	Gebonden via afsprakenset	Gebonden via afsprakenset	Gebonden via afsprakenset
Deelnemersovereenkomst Dienstverlener persoon	Gebonden door overeenkomst	-	Gebonden door overeenkomst
Deelnemersovereenkomst Dienstverlener zorgaanbieder	-	Gebonden door overeenkomst	Gebonden door overeenkomst
Toetredingsbeleid	Gebonden via intentieverklaring	Gebonden via intentieverklaring	Gebonden via intentieverklaring
Toetredingsproces	Gebonden via intentieverklaring	Gebonden via intentieverklaring	Gebonden via intentieverklaring
Zelfverklaring integriteit	Gebonden door ondertekening	Gebonden door ondertekening	-
Intentieverklaring Dienstverlener persoon	Gebonden via overeenkomst (niet in rechte afdwingbaar)	-	Gebonden via overeenkomst (niet in rechte afdwingbaar)

Intentieverklaring Dienstverlener zorgaanbieder	-	Gebonden via overeenkomst (niet in rechte afdwingbaar)	Gebonden via overeenkomst (niet in rechte afdwingbaar)
Governance	Gebonden door statuten	Gebonden door statuten	Gebonden door statuten
Statuten Stichting MedMij	-	-	Gebonden door burgerlijk recht
Coördinatie standaarden MedMij - Eisen	-	-	-
Coördinatie standaarden MedMij - Governance	-	-	-
Uitwerking beheerprocessen	Gebonden via beleid (afsprakenet)	Gebonden via beleid (afsprakenet)	Gebonden via beleid (afsprakenet)
Modelverwerkersovereenkomst Zorgaanbieder - Dienstverlener zorgaanbieder	-	Optioneel gebonden door overeenkomst met zorgaanbieder	-

## Afsprakenstelsel in de praktijk

### Doel

Het klantverhaal van Roos Dalstra beschrijft op toegankelijke wijze de praktische toepassing van het afsprakenstelsel.

### Het verhaal van Roos Dalstra

Hallo, ik ben Roos Dalstra, een vrouw van 54 jaar. Leuk dat jullie dit verhaal willen lezen over mijn ervaringen met MedMij, een afsprakenstelsel waar de leverancier van mijn persoonlijke gezondheidsomgeving aan deelneemt, zodat ik met die toepassing op een veilige manier mijn gezondheidsgegevens kan verzamelen bij en delen met zorgaanbieders. Zorgaanbieder is geen woord dat ik zelf gebruik. Ik heb het liever over Marlou en Evelien, mijn huisarts en haar praktijkondersteuner, en Ed, mijn apotheker.

Voor mijn behandeling helpt het enorm om informatie van bijvoorbeeld Ed te krijgen over de medicatie die hij aan me heeft verstrekt. Eerder voelde ik mij onzeker en had ik geen overzicht van de medicijnen die ik moest slikken. Gevoelsmatig had ik er geen grip op. Daarom wil ik mijn ervaringen graag met jullie delen, zodat ook jullie kennis kunnen maken met MedMij.

### Een persoonlijke gezondheidsomgeving

Al een aantal jaren heb ik diabetes en sinds kort maak ik gebruik van een persoonlijke gezondheidsomgeving. In mijn geval is dat een combinatie van een persoonlijk gezondheidsplatform en andere apps en apparaten die ik gebruik die op dit platform kunnen aansluiten. Zo heb ik mijn smartwatch, mijn weegschaal en mijn bloedglucosemeter aangesloten en maak ik gebruik van een diabetes-app waarin ik verschillende overzichten kan bekijken. Het persoonlijke gezondheidsplatform zorgt ervoor dat het allemaal mooi samen komt en ik heb een eigen dashboard om het allemaal te beheren. Hierin heb ik bijvoorbeeld geregeld dat mijn diabetesapp gebruik kan maken van de gegevens die ik van de zorgaanbieder heb ontvangen in het platform.

### Informatie uitwisselen met mijn huisarts

Ik was laatst in de huisartspraktijk voor controle door Evelien en zat in de wachtkamer te wachten totdat ik aan de beurt was. Mijn oog viel op een poster aan de wand met daarop de boodschap "Wij doen mee MedMij!" met daaronder de unieke naam van de praktijk die binnen de MedMij-gegevensuitwisseling wordt gehanteerd en die je kan gebruiken om de praktijk te vinden in de persoonlijke gezondheidsomgeving. Van MedMij had ik al gehoord. Mijn zoon Bart heeft me laatst namelijk geholpen om een persoonlijke gezondheidsomgeving te kiezen. "Dat is helemaal van deze tijd!", had hij gezegd. Daar stond toen ook MedMij bij.

"Mevrouw Dalstra". Het was Evelien die me kwam ophalen voor de controle. Ik zat nog helemaal met mijn gedachten bij de avond dat ik met Bart een persoonlijke gezondheidsomgeving heb uitgekozen. Ik weet nog dat hij me een app liet zien waarvan ik dacht: "Wat moet ik daar nou mee? Veel te ingewikkeld allemaal." Hij had toen gezegd: "Mam, geen probleem. Laten we gewoon online kijken welke gezondheidsomgeving bij jou past. Elke aanbieder die zich aan de MedMij-spelregels houdt, kan op een veilige manier gegevens uitwisselen met zorgaanbieders die ook via MedMij kunnen uitwisselen. Er is al aardig wat aanbod."

We zochten online en vonden een persoonlijke gezondheidsomgeving speciaal voor mensen met diabetes, die ook echt ondersteuning biedt bij de behandeling. “Wat handig!” dacht ik. Hij is trouwens ook eenvoudig in het gebruik, wel zo fijn. Ik ben af en toe echt een kluns met apps. De week daarna heb ik zelf een beetje gespeeld met het dashboard van de omgeving. Dat ging zo makkelijk. Ik heb het voor elkaar gekregen om de bloedwaarden uit mijn bloedglucosemeter in te laden. Echt handig! De overzichten die ik normaal altijd bij Evelien zie, kwamen er zo uitrollen.

Al lopend naar de kamer vroeg ik Evelien wat dat MedMij precies inhoudt. “Wat leuk dat je ernaar vraagt. Daarmee kunnen we alle informatie die we zo gaan vastleggen op een veilige en betrouwbare manier ook met jou delen. Heb je al een eigen gezondheidsomgeving?” reageerde Evelien gelijk heel enthousiast. “Ja, die heb ik laatst uitgezocht met mijn zoon, Bart. Dat is toevallig, nietwaar?” reageerde ik. Evelien lachte naar me. “Wat mooi,” dacht ik, “dan kan ik alles wat we zo bespreken straks even rustig nalezen.” Het stelde me meteen gerust.

Evelien vroeg of ik al informatie had vastgelegd in de omgeving. “Uuh, ja,” stamelde ik en ik greep mijn telefoon om de bloedwaarden te laten zien. “Ik gebruik deze app om mijn bloedwaarden en gewicht zelf bij te houden,” vertelde ik aan Evelien. “Wat goed. De bedoeling is dat je die informatie ook met mij kan gaan delen. Blijf daar dus vooral mee doorgaan.”

Na onze afspraak liep Evelien snel even met me mee. Ze liet me zien hoe ik de praktijk kon vinden in de app van mijn persoonlijke gezondheidsomgeving. Ik moest de app van het platform openen en klikken op ‘Voeg nieuw contact toe’. Daar kon ik de naam invoeren die op de poster in de wachtkamer staat. Ik kreeg de informatie over de praktijk in de app te zien met de vraag of ik de gegevensuitwisseling met de praktijk tot stand wilde brengen. Evelien zei: “Ik moet helaas weer verder, je bent alleen nog niet klaar. De stappen spreken echter voor zich.” Evelien liep weg. Ik sloot de app. Dat doe ik straks wel even rustig als ik thuis ben.

Toen ik weer thuis was, ging ik verder in de app. Ik klikte op de optie om verbinding te maken. Vervolgens kon ik DigiD gebruiken, dat had ik al eens samen met mijn zoon gebruikt voor toeslagen bij de Belastingdienst. Ik voerde mijn gebruikersnaam in om vervolgens een pincode in te voeren. Hierna kreeg ik toegang tot een scherm waarin ik toestemming moest geven voor de gegevensuitwisseling tussen mijn huisarts en mijn persoonlijke gezondheidsomgeving. Ik kreeg te zien dat mijn huisarts toestemming vroeg om laboratoriumwaarden te verstrekken aan de persoonlijke gezondheidsomgeving. Ik gaf toestemming.

De browser op mijn telefoon sloot zich en ik kwam weer terug in de app van mijn gezondheidsomgeving. Ik zag in de contacten dat mijn huisarts was toegevoegd met de status dat ik was verbonden. Ik was gekoppeld met mijn huisarts en klaar om gegevens uit te wisselen.

## Informatie uitwisselen met mijn apotheek

Nadat ik mijn huisarts had toegevoegd, ging ik kijken wie ik nog meer kon toevoegen. Na de keuze om een contact toe te voegen, ging ik naar het zoekscherm om te zoeken naar de apotheek van Ed. Nadat ik was ingelogd en toestemming had gegeven, kwam de gegevensuitwisseling gelijk tot stand. En zo kon ik ook het ziekenhuis en mijn tandarts toevoegen. Ik begrijp van het standaard scherm, dat ik steeds te zien krijg om toestemming te geven, dat ik steeds alleen toestemming geef voor de gegevensuitwisseling met mijn persoonlijke gezondheidsomgeving op dat moment. In de gebruiksvoorlichting die de leverancier van de persoonlijke gezondheidsomgeving toonde in een informatiepagina vond ik nog veel meer informatie over MedMij en waar ik goed op moest letten.

De toestemming voor de gegevensuitwisseling tussen mijn persoonlijke gezondheidsomgeving en het apothekerssysteem van Ed was de eerste stap om een overzicht te krijgen van de medicatie die ik via de apotheek heb ontvangen. Een actueel medicatieoverzicht heet dat in de omgeving. Eenmaal akkoord gegeven zag ik de medicatiegegevens binnenkomen in het medicatieoverzicht van de app. Dit overzicht had ik vanaf dat moment altijd beschikbaar binnen de app door hierop in te loggen met mijn vingerafdruk.

Iedere keer als ik medicijnen van een herhaalrecept of van een nieuw recept kreeg, werkte ik mijn medicatieoverzicht bij door de nieuwe gegevens binnen te halen. Toen dat een keer niet goed ging, nam ik contact op met de leverancier van de app via de contactgegevens die ik daarin vond. Deze hielp mij direct verder waardoor ik alsnog de nieuwste gegevens ontving.

Ik vond het zo leuk dat mijn medicatieoverzicht steeds werd bijgewerkt, dat ik het aan Ed vertelde. Hij reageerde gelijk ook heel enthousiast: "Handig hè, om al jouw medicatie-informatie op één plek te hebben?" "Wat ben jij goed op de hoogte," zei ik verbaasd tegen Ed. Hij begon te lachen en zei: "Ja, ik vind het interessant en ik ben vorige week naar een presentatie over dit onderwerp geweest." Hij wees me ook op de gebruikersvoorlichting die standaard wordt geleverd over het uitwisselen van gegevens via MedMij. "Als apotheker heb ik ook voorlichting mee gekregen van de leverancier van mijn informatiesysteem. Daarin staan veel goede tips en achtergronden", zei hij enthousiast.

Voortaan houd ik alles bij met mijn gezondheidsomgeving, ook wat ik wel en niet gebruik aan medicatie. Naast dat ik die informatie kan gaan delen met Evelien en Ed, heb ik er vooral zelf veel baat bij. Ik heb overal en altijd een actueel overzicht van wat ik aan medicatie verstrekt krijg en wat ik gebruik. Zeker in gesprekken met artsen is dat super. Ook de extra mogelijkheden die de omgeving me bieden, helpen me om meer grip te krijgen op mijn eigen gezondheid. Dat geeft me veel vertrouwen.

## Afsprakenet release 1.2.0

Voor u ligt release 1.2.0 van de afsprakenet van het MedMij Afsprakenstelsel. Release 1.2.0 is de opvolger van release 1.1.2 (zie [Changelog](#)).

De afsprakenet draagt bij aan veilige, interoperabele en betrouwbare gegevensuitwisseling tussen persoonlijke gezondheidsomgevingen en informatiesystemen van zorgaanbieders. Deze afspraken moeten partijen voldoende vertrouwen en mogelijkheden geven om de onderlinge gegevensuitwisseling in de praktijk tot stand te brengen. De afsprakenet is pre concurrentieel. De afspraken zijn tot stand gekomen in samenwerking met diverse partijen in de zorg, zoals softwareleveranciers, het ministerie van Volksgezondheid, Welzijn en Sport, Patiëntenfederatie Nederland en vertegenwoordigers van zorgaanbieders, onder andere via werkgroepen op de onderwerpen informatiestandaarden, gegevensuitwisseling/architectuur, juridisch en governance. Partijen die deelnemen aan het MedMij Afsprakenstelsel committeren zich aan de afspraken.

Het is mogelijk om beoogd deelname aan het afsprakenstelsel kenbaar te maken middels een aanmelding tot kandidaat-deelnemer. Zie voor meer informatie hierover <https://www.medmij.nl/leveranciers/>.

## Leeswijzer

Wet- en regelgeving vormen de belangrijkste kaders voor de afsprakenet. De set beschrijft alleen dat wat nog niet in wet- en regelgeving is vastgelegd en wat nodig is voor het vertrouwen en de interoperabiliteit van deelnemers in de onderlinge gegevensuitwisseling.

De documentatie van de afsprakenet is als volgt opgebouwd:

- **Releaseinfo:** Het hoofdstuk biedt meta-informatie over deze release van de afsprakenet.
- **Grondslagen:** Een beschrijving van de achtergrond, criteria aan, principes voor, opzet van en begrippenlijst binnen het afsprakenstelsel.
- **Juridische context:** Een uitwerking van de juridische analyses.
- **Architectuur en technische specificaties:** De architectuurbeschrijving geeft een overzicht van de vereisten aan en vormgeving van de gegevensuitwisseling via MedMij. Dit is vertaald in technische specificaties die deelnemers, aangesloten op het MedMij-netwerk, dienen te implementeren om te voldoen aan de afspraken.
- **Normenkader informatiebeveiliging:** Het Normenkader informatiebeveiliging beschrijft de maatregelen die deelnemers minimaal dienen te treffen op het gebied van privacy en informatiebeveiliging. Deze maatregelen verminderen mogelijke risico's en komen voort uit een risicoanalyse die jaarlijks stelselbreed wordt uitgevoerd.
- **Beleid:** Het beleid gaat in op de vraag hoe Stichting MedMij omgaat met een aantal belangrijke besturingsthema's en vormt de basis voor de [Operationele processen](#). Het beleid is richtinggevend voor het optreden van Stichting MedMij en de uitvoeringsorganisaties. Het bevat tevens verantwoordelijkheden voor deelnemers.
- **Operationele processen:** Een beschrijving van belangrijkste de operationele beheerprocessen die deelnemers raken.
- **Communicatie:** Het onderdeel communicatie bevat richtlijnen voor de communicatie over MedMij vanuit de deelnemers. Het bestaat uit afspraken over het gebruik van het merk MedMij, verplichte gebruikersvoorlichting en de opzet van een verplicht te gebruiken toestemmings- en bevestigingsverklaring.
- **Managementinformatie:** Managementinformatie beschrijft de sturingsinformatie die deelnemers periodiek dienen aan te leveren bij de beheerorganisatie.

Alle lezers wordt aangeraden om, alvorens de afspraken set te bestuderen, eerst kennis te nemen van de stelselbrede [Introductie](#) en [Afsprakenstelsel in de praktijk](#) (release-onafhankelijk) en daarna van de context van voorliggende afspraken set ([Grondslagen](#) en het [Juridisch kader](#)). Deze drie delen samen vormen een goed beeld van de achtergrond bij en de reikwijdte van het afsprakenstelsel. De [Architectuur en technische specificaties](#), het [Normenkader informatiebeveiliging](#), het [Beleid](#), de [Operationele processen](#), de afspraken rond [Communicatie](#) en [Managementinformatie](#) beschrijven vervolgens per onderwerp de verschillende afspraken.

## Releaseinfo

In deze sectie is meta-informatie opgenomen over de release van de afsprakenet. De [release- en versiebeschrijving](#) duidt de positionering en status van deze publicatie. Wijzigingen ten opzichte van eerder gepubliceerde versies (en een historisch overzicht van wijzigingen) zijn opgesomd in de [changelog](#).

Lezers met suggesties voor toekomstige releases kunnen daarvoor gebruik maken van de hun ter beschikking staande communicatiekanalen met MedMij, of via <https://www.medmij.nl/contact/>.



## Release- en versiebeschrijving

### Doel

De releasebeschrijving beschrijft de belangrijkste kenmerken van de release. De versie betreft de versie van de release en duidt aan in welk stadium van ontwikkeling of besluitvorming de release zich bevindt. Een release die is vastgesteld door de Stichting MedMij heeft altijd versie 1.0. Hogere versienummers zijn alleen mogelijk als er documentatiecorrecties worden doorgevoerd. Inhoudelijke wijzigingen op een al vastgestelde release leiden altijd tot een nieuwe release. In het [Change- en releasebeleid](#) is beschreven hoe releases worden genummerd.

Release	1.2.0
Versie	1.0: Versie vastgesteld door het bestuur en de eigenaarsraad van Stichting MedMij.
Doel	Het bieden van de formele basis voor de eerste productiefase van MedMij, waarin het MedMij-netwerk operationeel zal zijn en dienstverlening aan de gebruikers plaatsvindt. Deelnemers sluiten een deelnemersovereenkomst af met de beheerorganisatie en committeren zich aan de afspraken.
Doelgroep	<ul style="list-style-type: none"> <li>• potentiële <i>Deelnemers</i> (<i>Dienstverleners</i> persoon en <i>Dienstverleners zorgaanbieder</i>)</li> <li>• <i>Deelnemers</i></li> <li>• alle onderdelen van de MedMij-organisatie (Stichting MedMij, programma MedMij, MedMij Beheer)</li> <li>• andere geïnteresseerden in het MedMij Afsprakenstelsel</li> </ul>
Totstandkoming	De ontwikkeling van release 1.1.2 tot release 1.2.0 is uitgevoerd onder leiding van de MedMij-beheerorganisatie, in samenwerking met de Deelnemersraad en de Eigenaarsraad van MedMij, de Stichting MedMij en een keur aan andere betrokkenen bij MedMij.
Inwerkingtreding	Per datum van publicatie.: 31 januari 2020
Operationeel toepassingsgebied	<ul style="list-style-type: none"> <li>• Allen die op 30 oktober 2020 <i>Deelnemer</i> aan MedMij zijn. Deze <i>Deelnemers</i> zijn gehouden release 1.2.0 te implementeren, zonder dat dit evenwel een heracceptatie vereist.</li> <li>• Allen die na 31 januari 2020 zullen starten met een MedMij-acceptatie. Die acceptatie zal conform <a href="#">Testbeleid</a> uitgevoerd worden tegen versie 1.1.2 of versie 1.2.0 van het Afsprakenstelsel.</li> <li>• De MedMij-beheerorganisatie.</li> </ul>
Status (september 2018)	Afsprakenstelsel geformaliseerd via vaststelling door Stichting MedMij.

Functionele scope	<p>In aanvulling op release 1.1.2, ondersteunt release 1.2.0:</p> <ul style="list-style-type: none"> <li>• aanpassingen aan het change- en release- beleid: 'dakpansgewijze uitrol';</li> <li>• abonneren op notificaties;</li> <li>• specifieke uitwerking van managementrapportages;</li> <li>• exporteren van portabiliteitsrapporten door DVP's</li> <li>• enkele verbeteringen van de beveiliging.</li> </ul> <p>Zie ook <a href="#">Changelog release 1.2.0</a>.</p>
Licentie	<p>Creative Commons: Naamsvermelding-GeenAfgeleideWerken 4.0 Internationaal (CC BY-ND 4.0).</p>

## Changelog

De changelog beschrijft de wijzigingen die achtereenvolgens zijn doorgevoerd bij releases van het MedMij Afsprakenstelsel.

## Changelog release 1.2

## Changelog release 1.2.0

Release 1.2.0 zal enkele veranderingen omvatten waarvoor *Dienstverleners persoon* en/of *Dienstverleners zorgaanbieder* hun oplossingen (zeker of eventueel) zullen moeten aanpassen om compatibel te blijven (backwards-incompatible changes). Het gaat om wijzigingen voor zowel *Dienstverleners zorgaanbieder* als *Dienstverleners persoon*.

- **Abonneren en notificeren** — Het MedMij Afsprakenstelsel gaat het abonneren op notificaties over *Gegevensdiensten* (voor *Verzamelen*) mogelijk maken. Er zijn twee nieuwe use cases met bijbehorende use case-implementaties: *Abonneren* en *Notificeren*. Er zijn drie nieuwe interfaces: het subscription interface, het resource notification interface en het subscription notification interface. De schema's van de *Zorgaanbiederslijst* en de *OAuthclientlist* zijn hierop aangepast. De functionaliteit is optioneel: *Deelnemers* die er geen gebruik van wensen te maken, kunnen zich beperken tot het kunnen verwerken van de nieuw gestructureerde lijsten.
- **Versionering van interfaces** — Alle interfaces krijgen een versie, behorend bij de versie van het MedMij Afsprakenstelsel waarin zij zijn gedefinieerd. Dat maakt het mogelijk om meerdere versies van hetzelfde interface naast elkaar actief te laten zijn op het MedMij-netwerk, bijvoorbeeld in overgangperiodes naar een nieuwe release van het MedMij Afsprakenstelsel. Het betekent o.a. dat *Dienstverleners zorgaanbieder* (actieve) versienummers gaan opgeven voor in de *Zorgaanbiederslijst* en *Dienstverleners persoon* voor in de *OAuthclientlist*.
- **Zorgaanbiedersnamen** — De maximale lengte van de *Zorgaanbiedersnaam* is vergroot; daarnaast is er een verplichting voor de *Dienstverlener zorgaanbieder* toegevoegd om bij toevoeging aan de *Zorgaanbiederslijst* een verklaring van de *Zorgaanbieder* over het opvoeren van een *Zorgaanbiedersnaam* te kunnen overleggen.
- **Portabiliteit tussen PGO's** — *Dienstverleners persoon* moeten de nieuwe *UC Portabiliteitsrapport* ondersteunen. Voor deze exportfunctionaliteit is een XML-schema opgenomen.
- **Beheerrapport** — Beheerrapportages moeten door alle *Deelnemers* gaan worden aangeleverd. Voor deze rapportages is een XML-schema opgenomen in het MedMij Afsprakenstelsel.
- **Structuur Zorgaanbiederslijst en OAuthclientlist** — Er komen nieuwe versies van de XML-schema's van de *Zorgaanbiederslijst* en de *OAuthclientlist*, om versionering van interfaces mogelijk te maken, en om abonneren en notificeren mogelijk te maken. Voorts moet in de *Zorgaanbiederslijst* gebruik gemaakt gaan worden van base-URLs, waar de *Dienstverlener zorgaanbieder* zijn Resource Server daarmee heeft geconfigureerd.
- **Verplichting client\_id in het token request** — Het `client_id` wordt een verplichte parameter in het token request. Deze verandering is al in release 1.1.2 voorbereid door *Dienstverleners zorgaanbieder*; zij accepteren sindsdien token request met én zonder `client_id`. In release 1.2.0 worden de twee laatste stappen gezet: *Dienstverleners persoon* nemen de `client_id` op in het token request, terwijl *Dienstverleners zorgaanbieder* token requests zonder `client_id` gaan weigeren.
- **Controle op ingetrokken certificaten** — De eisen aan het controleren op ingetrokken certificaten zijn verruimd; CRL en OCSP Stapling behoren nu ook tot de mogelijkheden.

Verder zijn de volgende belangrijke veranderingen in het MedMij Afsprakenstelsel aangebracht.

- **Releasebeleid** — MedMij gaat een dakpansgewijs releasebeleid voeren, waarin steeds twee releases tegelijk actief zijn op het MedMij-netwerk: een verplichte en een al gepubliceerde opvolger daarvan. Operationele processen, testbeleid en het beleid inzake gecontroleerde livegangen zijn hierop aangepast.
- **Ruimte voor andere authenticatiemiddelen dan DigiD** — Het MedMij Afsprakenstelsel gaat meer verantwoordelijkheid bij de *Zorgaanbieder* neerleggen, maar dus ook meer ruimte aan de *Zorgaanbieder* geven, om andere authenticatiemiddelen dan enkel DigiD te gebruiken.
- **Coördinatie, regie en uitwisseling** — In de architectuur van het MedMij Afsprakenstelsel worden drie hoofdfuncties van elkaar onderscheiden — *Regie*, *Uitwisseling* en *Coördinatie* — die gezamenlijk al het gedrag op de Processen-en-Informatie- en op de Applicatie-laag omvatten. Aan deze scheiding

worden acht architectuurbeginselen verbonden, die richting geven aan de ontwikkeling van het MedMij Architectuur in de toekomst. Zo kunnen *Deelnemers* beter anticiperen op die ontwikkeling met de architectuurkeuzes in hun implementaties.

- **Twee-factor-authenticatie** — De eisen aan *Dienstverleners persoon* inzake twee-factor-authenticatie zijn geëxpliciteerd.

## Changelog release 1.1

Changelog release 1.1 bevat de changelogs voor de (tussen)versies van release 1.1.

## Changelog release 1.1.2

Release 1.1.2 omvat enkele veranderingen waarvoor *Dienstverleners persoon* en/of *Dienstverleners zorgaanbieder* hun oplossingen (zeker of eventueel) zullen moeten aanpassen om compatibel te blijven (backwards-incompatible changes). Het gaat allereerst om twee zekere wijzigingen voor *Dienstverleners zorgaanbieder*.

- De *Authorization Server* gaat controleren of een *Client* wel erkend is op de *Gegevensdienst* waarvoor hij een authorization request doet. Daartoe wordt de *OAuthclientlist* uitgebreid met, per *OAuthclient*, de *Gegevensdiensten* waarop deze erkend is. Het XML-schema van de *OAuthclientlist* wordt dus aangepast. Gedurende de beperkte invoeringsperiode zijn de huidige en de nieuwe *OAuthclientlist* beide beschikbaar. Deze wijziging gaat ook de mogelijkheid bieden voor zogenoemde gecontroleerde livegangen.
- In release 1.1.2 gaan *Authorization Servers* ook access token requests accepteren met een *client\_id*. Indien aanwezig gaan zij die ook controleren. In release 1.1.1 was de *client\_id* verplicht afwezig in de access token request. Deze stap is een voorbereiding op de uiteindelijke verplichtstelling, in een volgende release, van de *client\_id* in de access token request.

Verder is er één eventuele backwards-incompatible wijziging voor *Dienstverleners persoon*.

- Ter bestrijding van de "open redirector" kwetsbaarheid wordt het verboden om URI's in de state-parameter op te nemen. *Dienstverleners persoon* die dat eventueel wel hadden gedaan zullen deze moeten verwijderen.

Daarnaast zijn er vijf backwards-incompatible wijzigingen, één zekere en vier eventuele, voor zowel *Dienstverleners persoon* als *Dienstverleners zorgaanbieder*.

- De interfaces voor het ophalen van de *Gegevensdienstnamenlijst*, *OAuthclientlist*, *Whitelist* en *Zorgaanbiederslijst* zullen geversioneerd worden. Hiermee wordt de invoering van wijzigingen in de XML-schema's van die lijsten vereenvoudigd, omdat tijdens migraties meerdere interfaces (en dus XML-schema's) naast elkaar in gebruik kunnen zijn. De bovenstaande wijziging inzake de *OAuthclientlist* geldt als eerste voorbeeld. Aan de bevraging van de lijsten zal een query-parameter met een releasenummer toegevoegd worden.
- De state-parameter is verplicht in de authorization request. Dat is in release 1.1.1 ook al zo, maar stond niet helder in de tekst verwoord. Omdat we ermee rekening houden dat daardoor de state-parameter niet overal is opgenomen, zien we het als een change. De kans is evenwel groot dat deze zeer beperkt tot geen aanpassingen gaat vragen.
- Als in de authorization request een ongeldige *redirect\_uri* wordt meegegeven is dat niet alleen een fout, maar moet deze fout bovendien niet via die ongeldige *redirect\_uri* worden teruggemeld, maar direct aan de eindgebruiker. Dit stond nog niet vermeld in release 1.1.1, maar is desondanks bij menige *Deelnemer* al wel zo geïmplementeerd. We verwachten ook hier daarom beperkte wijzigingen.
- In release 1.1.2 wordt voor alle *https*-verbindingen de daarvoor door IANA aangewezen poort (443) verplicht. In release 1.1.1 bestonden nog mogelijkheden om andere poortnummers te kiezen, ook bijvoorbeeld voor de endpointadressen in de *Zorgaanbiederslijst*, hoewel daarvan amper of geheel geen gebruik is gemaakt. Waar in release 1.1.2 in de *Zorgaanbiederslijst* nog poortnummers voorkomen, zal dat altijd het IANA-poortnummer zijn.
- In april van dit jaar heeft het NCSC een nieuwe versie van haar TLS-richtlijnen gepubliceerd. Het MedMij Afsprakenstelsel volgt deze. *Deelnemers* kunnen er nu voor kiezen ook TLS 1.3 te implementeren, maar alleen als ook TLS 1.2 nog wordt geboden. Tot zover is deze change backwards-compatible. Sommige TLS-algoritmen hebben in de nieuwe TLS-richtlijnen echter hun classificatie "goed" verloren. Mochten *Deelnemers* deze in gebruik hebben, moeten zij worden afgevoerd.



Verder zal release 1.1.2 een hoeveelheid veranderingen omvatten die geen aanpassingen vereisen van de oplossingen van *Dienstverleners persoon* en *Dienstverleners zorgaanbieder* (backwards-compatible changes). Het gaat om de volgende.

- Het gaat mogelijk worden dat een groep van (minstens één) *Dienstverleners persoon* en (minstens één) *Dienstverleners Zorgaanbieder* zich tijdelijk organiseren in een zogenoemde 'gecontroleerde livegang'. *Dienstverleners zorgaanbieder* betrekken een afgebakende groep *Zorgaanbieders*, hun klanten. *Dienstverleners persoon* kunnen naar keuze een afgebakende groep *Personen* daarbij organiseren. Elke gecontroleerde livegang gaat om één geldige *Gegevensdienst*, die in de *Catalogus* staat. In een gecontroleerde livegang kan het aanbieden van die *Gegevensdienst* door de genoemde *Zorgaanbieders* beproefd worden op het live MedMij-netwerk, gedurende een korte periode, zodanig dat alleen de deelnemende *Dienstverleners persoon* deze *Gegevensdienst* ook van deze *Zorgaanbieders* kunnen afnemen. Het doel is dat daarna de betreffende *Zorgaanbieders* volledig live gaan op die *Gegevensdienst*. Gecontroleerde livegangen worden mogelijk gemaakt zonder enige technische of functionele ingreep, maar enkel door een administratieve ingreep, namelijk door een tijdelijke administratieve kopie te maken van de betreffende *Gegevensdienst*.
- In release 1.1.2 wordt naast het SAML-koppelvlak ook het CGI-koppelvlak van DigiD toegestaan, onder de kanttekening dat voor DigiD het SAML-koppelvlak de toekomstvast keuze is.
- Op drie punten is de beschrijving van de flow aan het eind van *UCI Verzamelen* en *UCI Delen* verbeterd: het is mogelijk om onmiddellijk na ontvangst van een access token tot gebruikersinteractie over te gaan, na optreden van een uitzondering hoeft de herhaling niet onderbroken te worden en er kan sprake zijn van herhaalde resource requests in meer situaties dan oorspronkelijk vermeld.
- De ordening van de verantwoordelijkheden op de Applicatie-laag heeft een ingrijpend nieuwe opzet gekregen, langs de lijnen van interfaces. Dit verbetert het overzicht en opent de mogelijkheid voor versionering van interfaces in de toekomst. Tegelijkertijd zijn de adresseringsverantwoordelijkheden verhelderd.
- In het normenkader:
  - is het toetsingskader nu in de hoofdttekst opgenomen, in plaats van in bijgevoegde documenten. Dat geldt ook voor de aanvullende auditverklaring, die in de hoofdttekst gegenereerd kan worden;
  - zijn drie normen toegevoegd en hebben drie normen toevoegingen gekregen. Bestaande aanvullende auditverklaringen blijven echter van kracht;
  - zijn enkele normen (door opdeling of samenvoeging) herordend;
  - is de tekst van enkele normen verduidelijkt;
- De beschrijving van de (limitatief) toegestane informatie-inhoud van het access token is verbeterd. Toegelicht is bovendien dat, en waarom, OpenID Connect niet wordt toegepast op het koppelvlak van *UCI Verzamelen* en *UCI Delen*.
- Toegelicht is dat, en waarom, OCSP Stapling vooralsnog niet wordt toegepast.
- Toegelicht is wat met een "full" redirect\_uri wordt bedoeld.
- Een keur aan kleinere tekstuele verbeteringen is doorgevoerd.

Release 1.1.2 wordt op 4 oktober 2019 gepubliceerd. Deelnemers worden geacht de op hen betrekking hebbende wijzigingen door te voeren, niet eerder dan na publicatie en niet later dan op 31 december 2019.

*Dienstverleners Zorgaanbieder* dragen zelf de verantwoordelijkheid om, wanneer zij eerder dan 31 december 2019 deelnemen aan een gecontroleerde livegang, tijdig de eerste hierboven genoemde wijziging te hebben doorgevoerd: controle van authorization request op basis van nieuwe *OAuthclientlist*. Zo lopen zijzelf en de andere partijen in die gecontroleerde livegang niet het risico onbedoelde *PGO Servers* toegang tot de (kopie-) *Gegevensdienst* van de gecontroleerde livegang te geven.

## Changelog release 1.1.1

De belangrijkste wijzigingen in deze release zijn:

### Architectuur en technische specificaties

- Opgenomen op de [Netwerk](#)-pagina dat de *Whitelist*-controle, onder bepaalde condities, ook na afronding van de TLS-handshake mag worden uitgevoerd.
- Pagina met toelichtingen afspraken set release 1.1 verwerkt in hoofdttekst [Architectuur en technische specificaties](#):
  - Applicatierollen en hun getalsverhoudingen;
  - Bedoeling van de beschikbaarheids- en de ontvankelijkheidstoets.
  - Eisen van DigiD inzake uitloggen.
  - G2- en G3-certificaten van PKIoverheid.
- Toelichting op betekenis start- en einddatum van een *Gegevensdienst* toegevoegd ([Metamodel](#)).
- Verschillende kleine aanpassingen doorgevoerd in het [Metamodel](#):
  - Samenstelling van de gegevensdienstnaam nader gedefinieerd.
  - Attribuut 'Vervangt' toegevoegd aan klasse Gegevensdienst.
- [Beschikbaarheid](#)- en [ontvankelijkheidstoets](#) opnieuw geformuleerd als beschikbaarheids- en ontvankelijkheidsvoorwaarde. Moment van van kracht worden gerelativeerd: tussen een vroegste en laatste moment.
- Nieuwe element (OAuth scope) mogelijk gemaakt als inhoud van access token. Custom HTTP header `medmijscope`: verwijderd.

#### Structuurwijzigingen catalogus n.a.v. release 1.1.1

De *Catalogus* is geen onderdeel van de afspraken set en kent haar eigen releasecyclus. Bovenstaande wijzigingen hebben echter wel op de volgende manier impact op de structuur van de *Catalogus*:

- Patchnummers verwijderd uit *Gegevensdienstnaam* en *Systeemrolcodes*.
- Kolom 'Vervangt' toegevoegd om opvolging van gegevensdiensten te kunnen aangeven.

De wijzigingen zijn ondertussen doorgevoerd.

### Normenkader informatiebeveiliging

Op basis van terugkoppeling uit eerste lopende audittrajecten is verduidelijking aangebracht in het normenkader:

- Eis aan het certificaat over de scope is geschrapt. De beoordeling van de MedMij scope wordt duidelijk uit de beoordeling van het normenkader.
- Toegevoegd dat verwacht wordt dat dezelfde eisen gesteld worden aan de uitvoerend auditor door de CBI als voor de afgifte van het NEN 7510 certificaat.
- In Beoordelingskader verduidelijking aangebracht in de auditmethode op diverse normen. Op basis hiervan zijn tevens enkele normen tekstueel verduidelijkt.
- Norm A.12.3.1 Back-up van informatie: toegevoegd dat deze ook voor de *Dienstverleners zorgaanbieder* geldt.
- Norm A.9.4.1 Beperking toegang tot informatie: aangegeven dat deze alleen voor de *Dienstverlener persoon* geldt.
- Rapportageformat auditverklaring: versie afsprakenstelsel aangepast.

### Beleid

- Gegevensdienstenbeleid: tekst onder kopje 'Mutaties van gegevensdiensten' aangepast.
- OAuthclient-namenbeleid: eis "dat de naam in het verleden niet door een andere *Dienstverlener* *persoon* gebruikt mag zijn" verwijderd.
- Verwijzing naar uitvoeringsorganisatie consequent vervangen naar Stichting MedMij. Onderscheid is voor het afsprakenstelsel niet relevant.

## Communicatie

- Toestemmings- en bevestigingsscherm: verduidelijkt dat de HTML- en CSS-bestanden enkel de tekst en vormgeving beschrijven. De *Dienstverlener zorgaanbieder* blijft verantwoordelijk voor alle overige aspecten, zoals beveiliging van de webpagina.

## Changelog release 1.1 versie 1.0

De versie van release 1.1 zoals vastgesteld door bestuur en eigenaarsraad van Stichting MedMij. De wijzigingen ten opzichte van versie 0.9 zijn:

- [Normenkader informatiebeveiliging](#): rapportageformat en beoordelingskader normenkader toegevoegd.
- [Toelichting AVG-normen](#): links naar formats gegevensbeschermingseffectbeoordelingen toegevoegd.
- Pagina known issues niet meer opgenomen: in overleg met de governancestructuur MedMij Afsprakenstelsel wordt prioriteitstelling bepaald.

## Changelog release 1.1 versie 0.9

### Afsprakenstelsel versus afsprakenstelsel

Met ingang van deze versie is een duidelijker onderscheid gemaakt tussen de verschillende onderdelen van het afsprakenstelsel. Het totaaloverzicht is te vinden bij de [Introductie](#) op het afsprakenstelsel. Deze changelog behandelt enkel de wijzigingen in de afsprakenstelsel. Wijzigingen in de overige onderdelen van het stelsel, zoals de deelnemersovereenkomsten en de catalogus, vinden niet releasematig plaats en zijn daarmee geen onderdeel meer van de changelog.

De belangrijkste wijzigingen in deze versie zijn:

### Grondslagen

- Definitie van Zorgaanbieder aangescherpt.
- Principe toegevoegd: "Aan de persoonlijke gezondheidsomgeving zelf worden eisen gesteld." (ter vervanging van Principe 8)
- Principe toegevoegd: "Afspraken worden aantoonbaar nageleefd en gehandhaafd."
- Principe toegevoegd: "Het afsprakenstelsel snijdt het gebruik van normen en standaarden op eigen maat."

### Juridische context

- De juridische context bestaat nu uit diverse toelichting op de juridische context van handelen door deelnemers aan het MedMij Afsprakenstelsel. Op de beginpagina is beschreven waar die toelichting, en daarmee met name advisering en ondersteuning aan deelnemers, uit bestaat.
- Er is een pagina toegevoegd met verantwoordelijkheden en normen vanuit de AVG. Deelnemers hierin ondersteund met informatie over verplichtingen die zij zelfstandig dienen te implementeren conform deze wetgeving en waarvan MedMij het belangrijk vindt dat deelnemers deze kennen. Dit was tevens een aanbeveling in de uitgevoerde PIA.
- In het juridisch kader zijn beschrijvingen van wet- en regelgeving geüpdatet. Tevens zijn bevindingen uit de PIA verwerkt, met name tekstueel.

### Deelnemersovereenkomsten

- De onderwerpen waar de overeenkomst op toeziet zijn geüpdatet naar aanleiding van de laatste wijzigingen in deze release.
- Artikelen onder 5 met betrekking tot doel van de gegevensverwerking zijn aangepast naar de scope van het MedMij Afsprakenstelsel.
- De overeenkomst is meer wederkerig gemaakt tussen deelnemers en de stichting.
- Enkele definities zijn aangescherpt.
- Verwerking van aanbevelingen vanuit een uitgevoerde PIA, met name tekstueel.

### Model verwerkersovereenkomst

- Eis verscherpt dat verwerking van data in de EU en conform EU wetgeving moet plaatsvinden door verwerkers in artikel 3.10 en 6.2.

### Architectuur en technische specificaties

#### Laagoverstijgend

- Verduidelijkt dat een hostname altijd een fully qualified domain name is en dat wildcards niet zijn toegestaan op de whitelist.

### *Applicatie*

- Verplicht gebruik GET-methode bij authorization request toegevoegd.
- Gebruik UUID vervangen door generieke eisen aan de tokens. (UUID mag niet meer gebruikt worden als enkel ID van het token.)
- Verplicht gebruik Authorization Request Header Field toegevoegd.
- Maximale duur gebruik lijsten voorgeschreven in situatie dat MedMij Registratie onbereikbaar is.
- Technische adressering MedMij Registratie toegevoegd.
- Toelichting op relatie tussen Authorization Server en Resource Server verduidelijkt.
- Verantwoordelijkheid voor afwezigheid van BSN's in de content van gegevensdiensten verwijderd.
- AuthorizationEndpoint hoeft niet meer aan één Zorgaanbieder gekoppeld te zijn. Zorgaanbiedernaam en Gegevensdienst moeten worden meegegeven in de scope-parameter van het OAuth-request.
- ResourceEndpoint hoeft niet meer aan één zorgaanbieder gekoppeld te zijn. De Zorgaanbiedernaam en Gegevensdienst moeten worden meegegeven in een custom-HTTP-header.

### *Netwerk*

- ZA Node gekoppeld aan één deelnemer.

### *Informatiemodellen*

- Informatiemodellen opnieuw geordend.
  - Scheiding aangebracht tussen conceptueel model en logische modellen. Logische modellen geïntroduceerd.
  - Relatie tussen conceptueel model en logische modellen enerzijds en XML-schema's anderzijds aangescherpt (resultierend in enkele wijzigingen in de schema's en de toelichting erop).
- Diverse modelmatige verbeteringen, waarvan de belangrijkste zijn:
  - Stringtypes vervangen door basisklassen.
  - Transactie vervangen door Systeemrol als primaire component van Transactieverzameling.
  - Gegevensdienst gekoppeld aan één use case.
  - Informatiestandaard toegevoegd.
  - Geldigheidsperiode aan Gegevensdienst toegevoegd.
  - Identificerende naam van gebruiksvriendelijke naam voor Gegevensdienst onderscheiden.
  - Afhankelijkheid tussen Gegevensdiensten mogelijk gemaakt.

### **Normenkader informatiebeveiliging**

- Op basis van een consultatie met auditors op versie 0.8 zijn enkele normen verder verduidelijkt of voorzien van een link naar ondersteunende documentatie.
- De toelichting is verplaatst naar het privacy- en informatiebeveiligingsbeleid.

### **Beleid**

- Dienstverleningsoverdrachtsbeleid toegevoegd.
- Beschrijving van de mogelijke mutaties van gegevensdiensten toegevoegd in het Gegevensdienstenbeleid.
- Informatieclassificatiebeleid toegevoegd.
- Performancebeleid toegevoegd.
- Beschrijving van de jaarlijkse stelselbrede risico-analyse onder privacy- en informatiebeveiligingsbeleid toegevoegd.
- Change en releasebeleid aangescherpt.
- Gegevensdienstenbeleid aangescherpt.
- Kwalificatie- en acceptatiebeleid vervangen door testbeleid.
- In OAuthclient-namenbeleid opgenomen dat OAuthclient-naam gelijk moet zijn aan een handelsnaam van de Dienstverlener persoon in het handelsregister.

- Aan het privacy- en informatiebeveiligingsbeleid is een pagina toegevoegd met achtergrond over de risicoanalyse die mede bepalend is voor diverse maatregelen op het gebied van informatiebeveiliging in het MedMij Afsprakenstelsel, zoals in de architectuur en technische specificaties of het aanvullend normenkader.

#### **Operationele processen**

- Proces erkenning als aanbieder van gegevensdienst toegevoegd.
- Proces beheren technische kwetsbaarheden toegevoegd.

#### **Communicatie**

- Paragraaf 'Uitingsvormen van het merk' gewijzigd.

#### **Managementinformatie**

- Afspraak over aanleveren managementinformatie over performance resource server door Dienstverlener zorgaanbieder verwijderd.

## Changelog release 1.1 versie 0.8

De belangrijkste wijzigingen in deze versie zijn:

### Grondslagen

- Aangepast: Doelstelling 7 verfijnd.
- Toegevoegd: Principes "Uitwisseling is een keuze", "Het MedMij-netwerk is gebruiksrechten-neutraal" en "De burger regisseert zijn eigen gezondheidsinformatie als uitgever".
- Toegevoegd: Deelnemers behandelen elkaar onderling gelijk (bij principes).
- Toegevoegd: Vrij verkeer over het MedMij-netwerk (deelnemers brengen elkaar geen kosten in rekening) (bij principes).

### Juridisch kader

- Toegevoegd: Wet gelijke behandeling op grond van handicap en chronische ziekte (wgbh/cz) toegevoegd als belangrijk kader voor leveranciers om toegankelijke toepassingen te realiseren.
- Toegevoegd: Verdere verduidelijking zienswijze van MedMij op de verwerkingsverantwoordelijkheden in het stelsel als toelichting op de AVG, evenals een aparte pagina bij het juridisch kader.
- Toegevoegd: Aanvullingen op de toelichting inzake de AVG en WGBO gezien vanuit de nieuwe UC Delen.

### Overeenkomsten en rechtsrelaties

- Gewijzigd: Bètaovereenkomsten gelden niet meer, er zijn Deelnemersovereenkomsten voor productiesituatie teruggekomen.
- Toegevoegd: In de Deelnemersovereenkomsten: een bepaling over de operationele processen en samenwerkingsafspraken en een bepaling over het niet rekenen van onderlinge vergoedingen voor gegevensuitwisseling.
- Toegevoegd: Zelfverklaring integriteit.
- Toegevoegd: In de Modelverwerkersovereenkomst is rekening gehouden met de verwerkingsverantwoordelijkheden die voortkomen uit UC Delen.

### Architectuur en technische specificaties

#### *Correctie*

- Aangepast: De positie van 'controleer beschikbaarheid' in de UC en UCI Verzamelen in lijn gebracht met de tekst.

#### *Doorontwikkeling*

- Aangepast: Catalogus losgekoppeld van afspraken en verwijzing opgenomen.
- Aangepast: De stelselnode wordt niet opgenomen op de whitelist.
- Aangepast: Altijd 'goede' (volgens NCSC) TLS-versies en -algoritmen voor front-channelverkeer vereist.
- Aangepast: Verwijzing naar NEN7513:2018 (specifieke versie) ingevoegd, en verantwoordelijkheid over logging aangepast zodat de positie van NEN7513 duidelijker is
- Toegevoegd: Gegevensdienstnamenlijst (use case, use case-implementatie, relatie met overige use cases).
- Toegevoegd: Service levels van MedMij Registratie, de Authorization Server en de Resource Server.
- Toegevoegd: Verantwoordelijkheid om gebruik te maken van DNSSEC.
- Toegevoegd: Verantwoordelijkheid om voldoende onvoorspelbaarheid van UUID's te waarborgen.
- Toegevoegd: Verantwoordelijkheid dat als OCSP-responder onbereikbaar is, TLS-sessie niet tot stand komt.



- Toegevoegd: Use case en use case-implementatie Delen.
- Toegevoegd: De 'scheme' bij adressering moet altijd uit kleine letters bestaan.
- Toegevoegd: Verantwoordelijkheid voor beheerorganisatie om historie van lijsten te bewaren.
- Toegevoegd: Aantekenen Bron en Gegevensdienst door Uitgever bij verzamelde gegevens.
- Toegevoegd: Eisen aan de syntax van de hostname.
- Toegevoegd: Uitzonderingssituatie: na authenticatie constateert dienstverlener zorgaanbieder dat persoon jonger is dan 16 jaar.
- Toegevoegd: Verantwoordelijkheid voor deelnemers om elkaar onderling gelijk te behandelen.

#### *Verduidelijking*

- Aangepast: Beschrijving van de wijze waarop de whitelistcontrole plaats moet vinden bij inkomend en uitgaand verkeer.
- Aangepast: Netwerk-laag is opnieuw beschreven. Relatie tussen Netwerk en Applicatie-laag is opnieuw vormgegeven.
- Aangepast: De te nemen beveiligingsmaatregelen uit RFC6819 zijn toegankelijk en specifiek vermeld.
- Aangepast: Rol PGO User Agent is gesplitst in PGO User Agent en PGO Presenter.
- Toegevoegd: Verantwoordelijkheid om nog korte tijd bereikbaar te zijn na uitfasering van de ZorgaanbiederGegevensdienst in de ZAL.
- Toegevoegd: Eis van betekenisloosheid van tokens in het MedMij-netwerk.
- Toegevoegd: Hanteren two-way TLS-handshake voor back-channelverkeer.
- Toegevoegd: Verantwoordelijkheid voor beheerorganisatie om geen verlopen entries in ZAL te publiceren.
- Toegevoegd: Hostname mag voorkomen als CN of als SAN.

#### **XML-schema's**

- Aangepast: Modellerings van het complexType MedMijNode in lijn gebracht met het metamodel.
- Toegevoegd: Gegevensdienstnamenlijst (XSD en XML-voorbeeldbestand).
- Toegevoegd: Eisen aan de XML-lijsten.

#### **Normenkader informatiebeveiliging**

- Gewijzigd: bij alle normen een rationale toegevoegd en de weging voor de auditor verwijderd.
- Gewijzigd: op basis van een hernieuwde risicoanalyse op het stelsel en een consultatie met auditors zijn normen verduidelijkt, toegevoegd of verwijderd.

#### **Governance**

##### *Beleid*

- Gewijzigd: positie beleid verduidelijkt op pagina Beleid.
- Gewijzigd: Zorgaanbiedersnamenbeleid aangescherpt.
- Gewijzigd: Toezicht- en handhavingsbeleid aangepast naar Nalevingsbeleid en nader uitgewerkt.
- Gewijzigd: Privacy- en informatiebeveiligingsbeleid aangescherpt.
- Gewijzigd: Toetredingsbeleid uitgebreid.
- Gewijzigd: Klachten- en geschillenbeleid nader uitwerkt.
- Toegevoegd: OAuthclient-namenbeleid toegevoegd.
- Toegevoegd: Samenwerkings- en escalatiebeleid.
- Toegevoegd: Gegevensdienstenbeleid.
- Toegevoegd: Kwalificatie- en acceptatiebeleid.

##### *Operationele processen*

- Gewijzigd: Operationele processen uitgebreid en nader uitwerkt.

### **Communicatie**

- Gewijzigd: Uitgangspunten Merkgebruik nader uitgewerkt.
- Gewijzigd: Toestemmingsverklaring verbeterd en in lijn gebracht met de architectuur.
- Gewijzigd: Gebruikersvoorlichting losgekoppeld van afspraken set en verwijzing opgenomen.
- Toegevoegd: Bevestigingsverklaring voor gebruik in UC Delen.

### **Managementinformatie**

- Toegevoegd: Beschrijving van de managementinformatie die periodiek door de deelnemer moet worden aangeleverd.

## Changelog release 1.0

Changelog release 1.0 bevat de changelogs voor de (tussen)versies van release 1.0.

## Changelog release 1.0 versie 1.0

Release 1.0 versie 0.991 vastgesteld door bestuur en eigenaarsraad Stichting MedMij. Geen inhoudelijke wijzigingen.

## Changelog release 1.0 versie 0.991

De belangrijkste wijzigingen in deze versie zijn:

### Architectuur en technische specificaties

- Gewijzigd: uitzondering 2, 3 en 4 in de UC en UCI Verzamelen leiden nu tot dezelfde terugkoppeling naar de PGO Server. Daarmee kan de PGO Server niet langer afleiden of er mogelijk een behandelrelatie bestaat tussen de zorgaanbieder en de persoon, voordat de persoon toestemming heeft gegeven om gegevens te delen met de PGO Server.
- Gewijzigd: de terugkoppeling in uitzondering 1 in de UC en UCI Verzamelen vindt plaats naar de PGO Server en niet naar de Zorggebruiker; hiermee wordt aangesloten bij de OAuth-specificaties.
- Toegevoegd: in de toelichting is opgenomen dat de in de UC en UCI's benoemde uitzonderingen in de autorisatieflow aanvullend of verdiepend zijn ten opzichte van de OAuth-specificaties; daarin benoemde uitzonderingssituaties moeten conform de standaard geïmplementeerd worden.

### XML-schema's

- Toegevoegd: XML-voorbeeldbestanden.
- Toegevoegd: ontwerpafwegingen.
- Verwijderd/gewijzigd: basisschema. De relevante elementen zijn nu opgenomen in de afzonderlijke XSD's van de lijsten.
- Gewijzigd: pattern HostnameType.
- Toegevoegd: patterns op BackchanneluriType en FrontchanneluriType.
- Toegevoegd: verplichte aanduiding tijdzone bij tijdstempel.
- Gewijzigd: opbouw van de namespace-URI.
- Gewijzigd: een van de elementen "Systeemrol" hernoemd naar "Systeemrolcode".
- Toegevoegd: controle op uniciteit van sleutelementen.
- Gewijzigd: release- en versienummering.

### Normenkader

- Gewijzigd: certificeringseisen NEN 7510 aangescherpt. Alleen Conformiteit Beoordelende Instellingen die NEN 7510 geaccrediteerd zijn door de Raad voor Accreditatie of een NEN 7510 licentieovereenkomst hebben met NEN mogen de certificering afgeven.

## Changelog release 1.0 versie 0.99

De belangrijkste wijzigingen in deze versie zijn:

### Architectuur en technische specificaties

- Toegevoegd: XML-producten voor de Zorgaanbiederslijst, de whitelist en de OAuth Client List.
- Toegevoegd: nadere afspraken over de technische adressering van endpoints en de opbouw van OAuth-URI's.
- Gewijzigd: uitbreiding en verbetering van het metamodel en de bijbehorende invarianten en stringtypes.
- Gewijzigd: relatie tussen de componenten op de applicatielaag enerzijds en de netwerklaag anderzijds.
- Gewijzigd: term "gateway" vervangen door de afzonderlijke componenten op de applicatielaag.
- Toegevoegd: afspraken over logging.
- Gewijzigd: whitelist is gesplitst in een whitelist en een OAuth Client List.
- Gewijzigd: frequentie van het ophalen van de ZAL, OAuth Client List en whitelist verhoogd.

### Governance

- Gewijzigd: eisen waaraan zorgaanbiedersnamen moeten voldoen.
- Verwijderd: proces opvragen en consolideren logging.

### Communicatie

- Gewijzigd: accessibility toestemmingsverklaring bètaversiefase verbeterd.

## Changelog release 1.0 versie 0.9

De belangrijkste wijzigingen in deze versie zijn:

### Grondslagen

- Gewijzigd: de tekst rond de optie van centrale voorzieningen om barrières te overwinnen is verduidelijkt en uitgebreid zodat het ook de keuze voor decentrale voorzieningen voor de aansluiting van zorgaanbieders op het MedMij-netwerk omvat.
- Gewijzigd: de begrippenlijst is ingekort en beschrijft nu enkel de belangrijkste begrippen die relevant zijn voor de grondslagen.

### Juridisch kader

- Toegevoegd: data van publicatie van toegepaste wetsartikelen.
- Gewijzigd: wet cliëntenrechten bij elektronische verwerking van gegevens in de zorg is opgenomen in de Wet gebruik burgerservicenummer in de zorg (Wet BSN-z). Toelichting op beide wetten in het juridisch kader zijn daarom samengenomen en de Wet BSN-z heeft een nieuwe titel gekregen, namelijk de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (Wabvpz).
- Gewijzigd: beschrijving van de relatie met de AVG is aangepast.

### Overeenkomsten

- Gewijzigd: nieuwe introductie op de overeenkomstenstructuur met een toelichting op de verschillende rechtsrelaties.
- Toegevoegd: in deelnemersovereenkomsten en verwerkersovereenkomst opgenomen dat alleen gegevens over personen ouder dan 16 jaar worden verstrekt.
- Toegevoegd: artikel met afspraken rond uittreding van een deelnemer (7.5).
- Gewijzigd: uitbreiding artikelen met betrekking tot het intellectueel eigendom (11).
- Toegevoegd: de verplichting om minimaal één gegevensdienst aan te bieden.

### Architectuur en technische specificaties

- Gewijzigd: beperking van de Juridica-laag tot alleen de rollen.
- Gewijzigd: restyling en detaillering van de totaalplaat en de platen per laag.
- Gewijzigd: detaillering op vele aspecten op alle lagen.
- Toegevoegd: grondige uitbreiding van de toelichtingen op de keuzes.
- Gewijzigd: strakkere ordening van het setje use cases en use case-implementaties.
- Toegevoegd: mitigatie van beveiligingsrisico's van het OAuth-protocol.
- Toegevoegd: eerste versie van een (logisch) metamodel.
- Toegevoegd: werken met PKI-overheid-servercertificaten voor versleuteling en authenticatie van gateways.
- Gewijzigd: opzet van de gegevenscatalogus.
- Toegevoegd: enkele gegevensdiensten.
- Verwijderd: use cases rond registratie (vervangen door operationele processen).
- Gewijzigd: OCSP in plaats van CRL voor controle geldigheid certificaten.

### Normenkader informatiebeveiliging

- Toegevoegd: beschrijving van manier van toetsing van de normen.
- Gewijzigd: introductie op de opzet en bedoeling van het normenkader.

### Governance

- Gewijzigd: inrichting Stichting MedMij.

- Gewijzigd: beleid op de volgende onderwerpen:
  - Toetreding: op termijn beschrijvingen verwijderd;
  - Klachten en geschillen: op termijn beschrijvingen verwijderd;
  - Change en release: passend gemaakt bij inrichting Stichting MedMij en aanduiding releases veranderd.
- Toegevoegd: zorgaanbiedersnamenbeleid.
- Verwijderd: op termijn beschrijving van inrichting governance.
- Toegevoegd: overzicht van de operationele processen waarbij deelnemers een rol spelen.

## **Communicatie**

- Toegevoegd: aangepast scherm voor de verkorte toestemmingsverklaring.



## Changelog release 1.0 versie 0.8

De belangrijkste wijzigingen in deze versie zijn:

### Grondslagen

- Gewijzigd: onderscheid gemaakt in gegevensdienstonafhankelijke en gegevensdienstafhankelijke afspraken.
- Verwijderd: de beschrijving van de interacties op hoofdlijnen rond het verkrijgen van nieuwe gegevens zodra deze bij de zorgaanbieder beschikbaar komen. Dit laat ruimte om dit in latere releases goed uit te werken.

### Juridisch kader

- Toegevoegd: bij de toepassing van de AVG informatie over dataportabiliteit toegevoegd.
- Toegevoegd: bij de toepassing van de wet Gebruik Burgerservicenummer in de Zorg tekst toegevoegd. Vanaf: "In het geval ...".
- Toegevoegd: aanpassingswet richtlijn inzake elektronische handel opgenomen.
- Toegevoegd: implementatiewet richtlijn consumentenrechten opgenomen.
- Toegevoegd: aansprakelijkheid wederom opgenomen. Dit dient nog verder uitgewerkt te worden.

### Overeenkomsten

- Gewijzigd: specifieke deelnemersovereenkomsten opgenomen voor de bètaversiefase (bètaversieovereenkomsten).
- Toegevoegd: toestemmingsverklaring bètafase opgenomen.
- Toegevoegd: modelverwerkersovereenkomst zorgaanbieder - dienstverlener zorgaanbieder MedMij opgenomen.
- Gewijzigd: tekst bij de pagina Overeenkomsten is herschreven. De basis hiervoor stond eerst op de pagina Juridica.

### Architectuur en technische specificaties

- Gewijzigd: architectuurplaten. In een matrixmodel zijn de rollen, processen en informatie in de verschillende lagen met elkaar in verbinding gebracht.
- Gewijzigd: teksten omgezet naar de vorm: rolbeschrijvingen en verantwoordelijkheden (afspraken met toelichtingen).
- Gewijzigd: solutions als bijlagen opgenomen in de vorm van usecases.
- Gewijzigd: use cases herschreven naar een nieuw format: flow, beschrijving processtappen, specificatie informatie en soms voorbeelden ter toelichting:
  - UC Registreren;
  - UC Opvragen zorgaanbiederslijst;
  - UC Verzamelen;
- Toegevoegd: afspraken over logging;
- Toegevoegd: model en eerste vulling van de gegevenscatalogus;
- Toegevoegd: use case implementaties bij de use cases op de laag Applicatie.

### Normenkader informatiebeveiliging

- Toegevoegd: normenkader met overzicht van informatiebeveiligingsmaatregelen.

### Governance

- Toegevoegd: inrichting van de governance uitgewerkt. Hierbij is onderscheid gemaakt tussen een inrichting voor de bètaversiefase en een inrichting op termijn.

- Toegevoegd: het beleid is uitgewerkt op de volgende onderwerpen:
  - Toetreding;
  - Toezicht en handhaving;
  - Klachten en geschillen;
  - Change en release;
  - Privacy en veiligheid;
  - Intellectueel eigendom.

## **Communicatie**

- Toegevoegd: communicatiehandboek met daarin afspraken over de manier waarop het merk MedMij mag worden gehanteerd.
- Gewijzigd: de gebruikersvoorlichting is aangepast en verplaatst naar communicatie. Bij zowel de Gebruikersvoorlichting persoon als de Gebruikersvoorlichting zorgaanbieder is een stuk tekst opgenomen omtrent de bèta-versiefase.
- Gewijzigd: bij de Gebruikersvoorlichting persoon is tevens een stuk tekst opgenomen omtrent algemene rechten, zoals het recht op rectificatie en het recht op vergetelheid.

## Changelog release 1.0 versie 0.3

Versie 0.3 van het Afsprakenstelsel MedMij is de eerstvolgende versie voor publicatie buiten het programma MedMij na versie 0.1. De 0.2 versie diende voor interne doeleinden. De 0.3 versie is een tussenversie op weg naar een 0.9 versie. De publicatie van deze 0.3 versie is bedoeld om een terugkoppeling te geven over de verwerking van de marktconsultatie op de 0.1 versie, onder begeleiding van Nederland ICT en OIZ. Het is tevens bedoeld als input voor een proof of concept (POC) fase in samenwerking met Zorgverzekeraars Nederland en het programma gespecificeerde toestemming (GTS). In deze POC worden de beschreven usecases verder uitgewerkt en getoetst waarbij ook gekeken wordt naar de toepassing van enkele centrale voorzieningen die nodig zijn in de werking van het afsprakenstelsel en GTS. Middels deze activiteiten wordt het afsprakenstelsel verder doorontwikkeld. Tussenresultaten worden voortdurend teruggekoppeld via de werkgroepenstructuur van het programma MedMij. Via die weg kunnen diverse belanghebbenden bij het afsprakenstelsel dan ook hun reactie geven op deze documentatie. Verder dient deze versie als startdocument voor een uit te voeren risicoanalyse naar informatiebeveiliging op basis waarvan het normenkader beveiliging voor het afsprakenstelsel ontwikkeld kan worden.

### Wijzigingen of aanvullingen in de uitgangspunten

- De definitie van het 'Minimum Viable Product' waarmee het afsprakenstelsel in de bètaversiefase live gaat (versie 1.0) is op hoofdlijnen beschreven.
- Het centrale kenmerk van het afsprakenstelsel – “decentrale operatie, centraal vertrouwen” – is beschreven.

### Wijzigingen of aanvullingen in de overeenkomsten

- Deelnemersovereenkomsten zijn samengevoegd tot één overeenkomst om de leesbaarheid van het geheel te vergroten. Artikel 3 is voor de verschillende rollen specifiek. Deelnemers krijgen wel een eigenstandige overeenkomst voor de rol waarin zij deelnemen ter ondertekening.
- Deelnemer is gebonden aan Nederlands recht (artikel 3, lid 2 dienstverlener persoon; artikel 3 lid 2 dienstverlener zorgaanbieder)
- Vereisten omtrent screening van personeel (artikel 3, lid 3 dienstverlener persoon; artikel 3 lid 3 dienstverlener zorgaanbieder)
- Vereisten rondom verplichtende kader model bewerkersovereenkomst (artikel 3, lid 10 dienstverlener persoon; artikel 3 lid 11 dienstverlener zorgaanbieder)
- Aanspreekbaarheid van de deelnemer voor de gebruiker vastgelegd (artikel 3, lid 11 dienstverlener persoon; artikel 3 lid 12 dienstverlener zorgaanbieder)
- Vereisten rondom het verlenen van medewerking om tot oplossingen te komen bij netwerkfalen (artikel 5, lid 2)
- Verwijzing naar het operationeel handboek opgenomen omtrent het handelen bij incidenten, calamiteiten en crisissituaties (artikel 6, lid 3)
- Verwijzing naar de Algemene verordening gegevensbescherming; was voorheen Wet bescherming persoonsgegevens (artikel 7, lid 1)
- Vereisten rondom toestemming voor alle partijen vastgelegd in de deelnemersovereenkomst (artikel 7, lid 3 en 4)
- Vereisten rondom logging vastgelegd in de deelnemersovereenkomst (artikel 7, lid 9)
- Gebruiksrecht MedMij zoals omschreven in de overeenkomst; was conform artikel 7, lid 2 (artikel 9, lid 3)
- Toevoeging artikel 10, lid 2
- Toevoeging verwijzing naar het proces uittreden in het operationeel handboek (artikel 11, lid 3)
- Vereisten rondom In het geval de deelnemer van juridische status verandert (artikel 15, lid 4)

### Wijzigingen of aanvullingen in het juridisch kader

- Relevante elementen uit de EGIZ opgenomen

- Bewerkers/verantwoordelijke-relatie tussen dienstverlener zorgaanbieder en de zorgaanbieder nader uitgewerkt
- Wbp termen vervangen voor de AVG termen.
- Verwijzingen naar verschillende relevante AVG documentatie opgenomen.
- Verwijzingen naar gebruikersovereenkomst vervangen door gebruikersvoorlichting.
- Wet kwaliteit, klachten en geschillen zorg verwijdt uit het juridisch kader.
- Verordening (EU) 2017/745 van het Europees parlement en de Raad betreffende medische hulpmiddelen opgenomen in het juridisch kader.

#### **Wijzigingen of aanvullingen in de functionele weergave**

- Nadere specificatie functionele use cases (opzoeken zorgaanbieder in het zorgaanbiedersregister, vinden/abonneren op informatie, notificeren, authenticatie, haal gegevens op uit xIS).

#### **Wijzigingen of aanvullingen in de technische weergave**

- Nadere uitwerking technisch architectuur gezichtspunt.
- Specificatie van een generiek Medmij Gateway prototype.
- Specificatie van een Medmij gateway voor het LSP, met tevens:
  - Mappings voor uitwisseling van medicatie informatie tussen HL7v3 en Medmij/FHIR voor uitwisseling met het LSP.
  - Specificatie van integratie met het LSP.
  - Specificatie van de Medmij FHIR API.
  - Specificatie infrastructuurmodel.
  - Specificatie van abonnementen en notificatie.
  - Specificatie van de authenticatie van de persoon door de zorgaanbieder.
  - Specificaties Testomgeving met hierop werkende demonstraties

#### **Wijzigingen of aanvullingen in het onderwerp governance**

- Nieuwe documentatie over rollen, verantwoordelijkheden, inrichting en beleid
- Eerste uitwerking van de inrichting van de MedMij-beheerorganisatie op zowel korte als lange termijn

## Engelse vertaling / English translation

### Language switch

The pages in these sections of the MedMij Trust Scheme are in the English language. Many basic terms in de Dutch sections have been given a standard equivalent in English, according to the table on this page.

## Architecture and technical specifications

### Explanatory Notes

An essential part of the MedMij Trust Scheme relates to the responsibilities that the participants in the Trust Scheme have, each within its own role, during the actual provision of the data transfer between the Individual's Domain and the Provider's Domain. These responsibilities are included in the architecture and the technical specifications of the MedMij Trust Scheme, which are elaborated on in these pages. These responsibilities have been organised into a number of abstraction layers, inspired by the [Nictiz interoperability model](#) (in Dutch).

To start with, participants must together ensure that certain business processes take place between the Individual's Domain and the Provider's Domain. These business processes relate to the collecting and sharing of health information. On this abstraction layer, there is not yet an automated handling of these processes but the responsibilities have only been formulated in terms of the content of these processes and of the health information that is handled in them. The process layer and the information layer from Nictiz's interoperability model have been combined into a single layer: [Process and Information](#).

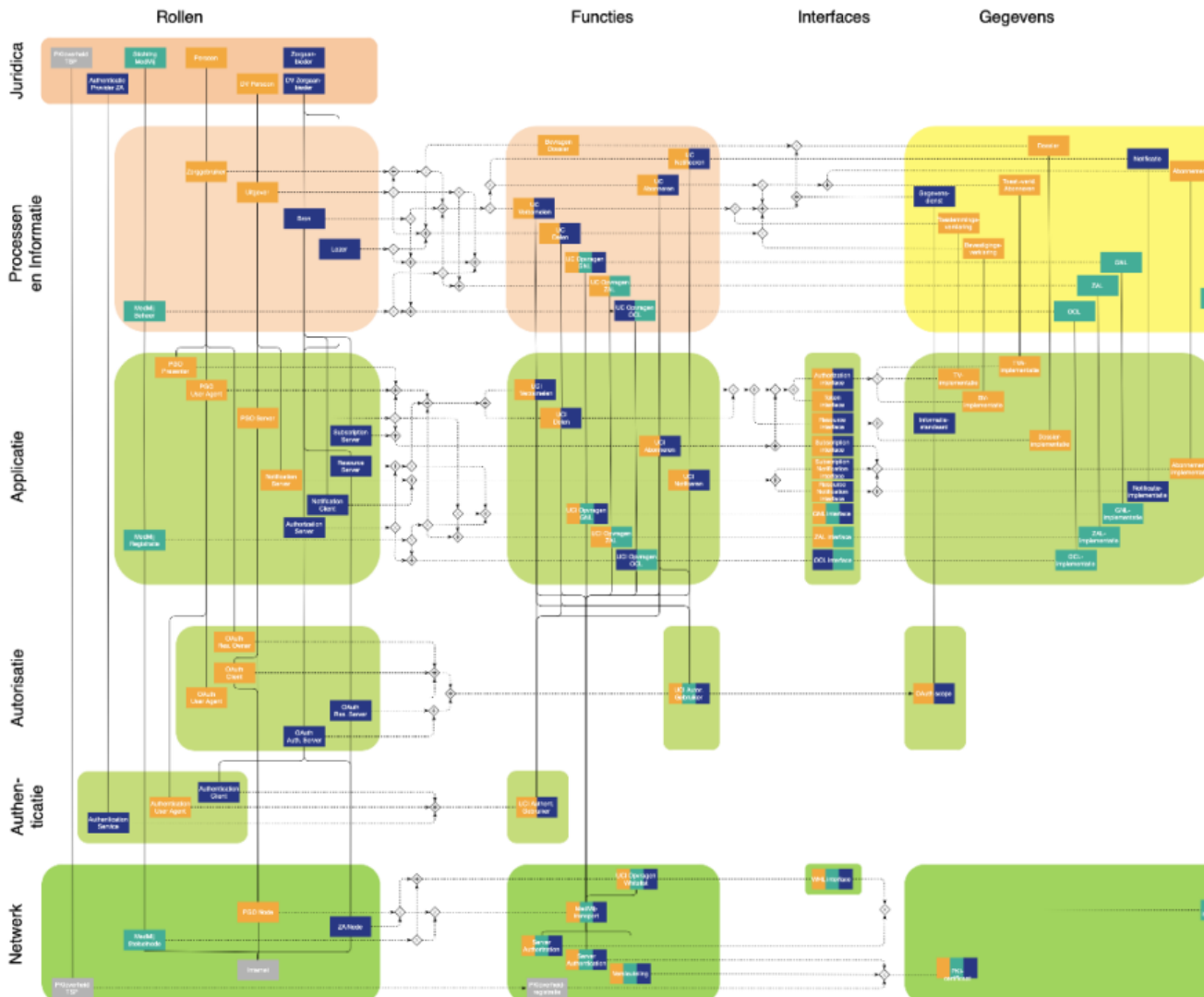
At the next abstraction layer, the [Application layer](#), it is described that, and how, these business processes with the related health information that is handled therein must be performed, with the different roles working together to this end. It is the most complex layer, which has two special sublayers: one for the authentication of the *Individual* and one for this authorisation of the information transfer.

At the lowest abstraction level, the [Infrastructure](#) layer, the responsibilities are included in the area of the network infrastructure.

The diagram below identifies these abstraction layers. On each layer, the architectural elements are stated that are needed in the layer in question, along with their reciprocal links within and between the layers. The diagram on this page is not intended to specify the relationship between all details in one go. This is done step by step on the pages that belong to the specification layers; on the page for each layer, the cutaway of the diagram that matches that layer is repeated and dealt with. On this page, the diagram is only intended to fulfil two roles:

- to give an overview of the layers (and columns) of the architecture of the MedMij Trust Scheme;
- to provide an index that allows the user to quickly find the layer for an architectural detail where this detail is discussed.

The explanation under the diagram also discusses what the columns, colours and lines in the diagram mean and prepares the reader for the viewing of the detailed pages.



## Explanatory Notes

Four columns have been used in the architecture, namely: roles, functions, interfaces and data. Interfaces only occur on the **Application** layer, for which they play a pivotal role. In each layer, there are roles specific to that layer that perform functions specific to that layer using data from Nictiz's interoperability model. This is precisely the reason why the process layer and the information layer from Nictiz's interoperability model are combined into a single layer that also includes a roles column. Because it concerns architecture for a framework, and not for a systems or solutions architecture, the roles column plays a key role in the coherence of the entire architecture. Roles are bundles of responsibilities. These responsibilities involve functions to be performed (second column), which in turn make use of data (fourth column). So, a role is not an individual party, nor is it a system or component. Individual parties will only need systems and components, such as the implementation of roles, when they perform the role.

The **Application layer** has two sublayers: an authorisation layer and an authentication layer. This is because for both of these two issues, standards are used that have their own roles structure, with which an explicit connection must be introduced. Additionally, it is possible in this way to give the

agreements that specifically arise from the design of these standards a recognizable and manageable place.

An additional level has been placed above the [Process and Information](#) layer, namely: [Legality](#). This layer only has the roles column, not the other two columns. The latter are namely discussed in the page [Agreements and legal relationships](#). This layer is only intended for the linking - role by role - of the architecture with the legal part of the MedMij Trust Scheme, so that it is made clear which architectural and technical responsibilities are linked to which legal roles.

In the authentication layer, it is not necessary to make further agreements about data. For this purpose, it is possible to fully revert to the specifications of the interfaces which are provided by the *Authentication Provider P*. This is why this column is lacking in the architecture.

The colours of the large areas correspond to the colours that Nictiz assigns to the relevant architectural aspects in its [interoperability model](#). The colours of the architectural elements (the small rectangles) indicate in which domain the relevant architectural element is placed. First of all, MedMij's corporate identity has been retained, so that:

- orange represents the Individual's Domain;
- blue represents the Provider's domain, and
- green represents the MedMij domain.

The grey colour represents external roles used by the MedMij Trust Scheme. Where multiple colours are combined, this indicates that the domains work together in the relevant architectural element.

The vertical lines in the architecture connect the roles, functions and data between the different layers.

In the MedMij Trust Scheme, the roles are sets of responsibilities that belong together. They occur on each layer of the architecture, from the [Legality](#) layer via the [Process and Information](#) layer and the [Application](#) layer down to and including the [Infrastructure](#) layer. The roles are linked to each other between two adjacent architectural layers. Each role on the one layer is paired with one or more roles on the layer below. In this way, the role links form the backbone of the MedMij Trust Scheme architecture.

A role is emphatically not a component or system. While it is true that many roles are realised by components and systems, the precise way in which this is done, and the extent to which components architecture or system architecture is used for this is for the *Service Provider* to decide, as long as the latter plays its roles properly on all layers, that is to say, carries the responsibilities for these roles. In this way, *Service Providers*, in both domains, are given all the scope they need to choose a business model as they see fit, within which subcontractors are given all the scope they need, as long as the ultimate responsibility for the MedMij Trust Scheme continues to lie inalienably with the *Service Provider*.

For a *Service Provider*, there must in other respects be maximum freedom to arrange a single role on the one level with multiple roles on the level below it. However, conversely, it must continue to be clear, on all layers, that a single *Service Provider* is responsible for each role. In other words, multiple roles cannot be depicted on a single lower one. It is indeed possible for multiple roles to be realised by a joint system, as long as their individual ultimate responsibilities remain intact.

That is, in general a single role on the higher architectural layer will be fleshed out with one or more affiliated roles in the layer below. Conversely, however, a single role on the lower architectural layer



belongs to a single affiliated role on the higher layer. Because the *Nodes* at [Infrastructure](#) layer are identified using a hostname, it can always be read from the logging at [Infrastructure](#) layer which *Participant* is responsible for which event.

The horizontal dotted lines indicate which roles perform which functions, and respectively which functions use which data. To prevent a confusing tangle of dotted lines, the figure uses joins and splits. Joins and splits are indicated by small diamond shapes. A join (juncture) is characterised by multiple incoming arrows and one outgoing arrow and a split (division) by one incoming and multiple outgoing arrows.

Two characters are used in the small diamond shapes:

- A multiplication sign stands for exclusive, which means that only one of the incoming arrows (at joins) or outgoing arrows (at splits) are simultaneous.
- A plus sign stands for inclusive, which means that all incoming arrows (at joins) or outgoing arrows (at splits) are always simultaneous.

For example, in the layer *Process and Information*, the *MedMij Maintenance* role is involved in:

- in three use cases: *UC Retrieve Dcd*, *UC Retrieve Rcd* and *UC Retrieve Isg*, but not simultaneously (exclusive).
- in the use case *UC Retrieve Dcd*, simultaneously (inclusive) with the role *Publisher*.

For each level, the agreements are elaborated on in a separate page:

- [Legality](#)
- [Process and Information](#)
- [Application](#), including Authentication and Authorisation
- [Infrastructure](#)

Each page may have subpages for subissues. These agreements always consist of:

- the identification of the roles on this layer/sublayer and the tie(s) from these roles to the roles on the layer above;
- the responsibilities that the roles on this layer/sublayer have in performing certain functions with certain data.

A separate page [Information Models](#), with three subpages, specifies the conceptual structure of (all or part of) the concept device of the architecture of the MedMij Trust Scheme and translates this via logical models into technical models of a number of components. In this way, the interoperability of the MedMij Network at a technical level is guaranteed.

In many cases, reference to a specification is made in the responsibilities. This can be a use case specified specifically for MedMij, for example, but is often also a standard, especially for information. The specification will not be written out in detail in the responsibility itself; it will instead be referred to. For example, there is no need to always adjust the responsibility for any detail adjustments in the specification. This would, definitely with standard specifications, result in an undesirable management burden on the trust scheme.

In the first instance, as a rule, the roles and responsibilities are concisely and thoroughly formulated. Only in the second instance are they elaborated upon. Accordingly, the approach taken is not that of providing a narrative explanation of the system but to provide a set of agreements, article by article. This makes the architecture suitable for use as an extension of the participant's agreement. The very

first question to ask is: *What is the agreement?* In the second instance, questions such as *Why was this chosen?* and *What does this agreement mean?* are important.

Where in the description of the architecture, the roles and responsibilities contained therein and the explanatory notes for them, use a name to refer to the architectural components, as they occur in the diagram above, the name is written *in italics* and with a capital letter. This also applies for the path expressions in the invariants for the [Information Models](#). Variables in the path expressions are written in *italics*, too, but start with a lower-case letter.

Some architecture components are also represented by a class, attribute, element or type in the [Information Models](#). Because the spelling of the names in the [Information Models](#) is more formal, the naming used in these models may differ a bit from that used in the rest of the architecture, namely in the use of spaces and capital letters. In the [Information Models](#), all names begin with a capital letter. In addition, capital letters may appear in the middle of a name if, but only if, the remaining part of the name there also appears as a separate name.

Technical code fragments are quoted in `monospace`.

## Roles and their numerical relationships

In the MedMij Trust Scheme, the roles are sets of responsibilities that belong together. They occur on each layer of the architecture, from the [Legality](#) Layer, via the [Process and Information](#) Layer and the [Application](#) layer to the [Infrastructure](#) layer. The roles are linked to each other between two adjacent architectural layers. Each role on the one layer is paired with one or more roles on the layer below. Therefore, a role is not a component or system. While it is true that many roles are realised by components and systems, the precise way in which this is done, and the extent to which components architecture or system architecture is used for this is for the *Service Provider* to decide, as long as the latter plays its roles properly on all layers, that is to say, carries the responsibilities for these roles.

For a *Service Provider*, there must be maximum freedom to arrange a single role on the one level with multiple roles on the level below it. However, conversely, it must continue to be clear, on all layers, that a single *service provider* is responsible for each role. In other words, multiple roles cannot be depicted on a single lower one. It is indeed possible for multiple roles to be realised by a joint system, as long as their individual ultimate responsibilities remain intact.

The *Nodes* on the [Infrastructure](#) layer are identified with a hostname. Therefore, since each *Publisher's Node* and *Issuer-Addressee Node* belongs to a *Service Provider*, the *Service Provider* can be recognised from the hostname.

The following applies in the Individual's Domain:

- a single *Individual's Service Provider* provides one or more *Publishers* and each *Publisher* is provided by a single *User's Service Provider*;
- a single *Publisher* is created by one or more *Publishing Servers* and each *Publishing Server* creates a single *Publisher*;
- a single *Publishing Server* is supported by one or more *Publisher's Nodes* and each *Publisher's Node* supports a single *Publishing Server*.

In this way, the hostname of a *Publisher's Node* can also be associated with one *Publishing Server* (with a user-friendly name) in the *OAuth Clientlist*.

The following applies in the Provider's Domain:

- a single *Provider's Service Provider* provides one or more *Issuers* and/of *Addressees* and each *Issuer* and/or *Addressee* is provided by a single *Provider's Service Provider*;
- a single *Issuer* and/or *Addressee* is created by one or more combinations of a single *Authorization Server* and a single *Resource Server* and each combination of a single *Authorization Server* and a single *Resource Server* creates a single *Issuer* and/or *Addressee*;
- a single *Authorization Server*, just like a single *Resource Server*, is supported by one or more *Issuer-Addressee Nodes*;
- each *Issuer-Addressee Node* supports either a single *Authorization Server* or a single *Resource Server* or the combination of a single *Authorisation Server* and a single *Resource Server*;
- each *Issuer-Addressee Node* has one or more endpoints and each endpoint belongs to a single *Issuer-Addressee Node*, such that the hostname is in the endpoint address of that *Issuer-Addressee Node*.

The fourth point allows an *Authorization Server* and a *Resource Server* to be distributed across various *Issuer-Addressee Nodes*, but also to combine these on the same node. The third point even allows that *Authorization Server* and *Resource Server* to be each projected separately on multiple *Issuer-Addressee Nodes*. It may then occur that there are hostnames in the endpoint addresses in the *Information service directory* for the respective *Provider's Information Services* which differ between the authorization endpoint, the token endpoint and the resource endpoint, and even for the same *Interface version*. However, there remains an important requirement that all of these hostnames belong to *Issuer-Addressee Nodes* of the same *Provider's Service Provider*. The entire flow that belongs to a certain *Provider's Information Service* should come under the ultimate responsibility of one of these *Service Providers*, namely the *Service Provider* that discloses that *Provider's Information Service*. In this way, that full ultimate responsibility can also be tested at the Infrastructure level. See the three (complex) [invariants](#) for *Provider's Information Service* of the "non-local dependency" type.

However much all ultimate responsibilities are borne by the *Providers* that are participants in the MedMij Trust Scheme, they may be able to opt partially or even fully outsource those responsibilities. In a potential system architecture, multiple *Resource Server* systems make use of the same *Authorization Server* system (whether or not this is outsourced). It is possible that those *Resource Server* systems come under the ultimate responsibility of a single *Provider's Service Provider*, whether or not the implementation is outsourced. It is also possible that two different *Provider's Service Providers* use the same subcontractor for the *Authorization Server*. The hostnames in the addresses of the *Authorization Endpoints/Token Endpoints* will then nevertheless differ between these two *Service Providers/Providers*, even if there was the same underlying *Authorization Server* system. For the *Provider's Information Services* for which *Provider's Service Provider A* is responsible, the hostname must be a *Node* belonging to A; for the *Provider's Information Services* for which *Provider's Service Provider B* is responsible, the hostname must be a *Node* belonging to B.

In this way, the architecture has intended to give the maximum scope to the business models and architectures of *Provider's Service Providers* without in doing so harming the interoperability and rigid ultimate responsibilities.

## Coordination, control and exchange

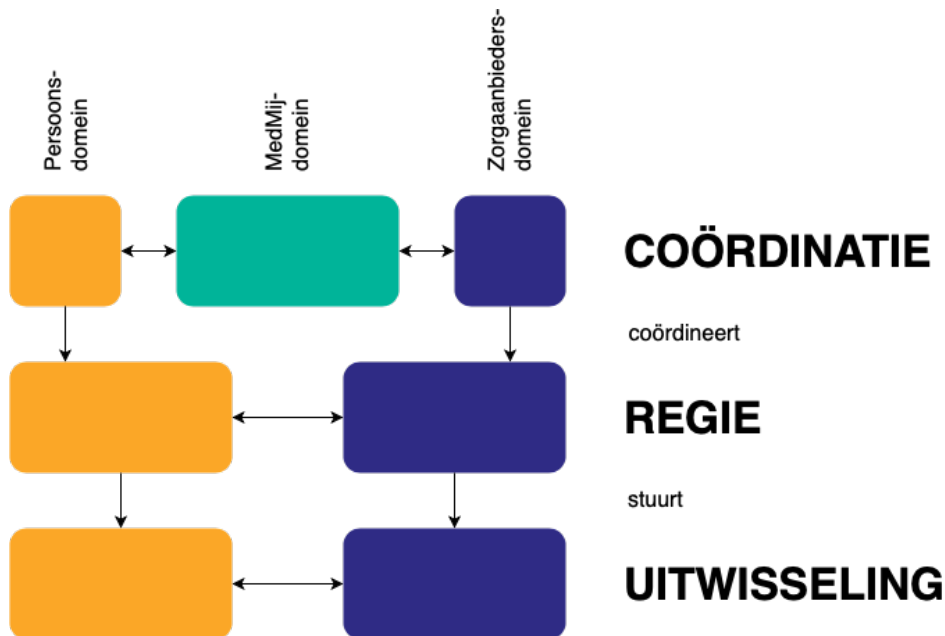
### The distinction between Control, Exchange and Coordination

The MedMij Trust Scheme distinguishes between three primary functions on the [Process and Information](#) layer and on the [Application](#) layer: *Control*, *Exchange* and *Coordination*. All of the behaviour of the roles concerned on these layers belongs to one of these three primary functions. There is an underlying relationship between the primary functions. Principle Options are linked to the primary functions (see below).

*Control* is the key element; the *Individual* controls (the exchange of) his health information, in interaction with the *Provider*. He does this as a publisher, in accordance with [principle 16](#) (in Dutch). This primary function encompasses, for instance, the *Individual* giving consent to the *Provider*, the authentication of the *Individual* by the *Provider*, the authorisation of the PHE by the *Provider* and entering into, terminating and maintaining subscriptions. In this way, *Control* always leads to agreements between the *Individual*, *Provider* and the *Individual's Service Provider*, and it is based on trust in the identity of the others in the agreement. The *Provider's Service Provider* is not a party to these agreements because it is not a data controller, as the *Individual's Service Provider* is. However, the *Provider's Service Provider* does play an important role in the creation of the agreements, as a processor on behalf of the *Provider*.

*Control* guides *Exchange*. *Exchange* implements the *Control*. This second primary function performs the actual data transfer, from the *Provider* to the PHE (*Compiling* and *Notifying*) or vice-versa (*Sharing*). All exchange takes place in accordance with the standardised *Information Services* and in the context of a *Control* agreement. *Control* and *Exchange*, in accordance with [principle 10](#) (in Dutch), are only performed by parties who are under the full responsibility of an *Individual's Service Provider* or a *Provider's Service Provider*, and hence are decentralised. MedMij is not individually involved with the performance of *Control* or *Exchange*.

Nevertheless, MedMij needs to perform a preparatory role to enable the parties to establish the underlying *Control*. *Coordination* is the third primary function, which provides trust between the *Individual's Domain* and the *Provider's Domain* so that these are able to find out from each other what they can and are permitted to do on the MedMij Network. This function is performed with the *Information service catalogue*, that says which *Information Services* are in force at any moment on the MedMij Network, and with four lists (*Information service glossary*, *OAuthclientlist*, *Whitelist* and the *Information service directory*), that say which *Participants* there are, and what they can and are permitted to do.



## Process and Information layer

The three primary functions are performed on this layer by the following roles.

primary function	Individual's Domain	MedMij Domain	Provider's Domain
<b>Coordination</b>	<ul style="list-style-type: none"> <li>Publisher</li> </ul>	<ul style="list-style-type: none"> <li>MedMij Maintenance</li> </ul>	<ul style="list-style-type: none"> <li>Issuer</li> <li>Addressee</li> </ul>
<b>Control</b>	<ul style="list-style-type: none"> <li>User</li> <li>Publisher</li> </ul>	-	<ul style="list-style-type: none"> <li>Issuer</li> <li>Addressee</li> </ul>
<b>Exchange</b>	<ul style="list-style-type: none"> <li>User</li> <li>Publisher</li> </ul>	-	<ul style="list-style-type: none"> <li>Issuer</li> <li>Addressee</li> </ul>

The three primary functions are performed on this layer in the following use cases.

primary function	Individual's Domain	MedMij Domain	Provider's Domain
<b>Coordination</b>	<ul style="list-style-type: none"> <li>UC Retrieve Isg</li> <li>UC Retrieve Dcd</li> </ul>	<ul style="list-style-type: none"> <li>UC Retrieve Isg</li> <li>UC Retrieve Dcd</li> </ul>	<ul style="list-style-type: none"> <li>UC Retrieve Isg</li> <li>UC Retrieve Rcd</li> </ul>

		<ul style="list-style-type: none"> <li>• <i>UC Retrieve Rcd</i></li> </ul>	
<b>Control</b>	<ul style="list-style-type: none"> <li>• <i>UC Collect</i> ( Authorization interface and Token interface)</li> <li>• <i>UC Share</i> (Authorization interface and Token interface)</li> <li>• <i>UC Subscribe</i></li> <li>• <i>UC Notify</i> (for subscription Notifications )</li> <li>• <i>UC Portability Report</i></li> </ul>	-	<ul style="list-style-type: none"> <li>• <i>UC Collect</i> (Authorization interface and Token interface), including the availability condition</li> <li>• <i>UC Share</i> (Authorization interface and Token interface), including the acceptability condition</li> <li>• <i>UC Subscribe</i></li> <li>• <i>UC Notify</i> (for subscription Notifications)</li> </ul>
<b>Exchange</b>	<ul style="list-style-type: none"> <li>• <i>UC Collect</i> (resource interface)</li> <li>• <i>UC Share</i> (resource interface)</li> <li>• <i>UC Notify</i> (for content-related Notifications)</li> </ul>	-	<ul style="list-style-type: none"> <li>• <i>UC Collect</i> (final phase)</li> <li>• <i>UC Share</i> (resource interface)</li> <li>• <i>UC Notify</i> (for content-related Notifications)</li> </ul>

## Application layer

The three primary functions are performed on this layer by the following roles.

primary function	Individual's Domain	MedMij Domain	Provider's Domain
<b>Coordination</b>	<ul style="list-style-type: none"> <li>• <i>Publishing Server</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>MedMij Registration</i></li> </ul>	<ul style="list-style-type: none"> <li>• <i>Authorization Server</i></li> </ul>
<b>Control</b>	<ul style="list-style-type: none"> <li>• <i>PHE User</i></li> <li>• <i>PHE User Agent</i></li> <li>• <i>Publishing Server</i></li> <li>• <i>Notification Server</i> (for subscription notifications)</li> <li>• <i>OAuth Resource Owner</i></li> <li>• <i>OAuth User Agent</i></li> <li>• <i>Client</i></li> <li>• <i>Authentication User Agent</i></li> </ul>		<ul style="list-style-type: none"> <li>• <i>Authorization Server</i></li> <li>• <i>Subscription Server</i></li> <li>• <i>Notification Client</i> (for subscription notifications)</li> <li>• <i>OAuth Authorization Server</i></li> <li>• <i>Authentication Client</i></li> <li>• <i>Authentication Service</i></li> <li>• <i>Subscription Server</i></li> </ul>
<b>Exchange</b>	<ul style="list-style-type: none"> <li>• <i>PHE User</i></li> <li>• <i>PHE User Agent</i></li> <li>• <i>Publishing Server</i></li> </ul>		<ul style="list-style-type: none"> <li>• <i>Resource Server</i></li> <li>• <i>OAuth Resource Server</i></li> <li>• <i>Notification Client</i> (for resource notifications)</li> </ul>

	<ul style="list-style-type: none"> <li>• <i>Notification Server</i> (for resource notifications)</li> <li>• <i>OAuth Resource Owner</i></li> <li>• <i>OAuth User Agent</i></li> <li>• <i>Client</i></li> </ul>		
--	--	--	--

The three primary functions are performed on this layer on the following interfaces. Each interface belongs to a single primary function.

primary function	interface
<b>Coordination</b>	<ul style="list-style-type: none"> <li>• <a href="#">Isg interface</a></li> <li>• <a href="#">Cld interface</a></li> <li>• <a href="#">Isd interface</a></li> </ul>
<b>Control</b>	<ul style="list-style-type: none"> <li>• <a href="#">User interface (Declarations)</a></li> <li>• <a href="#">Authorization interface</a></li> <li>• <a href="#">Token interface</a></li> <li>• <a href="#">Subscription interface</a></li> <li>• <a href="#">Subscription Notification interface</a></li> </ul>
<b>Exchange</b>	<ul style="list-style-type: none"> <li>• <a href="#">Resource interface</a></li> <li>• <a href="#">Resource Notification interface</a></li> </ul>

## Principles

The architecture of the MedMij Trust Scheme uses the following principles with regard to the primary functions.

1. **One interface, one primary function.** An interface (on the [Application](#) layer) belongs to precisely one primary function. Preferably, a role and a use case also belong to precisely one primary function. This preference is firmer on the [Application](#) layer than on the [Process and Information](#) layer. Furthermore, this preference is less firm for the user roles in both domains.
2. **Decentralised control and exchange.** Neither *MedMij Maintenance* nor any other party has a central or intermediary role in *Control* or *Exchange* between the Individual's Domain and the Provider's Domain. However, *MedMij Maintenance* does have an intermediary role in *Coordination*. This principle is an elaboration of [principle 7](#) (in Dutch).
3. **No sector-specific standards or solutions for *Coordination* and *Control*.** The MedMij Trust Scheme does not use any sector-specific solutions or standards for *Coordination* and *Control*. Sector-specificity of solutions or standards should not be understood here as only referring to content, but also to governance (of a standard). Health does not adhere to sector divisions; the *Control* on this should not be divided by sector since this would limit the control. Nor is there a preference for sector-specificity for *Exchange*, however, reality requires the use of sector-specific exchange standards (such as HL7 for the care sector and StUF, for instance, for the municipal field). By far the greatest standardisation of information with regard to content occurs within sectors. This principle does not affect [principle 19](#).



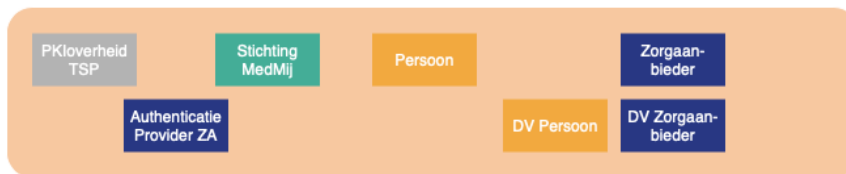
4. **No exchange without control.** *Exchange* does not take place where there is no underlying *Control* agreement. If *Exchanges* need to be included in the MedMij Trust Scheme which requires another form of identification than in those provided at any point in *Control*, the new identification must be added under the primary function *Control*. MedMij's main aim is to offer *Individuals Control* over their health information. *Coordination* merely provides what is required to achieve that aim.
5. **Standardised and coordinated exchange.** All of the data transfer in the context of *Exchange* occurs on the basis of standardised *Information Services*, which are contained in the *Information service catalogue*.
6. **Information service as a *Control* unit.** The *Control* unit between the *Individual* and the *Provider* is an entire *Information Service*. However, even though the *Exchange*, of a *Notification*, for instance, may involve a smaller unit, it is always as an element of a single *Information Service*. Each Subscription also relates to a single *Information Service*.
7. **A single language for *Coordination*.** All functionality of the primary function *Coordination* is based on a common set of [information models](#), which have been ordered into three layers: conceptual ([metamodel](#)), logical ([logical models](#)) and technical ([XML schemas](#)). These information models are part of the MedMij Trust Scheme. That does not apply to the information standards that are used for the *Information Services*. Although these are standardised for each *Information Service*, they are not standardised across all *Information Services* at the *Information service catalogue* level because this would trap MedMij in a single sector (see principle 3).
8. **Future-proof separation.** The separation between the three primary functions represents a structural aspect of the evolving MedMij Trust Scheme. That means that despite the great freedom of *Participants* to implement, they can limit their burden of implementation of new releases by also introducing this separation into their implementation architecture. The separation between the primary functions makes the evolution of the Trust Scheme more predictable for *Participants*.



## Legality

### Rollen

Juridica



#### Explanatory Notes

This layer contains the legal roles, which provide a legal basis for the roles on other levels of the architecture. The reason that this layer is included in this architecture is that its roles ensure coherence between the different architectural layers, and the architecture must also be guaranteed in the legal roles in the MedMij Trust Scheme. A legal role includes obligations for playing of roles at different architectural levels.

The roles named here in the architecture fall into two groups:

1. the legal roles, which are part of MedMij participant agreements: the *Individual's Service Provider*, *Provider's Service Provider* and *Stichting MedMij*.
2. the legal roles that are not part of the MedMij participant agreements but nonetheless have an executive obligation within the architecture. This means that an applicable participant's agreement will require it to enter into a legal relationship with that legal role. These concern the following:
  - *Individual* and *Provider*, whose underlying information relationship is served by MedMij data transfer;
  - *Authentication Provider*, that provides the authentication to *Providers* of *Individuals* who present themselves to the *Provider*;
  - *PKI TSP*, that issues certificates which enable the data transfer on the MedMij Network to be made secure.

In the architecture of the trust scheme, the *Individual* has an operational role to play in the authentication and authorisation of data transfer. Operationally, the *Provider* is entirely represented by the *Provider's Service Provider*.



makes this information available to *Addressees*. In this way, the *Individual* receives the [Control](#) that MedMij wishes to offer him/her. In this release of the MedMij Trust Scheme, the *Publisher* compiles health information from *Issuers* and shares this health information with *Addressees*.

In the Individual's Domain, in addition to the role of *Publisher*, there is also the role of *User*. Although *Publisher* acts on behalf of *User*, *User* cannot remain anonymous (i.e. be hidden behind the role of *Publisher*) in the related agreements on these and underlying layers. This is because the *User* is not only the user of *Publisher* but also and first and foremost the subject of the health information that *Issuer* must make available and that is made available to *Addressee*; authentication is needed for this. This is different in the Provider's Domain. In this release of the Trust Scheme, it is sufficient to see *Issuer* and *Addressee* as the roles that between them are fully responsible for what a *Provider* should do in operational terms. The implementation of this responsibility lies with the *Issuer* or *Addressee* respectively. This carries over into the Application Layer and the [Infrastructure](#) layer.

Because the *Stichting MedMij* too has operational responsibilities, what is shown here is the functional role of *MedMij Maintenance*.

## Responsibilities

### Explanatory Notes

The responsibilities in this layer are ordered into chapters and sections as follows:

- Personal record
  - Use cases
  - *Information services*
  - Authentication
  - Authorisation
- Lists
  - *Information service directory*
  - *Client directory*
  - *Information service glossary*
  - *Whitelist*
- Logging and portability

In multiple places, use cases (in this layer) and use case implementations (in the [Application](#) layer) are used. A use case implementation is the implementation of the use case with the same name. In this release of the MedMij Trust Scheme, there are nine use cases, seven of which occur between the Individual's Domain and the Provider's Domain. Of these seven, in order to guarantee interoperability in the MedMij Network, flow diagrams form part of the MedMij Trust Scheme. The other two occur entirely within the Individual's Domain. The MedMij Trust Scheme does require this to be provided but does not say (or only says in part) how this should be done; instead, this is left to the discretion of the MedMij Participants.

This relates to the following use cases:

Use case	flow diagram	Primary function(s)
<i>UC Collect</i>	with	<i>Control and Exchange</i>
<i>UC Share</i>	with	<i>Control and Exchange</i>
<i>UC Consult Personal record</i>	without	<i>Control</i>

<i>UC Portability Report</i>	without	<i>Control</i>
<i>UC Subscribe</i>	with	<i>Control</i>
<i>UC Notify</i>	with	<i>Control and Exchange</i>
<i>UC Retrieve Dcd</i>	with	<i>Coordination</i>
<i>UC Retrieve Rcd</i>	with	<i>Coordination</i>
<i>UC Retrieve Isg</i>	with	<i>Coordination</i>

For registration of *Participants* and of the important data needed as a result of their participation, for the time being no separate use cases have been identified, because registration is viewed as a secondary process. See for this the page [Operational processes](#) (in Dutch).

The interpretation by a *User* of care & health information that he has compiled from a *Provider*, and the interpretation by a *Provider* of such information that has been shared with him/her by a *User*, depends not only on the content of this information but also on the party that originally registered the relevant information. We do not merely use the term *Issuer* for this, because this term within the meaning of the MedMij Trust Scheme does not per se mean the original origin (the author) but only the direct origin seen from the *Publisher's* point of view. In the MedMij Trust Scheme, the author's role is not a [legal role](#). This means not only that within the limits of the MedMij Trust Scheme there is currently no basis for arranging an author's authenticity (using certificates, for example) but also means that information about the author, however significant, is, as far as the MedMij Trust Scheme is concerned, a *data content-related* matter. After all, this information is also used for the interpretation of the shared care & health information. Since, in accordance with [principle 1](#) (in Dutch), the MedMij Trust Scheme wants to be data-neutral, the author's information is deemed to be part of the content of an *Information service*.

## Personal record

### Use cases

1a. *Publisher* offers *User* the use case *UC Collect* in order to gather health information from *Issuer* from *Provider*, if the latter discloses this information that relates to this *User* and has this stored in a personal health Personal record (hereinafter: *Personal record*) of *User*. For this, the roles involved in this use case use the relevant [flow diagram](#).

#### Explanatory Notes

This responsibility also introduces the notion of a personal health Personal record. This means that in order to comply with this rule it is not enough to just provide the *User* with access to the health information; they have to be able to save and manage it, too. Because this function extends over various functional roles, for reasons of interoperability the specification of the flow diagram has been quoted.

1b. *Publisher* offers *User* the use case *UC Share* in order to place with the *Addressee* for a *Provider* - if they are receptive to this - health information that relates to this *User* and that originates from the *Personal record*. For this, the roles involved in this use case use the relevant [flow diagram](#) to this end.

#### Explanatory Notes

For a description of the similarities and differences between *UC Collect* and *UC Share*, see the page about [UC Share](#).

1c. *Publisher* ensures that when it comes to the *Personal record*, all information in it that has been compiled from the *Issuer* in the context of an *Information service* inextricably records this *Issuer* and *Information service* as the *Issuer* and compilation context. *Publisher* ensures that, if information is shared with the same or other *Provider*, this information on *Issuer* and context is delivered with it to the *Addressee*. Here, the designation of the *Issuer* uses the *Provider's Name*. Here, the designation of the context uses the relevant *Information service Name* from the [Information service glossary](#).

#### Explanatory Notes

This guarantees that the exchanged care & health information always makes it clear from which *Issuer* and in which context (*Information service*) it was compiled. An *Addressee* of this information can use this meta-information to make a more accurate interpretation of the relevant information. Should questions of interpretation still arise from this then the *Addressee* can apply to the relevant *Issuer*.

2a. *Publisher* provides *User* with the use case *UC Consult Personal record* in order to consult the personal health *Personal record*.

#### Explanatory Notes

See below 1. Because this function does not extend over multiple domains, it is not specified in more detail in a flow diagram. The *Participant* can choose how he wishes to arrange this according to his clients' needs. However, this must not be omitted, because in its absence the *User* cannot exercise any [Control](#) over the *Personal record*.

2b. In the context of the use case *UC Consult Personal record*, the *User* must at all times be able to check:

- which content of the *Personal record* is (and which is not) obtained via the MedMij transfer of the *Issuer* of the *Provider* in question and has not changed since then;
- which content of the *Personal record* has (and which has not) been placed - via MedMij transfer - with the *Addressee*, and for which *Provider*.

#### Explanatory Notes

This makes it clear for the *User* to which part of the content of their *Personal record* they can link the trust associated with the MedMij Trust Scheme. After all, it is certainly possible that a PHE (Individual Health Environment/PGO) only participates in certain parts of, and thus complies with, the MedMij Trust Scheme.

3a. If desired, *Publisher* offers *User* with the use case *UC Subscribe*. In this way, *User* can - for a *Subscription to Notifications* - enter into, extend, shorten or end one with a *Provider*, via *Issuer*. These *Notifications* relate to an *Information service*. The roles involved in this use case use the relevant [flow diagram](#) for this.

#### Subscriptions

*Subscriptions belong to the primary function Control.*

3b. For each combination of *User*, *Publisher*, *Provider* and *Information service* there must at any time be a maximum of one *Subscription*.

### Subscriptions

New requests for *Subscriptions* may replace existing ones.

3c. A *Publisher* or *Issuer* that offers the use case *UC Subscribe* also offers the use case *UC Notify*. The roles involved in this use case use the relevant [flow diagram](#) to this end.

### Notifications

This responsibility introduces the notion of a *Notification*. A *Notification* always belongs to no more than one *Subscription*. There are two types of *Notifications*:

- Resource *Notifications* notify *Publisher* (and possibly *User*) about the availability of new (health and other) information of *Provider* at the *Issuer* that relates to an *Information service* that the *User* is subscribed to with this *Provider*;
- Subscription *Notifications* notify *Publisher* (and possibly *User*) about the termination - by the *Provider*, via *Issuer* - of a *Subscription* (see responsibility 3d).

3d. An *Issuer* that supports the use case *UC Subscribe* terminates a *Subscription* if:

1. it receives a request to this end from the *Publisher*;
2. the *Issuer* - after sending a *Notification* - discovers that the *Publisher* does not know the *Subscription* in question;
3. the lifetime of the *Subscription* has expired;
4. the *Provider* no longer provides the relevant *Data Service*, or if the *Issuer* no longer makes available the relevant *Information service*. In this situation, the *Issuer* promptly terminates all relevant *Subscriptions*.

### Termination of Subscriptions

#### Termination of Subscriptions

No requirements are set regarding the termination of a *Subscription* if (health and other) information of a *User* is no longer available at a *Provider*, for example after a Personal record transfer or after the Personal record has been destroyed. If this situation occurs then it is simply the case that until the end date of the *Subscription*, no more content-related *Notifications* will be generated.

It could be that an *Authorization Client* wishes to send a *Notification* under an ongoing *Subscription* but that the *Client directory* states that the relevant *Client* can either no longer receive *Notifications* or else does not support (or no longer supports) the relevant *Information service*. In these cases, the *Notification* is not sent - instead, the *Subscription* remains intact (in principle). Because no *Notifications* are sent, there is no risk about maintaining the *Subscription*. If the *Client directory* contains an administrative error then this is still no reason to terminate the *Subscription* between *Individual* and *Provider*; if such an error is corrected then subsequently *Notifications* can start being sent again under the same *Subscription*. If such a situation happens to a *Notification Client* then there is a reason for the relevant *Provider's Service Provider* to get in touch with the relevant *Individual's Service Provider* and, where necessary, with the MedMij Maintenance organisation. See also responsibility 3e.



The fourth point assumes that the *Provider's Service Provider* maintains his own records of which *Information services* he makes available for which *Providers* and that he does not rely on the *Information service directory* or other lists for this. His processor relationships with *Providers* are after all the Issuer of these lists, not the other way round. It may be that the *Provider's Service Provider* makes an error in his own records and that - by virtue of the fourth point - the relevant *Subscriptions* are terminated. The MedMij Trust Scheme does not prevent this, because this error must be seen as an error by the *Provider's Service Provider* as processor for the *Provider*, in other words in the context of the *Service Provision Agreement* between these two, and not as one on the MedMij interface.

3e. A *Publisher* who intends to terminate the conducting of a certain *Information service* or to terminate the conducting of *Subscriptions* will notify his *Users* about this and will, as far as possible, have all current *Subscriptions* terminated.

3f. If an *Issuer* at a *Provider* detects a change in health information that belongs to an *Information service* to which an *Individual* has - with the *Provider* - a *Subscription* that is valid at that time - namely via a *Publisher*, then this *Issuer* provides this *Publisher* with a content-related *Notification*, by means of the [UC Notify](#).

3g. If an *Issuer* at a *Provider* detects a change in a *Subscription* that is currently valid that an *Individual*, via the *Publisher*, has entered into with the *Provider* then this *Issuer* will provide *Publisher* with a *Subscription Notification*, by means of the [UC Notify](#).

3h. The termination referred to in responsibility 3d leads or does not to the following:

- it does not lead to a *Subscription Notification* in the first and second cases;
- it does lead to a *Subscription Notification* in the third and fourth case.

3i. A *Subscription* has a duration that is calculated in whole days from the moment it is entered into, extended or shortened.

- The *Information service catalogue* states for each *Information service* the maximum duration of a *Subscription* to this *Information service*; if this maximum duration is 0 then for this *Information service* no *Subscriptions* can be entered into for it.
- The *Provider* has, within the limits set by the *Information service catalogue*, leeway for his own policy regarding the (maximum or other) duration of a *Subscription*, depending on the *Information service* in question. This is stated in the *Information service directory*.
- The *Provider* has, within the limits set by the *Information service directory*, leeway for his own policy regarding the (maximum or other) duration of a *Subscription*, depending on the *Individual* in question. This policy is part of the availability condition.
- The duration requested by an *Individual* - via his *Publisher* - of a *Subscription* is maximised at the maximum durations referred to in the three previous points.

## Information services

4. *Publisher* lets *User* with an *Information service* from the [Information service glossary](#) compile health information from an *Issuer* or else, for the benefit of a *Provider*, place it with an *Addressee*.

### Explanatory Notes

An *Information service* is a service that is geared to a specific and standardised set of health information that the *Issuer* can use to make such information available to *Publisher* in the context of the *UC Collect* or with which the *Addressee* receives such information placed for a *Provider*. The [Information service glossary](#) lists the *Information services* that are provided at any time but note that the *Information service catalogue* is the authority for this.

5. Each *Issuer* makes at least one *Information service* available at any time. Each *Addressee* makes at least one *Information service* available at any time.

#### Explanatory Notes

Making available an *Information service* - in this version of the MedMij Trust Scheme - refers to either arranging for an *Issuer* to compile, or for an *Addressee* to share, certain health information. Here, the term 'disclose' is used instead of the term 'offer', because as the provider of an *Information service*, it is the *Provider* who is seen, not the *Participant* (*Issuer* or *Addressee*). The *Participant* makes the *Information service* available on behalf of the *Provider* who is providing the *Information service*.

The terms 'offer' and 'disclose' represent the splitting of the responsibility for a delivered *Information service*. The *Provider* is, including as controller within the meaning of the GDPR, responsible for offering an *Information service* to the *Publisher*; the *Provider's Service Provider* is, including as processor within the meaning of the GDPR, responsible for disclosing this same *Information service* to this same *Publisher*. In other words, offering and disclosing are not linked up behind each other: the *Provider* offers the *Information service* not so much to the *Issuer/Addressee* but to the *Publisher*. Offering and disclosing are aspects of the same delivered *Information service*: the first being performed by the controller, the second by the processor.

6. *MedMij Maintenance* will only state in the *Information service directory* that a certain *Information service* is provided by a certain *Provider* via a certain *Issuer* or *Addressee* respectively if it (i.e. the *Stichting MedMij*) has established that the *Provider's Service Provider* who is also the *Issuer* or *Addressee* respectively, complies with the specific requirements that apply to this *Information service*.

#### Explanatory Notes

Because there is an indirect relationship, namely via the *Provider's Service Provider* to the *Provider*, it must be noted that a single *Provider* is sufficient (that provides access to a certain *Information service*) to ensure that the *Provider's Service Provider* has to qualify for this *Information Standard* in the MedMij Trust Scheme.

7a. For each *Information service* for which the *Information service directory* states that a certain *Provider* provides this, the *Issuer* or *Addressee* respectively will ensure that this *Information service* is delivered too. In doing so, no distinction at all is drawn between *Publishers* unless the MedMij Trust Scheme expressly requires this. This also applies for the possible other *Information service(s)* that is/are listed in the [Information service catalogue](#) (in Dutch as *Required* for the first-mentioned *Information service*).

#### Explanatory Notes

Just like with responsibility 6, responsibility 7a must take into account the indirect relationship via *Provider's Service Provider* to the *Provider* itself. This rule makes it the *Provider's Service Provider's* responsibility to ensure that the *Provider* with whom he has a service provision agreement also delivers the *Information service* that he has promised to deliver.

7b. The provisions regarding responsibility that are laid down in 7a also apply as long as the validity of the applicable entry in the *Information service directory* did not expire more than one hour (3600 seconds) previously.

#### Explanatory Notes

This provides scope for ensuring that sessions that are lagging behind that are still using the expired version of the *Information service directory* can still be completed.



## Authorisation

8a. *Issuer* ensures that every time before it allows *User* to have health information of *Provider* compiled using [UC Collect](#), that this *User* has expressly given *Consent* to *Provider* to have the relevant health information in the *Information service* provided to the *Publisher*. The request for *Consent* has a fixed formulation that is included in the [UC Collect](#). This *Consent* is only in force when the use case is being executed this way.

### Explanatory Notes

#### Explanatory Notes

In other words, it is the *Issuer* that obtains *Consent* from the *User*. The second sentence of this responsibility makes the consent functionally as simple as possible because in this release of the MedMij Trust Scheme health information can only be compiled with a single (one-off) request. The consent, however explicitly given, has exactly the same scope as that single (one-off) request.

8b. *Addressee* ensures again each time before he allows *User* to have health information placed for *Provider* that this *User* has expressly confirmed that he/she wishes to provide the health information involved in the *Information service* to *Provider*. The request for *Confirmation* has a fixed formulation that is included in [UC Share](#). This confirmation does not apply beyond this execution of *UC Share*.

### Explanatory Notes

This responsibility has been deliberately not integrated with responsibility 8a because the confirmation referred to here does not have the legal status of the *Consent* referred to in responsibility 8a.

8c. *Issuer* ensures that every time before it allows *User* to enter into a *Subscription* with *Provider* that this *User* has given his express *Consent* to *Provider* to have *Notifications provided* relating to the health & other information in the *Information service* to the *Publisher*. The request for *Consent* has a fixed formulation that is included in the [UC Subscribe](#).

### Explanatory Notes

*Issuer* accordingly also acts when *Notifications* are being made available, doing so in accordance with a *Consent* of the *User*. This *Consent* is given when entering into a *Subscription* and remains valid for the duration of the *Subscription*.

## Authentication

9. *Issuer* and *Addressee* ensure that the compliance referred to in 7 and the request for *Consent* or confirmation respectively referred to in 8a, 8b and 8c only take place once they have established the identity of the *User* with appropriate certainty.

### Explanatory Notes

It is described in the [Application](#) layer that the identity of the *User* is expressed using a BSN.

## Lists

### Four lists

In the MedMij Trust Scheme, for the primary function [Coordination](#), four lists are used for the interoperability and the trust between the Individual's Domain and the Provider's Domain.

list	abbreviation	is retrieved and used by		information content
		Publisher	Issuer / Addressee	
Information service directory	Dcd	X		which <i>Providers</i> offer which <i>Information services</i> , and possibly also <i>Subscriptions</i> to them, and which addresses they allow to be disclosed, given a certain <i>Interface Version</i>
Client directory	Cld		X	the names of PHEs, which <i>Information services</i> they are allowed to use and to which addresses possible <i>Notifications</i> can be sent under <i>Subscriptions</i> to these <i>Information services</i> , given a certain <i>Interface Version</i>
Information service glossary	lsg	X	X	the user-friendly names of <i>Information services</i>
Whitelist	Whl	X	X	which <i>Nodes</i> are allowed to be active in the MedMij Network

### Information service directory

10. *MedMij Maintenance* manages and publishes an *Information service directory* on behalf of the participating *Provider's Service Providers*. The published *Information service directory* always and only contains all current entries, and describes each *Provider*:

- which *Information services* this one currently provides via which *Issuer* and *Addressee*, and which technical addresses must be addressed for this at the *Provider's Service Provider*, given a certain *Interface Version*;
- for which *Information services* it is possible to enter into *Subscriptions* and via which technical addresses this can be done, given a certain *Interface Version*. In this release of the MedMij Trust Scheme, the *Information service catalogue* only permits *Subscriptions* on *Information services* that are based on the [UC Collect](#).

### Explanatory Notes

This agreement allocates to *MedMij Maintenance* the responsibility to distribute a list - for all the *Individual's Service Providers* - of *Providers* and the *Information services* and *Subscriptions* they provide. Without this function, the system would not function.

The *Information service catalogue* states for every *Information service* the maximum duration of a

*Subscription for (Notifications of) this Information service. For an Information service based on [UC Share](#), for the time being, 0 will always be stated here as the maximum duration, which means that no Subscriptions are possible for this Information service.*

11. The *Information service directory* complies with what is laid down for it in the [Information Models](#).

12. *MedMij Maintenance* manages and publishes, in the *Information service directory*, unique and user-friendly names of *Providers*, in the format <provider>@medmij. This is subject to the [naming policy](#) (in Dutch) that is in place.

#### Explanatory Notes

*Providers* can in their direct or indirect contact with *Users* give this name as their "MedMij name". *MedMij Maintenance* ensures uniqueness and has the final word when choosing the name.

13. *MedMij Maintenance* provides to *Publisher* a use case (*UC Retrieve Dcd*) to request the current version of this *Information service directory*. The roles involved use the relevant [flow diagram](#) for this.

#### Client directory

14a. *MedMij Maintenance* manages and publishes an up-to-date *Client directory* on behalf of the participating *Individual's Service Providers*. The published *Client directory* only contains at all times all current entries and describes for each *Client*:

- what the user-friendly names are that are used for the *Individual's Service Providers* in the [Declaration of consent](#) (in Dutch), the [Declaration of confirmation](#) (in Dutch) and the [Notification of User](#) (in Dutch);
- on which *Information services* the *Individual's Service Provider* supports the receiving of *Notifications* in the context of a *Subscription*, and to which technical addresses these *Notifications* must be delivered, given a certain Interface Version. In this release of the MedMij Trust Scheme, *Subscriptions* can only be entered into for *Information services* that are based on the *UC Collect*.

#### Explanatory Notes

In other words, the *Client directory* contains no names for *Provider's Service Providers*. It does not need to do so, because these do not occur in the [Declaration of consent](#) (in Dutch).

14b. The *Client directory* complies with that which is laid down for it in the [Information Models](#).

15. *MedMij Maintenance* offers to *Issuer* a use case (*UC Retrieve Rcd*) in order to request the current version of this *Client directory*. For this, the roles involved use the relevant [flow diagram](#).

#### Information service glossary

16. *MedMij Maintenance* manages and publishes the *Information service glossary*. This describes which user-friendly names belong to which *Information services*. The *Information service glossary* complies with that which is laid down for it in the [Information models](#).

17. *MedMij Maintenance* offers to *Publisher*, *Issuer* and *Addressee* a use case (*UC Retrieve Isg*) to request the actual version of the *Information service glossary*. For this, the roles involved use the relevant [flow diagram](#).

#### Whitelist

18. *MedMij Maintenance* manages and publishes a current *Whitelist* on behalf of the participating *Provider's Service Providers* and *Individual's Service Providers*. The *Whitelist* describes which *Nodes* may participate in MedMij data transfer. The *Whitelist* complies with that which is laid down for it in the [Information Models](#).

#### Explanatory Notes

In this layer, there is no use case for requesting the *Whitelist*. The *Whitelist* is only used in the [Infrastructure](#) layer. In this layer, there is indeed a use case implementation for this purpose.

### Logging and portability

19a. *The Publisher* will organise the *Personal record* in such a way that this can also serve as a log file, as referred to in the [GDPR \(General Data Protection Regulation\)](#) and [NEN 7513:2018](#), of the personal data compiled by any *User* from any *Issuer* and of the personal data placed by any *User* with any *Addressee*.

#### Explanatory Notes

Logging is intended to be able to provide a reliable overview of the events in which health information about a person is processed. The events can extend across different places and times. The intended overview is accordingly only possible if the log data from different Issuers can be combined. Even without directly targeting having a virtual worldwide and life-long patient *Personal record*, it is clear that standardised logging is a prerequisite for making the overview possible for the *Individual* concerned.

On 18 May 2018, a revision of the 2010 version of NEN 7513 was published. This standard, which has the number [NEN 7513:2018](#), is part of the [Information Security Standards](#) (in Dutch) of the MedMij Trust Scheme. Chapter 5 of the revised standard contains the information requirements, both the general ones and those seen from the specific perspective of the clients, care institutions and supervisory authorities. Chapter 6 translates these needs into an overview of the events to be logged, and chapter 7 provides a model of the data to be logged. The previous version ([NEN 7513: 2010](#)) has been withdrawn. The term *NEN 7513* in the [Electronic Data Processing Decree by Providers](#) is accordingly deemed to refer to the 2018 version.

19b. *The Publisher* will organise the *Personal record* in such a way that this can also serve as a log file of received *Notifications* and of *Subscriptions* entered into. *Issuer* will maintain a log file of sent *Notifications* and *Subscriptions* entered into.

19c. The retention period for the log files is at least 24 months and not more than 36 months. When the log files' retention period expires, they must be destroyed.

#### Explanatory Notes

The maximum retention period is determined for logging within the scope of MedMij traffic to prevent unnecessary storage of data and to protect the privacy of the user. These minimum and maximum retention periods for log files comply with the limits set for them by NEN7513 (in section 8.5).

20. *MedMij Maintenance* maintains an archive of all versions of the *Information service directory* ever distributed, doing the same for the *Client directory*, the *Whitelist* and the *Information service glossary*. The retention period, which is calculated from the end of the validity of the previous version, is not shorter than that for the log files as referred to in responsibility 19.

21a. *Publisher* provides *User* with the use case *UC Portability Report*. This enables *User* to automatically export a list, which is called the *Portability Report*, of all the times during a certain period that *User* has compiled this *Publisher* at a *Provider* in connection with health information in accordance with a certain *Information service*.

21b. *Publisher* pro-actively offers *User* with the export of a *Portability Report*:

- before *Publisher*, for whatever reason, halts its service provision to *User*,
- before *Publisher* removes the log files from which it would compile *Portability Reports* for *User* relating to a certain period.

21c. *Publisher* does not restrict *User* in the use of the *Portability Report* in the relationship between *User* and possible other and/or subsequent *Publishers*.

21d. The *Portability Report* complies with that which is laid down for it in the [Information Models](#) and has the technical form of an XML document that complies with the XML schema (sheet) that can be found on the page [XML schemas](#).

### Portability Report

The *Portability Report* provides *User* with a means of placing an important part of the health information that he has compiled in the *Personal record* in his PHE into any other PHEs he wishes (portability, transferability). This too contributes to the [Control](#) that the *User* has over his health information, to his continual free choice of *Individual's Service Provider* ([principle 7](#), in Dutch) and to limiting the disadvantage that he would suffer if his *Individual's Service Provider* were to halt its activities.

There is no guarantee that a *Portability Report* can be automatically 'played' by a PHE other than the one that actually created the report, although this may simply be because not all used *Information services* still have to be listed as valid in the *Information service catalogue*. In these types of cases, the *Portability Report* still provides information that is always precise and to some extent humanly readable and that can then be entered in the new PHE after all, if necessary by hand.

*Individual's Service Providers* can make their service provision to *Users* more powerful by providing an import function for *Portability Reports*. However, this is not mandatory and must be viewed in the light of [principle 3](#) (in Dutch).

A more powerful means of portability would be to have an exchange standard between PHEs. However, this would give rise to significant complexity and expenditure, not least because all previous versions of the MedMij Trust Scheme would have to be taken into consideration, as would *Information services* that by then were no longer listed as valid in the *Information service catalogue*.

## UC Collect

### Explanatory Notes

The figures below depict the flow diagram of the use case *Collect* for four different perspectives:

- the overall perspective;
- the perspective of the *Publisher*, who falls under the *Individual's Service Provider*. The last-named can read this figure as his mandatory participation in the use case *Collect*;
- the perspective of the *Issuer*, who falls under the *Provider's Service Provider*. The last-named can read this figure as his mandatory participation in the use case *Collect*;
- the perspective of the *User*.

The flow diagrams show first of all the situation in which all actions are successful, up to and including the final collection of the health information (this is known as the 'happy flow'). In line with the MedMij corporate identity, the two orange paths belong to the Individual's Domain and the blue to the Provider's Domain. Many actions in the flow diagrams are shown in colour. Together, the actions coloured in light grey form the authorisation flow with the actions coloured in light yellow together forming the authentication flow. In the flow diagrams for the specific perspectives, it is only those actions within the path that belongs to that perspective that are named. The actions in the other paths are compressed and depicted without names.

Finally, we will discuss the exceptions to the happy flow. Here, we will only work from the overall perspective.

## Overall perspective (happy flow)

### Explanatory Notes

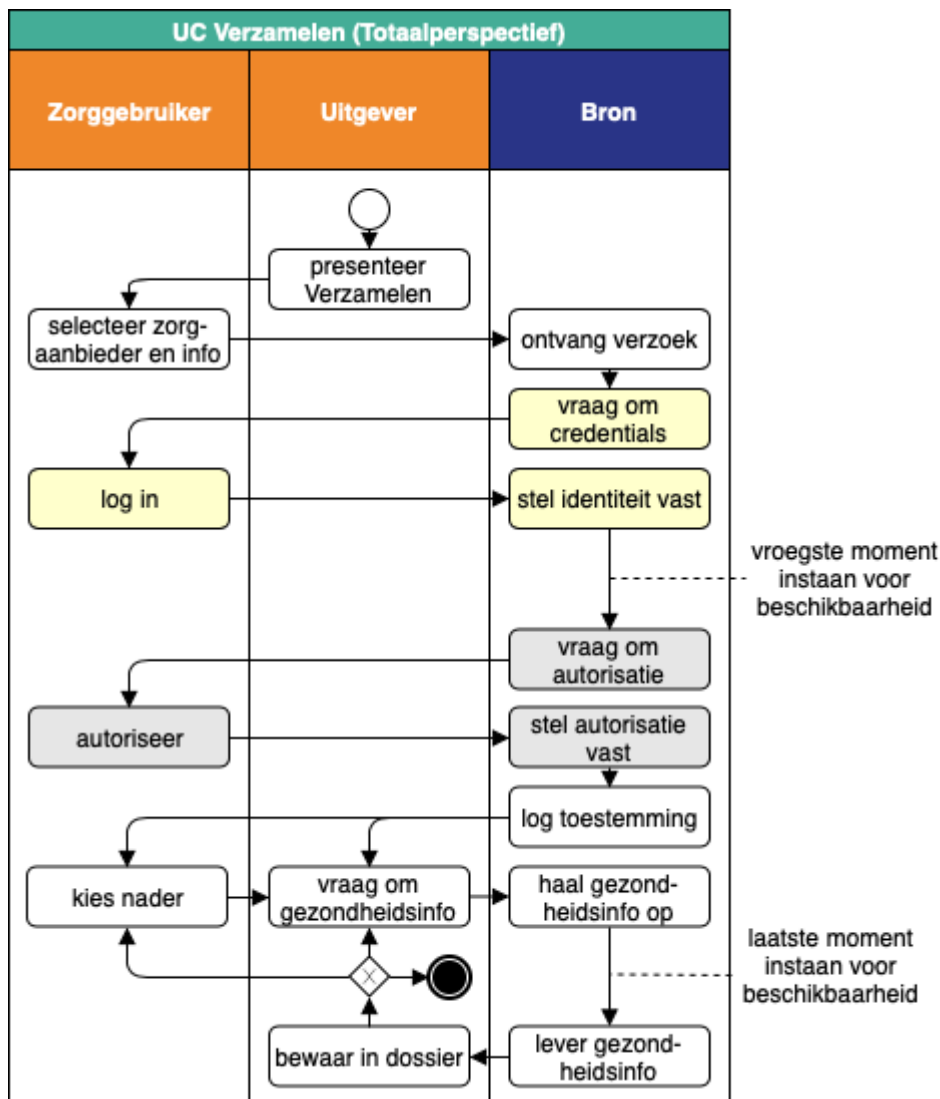
In all cases, each completion of the flow described in the diagram only has a single one of each of the roles named at the top.

The overall process of the *UC Collect* comprises the following steps:

- The *Publisher* presents the *User* with the option of collecting.
- The *User* expressly chooses the *Provider* for which he would like to collect information and the specific *Information service*. If desired, the *Information service Names* from the *Information service glossary* can be used for this. The request is passed to the relevant *Issuer*.
- The *Issuer* allows the *User* to authenticate himself.
- If this is successful, the earliest moment comes at which the *Issuer* guarantees that the *Provider* has - for the relevant *Information service* - any health information of this *Individual* available at all; otherwise, the happy flow terminates. The MedMij Trust Scheme recommends that the availability condition be made effective from the earliest stated moment. In this release, the MedMij Trust Scheme permits this condition to become effective later on but not later than the final moment stated in the figure.
- The *Issuer* asks the *User* whether he consents to the provision of the requested information to the *Publisher*. This request can be found on the page [Declaration of consent](#) (in Dutch).
- The *Issuer* logs this consent and lets *Publisher* know that consent was granted.
- The *Publisher* can now ask the *Issuer* questions about the health information.
- At the latest after receipt of the request, *Issuer* will guarantee that the *Provider* has some health information available about the *Individual* for the relevant *Information service*; otherwise, the happy flow terminates.
- Upon receipt, *Publisher* stores this information in the Personal record.

- If the *Information service* that *User* has authorised consists of multiple *Transactions* (see the [Information service catalogue](#), in Dutch, for this) then the *Publisher* may subsequently ask the *Issuer* again for the *Transactions* still remaining, possibly after new interaction with the *User*.
- The information stored includes the meta-information referred to in responsibility 19 of the [Process and Information Layer](#).

The availability condition belongs with [Control](#), not with [Exchange](#). The condition gives the *Provider* leeway to participate in the [Control](#) given to the *Individual*. However, because existing implementation architectures often centralise [Exchange](#) instead of [Control](#), they find it difficult to implement the availability condition during the control phase. This is why for the time being, the MedMij Trust Scheme offers the option of implementing this during the [Exchange](#) phase.



## Exceptions (overall perspective)

### Explanatory Notes



The table below describes the situations that relate to exceptions. All are discovered by the *Issuer*. In order to prevent *Publisher* from obtaining information about the existence of any treatment relationships before consent has been given for this, the distinction between the exceptions 2, 3 and 4 must not be made by *Publisher*.

These exceptions will be discussed again in the Application layer, with the [use case implementation Collect](#) but in this case now with their precise implementation and format of the error messages too.

The question of whether the *Provider* makes the requested health information available to the *Individual* is, first of all, a matter between *Provider* and *Individual*, who must have a treatment relationship for this. If there is such a treatment relationship then legislation applies to this making available (see [Legal Framework](#), in Dutch). Within this Trust Scheme, there is room for the *Provider* to make their own decision. However, because *Provider* and *Individual* are not *Participants* in the MedMij Trust Scheme, the MedMij Trust Scheme does not specify the precise logic to be used to decide whether to provide the health information or not. For reasons of privacy, however, the MedMij Trust Scheme does require there to be - or have been - a treatment relationship that the relevant health information is a part of and that the *Individual* is at least sixteen years old (see exception UC Collect 3).

When it comes to providing data about a person less than sixteen years old, consent or an authorisation to give consent must be granted by the person who bears the parental responsibility or statutory responsibility for the person who is less than sixteen years old. Because this version of the MedMij Trust Scheme does not yet provide for such consents or authorisations to give consent, this check can for the time being be made part of the availability condition. If a future release of the MedMij Trust Scheme does indeed include such consents or authorisations then the age condition must be kept separate from the availability condition.

nr.	exception	action	follow-up
UC Collect 1	<i>Issuer</i> finds the received request to be invalid.	<i>Issuer</i> informs <i>Publisher</i> about this exception. <i>Publisher</i> then informs <i>User</i> about this.	The entire flow stops immediately after being informed about the exception.
UC Collect 2	<i>Issuer</i> cannot establish the identity of the <i>User</i> .	<i>Issuer</i> informs <i>Publisher</i> that the request will not be granted.	The entire flow stops immediately after being informed about the exception.
UC Collect 3	<p><i>Issuer</i> establishes at any moment that there is no health information on the <i>Individual</i> with the <i>Provider</i> available for this <i>Information service</i>. This is always said to be the case if either:</p> <ul style="list-style-type: none"> <li>no treatment relationship can be demonstrated that would provide the basis for the collecting;</li> <li><i>User</i> is not yet sixteen years old. See the explanatory notes about the <a href="#">Availability condition and acceptability condition</a>.</li> </ul>		
	The submitted <a href="#">Declaration of consent</a> (in Dutch) is not issued.		

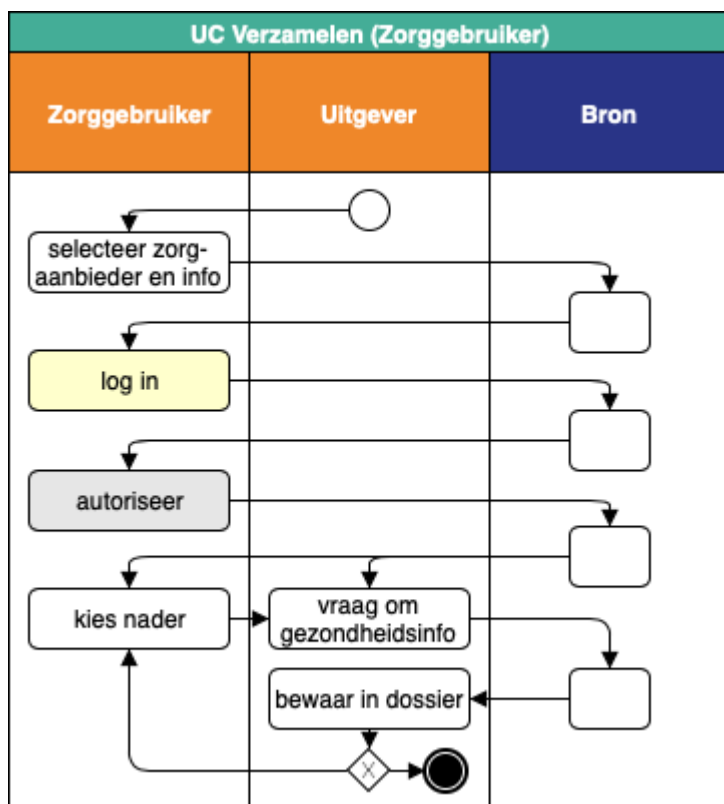


UC Collect 4			
UC Collect 5	<i>Issuer</i> is unable to determine the answer to the consent request.	<i>Issuer</i> informs <i>Publisher</i> about this exception. <i>Publisher</i> then informs <i>User</i> about this.	The entire flow stops immediately after being informed about the exception.
UC Collect 6	Even after consent has been given, <i>Issuer</i> can still decline to make health information available to the <i>Publisher</i> .	<i>Issuer</i> informs <i>Publisher</i> about this exception. <i>Publisher</i> then informs <i>User</i> about this, stating the reasons for this.	If the health information is indeed available in part (including if authorised) then the flow can still provide this.

## Perspective of the User (happy flow)

### Explanatory Notes

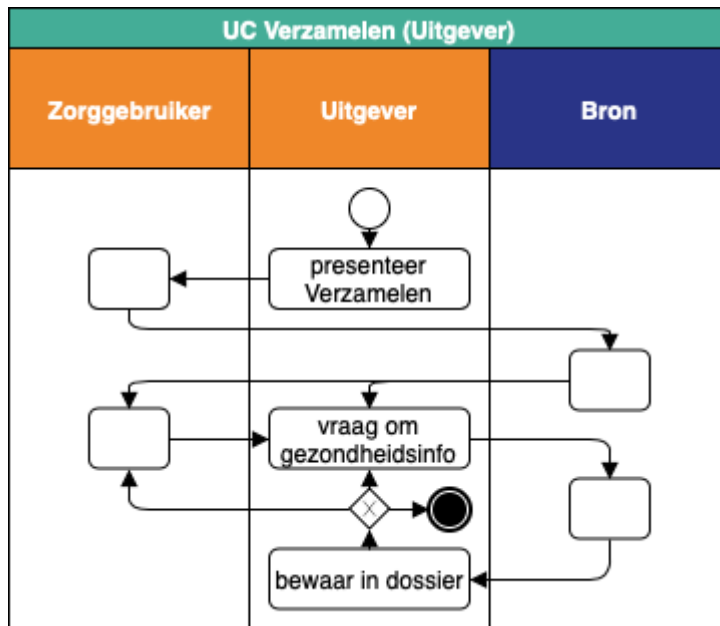
The *User* must complete three steps: the selection of *Provider* and *Information service*, the login and the authorisation. If all steps are successfully completed then the *Publisher* saves the consent for him, along with the health information received.



## Perspective of the Publisher (happy flow)

### Explanatory Notes

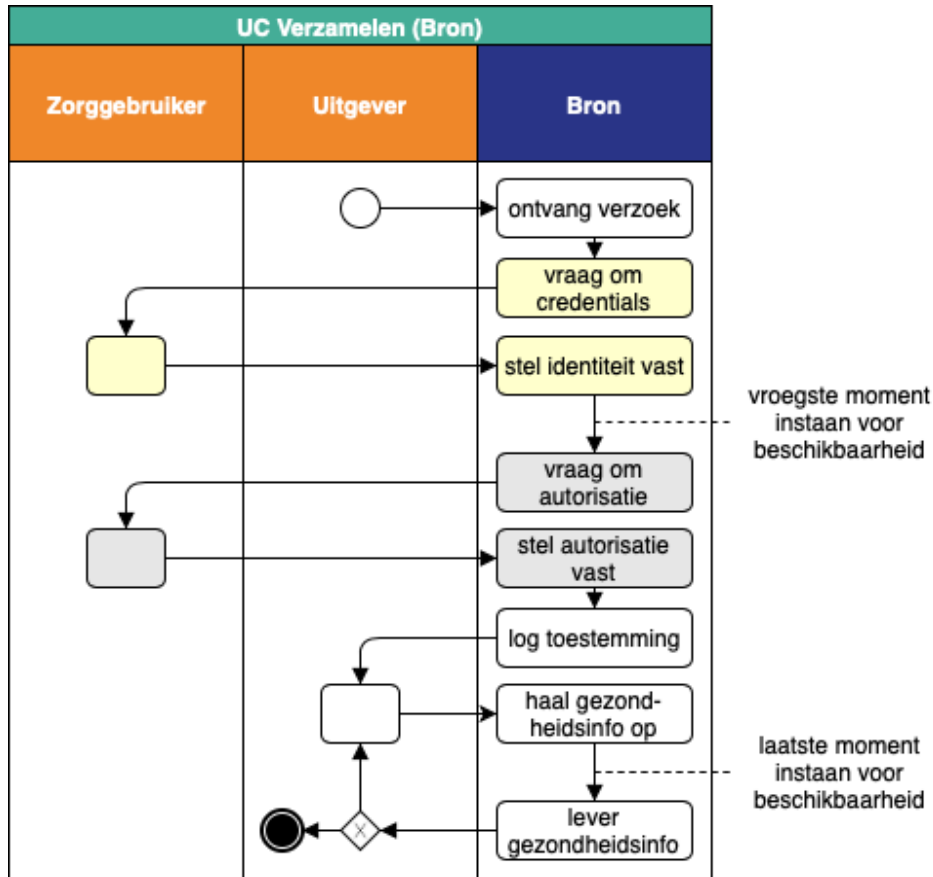
The *Publisher* starts the use case by presenting the *User* with the option to collect. After some time, they will receive from the *Issuer* the message that consent for this has been granted, following which they log this consent and retrieve the health information from the *Issuer* and saves.



### Perspective of the Issuer (happy flow)

### Explanatory Notes

After receiving the request to collect, the *Issuer* directs the authentication and the consent. If these are successful then he logs the consent and sends it to the *Publisher*. Ultimately the latter will return the request and receive the reply.



## UC Share

### Explanatory Notes

This page contains the flow diagrams for the *UC Share*. The use case is a mirror image of *UC Collect*. However, this 'reflection' does not mean that the roles of *Publisher* and *Issuer* are now allocated conversely, that is to say to *Provider's Service Provider* and *Individual's Service Provider* respectively. Such a turnaround would create a weaker, more process logistics-oriented form of management and take away the initiative from the *Individual's Service Provider* and thus from the *User* too. The MedMij Trust Scheme supports a stronger form of management and control, whereby also in the case of the *UC Share* the initiative lies with the *Publisher*. However, instead of dealing with an *Issuer* from where the *Publisher* obtains health information, he now deals with an *Addressee* to whom he provides such information. Just like the *Issuer* role in *UC Collect*, the *Addressee* role in this version of the MedMij Trust Scheme is now only linked to the legal role of the *Provider's Service Provider*.

A second benefit of choosing this option is that the *UC Share* has largely the same set-up as the *UC Collect*. As a result, this applies respectively to use case-implementations too, which accordingly can be re-used from each other. This does not affect the fact that there are some significant differences. At the *Process and Information* layer, they are as follows:

- Before the start of the use case, *User* should be able to simply indicate the information in their *Personal record* that they wish to share with a *Provider* still to be specified, and in doing so may assume that the *Publisher* knows which *Information service* applies.
- In contrast to *UC Collect*, the *Provider* must be given the opportunity to decide whether to 'open himself up' to the receipt of the relevant information. The *Addressee* must - after authentication of *User* - be able to determine whether the relevant information is welcome for the relevant *Provider*. This check on receptiveness will be carried out automatically, with the emphasis on achieving the synchronous user experience but with the implementation method being freely chosen.
- From a legal point of view, no explicit consent by the *User* needs to be given to the *Provider* for being allowed to receive the health information; this follows from the provision by the *User*. However, there are consent requirements in the relationship *User-Publisher* (regarding permission to provide the health information) but these relate to the relevant legislation and regulations. Nevertheless, just like in *UC Collect*, the *User* is asked to provide a confirmation.
- At the end of the use case, provided that the *Provider* turned out to be receptive to this, the relevant information will be placed by the *Publisher* with the *Provider*, via the *Addressee*. Just like with *UC Collect* - where no further requirements are set for the way in which the information is to be retrieved by the *Issuer* from the *Provider* - this applies in the *UC Share* too for the placement. All that is important here is that the *User* can assume that the *Provider* has taken note of the relevant information. The question of how to ensure this is not trivial but is instead left to the arrangements that the *Provider's Service Provider* makes and to the *Service Provision Agreement* that he enters into in this regard with the *Provider*.

The figures below depict the flow diagram for the use case *Share* from four different perspectives:

- the overall perspective;
- the perspective of the *User*;
- the perspective of the *Publisher*, who falls under the *Individual's Service Provider*. The last-named can read this figure as his mandatory participation in the use case *Share*;
- the perspective of the *Addressee*, who falls under the *Provider's Service Provider*. The last-named can read this figure as his mandatory participation in the use case *Share*.

First of all, the flow diagrams show the situation in which all actions are successful up to and including the ultimate sharing of the health information (this situation is known as the 'happy flow'). In line with the MedMij corporate identity, the two orange paths belong to the Individual Domain and the blue to the Provider's Domain. Many actions in the flow diagrams are shown in colour. Together, the actions coloured in light grey form the authorisation flow with the actions coloured in light yellow together forming the authentication flow. In the flow diagrams for the specific perspectives, it is only those actions within the path that belongs to that perspective that are named. The actions in the other paths are compressed and depicted without names.

Finally, we will discuss the exceptions to the happy flow. Here, we will only work from the overall perspective.

## Overall perspective (happy flow)

### Explanatory Notes

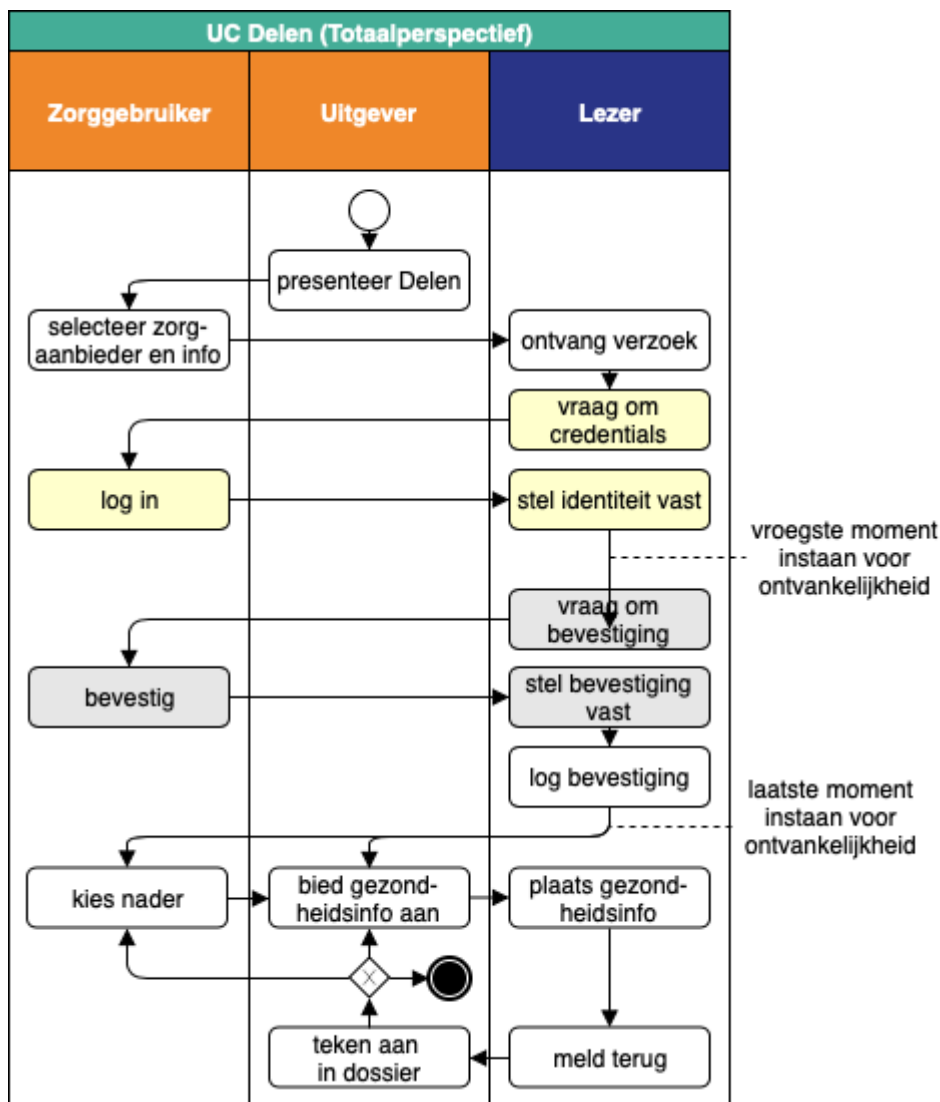
In all cases, each completion of the flow described in the diagram only has a single one of each of the roles named at the top.

The overall process of the UC Share has the following steps:

- The *Publisher* presents the *User* with the option to share.
- The *User* chooses the *Provider* that he wishes to share the information with and the *Information service*. If desired, the *Information service Names* from the *Information service glossary* can be used for this. The request goes to the relevant *Addressee*.
- The *Addressee* lets the *User* authenticate himself.
- This is then the earliest moment at which the *Addressee* guarantees that the *Provider* for the relevant *Information service* wishes to receive at least some health information about this *Individual*; otherwise, the happy flow terminates. The MedMij Trust Scheme recommends that the acceptability condition be made effective from the earliest stated moment. For the time being, the MedMij Trust Scheme permits a situation where this condition does not become effective until later on but no later than at the final moment stated in the figure.
- The *Addressee* asks the *User* whether he confirms the wish to have the information provided to the *Provider*. The question that the *User* has to be asked during the step 'confirm' is stated on the page [Declaration of Confirmation](#).
- The *Addressee* logs this confirmation and lets the *Publisher* know whether it was successful.
- Before the flow is then handed over to the *Publisher*, the *Addressee* will guarantee that the *Provider* wishes to receive - for the relevant *Information service* - at least some health information from this *Individual*; otherwise, the happy flow terminates.
- The *Publisher* can now place the health information with the *Addressee*.
- If the *Information service* that the *User* has authorised consists of multiple *Transactions* (see the [Information service catalogue](#) for this) then the *Publisher* may subsequently place with the *Addressee* again for the *Transactions* still remaining, possibly after new interaction with the *User*.
- Along with the information, the *Publisher* records the meta-information that is referred to in responsibility 19 of the [Processes and Information Layer](#).

See the block of explanatory notes about control and exchange at the bottom of the homepage of [Architecture and technical specifications](#). The acceptability condition is an aspect of the control, not of the exchange. The condition gives the *Provider* scope to participate in the control given to the *Individual*. However, because existing implementation architectures often centralise Exchange instead of Control, they find it difficult to implement the availability condition during the control phase.

This is why for the time being, the MedMij Trust Scheme offers the option of implementing this during the Exchange phase. However, with an eye to the future, *Participants* are advised to make an appropriate distinction in their implementation architectures between control and exchange and to get the first echelon to steer the second.



## Exceptions (Overall perspective)

### Explanatory Notes

The table below describes the situations that relate to exceptions. All are discovered by the *Addressee*. In order to prevent the *Publisher* from obtaining information about the existence of treatment relationships without confirmation (already or otherwise) being given for this, the distinction between exceptions 2, 3 and 4 must not be made by the *Publisher*.

In the case of the [use case implementation Share](#), these exceptions will be discussed again in the Application layer but now also in respect of their precise implementation and the format of the error messages.

The question of whether the *Provider*, in the check on receptiveness, declares himself receptive for the health information provided by the *Individual*, is, first of all, a matter between the *Provider* and the *Individual*, who must have a treatment relationship for this. Given such a treatment relationship, legislation applies to this receptiveness (see [Legal Framework](#)). Within this Trust Scheme, there is room for the *Provider* to make their own decision. However, because *Provider* and *Individual* are not *Participants* in the MedMij Trust Scheme, the MedMij Trust Scheme does not specify the precise logic to be used for the decision of whether to be receptive for the health information or not. However, for privacy reasons, the MedMij Trust Scheme does require that a treatment relationship must (have) existed in which the relevant health information belongs and that the *Individual* is at least sixteen years old (see exception UC Share 3).

When it comes to the sharing of data of a person who is less than sixteen years old, consent or authorisation to give consent must be granted by the person who bears the parental responsibility or statutory responsibility for the person who is less than sixteen years old. Since this version of the MedMij Trust Scheme does not yet provide for such consents or authorisations, at the current time this check can be made part of the acceptability condition. If a future release of the MedMij Trust Scheme does actually include such consents or authorisations then the age condition must be kept separate from the acceptability condition.

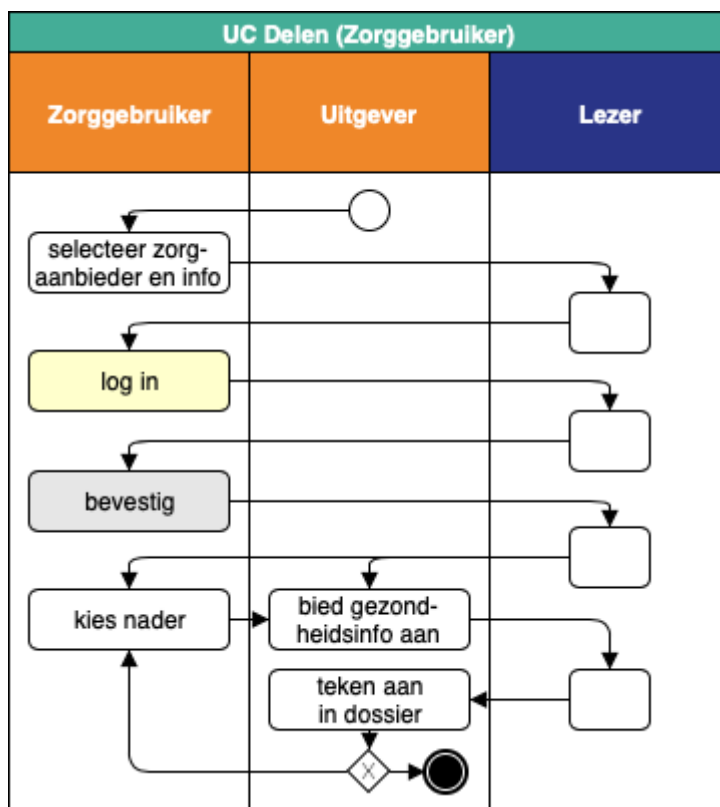
nr.	exception	action	follow-up
UC Share 1	<i>Addressee</i> finds the received request to be invalid.	<i>Addressee</i> informs <i>Publisher</i> about this exception. <i>Publisher</i> then informs <i>User</i> about this.	The entire flow stops immediately after being informed about the exception.
UC Share 2	<i>Addressee</i> is unable to establish the identity of the <i>User</i> .	<i>Addressee</i> informs <i>Publisher</i> that sharing will not be permitted.	All stop the flow immediately after being informed about the exception.
UC Share 3	<i>Addressee</i> establishes at any time that relevant information of the <i>Individual</i> from the <i>Provider</i> is not welcome. This is always said to be the case if either: <ul style="list-style-type: none"> <li>no treatment relationship can be demonstrated that would provide the basis for the sharing;</li> <li><i>User</i> is not yet sixteen years old. See the explanatory notes about the <a href="#">Availability condition and the acceptability condition</a>.</li> </ul>		
UC Share 4	The confirmation is not given.		
UC Share 5	<i>Addressee</i> is unable to determine the answer to the confirmation request.	<i>Addressee</i> informs <i>Publisher</i> about this exception. <i>Publisher</i>	

		then informs <i>User</i> about this.	The entire flow stops immediately after being informed about the exception.
UC Share 6	Even after confirmation, <i>Publisher</i> cannot yet place the health information with the <i>Addressee</i> .	<i>Publisher</i> then informs <i>User</i> about this, stating the reasons for it.	If health information can indeed be placed in part (including if authorised) then the flow can still provide this.

## Perspective of the *User* (happy flow)

### Explanatory Notes

To start with, the *User* must complete three steps: selection of *Provider* and *Information service*, logging in and confirmation. He may subsequently opt to have further information placed.

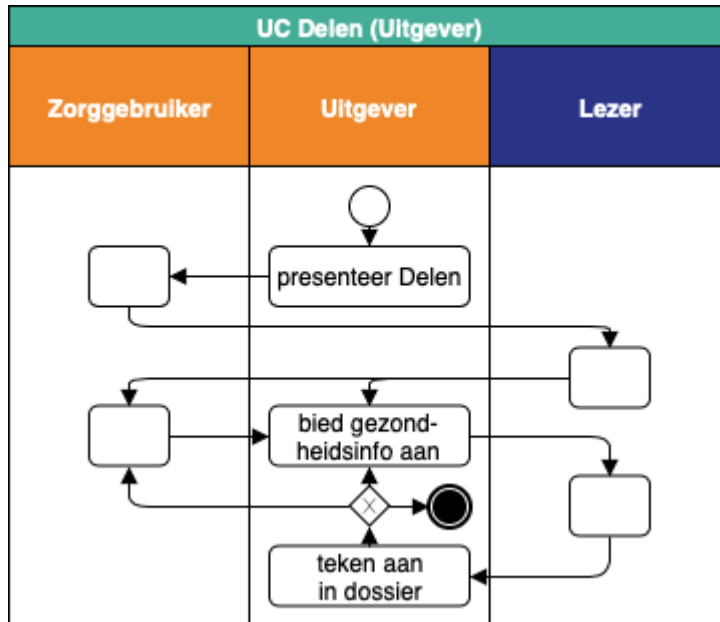


## Perspective of the *Publisher* (happy flow)

### Explanatory Notes

The *Publisher* starts the use case by presenting the *User* with the option to share. After some time, he will receive from the *Addressee* the message that the relevant wish has been confirmed by *User*, following which he offers the health information to the *Addressee*. He records the response to this in the *Personal record*.

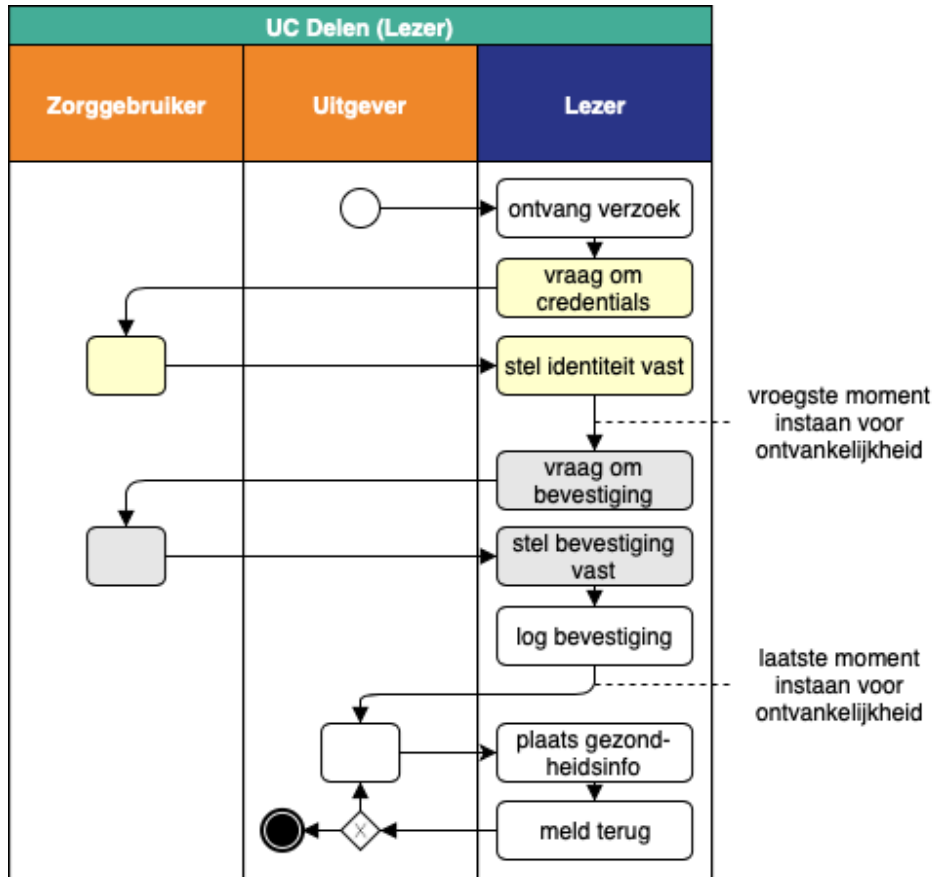




## Perspective of the *Addressee* (happy flow)

### Explanatory Notes

After receiving the request to share, the *Addressee* directs the authentication and the confirmation. If these are successful then they log the confirmation. Ultimately the *Publisher* provides them with the health information for placement with the *Provider*. The *Addressee* reports the result of this.



## UC Subscribe

### Explanatory Notes

The figures below contain the flow diagram for the use case *Subscribe* from four different perspectives:

- the overall perspective;
- the perspective of the *Publisher*, who falls under the *Individual's Service Provider*. The last-named can read this figure as his mandatory participation in the use case *Subscribe*;
- the perspective of the *Issuer*, who falls under the *Provider's Service Provider*. The last-named can read this figure as his mandatory participation in the use case *Subscribe*;
- the perspective of the *User*.

The use case *Subscribe* belongs entirely to the primary function *Control*. It includes the entering into, the changing of the duration of and the termination of *Subscriptions*.

First of all, the flow diagrams show the situation in which all actions are successful, up to and including the ultimate entering into of a *Subscription* (this situation is known as the 'happy flow'). The two orange paths belong to the Individual Domain and the blue one to the Provider's Domain. Together, the actions coloured in light grey form the authorisation flow with the actions coloured in light yellow together forming the authentication flow. In the flow diagrams for the specific perspectives, it is only those actions within the path that belongs to that perspective that are named. The actions in the other paths are compressed and depicted without names.

Finally, we will discuss the exceptions to the happy flow. Here, we will only work from the overall perspective.

## Overall perspective (happy flow)

### Explanatory Notes

In all cases, each completion of the flow described in the diagram only has a single one of each of the roles named at the top.

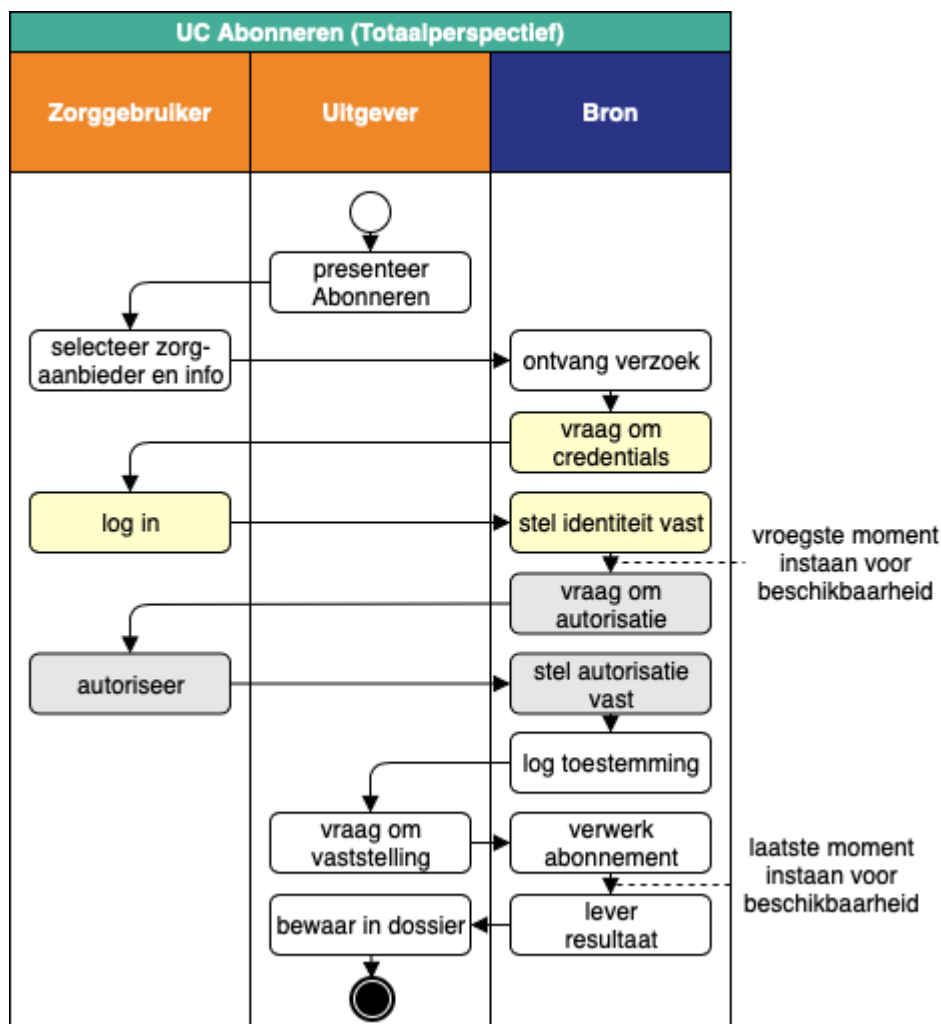
The overall process of the *UC Subscribe* has the following steps:

- The *Publisher* presents the *User* with the option of entering into, modifying or terminating *Subscriptions*.
- The *User* explicitly selects for the entering into a *Subscription* the *Provider* and the specific *Information service* and selects for the modification or termination of the relevant *Subscription*. If desired, the *Information service Names* from the *Information service glossary* can be used for this. The request is passed to the relevant *Issuer*.
- The *Issuer* allows the *User* to authenticate himself.
- If it relates to the entering into or modification of a *Subscription*, this is then the earliest moment at which the *Issuer* guarantees that the *Provider* has - for the relevant *Information service* - at least some health information available from this *Individual*; otherwise, the happy flow terminates. The MedMij Trust Scheme recommends that the availability condition be

made effective from the earliest stated moment. In this release, the MedMij Trust Scheme permits this condition to become effective later on but not later than the final moment stated in the figure. The termination of a *Subscription* cannot be refused by the *Provider*.

- The *Issuer* asks the *User* whether he gives his consent to the provision of the requested information to the *Publisher*. This request can be found on the page [Declaration of consent for subscription](#).
- The *Issuer* logs this consent and lets *Publisher* know that consent was granted.
- The *Publisher* can now ask the *Issuer* for the latter's determination of the entering into, modification or termination of the *Subscription*.
- If it relates to the entering into or modification of a *Subscription* then no later than the receipt of the request the *Issuer* will guarantee that the *Provider* for the relevant *Information service* has at least some health information available from this *Individual*; otherwise, the happy flow terminates.
- Upon receipt of the result, the *Publisher* processes the new, modified or terminated *Subscription* in the *Personal record*.
- The information stored includes the meta-information referred to in responsibility 19 of the [Process and Information](#) layer.

The availability condition belongs with [Control](#), not with [Exchange](#). The condition gives the *Provider* leeway to participate in the [Control](#) given to the *Individual*. However, because existing implementation architectures often centralise *Exchange* instead of [Control](#), they find it difficult to implement the availability condition during the control phase. This is why for the time being, the MedMij Trust Scheme offers the option of implementing this during the *Exchange* phase.



## Exceptions (overall perspective)

### Explanatory Notes

The table below describes the situations that relate to exceptions. All are discovered by the *Issuer*. In order to prevent *Publisher* from obtaining information about the existence of any treatment relationships before consent has been given for this, the distinction between the exceptions 2, 3 and 4 must not be made by *Publisher*.

The question of whether *Provider* makes the requested health information available to the *Individual* is, first of all, a matter between the *Provider* and the *Individual*, who must have a treatment relationship for this. Given such a treatment relationship, legislation applies to this provision (see [Legal Framework](#)). Within this Trust Scheme, there is room for the *Provider* to make their own decision. However, because *Provider* and *Individual* are not *Participants* in the MedMij Trust Scheme, the MedMij Trust Scheme does not specify the precise logic to be used to decide whether to provide the health information or not. However, for privacy reasons the MedMij Trust Scheme

does require that a treatment relationship must exist or must have existed in which the relevant health information belongs and that the *Individual* must be at least sixteen years old (see exception UC Subscribe 3).

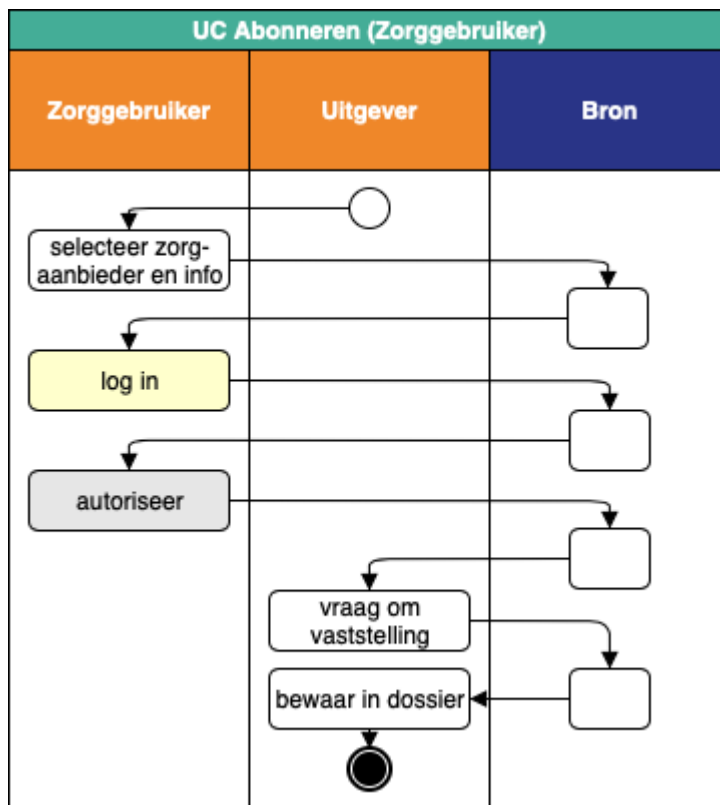
When it comes to providing data about a person less than sixteen years old, consent or an authorisation to give consent must be granted by the person who bears the parental responsibility or statutory responsibility for the person who is less than sixteen years old. Because this version of the MedMij Trust Scheme does not yet provide for such consents or authorisations to give consent, this check can for the time being be made part of the availability condition. If a future release of the MedMij Trust Scheme does indeed include such consents or authorisations then the age condition must be kept separate from the availability condition.

nr.	exception	action	follow-up
UC Subscribe 1	<i>Issuer</i> finds the received request to be invalid.	<i>Issuer</i> informs <i>Publisher</i> about this exception. <i>Publisher</i> then informs <i>User</i> about this.	The entire flow stops immediately after being informed about the exception.
UC Subscribe 2	<i>Issuer</i> cannot determine the identity of the <i>User</i> .	<i>Issuer</i> informs <i>Publisher</i> that the request will not be granted.	The entire flow stops immediately after being informed about the exception.
UC Subscribe 3	<i>Issuer</i> determines at any time on behalf of the <i>Provider</i> that the availability condition is not being complied with. This is always said to be the case if either: <ul style="list-style-type: none"> <li>no treatment relationship can be demonstrated that would provide the basis for the compiling;</li> <li><i>User</i> is not yet sixteen years old. See the explanatory notes to <a href="#">Availability condition and acceptability condition</a>.</li> </ul>		
UC Subscribe 4	User does not issue a <a href="#">Declaration of consent for subscription</a> (in Dutch).		
UC Subscribe 5	<i>Issuer</i> is unable to determine the answer to the consent request.	<i>Issuer</i> informs <i>Publisher</i> about this exception. <i>Publisher</i> then informs <i>User</i> about this.	The entire flow stops immediately after being informed about the exception.
UC Subscribe 6	Even after consent for this has been given, <i>Issuer</i> can still decline to provide the health information or the <i>SubscriptionInformation</i> to the <i>Publisher</i> .	<i>Issuer</i> informs <i>Publisher</i> about this exception. <i>Publisher</i> then informs <i>User</i> about this, stating the reasons for it.	If the health information is indeed available in part (including if authorised) then the flow can still provide this.

## Perspective of the *User* (happy flow)

### Explanatory Notes

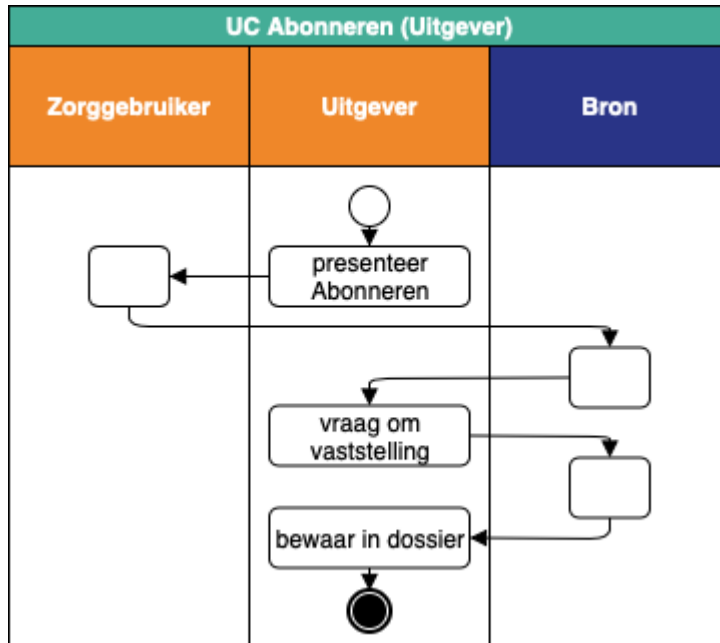
The *User* must complete three steps: selection of *Provider* and *Information service*, the login and the authorisation. If all steps are successful then the *Publisher* stores this determination for him.



### Perspective of the *Publisher* (happy flow)

### Explanatory Notes

The *Publisher* starts the use case by presenting the *User* with the option of subscribing. After some time, he receives from the *Issuer* the message that the consent for this has been granted, following which he logs this consent and arranges for the subscription to be determined by the *Issuer*, and stores it.

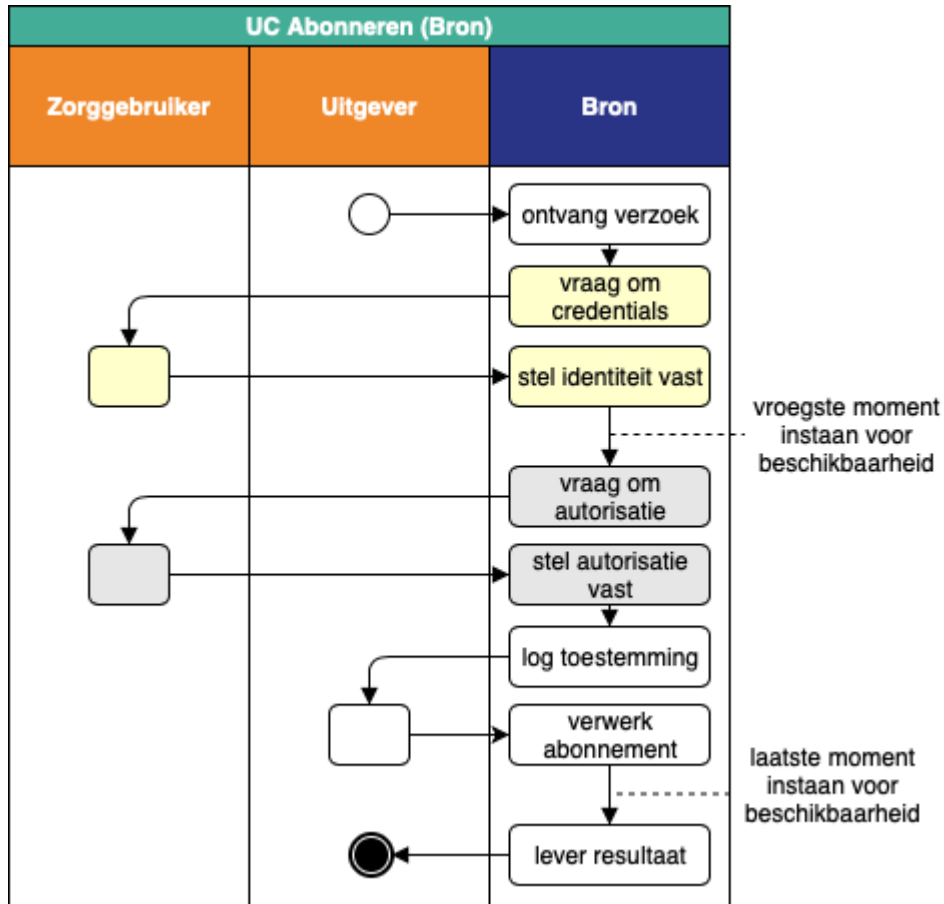


## Perspective of the *Issuer* (happy flow)

### Explanatory Notes

The *Issuer* directs the authentication and the consent once he has received the request. If these are successful then he logs the consent and sends it to the *Publisher* who will ultimately request the determination and receive the answer.





## UC Notify

### Explanatory Notes

The figures below show the flow diagram for the use case *Notification* from four different perspectives:

- the overall perspective;
- the perspective of the *User*;
- the perspective of the *Publisher*, who falls under the *Individual's Service Provider*. The last-named must read this figure as his mandatory participation in the use case *Notification*;
- the perspective of the *Issuer*, who falls under the *Provider's Service Provider*. The last-named must read this figure as his mandatory participation in the use case *Notification*.

First of all, the flow diagrams show the situation in which all actions are successful (this situation is known as the 'happy flow'). The orange paths belong - in line with the MedMij corporate identity - to the Individual Domain, with the blue to the Provider's Domain. In the flow diagrams for the specific perspectives, it is only those actions within the path that belongs to that perspective that are named. The actions in the other paths are compressed and depicted without names.

Finally, we will discuss the exceptions to the happy flow. Here, we will only work from the overall perspective.

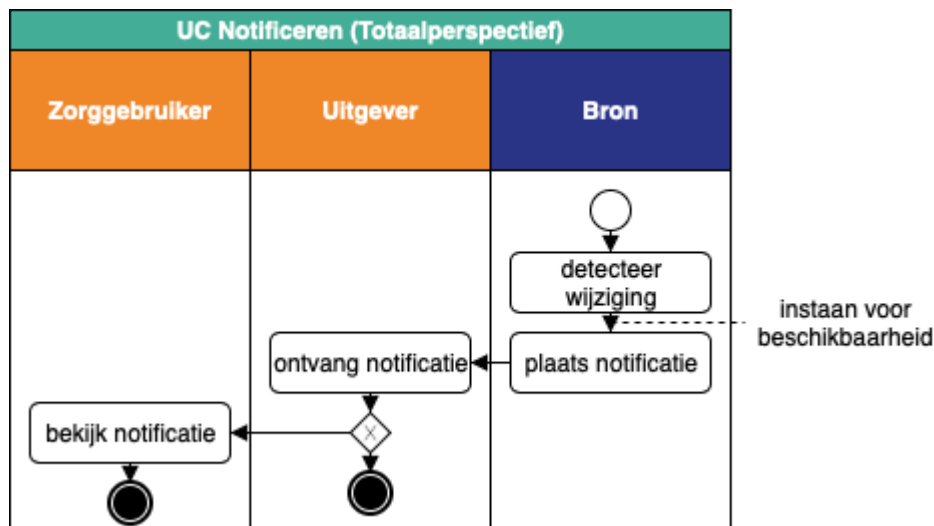
## Overall perspective (happy flow)

### Explanatory Notes

In all cases, each completion of the flow described in the diagram only involves a single one of each of the roles named at the top of it.

The overall process of the *UC Notify* has the following steps:

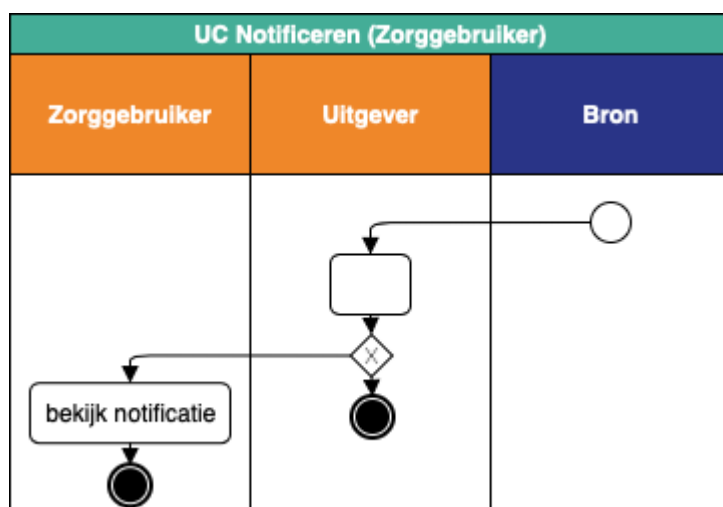
- Either the *Issuer* detects a change in (health or other) information for which *User* has entered into a *Subscription* (a content-related change) or else the *Issuer* terminates, on his own initiative, a specific *Subscription* (a subscription change).
- If it relates to a content-related change then it is determined that the *Provider* guarantees the availability of the relevant health information. The notion of availability is the same as the one in [UC Collect](#).
- The *Issuer* places a *Notification* with the *Publisher* and stores the meta-information that is referred to in responsibility 19b of the [Process and Information](#) layer.
- Upon receipt of a *Notification*, the *Publisher* stores the meta-information that is referred to in responsibility 19b of the [Process and Information](#) layer.
- The *Publisher* may inform the *User* about the *Notification*. If this is done by means of a text message (SMS) then the texts that are used for this are included on the page [Notification of User](#) (in Dutch).



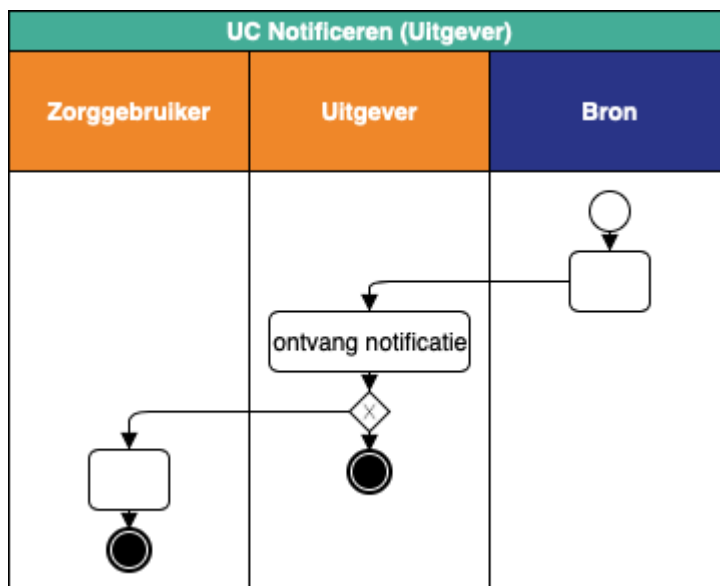
## Exceptions (overall perspective)

nr.	exception	action	follow-up
UC Notify 1	<i>Publisher</i> finds the received <i>Notification</i> to be invalid.	<i>Publisher</i> informs <i>Issuer</i> about this exception.	The entire flow stops immediately after being informed about the exception.
UC Notify 2	<i>Publisher</i> cannot process the <i>Notification</i> at all or else cannot do so completely or in time.	<i>Publisher</i> informs <i>Issuer</i> about this exception.	The entire flow stops immediately after being informed about the exception.

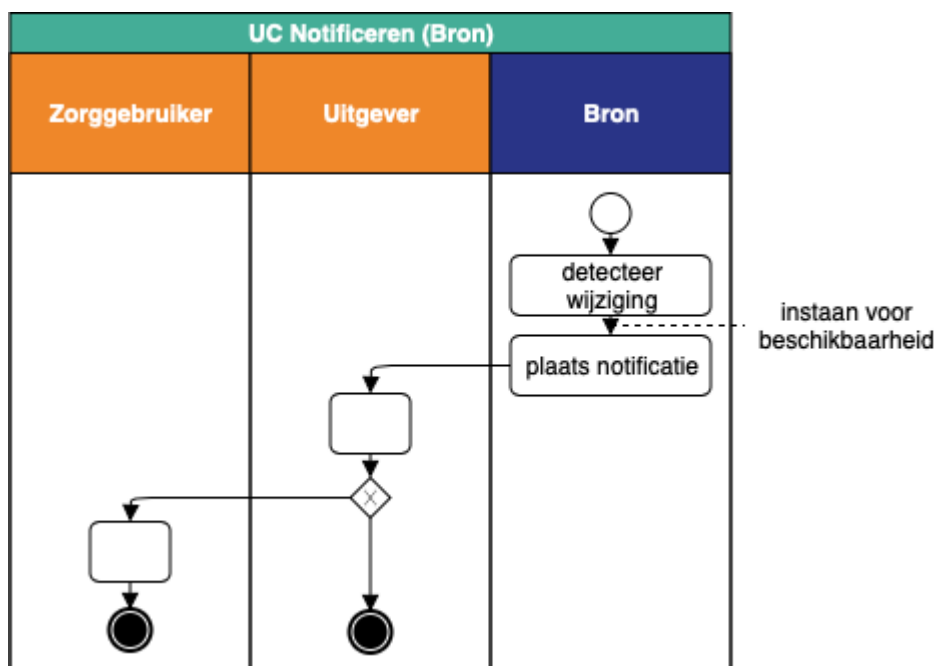
## Perspective of the *User* (happy flow)



## Perspective of the *Publisher* (happy flow)



Perspective of the *Issuer* (happy flow)

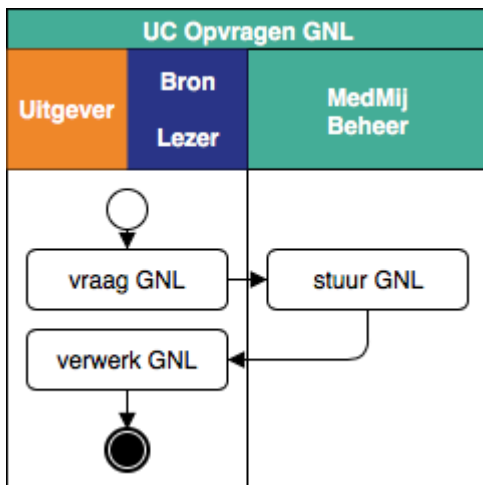


## UC Retrieve Isg

### Flow diagram

#### Explanatory Notes

In all cases, each completion of the flow described in the diagram only has a single one of each of the roles named at the top. In the left column, this means: a single *Publisher* or a single *Issuer* /*Addressee*.

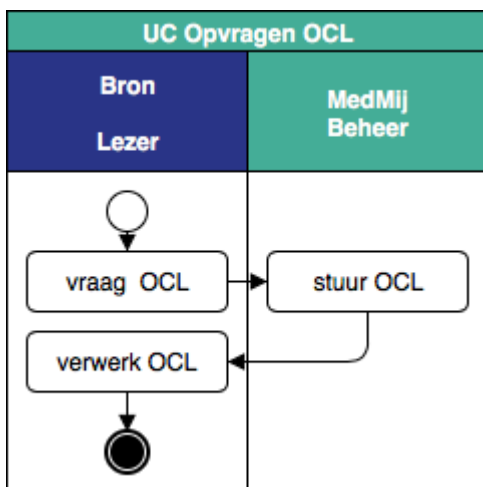


## UC Retrieve Rcd

### Flow diagram

#### Explanatory Notes

In all cases, each completion of the flow described in the diagram only has a single one of each of the roles named at the top.

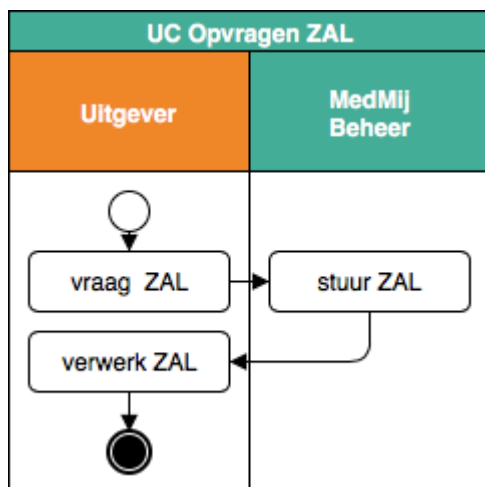


## UC Retrieve Dcd

### Flow diagram

#### Explanatory Notes

In all cases, each completion of the flow described in the diagram only has a single one of each of the roles named at the top.



## Availability condition and acceptability condition

### Responsibilities

1a. The *Provider* pursues policy in respect of the keeping available of health information (and *Subscriptions* to *Notifications* about it) for, and being receptive for health information from, certain *Individuals* on certain *Information services*.

1b. The *Provider's Service Provider* carries out, as the processor for each controller *Provider*, his policy referred to in responsibility 1a in [UC/UCI Collect](#), [UC/UCI Subscribe](#), [UC/UCI Share](#) and [UC/UCI Notify](#). The *Provider's Service Provider* does not carry out any policy of his own in this regard that is in addition to that of the *Providers*.

1c. The policy referred to in responsibility 1a only discriminates in respect of a single aspect, namely that of the *Individual* and the *Information service*. In particular, discrimination in respect of *Individual's Service Provider* is excluded, unless this is required by the MedMij Trust Scheme.

#### Explanatory Notes

##### Explanatory Notes

The guaranteeing of the availability condition and the acceptability condition comes into force:

- somewhere between the user authentication and the exchange of health information in [UC/UCI Collect](#) and [UC/UCI Subscribe](#), and in [UC/UCI Share](#) respectively;
- immediately at the start of [UC/UCI Notify](#);

There are two reasons for this:

1. It aims to ensure that - as soon as possible after the authentication of the *Individual*, and in any case before the health information is exchanged between *Publishing Server* and *Resource Server* - it may be assumed that two conditions have been fulfilled for the compiling or sharing of the relevant information, namely: the existence of a (current or past) treatment relationship as a basis for it and that the *Individual* in question is at least sixteen years old. It is the ultimate legal responsibility of the *Provider* to verify these conditions or to arrange for this to be done. With regard to the age issue, see also the [Legal Framework](#) (in Dutch).
2. They give the *Provider* the opportunity to impose - at his discretion - additional one-off or systematic restrictions on the arranging of the compiling or sharing of information or on the arranging of the subscribing to notifications, for example for technical reasons or due to special situations, special patients or harrowing content.

In other words, the *Provider's Service Provider* guarantees - in letting the process proceed - that the treatment relationship is present and that the age is sufficient. How the *Provider's Service Provider* guarantees this (with the *Provider*) is entirely up to him. The following, for instance, may contribute to this guaranteeing:

- legal means, such as provisions in the service provision agreement between *Provider* and *Provider's Service Provider*;
- organisational measures relating to the way in which *Providers* manage the Personal record, so that it can be seen from the Personal record information, its organising or even from its mere presence, whether it is based on a treatment relationship;
- automated logic that for a certain *Individual* and a certain *Information service* determines the receptiveness/availability at a certain *Provider*, this following on from organisational measures.



The MedMij Trust Scheme does not make it mandatory to explicitly administer the age data and the treatment relationship data. If the existence of a treatment relationship or a sufficient age can - on legal and/or organisational grounds - be implied by other data then the last-named data may also be used with this implication. This is why the MedMij Trust Scheme does not specify any logic for the conditions; instead, it solely lays down two necessary components of their post condition: the *Individual* is of sufficient age, and the existence of a current or former applicable treatment relationship.

If unavailability is found to be the case then this says nothing about the precise reason for it. It cannot even be concluded from this that either the treatment relationship is lacking or the *Individual* is not old enough. This is because the *Provider* can also have refused for other reasons.

For reasons of data minimisation and user-friendliness, the availability condition and the acceptability condition will preferably come into force as soon as possible, namely immediately after the authentication of the *Individual* and still prior to the authorisation request (the early variant). The availability condition and the acceptability condition belong by their nature with the [primary function Control](#) and not with *Exchange*. Conversely, the implementation of the conditions for some *Participants* would be easier if these conditions did not need to come into force until the process has arrived at the *Resource Server* (the late variant).

The early and late variants are compared below from the perspectives of data minimisation and user-friendliness. Both issues must be viewed from the perspective of the entire use case and all roles involved, as choosing between the early and the late variant has consequences at multiple places simultaneously. The weighing-up for this issue distinguishes between four different situations, depending on two questions:

- Does the *Provider* consider the information to (ultimately or otherwise) be available/receptive or himself to be available/receptive to it?
- Does the *Individual* (ultimately or otherwise) give his consent for this?

By the way, the late variants differ subtly between both [UC/UCI Collect](#) and [UC/UCI Share](#). In [UC/UCI Share](#), in comparative terms, the late variant is still a step earlier than in [UC/UCI Collect](#). This is because otherwise a processing (namely: a placement) of health information by the *Resource Server* would take place even before it turned out that the *Provider* was not receptive to this. In [UC/UCI Collect](#) this can take place a step later because the action to be prevented is only the exchange with the *Publishing Server*.

In terms of data minimisation, the two variants can be compared as follows:

	(ultimately or otherwise) indeed available/receptive	(ultimately or otherwise) not available /not receptive
(ultimately or otherwise) indeed consent given	<ul style="list-style-type: none"> <li>• If separate automated logic is used for a test of availability or receptiveness, the early variant requires additional data transfer compared to the late variant, namely between <i>Authorization Server</i> and the component(s) that it addresses in order to execute this test. This data transfer does, however,</li> </ul>	<ul style="list-style-type: none"> <li>• In contrast to the early variant, in the late variant all the data transfer unnecessarily takes place after the authentication (the consent request, the distributing of Authorisation code and access token and the addressing of the <i>Resource Server</i>). This data transfer extends across responsibility boundaries.</li> <li>• In the late variant, the <i>Publishing Server</i> unnecessarily learns more about the availability/receptiveness, and thus</li> </ul>

	<p>take place entirely within the responsibility of a single controller (i.e. a party that has responsibility for processing); no provision takes place.</p> <ul style="list-style-type: none"> <li>Only in the early variant does the <i>Authorization Server</i> additionally learn that the treatment relationship and age are in order. In the late variant, it is only the <i>Resource Server</i> that learns this. This does not affect the fact that both come under the same ultimately responsible <i>Provider's Service Provider</i>.</li> </ul>	<p>about the <i>Individual</i>, from the <i>Resource Server</i> than in the early variant from the <i>Authorization Server</i>. In the early variant, the relevant exception can, after all, viewed from the <i>Publishing Server</i>, also be caused by failing authentication or refusal to give consent. In the late variant, however, the <i>Publishing Server</i> does indeed come to know, through receipt of the unnecessary Authorisation code, that there is both a treatment relationship and an age that is sufficient.</p>
<b>(ultimately or otherwise) no consent</b>		<p>In contrast to in the early variant, in the late variant a superfluous consent request is made. This data transfer takes place across the relatively unsafe front-channel.</p>

The two variants can be compared with each other as follows in respect of user-friendliness:

	<b>(ultimately or otherwise) indeed available /receptive</b>	<b>(ultimately or otherwise) not available/ not receptive</b>
<b>(ultimately or otherwise) consent indeed given</b>	no difference	<p>In the early variant, the <i>Individual</i> is informed immediately, so that he /she:</p> <ul style="list-style-type: none"> <li>does not need to carry out any unnecessary or confusing act (meaningless consent) that has legal consequences, as is the case in the late variant;</li> <li>learns more precisely than in the late variant why an exchange has failed. In the late variant, this failing can occur for other reasons, so that the <i>Individual</i> would have to rely on support queries for clarification, which may even be directed at the <i>Provider</i>. In the early variant, while it's true that the Exceptions 2, 3 and 4 in <i>UC/UCI Collect</i>, <i>UC/UCI Subscribe</i> and <i>UC/UCI Share</i> are all included in a single notification to the <i>Publishing Server</i>, so that the latter cannot distinguish between failing authentication, failing authorisation and failing availability/receptiveness, the <i>Individual</i> does indeed know himself/herself the result of the authentication and authorisation, thanks to his/her prior direct interaction with the <i>Authorization Server</i>, and accordingly can deduce after all from this combined notification - without the <i>Publishing Server</i> knowing about this - whether there was failing availability/accessibility.</li> </ul>
<b>(ultimately or</b>		

**otherwise)  
no  
consent**

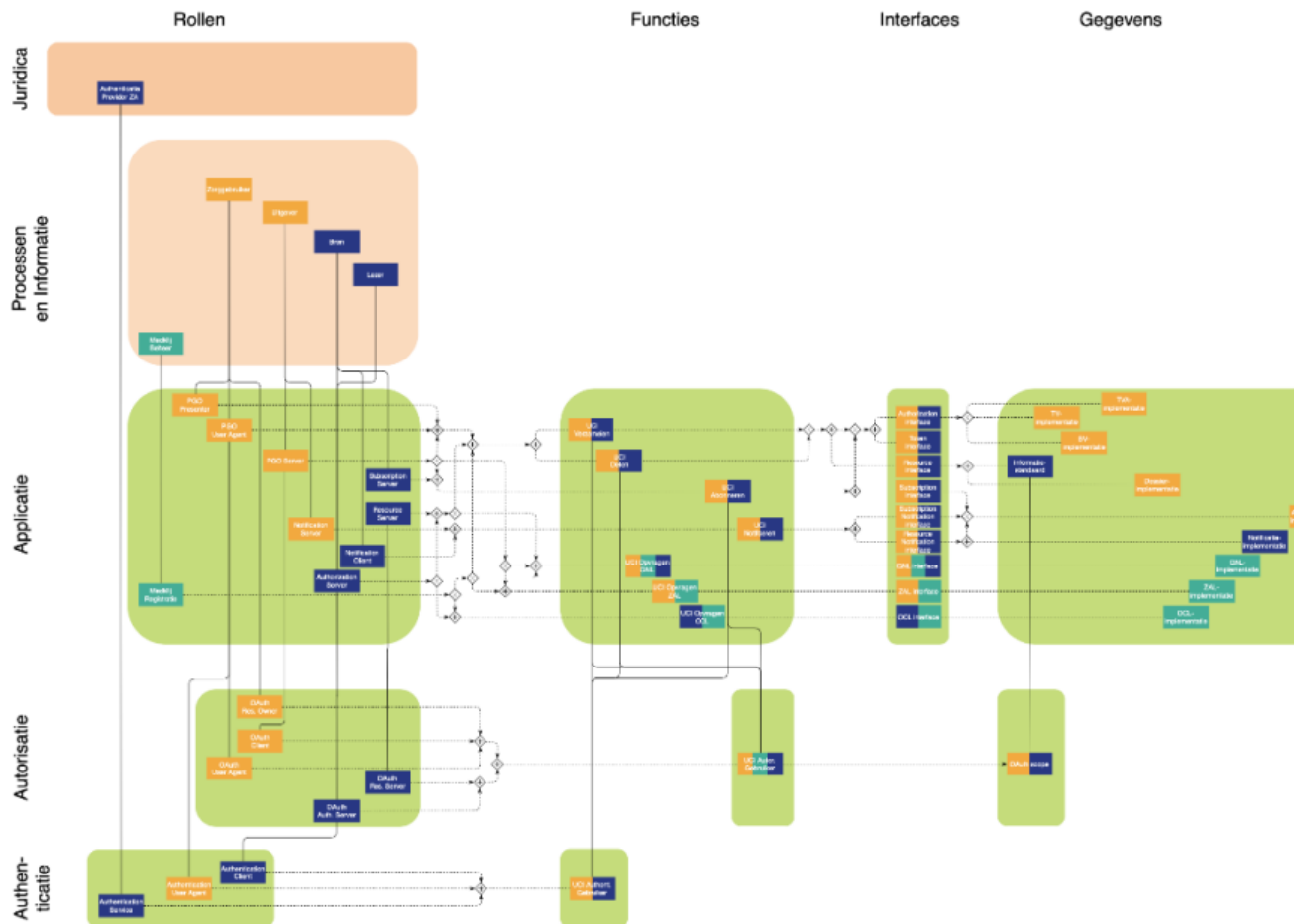
In the early variant, the Individual is informed immediately and does not need to carry out any unnecessary or confusing act (hollow rejection), in contrast to the late variant.

The cases where the *Provider* considers the information to be available/receptive (or himself available/receptive for the information), based on the reasonable behaviour of the *Publishing Server*, are probably more numerous than those where this is not the case. On the other hand, the disadvantages of the early variant for the first-named cases are relatively minor, because the *Provider's Domain* and the *Authorization Server* must already be sufficiently protected for other reasons, even if this is just due to the use made of the BSN. In addition, there is only additional data transfer in so far as automated logic is deployed that means that roles other than the *Authorization Server*, and thus outside the MedMij Trust Scheme, are addressed for this.

In this release, the MedMij Trust Scheme accordingly recommends the early variant, due to the aforementioned analysis. However, the MedMij Trust Scheme also permits the late variant, in order to give *Provider's Service Providers* both the opportunity to link up quickly and the time to consider how the early variant could be implemented over time.

Responsibility 1c guarantees the all-to-all principle ([principle 7](#), in Dutch) by forbidding the *Provider's Service Providers* to exclude certain *Individual's Service Providers* from *Subscriptions to Information services* (and from the Information services themselves) that they disclose from any *Provider*.

## Application



### Introduction

For an overview of all the architectural layers and an explanation of the meaning of the symbols and lines, see the [overview page](#).

The abbreviation:

- DCf stands for *Declaration of confirmation* (in Dutch);
- Isg stands for *Information service glossary*;
- Cld stands for *Client directory*;
- DCs stands for *Declaration of consent* (in Dutch)
- DCs-S stands for *Declaration of consent for subscription* (in Dutch);
- Isd stands for *Information service directory*.

## Roles

### 1. Publisher:

- offers *User*, with, in the context of the applicable *Service Provision Agreement*, an automated role for use, here called the: *Publishing Server*. A single *Publisher* offers one or more *Publishing Servers*, with each *Publishing Server* being offered by a single *Publisher*.

- b. makes, if they offer *UC Notify* to *Provider*, an automated *Notification Server* role available, allowing the *Provider* to offer *Notifications*. A single such *Publisher* one or more *Notification Servers*, with each *Notification Server* being offered by a single *Publisher*.
2. *Issuer*:
  - a. offers, and *Addressee* offers, an automated service, for the exchanging - on behalf of *Providers* - of health information with *Publishing Server*, which consists of *Authorization Server* and *Resource Server*. A single *Issuer* and/or *Addressee* offer(s) one or more combinations of a single *Authorization Server* and a single *Resource Server* and each combination of a single *Authorization Server* and a single *Resource Server* is offered by a single *Issuer* and/or *Addressee*.
  - b. offers, if they offer *UC Subscribe*, an automated service for entering into *Subscriptions* on behalf of *Providers*, consisting of *Authorization Server* and *Subscription Server*. Each such *Issuer* offer(s) one or more combinations of a single *Authorization Server* and a single *Subscription Server* and each combination of a single *Authorization Server* and a single *Subscription Server* is offered by a single *Issuer*.
  - c. offers, if they offer *UC Notify*, an automated role for posting of *Notifications* on behalf of *Providers*, which is called *Notification Client*. Each such *Issuer* offers one or multiple *Notification Clients*, with each *Notification Client* being offered by a single *Issuer*.
3. *User* uses two automated roles for access to the functionality of *Publishing Server* and *Authorization Server*. *Presenter* for the presentation of the functionality to *User* and *User Agent* for the addressing of *Publishing Server* and *Authorization Server*.
4. *MedMij Maintenance* makes an automated service available to all stakeholders, which is named here: *MedMij Registration*.
5. For the authentication of *User*, the *Authorization Server* in question, in the role of *Authentication Client*, will use the *Authentication Service* offered by an *Authentication Provider*.
6. For the Authorization of *Publishing Server* for access to *Resource Server*, as part of *UCI Collect* and *UCI Share*, or to *Subscription Server* as part of *UCI Subscribe*, the *User Agent*, *Publishing Server*, *Authorization Server* and *Resource Server*, or *Subscription Server*, will use *OAuth 2.0*, using *Authorization Code* as grant type, whereby:
  - a. the role of *OAuth User Agent* is offered by the *User Agent*;
  - b. the role of *Client* is offered by the *Publishing Server*;
  - c. the role of *OAuth Resource Server* is offered by the *Resource Server*, in the case of *UCI Collect* and *UCI Share*, and by the *Subscription Server* in case of *UCI Subscribe*;
  - d. the role of *OAuth Authorization Server* is offered by the *Authorization Server*.
7. *MedMij data transfer* is defined as all the data transfer in the context of any use case implementation in this layer or in the *Infrastructure* Layer, directly between two different roles that are of the following four types of roles, namely:
  - first *Publishing Server* or *Notification Server*,
  - second, *User Agent*,
  - third *Authorization Server*, *Resource Server*, *Subscription Server* or *Notification Client*, and
  - fourth, *MedMij Registration*,

given that:

- in all cases these roles contain any Authorization roles that they respectively offer,
  - in all cases these roles exclude any Authentication roles that they respectively offer, and
  - in all cases these roles, with regard to the use case implementations in the *Infrastructure* layer, include the *Infrastructure* roles that they function on.
1. All the *MedMij data transfer*, insofar as the *User Agent*:
    - is involved in it - is called: *frontchannel data transfer*;
    - is not involved in it - constitutes the *backchannel data transfer*.

## Notes

Here, the roles of the [Process and Information](#) Layer are translated into roles on the application level. For details of the general basic principles regarding the numerical relationships between the roles, see the page [Architecture and technical specifications](#).

In the Individual's Domain, three roles are distinguished between the *Presenter*, *User Agent* and the *Publishing Server*. This is necessary in order to be able to make the connection with the roles in line with OAuth. *Presenter* and *User Agent* are all front-end roles for the *Publishing Server*, and can both be implemented in a browser for instance, but for a good binding to the *OAuth* role and *Authentication* role, and to have good security measures, it is necessary to distinguish between these two roles. As elsewhere in the MedMij Trust Scheme, here too it is about roles, in other words about sets of responsibilities, and not about implementation components.

In the Provider's Domain such a division is not necessary. Where an *Individual* is operationally involved in the information transfer - namely to have themselves identified and authenticated, and to have the transfer authorised - the *Provider* has completely represented themselves in operational terms by their *Service Provider* and their *Authorization Server* and *Resource Server*. Even though in many cases the health information will ultimately be obtained from an underlying system, this is not an issue for the MedMij Trust Scheme. It is sufficient to place the ultimate responsibility (black box) with the *Authorization Server* and *Resource Server*.

In line with options in the [Process and Information Layer](#), these servers act on behalf of any and all underlying systems in the Provider's domain, such as xIS systems. This underlying complexity is a black box. It is possible that an individual xIS acts for both servers but then all responsibilities linked with these roles must have been filled in too, both the directly linked responsibilities (in the Application Layer) and the indirectly linked responsibilities (in the layers above and below).

The choice made, in OAuth, to opt for the grant type Authorization Code fits the typical software architecture found in the Individual's Domain for MedMij: access to a PHE service via components that are not under the control of the *Client* and that must be considered to be relatively unsafe. In this layer, in respect to this access, we distinguish between two roles: the *Presenter* role, who is responsible for the presentation of the functionality to the *User*, and the role *User Agent*, who is responsible for addressing the *Publishing Server* and the *Authorization Server*. It is the role *User Agent* that is linked with the roles *OAuth User Agent* and *Authentication User Agent*. The *User Agent* ultimately also addresses the *Authentication Service*.

## Authorization Server, Resource Server and Subscription Server

The roles *Authorization Server* and *Resource Server* respectively (in [UCI Collect](#) and [UCI Share](#)) or *Subscription Server* (in [UCI Subscribe](#)) work together in a single uninterrupted session in the MedMij Trust Scheme. Their underlying relationship is a process link. In other words, they are orchestrated under a single process. However, roles in the MedMij Trust Scheme are groups of responsibilities, not implementation components. This means it is down to the *Provider's Service Provider* to make choices in his implementation and in his business model about whether to keep separate or actually combine these two roles. If the roles are separate then it is also certainly possible that a single *Authorization Server* or *Subscription Server* can work with multiple *Resource Servers* and that a single *Resource Server* can do business with multiple *Authorization Servers* or *Subscription Servers*. However, together they must always demonstrate the behaviour that is required by the MedMij Trust



Scheme. By the way, the OAuth specification also mentions this discretion (i.e. freedom) regarding implementation.

Because the session coordination in the Provider's Domain extends across the dividing line between *Authorization Server* and *Resource Server* or *Subscription Server*, an interface must be realised in which this session coordination is retained in the case of the separate implementation of *Authorization Server* and *Resource Server* or *Subscription Server*. In addition - if the relationship between *Authorization Server* and *Resource Server* or *Subscription Server* is not one-to-one - it must be ensured that the right two find each other for the communication about a specific access token.

Despite this discretion regarding implementation, the responsibilities in the MedMij Trust Scheme influence the implementation architecture in the Provider's Domain. The addressing, in particular, requires it to be the case that for a single combination of *Provider*, *Information service*, *Interface Version* (and *System Role*) there can only be a single authorization endpoint and a single token endpoint (and a single resource endpoint or subscription endpoint respectively). In addition, restrictions on the information content of Authorization codes and access tokens prevent the interface between *Authorization Server* and *Resource Server* or *Subscription Server* from being realised via the Individual's Domain. Apart from a few exceptions, that interface is an internal matter for the Provider's Domain. This serves [principles](#) (in Dutch) P1 and P7 as well as that of minimisation, and thus that of privacy too. The most important exception is that the Authorization code and the access token may if desired contain an identification of the service that issued it. In this way, the (actual or intended) acceptor of the Authorization code or the access token can find the *Authorization Server* or *Subscription Server* where the validation of the Authorization code or the access token must take place.

Even if there is separate implementation, it is still a single *Provider's Service Provider* who is ultimately responsible in respect of MedMij for the joint behaviour of *Authorization Server* and *Resource Server* or *Subscription Server*. This means that the interoperability between *Authorization Server* and *Resource Server* or *Subscription Server* must come under the agreement that the relevant *Provider's Service Provider* establishes with any subcontractors, for example, if the *Provider's Service Provider* itself operates the *Resource Server* or *Subscription Server* but contracts a subcontractor for the *Authorization Server*. See also the explanatory notes under the Roles on the [Infrastructure](#) page for details of how *Nodes* are dealt with at an Infrastructure level if a *Provider's Service Provider* uses subcontractors for *Authorization Server* or *Subscription Server* functionality, for example.

It is conceivable that a community of service providers in the Provider's Domain agree on a trust scheme alongside and in compliance with the MedMij Trust Scheme, in which the matter of the internal architecture of the Provider's Domain is addressed. In addition to the aforementioned separation, this could, for instance, include architectural choices about the availability test and receptiveness test.

### Authorization versus authentication

It is important to make a clear distinction between Authorization and authentication in the MedMij Trust Scheme. Not only are these different functionalities, with authentication intended to establish someone's identity and Authorization used to manage access rights, the associated roles cannot simply be combined in the MedMij Trust Scheme. The *Authorization Server* has the role to, on behalf of the *Provider*, at the request of the *Individual*, distribute Authorizations to the *Publishing Server*. To

be able to do reliably, and to meet the legal obligation of the *Provider*, the *Authorization Server* activates the (external) *Authentication Service*.

This does not mean, however, that the *Authorization Server*, in turn, starts to provide identity services to the *Publishing Server* by, for example, include an identity linked to the BSN with the access token that it distributes. This would constitute an improper widening of its authentication role, which should stay limited to the responsibilities towards the *Provider* and should not extend to operating the *Publishing Server*. Aside from that, it would create a centre of *Individual* identity in the MedMij landscape that, given MedMij's control objectives, should not be in the *Provider's* domain, but in the *Individual's* Domain, and within that domain preferably as close as possible to the *Individual*.

This is why the interface between *Publishing Server* and *Authorization Server* is not where *Individual* identities are exchanged, neither using, for example, the standard OpenID Connect, neither with another standard that is used for that purpose. This does not mean that such standards cannot be used in other future interfaces in the MedMij Trust Scheme, i.e. in interfaces that are intended for identity authentication services, instead of for Authorization purposes.

The OAuth 2.0 and SAML 2.0 standards — as example; the selected *Authentication Service* can use an interface other than SAML — therefore serve different purposes: OAuth for Authorization and SAML for authentication. Amongst other things, this ensures that the role structure is different. In OAuth there is a user (*resource Owner*) that via his browser or app (*User Agent*) offers access for one application (*Client*) to another one (*Resource Server*), which last-named one has itself assisted for this by an *Authorization Server*. In SAML there is a user that uses a browser or app (*User Agent*) to log in to a service (*Service Provider*), which has itself assisted for this by an *Identity Provider*.

All the same, there are important similarities between the ways in which they work.

- Both assume that the end-user presents himself via a relatively unsafe channel (the *User Agent*, the "front-channel"), while at the same time more sensitive information must be exchanged ("back-channel") that does not pass through this channel.
- In both cases, the *User Agent* must be led back and forth (redirect). In the case of OAuth, this is from *Client* to the *Authorization Server* and back. In the case of SAML, this is from the *Service Provider* to the *Identity Provider* and back.
- In the case of both, the *Client* (in the case of OAuth the *Client* and in the case of SAML the *Service Provider*) do not receive the desired information (in the case of OAuth the access token, in the case of SAML the user's identity) directly but via a retrieval certificate (in the case of OAuth the Authorization code, in the case of SAML the artefact). The retrieval certificate passes in front (via the *User Agent*), after which the desired information is retrieved behind with the retrieval certificate.

### MedMij data transfer

Article 7 delineates the *MedMij data transfer* in respect of the [Infrastructure](#) Layer. All the *MedMij data transfer* is across domain borders. In addition, neither any transfer between *Presenter* and *User Agent* nor any transfer between *Authorization Server* and *Resource Server* is part of *MedMij data transfer*. Authentication data transfer is also excluded because the MedMij Trust Scheme does not impose requirements as to which (external) *Authentication Service* to use. The MedMij Trust Scheme requires that an appropriate authentication be performed by *Provider*, but the data transfer needed for that — between *Authorization Server*, *Authentication Service* and *User Agent* — does not constitute MedMij data transfer. It is, nonetheless, the *Provider*, being the controller, who remains



responsible for an appropriate choice of Authentication Service and for having the authentication data transfer set up.

This delineation is also the prelude to point 8 following it. The distinction made there between frontchannel and backchannel data transfer is necessary for the formulation of security responsibilities (see [Infrastructure](#) Layer). With respect to point 7, it must be taken into consideration that there is also a use case implementation in the [Infrastructure](#) Layer: *UCI Retrieve Whl*.

## Responsibilities

### Use cases and Information services

#### Notes

For most use cases (see the [Process and Information](#) Layer), a use case implementation (UCI) is prescribed in this (Application) layer. This is regarding the following.

use case implementation	Flow diagram	Primary function
<i>UCI Collect</i>	with	<i>Control and Exchange</i>
<i>UCI Share</i>	with	<i>Control and Exchange</i>
<i>UCI Subscribe</i>	with	<i>Control</i>
<i>UCI Notify</i>	with	<i>Control or Exchange</i>
<i>UCI Retrieve Isd</i>	with	<i>Coordination</i>
<i>UCI Retrieve Rcd</i>	with	<i>Coordination</i>
<i>UCI Retrieve Isg</i>	with	<i>Coordination</i>

1a. The above roles implement the use case *UC Collect* with the use case implementation *UCI Collect*. They use the relevant [flow diagram](#) for this. The entire process is carried out uninterrupted.

1b. The above-named roles implement the use case *UC Share* with the use case implementation *UCI Share*. They use for this the relevant [flow diagram](#). The entire process is carried out uninterrupted.

1c. Insofar as offered by the relevant *Publisher*, or the relevant *Issuer*, *UC Subscribe* and *UC Notify*, the above roles implement the *UC Subscribe* using the use case implementation *UCI Subscribe* and the *UC Notify* using the use case implementation *UCI Notify*. The entire process is carried out uninterrupted.

#### Notes

The user experience is best served by keeping the entire process uninterrupted.

2. If a *Publisher* makes a certain *Information service* available for his *Users* and to this end arranges delivery by a *Issuer* or *Addressee* then the *Publishing Server* of this *Publisher* and the *Authorization Server* and

*Resource Server* of this *Issuer* or *Addressee* respectively will implement for this the use case implement that belongs to the *Information service* and use the Information Standards that belong to the *Information service* as included in the *Information service catalogue*.

#### Notes

In this way, it is guaranteed that the correct use case implementations and information standards are used.

## Authorization and OAuth

3. In the use case implementations [UCI Collect](#), [UCI Share](#) and [UCI Subscribe](#), *Publishing Server* on one side and *Authorization Server* and *Resource Server* or *Subscription Server* on the other process their mutual data transfers as per the [OAuth 2.0](#) standard.

#### Notes

In accordance with the statutory obligation, *User* gives, in the [UC Collect](#) and the [UC Subscribe](#), active consent to the *Provider*. In the [UC Share](#), this requirement does not apply, but even so, a confirmation is made at this moment by the *User*. The *Presenter* presents a window in which the *User* can give this consent or confirmation respectively. Since the BSN cannot be used in the Individual's Domain, a substitute identification of the *User* must be used. See responsibility 5.

4. OAuth2.0 offers four types of [Authorization grants](#), but the OAuth roles limit themselves to the [Authorization Code](#).

#### Notes

This one type can be used to serve all the situations that occur in the MedMij Trust Scheme. In order to maximise the interoperability, MedMij opts to exclude the other three types.

5. The *Client* and *OAuth Resource Server* will only exchange tokens of the Bearer Token type, in accordance with [RFC6750](#).

#### Notes

It is the OAuth standard that releases the (access) token type. Token types differ in the degree of confidence with which the *Resource Server* can offer the requested resources to the *Client* when the last-named submits the access token to the former. In its simplest form (Bearer Token), the *Resource Server* simply offers the related resources to each *Client* who submits a valid access token. This is done "to bearer", in the same way that a bank can cash a check to bearer. However, there are security risks associated with this, because the access token may have been stolen after being issued or otherwise alienated from the *Client* to whom it was distributed. As a result, other token types can ask for more guarantees, such as an identity of the *Client* or a client secret. Bearer Token is, however, the only well standardized and widely used type of token. It does place much responsibility for the management of the security risks with *Client* and *Authorization Server*. This is why [Chapter 5 of the specification of the standard RFC6750](#) explicitly focuses on these security risks and on the measures to deal with them. See responsibility 18 for details.

6. The *Client* only uses a single scope at a time. The *OAuth Authorization Server* generates Authorization codes and access tokens with a single scope that must be included in its entirety in the *Information service* requested by the *Client*.

#### Notes

The OAuth scope is included in the generation of codes and tokens. This is related to the *Information service*. Although it is possible in technical terms to include multiple scopes, the scope is limited to a single *Information service* per request.

7. The *OAuth Authorization Server* sets the validity duration for each issued Authorization code and each access token issued at precisely 15 minutes (900 seconds). Furthermore, it does not issue any refresh tokens.

#### Notes

This is a measure against security risks 4.4.1.1 and 4.4.1.3 from RFC 6819. In addition, the entire flow of *UCI Collect* is executed uninterrupted (see under 1). The 900 seconds must then be sufficient for the *Client* to offer the access token to the *Authorization Server*. A refresh token is then unnecessary.

8a. The *OAuth Authorization Server* generates Authorization codes and access tokens in such a way that the probability of guessing them is no greater than  $2^{-128}$  with the random number generators used for this being cryptographically secure, too.

8b. If desired, it is permitted to include one or more of the information elements from the following limited list in the Authorization codes and access tokens:

- an identifier of the Authorization code or the access token respectively, offered that the identifier itself meets the requirements specified in responsibility 8a;
- a progress moment of the validity of the token, under the conditions that both:
  - the value of it is in line with the responsibilities in the MedMij Trust Scheme, and
  - its expiry can be used to conclude that the Authorization code or the access token is invalid, this conclusion being drawn by the *Authorization Server* or the *Resource Server*, but that its validity can **not** be concluded if it has not expired yet, for which a validation of the entire token against the internal records of the *Authorization Server* is namely the sole authority;
- an identification of the service that issued the token;
- the scope for which the Authorization code or the access token was issued, in the form of a copy of the scope parameter of the authorization request in response to which the Authorization code or the access token was issued;
- the name of the token's format;
- a digital signature.

8c. No information other than that named in responsibility 8b may be present in the Authorization code or the access token, even if not encrypted. Various options may be taken with respect to the information content of the token between Authorization code and access token. The *Client* must not interpret the content of the token.

8d. With regard to both Authorization codes and access tokens, the *OAuth Authorization Server* issuing them ensures that there are never two identical valid ones in circulation.

## Notes

This is a measure against security risk [4.4.1.3](#) from RFC 6819. Two important requirements are to be laid down for the Authorization codes and access tokens that are put into circulation: uniqueness and confidentiality. The requirement of confidentiality weighs heavily in the MedMij Trust Scheme. Because the Authorization code (indirectly) and the access token (directly) grant access to personal health information, MedMij opts for a format that is virtually meaningless and that is only given meaning by confrontation with local and properly protected records of the *Authorization Server*. The maximum permissible probability of guessing it is laid down in [RFC6749, section 10.10](#). It must not be possible to use a comparison of multiple Authorization codes or access tokens to work out how they are generated.

When an identifier has been included in the access token, it can be used as identification of the *Authorization Server* session during which the token was issued, so that the *Resource Server* can resume this session when offered the access token. It will then also be possible for such an identifier not be included in the Authorization code or access token, but to be identical to the Authorization code or access token. Whichever it is, it remains subject to responsibility 8a.

If a progress moment is included in the access token, it becomes possible to get the *Resource Server* to refrain from unnecessary consultation of the *Authorization Server* if this is to be implemented separately. The second condition for this option prevents a situation where any corruption in the *Individual's Domain*, namely of the Authorization code or the access token whereby the progress moment would be abandoned, leads to wrongful access or to the wrongful placement of health information. The accepting of an Authorization code or an access token always occurs in line with the internal records of the *Authorization Server*. This corruption can also bring forward the progress moment but this causes little damage. By the way, in this version of the MedMij Trust Scheme, in which the validity duration has a fixed value, the *Client* will work out itself when it no longer makes sense to still offer an Authorization code or access token. This means that the added value of a progress moment in the Authorization code or the access token can at most be seen in possible future versions.

The service that issued the token is however already a useful information element in this version of the MedMij Trust Scheme. In situations where a *Resource Server* works with multiple *Authorization Servers* that are implemented separately, when offered with an access token it must be able to determine which *Authorization Server* must be addressed. This addressing can for instance be done by means of Token Introspection in line with [RFC7662](#). The appropriate Issuer for this information is the access token itself, which has information about its origin. This origin information does not cause any additional privacy risks, because the *Client* knows anyway who it has received the access token from.

Furthermore, the *OAuth Authorization Server* may also include a copy of the scope in (the Authorization code or) the access token, namely the scope that it previously received in the authorization request from the *Client* (see [authorization interface](#), responsibility 1). In this way, the *Resource Server* does not have to be informed separately by the *Publishing Server* about the scope. While it's true that the Authorization code or the access token does carry additional meaning, the risks of it are not as great as the risks of letting the *Publishing Server* send the scope separately, which scope could, for instance, differ from that for which the Authorization code or the access token

was issued.

The list of permitted information elements is limited. No other information, not even if encrypted, may be included in the Authorization code or the access token. This exclusion certainly applies to the following too:

- Information about *Individual*;
- Information about *Provider or Information service*, whether or not in relation to *Individual*, outside the scope;
- naming of, and restrictions on, the intended acceptors of the Authorization code or the access token. In respect of this point, it is namely the *Information service directory* that is the authority: if the *Client* has retrieved an access token at a place that was mentioned in the *Information service directory* to this end then it must be able to provide this access token at the place that is mentioned in the *Information service directory* to this end.

The ban on interpretation by the *Client* of the Authorization code and access token ensures that a minimum dependency is created between the service providers in the Individual's Domain on the one hand and those in the Provider's domain on the other, so that [principles](#) P1 and P7 are complied with as much as possible and internal complexity and implementation choices in the Provider's domain do not filter through to or influence the implementation in the Individual's Domain.

The limitations of the Authorization code's and the access token's ability to carry a meaning, even if encrypted, promote privacy by means of data minimisation. In addition, they prevent new risks relating to the compromising of this information content. Such compromising would be difficult to discover and ward off in the Provider's Domain, if it had been decided to this end to refrain from having internal Authorization records because the information is already being transported in the Authorization code or the access token, via the *Client*.

#### 9. The [Client type](#) of the *Client* is confidential.

##### Notes

In order to be able to guarantee privacy, it is important that the OAuth *Authorization Server* is sufficiently certain about the identity of the *Client*. This certainty is dependent on the extent to which the *Client* can keep his credentials confidential. To this end, the OAuth specification distinguishes between two [client types](#): confidential and public. The first type can give the *Authorization Server* a sufficient degree of confidentiality for his credentials but the second cannot. It is a main aim of MedMij to guarantee such trust in a trust scheme and not to leave this to the individual players. This is why the MedMij Trust Scheme links responsibilities to *Clients* so that they can be trusted in respect of *Authorization Servers*. We expect that a large proportion of the implementations of the *Client* (i.e. of the *Publishing Server*) can offer this confidentiality because their architecture is what the OAuth specification calls [web application](#). Other kinds of *Publishing Server* architectures, such as that of an app, are also possible, albeit only on the condition that the *Client* processes all the credential transfers in the background on a server, not through the user interface.

## Lists

10a. *MedMij Registration* and every *Publishing Server* implement the use case [UC Retrieve Dcd](#) using use case implementation [UCI Retrieve Isd](#), based on the stipulations with respect to the Isd interface on [Isd, Cld and Isd interface](#). They use the relevant [flow diagram](#) for this.

10b. *Publishing Server* obtains at least every fifteen minutes (900 seconds) the most recent *Isd* implementation of *MedMij Registration*.

10c. *Publishing Server* validates each newly obtained *Isd implementation* against the [XML Schema description of the \*Information service directory\*](#). This XML Schema description is a technical implementation of the MedMij metamodel.

11a. *MedMij Registration, Authorization Server* and *NotificationClient* implement the use case [UC Retrieve Rcd](#) using use case implementation [UCI Retrieve Rcd](#), based on the stipulations with respect to the Cld interface on [Isg, Cld and Isd interface](#). They use the relevant [flow diagram](#) for this.

11b. *Authorization Server* and *Notification Client* obtain at least every fifteen minutes (900 seconds) the most recent *Cld implementation* of *MedMij Registration*.

11c. *Authorization Server* and *Notification Client* validate each new *Cld implementation* obtained against the [XML Schema description of the [Client directory](#)/display/MedMijAfsprakenstelsel120/XML-schema%27s]. This XML Schema description is a technical implementation of the [MedMij metamodel](#).

12a. *MedMij Registration, Publishing Server* and *Authorization Server* implement the use case [UC Retrieve Isg](#) using use case implementation [UCI Retrieve Isg](#), based on the stipulations with respect to the Isg interface on [Isg, Cld and Isd interface](#). They use the relevant [flow diagram](#) for this.

12b. *Publishing Server* and *Authorization Server* obtain at least every fifteen minutes (900 seconds) the most recent *Isg implementation* of *MedMij Registration*.

12c. *Publishing Server* and *Authorization Server* validate each new *Isg implementation* obtained against the [XML Schema description of the Isg](#). This XML Schema description is a technical implementation of the [MedMij metamodel](#).

## Security

13. In the data transfer for [UCI Collect](#), [UCI Share](#), [UCI Subscribe](#), [UCI Notify](#), [UCI Retrieve Isd](#), [UCI Retrieve Rcd](#) and [UCI Retrieve Isg](#), the roles involved use the functions *Encryption*, *Server Authentication* and *Server Authorization*, as per the stipulations in the [Infrastructure Layer](#).

14. For all data transfer between them, *Client* and *OAuth Authorization Server* use [PKI overheid](#) certificates and server certificates for the purpose of authenticating the other server during data exchange.

### Notes

This is a measure against security risks [4.4.1.1](#), [4.4.1.3](#), [4.4.1.4](#) and [4.4.1.5](#) in [RFC 6819](#). In this release of the MedMij Trust Scheme, PKI certificates are used for two purposes in the [Infrastructure Layer](#): authentication of servers and encryption, which guarantee the confidentiality and integrity of the content of the data transfer.

15. The *Client* realises the following security measures, in accordance with [RFC6819](#):

security measure	section in RFC6819	mitigated risk(s)
Clients should use an appropriate protocol, such as OpenID or SAML to implement user login. Both support audience restrictions on clients.	<a href="#">4.4.1.13</a>	<a href="#">4.4.1.13</a>
All clients must indicate their client ids with every request to exchange an Authorization "code" for an access token.		
Keep access tokens in transient memory and limit grants.	<a href="#">5.1.6</a>	
Keep access tokens in private memory.	<a href="#">5.2.2</a>	<a href="#">4.1.3</a>



The "state" parameter should be used to link the authorization request with the redirect URI used to deliver the access token.	5.3.5	4.4.1.8
CSRF defence and the "state" parameter created with secure random codes should be deployed on the client side. The client should forward the authorization "code" to the authorization server only after both the CSRF token and the "state" parameter are validated.		4.4.1.12

16. The *Client* realises the following security measures, in accordance with [RFC6819](#):

security measure	section in RFC6819	mitigated risk(s)
Client applications should not collect authentication information directly from users and should instead delegate this task to a trusted system component, e.g. the system browser.	4.1.4	4.1.4
The client server may reload the target page of the redirect URI in order to automatically clean up the browser cache.	4.4.1.1	4.4.1.1
If the client authenticates the user, either through a single-sign-on protocol or through local authentication, the client should suspend the access by a user account if the number of invalid Authorization "codes" submitted by this user exceeds a certain threshold.	4.4.1.12	4.4.1.12
Client developers and end users can be educated to not follow untrusted URLs.	4.4.1.8	4.4.1.8
For newer browsers, avoidance of iFrames during Authorization can be enforced on the server side by using the X-FRAME-OPTIONS header. For older browsers, JavaScript frame-busting techniques can be used but may not be effective in all browsers.	5.2.2.6	4.4.1.9
Explain the scope (resources and the permissions) the user is about to grant in an understandable way	5.2.4.2	4.2.2

17. The *OAuth Authorization Server* realises the following security measures, in accordance with [RFC6819](#):

security measure	section in RFC6819	mitigated risk(s)
Authorization Servers should consider such attacks: Password Phishing by Counterfeit Authorization Server	4.2.1	4.2.1
Authorization Servers should attempt to educate users about the risks posed by phishing attacks and should provide mechanisms that make it easy for users to confirm the authenticity of their sites.		
Authorization Servers should decide, based on an analysis of the risk associated with this threat, whether to detect and prevent this threat.	4.4.1.10	4.4.1.10

The Authorization Server may force a user interaction based on non-predictable input values as part of the user consent approval.		
The Authorization Server could make use of CAPTCHAs.		
The Authorization Server should consider limiting the number of access tokens granted per user.	4.4.1.11	4.4.1.11
The Authorization Server should send an error response to the client reporting an invalid Authorization "code" and rate-limit or disallow connections from clients whose number of invalid requests exceeds a threshold.	4.4.1.12	4.4.1.12
Given that all clients must indicate their client ids with every request to exchange an Authorization "code" for an access token, the Authorization Server must validate whether the particular Authorization "code" has been issued to the particular client.	4.4.1.13	4.4.1.13
Best practices for credential storage protection should be employed.	5.1.4.1	4.4.1.2
Enforce system security measures.	5.1.4.1.1	4.3.2 and 4.4.1.2
Enforce standard SQL injection countermeasures.	5.1.4.1.2	
Store access token hashes only.	5.1.4.1.3	
The Authorization Server should enforce a one-time usage restriction.	5.1.5.4	4.4.1.1
If an Authorization Server observes multiple attempts to redeem an Authorization "code", the Authorization Server may want to revoke all tokens granted based on the Authorization "code".	5.2.1.1	
Bind the Authorization "code" to the redirect URI.	5.2.4.5	4.4.1.3
The Authorization Server associates the Authorization "code" with the redirect URI of a particular end-user Authorization and validates this redirect URI with the redirect URI passed to the token's endpoint,		4.4.1.7

## Notes

When it came to drawing up the responsibilities 15, 16 and 17, use was made of [RFC 6819](#) of IETF, which contains an extensive Information service catalogue of the risks, including a series of measures per risk. Where the risk applies to the usage of OAuth within MedMij, and the measures comply with the MedMij principles, they have been included in the trust scheme.

With regard to the provisions in [section 3.1 of RFC 6819](#), it can be argued that MedMij proceeds on the following basis:

- handles instead of assertions, so that the *OAuth Resource Server* must be able to refer to data of the *OAuth Authorization Server*;
- bearer tokens instead of proof tokens. See in this regard responsibility 5 in this layer.

In [chapter 4 of RFC 6819](#) there is an extensive list of security risks. Not applicable are, for this release of the trust scheme:



- threat 4.1.2: [Obtaining Refresh Tokens](#), because the trust scheme does not work with refresh tokens;
- threat 4.2.3: [Malicious Client Obtains Existing Authorization by Fraud](#), because in the trust scheme there is a strict rule that Authorization (for the time being) may only be used once;
- threat 4.3.4: [Obtaining Client Secret from Authorization Server Database](#), because authentication of *Clients* in MedMij works on the basis of PKI server certificates, not on the basis of client secrets;
- threat 4.3.5: [Obtaining Client Secret by Online Guessing](#), because authentication of *Clients* in MedMij is done on the basis of PKI server certificates, not on the basis of client secrets.

The following do indeed apply:

- threat 4.1.3: [Obtaining Access Tokens](#);
- threat 4.1.4: [End-user Credential Phished Using Comprised or Embedded Browser](#);
- threat 4.1.5: [Open Redirectors on Client](#);
- threat 4.2.1: [Password Phishing by Counterfeit Authorization Server](#);
- threat 4.2.2: [User Unintentionally Grants Too Much Access Scope](#);
- threat 4.2.4: [Open Redirector](#);
- threat 4.3.1: [Eavesdropping Access Tokens](#);
- threat 4.3.2: [Obtaining Access Tokens from Authorization Server Database](#);
- threat 4.3.3: [Disclosure of Client Credentials during Transmission](#);
- threat 4.1.1: [Obtaining Client Secrets](#);
- threat 4.4.1.1: [Eavesdropping or Leaking Authorization Code](#);
- threat 4.4.1.2: [Obtaining Authorization "codes" from Authorization Server Database](#);
- threat 4.4.1.3: [Online Guessing of Authorization "codes"](#);
- threat 4.4.1.4: [Malicious Client Obtains Authorization](#);
- threat 4.4.1.5: [Authorization "code" Phishing](#);
- threat 4.4.1.6: [User Session Impersonation](#);
- threat 4.4.1.7: [Authorization "code" Leakage through Counterfeit Client](#);
- threat 4.4.1.8: [CSRF against redirect-URI](#);
- threat 4.4.1.9: [Clickjacking Attack against Authorization](#);
- threat 4.4.1.10: [Resource Owner Impersonation](#);
- threat 4.4.1.11: [DoS Attacks That Exhaust Resources](#);
- threat 4.4.1.12: [DoS Using Manufactured Authorization "codes"](#);
- threat 4.4.1.13: [Code Substitution \(OAuth Login\)](#).

In relation to the MedMij Trust Scheme, the measures that must be taken to mitigate these risks can be broken down into three groups:

- measures which have already been provided for by means of one or more responsibilities in the MedMij Trust Scheme, such as:
  - use of TLS ([Infrastructure Layer](#));
  - use of an (external) *Authentication Service* ([Application Layer](#));
  - limitation of the scope and duration of validity of Authorization codes and access tokens ([Application Layer](#));
  - responsibility 3 on the [Token interface](#);
- measures that despite being suggested by [RFC6819](#) have not been made part of the MedMij Trust Scheme, because they do not comply with its principles or with other responsibilities in the system;
- other measures, which still need to be taken by *Publishing Server*, *Client* or *OAuth Authorization Server* and are specified in responsibilities 15-17.

18. *Client, OAuth Authorization Server and OAuth Resource Server* implement the security measures that apply to these respective roles, in line with [section 5.3 of RFC6750](#).

**Notes**

This responsibility is included because information can be obtained with the bearer token without the identity being checked again. This is why measures must be taken to guarantee that the token can only be used correctly.

## Interfaces\_

### Interfaces and use cases

These pages list the responsibilities associated with the interfaces in the MedMij Trust Scheme. Each use case implementations uses one or several of these interfaces. The below table shows exactly which interface is used by which use case implementation.

primary function	Control					
interface	user interface	authorization interface	token interface	subscription interface	subscription notification interface	resource notification interface
offered by role	Authorization Server			SubscriptionServer	NotificationServer	
<b>UCI Collect</b>	X	X	X			
<b>UCI Share</b>	X	X	X			
<b>UCI Subscribe</b>	X	X	X	X		
<b>UCI Notify</b>					X	X
<b>UCI Retrieve Isg</b>						
<b>UCI Retrieve Rcd</b>						
<b>UCI Retrieve Isd</b>						

Responsibilities concerning the addressing of these interfaces are detailed below. Responsibilities for the specific interfaces are included in the specific sub-pages, which are clickable in the above table.

### Addressing

## Addresses and interfaces

In the six interfaces in the flows of [UCI Collect](#), [UCI Share](#), [UCI Subscribe](#) and [UCI Notify](#), Application roles address each other based on a URI. The below table provides an overview.

primary function	interface	addressee	message	channel
Control	authorization interface	Authorization endpoint of the Authorization Server	authorization request	frontchannel
		Client (redirect_uri)	Authorization response	
	token interface	Token Endpoint of the Authorization Server	access token request	backchannel
	subscription interface	Subscription Endpoint of the Subscription Server	subscription request	
Exchange	subscription notification interface	Subscription Notification Endpoint of the Notification Server	subscription notification	backchannel
	Resource interface	Resource Endpoint of the Resource Server	resource request	
	resource notification interface	Resource Notification Endpoint of the Notification Server	resource notification	

The responsibilities that now follow determine the structure of the URIs, which the address user's address determinant uses to address the addressee, and also determine how the parameters are filled in. The address is always structured the same, also for frontchannel and backchannel. Despite that, we do make a distinction in the [logical information model](#), in the *Information service directory*, between *Frontchanneluri* and *Backchanneluri*. This keeps the model more flexible, in case there were ever addressing differences between frontchannel and backchannel.

1a. The *Client* compiles, in accordance with [RFC 3986](#), the URI that they use to address either himself, the *Authorization Server*, *Subscription Server* or the *Resource Server*. The *Notification Client* compiles, in accordance with [RFC 3986](#), the URI that they use to address the *Notification Server*.

1b. The URIs specified in responsibility 1a have a hostname that is a fully-qualified domain name, in accordance with [RFC3696, section 2](#), and has the pattern scheme://host path, whereby:

- scheme is always https, in lowercase;
- host is a hostname in which
  - only the characters `[a-z]`, `[0-9]`, `"."` (full stop) and `"-"` (hyphen) occur;
  - each full stop separates two successive segments and is not part of either of the separated segments;
  - the first character of a segment is not a hyphen;
  - each segment is at least one character long;
  - the last segment is at least two characters long;
  - the last character must not be a hyphen;
  - it has a maximum of 255 characters;

- it has at least two segments;
- path has the syntax of path-abempty from [section 3.3 of RFC 3986](#) (and thus can be empty) but does not end with a /.

#### Explanatory Notes

The requirement that https is in lowercase follows the canonical form as specified in [section 3.1 of RFC 3986](#). The requirements laid down for the hostname are based on (amongst others) [RFC 952](#) and [RFC 1123](#). The last segment is what is known as the 'top-level domain'.

2a. In all addressing in the [authorization interface](#), the [token interface](#), the [subscription interface](#), the [subscription notification interface](#), the [resource notification interface](#) and the [Resource interface](#), use of the port number specified for https, as included in the [Service Name and Transport Protocol Port Number Registry](#) of IANA, is compulsory.

#### Explanatory Notes

This therefore also goes for the `redirect_uri`.

In release 1.1.1 of the MedMij Trust Scheme, this responsibility applied only to frontchannel data transfer, as the *Provider's Service Provider* was free to choose a port number other than that specified on the IANA list at https (443) for backchannel data transfer. However, this leads to additional security management burden on the *Publishing Server* that allows for multiple destination port numbers for outgoing data transfer. This management burden indirectly also leads to additional security risks. On the other hand, however, the tightening applied through this release is not expected to seriously restrict the *Provider's Service Provider*, because they already use the port number from the IANA list specified for https. A possible exception hereto is the situation where the *Authorization Server* and/or *Resource Server* run in a multi-tenant environment.

2b. For the compilation of all addresses of the authorization request, the token request, the subscription request, and the resource request, the *Client* obtains the first elements from the URI, i.e. host and path, from the *Information service directory*, based on the applicable *Provider* and either *Information Service* (if addressee is *Authorization Server*) or *System Role* (if addressee is *Resource Server*). Other elements of the general URI syntax, such as user, password, query and fragment, are absent from the addresses.

2c. The addresses for the subscription notification and the resource notification obtain the *Notification Client* from the *Client directory*, based on the applicable *Client* and *Information Service*.

#### Information service directory and Client directory

In other words, the *Information service directory* is used by the *Client* to, given a certain *Interface Version*, know the endpoint that matches the applicable *Provider*, *Information Service* and, for the resource endpoint, *System Role*. In the same way, the *Notification Client* uses the *Client directory* to, given a certain *Interface Version*, know the endpoint that matches the applicable *Client* and *Information Service*. This is why a single endpoint address must follow from a single such set. However, in the contrary situation, this is not a requirement. It is possible to, in any combination required by the *Provider's Service Provider*, reuse endpoint addresses for multiple such sets in the *Information service directory*, or by the *Individual's Service Provider* on the *Client directory*.

3. *MedMij Registration* is addressed in *UCI Retrieve Isd*, *UCI Retrieve Rcd* and *UCI Retrieve Isg* with the hostname [stelselnode.medmij.nl](https://stelselnode.medmij.nl).

## User interface (declarations)

### Explanatory Notes

The user interface forms part of the [Control primary function](#).

1a. The question that the *User* must be asked in the "authorise" step in [UCI Collect](#) is specified in the [Declaration of consent](#) page. The following applies in this regard:

- the user-friendly depiction of the identity of the *Provider* (Name of Provider) is determined by the relevant *Provider's Service Provider*, in its service provision relationship with the relevant *Provider*;
- the user-friendly depiction of the *Information Service* (Name of Information Service) is obtained from the scope that the *Authorization Server* received in the very first step of the flow, which corresponds to the *Depiction Name* that is included with the relevant *Information Service* in the *Information service glossary*;
- the user-friendly depiction of the identity of the *Publisher* (Name SupplierPHE) is obtained from the *Client directory*, based on the *redirect\_uri* (from OAuth) obtained in step 1.

1b. The question that the *User* must be asked in the "confirm" step in [UCI Share](#) is specified in the [Declaration of confirmation](#) page. The following applies in this regard:

- the user-friendly depiction of the identity of the *Provider* (Name of Provider) is determined by the relevant *Provider's Service Provider*, in its service provision relationship with the relevant *Provider*;
- the user-friendly depiction of the *Information Service* (Name of Information Service) is obtained from the scope that the *Authorization Server* received in the flow's very first step, which corresponds to the *Depiction Name* that is included with the relevant *Information Service* in the *Information service glossary*;
- the user-friendly depiction of the identity of the *Publisher* (Name SupplierPHE) is obtained from the *Client directory*, based on the *redirect\_uri* (from OAuth) that was obtained in step 1.

1c. The question that the *User* must be asked in the "authorise" step in [UCI Subscribe](#) is specified in the [Declaration of consent for subscription](#) page. The following applies in this regard:

- the user-friendly depiction of the identity of the *Provider* (Name of Provider) is determined by the relevant *Provider's Service Provider*, in its service provision relationship with the relevant *Provider*;
- the lifetime offered for the Subscription (Duration) based on the policy of the Provider is determined based on the lifetime requested by the Individual, and will never exceed the maximum lifetime specified in the *Information service catalogue* for the *Information Service* in question;
- the user-friendly depiction of the *Information Service* (Name of Information Service) is obtained from the scope that the *Authorization Server* received in the very first step of the flow, which corresponds to the *Depiction Name* that is included with the relevant *Information Service* in the *Information service glossary*;
- the user-friendly depiction of the identity of the *Publisher* (Name SupplierPHE) is obtained from the *Client directory*, based on the *redirect\_uri* (from OAuth) obtained in step 1.

### Explanatory Notes

Name of Provider, Name of Information Service and Name SupplierPHE are placeholders, as included in the [Declaration of consent](#) and the [Declaration of confirmation](#).  
Duration is a placeholder, as included in the [Declaration of consent for subscription](#).





## Authorization interface\_

### Explanatory Notes

The authorization interface forms part of the [Control primary function](#).

This page shows only the responsibilities with respect to the authorization interface that are not yet specified in the [OAuth 2 specification](#).

1a. The parameters in the authorization request are populated as follows:

parameter	entry	explanatory notes
response_type	literal value code	This is the result of responsibility 4 in the <a href="#">Application Layer</a> .
client_id	the hostname, which is included in the <i>Client directory</i> , of the <i>Node</i> of the <i>Client</i> submitting the authorization request	
redirect_uri	<ol style="list-style-type: none"> <li>such that the hostname included therein is the same as the client_id and no port number is included</li> <li>the redirect_uri must be complete and redirect to a https-protected endpoint</li> </ol>	See responsibilities 1 and 2a on the <a href="#">Interfaces</a> page. The second requirement is a measure against security risks <a href="#">4.1.5</a> , <a href="#">4.2.4</a> , <a href="#">4.4.1.1</a> , <a href="#">4.4.1.5</a> and <a href="#">4.4.1.6</a> in RFC 6819. See in addition <a href="#">Token interface</a> , the explanatory notes under responsibility 4.
scope	<p>optional:</p> <ul style="list-style-type: none"> <li>the literal value subscribe</li> <li>followed by tilde ~</li> <li>followed by a non-negative whole number, specifying the requested maximum duration of the <i>Subscription</i></li> <li>followed by a forward slash /</li> </ul> <p>followed by, compulsory:</p>	<p>The scope therefore consists of an optional element followed by two compulsory elements.</p> <p>The optional element is used to enter into, renew, or terminate a <i>Subscription</i>. If the requested maximum duration of the <i>Subscription</i> is 0, this means the request to terminate the possible <i>Subscription</i> to that <i>Information Service</i> with that <i>Provider</i>.</p> <p>The two compulsory elements follow the possible optional elements and is made up of two, separated by a tilde. In this version of the MedMij Trust Scheme, there must only be one of each. When the <i>Provider Name</i> is interpreted by the recipient, they will have to add the suffix @medmij again. No scopes or elements of scopes other than those specified here are included.</p> <p>The following are examples of syntactically correct scopes:</p>

	<ul style="list-style-type: none"> <li>the relevant (single) <i>Provider Name</i>, stripped of the @medmij suffix, followed by</li> <li>a tilde (~), followed by</li> <li>the <i>Information Service ID</i> of the relevant (single) <i>Information Service</i> from the <i>Information service glossary</i>.</li> </ul>	<ul style="list-style-type: none"> <li>randomcareprovider~42, for the one-off purchase of <i>Information Service 42</i> from randomcareprovider@medmij;</li> <li>subscribe~180/randomcareprovider~42, to enter into a <i>Subscription to Information Service 42</i> with randomcareprovider@medmij for a maximum of 180 days, or change the <i>Subscription to Information Service 42</i> with randomcareprovider@medmij to a maximum of 180 days from today;</li> <li>subscribe~0/randomcareprovider~42, to terminate the <i>Subscription to Information Service 42</i> with randomcareprovider@medmij.</li> </ul>
state	<ol style="list-style-type: none"> <li>in accordance with <a href="#">section 4.1.1. of RFC 6749</a></li> <li>the value must not contain URI</li> </ol>	<p>The <i>Client</i> uses this to give information to the <i>OAuth Authorization Server</i>, from which the former can subsequently (during the redirect) deduce which request the Authorization code belongs to. This information is in other respects meaningless for the <i>OAuth Authorization Server</i>. The second requirement is a measure against security risk <a href="#">4.1.5</a>. The state parameter cannot be intended to be added to, or otherwise incorporated into the redirect_uri.</p>

1b. The *Client* ensures that when it comes to the authorization request it is the http method GET that is used, not POST.

### Explanatory Notes

In the [OAuth specification, section 3.1](#), it is made mandatory for the Authorization Server to accept GET, with POST being kept optional. Because GET is easily the most appropriate http method for the authorization request in the MedMij Trust Scheme, this responsibility applies in order to ensure that the *Authorization Server* is not faced with unnecessary implementation costs. Although this responsibility is a responsibility of the *Client*, since this comes under the responsibility of a MedMij participant the request is ultimately executed by the *OAuth User Agent*.

2. After receiving an authorization request with a certain client\_id and a certain *Provider* and *Information Service ID* in the scope, the *Authorization Server* will verify whether:

- this *Information Service ID* is used for the client\_id in question on the *Client directory*;
- they, on behalf of this *Provider* make this *Information Service* available, as confirmed by the *Information service directory*;
- if the scope also includes subscribe:
  - whether a subscription notification and a Resource Notification Endpoint are also specified for the client\_id and *Information Service* in question on the *Client directory*;
  - they, on behalf of this *Provider* also make *Subscriptions* to this *Information Service* available, as confirmed by the *Information service directory*.

If any of these verifications fails, the *Authorization Server* will treat this as exception 1b as per responsibility 6.

### Verification of recognition on Information Service

This way, the *Authorization Server* prevents acceptance of a request that has turned out not to be permitted after consultation of *Client directory* or *Information service directory*.

3. During the processing of an authorization request, *Authorization Server*, in its role of *Authentication Client* and before asking the *User* for OAuth Authorization, will have the *User* authenticated by the *Authentication Service*.

### Authentication

In accordance with [flow diagram](#) under 1. The Provider in the Provider's Domain and thus in the BSN domain is obliged - for the provision of data from a health record - to use the BSN to verify the identity of the individual.

The MedMij Trust Scheme places the use of the *Authentication Service* in the OAuth flow, under the operational responsibility of the *Authorization Server*. The last-named acts in this regard under the responsibility of individual *Providers*, because they are the reason why the *Individual* authenticates himself.

The direct interaction of the *Individual* with the *Authorization Server* is intended to authorise the *Publishing Server* to address the *Resource Server*. This ultimately delivers the *Information Service*.

4. Immediately after authentication of the *User*, as specified in responsibility 3, and only if successful, the *OAuth Authorization Server* will ask the *User* for a [Declaration of consent](#) (in the case of [UCI Collect](#) or [UCI Subscribe](#)) or a [Declaration of confirmation](#) (in the case of [UCI Share](#)), as per the relevant stipulations on page [User interface \(Declarations\)](#), in compliance with standard [OAuth 2.0](#), in the way it is used in the MedMij Trust Scheme.

5. Prior to issuing an Authorization code through the `redirect_uri` included in the authorization request, the *OAuth Authorization Server* will record this Authorization code and the `redirect_uri` used for it.

### Explanatory Notes

This is a measure against security risks [4.4.1.3](#), [4.4.1.5](#) and [4.4.1.7](#) from RFC 6819 (see [Application Layer](#), responsibility 18). See responsibility 4 for the [Token interface](#).

6. *Authorization Server* and *Publishing Server* handle exceptional situations with respect to the authorization interface as per the below table.

Number	Implements exceptions	Exception	Action	Notification	Follow-up
authorization interface 1a	UC Collect 1 UC Share 1 UC Subscribe 1	<i>Authorization Server</i> receives an authorization request without a (valid) <code>redirect_uri</code> and /or without a (valid) <code>client_id</code> .	<i>Authorization Server</i> informs <i>Presenter</i> of this exception. <i>Authorization Server</i> does not execute a redirect to the <i>Client</i> , not with an error message either.	in accordance with <a href="#">OAuth 2.0 specification</a> , section 4.1.2.1	All stop the flow of the <i>UCI Collect/UCI Share</i> immediately after having been informed of the exception.

authorization interface 1b		<i>Authorization Server</i> receives an invalid authorization request, other than exception 1.	<i>Authorization Server</i> informs <i>Publishing Server</i> of this exception. <i>Publishing Server</i> informs <i>User</i> thereof.	in accordance with <a href="#">OAuth 2.0 specification</a> , section 4.1.2.1, with the applicable error code specified there
authorization interface 2	UC Collect 2 UC Share 2 UC Subscribe 2	<i>Authorization Server</i> cannot establish the identity of the <i>User</i> .	<i>Authorization Server</i> informs <i>Publishing Server</i> of this exception. <i>Publishing Server</i> informs <i>User</i> that no progress can be made on his request but leaves the cause of this completely aside.	In accordance with <a href="#">OAuth 2.0 specification</a> , section 4.1.2.1, error code access denied, with the error description containing the message "Access denied."
Authorization interface 3	UC Collect 3 UC Share 3 UC Subscribe 3	While processing the authorization request, the <i>Authorization Server</i> establishes that: <ul style="list-style-type: none"> <li>• in case of <a href="#">UCI Collect</a>: no health information for <i>Individual</i> is available at <i>Provider</i> for the <i>Information Service</i>;</li> <li>• in case of <a href="#">UCI Share</a>: <i>Provider</i> is not receptive for the <i>Information Service</i> of <i>Individual</i>;</li> <li>• in case of <a href="#">UCI Subscribe</a>: <i>Provider</i> does not make <i>Notifications</i> available for <i>Individual</i> on that <i>Information Service</i>. See the explanatory notes to <a href="#">Availability condition and acceptability condition</a>.</li> </ul>		
Authorization interface 4	UC Collect 4 UC Share 4 UC Subscribe 4	The authorization request is denied.		

authorization interface 5	UC Collect 5 UC Share 5 UC Subscribe 5	<i>Authorization Server</i> cannot establish the Authorization.	<i>Authorization Server</i> informs <i>Publishing Server</i> of this exception. <i>Publishing Server</i> then informs <i>User</i> about this.	In accordance with <a href="#">OAuth 2.0 specification</a> , section 4.1.2.1, error code access denied, with the error description including the message "Authorization failed."
---------------------------	---	---	---	--

### Explanatory Notes

Exceptional situations can be considered implementation counterparts to the exceptions of the [UC Collect](#) and the [UC Share](#). However, these are not organised by interface on the Application Layer. All exceptions are detected by the *Authorization Server*. In this version of the MedMij Trust Scheme, it has been determined that they always lead to the quickest possible termination of the flow by all roles involved. However, the other roles must first be informed about this. In order to prevent the *Publishing Server* from obtaining information about the treatment relationships before consent has (already or otherwise) been given for this, the distinction between the exceptions 2, 3 and 4 must not be made by the *Publishing Server*.

This table only contains the exceptional situations for which the MedMij Trust Scheme lays down its own requirements for the implementation. The [specification of OAuth 2.0](#) also contains more generic exceptional situations, such as the situation in which the redirect URI turns out to be invalid. These exceptional situations must be implemented too.

## Token interface\_

### Introduction

This page shows only the responsibilities with respect to the token interface that are not yet specified in the [OAuth 2 specification](#).

1. The parameters in the access token request are filled in as follows:

parameter	entry	explanatory notes
grant_type	literal value "Authorization_code"	This is the result of responsibility 4 in the <a href="#">Application Layer</a> .
code	in accordance with responsibility 8a-d in the <a href="#">Application Layer</a>	See the explanatory notes for responsibility 8a-d in the <a href="#">Application Layer</a> .
client_id	the hostname of the <i>Node</i> of the <i>Client</i> that submitted the authorization request that returned the Authorization code that has now been issued	The <a href="#">OAuth 2.0 specification</a> will not make this parameter compulsory if the <i>Client</i> authenticates itself, which happens in the MedMij Trust Scheme using mutual TLS. And the need to use it is limited by responsibility 4 on this page, which guarantees that the access token is only offered to the <i>Client</i> to whom consent has been granted by the <i>OAuth Resource Owner</i> . <a href="#">Chapter 2 of an internet draft on the subject</a> , however, states that the client_id is not to be used after all when mutual TLS is used. The latter is the case in the MedMij Trust Scheme (see <a href="#">Infrastructure Layer</a> ).
redirect_uri	the same value as in the previous authorization request	

2. The parameters in the [access token response](#) are populated as follows:

parameter	entry	explanatory notes
access_token	The access token issued.	
token_type	literal value "Bearer"	
expires_in	900	In accordance with responsibility 7 on the <a href="#">Application Layer</a> .

refresh_token	not used	In accordance with responsibility 7 on the <a href="#">Application Layer</a> .
scope	<p>In accordance with <a href="#">section 5.1 of the OAuth 2.0 specification</a>. In addition thereto: compulsory if the authorization request requests a <i>Subscription</i>. In that case, the scope parameter equals that in the <a href="#">authorization request</a> in question, albeit with the <i>Subscription</i> duration set to the duration assigned by the <i>Authorization Server</i>, which may therefore be a limited value, in whole days from today. The assigned duration of the <i>Subscription</i> is:</p> <ul style="list-style-type: none"> <li>• not longer than the <i>Subscription</i> duration requested in the authorization request;</li> <li>• not longer than the maximum subscription duration specified by the Provider on the Information service directory for that <i>Information Service</i> and that <i>Interface version</i>;</li> <li>• is 0 in case of a termination request.</li> </ul>	

#### Maximum duration

Given that a *Provider* on the *Information service directory* is not allowed to specify a maximum subscription duration that exceeds the maximum subscription duration for the *Information Service* in question as specified in the [Information service catalogue](#), the scope will not show an actual subscription that exceeds the maximum subscription duration for the *Information Service* in question, as specified in the [Information service catalogue](#).

3. The *Client* provides a certain Authorization code a maximum of one time to the *Authorization Server* to obtain an access token. The *Authorization Server* removes an Authorization code when it has been offered once for the obtaining of an access token.

#### Explanatory Notes

This is a measure against [security risk 4.1.1](#) from RFC 6819 (see [Application Layer](#), notes to responsibilities 15-17). The removal of an Authorization code means that the *Authorization Server* keeps track of an Authorization code that has been issued once, in order to see whether it has already been used at some time to obtain an access token. If an Authorization code has been provided for a second or subsequent time to obtain an access token then the *Authorization Server* will reject it and terminate the flow. If the *Client* to whom it was rejected was in bad faith then this has averted a hazard. If however they were in good faith and acted in accordance with the MedMij Trust Scheme then they were not the party that had already provided the Authorization code previously, which means there appears to be a security breach.

4. The *OAuth Authorization Server* will not transfer an access token if the token does not include a `redirect_uri`, and neither if the token request includes a `redirect_uri` that is not identical to the `redirect_uri` that the *OAuth Authorization Server*, upon issuing it, has linked to the Authorization code provided in the token request.



## Explanatory Notes

This is a measure against security risks [4.4.1.3](#), [4.4.1.5](#) and [4.4.1.7](#) from RFC 6819 (see [Application layer](#), responsibility 18).

With respect to the `client_id` and `redirect_uri` parameters in the authorization request and the access token request, the following applies:

- the `client_id` in the authorization request must match the hostname of the `redirect_uri` in the same authorization request (responsibility 1 for [authorization interface](#));
- the `redirect_uri` in the access token request must match the `redirect_uri` in the authorization request (this responsibility).

In the access token request, the `redirect_uri` will then not play the role of addressing the response, as it does in the authorization request, but solely be a return link back to the `redirect_uri` of the [authorization interface](#). In the processing of the [Token interface](#), there is no redirection at all, as it takes place on the backchannel in its entirety.

5. After receiving an access token request in *UCI Collect* or *UCI Share*, the *OAuth Authorization Server* will, if an access token must be issued in response, provide this access token to the *Client* after a maximum of ten (10) seconds. This behaviour of the *OAuth Authorization Server* is available at least 99.5% of the time.

6. *OAuth Authorization Server* and *Client* handle exceptional situations with respect to the token interface as per the below table.

Number	Implements exception	Exception	Action	Notification	Follow-up
Token interface 1	UC Collect 6 UC Share 6 UC Subscribe 6	<i>Authorization Server</i> must reject the token request based on one of the reasons specified in the <a href="#">OAuth 2.0 specification</a> , section 5.2.	<i>Authorization Server</i> informs <i>Publishing Server</i> of this exception. <i>Publishing Server</i> then informs <i>User</i> about this.	with the error code applicable in accordance with <a href="#">OAuth 2.0 specification</a> , section 5.2	All stop the flow of the <i>UCI Collect / UCI Share</i> immediately after having been informed of the exception.
Token interface 2	UC Collect 3 UC Share 3 UC Subscribe 3	While processing the token request, the <i>Authorization Server</i> establishes that: <ul style="list-style-type: none"> <li>• in case of <i>UCI Collect</i>: no health information for <i>Individual</i> is available at <i>Provider</i></li> </ul>	<i>Authorization Server</i> informs <i>Publishing Server</i> of this exception. <i>Publishing Server</i> informs <i>User</i> that no progress can be made on his request but leaves the cause of this completely aside.	In accordance with <a href="#">OAuth 2.0 specification</a> , section 4.1.2.1, error code access denied, with the error description containing the message "Access denied."	



		for the <i>Information Service</i> ; • in case of <i>UCI Share</i> : <i>Provider</i> is not receptive for the <i>Information Service of Individual</i> . See the explanatory notes to <a href="#">Availability condition and acceptability condition</a> .		
--	--	--	--	--

### Explanatory Notes

Exceptional situations can be considered implementation counterparts to the exceptions of the [UC Collect](#) and the [UC Share](#). However, these are not organised by the interface on the Application Layer. All exceptions are detected by the *Authorization Server*. In this version of the MedMij Trust Scheme, it has been determined that they always lead to the quickest possible termination of the flow by all roles involved. However, the other roles must first be informed about this.

This table only contains the exceptional situations for which the MedMij Trust Scheme lays down its own requirements for the implementation. The [specification of OAuth 2.0](#) also contains more generic exceptional situations, such as the situation in which the redirect URI turns out to be invalid. These exceptional situations must be implemented too.

## Resource interface\_

### Introduction

#### Introduction

The Resource interface forms part of the Exchange [primary function](#).

This page shows only the responsibilities with respect to the Resource interface that are not yet specified in:

- the [OAuth 2 specification](#).
- the information standard for the *Information Service* that is addressed on the Resource interface.

1. To send the access token, in the resource request, the *Client* uses the method authorization request Header Field, as described in section 2.1 of RFC6750.

### Explanatory Notes

The authorization request Header Field method offers the best security.

2. After receiving a resource request, in *UCI Collect* or *UCI Share*, the *Resource Server* will, if a resource response is required, after a maximum of sixty (60) seconds, make this resource response available to the *Publishing Server*. This behaviour of the *Resource Server* is available at least 98.5% of the time.

3. In so far as the transfer between *Publishing Server* and *Resource Server*, namely in the use case implementations *UCI Collect* and *UCI Share*, there is, in the control data, a data element from which the identity of the *User* can be derived, they use for this nothing else than the OAuth data that they had to exchange in their respective *Client* and *OAuth Resource Server*. *Publishing Server*, *Authorization Server* and *Resource Server* make properly secured arrangements where they can if necessary establish the identity of the *User* themselves.

### Explanatory Notes

With a view to guaranteeing privacy and keeping the architecture of the MedMij Trust Scheme as simple as possible, it has been decided to keep the identifier for the *User* as meaningless as possible 'en route'. All meaning is linked on both sides by consulting internal registrations. Because the *Publishing Server*, *Authorization Server* and *Resource Server* process an OAuth flow together, they possess (after authentication of the *User*) tokens that represent the identity of the *User*, namely (first) the Authorization code and (later) the access token. Apart from these, no identifying data elements need to be or will be included in the transfer. The FHIR data element *PatientID* will *not* be used.

4. *OAuth Resource Server* and *Client* handle exceptional situations with respect to the Resource interface as per the below table.

Number	Implements exception	Exception	Action	Notification	Follow-up
Resource interface 1	UC Collect 6, UC Share 6	The validation of the access token by <i>Resource Server</i> fails.	<i>Resource Server</i> informs <i>Publishing Server</i> of this	as <i>OperationOutcome</i> in accordance with FHIR specification, analogous to Resource	All stop the flow immediately after being

			exception. <i>Publishing Server</i> then informs <i>User</i> about this.	interface exception 2, but with issue type "security" or "suppressed".	informed about the exception.
Resource interface 2	UC Collect 5, UC Share 5	<i>Resource Server</i> is unable to fulfil the request in full, on time, or at all, for reasons other than Resource interface exception 1. See also the explanatory notes to <a href="#">Availability condition and acceptability condition</a> .	<i>Resource Server</i> informs <i>Publishing Server</i> of this exception. <i>Publishing Server</i> then informs <i>User</i> about this.	in accordance with the specification of the <i>Information standard</i> used	The flow can be continued.

## Subscription interface\_

### Introduction

The subscription interface forms part of the [Control\\_primary function](#). This page shows only the responsibilities with respect to the Resource interface that are not yet specified in the [OAuth 2 specification](#).

1a. The subscription request is:

- if the *Individual*, through this *Individual's Service Provider*, does not yet have a *Subscription* with this *Provider* to (Notifications about) this *Information Service*: a HTTP POST request;
- if the *Individual*, through this *Individual's Service Provider*, already has a *Subscription* with this *Provider* to (Notifications about) this *Information Service*: a HTTP PUT request;

### Subscription request

Through the subscription request, the *Publishing Server* sends the *Subscription Server* a new *Subscriptions* resource, along with the, as yet, unilateral consent of the *Individual*, thus also requesting a subscription response, which also includes the consent of the *Provider*. This is how the agreement comes about. Consent for a termination of a *Subscription* is obtained from both parties in this same way, even though the *Provider* cannot reject such a termination.

1b. To send the access token, in the subscription request, the *Client1* uses the method authorization request Header Field, as described in [section 2.1 of RFC6750](#).

### Explanatory Notes

The authorization request Header Field method offers the best security.

1c. The *Client* and the *Subscription Server* use JSON [for the exchange of subscription requests and subscription responses](#).

2. The parameters of the subscription request are populated as follows:

parameter	entry	explanatory notes
Provider	compulsory, the same value as for the <i>Provider</i> in the scope of the previous token response	-
Information Service	compulsory, the same value as for the <i>Information Service</i> in the scope of the previous token response	-
duration	compulsory, the same value as for the duration parameter in the scope of the previous token response	-
client_id	compulsory, the same value as the client_id used in the previous authorization request	-
replaces	<ul style="list-style-type: none"> <li>• absent, if the <i>Individual</i>, through this <i>Individual's Service Provider</i>, does not yet have a</li> </ul>	In the case of <i>replaces</i> , the subscription_id identifies the <i>Subscription</i> that will be terminated

	<p><i>Subscription</i> with this <i>Provider</i> to (<i>Notifications</i> about) this <i>Information Service</i>:</p> <ul style="list-style-type: none"> <li>compulsory, if the <i>Individual</i>, through this <i>Individual's Service Provider</i>, already has a <i>Subscription</i> with this <i>Provider</i> to (<i>Notifications</i> about) this <i>Information Service</i>, and then populated with the <code>subscription_id</code> of that <i>Subscription</i>.</li> </ul>	for this subscription request (if <code>duration=0</code> ) or amended (different).
--	---	---

### Introduction

Through the subscription request, the *Publishing Server* requests the *Subscription Server* to create a *Subscription*, possibly to replace an existing one, or to terminate it. In doing so, the *Publishing Server* also already establishes that the *Individual* has consented to this change.

3a. After receiving the subscription request, the *Subscription Server* will verify on the *Authorization Server* whether the included access token has been issued for a *Subscription* with the *Provider* in question, to *Notifications* of the *Information Service* in question and with the duration in question. If not, the *Subscription Server* will treat it as a Subscription interface 1 exception.

### Explanatory Notes

The access token, therefore, needs to have a scope that matches the parameters of the subscription request exactly.

3b. If `replaces` has a value, the *Subscription Server* verifies that this parameter identifies a *Subscription* of the same *Individual*, through the same *Individual's Service Provider*, to the same *Information Service* with the same *Provider*. If not, the *Subscription Server* will treat it as a Subscription interface 1 exception.

### Explanatory Notes

This way, the *Subscription Server* checks that the *Publishing Server* knows the *Subscription* that it was going to terminate or change through this subscription request.

4. The only parameter in the subscription response is populated as follows.

parameter	entry	explanatory notes
<code>subscription_id</code>	identification which the <i>Subscription Server</i> uses to uniquely identify the <i>Subscription</i> for this <i>Individual</i> and the <i>Individual's Service Provider</i>	<p>This value uses the <i>Notification Server</i> to identify the <i>Subscription</i> that goes with an incoming <i>Notification</i>. This also identifies the <i>Subscription</i> in log files.</p> <p>The <code>subscription_id</code> can be an integer value or an UUID, but can also be populated as per another valid identification pattern.</p>

### Subscription response

Through the subscription response, the *Subscription Server* reports that the *Provider* also accepts the *Subscription*.

5. *Subscription Server* and *Client* handle exceptional situations with respect to the subscription interface as per the below table.

Number	Implements exception	Exception	Action	Notification	Follow-up
Subscription interface 1	UC Subscribe 6	The validation of the access token by <i>Subscription Server</i> fails, or the availability condition is not met. See also the explanatory notes to <a href="#">Availability condition and acceptability condition</a> .	<i>Subscription Server</i> informs <i>Publishing Server</i> of this exception. <i>Publishing Server</i> then informs <i>User</i> about this.	In accordance with <a href="#">HTTP specification</a> with status code 401 "Not authorised"	All stop the flow immediately after being informed about the exception.
Subscription interface 2		<i>Subscription Server</i> receives an invalid request.		In accordance with <a href="#">HTTP specification</a> with status code 400 "Invalid request"	
Subscription interface 3	UC Subscribe 3	<i>Subscription Server</i> is unable to fulfil the request in full, on time, or at all, for reasons other than Subscription interface exception 1 or Subscription interface exception 2.		In accordance with <a href="#">HTTP specification</a> with status code 500 "Internal server error"	

6. After receiving a subscription request, in *UCI Subscribe*, the *Subscription Server* will, if a subscription response is required, after a maximum of sixty (60) seconds, make this resource available to the *Publishing Server*. This behaviour of the *Subscription Server* is available at least 98.5% of the time.

## Subscription notification interface\_

### Explanatory Notes

The subscription notification interface forms part of the [Control primary function](#), while the [resource notification interface](#) forms part of the [Exchange primary function](#).

- 1a. The *Notification Client* and the *Notification Server* use HTTP 1.1 on the subscription notification interface.
  - 1b. The *Notification Client* sends the subscription notification through an [HTTP POST](#) of a *Notification* on the *Subscription Notification Endpoint* found on the *Client directory*.
  - 1c. For *Notifications* and error messages on the subscription notification interface, *Notification Client* and the *Notification Server* use the [JSON](#) format.
2. The three parameters in the subscription notification are populated as follows.

parameter	entry	explanatory notes
subscription_id	The value that the <i>Subscription Server</i> has used to identify this <i>Subscription</i> in the <a href="#">subscription response</a> .	An event at a <i>Provider</i> can, in theory, lead to multiple <i>Notifications</i> . Every <i>Notification</i> relates to one single <i>Subscription</i> .
notification_type	The literal value subscription.	This allows the <i>Notification Server</i> to differentiate the subscription notification from the resource notification.
duration	The remaining duration of the <i>Subscription</i> in whole days. If this value is 0, the <i>Subscription</i> has been terminated by the <i>Provider</i> . In all other cases, this value is not greater than the remaining duration, based on the <i>Subscription</i> records of the <i>Subscription Server</i> . The value can be smaller than this remaining duration if the policy of the <i>Provider</i> with respect to the availability condition allows the limitation of the subscription.	<i>Subscriptions</i> can be terminated by both <i>Provider</i> and <i>Publisher</i> . Termination by <i>Publisher</i> goes through the <a href="#">subscription interface</a> . Termination by <i>Provider</i> goes through the subscription notification interface. The limitation options allow the <i>Provider</i> to adhere to the availability policy at all times.

3. The only parameter of the subscription notification response is populated as follows.

parameter	entry	explanatory notes
notification_id	identification that the <i>Notification Server</i> uses to uniquely identify the <i>Notification</i> for this <i>Subscription</i>	This can, for example, be an integer value or an UUID, but can also be populated as per another valid ID pattern.

4. After receiving a subscription notification, the *Notification Server* will, if a subscription notification response is required, after a maximum of ten (10) seconds, make this response available to the *Notification Client*. This behaviour of the *Notification Server*

5. *Notification Server* and *Notification Client* handle exceptional situations with respect to the subscription notification interface as per the below table.

Number	Implements exception	Exception	Action	Notification	Follow-up
Subscription notification interface 1	UC Notify 1	<i>Notification Server</i> considers the <i>Notification</i> received to be invalid.	<i>Notification Server</i> informs <i>Notification Client</i> of this exception.	In accordance with <a href="#">HTTP specification</a> with status code 400 "Invalid request", and with the applicable error code ("invalid_subscription_id", "invalid_notification_type" or "invalid_duration") in the body	All stop the flow immediately after being informed about the exception. When <i>Notification Client</i> receives an error "invalid_subscription_" the <i>Subscription</i> must be terminated right away and without having to send a subscription notification again.
Subscription notification interface 2	UC Notify 2	<i>Notification Server</i> is unable to process the request in full, on time, or at all.	<i>Notification Server</i> informs <i>Notification Client</i> of this exception.	In accordance with <a href="#">HTTP specification</a> with status code 500 "Internal server error"	All stop the flow immediately after being informed about the exception.



## Resource notification interface\_

### Explanatory Notes

The resource notification interface forms part of the [Exchange primary function](#), while the subscription notification interface forms part of the [Control primary function](#).

- 1a. The *Notification Client* and the *Notification Server* use HTTP 1.1 on the resource notification interface.
- 1b. The *Notification Client* sends the resource notification through an [HTTP POST](#) of a *Notification* on the *Subscription Notification Endpoint* found on the *Client directory*.
- 1c. For *Notifications* and error messages on the resource notification interface, *Notification Client* and the *Notification Server* use the [JSON](#) format.
2. The two parameters in the resource notification are populated as follows.

parameter	entry	explanatory notes
subscription_id	The value that the <i>Subscription Server</i> has used to identify this <i>Subscription</i> in the subscription response.	An event at a <i>Provider</i> can, in theory, lead to multiple <i>Notifications</i> . Every <i>Notification</i> relates to one single <i>Subscription</i> .
notification_type	The literal value resource.	This allows the <i>Notification Server</i> to differentiate the resource notification from the subscription notification.

### Explanatory Notes

This does not include, as is the case in the subscription notification, a duration because that forms part of the [Control primary function](#). Communication on the *Subscription* records happens entirely on the [subscription notification interface](#). The resource notification interface is intended solely for content-related notifications. In future releases of the MedMij Trust Scheme, the resource notification may include a further indication of the part of the *Information service* where new information is available.

3. The only parameter of the resource notification response is populated as follows.

parameter	entry	explanatory notes
notification_id	identification that the <i>Notification Server</i> uses to uniquely identify the <i>Notification</i> for this <i>Subscription</i>	The id can, for example, be an integer value or an UUID, but can also be populated as per another valid ID pattern.

- 4a. A *Notification Client* sends, [within one \(1\) hour](#) after new (health) information becoming available for that *User* relating to that *Information service*, a related resource notification to the *Notification Server* in question.

### Notifications

New (health) information is considered to have become available at the moment that the information is designated as "available to *User*" on behalf of the *Provider* (manually or automatically).

4b. After receiving a resource notification, the *Notification Server* will, if a resource notification response is required, after a maximum of ten (10) seconds, make this response available to the *Notification Client*. This behaviour of the *Notification Server* is available at least 98.5% of the time.

5. *Notification Server* and *Notification Client* handle exceptional situations with respect to the resource notification interface as per the below table.

Number	Implements exception	Exception	Action	Notification	Follow-up
Resource notification interface 1	UC Notify 1	<i>Notification Server</i> considers the resource notification received to be invalid.	<i>Notification Server</i> informs <i>Notification Client</i> of this exception.	In accordance with <a href="#">HTTP specification</a> with status code 400 "Invalid request", and with the applicable error code ("invalid_subscription_id" or "invalid_notification_type") in the body	All stop the flow immediately after informed about this exception. When <i>Notification Client</i> receives an error "invalid_subscription_id" the <i>Subscription</i> terminated right and without having send a notification
Resource notification interface 2	UC Notify 2	<i>Notification Server</i> is unable to process the request in full, on time, or at all.	<i>Notification Server</i> informs <i>Notification Client</i> of this exception.	In accordance with <a href="#">HTTP specification</a> with status code 500 "Internal server error"	All stop the flow immediately after informed about this exception.

## Isg, Cld and Isd interface

1. The URI of the:

- *Information service directory* is [https://stelselnode.medmij.nl/MedMij\\_Zorgaanbiederslijst.xml?api=1.2.0](https://stelselnode.medmij.nl/MedMij_Zorgaanbiederslijst.xml?api=1.2.0)
- *Client directory* is [https://stelselnode.medmij.nl/MedMij\\_OAuthclientlist.xml?api=1.2.0](https://stelselnode.medmij.nl/MedMij_OAuthclientlist.xml?api=1.2.0)
- *Information service glossary* is [https://stelselnode.medmij.nl/MedMij\\_Gegevensdienstnamenlijst.xml?api=1.2.0](https://stelselnode.medmij.nl/MedMij_Gegevensdienstnamenlijst.xml?api=1.2.0)

### List interface versions

From MedMij Trust Scheme release 1.1.2 onwards, list interfaces have a version number to make it possible to have multiple versions in production simultaneously. As of release 1.1.2, the versions are differentiated from each other through a query parameter in the URI.

The version number is identical to that of the release in question. Successive versions of list interfaces may, therefore, be identical in terms of their content. In release 1.1.2, the list interfaces for the *Information service directory*, the *Information service glossary* (and the *Whitelist*) are identical to those in release 1.1.1. The Cld interface, however, is different in release 1.1.2 and release 1.1.1.

2. The participation of *MedMij Registration* in each of the use case implementations *UCI Retrieve Isd*, *UCI Retrieve Rcd* and *UCI Retrieve Isg* is available at least 99.9% of the time. If the participation referred to becomes unavailable then *MedMij Maintenance* will allow a maximum of eight hours (480 minutes) to elapse before it is available again.

3. In the event of such an incident, *MedMij Maintenance* informs *Publishers*, *Sources* and *Readers* that the incident has occurred and tells them the expected downtime. *MedMij Maintenance* informs the parties about scheduled maintenance that will lead to temporary unavailability.

4. If *MedMij Registration* is unavailable in *UCI Retrieve Isd*, *UCI Retrieve Rcd* and/or *UCI Retrieve Isg* then the relevant requesters are allowed to use - for a maximum of 10 hours - the most recent copy of the relevant list in the cache.

## Use case implementations

### Introduction

This page groups together the pages of the various use case implementations:

- [\*UCI Collect\*](#)
- [\*UCI Share\*](#)
- [\*UCI Subscribe\*](#)
- [\*UCI Notify\*](#)
- [\*UCI Retrieve Isg\*](#)
- [\*UCI Retrieve Rcd\*](#)
- [\*UCI Retrieve Isd\*](#)

## UCI Collect

### Notes

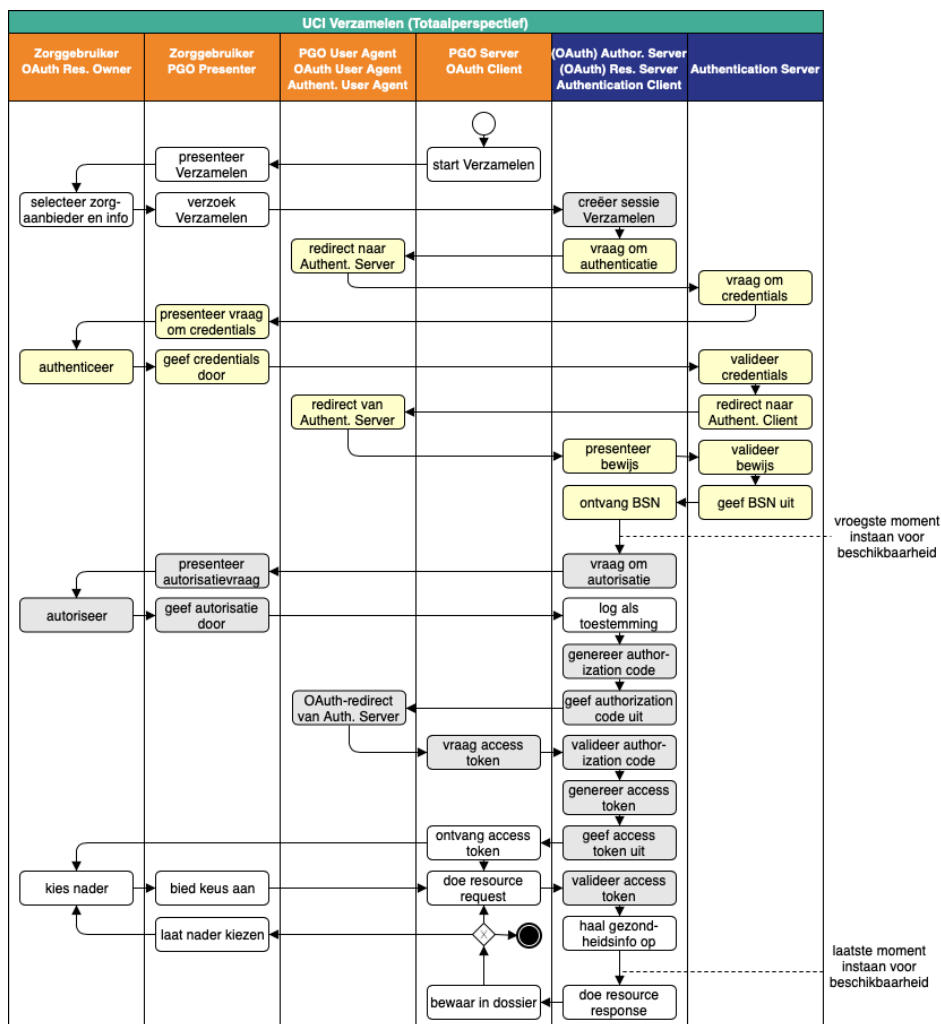
The figures below show the flow diagram of the use case implementation *Compile*, from four different perspectives:

- the overall perspective, with both the happy flow and the exceptions;
- the perspective of the *Publishing Server* (= *Client*), who comes under the *Individual's Service Provider*. The last-named can read this figure as his mandatory participation in the use case implementation *Compile*;
- the perspective of the (OAuth) *Authorization Server*/(OAuth) *Resource Server*/*Authentication Client*, who comes under the *Provider's Service Provider*. The last-named can read this figure as his mandatory participation in the use case implementation *Compile*;
- the perspective of the *User* (= *OAuth Resource Owner*).

The flow diagrams only show the situation in which all actions are successful up to and including the ultimate compiling of the health information (this situation is known as the 'happy flow'). In line with the MedMij corporate identity, the orange paths belong to the Individual's Domain and the blue to the Provider's Domain. Various actions are coloured in the flow diagrams. Together, the actions coloured in light grey form the Authorization flow in accordance with OAuth 2, whereas the actions coloured in light yellow together form the authentication flow. In other words, these colours only refer to the standards used and say nothing about which component has to execute the step. Authentication is thus embedded in Authorization. In the flow diagrams for the specific perspectives, it is only those actions in the path that belong to that perspective that are named. The actions in the other paths are compressed and depicted without names. Responsibilities with respect to exceptions to the happy flow are included in the respective interface, contrary to the [Processes & Information Layer](#), where use case are specified with the exceptions.

## Overall perspective

### Happy flow



## Notes

In each completion of the flow described in the diagram, there is in all cases only a single one of each of the roles named above.

The flow has the following steps:

1. The *Publishing Server* starts the flow by presenting the option in the *Presenter* of the *User* to compile a particular *Information service* from a certain *Provider*. This always relates to precisely one *Information service* (a single scope, in OAuth terms). From the *Information service directory*, the *Publishing Server* knows which *Information services* are offered by a *Provider*. If desired, the *Information service Names* from the *Information service glossary* are used.
2. The *User* makes explicit his selection and gets the *OAuth User Agent* to send a compile request to the *Authorization Server*. The address of the authorization endpoint is taken from the *Isd*. The *redirect\_uri* indicates to where the *Authorization Server* must hereafter redirect the *OAuth User Agent* (with the Authorization code).
3. The *Authorization Server* now begins the OAuth flow (in his role as *OAuth Authorization Server*) by creating a session.
4. The *Authorization Server* (now in the role of *Authentication Client*) starts the authentication flow by redirecting the browser to the *Authentication Server*, providing a *redirect\_uri*, which indicates to where *Authentication Server* must later return the *OAuth User Agent*, after the *User* has logged in.
5. The *Authentication Server* asks the *User* for login details via the *Presenter*.
6. When these are correct then *Authentication Server* redirects the *OAuth User Agent* back to the *Authorization Server*, whilst giving him a retrieval certificate

7. With this retrieval certificate, the *Authorization Server* retrieves the BSN (citizen service number) directly from *Authentication Server*.
8. The earliest moment then comes when the *Authorization Server* guarantees that the *Provider* - for the relevant *Information service* - has any health information of this *Individual* available at all; otherwise, the happy flow terminates. Part of this is that the *Individual* must be at least 16 years old for this.
9. If this is successful then the *Authorization Server* presents - via the *Presenter* to *User* the question of whether the last-named permits him to send the requested personal health information to the *Publishing Server* (as *Client*). Under the flow diagram it is specified which information, and from where, is processed by the *OAuth Authorization Server* in the *Declaration of consent* to be submitted to the *User*.
10. Upon agreement, the *Authorization Server* logs this as consent, generates an Authorization code and sends this as a retrieval certificate, by means of a browser redirect, along with the *redirect\_uri* received in step 1, to the *Publishing Server*. The *Authorization Server* sends with it the local state information that it received in the initial step of the *Publishing Server*. The last-named recognises in it the request that it must associate the Authorization code with.
11. The *Publishing Server* not only interprets this Authorization code as a retrieval certificate but also deduces from it that the consent has been given and logs the obtaining of the retrieval certificate.
12. The *Publishing Server* applies again to the *Authorization Server* with this retrieval certificate but now without the intermediation of the *OAuth User Agent* for an access token.
13. The *Authorization Server* now generates an access token and sends it to the *Publishing Server*.
14. The *Publishing Server* is now ready to send the request for health information to the *Resource Server* after it has prompted the user to make any further choices that may be required. It obtains the address of the resource endpoint from the *Isd*. It places the access token in the message and ensures that no BSN is included in the message.
15. The *Resource Server* checks whether the received token grants entitlement to the requested resources and retrieves them from underlying sources or other sources. The final moment then comes at which the *Resource Server* must guarantee that the *Provider* has the health data available for the relevant *Information service*. If this information is available then the *Resource Server* sends it in a resource response to the *Publishing Server*. If it isn't then the *Resource Server* terminates the happy flow
16. and will also retain the received health information in the personal record. If the *Information service* for which the *User* has authorised consists of multiple *Transactions* (see the [Information service catalogue](#) for details), or if one *Transaction* as per the relevant *Information standard* consists of multiple requests, the *Publishing Server* may subsequently request the *Resource Server* for the remaining *Transactions* after that, possibly after a new interaction with the *User*. This is possible as long as the access token is valid.

---

Generally, the Authorization interface, the token interface, and the resource interface are all addressed, in that order, in the case of one-off use of *UCI Collect*. If the *Publishing Server*, however, still has an access token that has not expired yet for the *Provider-Information service* combination in question, it can immediately address the resource interface.

---

The MedMij Trust Scheme recommends that the availability condition be made effective from the earliest stated moment. For the time being, the MedMij Trust Scheme permits this condition to become effective later on but not later than the final moment stated in the figure.

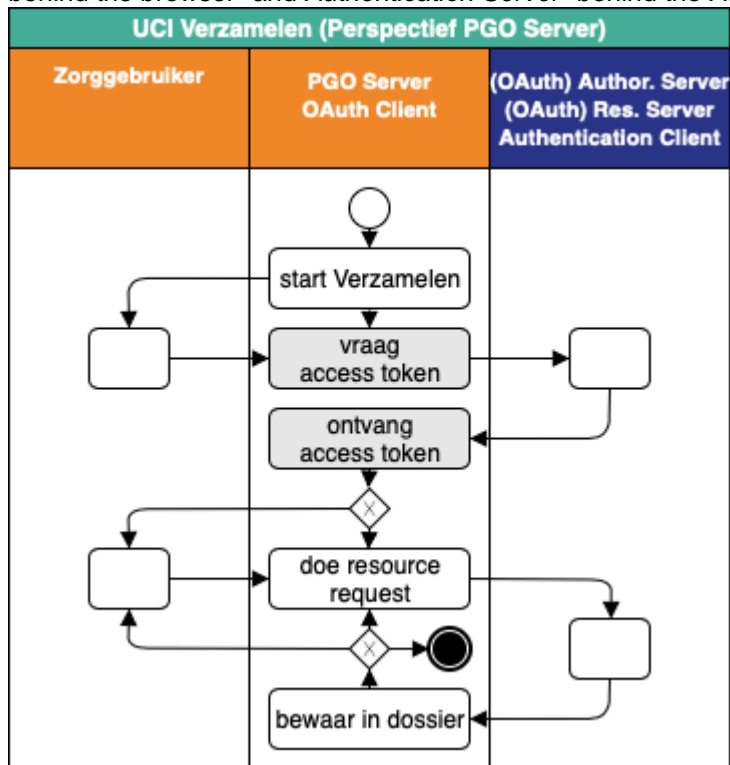
When implementing the condition of availability at the *Provider* for the health data to be compiled, it makes sense to take privacy requirements into consideration. If the *Provider's Service Provider* were to create new data compilations for the availability condition then processing always takes place under the responsibility of a single *Provider*. The combining of processing or inadequate segregation must be avoided. This can only be deviated from under the explicit instruction of the *Provider(s)* and require a careful weighing-up beforehand, due to the associated privacy risks.

## Specific perspectives

## Perspective of Publishing Server (happy flow)

### Notes

Please find below the same flow diagram but this time shown from the perspective of the *Publishing Server*. In other words, all in-between steps that are not visible to the *Publishing Server* are shorted. *User* is "hidden behind the browser" and *Authentication Server* "behind the *Authorization Server*".



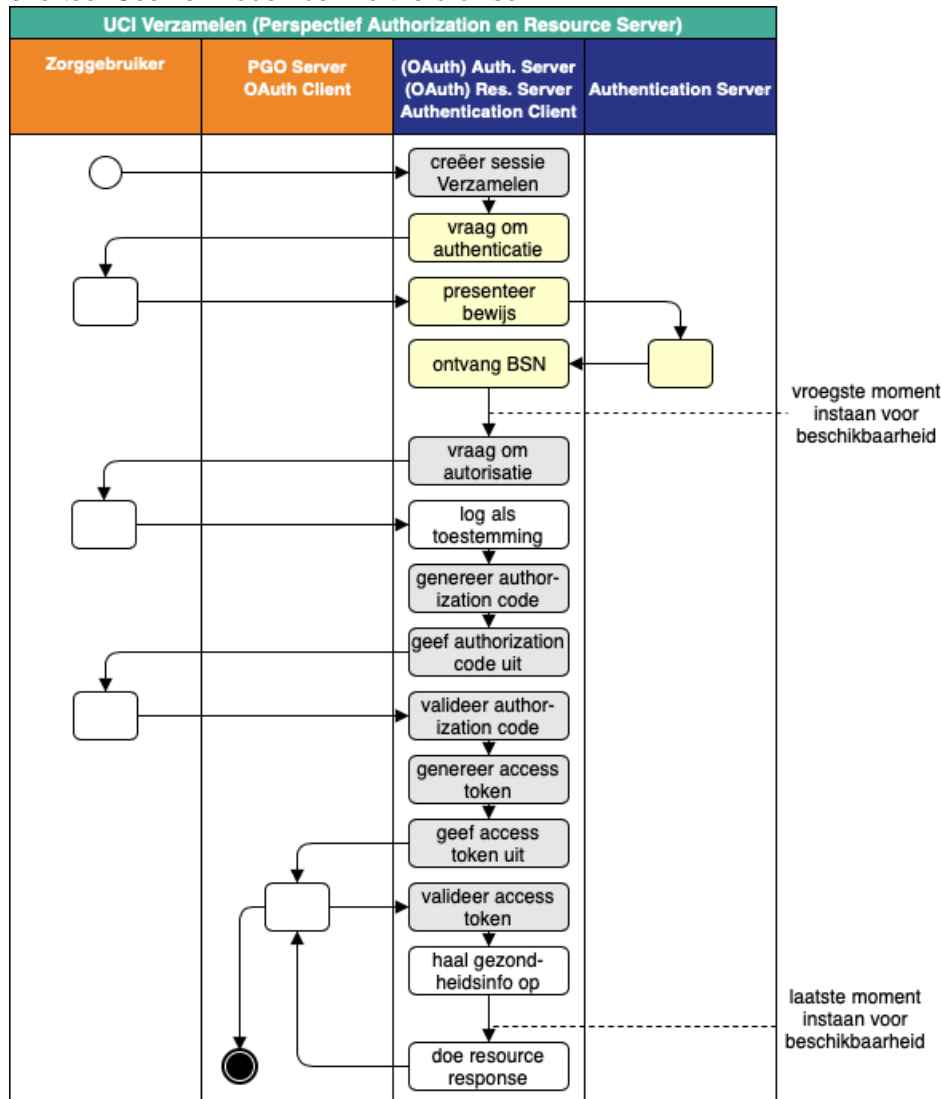
## Perspective of Authorization Server/Resource Server (happy flow)

### Notes

Please find below the same flow diagram but this time shown from the perspective of the *Authorization*



/Resource Server. In other words, all in-between steps that are not visible to the *Publishing Server* are shorted. *User* is "hidden behind the browser".

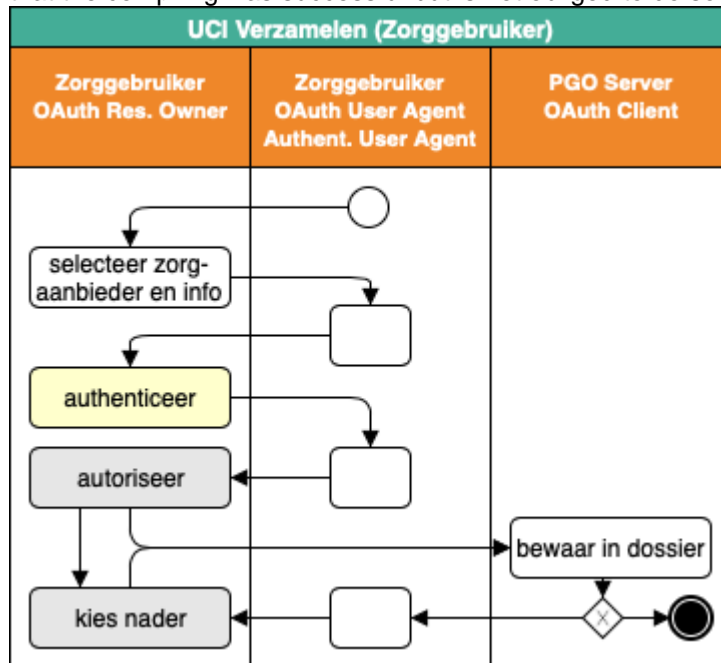


## Perspective of User (happy flow)

### Notes

Please find below the same flow diagram but this time shown from the perspective of the *User*. In other words, all in-between steps that are not visible to the *User* are shorted. Almost everything is "hidden behind the browser". We have only kept the final step of *Publishing Server* visible because the retention of the

compiled health information has meaning for the *User*. The *Publishing Server* will probably let the *User* know that the compiling was successful but is not obliged to do so.

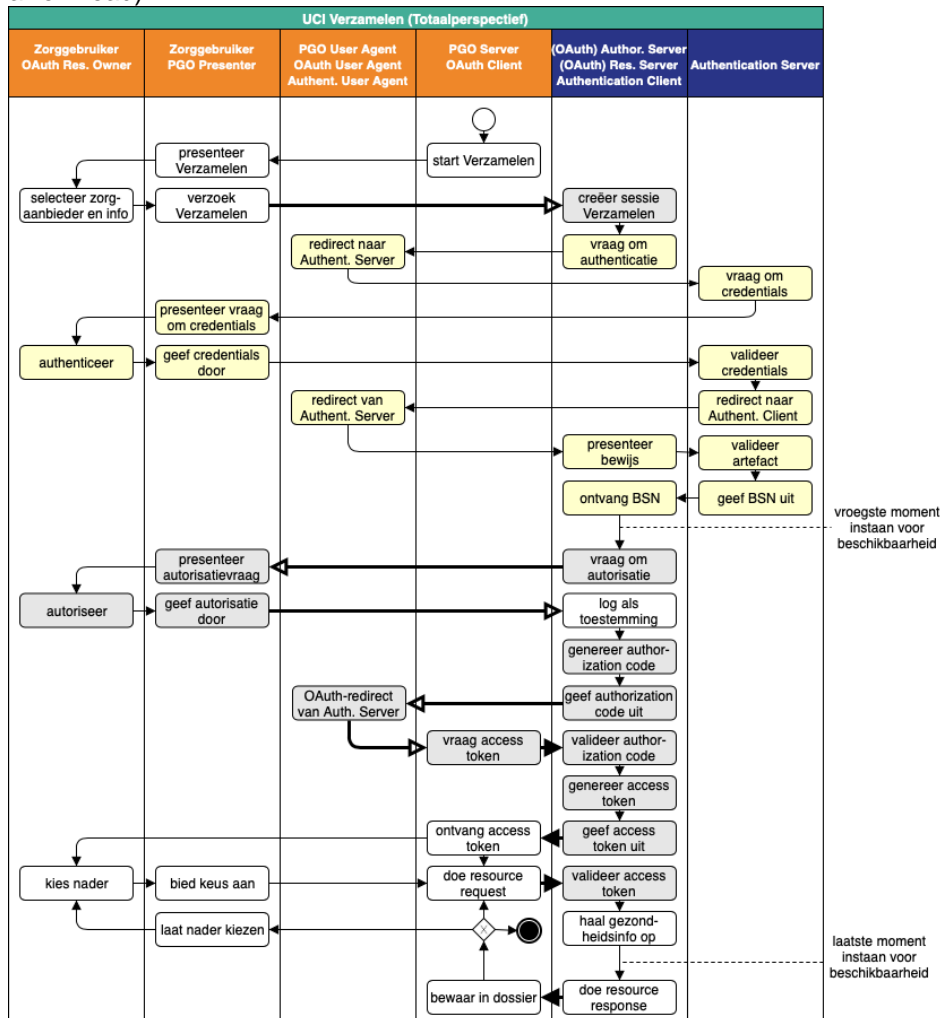


## Frontchannel and backchannel

### Notes

In the flow diagram below for UCI Collect, the thick arrows show the *MedMij data transfer* and include the five

cases of frontchannel data transfer (open arrowhead) and four cases of backchannel data transfer (closed arrowhead).



## UCI Share

### Explanatory Notes

The figures below show the flow diagram of the use case implementation *Share*, from four different perspectives:

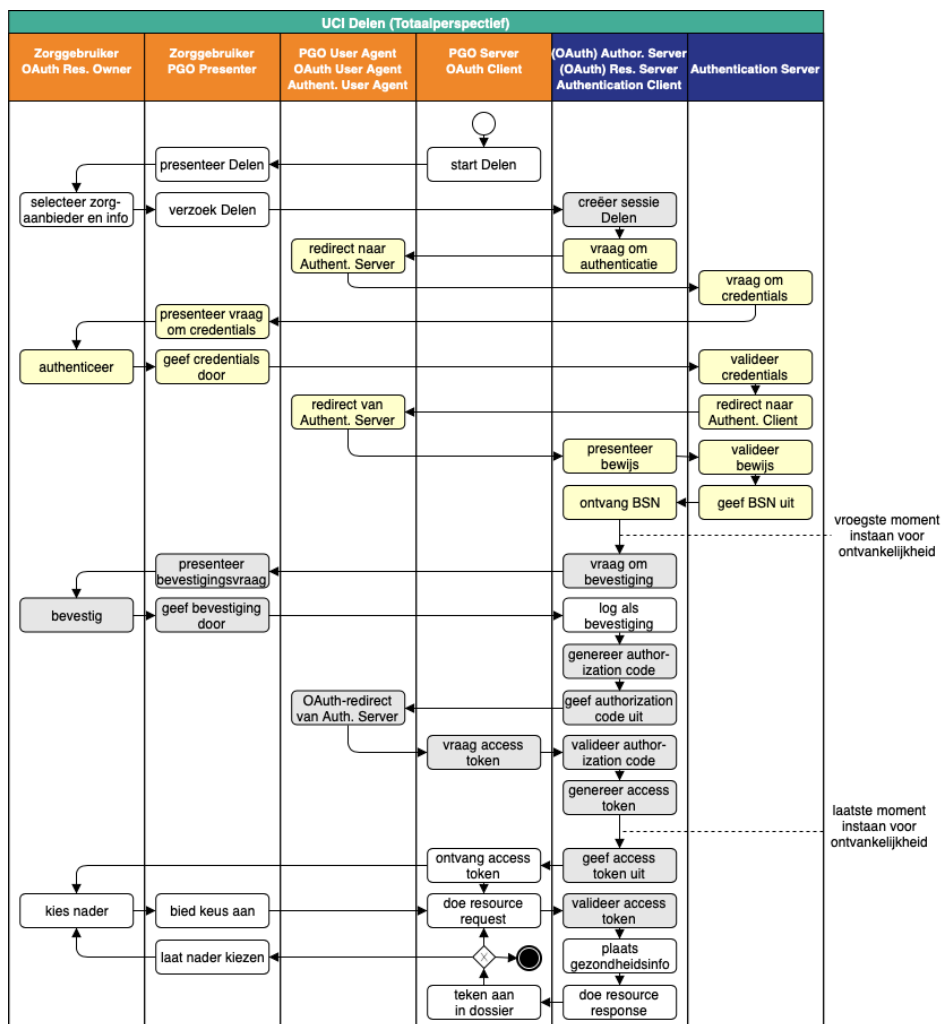
- the overall perspective, with both the happy flow and the exceptions;
- the perspective of the *Publishing Server* (= *Client*), who comes under the *Individual's Service Provider*. The last-named can read this figure as his mandatory participation in the use case implementation *Share*;
- the perspective of the (*OAuth*) *Authorization Server*/(*OAuth*) *Resource Server*/*Authentication Client*, who comes under the *Provider's Service Provider*. The last-named can read this figure as his mandatory participation in the use case implementation *Share*;
- the perspective of the *User* (= *OAuth Resource Owner*).

The flow diagrams only show the situation in which all actions are successful up to and including the ultimate compiling of the health information (this situation is known as the 'happy flow'). In line with the MedMij corporate identity, the orange paths belong to the Individual's Domain and the blue to the Provider's Domain. Various actions are coloured in the flow diagrams. Together, the actions coloured in light grey form the Authorization flow in accordance with OAuth 2, whereas the actions coloured in light yellow together form the authentication flow. In other words, these colours only refer to the standards used and say nothing about which component has to execute the step. Authentication is thus embedded in Authorization. In the flow diagrams for the specific perspectives, it is only those actions in the path that belong to that perspective that are named. The actions in the other paths are compressed and depicted without names.

Responsibilities with respect to exceptions to the happy flow are included in the respective interface, contrary to the [Processes & Information Layer](#), where use case are specified with the exceptions.

## Overall perspective

### Happy flow



## Explanatory Notes

In each completion of the flow described in the diagram, there is in all cases only a single one of each of the roles named above.

The flow has the following steps:

1. The *Publishing Server* starts the flow by presenting in the *Presenter* of the *User* the possibility of sharing a particular *Information service* with a certain *Provider*. This always relates to precisely one *Information service* (a single scope, in OAuth terms). From the *Information service directory*, the *Publishing Server* knows which *Information services* are offered by a *Provider*. If desired, the *Information service Names* from the *Information service glossary* are used.
2. The *User* makes explicit his selection and gets the *OAuth User Agent* to send a share request to the *Authorization Server*. The address of the authorization endpoint is taken from the *Isd*. The redirect URI indicates where the *Authorization Server* must hereafter redirect the *OAuth User Agent* to (with the authorization code).
3. The *Authorization Server* now begins the OAuth flow (in his role as *OAuth Authorization Server*) by creating a session.

4. The *Authorization Server* (now in the role of *Authentication Client*) starts the authentication flow by redirecting the *OAuth User Agent* to the *Authentication Server*, providing a redirect URI, which indicates to where *Authentication Server* must later return the *OAuth User Agent*, after the *User* has logged in.
5. The *Authentication Server* asks the *User* for login details via the *Presenter*.
6. When these are correct then *Authentication Server* redirects the *OAuth User Agent* back to the *Authorization Server*, whilst giving him a retrieval certificate
7. With this retrieval certificate, the *Authorization Server* retrieves the BSN (citizen service number) directly from *Authentication Server*.
8. The earliest moment then comes at which the *Authorization Server* guarantees that the *Provider* - for the *Information service* in question - is receptive to the health information of this *Individual*; otherwise, the happy flow terminates. One important factor here is that the *Individual* must be at least 16 years old for this.
9. If this is successful then the *Authorization Server* presents - via the *Presenter* - to the *User* the question of whether the last-named confirms that it will allow the requested personal health information to be offered by the *Publishing Server* (as *Client*). Under the flow diagram, it is specified which information, and from where, the *OAuth Authorization Server* processes in the confirmation request to be submitted to the *User*.
10. Upon agreement, the *Authorization Server* logs this as confirmation, generates an Authorization code and sends this as a retrieval certificate by means of a browser redirect - along with the redirect URI received in step 1 - to the *Publishing Server*. The *Authorization Server* sends with it the local state information that it received in the initial step of the *Publishing Server*. The last-named recognises in it the request that it must associate the Authorization code with.
11. The *Publishing Server* not only interprets this Authorization code as a retrieval certificate, but also deduces from it that the confirmation has been given and logs the obtaining of the retrieval certificate.
12. The *Publishing Server* applies again to the *Authorization Server* with this retrieval certificate but now without the intermediation of the *OAuth User Agent* for an access token.
13. The *Authorization Server* then generates an access token. The final moment then comes at which the *Authorization Server* must guarantee that - for the *Information service* in question - the *Provider* is receptive for the health data of the relevant *Individual*. If this is the case then the *Authorization Server* sends the access token to the *Publishing Server*. If it isn't then the *Authorization Server* terminates the happy flow and does not send an access token to the *Publishing Server*.
14. The *Publishing Server* is now ready to send the health information to the *Resource Server* after it has prompted the user to make any further choices that may be required. It obtains the address of the resource endpoint from the *Isd*. It places the access token in the message and ensures that no BSN is included in the message.
15. The *Resource Server* checks whether the received token grants entitlement to present the information, places this with underlying or other destinations and sends a reply in a FHIR response to the *Publishing Server*.
16. He creates a record about this with the health information provided in the personal record. If the *Information service* for which the *User* has authorised consists of multiple *Transactions* (see the [Information service catalogue](#) for details), the *Publishing Server* may subsequently request the *Resource Server* for the remaining *Transactions* after that, possibly after a new interaction with the *Provider*. This also goes for situations where one *Transaction*, as shown by the relevant *Information standard*, consists of multiple FHIR creates. This is possible as long as the access token is valid.

Generally, the Authorization interface, the token interface, and the resource interface are all addressed, in that order, in the case of one-off use of *UCI Share*. If the *Publishing Server*, however, still has an access token that has not expired yet for the *Provider-Information service* combination in question, it can immediately address the resource interface.

The MedMij Trust Scheme recommends that the acceptability condition be made effective from the earliest stated moment. For the time being, the MedMij Trust Scheme permits this condition to become effective later on but not later than the final moment stated in the figure.

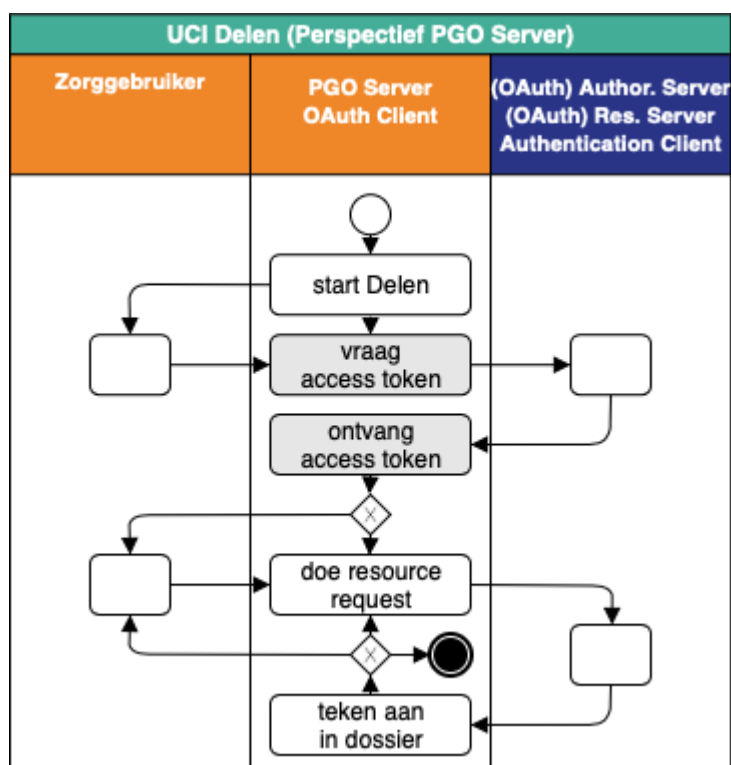
During the implementation of the test for the *Provider's* receptiveness for the health data to be shared, it makes sense to take privacy requirements into consideration. If the *Provider's Service Provider* is to build new data compilations for the receptiveness test then processing always takes place under the responsibility of a single *Provider*. The combining of processing or inadequate segregation must be avoided. This may only be deviated from under the explicit instruction of the *Provider(s)* and requires a careful weighing-up beforehand, due to the associated privacy risks.

## Specific perspectives

### Perspective of Publishing Server (happy flow)

#### Explanatory Notes

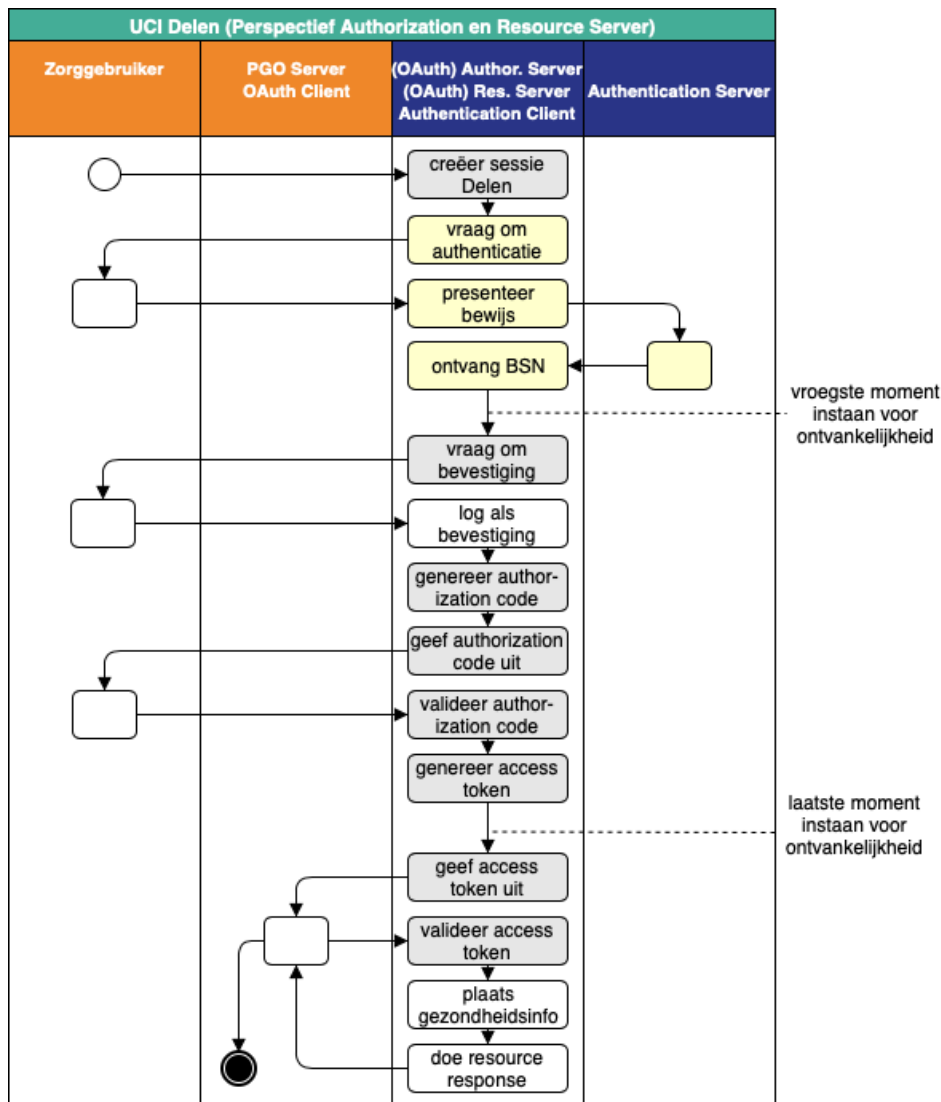
Please find below the same flow diagram but this time shown from the perspective of the *Publishing Server*. In other words, all in-between steps that are not visible to the *Publishing Server* are shorted. *User* is "hidden behind the browser" and *Authentication Server* "behind the *Authorization Server*".



### Perspective of Authorization Server/Resource Server (happy flow)

#### Explanatory Notes

Please find below the same flow diagram but this time shown from the perspective of the *Authorization/Resource Server*. In other words, all in-between steps that are not visible to the *Publishing Server* are shorted. *User* is "hidden behind the browser".

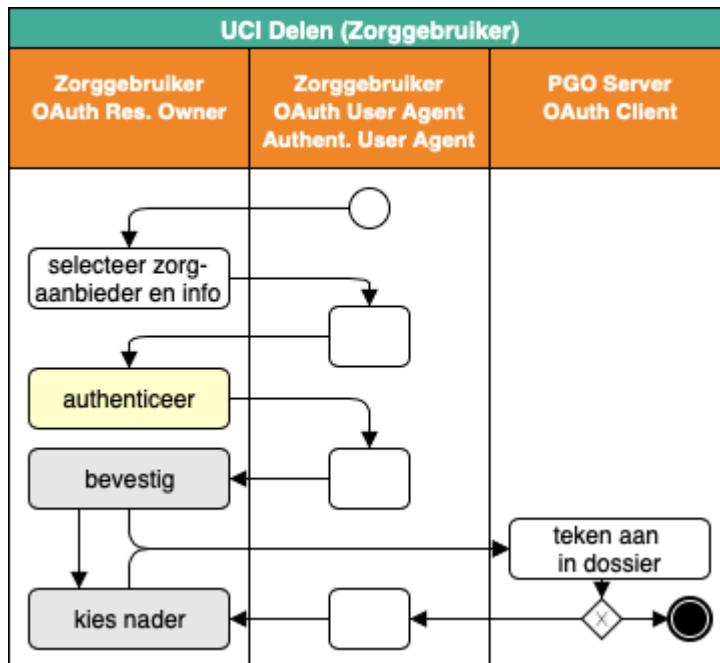


### Perspective of User (happy flow)

#### Explanatory Notes

Please find below the same flow diagram but this time shown from the perspective of the *User*. In other words, all in-between steps that are not visible to the *User* are shorted. Almost everything is "hidden behind the browser". We have only kept the final step of *Publishing Server* visible because the marking of the shared health information has meaning (i.e. significance) for the *User*. The *Publishing Server* will probably inform the *User* that the sharing was successful but is not obliged to do so.

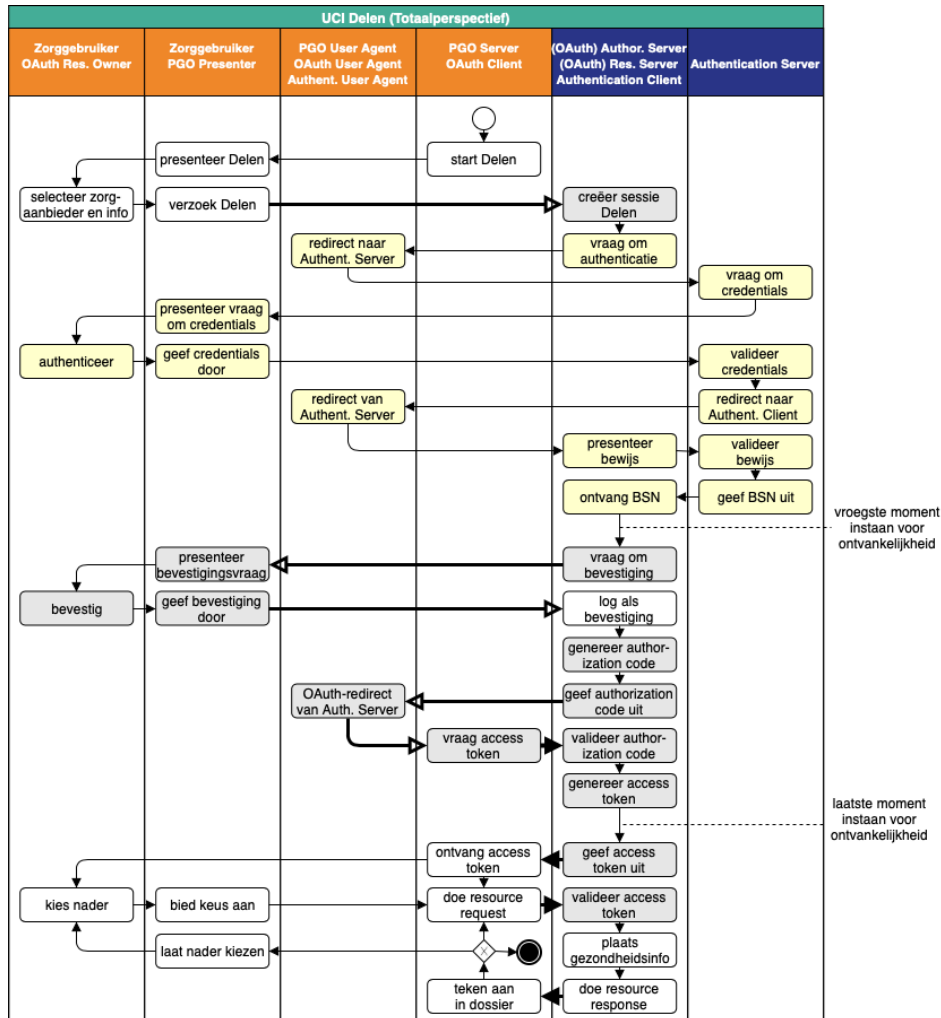




## Frontchannel and backchannel

### Explanatory Notes

In the flow diagram below for UCI Share, the thick arrows show the *MedMij data transfer* and include the five cases of frontchannel data transfer (open arrowhead) and four cases of backchannel data transfer (closed arrowhead).



## UCI Subscribe

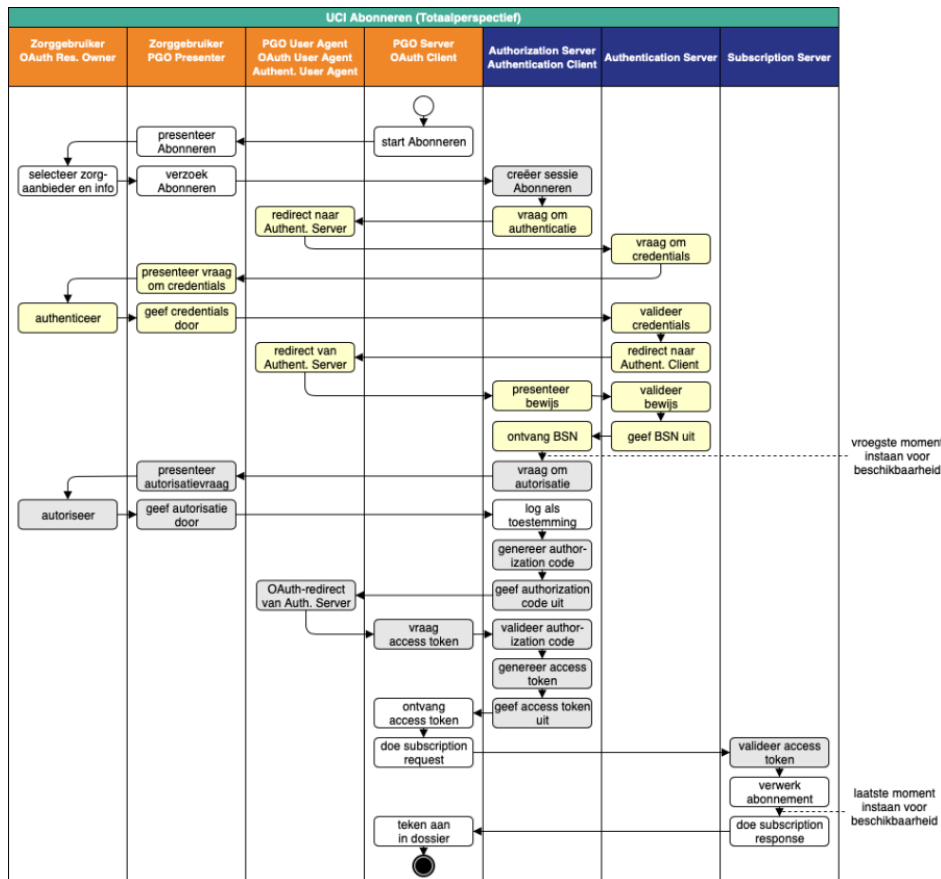
### UCI Subscribe | Explanatory Notes

The figures below show the flow diagram of the use case implementation UCI *Subscribe*, from four different perspectives:

- the overall perspective, with both the happy flow and the exceptions;
- the perspective of the *Publishing Server (= Client)*, who comes under the *Individual's Service Provider*. The last-named can read this figure as his mandatory participation in the use case implementation *Subscribe*;
- the perspective of the *Authorization Server/Subscription Server/Authentication Client*, who comes under the *Provider's Service Provider*. The last-named can read this figure as his mandatory participation in the use case implementation *Subscribe*;
- the perspective of the *User (= OAuth Resource Owner)*.

The flow diagrams only show the situation in which all actions are successful, up to and including the ultimate entering into of the *Subscription* (the so-called 'happy flow' situation). In line with the MedMij corporate identity, the orange paths belong to the *Individual's Domain* and the blue to the *Provider's Domain*. Various actions are coloured in the flow diagrams. Together, the actions coloured in light grey form the Authorization flow in accordance with OAuth, whereas the actions coloured in light yellow together form the authentication flow. In other words, these colours only refer to the standards used and say nothing about which component has to execute the step. Authentication is thus embedded in Authorization. In the flow diagrams for the specific perspectives, it is only those actions in the path that belong to that perspective that are named. The actions in the other paths are compressed and depicted without names.

Responsibilities with respect to exceptions to the happy flow are included in the respective interface, contrary to the [Processes & Information Layer](#), where use case are specified with the exceptions.



## UCI Subscribe

### UCI Subscribe

In each completion of the flow described in the diagram, there is in all cases only a single one of each of the roles named above.

The flow has the following steps:

1. The *Publishing Server* starts the flow by presenting in the *Presenter* of the *User* the possibility to *Subscribe* to *Notifications* for a certain *Information service* with a certain *Provider*. This always relates to precisely one single *Information service*. From the *Information service* directory, the *Publishing Server* knows which *Information services* a *Provider* offers *Subscriptions*. If desired, the *Information service* Names from the *Information service* glossary are used.
2. The *User* makes explicit his selection and gets the *OAuth User Agent* to send a subscribe request to the *Authorization Server*. The address of the authorization endpoint is taken from the *Isd*. The *redirect\_uri* indicates to where the *Authorization Server* must hereafter redirect the *OAuth User Agent* (with the Authorization code).
3. The *Authorization Server* now begins the OAuth flow (in his role as *OAuth Authorization Server*) by creating a session.
4. The *Authorization Server* (now in the role of *Authentication Client*) starts the authentication flow by redirecting the browser to the *Authentication Server*, providing a *redirect\_uri*, which indicates to where *Authentication Server* must later return the *OAuth User Agent*, after the *User* has logged in.
5. The *Authentication Server* asks the *User* for login details via the *Presenter*.

6. When these are correct then *Authentication Server* redirects the *OAuth User Agent* back to the *Authorization Server*, whilst giving him a retrieval certificate
7. With this retrieval certificate, the *Authorization Server* retrieves the BSN (citizen service number) directly from *Authentication Server*.
8. The earliest moment then comes when the *Authorization Server* guarantees that the *Provider* - for the relevant *Information service* - has any health information of this *Individual* available at all; otherwise, the happy flow terminates. One important factor here is that the *Individual* must be at least 16 years old for this.
9. If this is successful then the *Authorization Server* presents - via the *Presenter* to *User* the question of whether the last-named permits him to send the requested personal health information (*Notifications*) to the *Publishing Server* (as *Client*). Under the flow diagram it is specified which information, and from where, is processed by the *OAuth Authorization Server* in the *Declaration of consent Subscribe* to be submitted to the *User*.
10. Upon agreement, the *Authorization Server* logs this as consent, generates an Authorization code and sends this as a retrieval certificate, by means of a browser redirect, along with the *redirect\_uri* received in step 1, to the *Publishing Server*. The *Authorization Server* sends with it the local state information that it received in the initial step of the *Publishing Server*. The last-named recognises in it the request that it must associate the Authorization code with.
11. The *Publishing Server* not only interprets this Authorization code as a retrieval certificate but also deduces from it that the consent has been given and logs the obtaining of the retrieval certificate.
12. The *Publishing Server* applies again to the *Authorization Server* with this retrieval certificate but now without the intermediation of the *OAuth User Agent* for an access token.
13. The *Authorization Server* now generates an access token and sends it to the *Publishing Server*.
14. The *Publishing Server* is now ready to send the request for the establishment of the *Subscription* to the *Subscription Server*. It obtains the address of the subscription endpoint from the *Isd*. It places the access token in the message and ensures that no BSN is included in the message.
15. The *Subscription Server* checks that the token received grants entitlement to the requested *Subscription*. The final moment then comes at which the *Subscription Server* must guarantee that the *Provider* has the health data available for the relevant *Information service*. If this information is available then the *Subscription Server* sends it in a subscription response to the *Publishing Server*. If it isn't, the *Subscription Server* terminates the happy flow,
16. and saves the established *Subscription* to the *Personal Record*.

Generally, the Authorization interface, the token interface, and the resource interface are all addressed, in that order, in the case of one-off use of *UCI Subscribe*. If the *Publishing Server*, however, still has an access token that has not expired yet for the *Provider Information service Interface version* combination in question, it can immediately address the subscription interface.

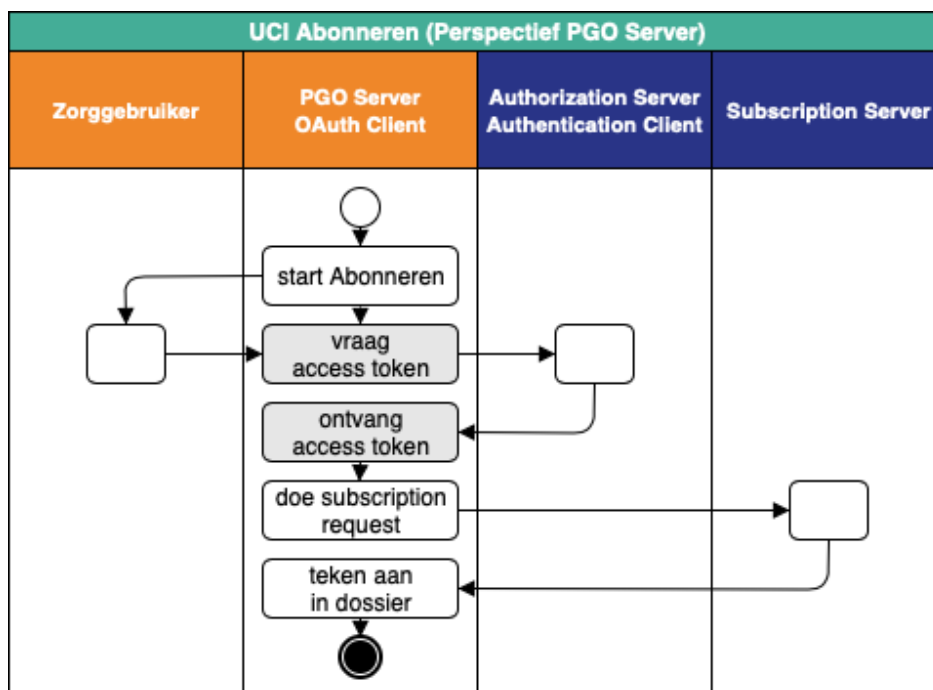
The MedMij Trust Scheme recommends that the availability condition be made effective from the earliest stated moment. For the time being, the MedMij Trust Scheme permits this condition to become effective later on but not later than the final moment stated in the figure.

When implementing the condition of availability at the *Provider* for the health data to be compiled, it makes sense to take privacy requirements into consideration. If the *Provider's Service Provider* were to create new data compilations for the availability condition then processing always takes place under the responsibility of a single *Provider*. The combining of processing or inadequate segregation must be avoided. This can only be deviated from under the explicit instruction of the *Provider(s)* and require a careful weighing-up beforehand, due to the associated privacy risks.

## Perspective of the Publishing Server

### Perspective of the Publishing Server

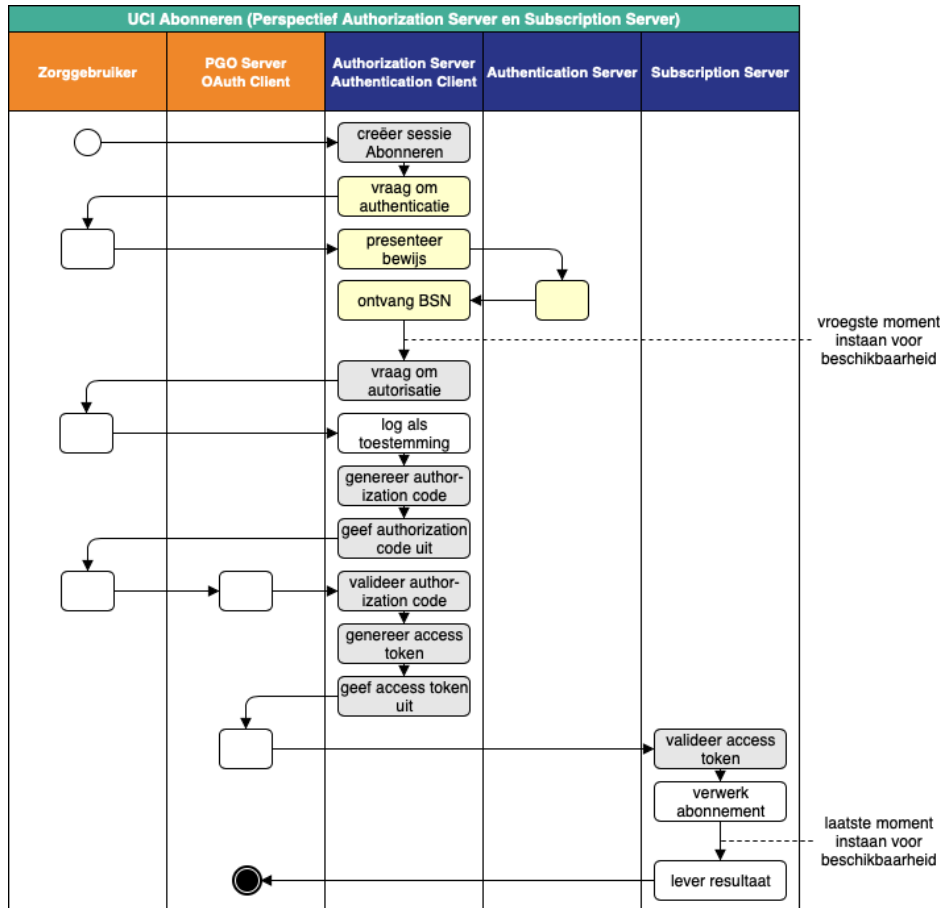
The *Publishing Server* launches the *UC Subscribe*. Through a redirect, it receives an Authorization code, with which it requests an access token on the token interface. After receiving the access token, it addresses the Subscription Server to have the start, change, or termination of the *Subscription* established.



### Perspective of the *Authorization Server*, *Authentication Server* and *Subscription Server*

#### Perspective of the Authorization and the Subscription Server

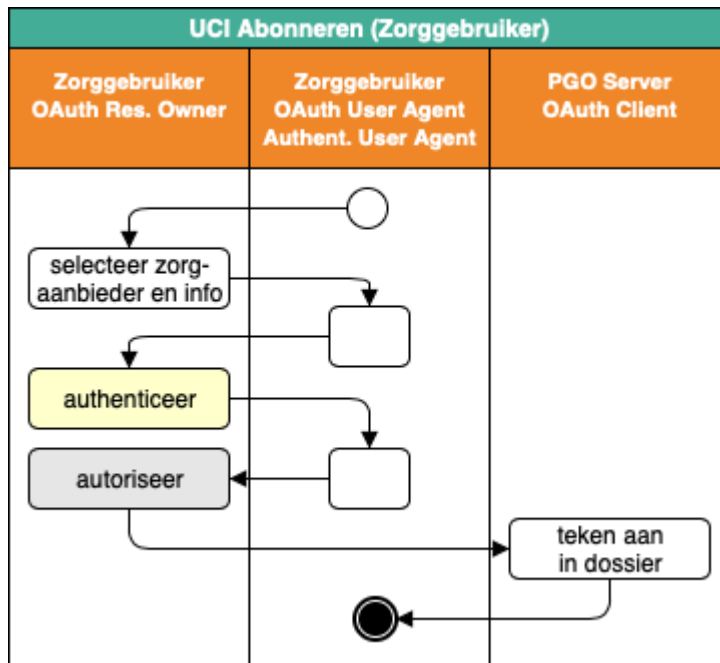
The *Authorization Server* creates, at the request of the *User*, a session for *UC Subscribe* and goes through the usual authentication and Authorization steps. Through a redirect, it receives an Authorization code, with which it requests an access token on the token interface. After receiving the access token, it addresses the Subscription Server to have the start, change, or termination of the *Subscription* established.



## Perspective of the *User*

### Perspective of the Authorization and the Subscription Server

The *User* selects the *Provider* and the *Information service* to which he wishes to subscribe or subscribe again, authenticates himself and gives Consent. After that, the Publishing Server records the subscription change (which it has had established by the *Subscription Server*) in the *Personal Record*.

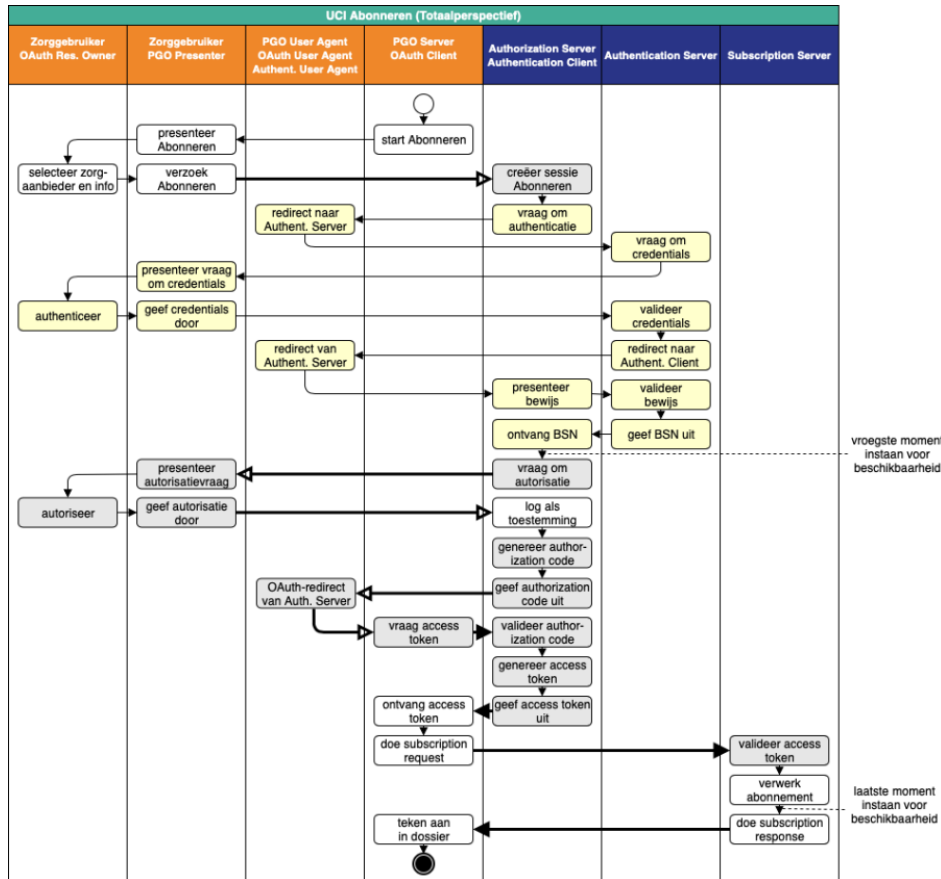


## Frontchannel and backchannel

### Frontchannel and backchannel

In the flow diagram below for *UCI Subscribe*, the thick arrows show the *MedMij data transfer* and include the five cases of frontchannel data transfer (open arrowhead) and four cases of backchannel data transfer (closed arrowhead).





## UCI Notify

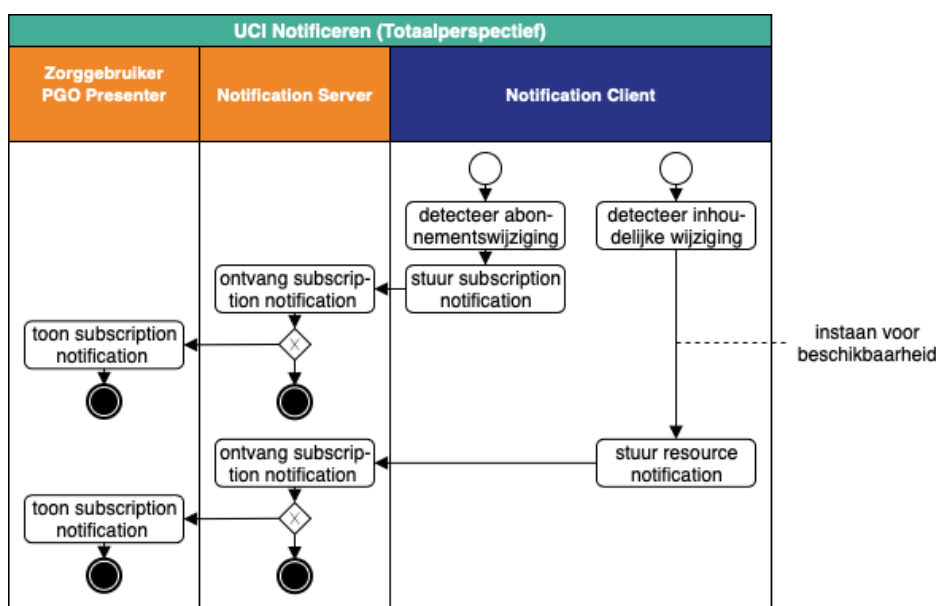
### UCI Notfiy | Explanatory Notes

The figures below show the flow diagram of the use case implementation *UCI Notify*, from four different perspectives:

- the overall perspective, with both the happy flow and the exceptions;
- the perspective of the *Notification Server* who comes under the *Individual's Service Provider*. The last-named can read this figure as his mandatory participation in the use case implementation *Subscribe*;
- the perspective of the *Notification Client*, who comes under the *Provider's Service Provider*. The last-named can read this figure as his mandatory participation in the use case implementation *Subscribe*;
- the perspective of the *User* (= *OAuth Resource Owner*).

The flow diagrams only show the situation in which all actions are successful, up to and including the ultimate entering into of the *Subscription* (the so-called 'happy flow' situation). In line with the MedMij corporate identity, the orange paths belong to the *Individual's Domain* and the blue to the *Provider's Domain*. Various actions are coloured in the flow diagrams. Together, the actions coloured in light grey form the Authorization flow in accordance with OAuth, whereas the actions coloured in light yellow together form the authentication flow. In other words, these colours only refer to the standards used and say nothing about which component has to execute the step. Authentication is thus embedded in Authorization. In the flow diagrams for the specific perspectives, it is only those actions in the path that belong to that perspective that are named. The actions in the other paths are compressed and depicted without names.

Responsibilities with respect to exceptions to the happy flow are included in the respective interface, contrary to the [Processes & Information Layer](#), where use case are specified with the exceptions.



### UCI Notify | Explanatory Notes

In all cases, each completion of the flow described in the diagram only has a single one of each of the roles named at the top.

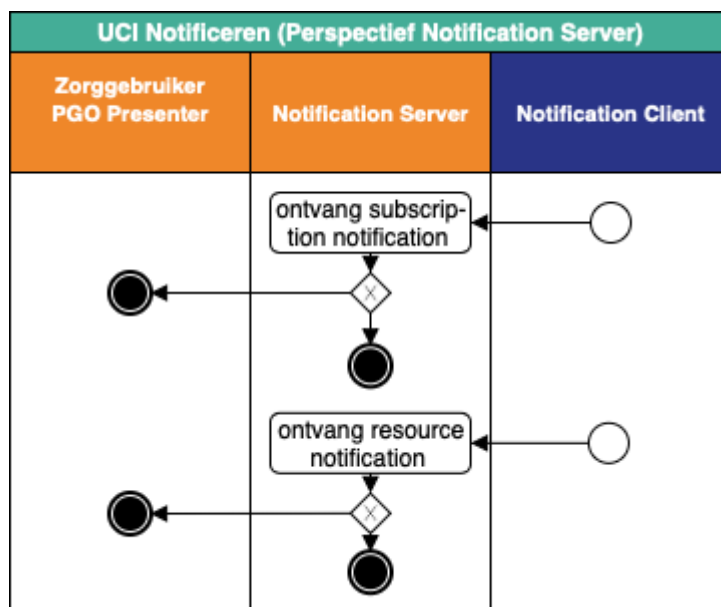
The flow has the following steps:

1. The *Notification Client* detects a change to the content of the health information for which the *User* has entered into a valid *Subscription*, or the *Notification Client* detects that the *Provider* terminates a certain subscription.
2. In both cases, the *Notification Client* determines based on the *client\_id* that was used in entering into the *Subscription*, in the *Client directory* the correct *Resource Notification Endpoint*, or *Subscription Notification Endpoint*.
3. The *Notification Client* sends subscription notification or resource notification to the *Notification Server*.
4. The *Notification Server* checks the *Notification*, possibly shows it to the *User* and sends a response to the *Notification Client*.

### Perspective of the *Notification Server*

#### Notification Server

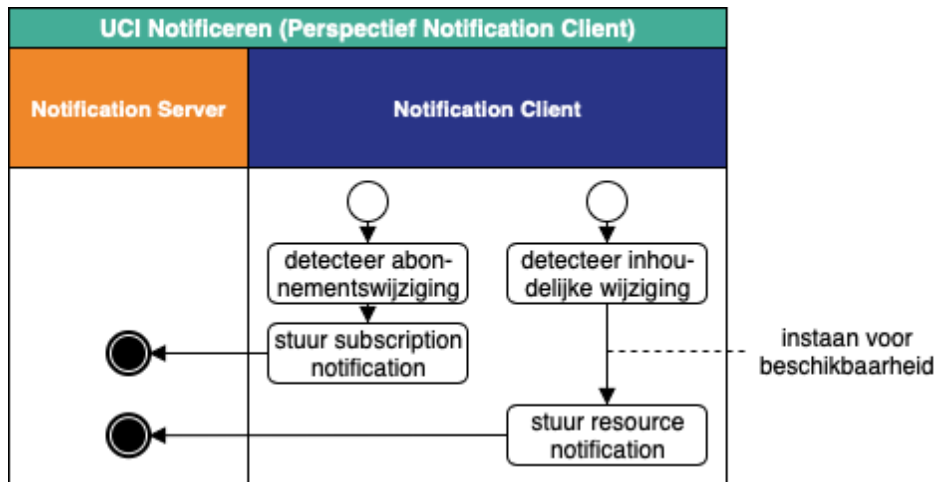
The *Notification Server* receives a subscription notification or a resource notification and possibly forwards it to the *User (Presenter)*.



### Perspective of the *Notification Client*

#### Notification Client

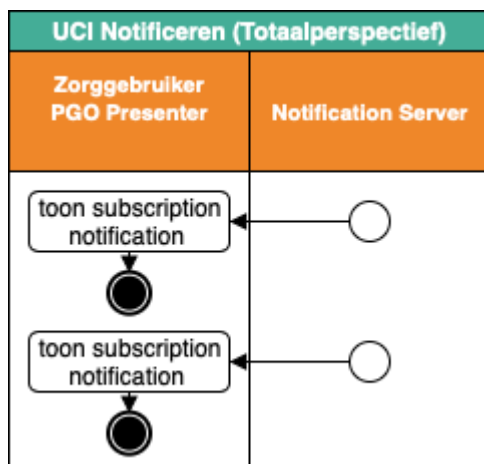
The *Notification Client* detects a change to the content or a change to the subscription and sends a resource notification or subscription notification respectively to the *Notification Server*.



### Perspective of the User

#### User

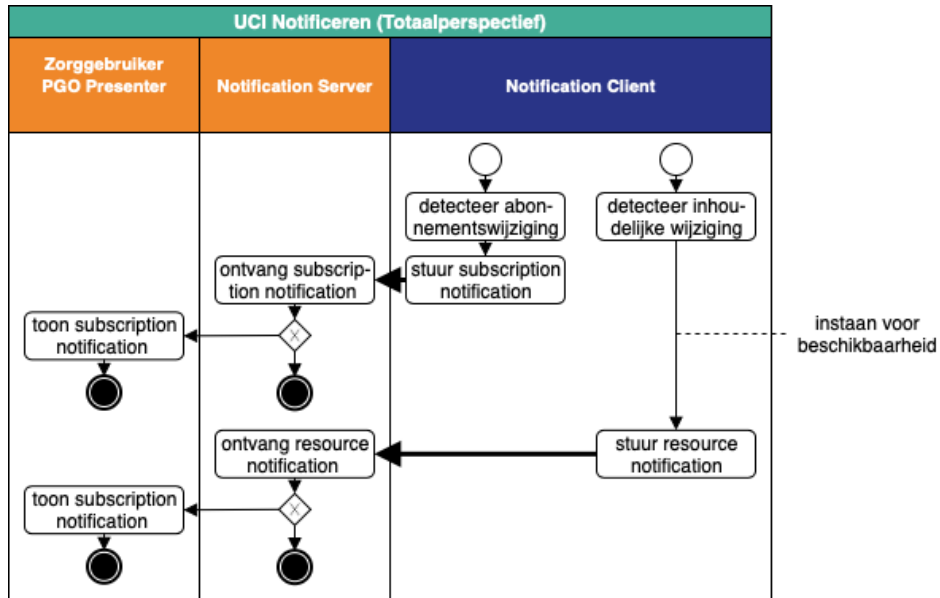
The *Presenter* shows a subscription notification or a resource notification.



### Frontchannel and backchannel

#### Frontchannel and backchannel

Both kinds of *Notifications* are backchannel data transfers.



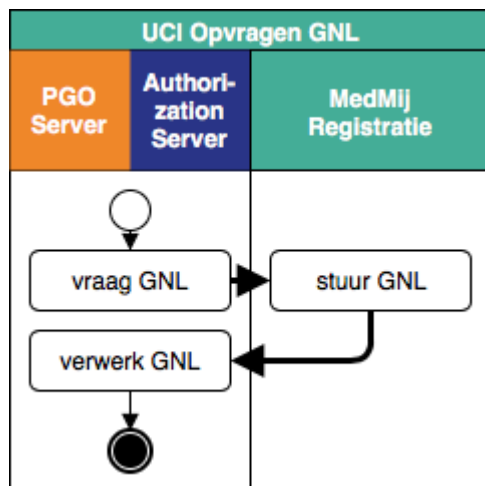
## UCI Retrieve Isg

### Flow diagram

#### Explanatory Notes

In each completion of the flow described in the diagram, there is in all cases only a single one of each of the roles named above. In the left-hand path, this means a single *Publishing Server* or a single *Authorization Server*.

Both interactions with *MedMij Registration* are backchannel data transfers.



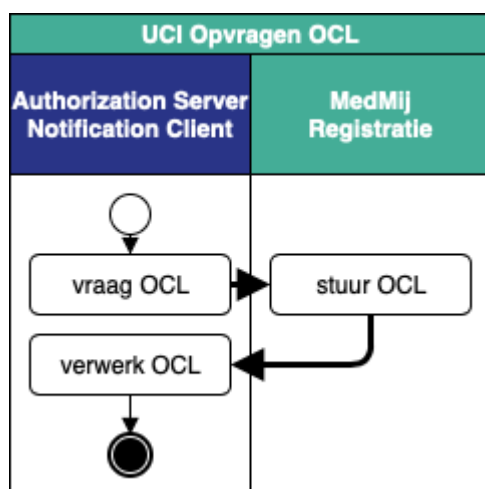
## UCI Retrieve Rcd

### Flow diagram

#### Explanatory Notes

In each completion of the flow described in the diagram, there is in all cases only a single one of each of the roles named above.

Both interactions with *MedMij Registration* are backchannel data transfers.



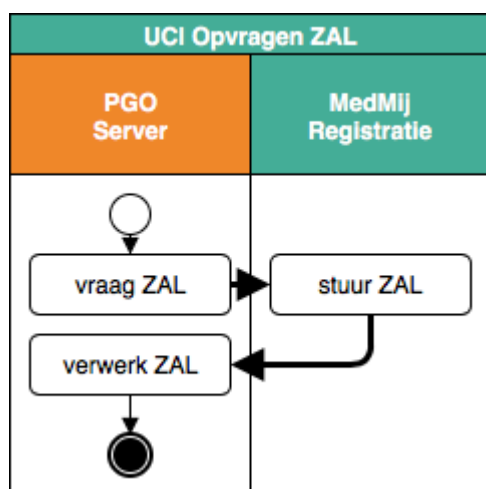
## UCI Retrieve Isd

### Flow diagram

#### Explanatory Notes

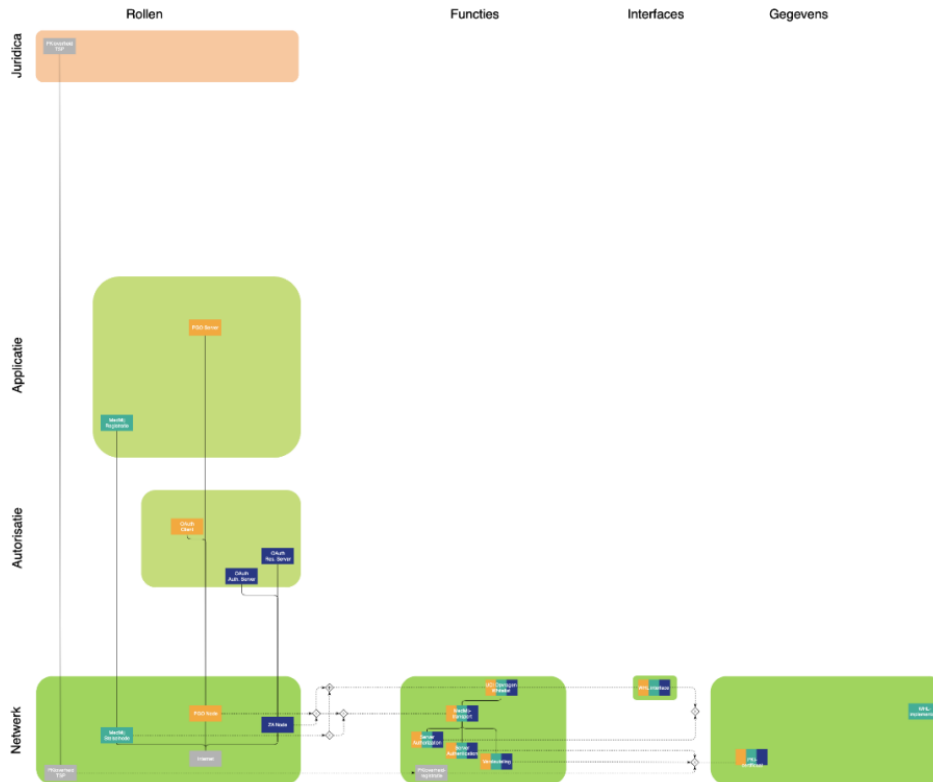
In each completion of the flow described in the diagram, there is in all cases only a single one of each of the roles named above.

Both interactions with *MedMij Registration* are backchannel data transfers.





## Infrastructure



### Introduction

In this layer, the infrastructure roles (*Nodes*) on the MedMij Network are determined and provided with responsibilities in the areas of encryption, authentication of *Nodes* and Authorization of *Nodes*. This last point refers to the fact that it must in each case be established anew that a *Node* is entitled to be on the MedMij Network. PKI certificates are used for encryption and authentication.

Basically, Authorization can be included in the MedMij Trust Scheme in two ways:

- via these same PKI certificates, in which it can be seen from the certificate holder's domain name whether it relates to a *MedMij Node*, by demanding of it that this domain name has the form <service provider>.medmij.nl;
- or via a list of authorised *MedMij Nodes* (a whitelist) that MedMij manages itself.

The advantages of the first option would be that:

- in this way, maximum use would be made of arrangements that are already necessary for other purposes too, namely for the use of PKI certificates;
- in this way, the degree of operational central involvement on the part of Stichting MedMij is minimised, as are accordingly the associated costs and risks. In the second option, Stichting MedMij would itself have to start managing a list and disclosing it to all servers in order to make the operational data transfer possible. In the first option, only a name service is needed for the [medmij.nl](https://medmij.nl) domain names. This last service is a well-standardised, well understood and easily outsourced service, that would result in lower costs, reduced risks and less dependency for the participants;

- in this way, MedMij will comply as far as possible with its [architectural principle \[NL\]](#) P6: MedMij only arranges what is necessary.

Despite this, the second option was chosen, because the check on the hostnames and the certificates needed for the first option would only result in undesirable side effects. The following options were explored in this regard:

- The MedMij Maintenance organisation becomes **Registration Authority (RA)** in PKIoverheid, in respect of all relevant Certificate Authorities (CAs). However, PKIoverheid does not have this option.
- The MedMij Maintenance organisation issues a **domain declaration** so that participants can themselves request a subdomain under [.medmij.nl](#) from a CA. In this way, the maintenance organisation can indeed influence the issuing of a certificate but it is not possible to revoke it later unless there has been a misuse. After all, there is no legal relationship between the owner of the domain (the maintenance organisation) and the CA.
- In a similar way to the way in which some parties issue professional certificates, a **customised certification service** is conceivable. The product terms and conditions (valid from the date of the certificate application) then explicitly stipulate that if the registration in an external register is cancelled, the certificate will be revoked by the CA. This requires the register holder (the maintenance organisation) to pass on changes to all CAs. This does not become cost-attractive until there are a considerable number of certificate holders, which there will not be in MedMij for the time being.
- MedMij could set up its **own PKI environment** (different from PKIOverheid). This option was not explored further, due to the complexity and responsibility that would rest on the shoulders of the maintenance organisation.
- The Stichting MedMij could itself be a **holder** of all certificates, whereby participants are mandated for maintenance tasks relating to their own subset of certificates. The Foundation can revoke certificates. Identification of the service provider to the user is not possible, because the certificates are in the name of Stichting MedMij.
- A **custom field** could be used in certificates. The MedMij Maintenance Organisation could be allowed to control the way in which this field is dealt with. This probably requires arrangements to be made with all CAs. This gives you control over the issuing of certificates but does not give the maintenance organisation any options for having the certificate revoked.

The table below summarises how the security functions security, authentication and Authorization are organised in the responsibilities in this layer. With Authorization, the distinction drawn between incoming and outgoing data transfer is made because in these two cases, the identification of the other *Node* takes place differently.

	frontchannel data transfer	outgoing backchannel data transfer	incomingbackchannel data transfer	
<i>encryption</i> according to TLS, with PKIoverheid certificate	always			
<i>identification</i> on the basis of ...	redirect_uri or <i>Information service directory</i>		PKIoverheidcertificate	
<i>authentication</i> , on the basis of PKIoverheid certificate, of ...	only the TLS server	TLS client <u>and</u> TLS server		

Authorization on the basis of checks against the <i>Whitelist</i>	no	prior to the TLS handshake	seeresponsibility 14a
---	----	----------------------------	-----------------------

## Roles

### 1. Functionality in the *MedMij Network*:

- each *Publishing Server*, including its *OAuth* role, functions on one or more *Publisher's Nodes*. In the case of frontchannel data transfer, each *Publishing Server* uses a single *Publisher's Node*, namely one with a hostname that is stated for this *Publishing Server* on the *Client directory*.
- each *Authorization Server*, including its *OAuth* role, functions on one or more *Issuer-Addressee Nodes*;
- each *Subscription Server*, including its *OAuth* role, functions on one or more *Issuer-Addressee Nodes*;
- each *Notification Client* functions on one or more *Issuer-Addressee Nodes*;
- each *Resource Server*, including his *OAuth* role, functions on one or more *Issuer-Addressee Nodes*;
- precisely one *MedMij Coordination Node* functions, on which *MedMij Registration* functions.

#### Explanatory Notes

##### Explanatory Notes

With regard to the basic principles of the numerical relationships between the roles, see the page on [Architecture and technical specifications](#).

The exception to this regarding the frontchannel data transfer is necessary so that the *Client directory* can function. In other words, it is possible for a *Publishing Server* to deploy different certificates for frontchannel and backchannel data transfers, as long as the *Client directory* contains the same hostname in the certificate for frontchannel data transfer that is stated in the redirect URI regarding *OAuth*.

There is precisely one *MedMij Coordination Node* in the *MedMij Network*. Without this *MedMij Coordination Node* there is no *MedMij Network*.

In line with choices made in the [Process and Information Layer](#), in the Provider's domain only the *Issuer-Addressee Nodes* occur in the *MedMij Network*. This means that for instance the underlying xISs will not use the *MedMij Network* to communicate with the *Issuer-Addressee Node*. This data transfer is hidden behind the *Issuer-Addressee Node*. All routing needed for this is processed by the server implementations and takes place without the *MedMij Trust Scheme* seeing it.

### 2. On a single:

- *Publisher's Node* either a single *Publishing Server*, a single *Notification Server* or the combination of a single *Publishing Server* and a single *Notification Server* functions.
- *Issuer-Addressee Node* either a single *Authorization Server*, a single *Resource Server*, a single *Subscription Server*, a single *Notification Client*, or a combination of the aforementioned roles functions.

#### Explanatory Notes

##### Explanatory Notes

For details of the general principles regarding the numerical relationships between the roles, see the

page [Architecture and technical specifications](#).  
3. One or more *PKI TSPs* act as *PKI TSP*.

## Responsibilities

### TLS and certificates

1a. All the data transfer across the *MedMij Network* is protected with [Transport Layer Security](#) (TLS).

1b. Only TLS versions and TLS algorithms are used that are classified as "good" in the [ICT security guidelines for Transport Layer Security \(TLS\), version 2.0](#) issued by the NCSC. A *Node* only offers TLS 1.3 if it also offers TLS 1.2.

#### Algorithms

It is not mandatory to offer *all* algorithms that have been classified as "good" in the aforementioned guidelines.

1c. The use of [TLS False Start](#) is prohibited.

#### Explanatory Notes

Usage of [TLS False Start](#) is prohibited, in order to prevent content-related processing of exchanged data taking place before authentication and Authorization have been successful for the exchange in question (see below).

2. In order to be able to authenticate and authorise themselves on the *MedMij Network*, each *Publisher's Node*, each *Issuer-Addressee Node* and the *MedMij Coordination Node* can submit a PKI-overheid certificate, namely a server certificate from a *PKI TSP*.

3. All certificate holders undertake to comply with the requirements from the PKI-overheid system that apply to them. A single organisation may have multiple certificates.

#### Explanatory Notes

The decision to opt for the [PKI](#) standard fits in with principle P19 of the MedMij Trust Scheme. There are other ways to ensuring trust in an infrastructure of automated systems but these are by no means as tried-and-trusted as PKI, which is supported and tested worldwide by governments and market players.

Using the PKI standard raises the issue of which PKI system(s) can or must be used. Such a PKI system provides for a hierarchy of organisations that issue certificates, such that the trustworthiness of the certificates of such an organisation rests on the trustworthiness of the organisation directly above it in this hierarchy, because the certificates of the lower-in-hierarchy have been signed by those of the higher-in-hierarchy. At the top of such a hierarchy there is what is known as the root Certificate Authority (root CA) which cannot derive its trustworthiness from a higher authority and signs its own (master and other) certificates and in this way is a mainstay of the trust placed in the entire relevant PKI system.

The MedMij Trust Scheme could have opted to set up a PKI system specifically for MedMij but the cost of doing so, both for itself and for its participants, do not provide sufficient benefits when it is the

case that another suitable PKI system is available. After all, participants and their services could become involved in trust schemes other than those of MedMij. In addition, such a choice does not fit in with [principle \[NL\] P6](#).

Because the MedMij Network is a critical infrastructure from both a national and social point of view, with strict requirements set for its trustworthiness, the MedMij Trust Scheme opts for the only PKI system currently available whose trustworthiness is ultimately founded on a single Dutch public-law legal entity, namely [PKIoverheid](#) with the State of the Netherlands as root CA. In this way, the governance of the root CA is transparent and accessibly allocated.

In other words, when it comes to the trust that the MedMij Trust Scheme provides its participants with, this is based in part on the PKIoverheid system, on the [schedule of requirements](#) adopted by that system for the TSPs involved in that system, and on the [certification hierarchy](#) of PKIoverheid. Participants in the MedMij Trust Scheme must accordingly obtain service certificates from a [TSP that is affiliated with](#) PKIoverheid that (i.e. the TSP) is right for that participant.

### Function: *Encryption*

4. On the *MedMij Network*, all the data transfer is encrypted in line with TLS, as referred to in responsibility 1.

### Function: *Server Authentication*

5. During the TLS handshake referred to in responsibility 1, the TLS server does the following to the TLS client in the server hello step:

- in the case of backchannel data transfer, the TLS server always submits a request for a certificate. If the TLS client does not hand over a certificate in response then the handshake is immediately terminated.
- in the case of frontchannel data transfer, the TLS server will never submit a request for a certificate.

### Explanatory Notes

In the case of backchannel data transfer, therefore, two-way authentication takes place; with frontchannel data transfer, one-way authentication.

6a. *Issuer-Addressee Node, Publisher's Node and MedMij Coordination Node* validate during the TLS handshake at the beginning of a TLS session whether it is a PKIoverheid certificate and check, with the *Certification Authority* on the basis of [CRL](#) of [OCSP](#), whether the received certificate is valid. If any one of these checks fails, the certificate will not be accepted and the TLS session will not be started.

6b. If the [OCSP](#) is used in the context of responsibility 6a, the OCSP response may be stapled to the certificate ([OCSP Stapling](#)).

### Certificate revocation

The stapling of an OCSP response to the certificate is permitted in the MedMij Trust Scheme. The recipient may use this OCSP response but the check on whether the certificate has been revoked may also be performed in another way. When the choice is made to only perform the check via OCSP, it is possible that an OCSP responder will not give a response or it will not give this in time. In that case, it is possible to choose to start the TLS session (soft fail). The primary mechanism within the MedMij Trust Scheme for determining whether nodes may access each other is the *Whitelist* check. For all of the requirements related to PKIoverheid certificates, see <https://www.logius.nl/diensten/pkioverheid/aansluiten-als-tsp/pogramma-van-eisen>.

6c. With due observance of responsibility 6a, *Issuer-Addressee Node*, *Publisher's Node* and *MedMij Coordination Node* accept both G2 and G3 certificates from each other by:

- trusting the root certificates State of the Netherlands Root CA - G2 and State of the Netherlands Root CA - G3, as published on <https://cert.pkioverheid.nl>;
- recognising and trusting all *PKI TSP certificates* and domain certificates under the respective G2 and G3 hierarchies, in so far as they, according to <https://cert.pkioverheid.nl>:
  - come under the G3 Domain Organisation Services and are of the type Server or else
  - come under the G2 Domain Organisation;
  - have not been revoked.
- processing and using - within 10 working days - changes that apply to G2 and G3 that are set out on <https://cert.pkioverheid.nl>.

### Explanatory Notes

*PKI TSPs* issue certificates under various root certificates of the State of the Netherlands, namely an old one (G2) and a new one (G3). The classification of certificate types (domains) differs between G2 and G3. The validity of G2 certificates ends on 22 March 2020 at the latest. Although no more G2 certificates with a validity of three years can accordingly be issued, it has to be possible for the time being to use older G2 certificates for MedMij purposes. In other words, where PKloverheid certificates have to be accepted, it has to be possible for them to be G2 or G3 certificates. The MedMij Trust Scheme has no reason to impose additional restrictions on the way in which PKloverheid makes the transition from G2 to G3.

Responsibility 6c corresponds to requirements relating to the [eRecognition Trust Scheme](#), with the proviso that EV certificates do not have to be accepted in the MedMij Trust Scheme. The more comprehensive validation of certificate holders that is deployed for EV certificates is envisaged in the acceptance process for participants in the MedMij Trust Scheme.

Since stapling of OCSP responses is permitted, each *Node* which will have to check a certificate must support stapling to the extent that only the fact that a stapled OCSP response is used should not give rise to an error message or the otherwise sudden termination of the TLS handshake or session.

## Function: *Server Authorization*

### Distribution of the *Whitelist*

7. The *MedMij Coordination Node* provides *Publisher's Node* and *Issuer-Addressee Node* with a use case implementation (*UCI Retrieve Whl*) to request the current version of the *Whl implementation*. The roles involved use the relevant [flow diagram](#) for this.

### Explanatory Notes

The *Whl implementation* is the implementation of the *Whitelist* in XML.

8. The participation of the *MedMij Coordination Node* in *UCI Retrieve Whl* is available at least 99.9% of the time. *MedMij Registration* allows - once the participation of *MedMij Coordination Node* in the use case becomes unavailable - a maximum of eight hours (480 minutes) to elapse before it is available again.

9. *Publisher's Nodes* and *Issuer-Addressee Nodes* obtain the most recent *Whl implementation* from *MedMij Coordination Node* at least every fifteen minutes (900 seconds).

10. The *MedMij Coordination Node* has `stelselnode.medmij.nl` as its hostname. The *MedMij Coordination Node* is not on the *Whl implementation*; however, for the check made against the *Whitelist implementation* it is considered to be on it all the same.

#### Explanatory Notes

By authorising the *MedMij Coordination Node* in this way for MedMij data transfer, it is ensured that even in error situations or bootstrap situations a *Publisher's Node* or *Issuer-Addressee Node* can address the *MedMij Coordination Node* in order to retrieve a *Whl implementation*.

11. *Publisher's Nodes* and *Issuer-Addressee Nodes* validate each newly obtained *Whitelist* against the *Whitelist's* XML schema description. This XML schema description is a technical implementation of the *MedMij metamodel*. All hostnames on the *Whitelist* are fully-qualified domain names, in accordance with RFC3696, section 2.

12. For the purpose of technical security of the data transfer that takes place in relation to *UCI Retrieve Whl*, the roles involved make use of *Encryption*, *Server Authentication* and *Server Authorization*, in line with the provisions in this *Infrastructure* Layer.

#### Using the *Whitelist*

13. *Issuer-Addressee Node*, *Publisher's Node* and *MedMij Coordination Node* allow backchannel data transfer to pass through the *MedMij Network* when and only when they have established that the hostname of the other *Node* is present on the most recent *Whitelist*.

#### Explanatory Notes

In the case of frontchannel data transfer, no *Server Authorization* takes place.

14a. The *Node* that

- is to become the TLS client carries out the check referred to in responsibility 13 against the *Whitelist* prior to the start of the TLS handshake. If this check cannot be carried out or else delivers a negative result then the TLS handshake is not started.
- is the TLS server, carries out in its entirety the check referred to in responsibility 13 against the *Whitelist* prior to any subsequent step being taken by the *OAuth Authorization Server* or *OAuth Resource Server* according to the specifications of *UCI Collect*, *UCI Share*, *UCI Subscribe* and *UCI Notify*. This requirement is called a 'sequence'. If the check against the *Whitelist* cannot be carried out or else delivers a negative result then the process is terminated immediately and no start is made to the execution of this next step. In this case, the check against the *Whitelist* is successful if and only if at least one of the following names appears on the *Whitelist* that (i.e. the name) is taken from the certificate provided by the TLS client, namely the Common Name or one of any Subject Alternative Names that there are.

14b. In so far as the *Provider's Service Provider* opts to carry out the check against the *Whitelist* after the TLS handshake has ended then this check is separated logically from the next step referred to. The required sequence can be shown using code inspections, penetration tests and inspections of logs.

#### Explanatory Notes



In the case of outgoing data transfer, the TLS client envisaged can already carry out the check against the *Whitelist* before they initiate the TLS handshake because they have already identified the envisaged TLS server in order to know who they have to address at all. However, in the case of incoming data transfer, the TLS server cannot identify the TLS client that presents himself until during or after the TLS handshake, doing so by means of the certificate that they must receive in accordance with responsibility 2. A hostname must then occur that can be found in the *Whitelist*. By permitting names other than the Common Name to contain the hostname authorised by MedMij, such as a Subject Alternative Name, the MedMij Trust Scheme gives participants the option to re-use certificates for multiple MedMij nodes or for purposes other than participation in MedMij. The earliest - and at first sight the most secure - moment to carry out the check against the *Whitelist* is in that case during the TLS handshake, between the receipt of the certificate from the TLS client and the envisaged sending of the Finished message. If this check cannot be carried out or else delivers a negative result then instead of the Finished message the exception `access_denied` is sent. Although section 7.2.2 of the [TLS specification](#) provides for this possibility, many standard implementations do not. It is sometimes possible to modify these standard implementations but doing so may create new security risks, due for example to the complexity of managing customised modifications to standard implementations.

This is why the MedMij Trust Scheme wants to offer more leeway regarding implementation, without however accepting the risk that content-related information from a TLS client will start being processed that originates from a TLS client before the check against the *Whitelist* has ensured that this TLS client was authorised for MedMij data transfer. Because there are multiple ways to implement this even after the TLS handshake has ended, the MedMij Trust Scheme does not require any fixed architectural variant (such as with a reverse proxy) for this but does set the requirement regarding sequence, in addition to that of having a logical separation. It has to be possible to show this by means of code inspection, penetration tests and inspections of logs.

15. If a *Whitelist* check, in the context of responsibility 14, cannot be performed, or if it produces a negative result, this breaks the progress of the performance of the use case implementation and the respective Application roles do not inform each other of this.

#### Explanatory Notes

If the *Whitelist* check is unsuccessful then this indicates an untrustworthy counterparty, which is why the latter is not informed about this.

## Domain Name System

16. *Individual's Service Provider*, *Provider's Service Provider* and *MedMij Maintenance* in their role as DNS Server or its client are responsible for the signature of the name records belonging to the hostnames of *MedMij Nodes*, or the *MedMij Coordination Node* respectively, in accordance with DNSSEC.

17. The *MedMij Coordination Node* and each *MedMij Node*, in his role as DNS resolver in the Domain Name System, checks whether the name records received have been signed in accordance with DNSSEC and validates this in accordance with DNSSEC. Both this check and validation must be successful; if they are not then they decide not to connect with the relevant hostname.

#### Explanatory Notes

Explanatory Notes

Usage of DNSSEC ([RFC 4033](#), [RFC 4034](#), [RFC 4035](#)) reduces the vulnerability of the Domain Name System to [DNS spoofing](#), for example.



## Composition of the Client directory

18. For each *Publishing Server*, the *Client directory* only contains the *Publisher's Node* which the respective *Publishing Server* uses to handle the frontchannel data transfer.

### Information

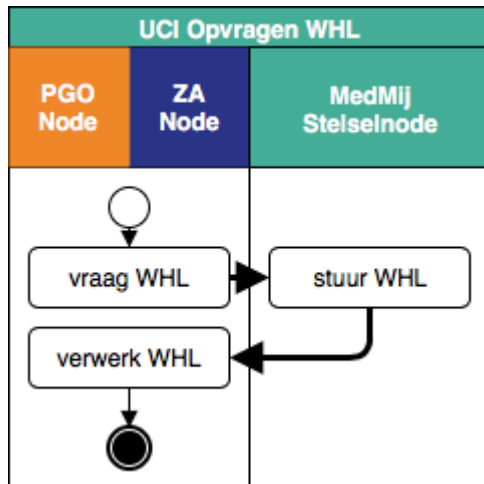
In accordance with the provisions under point 1 under Roles, a *Publishing Server* may use multiple *Publisher's Nodes*, but a *Publishing Server* may only use a single *Publisher's Node* for all of its frontchannel data transfer, in other words on the authorization interface. The content of the *Client directory* is only used on that authorization interface, for two purposes:

- taking note of the *Information Services* on which the *Publishing Server* has been acknowledged, so that the *Authorization Server* can refuse an authorization request if the *Publishing Server* has not been acknowledged on the *Information Service* for which it requests Authorization;
- taking note of the name of the *Individual's Service Provider* that should appear in the [Declaration of consent](#) and the [Declaration of confirmation](#).

That is why, for a *Publishing Server*, only that one *Publisher's Node* which uses this *Publishing Server* for its frontchannel data transfer has to be included in the *Client directory*. In order to not distribute any redundant data, any other *Publisher's Nodes* from the *Client directory* are excluded.

## Use Case Implementation Request Whl

### Flow diagram



#### Explanatory Notes

In all cases, each completion of the flow described in the diagram only involves a single one of each of the roles named at the top. In the left-hand path, this means: a single *Publisher's Node* or a single *Issuer-Addressee Node*.

Both interactions with the *MedMij Coordination Node* are backchannel data transfer.

## Whl Interface

1. *MedMij Coordination Node* is addressed in *UCI Retrieve Whl* with the hostname `stelselnode.medmij.nl`. The URI of the *Whitelist* is `https://stelselnode.medmij.nl/MedMij_Whitelist.xml?api=1.2.0`

### Versioning of list interfaces

The list interfaces have a version number from release 1.1.2 of the MedMij Trust Scheme. This makes it possible to have multiple versions of these interfaces in production at the same time. From version 1.1.2, the versions will be distinguished from each other by means of a query parameter in the URI.

The version number is identical to the number of the release in question. This means that subsequent versions of the list interfaces may be identical in content.

2. The participation of *MedMij Coordination Node* in *UCI Retrieve Whl* is available at least 99.9% of the time. If the participation referred to becomes unavailable then *MedMij Maintenance* will allow a maximum of eight hours (480 minutes) to elapse before it is available again.

3. In the event of such an incident, *MedMij Maintenance* informs *Publishers*, *Sources* and *Readers* that the incident has occurred and tells them the expected downtime. *MedMij Maintenance* informs the parties about scheduled maintenance that will lead to temporary unavailability.

4. If *MedMij Coordination Node* in *UCI Retrieve Whl* is unavailable then the relevant requesters may use the most recent copy of the relevant list in the cache for a maximum of 10 hours.

### Explanatory Notes

The *Whitelist* is not designed to block compromised nodes. In these cases, the relevant certificate must be revoked, the systems cleaned up and a new certificate installed. This is why - for the downtime referred to in this responsibility - the lagging behind of the content of the *Whitelist* is not a security risk.

## Information models

### Explanatory Notes

The pages under this page contain, on three abstraction levels, models of parts of the information that plays a role in the architecture of the MedMij Trust Scheme in the [primary function Coordination](#). It is the precise "language" of the primary function *Coordination*. The three abstraction levels differ in scope, style and structure, but all three of them contain the same components:

- a model diagram with the structure of the types of information involved;
- a list of invariants that impose additional requirements on the model's instances;
- a list of 'basic classes', in other words, classes whose structure is not elaborated on in the diagram but whose values are individually deemed to be meaningful.

The three abstraction levels are:

- the conceptual level with the [metamodel](#);
- the logical level with three [logical models](#);
- the technical level with four [XML schema descriptions](#) and a spreadsheet table diagram.

In this version of the MedMij Trust Scheme, the scope of all three of the levels is limited to the types of information that are important for the four lists to be published by the MedMij Maintenance organisation and for the *Information service catalogue*. The [metamodel](#) contains the relevant classes from the point of view of adaptability and expandability in the longer term. Within the limits of object-oriented thinking, which a large proportion of the target audience for these models will be familiar with, this is best achieved with the systematic application of association classes. This is explained in more detail on the [metamodel](#) page.

Between them, the [logical models](#) have the same scope but take a step towards the implementation of the list and the *Information service catalogue*. This is why they have a hierarchical set-up and thus are less adaptable and less expandable. In addition, there are three separate logical models:

- one for the four lists, which are published during the operation of the MedMij Network;
- one for the *Information service catalogue*, which is published with the Trust Scheme on [this page](#);
- one for the *MedMij Coordination Node*, which is published in the Trust Scheme itself, on [this page](#) (responsibility 3);
- one for the two types of *reports*, with which *Participants* have to report about their operation on the MedMij Network.

The [technical models](#) build on this and are also hierarchical but additionally opt for technology: XML and spreadsheet. On this level, there is a separate model (XML schema description) for each list and each report. For the *Information service catalogue*, the implementation technology is a table in a spreadsheet. There is no separate technical model for the *MedMij Coordination Node*.

Lower abstraction levels inherit the relevant information types, invariants and basic classes from higher ones. However, there can be changes to structure and name in this regard. These abstraction steps are explained in more detail on the relevant pages. In this way, the process from conceptual specification to technical implementation is made as verifiable and manageable as possible.

## Metamodel\_

### Explanatory Notes

The metamodel organises key concepts from the MedMij Trust Scheme. It is a conceptual data model, in the form of a UML class diagram. The metamodel focuses on providing a coherent description of concepts and relationships, which among other things are used in MedMij's [primary function Coordination](#). The metamodel is first and foremost the basis for the structure of:

- the *Information service directory*, from which the *Client* can see which *Providers* currently offer which *Information Services* and with which it can use, given a certain *Interface version*, to find the relevant technical addresses (URIs) of the *OAuth Authorization Server* (two Endpoints: the *Authorization Endpoint* and the *Token Endpoint*) and the *OAuth Resource Server* (the *Resource Endpoint*);
- the *Whitelist*, with which the *Nodes* accept each other as MedMij nodes;
- the *Clientdirectory*, in which the *OAuth Authorization Server*:
  - can find a user-friendly name of the *Client* to use in the [Declaration of consent \[NL\]](#) or the [Declaration of confirmation \[NL\]](#);
  - can see the *Information Services* for which the *Client* is qualified;
- the *Information service glossary*, from which the *Client* can see which *Depiction Names* the *Information Services* have that are at any moment available on the MedMij Network.

A fifth list, the *Information service Information service catalogue*, is published by MedMij as an annex to the MedMij Trust Scheme on [this page](#). Finally, the metamodel is the conceptual basis for two reports that are expected from Participants:

- the *Maintenance Report*, which each *Participant* uses to periodically inform the *Maintenance Organisation* about key figures on the functioning of the MedMij Network;
- the *Portability Report*, with which the *Individual* is informed by its *Individual's Service Provider* about which health information that *Individual* has collected from *Providers* in his PHE so that he could supplement another one or a new PHE once again with the same collection actions.

There are logical models available for all seven of them on a [separate page](#), which are implementations of the metamodel.

The metamodel has been set up in a certain style, with association classes in particular. The advantage of this is that it means that the metamodel remains as adaptable and expandable as possible. Common constructions, such as attributes and specialisation are all implementations of association classes. However, we want to leave implementation to the [logical models](#) and the technical models (the [XML schemas](#)). A second advantage is that existence-dependent relationships become explicit. 'Existence-dependent' means that one class is meaningless without the other, and thus that the first-named class cannot exist without the last-named class. An association class is always existence-dependent on the two classes that associate it.

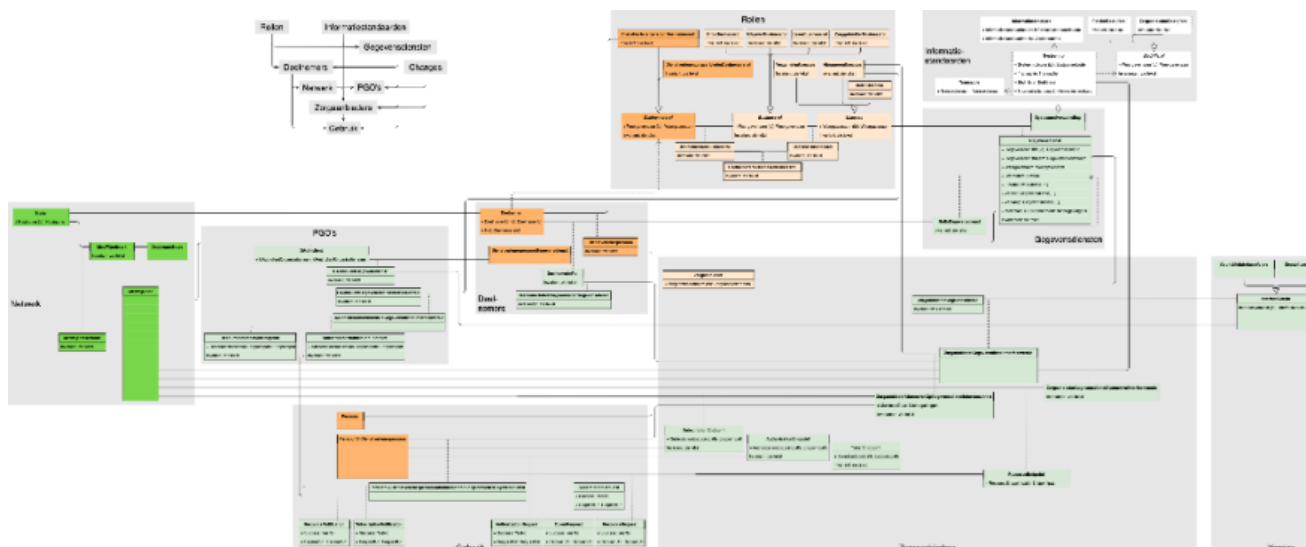
This modelling style has been deviated from in a couple of respects, namely through the usage of:

- the uses relationship, especially in the *Information Standards Domain*, because that domain is not managed by MedMij;
- the aggregation relationship, ditto;
- the object-oriented specialisation, namely where we give a summarised definition of *Participants Role*, *Business Role*, *Usecase* and *Organisational Role*;
- attributes for identification or specification.

In all these cases, association classes could also be used but that would unnecessarily complicate the model's presentation.

For the overview, the metamodel has been organised into nine model domains: *Roles*, *Participants*, *PHEs*, *Providers*, *Information Services*, *Information standards*, *Infrastructure*, *Changes* and *Use*. There is a chart in the top left of the metamodel figure that shows how the various areas make use of concepts from other areas.

The names of the classes and the attributes all start with a capital letter. The rest of the names consist solely of lowercase letters, apart from where the rest of the name also occurs in the metamodel as a separate name or if a proper name is used that requires something different. In other words, the metamodel notes *Client*, because the name *OAuth* is a proper name in which the *A* is written as a capital letter, and because the name *Client* does not occur as a separate name in the metamodel. The metamodel notes *ProviderInformationservice*, with a capital first *I*, because *Information Service* does indeed occur as a separate name.



## Explanatory Notes

The MedMij Maintenance organisation keeps track of which *Organisations*, by entering into a *Participant's Agreement*, become a *Participant*. There are *Participants* in two Roles: *ServiceproviderindividualParticipants* role and *ServiceproviderproviderParticipants* role. These correspond with the respective roles *Individual's Service Provider* and *Provider's Service Provider* on the [legal layer](#).

*Organisations* use *Nodes* that they are the holder of. When an *Organisation* is a *Participant*, it will register such a *Node* as a *ParticipantNode* with the MedMij Maintenance organisation. On the *MedMij Infrastructure*, such a *ParticipantNode* appears as a *MedMijNode*. The *Hostnames* of these *MedMij Nodes* are disclosed by the MedMij Maintenance organisation via the *MedMij Network*. The *MedMij Nodes* use this list as a *Whitelist*, i.e. to determine whether a *Node* that presents itself is authorised to be active in the *MedMij Network*. This *Whitelist* appears as an implementation component only in the [logical models](#). This also applies for the *MedMijSystemNode*, which is the *Node* that *MedMij Maintenance* uses to publish four lists. The *MedMijSystemNode* does not explicitly appear in the *Whitelist*, but it is indeed authorised to participate in the *MedMij Network*. What is more, without the *MedMijSystemNode* the *MedMij Network* cannot work.

For the *MedMijNodes* of *Participants* who are *Serviceproviderindividual* (or better put: for the *Clients* on the [Application Layer](#) during the authorization phase of [UCI Collect](#) and [UCI Share](#)), the

*Clientdirectory* contains user-friendly names (*Organisationname*), in order to be used in the [Declaration of consent \[NL\]](#) and the [Declaration of confirmation \[NL\]](#). The *Clientdirectory* is an implementation component and appears in the [logical models](#). When a Client (a PHE) enables the use of Subscriptions for the Individual, it must offer endpoints for the two types of notifications that the *Provider* must be able to send in that context, namely a *SubscriptionNotificationEndpoint* and a *ResourceNotificationEndpoint*.

In the *Rolesmodel* domain, the *Participant Roles*, *Business Roles* and *Use Cases* appear that exist in this release of the MedMij Trust Scheme, along with their permitted combinations. In the *Participantsmodel* domain, the *Participants* in the MedMij Trust Scheme are addressed and for which *Providers* they disclose which *Information Services*.

*Information Services* belong to a *Usecase* and have a validity period. In addition, by means of the attribute *Required*, it is required from some *Information Services* that, as a *Provider* that offers an *Information Service*, they must also offer certain other *Information Services*, too. This list will often be empty but it makes little sense, for example, to offer the *Share* of an agreement request without also providing the *Collect* of the response to it. The class *RoleInInformationservice* is used, via the *Participant*, to link the MedMij roles *ServiceproviderindividualParticipantsrole* and *ServiceproviderproviderParticipantsrole* with the corresponding roles that Nictiz has formulated in the Information Standards domain, namely *PatientOrganisationalrole* and *ProviderOrganisationalrole*.

The classes in the model domain *Information Standards*, including their names, must be understood in the sense in which Nictiz uses them in the context of the *Information Standards* that are permitted for use in MedMij. This is why the outlines of these classes are shown as dotted lines. An *Organisational Role*, which there are two of (*PatientOrganisationalrole* and *ProviderOrganisationalrole*), are accepted by a *System Role*. Each *System Role* must have an *Information Standard*. *System Roles* are grouped into *System Role compilations* that together with a *Usecase* form an *Information service*. A current example of a *System Role compilation* is a compilation of four *System Roles*, two of which (one for each relevant *Organisational Role*) exchange an overview of available PDF documents and two of which (again one for each relevant *Organisational Role*) exchange a PDF document from that overview. *Information services* are offered as a unit (that is to say with their entire *System Role compilation*) to *Care Users*, and these users will also authorise them all at once.

At the bottom of the model, the link is made with the *Providers*. This model domain is the basis for the [logical model](#) of the *Information service directory*. When a *Provider* offers a certain *Information Service* in accordance with a certain *Interface Version*, then a *ProviderInformationserviceInterfaceversion* belongs to this, too. When a *Provider* additionally offers *Subscriptions* to this *Information service*, a *ProviderSubscribeToInformationserviceInterfaceversion* belongs to this too. These classes are used to inform *Care Users* about which of the *Providers* (*Subscribe to*) offer which *Information services*. Furthermore, within an *Information service* there are one or more *System Roles*. This relationship is included in the class *ProviderInformationserviceSystemroleInterfaceversion*.

Interfaces are versioned: various versions of interfaces can be offered on the MedMij Network at the same time. For this reason, there is the *Interface Version* class in the *Changes* model area. All endpoints in the *Information service directory* and the *Client directory* (see below) belong to a single *Interface Version*.

A *Provider* can limit the maximum subscription duration that it offers for an *Information Duration*, on an *Interface Version*. Furthermore, it really must remain below the maximum duration that MedMij has stated for that *Information service* in the [Information service catalogue](#). The maximum duration states the turnaround time in days, where the value 0 indicates that a subscription is not supported.

One *AuthorizationEndpoint*, one *TokenEndpoint* and if *Subscriptions* are also offered on this, one *SubscriptionEndpoint*, belong to a *ProviderInformationservice*. One *ResourceEndpoint* belongs to a



*ProviderInformationSystemServiceSystemrole*. For all types of endpoints, the metamodel designates the *Endpointpath*, the path in the URI used to address the endpoints, and an *Interface Version*, which enables versions of the same endpoints which are operating simultaneously to be distinguished. In this version of the MedMij Trust Scheme, the standard IANA port is used for https on both the frontchannel and the backchannel. Therefore, port numbers do not need to be specified in the endpoint addresses.

These components are collected together with the *Hostname* of the relevant *MedMijNode* into a URI that is considered to be the address of the respective endpoint. This is done in the [logical model](#) (with invariants). The requirements for all of these components and the way in which they are collected into URIs is described on the [Interface](#) page.

The same *Provider* may - for different *Information services* - utilise services of various *Participants*. However, a single *ProviderInformationService* must have precisely one *ParticipantInRole*. This is why the class *ParticipantInRoleProviderInformationService* has been included in the metamodel, namely in the *Participants* model Domain.

For the purpose of the Maintenance Report and the Portability Report, Participants must be able to submit information about what is happening on the MedMij Network. This information is fixed by the *Changes* model area. This information is mainly based on requests that are made across the MedMij Network. There are six types. The *RequestUri* or whether the request was unsuccessful must be known for each request.

---

Invariants, i.e. restrictions that apply at all times, are shown at the bottom in a separate table. There are various types of these, which are named in the right-hand column:

- Summaries state that a certain class has a fixed number of explicitly named instances.
  - Numerical relationships stipulate numerical requirements for the number of instances that a class has or for the relationship between the numbers in multiple classes.
  - Local dependencies impose restrictions on the content-related relationships between attributes of the same class.
  - Non-local dependency imposes restrictions on the content-related relationships between instances of different classes.
  - Role connections limit the role combinations of different role classes. They correspond to (amongst other things) the role connections between the different layers.
- 

The classes in the metamodel belong to the different [layers](#) in the architecture of the trust scheme. The relevant layer is shown by colouring in the classes. Only in the case of the Nictiz classes in the *Register of Information Standards* have we not done this.

---

It is clear from this metamodel how addressing is dealt with in the MedMij Trust Scheme. The addressing system consists of three components:

- MedMij Provider names for *Providers*, as described in responsibility 13 in the [Process and Information layer](#);
  - *Information services* with *System Roles* as included in the *Information service catalogue* or *Register of Information Standards* respectively;
  - Each *Provider* has for each *ProviderInformationService* (which they offer via a *Provider's Service Provider*) a single *AuthorizationEndpoint* and a single *TokenEndpoint* and for each *ProviderInformationServiceSystemrole* within it a single *ResourceEndpoint*. The endpoints each have a URI as a technical address.
-



Where the metamodel refers to periods, limited by a start and an end, this start and end must be interpreted as beginning moments. If it relates to a start date and end date, as is the case in the attributes of *Information service*, the begin moments of these dates are accordingly meant, at 00h00m00. The start is interpreted as the begin of the validity and the end as the begin of the invalidity. This is why the validity runs from start to end (and not 'up to and including'). This also means that if the end is lacking that the validity extends for an indefinite period of time.

## Invariants

The above diagram is organised by (existence-) dependencies between classes. Within this organisation, there are also consistency requirements that are imposed on the instances of these classes. These are the invariants that are shown in the table below. An invariant expresses the fact that an instance of the relevant class does not exist if it does not comply with the invariant. The table makes no other statement about how the monitoring of this consistency is implemented. In many implementations, temporary inconsistencies are permitted and are only refused or remedied later on. There are many ways to do this but the MedMij Trust Scheme wants to allow great leeway in the way in which the consistency in registrations is guaranteed. The path expressions in the invariants consist of names separated by full stops. A step is always taken from a certain class to a class on whom the first-named class is directly existence-dependent. The name of the side of the association about which the step is taken is deemed to bear the name of the relevant endpoint of the association, i.e. of the step's destination.

Relates to instances of class ...	Invariant
<i>Subscribe Usecase</i>	There is precisely one instance of this.
<i>AuthorizationEndpoint</i>	For each <i>AuthorizationEndpoint</i> <i>a</i> and for each <i>ParticipantInRoleProviderInformationservice</i> <i>d</i> , it is true that: IF <i>d.ProviderInformationserviceInterfaceversion</i> = <i>a.ProviderInformationserviceInterfaceversion</i> THEN <i>d.ParticipantInRole.Participant</i> = <i>a.MedMijNode.ParticipantNode.Participant</i>
<i>Organisational Role</i>	Each <i>Organisational Role</i> is either <i>PatientOrganisationalrole</i> or <i>ProvidersOrganisation</i>
<i>Organisational Role</i>	For each <i>Organisational Role</i> <i>b</i> it is true that: IF ( <i>b</i> : <i>PatientOrganisationalrole</i> THEN <i>b.Depictionname</i> = "Patient"; <i>b</i> : <i>ProvidersOrganisation</i> THEN <i>b.Depictionname</i> = "Provider"; IF NOT THEN ERROR
<i>IssuerBusinessrole</i>	There is precisely one instance of this.
<i>Business Role</i>	For each <i>Business Role</i> <i>b</i> it is true that: IF ( <i>b</i> : <i>IssuerBusinessrole</i> THEN <i>b.Depictionname</i> = "Issuer"; <i>b</i> : <i>AddresseeBusinessrole</i> THEN <i>b.Depictionname</i> = "Addressee"; <i>b</i> : <i>PublisherBusinessrole</i> THEN <i>b.Depictionname</i> = "Publisher"; IF NOT THEN ERROR
<i>ParticipantInRole</i>	For each <i>ParticipantInRole</i> <i>d</i> it is true that: <i>d.ParticipantInRole</i> and <i>d.RoleInInformationservice</i> .

	<i>ParticipantsroleUsecaseBusinessrole.Participantsrole</i> identical.
<i>ParticipantInRoleProviderInformationservice</i>	For each <i>ParticipantInRoleProviderInformationservice</i> is true that: <i>d. ProviderInformationservice. Informationservice = d.ParticipantInRole. RoleInInformationservice.Informationservice</i>
<i>Individual's Service Provider</i>	There is no more than a single instance of this with <i>Participant</i> , and precisely one of them if the <i>Participant</i> Role of the last-named is of the type <i>Service ProviderindividualParticipantsrole</i> .
<i>Participant's Role</i>	For each <i>Participant's Role d</i> it is true that: IF ( <i>d : Service ProviderindividualParticipantsrole</i> THEN <i>d.Depiction = "Individual's Service Provider"</i> ; <i>d : Service ProviderProviderParticipantsrole</i> THEN <i>d.Depiction = "Provider's Service Provider"</i> ; IF NOT THEN ERROR
<i>ParticipantsroleBusinessrole</i>	There are precisely three instances of this, namely: <ul style="list-style-type: none"> <li>• a single one such that <i>ParticipantsroleBusinessrole : Service ProviderindividualParticipantsrole</i> and <i>ParticipantsroleBusiness.Businessrole : PublisherBusinessrole</i>;</li> <li>• a single one such that <i>ParticipantsroleBusinessrole : Service ProviderProviderParticipantsrole</i> and <i>ParticipantsroleBusiness.Businessrole : IssuerBusinessrole</i>; and</li> <li>• a single one such that <i>ParticipantsroleBusinessrole : ServiceproviderproviderParticipantsrole</i> and <i>ParticipantsroleBusiness. Business Role: AddresseeBusinessrole</i>;</li> </ul>
<i>ParticipantsroleUsecaseBusinessRole</i>	This class consists of precisely one instance for each combination of an instance <i>d</i> of <i>ParticipantsroleBusinessrole</i> and an instance <i>u</i> of <i>UsecaseBusinessrole</i> for which it is true that: <i>d. BusinessRole = u.BusinessRole</i> .
<i>ShareUsecase</i>	There is precisely one instance of this.
<i>Service ProviderindividualParticipantsrole</i>	There is precisely one instance of this.

<i>Service ProviderParticipant</i> role	There is precisely one instance of this.
<i>Information service</i>	There are none or more <i>Information services</i> .
<i>Information service</i>	For each <i>Information service</i> <i>g</i> it is true that: <i>g.Start date</i> before <i>g.End date</i> .
<i>Information service</i>	For each <i>Information service</i> <i>g1</i> and <i>g2</i> it is true that: if <i>g1</i> occurs in <i>g1.Required</i> THEN ( <i>g2</i> is stated as an <i>Information service</i> in <i>Information service catalogue</i> AND <i>g1.Start date</i> is not before <i>g2.Start date</i> AND <i>g1.End date</i> is not after <i>g2.End date</i> )
<i>Information service</i>	For each <i>Information service</i> <i>g</i> it is true that: <i>g.Information servicename</i> is a concatenation of <i>g.Information service name</i> , <i>g.Depictionname</i> and the first two <i>g.Systemrole</i> sequences (in so far as present and with the separate stop) of <i>g.Systemrole.Informationstandard</i> . <i>Informationstandardversion</i> , with a space as delimiter.
<i>Information service</i>	For each two different <i>Information services</i> <i>g1</i> and <i>g2</i> it is true that: <i>g1.Information servicename</i> != <i>g2.Information servicename</i>
<i>Published Interface Version</i>	There is precisely one instance of this.
<i>AddresseeBusinessrole</i>	There is precisely one instance of this.
<i>MedMijnnetwork</i>	There is precisely one instance of this.
<i>MedMijSystemNode</i>	There is precisely one instance of this.
<i>Node</i>	The hostname of a Node contains a domain name that is a fully-qualified domain name, in accordance with <a href="#">RFC 2801 section 2</a> .
<i>Client</i>	For each <i>Client</i> <i>o</i> it is true that: <i>o.ClientOrganisation</i> complies with the <a href="#">Clientnamepolicy</a> [NL].
<i>ClientSubscribeToInformationserviceInterfaceversion</i>	Each <i>ClientSubscribeToInformationserviceInterface</i> has precisely one <i>ResourceNotificationEndpoint</i> .
<i>ClientSubscribeToInformationserviceInterfaceversion</i>	Each <i>ClientSubscribeToInformationserviceInterface</i> has precisely one <i>SubscriptionNotificationEndpoint</i> .

<i>ClientInformationservice</i>	<p>For each <i>ClientInformationservice</i> <i>zg</i>, it is true that: IF there is an <i>ClientSubscribeToInformationserviceInterfaceversion</i> so that:</p> <ul style="list-style-type: none"> <li>• <i>zagi1.ClientInformationserviceInterfaceversion.ProviderInformationservice</i> = <i>zg</i> and</li> <li>• <i>zagi1.ClientInformationserviceInterfaceversion.Interface Version</i> is the <i>Published Interface Ver</i>.</li> </ul> <p>THEN there is an <i>ClientSubscribeToInformationserviceInterfaceversion</i> <i>zagi2</i> so that:</p> <ul style="list-style-type: none"> <li>• <i>zagi2.ClientInformationserviceInterfaceversion.ProviderInformationservice</i> = <i>zg</i> and</li> <li>• <i>zagi2.ClientInformationserviceInterfaceversion.Interface Version</i> is the <i>Mandatory Interface ver</i></li> </ul>
<i>ProviderInformationservice</i>	<p>For each <i>ProviderInformationservice.Informationset</i> <i>TransactionCompilation.Transaction.Systemrole</i> <i>s</i> f which it is true that <i>s.Organisationalrole</i> = <i>ProviderOrganisationalrole</i>, it is true that there is a <i>ProviderInformationserviceSystemrole</i> <i>z</i> so that <i>z.</i> <i>Systemrole</i> = <i>s</i>.</p>
<i>ProviderInformationservice</i>	<p>Each <i>ProviderInformationservice</i> has precisely one <i>AuthorizationEndpoint</i>.</p>
<i>ResourceEndpoint</i>	<p>For each <i>ResourceEndpoint</i> <i>r</i> and for each <i>ParticipantInRoleProviderInformationservice</i> <i>d</i>, it is t that: IF <i>d.ProviderInformationserviceInterfaceversion</i> = <i>r.</i> <i>ProviderInformationserviceSystemroleInterfacevers</i> <i>ProviderInformationserviceInterfaceversion</i> THEN <i>d.ParticipantInRole.Participant</i> = <i>r.MedMijNo</i> <i>ParticipantNode.Participant</i></p>
<i>ResourceEndpoint</i>	<p>For each <i>ResourceEndpoint</i> <i>r</i>, it is true that: IF <i>r.ProviderInformationserviceSystemroleInterface</i> <i>ProviderInformationserviceInterfaceversion.</i> <i>ProviderInformationservice.Informationservice</i> is ba an <i>Information Standard</i> from the <a href="#">Register of Inform</a> <a href="#">Standards</a>, &lt;ac:structured-macro ac:name="unmigrated-wiki-m ac:schema-version="1" ac:macro-id="12e76043-9b 4676-a211-2bebc1511192"&gt;&lt;ac:plain-text-body&gt;&lt;! [THEN <i>r</i> is equal to that referred in the technical de: the <i>Information Standard</i> [base].</p>

<i>ResourceNotificationEndpoint</i>	For each <i>ResourceNotificationEndpoint</i> <i>s</i> , it is true that: <i>s.MedMijNode.ParticipantNode.Participant</i> = <i>s.ClientSubscribeToInformationService.Client.MedMijParticipantNode.Participant</i>
<i>RoleInInformationService</i>	This class consists of precisely a single instance <i>r</i> for each combination of an instance <i>d</i> of <i>r</i> . <i>ParticipantsroleUsecaseBusinessrole</i> and an instance <i>g</i> of <i>InformationService</i> for which it is true that: <i>g.UsecaseBusinessrole.Usecase</i>
<i>SubscriptionEndpoint</i>	For each <i>SubscriptionEndpoint</i> <i>s</i> and for each <i>ParticipantInRoleProviderInformationService</i> <i>d</i> , it is true that: IF <i>d.ProviderInformationServiceInterfaceVersion</i> = <i>s.ProviderSubscribeToInformationServiceInterfaceVersion</i> THEN <i>d.ParticipantInRole.Participant</i> = <i>s.MedMijNode.ParticipantNode.Participant</i>
<i>SubscriptionEndpoint</i>	For each <i>ProviderInformationService</i> <i>zg</i> , for each <i>ProviderInformationServiceInterfaceVersion</i> <i>zgi</i> of <i>zg</i> , for each <i>ProviderSubscribeToInformationServiceInterfaceVersion</i> <i>zgi</i> , for each <i>ResourceEndpoint</i> <i>r</i> of <i>zgi</i> and for <i>ParticipantInRoleProviderInformationService</i> <i>d</i> of <i>zg</i> true that: <i>r.MedMijNode.ParticipantNode.Participant</i> = <i>d.ParticipantInRole.Participant</i>
<i>SubscriptionNotificationEndpoint</i>	For each <i>SubscriptionNotificationEndpoint</i> <i>s</i> , it is true that: <i>s.MedMijNode.ParticipantNode.Participant</i> = <i>s.ClientSubscribeToInformationService.Client.MedMijParticipantNode.Participant</i>
<i>System Role</i>	For each <i>System Role</i> <i>s</i> it is true that: IF <i>s.Organisationalrole : PatientOrganisationalrole</i> THEN true that for all <i>RoleInInformationService</i> <i>r</i> : (IF <i>s</i> in <i>r.InformationService.TransactionCompilation</i> THEN <i>r.ParticipantsroleUsecaseBusinessrole.ParticipantsroleUsecaseBusinessrole</i> Service <i>ProviderIndividualParticipantsrole</i> )
<i>System Role</i>	For each <i>System Role</i> <i>s</i> it is true that: IF <i>s.Organisationalrole : ProviderOrganisationalrole</i> THEN true that for all <i>RoleInInformationService</i> <i>r</i> : (IF <i>s</i> in <i>r.InformationService.TransactionCompilation</i> THEN <i>r.ParticipantsroleUsecaseBusinessrole.ParticipantsroleUsecaseBusinessrole</i> Service <i>ProviderProviderParticipantsrole</i> )
<i>TokenEndpoint</i>	

	<p>For each <i>TokenEndpoint</i> <i>t</i> and for each <i>ParticipantInRoleProviderInformationservice</i> <i>d</i>, it is that:</p> <p>IF <i>d.ProviderInformationserviceInterfaceversion</i> = <i>t.ProviderInformationserviceInterfaceversion</i></p> <p>THEN <i>d.ParticipantInRole.Participant</i> = <i>t.MedMijNode.ParticipantNode.Participant</i></p>
<i>PublisherBusiness Role</i>	There is precisely one instance of this.
<i>Usecase</i>	<p>For each <i>Usecase</i> <i>u</i> it is true that: IF ( <i>u</i> : <i>CollectUsecase</i> THEN <i>u.Depictionname</i> = "Collect"; <i>u</i> : <i>ShareUsecase</i> THEN <i>u.Depictionname</i> = "Share"; IF NOT THEN E</p>
<i>Usecase Business Role</i>	<p>There are precisely four instances of this, namely:</p> <ul style="list-style-type: none"> <li>• a single one such that <i>UseCaseBusinessrole.Businessrole</i> : <i>PublisherBusinessrole</i> and <i>UseCaseBusinessrole.Usecase</i> : <i>CollectUsecase</i></li> <li>• a single one such that <i>UseCaseBusinessrole.Businessrole</i> : <i>PublisherBusinessrole</i> and <i>UseCaseBusinessrole.Usecase</i> : <i>ShareUsecase</i></li> <li>• a single one such that <i>UseCaseBusinessrole.Businessrole</i> : <i>IssuerBusinessrole</i> and <i>UseCaseBusinessrole.Usecase</i> : <i>CollectUsecase</i></li> <li>• a single one such that <i>UseCaseBusinessrole.Businessrole</i> : <i>AddresseeBusinessrole</i> and <i>UseCaseBusinessrole.Usecase</i> : <i>ShareUsecase</i></li> </ul>
<i>Mandatory Interface Version</i>	There is precisely one instance of this.
<i>CollectUsecase</i>	There is precisely one instance of this.
<i>ProvidersOrganisationalrole</i>	There is precisely one instance of this.
<i>Provider</i>	Each <i>Provider</i> has at least one <i>ProviderInformation</i>
<i>Provider</i>	Each <i>Provider</i> has with each <i>Information Service</i> not more than a single <i>ProviderInformationservice</i> .
<i>Provider</i>	<p>For each <i>ProviderInformationservice</i> <i>zg1</i> and for each <i>Information Service</i> <i>g</i> in <i>zg1.Information Service.Representation</i> it is true that:</p> <p>there is a <i>ProviderInformationservice</i> <i>zg2</i>, so that <i>zg2.Provider</i> = <i>zg1.Provider</i> and <i>zg1.Informationservice</i> = <i>zg2.Informationservice</i></p>
<i>Provider</i>	For each <i>ProviderInformationservice</i> <i>zg1</i> and for each <i>Information service</i> <i>g</i> in <i>zg1.Information service.Representation</i>

	<p>it is true that:  there is, unlike for <i>zg1</i>, <u>no</u> <i>ProviderInformationservice</i>  , so that <i>zg1.Provider = zg2.Provider</i> and  either <i>zg2.Informationservice</i> follows <i>g</i> or <i>g</i> follows  <i>Informationservice</i>.  'Follows' is (recursively) defined as follows here:  <i>Information service h1</i> follows <i>Information service h</i>  either <i>h1=h2</i> or else <i>h2</i> follows a <i>Information service</i>  <i>Replaces</i>.</p>
<i>ProviderSubscribeToInformationservice</i>	<p>For each <i>ProviderInformationservice zg</i>, For each  <i>ProviderSubscribeToInformationservice zaog</i> of <i>zg</i>,  each <i>SubscriptionEndpoint s</i> of <i>zaog</i> and for each  <i>ParticipantInRoleProviderInformationservice d</i> of <i>zg</i>  true that:  <i>s.MedMijNode.ParticipantNode.Participant = d</i>.  <i>ParticipantInRole.Participant</i></p>
<i>ProviderSubscribeToInformationserviceInterfaceversion</i>	<p>For each  <i>ProviderSubscribeToInformationserviceInterfaceversion</i>  , it is true that:  <i>zgi.ProviderInformationserviceInterfaceversion</i>.  <i>ProviderInformationservice.Informationservice.Use</i>  = <i>CollectUseCase</i></p>
<i>ProviderSubscribeToInformationserviceInterfaceversion</i>	<p>Each  <i>ProviderSubscribeToInformationserviceInterfaceversion</i>  has precisely one <i>SubscriptionEndpoint</i>.</p>
<i>ProviderSubscribeToInformationserviceInterfaceversion</i>	<p>For each  <i>ProviderSubscribeToInformationserviceInterfaceversion</i>  , it is true that:  <i>zgi.MaximumDuration &lt;= zgi</i>.  <i>ProviderInformationserviceInterfaceversion</i>.  <i>ProviderInformationservice.Informationservice</i>.  <i>MaximumDuration</i></p>
<i>ProviderInformationservice</i>	<p>For each <i>ProviderInformationservice zg</i>, it is true th  IF there is a <i>ProviderInformationserviceInterfaceversion</i>  <i>zgi1</i> so that:</p> <ul style="list-style-type: none"> <li>• <i>zg1.ProviderInformationservice = zg</i> and</li> <li>• <i>zg1.Interfaceversion</i> is the <i>Published Interface</i> '</li> </ul> <p>THEN there is a  <i>ProviderInformationserviceInterfaceversion zgi2</i></p> <ul style="list-style-type: none"> <li>• <i>zgi2.ProviderInformationservice = zg</i> and</li> <li>• <i>zgi2.Interfaceversion</i> is the <i>Mandatory Interface</i></li> </ul>



<i>ProviderInformationservice</i>	<p>For each <i>ProviderInformationservice</i> <i>zg</i>, it is true th IF there is a <i>ProviderSubscribeToInformationserviceInterfacever</i> <i>zagi1</i> so that:</p> <ul style="list-style-type: none"> <li>• <i>zagi1.ProviderInformationserviceInterfaceversic</i> <i>ProviderInformationservice</i> = <i>zg</i> and</li> <li>• <i>zagi1.ProviderInformationserviceInterfaceversic</i> <i>Interface Version</i> is the <i>Published Interface Ver</i>.</li> </ul> <p>THEN there is a <i>ProviderSubscribeToInformationserviceInterfac</i> <i>zagi2</i> so that:</p> <ul style="list-style-type: none"> <li>• <i>zagi2.ProviderInformationserviceInterfaceversic</i> <i>ProviderInformationservice</i> = <i>zg</i> and</li> <li>• <i>zagi2.ProviderInformationserviceInterfaceversic</i> <i>Interface Version</i> is the <i>Mandatory Interface ver</i></li> </ul>
<i>ProviderInformationservice</i>	<p>For each <i>ProviderInformationservice.Informationse</i> <i>TransactionCompilation.Transaction.Systemrole s</i> f which it is true that <i>s.Organisationalrole</i> = <i>ProviderOrganisationalrole</i>, it is true that there is a <i>ProviderInformationserviceSystemrole z</i> so that <i>z.</i> <i>Systemrole</i> = <i>s</i>.</p>
<i>ProviderInformationservice</i>	<p>Each <i>ProviderInformationservice</i> has precisely one <i>AuthorizationEndpoint</i>.</p>
<i>ProviderInformationservice</i>	<p>Each <i>ProviderInformationservice</i> has precisely one <i>TokenEndpoint</i>.</p>
<i>ProviderInformationservice</i>	<p>Each <i>ProviderInformationservice</i> has precisely one <i>ParticipantInRoleProviderInformationservice d</i>, and a way that <i>d.ParticipantInRole.Participant.Role</i> = <i>S</i> <i>ProviderProviderParticipantsrole</i>.</p>
<i>ProviderInformationserviceSystemRoleInterfaceversion</i>	<p>Each combination of a <i>ProviderInformationserviceInterfaceversion</i> and a <i>S</i> <i>Role</i> has no more than one <i>ProviderInformationserviceSystemRoleInterfacever</i>.</p>
<i>ProviderInformationserviceSystemRoleInterfaceversion</i>	<p><i>ProviderInformationserviceSystemRoleInterfacever</i> <i>SystemRole.OrganisationalRole</i> = <i>ProviderOrganisationalRole</i></p>
<i>ProviderInformationserviceSystemRoleInterfaceversion</i>	<p>Each <i>ProviderInformationserviceSystemRoleInterfacever</i> has precisely one <i>ResourceEndpoint</i>.</p>



<i>CareuserBusinessrole</i>	There is precisely one instance of this.
-----------------------------	--

## Basic classes

Basic class	Definition
<i>Date</i>	In accordance with the type xs:date, as specified in <a href="#">XML schema 1.0</a> .
<i>ParticipantId</i>	String of at least one, and a maximum of 30 characters.
<i>Endpointpath</i>	See addressing responsibilities on the <a href="#">Interfaces</a> page.
<i>InformationserviceId</i>	String of at least one, and a maximum of 30, character(s).
<i>Informationservicename</i>	String of at least three, and a maximum of 50, characters.
<i>Hostname</i>	See addressing responsibilities on the <a href="#">Interfaces</a> page.
<i>Information Standard name</i>	String of at least three, and a maximum of 50, characters.
<i>InterfaceversionId</i>	String of at least one, and a maximum of 30 characters.
<i>NonNegativeInteger</i>	In accordance with the type xs:nonNegativeInteger, as specified in <a href="#">XML schema 1.0</a> .
<i>ClientOrganisationname</i>	In accordance with the applicable <a href="#">Client name policy [NL]</a> .
<i>RequestUri</i>	String of at least twelve, and a maximum of 2048 characters.
<i>Systemrolecode</i>	String of at least one, and a maximum of 30, character(s).
<i>Transactionname</i>	String of at least three, and a maximum of 50, characters.
<i>Version number</i>	One or more number sequences, each consisting of one or more digits 0 to 9 inclusive, separated by a full stop
<i>Depictionname</i>	String of at least three, and a maximum of 50, characters.
<i>YesNo</i>	In accordance with the type xs:boolean, as specified in <a href="#">XML schema 1.0</a> .
<i>Providername</i>	In accordance with applicable <a href="#">Providersnamepolicy. [NL]</a>

## Logical models

### Explanatory Notes

There is only a single [metamodel](#) but there are multiple logical models. Logical models prepare the implementation of certain components of the [metamodel](#). This version of the MedMij Trust Scheme has three logical models. Each of them is required for one or more specific implementation components in the MedMij Trust Scheme. This relates to the following components:

- the four lists published by *MedMij Registration: Information service glossary, Clientlist, Whitelist and Information service directory*;
- the *Information service catalogue of Information services* to be published in the MedMij Trust Scheme;
- the (*Hostname* of the) *MedMijSystemNode* to be published in the MedMij Trust Scheme;
- the two reports requested from the Participants: *Maintenance Report* and *Portability Report*.

The four lists have been combined into a single logical model, under the class *MedMijMaintenancelist*, because they share basic characteristics. Something similar applies to the two reports, under the class *MedMijReport*

Logical models obey the [metamodel](#) but specify it. In the step from [metamodel](#) to logical model, (logical and other) classes, invariants and basic classes may be added. However, the logical models primarily build on the [metamodel](#) by using its classes and attributes. In that case, logical classes, values and basic classes accordingly have corresponding classes in the [metamodel](#). The similarities are shown below with the logical model named in a table. Where the table for a certain logical class, value or basic class does not name the similarity with the [metamodel](#), it means that this is new for the logical level.

Logical classes have fewer or more attributes than the corresponding classes in the [metamodel](#). Where there are fewer, this means that the omitted attributes do not need to be included in the component to be implemented, for example of a list to be published. Where there are more, these attributes are passed down from a class in the [metamodel](#) that the corresponding class in that metamodel was existence-dependent on. In the [metamodel](#), the last-named class was accordingly accessible for the existence-dependent class but it is no longer present in the specific logical model and thus is no longer accessible either. This means that if the relevant class in the logical model has not taken over the attribute then this will be lost.

Where an invariant from the [metamodel](#) fits within the scope of the specific logical model, this also appears as an invariant with the logical model, although the formulation will have been adapted to the organisation and naming used in the logical model. In addition, new invariants too may appear on the logical level. Most of them are inheritances: in the step from the [metamodel](#) to a logical model, links between classes become broken. If these links are important after all in the logical model then attributes from the [metamodel](#) are bequeathed from a certain class in the [metamodel](#) to a lower class, for which a pendant does actually occur in the logical model. Here, "lower class" refers to the fact that this is existence-dependent on the other (higher) class. Such an inheritance invariant is written with a . In front of that arrow, we see the inheriting attribute of the *logical* class, and behind it, we see the path *in the metamodel* to the bequeathing class.

Where applicable, the basic classes too from the [metamodel](#) are taken over by the logical model. There is a single place in the logical model where new basic classes appear as well.

The logical models have a structure that is more oriented towards implementation than the [metamodel](#) is. This [metamodel](#) is based on association classes and existence-dependency, whereas the logical models are more hierarchical in nature. Hierarchy is a constriction of associative existence-dependency but is a better fit with many types of standard implementation technology, this certainly including XML, in which the four lists are implemented. This constriction does, however, mean that the logical models are less long-lasting and less expandable than the [metamodel](#); something that for the [metamodel](#) is a simple expansion can correspond to a substantial modification of the logical models. This is the price you pay for hierarchy.

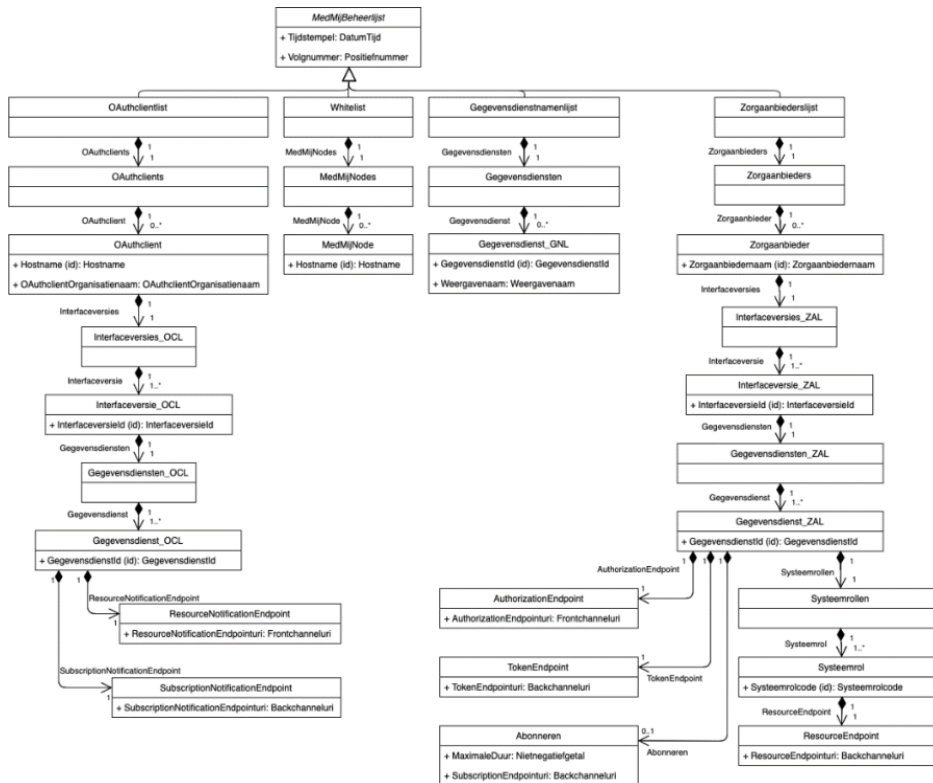
When translating the associativity of the [metamodel](#) into the hierarchy of the logical models, a number of rules of thumb have been applied:

- The top of the hierarchy of a logical model is determined by the scope of the implementation component. The *Information service directory*, for example, lists first of all the *Providers*. Starting from that "logical centre", the hierarchy descends from top to bottom, without exceeding the scope of the implementation. In the logical model, the step towards the bottom in the hierarchy typically takes the form of a 'uses' relationship (the dotted-line arrow).
- En route, a composition hierarchy is built, and in each step a selection is made from the attributes available in the [metamodel](#), on the basis of the scope of the implementation component. In doing so, logical classes are not combined into a granular class, not even if no attribute at all is left over. The class granularity of the logical model is accordingly comparable with that of the [metamodel](#).
- In addition, as described above, attributes in the [metamodel](#) that threaten to fall outside its scope but that are actually needed are bequeathed to within the scope. Where this is done, the inheritance is specified in the list of logical invariants.
- Lower classes in the uses hierarchy lie completely within the logical scope of the higher one. In this way, a hierarchy also creates closed "name spaces". This means that their naming is simpler and shorter than in the [metamodel](#), where it is precisely the case that all contexts are open-ended. In the logical models, therefore, the names of the classes do not become meaningful until higher classes are considered with them. However, this does simplify the implementation. In a separate table for each logical model, it is ensured that these name changes do not cause the link with the [metamodel](#) to become lost.
- In a single instance, the previous point has the consequence that there is a risk that a homonym could arise within a single logical model (such as Information service and Information services in the logical model of the lists and the reports). In that case, the names will be expanded so that their hierarchical context becomes visible (namely with */sg, { }* *CId, \_Isd, \_BR \_and \_PR*).

Note that the uses hierarchy places the existence-dependent relationship upside down. In the corresponding classes in the [metamodel](#), in the uses relationship the used class is placed above the using class, whereas the reverse is true in the logical models. This characterises the decisive difference between the [metamodel](#)'s conceptual way of thinking and the logical models' build-oriented way of thinking. When it comes to making the MedMij Trust Scheme both consistent and long-lasting, it makes sense to place the [metamodel](#) centre-stage in respect of model Maintenance and then to keep the logical models consistent with it. In this way, the [metamodel](#) also ensures that the various logical models remain consistent in the long term too. In fact, the trustworthiness and interoperability that the MedMij Trust Scheme has to deliver is dependent on this consistency.

## Lists

### Logical model



## Logical invariants

Relates to instances of logical class ...	Invariant	Component	Explanatory Note
<i>Subscribe</i>	For each <i>Subscribe</i> <i>a</i> the following applies: <i>a.MaximumDuration</i> <= the maximum duration of <i>Subscriptions</i> on that <i>Information service</i> as stated in the <a href="#">Information service catalogue</a>	<i>Information service directory</i>	A <i>Provider</i> can limit the maximum subscription duration that it offers for a <i>Information Duration</i> , on an <i>Interface Version</i> . Furthermore, it really must remain below the maximum duration that MedMij has stated for that <i>Information service</i> in the <a href="#">Information service catalogue</a>
<i>Subscribe</i>	For each <i>Subscribe</i> <i>a</i> , the following applies: <i>a.SubscriptionEndpointuri</i> combination of <i>s.MedMijNode.ParticipantNode.Node.Hostname</i> and	<i>Information service directory</i>	See the <a href="#">Interface</a> page.

	<i>s.AuthorizationEndpointpath</i> , in accordance with the addressing responsibilities on the <a href="#">Interfaces</a> page.		
<i>AuthorizationEndpoint</i>	For each <i>AuthorizationEndpoint a</i> , the following applies: <i>a.AuthorizationEndpointuri</i> combination of <i>a.MedMijNode.ParticipantNode.Node.Hostname</i> and <i>a.AuthorizationEndpointpath</i> , in accordance with the addressing responsibilities on the <a href="#">Interfaces</a> page.	<i>Information service directory</i>	See the <a href="#">Interfaces</a> page.
<i>Informationservice_Cld</i>	For each <i>Informationservice_Cld g</i> with its corresponding <i>ProviderInformationservice z</i> it is true that: <i>g.InformationserviceId z.Informationservice.InformationserviceId</i>	<i>Information service directory</i>	In this way, the <i>Information service directory</i> inherits the <i>Informationservices</i> of the <i>Information service catalogue</i>
<i>Informationservice_Isd</i>	For each <i>Informationservice_Isd g</i> with its corresponding <i>ProviderInformationservice z</i> it is true that: <i>g.InformationserviceId z.Informationservice.InformationserviceId</i>	<i>Information service directory</i>	In this way, the <i>Information service directory</i> inherits the <i>Informationservices</i> of the <i>Information service catalogue</i>
<i>Information service Names List</i>	There is precisely one instance of this.	<i>Information service Names List</i>	This is a loner in the model.
<i>Interfaceversions_Isd</i>	For each <i>Information service_Cld g1</i> it is true that: IF: <ul style="list-style-type: none"> <li><i>g1.Information services_Cld.Interfaceversion_Cld</i> is the published <i>Interface version</i></li> <li>there is a <i>Subscribe a1</i> so that <i>a1.Informationservice_Cld = g1</i></li> </ul> THEN there is a <i>Informationservice_Isd g2</i> for which the following applies: <ul style="list-style-type: none"> <li><i>g2.InformationserviceID = g1.InformationserviceID</i></li> <li><i>g1.Information services_Cld.Interfaceversie_Cld</i> is the mandatory <i>Interface version</i></li> <li>there is a <i>Subscribe a2</i> so that <i>a2.Information service_Cld = g2</i></li> </ul>	<i>Information service directory</i>	On <i>Information Services</i> which are provided by a <i>Client</i> under the published <i>Interface Version Subscriptions</i> , these are also provided under the mandatory <i>Interface Version Subscriptions</i> .
<i>Interfaceversions_Isd</i>			

	For each <i>Interfaceversions_Isd</i> , <i>Interfaceversion_Isd</i> <i>vi</i> mandatory service and its published <i>Interfaceversion_Isd</i> <i>gi</i> , it is true that IF there is an <i>InformationService_Isd</i> <i>g1</i> for which <i>g1.InformationServices_Isd</i> is true. <i>Interfaceversion_Isd</i> = <i>gi</i> THEN there is an <i>InformationService_Isd</i> <i>g2</i> for which <i>g2.InformationServices_Isd</i> is true. <i>Interfaceversion_Isd</i> = <i>vi</i>	<i>Information service directory</i>	<i>Information Services</i> which are provided by a <i>Provider</i> under the published <i>Interface Version</i> , are also provided under the mandatory <i>Interface Version</i> .
<i>Interfaceversions_Isd</i>	For each <i>InformationService_Isd</i> <i>g1</i> it is true that: IF: <ul style="list-style-type: none"> <li><i>g1.InformationServices_Isd.Interfaceversion_Isd</i> is the published <i>Interfaceversion</i></li> <li>there is a <i>Subscribe a1</i> so that <i>a1.InformationService_Isd</i> = <i>g1</i></li> </ul> THEN there is a <i>InformationService_Isd</i> <i>g2</i> for which the following applies: <ul style="list-style-type: none"> <li><i>g2.InformationServiceID</i> = <i>g1.InformationServiceID</i></li> <li><i>g1.InformationServices_Isd.Interfaceversion_Isd</i> is the mandatory <i>Interface Version</i></li> <li>there is a <i>Subscribe a2</i> so that <i>a2.InformationService_Isd</i> = <i>g2</i></li> </ul>	<i>Information service directory</i>	On <i>Information Services</i> which are provided by a <i>Provider</i> under the published <i>Interface Version Subscriptions</i> , these are also provided under the mandatory <i>Interface Version Subscriptions</i> .
<i>MedMijNode</i>	For each <i>MedMijNode m</i> it is true that: <i>m.Hostname</i> = <i>m.ParticipantNode.Node.Hostname</i>	<i>Whitelist</i>	In this way, the <i>MedMijNode</i> inherits the <i>Hostname</i> of the <i>Node</i> that it is.
<i>MedMijNode</i>	The hostname of a <i>MedMijNode</i> contains a domain name that is a fully-qualified domain name, in accordance with <a href="#">RFC3696, section 2</a> .	<i>Whitelist</i>	This is a measure to combat risk <a href="#">4.4.1.4</a> from RFC 6819.
<i>Client</i>	For each <i>Client o</i> : <i>o.ClientOrganisationname</i> complies with the <a href="#">Client names policy</a> .	<i>Application</i>	See the <a href="#">Clientname policy</a>
<i>Client</i>	For each <i>Client o</i> it is true that: <i>o.Hostname</i> = <i>o.MedMijNode.Hostname</i> .	<i>Clientlist</i>	In this way, the <i>Clientlist</i> inherits the <i>Hostnames</i> of the <i>Nodes</i> .
<i>Clientlist</i>	There is precisely one instance of this.	<i>Clientlist</i>	

			This is a loner in the model.
<i>ResourceEndpoint</i>	For each <i>ResourceEndpoint</i> <i>r</i> it is true that: <i>r.ResourceEndpointuri</i> combination of <i>r.MedMijNode.ParticipantNode.Node.Hostname</i> and <i>r.ResourceEndpointpath</i> , in accordance with the addressing responsibilities on the Interfaces page.	<i>Information service directory</i>	See the <a href="#">Interfaces</a> page.
<i>ResourceNotificationEndpoint</i>	For each <i>ResourceNotificationEndpoint</i> <i>r</i> it is true that: <i>r.ResourceNotificationEndpointuri</i> combination of <i>r.MedMijNode.ParticipantNode.Node.Hostname</i> and <i>r.AuthorizationEndpointpath</i> , in accordance with the addressing responsibilities on the <a href="#">Interfaces</a> page.	<i>Clientlist</i>	See the <a href="#">Interfaces</a> page.
<i>SubscriptionNotificationEndpoint</i>	For each <i>SubscriptionNotificationEndpoint</i> <i>s</i> it is true that: <i>s.SubscriptionNotificationEndpointuri</i> combination of <i>s.MedMijNode.ParticipantNode.Node.Hostname</i> and <i>s.AuthorizationEndpointpath</i> , in accordance with the addressing responsibilities on the <a href="#">Interfaces</a> page.	<i>Clientlist</i>	See the <a href="#">Interfaces</a> page.
<i>System Role</i>	For each <i>SystemRole</i> <i>s</i> with its corresponding <i>ProviderInformationServiceSystemRole</i> <i>z</i> it is true that: <i>s.SystemRoleCode</i> <i>z.SystemRole.SystemRoleCode</i>	<i>Information service directory</i>	In this way, the <i>Information service directory</i> inherits the <i>Systemrolecodes</i> of the <i>Register of Information Standards</i> .
<i>TokenEndpoint</i>	For each <i>TokenEndpoint</i> <i>t</i> it is true that: <i>t.TokenEndpointuri</i> combination of <i>t.MedMijNode.ParticipantNode.Node.Hostname</i> and <i>r.TokenEndpointpath</i> , in accordance with the addressing responsibilities on the Interfaces page.	<i>Information service directory</i>	See the <a href="#">Interfaces</a> page.
<i>Whitelist</i>	There is precisely one instance of this.	<i>Whitelist</i>	This is a loner in the model.
<i>Information service directory</i>	There is precisely one instance of this.	<i>Information service directory</i>	This is a loner in the model.

## Logical basic classes



Basic class	Definition	Origin
<i>Backchanneluri</i>	See addressing responsibilities on the <a href="#">Interfaces</a> page. The domain name is a fully-qualified domain name, in accordance with <a href="#">RFC3696, section 2</a> .	logical model
<i>DateTime</i>	In accordance with the type xs:dateTime, as specified in <a href="#">XML schema 1.0</a> and including a timezone indication.	logical model
<i>Frontchanneluri</i>	See addressing responsibilities on the <a href="#">Interfaces</a> page. The domain name is a fully-qualified domain name, in accordance with <a href="#">RFC3696, section 2</a> .	logical model
<i>InformationserviceId</i>	String of at least one, and a maximum of 30, character(s).	<a href="#">metamodel</a>
<i>Hostname</i>	See addressing responsibilities on the <a href="#">Interfaces</a> page.	<a href="#">metamodel</a>
<i>InterfaceversionId</i>	String of at least one, and a maximum of 30 characters.	<a href="#">metamodel</a>
<i>ClientOrganisationname</i>	In accordance with applicable <a href="#">Client names policy</a> .	<a href="#">metamodel</a>
<i>Positivenumber</i>	A whole number that is not equal to 0.	logical model
<i>Systemrolecode</i>	String of at least one, and a maximum of 30, character(s).	<a href="#">metamodel</a>
<i>Depictionname</i>	String of at least three, and a maximum of 50, characters.	<a href="#">metamodel</a>
<i>Providername</i>	In accordance with applicable <a href="#">Providersnamespolicy [NL]</a>	<a href="#">metamodel</a>

### Link with metamodel

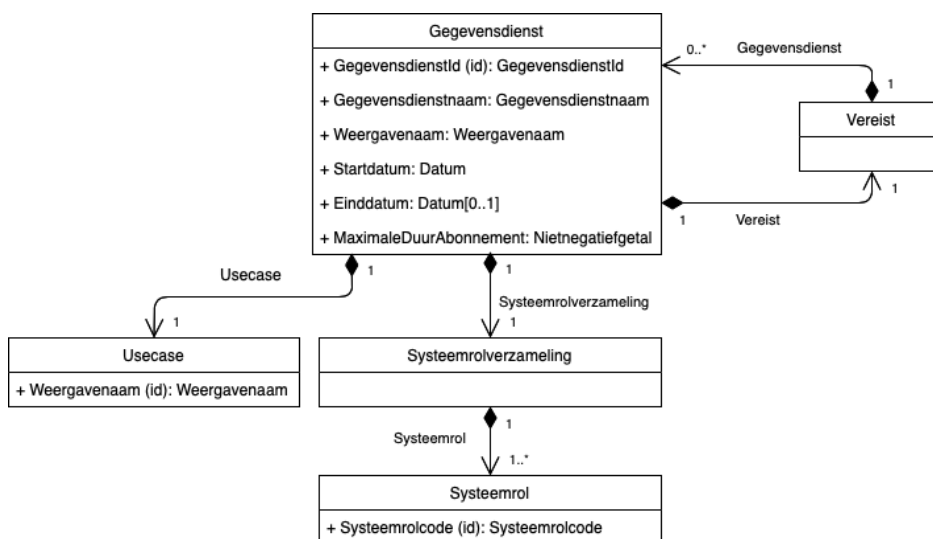
Class in logical model	Origin class in metamodel
<i>Subscribe</i>	<i>CareproviderSubscribeToInformationserviceInterfaceversion</i>
<i>AuthorizationEndpoint</i>	<i>AuthorizationEndpoint</i>
<i>Informationservice_Isg</i>	<i>Information service</i>
<i>Informationservice_Cld</i>	<i>ClientInformationServiceInterfaceversion</i>
<i>Informationservice_Isd</i>	<i>ProviderInformationserviceInterfaceversion</i>
<i>Interfaceversion_Cld</i>	<i>Interfaceversion</i>
<i>Interfaceversion_Isd</i>	<i>Interfaceversion</i>
<i>MedMijNode</i>	<i>MedMijNode</i>
<i>Client</i>	<i>Client</i>
<i>ResourceEndpoint</i>	<i>ResourceEndpoint</i>
<i>ResourceNotificationEndpoint</i>	<i>ResourceNotificationEndpoint</i>
<i>SubscriptionNotificationEndpoint</i>	<i>SubscriptionNotificationEndpoint</i>



System Role	ProviderInformationSystemServiceSystemrole
TokenEndpoint	TokenEndpoint
Provider	Provider

## Information service catalogue

### Logical model



### Logical invariants

Relates to instances of class ...	Invariant	Component	Explanatory Notes	Nature	Origin
Usecase	For each <i>Usecase</i> <i>u</i> it is true that: <i>u.Depictionname</i> = "Collect" OR <i>u.Depictionname</i> = "Share"	Information service catalogue	This links the names of the subclasses to the depiction names.	local dependency	metamodel (with <i>Usecase</i> )

### Logical basic classes

Basic class	Definition	Origin
<i>Date</i>	In accordance with the type <code>xs:date</code> , as specified in <a href="#">XML schema 1.0</a> .	metamodel
<i>InformationserviceId</i>	String of at least one, and a maximum of 30, character(s).	metamodel
<i>Informationservicename</i>	String of at least three, and a maximum of 50, characters.	metamodel
<i>NonNegativeInteger</i>	In accordance with the type <code>xs:nonNegativeInteger</code> , as specified in XML schema 1.0.	metamodel
<i>Systemrolecode</i>	String of at least one, and a maximum of 30, character(s).	metamodel
<i>Depictionname</i>	String of at least three, and a maximum of 50, characters.	metamodel

## Link with metamodel

Class/value in logical model	Origin class in metamodel
<i>Information service</i>	<i>Information service</i>
<i>Usecase</i>	<i>Usecase</i> , <i>CollectUsecase</i> and <i>ShareUsecase</i>

### Explanatory Notes

#### Explanatory Notes

The class *Usecase* is an abstract class in the [metamodel](#). However, concrete classes are needed in the logical model, namely in the composition hierarchy. In the context of the *Information service catalogue*, we are not interested here in the whole semantics of the conceptual classes *CollectUsecase* and *ShareUsecase* but only in their respective instances, with the *Depictionname* that they receive from the abstract class *Usecase*, by means of an invariant. In this logical model, this is why we use a concrete class *Usecase* that instantiates to these two.

## MedMijSystemNode

### Logical model

MedMijStelselNode
+ Hostname: Hostname

### Logical invariants

Relates to instances of class	Invariant	Component	Explanatory Notes	Nature
...				
<i>MedMijSystemNode</i>	For the <i>MedMijSystemNode</i> <i>m</i> it is true that: <i>m.Hostname</i> <i>m.Node.Hostname</i>	<i>MedMijSystemNode</i>	In this way, the <i>MedMijSystemNode</i> , inherits - from the <i>Node</i> that it is - the <i>Hostname</i> .	inheritance

### Logical basic classes

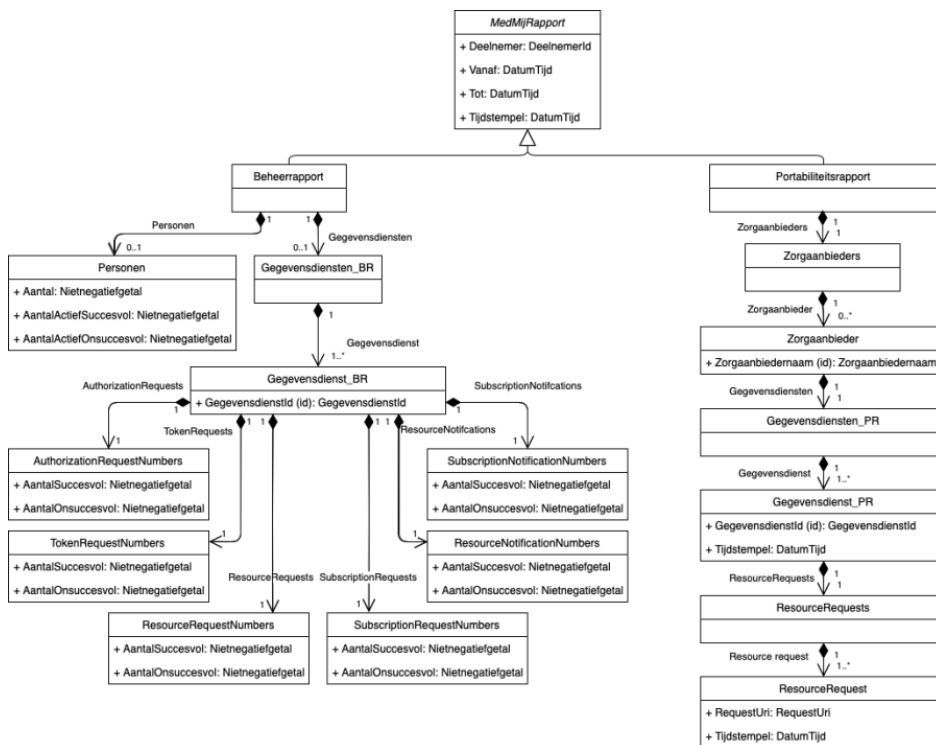
Basic class	Definition	Origin
<i>Hostname</i>	See addressing responsibilities on the Interfaces page.	<a href="#">metamodel</a>

## Link with metamodel

Class in logical model	Origin class in metamodel
<i>MedMijSystemNode</i>	<i>MedMijSystemNode</i>

## Reports

### Logical model



## Logical invariants

Relates to instances of logical class ...	Invariant	Component	Explanatory Notes	Nature	Origin
<i>Maintenance Report</i>	There is precisely one instance of this.	<i>Maintenance Report</i>	This is a loner in the model.	numerical relationship	logical model
<i>Information service_BR</i>	For each <i>Information service_BR</i> $g$ with its corresponding <i>ProviderInformationservice</i> $z$ it is true that: $g$ . <i>InformationserviceId</i> $z$ . <i>Informationservice</i> . <i>InformationserviceId</i>	<i>Maintenance Report</i>	In this way, the <i>Maintenance Report</i> inherits the <i>InformationserviceID</i> s from the <i>Information service catalogue</i> .	inheritance	logical model
<i>Information service_PR</i>	For each <i>Information service_PR</i> $g$ with its corresponding <i>ProviderInformationservice</i> $z$ it is true that: $g$ . <i>InformationserviceId</i> $z$ . <i>Informationservice</i> . <i>InformationserviceId</i>	<i>Portability Report</i>	In this way, the <i>Portability Report</i> inherits the <i>InformationserviceID</i> s from the <i>Information service catalogue</i> .	inheritance	logical model
<i>Portability Report</i>	There is precisely one instance of this.	<i>Portability Report</i>	This is a loner in the model.	numerical relationship	logical model

## Logical basic classes

Basic class	Definition	Origin
<i>DateTime</i>	In accordance with the type <code>xs:dateTime</code> , as specified in <a href="#">XML schema 1.0</a> and including a timezone indication.	logical model
<i>ParticipantId</i>	String of at least one, and a maximum of 30 characters.	<a href="#">metamodel</a>
<i>InformationServiceId</i>	String of at least one, and a maximum of 30, character(s).	<a href="#">metamodel</a>
<i>NonNegativeInteger</i>	In accordance with the type <code>xs:nonNegativeInteger</code> , as specified in XML schema 1.0.	logical model
<i>RequestUri</i>	String of at least twelve, and a maximum of 2048 characters.	<a href="#">metamodel</a>
<i>Providername</i>	In accordance with applicable <a href="#">Providersnamespolicy (NL)</a>	<a href="#">metamodel</a>

## Link with metamodel

Class in logical model	Origin class in metamodel
<i>Information service_BR</i>	<i>Information service</i>
<i>Information service_PR</i>	<i>Information service</i>
<i>ResourceRequest</i>	<i>ResourceRequest</i>
<i>Provider</i>	<i>Provider</i>

## XML schemas

### XML schemas

#### Explanatory Notes

On this page we find the XML schemas of:

- the lists that are made available by *MedMij Maintenance* to *Issuer* and *Publisher* for a range of purposes.
- the reports that *Participants* must be able to deliver.

The XML schemas are an implementation of the [logical models](#) of the lists in XML syntax and accordingly fulfil the role of technical model. XML fits the hierarchical structuring that has already been deployed in the [logical models](#). In addition, XML schemas and XML files are serial in nature. In other words, the translation from the [logical model](#) requires the classes to be placed behind each other without allowing their diagrammatical organisation in the [logical model](#) to disappear. A composition relationship in the logical model becomes a nesting in the XML schema. XML tags are used in order to be able to mutually separate the model elements that have been placed behind each other, both in the XML schema and in the XML instance, and to offer the elements with meta information.

Just like they do on the conceptual level of the [metamodel](#) and on the logical level of the [logical model](#), invariants appear on the technical level too. XML is even able to check some of these invariants automatically. In such XML validation, it is checked whether a certain XML file complies with the structure of a certain XML schema. The MedMij Trust Scheme utilises this feature too by requiring the recipient of the four lists to carry out such a validation. The XML schemas for this are made available as part of the MedMij Trust Scheme. This validation offers additional certainty about the correctness of the distributed lists and in this way helps to improve the reliability of the MedMij network's operation.

All the same, there are still various ways to translate the lists' [logical model](#) into their XML schemas. In the MedMij Trust Scheme, the following considerations have been used in this regard:

- All types and elements that are used for one of the lists or reports are defined in the XML schema of the list or in the report in question. In other words, no use has been made of a basic common sheet. In this way, the dependency between the XML schemas is limited and it becomes easier to modify one of the schemas without having to modify the other schemas too. However, the definitions must continue to fit the [metamodel](#) and the [logical model](#); a modification in one of these models makes it necessary to modify all XML schemas that are affected by this change.
- There are four technical components that are associated with the lists' and reports' [logical model](#). The highest class of each component becomes the root element of the relevant XML schema. The attributes of the above abstract classes (*MedMijMaintenanceList* and *MedMijReport*) are distributed respectively across the technical models of the four lists and the two reports. In other words, for each list or report, there is a separate XML schema. Therefore, the homonymy of Information Service and Information Services is no longer a problem and the suffixes *\_Isd*, *\_Isq*, *\_CId*, *\_BR* and *\_PR* in the names may be omitted.
- Just as in the step from the metamodel to the logical models, the granularity of the classes remains the same. No classes are combined to create a more compact schema.
- Each of the logical classes, apart from the class that serves as the 'root', are defined individually as *complexType* in the XML schema, so that they can be reused within the XML schema.

- Each of the basic classes is defined individually as simpleType in the XML schema so that they can be reused within the XML schema.
- All classes and attributes from the [logical model](#) are modelled as elements in the XML schema. This enables there to be a clear translation of the [logical model](#); no distinction between elements and attributes needs to be applied. Elements offer more options than attributes do, which is why (as a generic choice) they are preferred.
- Where reference is made in the [logical model](#) to 'identifiers', a 'uniqueness constraint' has been included in the XML schema.

## Schemas

List or report	Filename	Release	Version of file
Information service directory	<a href="#">MedMij_Zorgaanbiederslijst.1.2.0.xsd</a>	3	6
Whitelist	<a href="#">MedMij_Whitelist.1.2.0.xsd</a>	2	9
Clientlist	<a href="#">MedMij_OAuthclientlist.1.2.0.xsd</a>	4	7
Information service glossary	<a href="#">MedMij_Gegevensdienstnamenlijst.1.2.0.xsd</a>	1	7
Maintenance Report	<a href="#">MedMij_Beheerrapport.1.2.0.xsd</a>	1	1
Portability Report	<a href="#">MedMij_Portabiliteitsrapport.1.2.0.xsd</a>	1	1

Only the above-mentioned files, with the stated release and version number, may be used in this release of the MedMij Trust Scheme.

### Sample files (XML)

A sample file of each list is available. This file is not part of the official specifications of the MedMij Trust Scheme.

List	Filename	Version of sample file	Belongs to XML schema of the list with release number
Information service directory	<a href="#">MedMij_Zorgaanbiederslijst_example.xml</a>	3	3
Whitelist	<a href="#">MedMij_Whitelist_example.xml</a>	5	2
Clientlist	<a href="#">MedMij_OAuthclientlist_example.xml</a>	5	4
Information service glossary	<a href="#">MedMij_Gegevensdienstnamenlijst_example.xml</a>	2	1
Maintenance Report	<a href="#">MedMij_Beheerrapport_example.xml</a>	1	1
Portability Report	<a href="#">MedMij_Portabiliteitsrapport_example.xml</a>	1	1

## Explanatory Notes

### Time aspect

The [metamodel](#) and the [logical models](#), with their invariants, work "over time". They describe how the classes are related at each moment. However, the XML files for the lists are specific snapshots in time of the classes' instances. This is why a time element must be added to those lists that are generated at different moments, in order to be able to distinguish between them and in order to be able to retrospectively establish a list's validity duration.

- Each XML file has an indication of the version it is. The combination of a Serial number and a Timestamp is used for this. This fulfils three information requirements:
  - When two lists (of the same type) with successive Serial numbers are available then the validity duration of the older list can be established. This helps in the interpretation of audit logs and in error tracking.
  - Lists can be uniquely identified. This can be done using Serial number or Timestamp, whereby human users often find the Serial number to be the most intuitive to use.
  - It can be verified for each list as to when the last change was made. This will usually be a 'functional' change, not an error recovery. By comparing successive versions, this can be used to deduce when the current list was most recently amended; this can be useful when assessing the effects of changes or when error tracking.
- Timestamp consists of Date, Time and Timezone indication, based on the xs:dateTime type. Opting for a native XML datatype simplifies the implementation. However, there is a restriction on the element, which forces a Timezone indication to always be provided.

### Release Maintenance

The filenames of the XML schemas and XML sample files have been chosen such that they do not change if the content of the XML schema changes. This makes it easier to implement changes. It is customary to include meta-information not in the filename but in the XML files themselves (especially in the header). This is why it is not necessary to use - in addition to the information in the file - the filename for version indication too. Each of the XML schemas has its own release numbering. This enables them to be modified independently of each other. This prevents implementation from being an unnecessary burden when a change is made. The release number is a whole number, for reasons of simplicity. Always - but only if - an XML schema is changed is the release number increased by one. The XML schemas are an integral part of the trust scheme. As a result, a change in the XML schemas leads to a new release of the agreements system. However, in the reverse situation it does not need to be the case that a change in the other agreements within the agreements system makes it necessary to change the XML schema. Since a change in an XML schema quickly leads to incompatibility with other versions (note that XML files that are based on different versions of the XML schema will not be validated by the 'other' XML schema), it has been decided to include the release number in the indication of the namespace. This is why an XML file's reference to the namespace also includes the release number. In this way, it is ensured that XML files are not validated using a wrong version of the XML schema. The XML schemas and the sample XML files are also given a version number. The version number is a whole number that is increased by one upon each change in the file. Version numbering is used to distinguish between file versions during the development process. The number is also present in production versions; this makes it unnecessary to modify the XML products when there is a status change to a release of the MedMij Trust Scheme, even if their content has not changed. The version number is included in the file as a comment, because it does not need to be machine-readable and because this creates a clear system for the XML schemas and the XML sample files. The comment has the form: `<!--File version:`

[version number]--> and can be found on the second line of a file. For reasons of simplicity and clarity, the version numbering is independent of the release numbering for the XML schemas.

## Namespaces

An URL is used to indicate namespaces. This is the easiest option because this - unlike with an URN - does not require any namespace registration with IANA. The namespace URL has the following structure: `xmlns://afsprakenstelsel.medmij.nl/[nameList|nameReport]/release[releasenummer]` .

- A namespace URL uses `xmlns://` as the schema indication. This makes it clear that this is merely an identification and that the URL is not intended to be used for dereferencing (for example to download the XML schema).
- The domain `afsprakenstelsel.medmij.nl` is a unique hostname on the Internet. Using it provides both sufficient recognisability and uniqueness
- The `nameList` has one of the following values: Whitelist, Clientlist, Information service directory or Information service glossary.
- The `nameReport` has one of the following values: Maintenance Report or Portability Report.
- The indication `release` is added to make it easier for people to read and hence to improve clarity.

Where the metamodel has not defined any names, for reasons of consistency and elegance we opt to use lowercase for the URL's structure. The following is used here: `elementFormDefault = "qualified"`. This makes the XML schemas easier to read, because no prefixes are needed to define the elements and because it does not impair any functionality. The prefixes for the namespaces are kept as short as possible in order to make the XML schemas easier to read, and always consist of three letters and are entirely in lowercase. The following table shows which prefix is used for which list or report.

List or report	Prefix
<i>Information service glossary</i>	lsg
<i>Clientlist</i>	cld
<i>Whitelist</i>	whl
<i>Information service directory</i>	isd
<i>Maintenance Report</i>	bhr
<i>Portability Report</i>	pbr

## Syntactic options

The XML schemas are based on [XML 1.0|<https://www.w3.org/TR/REC-xml/>] and XML Schema 1.0 (built up from specifications relating to [structure|<https://www.w3.org/TR/xmlschema-1/>] and [data types|<https://www.w3.org/TR/xmlschema-2/>]). These versions provide sufficient functionality and enjoy widespread implementation and support. The filename of a XML schema has the structure `MedMij_[nameList].xsd`. The variable `nameList` relates to one of the following values: Whitelist, Clientlist, Information service directory or Information service glossary. The XML schemas contain the XML Declaration `<?xml version="1.0" encoding="UTF-8"?>`. The presence of a declaration is recommended by [XML 1.0|<https://www.w3.org/TR/xml/#sec-prolog-dtd>]. When using UTF-8, the encoding is optional. However, the encoding is explicit because it prevents potential uncertainty about the intention of or the correct compliance with the specifications. No use is made of the



pseudo-attribute standalone because XML schemas are used instead of DTDs. To make them easier to read, the XML schemas are pretty-printed; readability is further improved by using line breaks and indents. Furthermore, each XML schema uses a standard sequence in its structure:

- The root element, preceded by the comment text `<!--Root element-->`.
- The definition of the logical classes, preceded by the comment text `<!--Logical classes-->`.
- The definition of the basic classes, preceded by the comment text `<!--Basic classes-->`.

There is leeway within them as to the order in which the classes are defined. The uniqueness constraints use `<xs:unique>`. The (mandatory or other) name of uniqueness constraints in XML is built up in line with `Unique_{nameClass}`. In this way, the characteristic of the attribute `Hostname` of the class `MedMijNode` from the `[logical model]/display/MedMijAfsprakenstelsel120/Logische+modellen` to which the whitelist belongs translates into a uniqueness constraint with the name `Unique_MedMijNode`. It is sufficient to have the name of the class (without the hierarchical context), because class names based on the `[logical model]/display/MedMijAfsprakenstelsel120/Logische+modellen` are unique. The name of the attribute does not need to be quoted. The attributes that between them form the identity of a class's instance are depicted in the `[logical model]/display/MedMijAfsprakenstelsel120/Logische+modellen`. Within `<xs:unique>`, only `<xs:selector>` is used for the XPath expression; `<xs:field>` is included (in accordance with the XML specification) but left empty (has the entry `.` (full stop)). This is an easier option than having to provide a criterion for the splitting of the XPath expression between `<xs:selector>` and `<xs:field>`. Use is made of `<xs:sequence>` within all complexTypes, with `<xs:all>` not being used here, because in this way elements can be used more than once. This is a characteristic that is used a great deal; it is inherent to the nature of the lists and is relevant to many of the composition relationships (who do not have any maximum scope for the compilation). The XML schemas do not contain a Byte Order Mark. According to [XML 1.0|<https://www.w3.org/TR/xml/#charencoding>], using a Byte Order mark is optional for UTF-8. [RFC 3629, chapter 6|<https://tools.ietf.org/html/rfc3629#section-6>], argues that the Byte Order Mark must be prohibited where UTF-8 is made mandatory.

## Basic classes

### Explanatory Notes

The definition of the basic classes in the [logical model](#) is translated into simpleTypes in the XML schema, which builds on a native XML data type and which sometimes attaches additional restrictions to it.

Please note that the patterns for *Backchanneluri* and *Frontchanneluri* are identical.

Basic class	Basis (XML data type)	minLength	maxLength	pattern
<i>Backchanneluri</i>	<i>xs:string</i>			<code>https://([a-z0-9])([a-z0-9-])*([a-z0-9])([a-z0-9-])*([a-z0-9])([a-z0-9-])*([a-z0-9])?(/[a-z0-9-])*</code>
<i>DateTime</i>	<i>xs:dateTime</i>			<code>.{20,}</code>
<i>Duration</i>	<i>xsd:duration</i>			
<i>Frontchanneluri</i>	<i>xs:string</i>			<code>https://([a-z0-9])([a-z0-9-])*([a-z0-9])([a-z0-9-])*([a-z0-9])([a-z0-9-])*([a-z0-9])?(/[a-z0-9-])*</code>

<i>InformationServiceId</i>	xs:string	1	30	
<i>Hostname</i>	xs:string			(([a-z0-9])([a-z0-9-])*(\.)+([a-z0-9])([a-z0-9-])*([a-z0-9]))
<i>NonNegativeInteger</i>	xs:nonNegativeInteger			
<i>ClientOrganisationname</i>	xs:string	3	50	
<i>Positivenumber</i>	xs:positiveInteger			
<i>Systemrolecode</i>	xs:string	1	30	
<i>Depictionname</i>	xs:string	3	50	
<i>Providername</i>	xs:string	10	287	([a-z][0-9]{0,4})+((- & \.)?([a-z][0-9]{0,4})+)*@medmij

## XML files for lists

### Explanatory Notes

The XML files that MedMij Maintenance uses to disclose the *Information service directory*, the *Whitelist*, the *Client directory* and the *Information service glossary* comply with certain requirements, so that *Publishing Server*, *Authorization Server* and *MedMijNode* know what they can count on when it comes to the correct processing of these lists.

1. The XML file of the *Information service directory* is called *MedMij\_Providerslist.xml*. The XML file of the *Whitelist* is called *MedMij\_Whitelist.xml*. The XML file of the *Client directory* is called *MedMij\_Clientlist.xml*. The XML file of the *Information service Names List* is called *MedMij\_Informationsservicenameslist.xml*.
2. In the event of a change in one list that leads to renewed publication, the serial number of this list is increased by one.

### Explanatory Notes

The lists' filenames have been chosen such that they do not change if the content of the XML schema changes. This makes it easier to implement changes. It is customary to take meta-information not from the filename but from the XML files themselves (especially from the header). This is why it is not necessary to - in addition to the information in the file - also deploy the filename to indicate the version.

3. The XML files referred to in responsibility 1 utilise a default namespace, this being the namespace in which the matching XML schema is defined, without a prefix.

### Explanatory Notes

The absence of (unnecessary) prefixes benefits readability and prevents a situation where - for the implementation - use is made of namespace indications and prefixes that may change in the future.

4. The XML files referred to in responsibility 1:
  - comply with [XML 1.0](#) and [XML Schema 1.0](#).
  - are pretty-printed (i.e. mandatory use of line breaks and indents).
  - contain the XML Declaration `<?xml version="1.0" encoding="UTF-8"?>`.
  - do not contain a Byte Order Mark.

### Explanatory Notes

These four requirements also apply for the XML schemas that apply to the XML files. Accordingly, for the relevant explanatory notes please refer to those on the page about these [XML schemas](#).

## Grondslagen

De grondslagen beschrijven het fundament waarop de uitwerking van de afspraken in het afsprakenstelsel is gebaseerd.

Allereerst worden de omgeving van en de 'opdracht' aan het afsprakenstelsel geschetst. De [Achtergrond](#) beschrijft de achtergrond en de probleemstelling van het afsprakenstelsel, evenals de keuze voor een vrijwillig en decentraal afsprakenstelsel met dienstverleners. De [Criteria](#) expliciteren waaraan het afsprakenstelsel moet voldoen (randvoorwaarden) en op grond van welke factoren het succes van het afsprakenstelsel wordt afgemeten (doelen).

Vervolgens worden de belangrijkste ontwerpkeuzes benoemd, waarmee het afsprakenstelsel invulling geeft aan de opdracht. De [Principes](#) geven een overzicht van de richtinggevende ontwerpkeuzes. De [Opzet](#) van het afsprakenstelsel geeft aan hoe dit zich doorvertaalt in de werking van de gegevensuitwisseling en doet dat aan de hand van een overzicht van de betrokken rollen, hun verantwoordelijkheid en de interacties tussen de rollen.

Tot slot geeft de [Begrippenlijst](#) de formele definities van begrippen die in de uitwerking van het afsprakenstelsel worden gebruikt.

## Achtergrond

### Groeimodel

De achtergrond beschrijft mede het afsprakenstelsel zoals dat uiteindelijk beoogd is te werken. In de voorliggende release 1.1 van het afsprakenstelsel worden nog niet alle functionaliteiten aangeboden. De [Release- en versiebeschrijving](#) geeft een overzicht van de inhoud van voorliggende van het MedMij Afsprakenstelsel.

### Doel

De achtergrond beschrijft welke problematiek met het afsprakenstelsel moet worden opgelost en waarom is gekozen voor een afsprakenstelsel als oplossing.

Het programma MedMij streeft ernaar dat persoonlijke gezondheidsomgevingen een prominente plek gaan innemen in de Nederlandse zorg. In 2020 moet een kritische massa zijn bereikt voor wat betreft gebruik en aanbod van persoonlijke gezondheidsomgevingen onder zorgaanbieders, patiënten of personen in het algemeen en leveranciers van de technische oplossingen.

De persoonlijke gezondheidsomgeving geeft de mogelijkheid tot regie over de eigen gezondheid en over het delen van gegevens. Het biedt rust, vertrouwen en inzicht doordat een goed beeld ontstaat van hoe de persoonlijke gezondheid zich ontwikkelt en wat de persoon eraan kan doen om die te verbeteren. Het gebruik van een persoonlijke gezondheidsomgeving kan tevens de professional helpen om de juiste en beste zorg en ondersteuning te leveren. Het biedt ook kansen voor efficiëntere besteding van de tijd van zowel de professional als van de persoon. De persoonlijke context komt met het gebruik van een persoonlijke gezondheidsomgeving beter tot zijn recht. Ook kunnen professionals eenvoudiger toegang krijgen tot relevante informatie die gedeeld wordt door de persoon. Mensen zijn zelf beter geïnformeerd. Dit bevordert de samenwerking en communicatie tussen professionals en de persoon: zij worden meer en meer partners in gezondheid.

Het programma bevordert de opkomst van persoonlijke gezondheidsomgevingen door gericht barrières weg te nemen die de ontwikkeling en het gebruik in de weg staan en randvoorwaarden te stellen aan de kwaliteit en rechtmatigheid. Op dit moment wordt het potentieel van persoonlijke gezondheidsomgevingen onderbenut. Personen en zorgaanbieders hebben nog onvoldoende vertrouwen in elektronische gegevensuitwisseling en hebben weinig ervaring op kunnen doen met het concept. Leveranciers van ict-oplossingen zijn op hun beurt terughoudend met investeringen zolang personen en zorgaanbieders geen vraag articuleren; daarbovenop zijn er vraagstukken rond interoperabiliteit en authenticatie. Het programma zet in op een afsprakenstelsel en heeft daarvoor het label MedMij gelanceerd.

## De persoonlijke gezondheidsomgeving

Patiëntenfederatie Nederland hanteert de volgende definitie van een persoonlijke gezondheidsomgeving:

### Definitie persoonlijke gezondheidsomgeving

Een persoonlijk gezondheidsdossier (PGD):

- Is een universeel toegankelijk, voor leken begrijpelijk, gebruiksvriendelijk en levenslang hulpmiddel om relevante gezondheidsinformatie te verzamelen, te beheren en te delen, en

om regie te kunnen nemen over gezondheid en zorg en om zelfmanagement te ondersteunen via gestandaardiseerde gegevensverzamelingen voor gezondheidsinformatie en geïntegreerde digitale zorgdiensten.

- Wordt beheerd en/of gedeeld door de patiënt of zijn wettelijke vertegenwoordiger.
- Is op zo danige wijze beveiligd dat de vertrouwelijkheid van gezondheidsgegevens en de privacy van de gebruiker worden beschermd.
- Is geen wettelijk medisch dossier, tenzij aldus gedefinieerd en daarom onderworpen aan wettelijke beperkingen.

Bron: Bierma, L. & Heldoorn, M. (2013), *Het persoonlijk gezondheidsdossier - De visie van patiëntenfederatie NPCF*.

Een persoonlijke gezondheidsomgeving is daarmee een digitale omgeving die je in staat stelt om al je relevante gezondheidsgegevens, die verspreid staan opgeslagen bij professionals, zorginstellingen en overheden, overzichtelijk en veilig in te zien, aan te vullen met eigen metingen en te delen met wie je dat wilt. Inhoudelijke functionaliteiten, bijvoorbeeld in de vorm van digitale zorgdiensten, zijn optioneel en zullen per individu verschillen op basis van persoonlijke behoefte en situatie. Een persoon moet daarbij kunnen kiezen voor één persoonlijke gezondheidsomgeving en niet gedwongen worden meerdere omgevingen bij te houden. Leveranciers van persoonlijke gezondheidsomgevingen maken gebruik van informatie uit achterliggende systemen van zorgaanbieders en kunnen via hun persoonlijke gezondheidsomgeving waarde toevoegen aan die gegevens met behulp van digitale zorgdiensten. Ook zullen er aanbieders van losse functionaliteit zijn, zoals van mobiele apps, die via het MedMij Afsprakenstelsel gegevens kunnen uitwisselen.

Grip op je eigen gezondheidsgegevens en toegang tot digitale functionaliteit stellen je in staat op je zelfgekozen manier aan je eigen gezondheid te werken en je zorgproces te laten ondersteunen.

## Huidige situatie

Het aanbod en gebruik van persoonlijke gezondheidsomgevingen komen moeizaam op gang. De voordelen van persoonlijke gezondheidsomgevingen, als middelen die de persoon in staat stellen regie over het zorgproces te nemen en zelfmanagement toe te passen, blijven daardoor grotendeels uit. De doelstelling van het programma MedMij om in 2020 een kritische massa bereikt te hebben, zal niet worden gerealiseerd zonder ingrijpen.

De ontwikkeling van persoonlijke gezondheidsomgevingen wordt gehinderd door een aantal barrières, die spelen bij personen, zorgaanbieders en de leveranciers van de persoonlijke gezondheidsomgevingen. We benoemen de belangrijkste daarvan.

Personen – al dan niet reeds patiënt – hebben niet altijd voldoende vertrouwen om gevoelige gegevens over hun gezondheid te delen met andere partijen dan de zorgaanbieder zelf, zoals leveranciers van persoonlijke gezondheidsomgevingen. De bestaande wet- en regelgeving die eisen stelt aan de omgang met persoonsgegevens gaat nog uit van medische dossiers die beheerd worden door zorgaanbieders met een medisch beroepsgeheim en niet van persoonlijke gezondheidsomgevingen waarbij personen zelf individuele afwegingen maken over het wel of niet willen gebruiken van een persoonlijke gezondheidsomgeving. De waarborgen die nodig zijn om hun relatief kwetsbare positie te beschermen zijn nog onvoldoende aanwezig; zo is er bijvoorbeeld geen patiëntgeheim naar analogie met het medisch beroepsgeheim van zorgaanbieders.

Zorgaanbieders ervaren eveneens terughoudendheid bij het delen van gegevens over patiënten via persoonlijke gezondheidsomgevingen van veelal andere ict-leveranciers en organisaties. Juist doordat zij zijn gehouden aan het medisch beroepsgeheim, willen zij zeker weten dat de gegevens alleen bij de patiënt zelf (of een gemachtigde) terechtkomen. Ook willen zij zekerheid over de vraag in welke mate zij aansprakelijk gesteld kunnen worden bij medische schade die het gevolg is van informatie uit persoonlijke gezondheidsomgevingen. Verder speelt dat de technische en organisatorische complexiteit van veel initiatieven rond elektronische dossiers niet bijdragen aan het vertrouwen in de bescherming van gegevens. Daarnaast speelt bij zorgaanbieders onzekerheid over de te kiezen oplossing voor hun interactie met

persoonlijke gezondheidsomgevingen; er zijn verschillende niet-gestandaardiseerde oplossingen denkbaar die geen van alle (nog) in staat zijn alle patiënten te bereiken. De vrees voor een lock-in of relatief hoge investeringen in de verkeerde oplossing leidt tot conservatief gedrag en een keuze voor oplossingen die vaak niet verder komen dan een aan de zorgaanbieder zelf verbonden digitale gezondheidsomgeving. Tot slot is er onduidelijkheid over de financiering van functionaliteiten en randvoorwaardelijke diensten rond de persoonlijke gezondheidsomgevingen. Het is niet helder op welke wijze investeringen door zorgaanbieders worden terugverdiend, hetzij doordat afzonderlijk wordt betaald voor informatiediensten, hetzij als component in de bekostiging van zorgproducten.

Voor de leveranciers van persoonlijke gezondheidsomgevingen speelt net zo goed onzekerheid over interoperabiliteit. Bij gebrek aan standaardisatie zijn veel investeringskeuzes risicovol, terwijl het daarbij niet gaat om verschillen waar de patiënt iets van zal merken. Het zijn veeleer keuzes van het type 'rijden we links of rechts op de weg?'. Hoe meer partijen 'op dezelfde weg rijden', hoe groter het effect van een investering in de gestandaardiseerde optie. In termen van persoonlijke gezondheidsomgevingen betekent dit dat zoveel mogelijk zorginformatie kan worden ontsloten met dezelfde oplossing. Leveranciers van zorginformatiesystemen zien interoperabiliteit soms juist als bedreiging voor huidig marktaandeel, in plaats van als een kans voor vergroting ervan. Naast interoperabiliteitsvraagstukken spelen ook onzekerheden over de mogelijkheid om te voldoen aan de wettelijke eisen rond privacy. Zo zijn er nauwelijks generieke authenticatievoorzieningen beschikbaar die voldoende sterk zijn om omgevingen met persoonlijke gezondheidsinformatie te beveiligen. Ten slotte is voor leveranciers onduidelijk wie de financier en wie de klant is van diensten rond een persoonlijke gezondheidsomgeving.

Voor alle partijen geldt dat de afwezigheid van standaardisatie zich niet beperkt tot technische afspraken of ict alleen. Ook de variëteit die zich voordoet aan afspraken (of het gebrek daaraan) rond privacy, beveiliging, besturing, toezicht, handhaving, financiering, communicatie en dergelijke is een belemmering. Het many-to-many-kenmerk van de beoogde gegevensuitwisseling - een veelheid aan personen wisselt met behulp van een veelheid aan leveranciers gegevens uit met een veelheid aan zorgaanbieders - vereist een stevige standaardisatie, omdat het anders vrijwel onmogelijk is om een voor personen en zorgaanbieders werkbaar en maatschappelijk betaalbare gegevensuitwisseling van de grond te krijgen.

De barrières bij personen, zorgaanbieders en leveranciers hebben een blokkerend effect op elkaar. Als vraag ontbreekt komt ook het aanbod niet van de grond, en vice versa. Er is sprake van een nog nauwelijks bestaande tweezijdige 'markt' die pas op gang komt als er een significante eerste stap wordt gezet door een van de spelers. De sleutel ligt bij het beïnvloeden van de karakteristieken van het aanbod, omdat daarmee zowel de barrières bij de aanbieders (zorgaanbieders en softwareleveranciers) als die bij personen kunnen worden geslecht.

## Wat is er nodig om de barrières te overwinnen?

Personen zullen vertrouwen krijgen in persoonlijke gezondheidsomgevingen als zij zekerheid verkrijgen over de betrouwbaarheid van hun gegevens. Transparantie – zien dat aan normen wordt voldaan – en reële aansprakelijkheid – toegankelijke verhaalsmogelijkheden als er toch schade ontstaat – zijn daarbij cruciaal. Deze combinatie zorgt ervoor dat papieren normen ook in de praktijk worden nageleefd.

Voor zorgaanbieders is van het belang dat het mogelijk is om personen betrouwbaar online te authenticeren, zodat vertrouwen ontstaat in het verstrekken van gegevens aan de juiste persoon. Voor aanbieders van persoonlijke gezondheidsomgevingen is het daarbij van belang dat er ook generieke authenticatiemogelijkheden beschikbaar zijn; het gaat om oplossingen die niet afhankelijk zijn van de specifieke ict-partij of zorgaanbieder, maar die tegen geringe kosten het gewenste hoge niveau van betrouwbaarheid bieden.

Interoperabiliteit is zowel voor zorgaanbieders als ict-leveranciers van groot belang om de risico's van investeringen te verkleinen en voor een positief netwerkeffect te zorgen, waarbij zoveel mogelijk personen, ict-oplossingen en zorgaanbieders met elkaar worden verbonden. Dit vergroot de mogelijkheden tot kwalitatief betere en veiligere zorgverlening. De gegevensuitwisseling moet dan wel met zekerheid veilig zijn



en de privacy van betrokkenen voldoende beschermen. Onzekerheid over de financiering kan worden opgelost met een financieringsstructuur waarin duidelijk is welk type partijen bereid is waarvoor te betalen.

## Welke opties zijn er om de barrières te overwinnen?

Om de eerdergenoemde barrières te overwinnen is een interventie nodig. De vorm van deze interventie kent vier opties:

1. Veelal wordt wetgeving ingezet als manier om collectieve belangen te borgen en eisen te stellen aan het gedrag van partijen op een markt. Ook in het domein van persoonlijke gezondheidsomgevingen is al veel generieke wetgeving van kracht en wordt op afzienbare termijn verdere aanscherping voorzien, onder andere door de Europese Algemene Verordening Gegevensbescherming. Voor de aanvullende interventies die specifiek betrekking hebben op persoonlijke gezondheidsomgevingen, zoals de hiervoor genoemde vraagstukken rond het ontbreken van een 'patiëntgeheim' en vraagstukken rond aansprakelijk kan de wenselijkheid van mogelijke wet- en regelgeving worden verkend. Er is echter nog weinig ervaring opgedaan met een succesvolle markt voor persoonlijke gezondheidsomgevingen, waardoor het verstandig is om voorlopig behoedzaam te zijn met wet- en regelgeving zodat voldoende flexibiliteit blijft bestaan. Wetgeving heeft als nadeel dat de doorlooptijd lang is, wat maakt dat het instrument vooral geschikt is als de gewenste richting al uitgekristalliseerd is.
2. Partijen als zorgaanbieders en eventueel zorgverzekeraars kunnen de markt ook stimuleren door hun inkoopmacht te gebruiken. Artsen schrijven nu soms ook al apps voor. Als er voldoende vragers op de markt zijn die hetzelfde kader hanteren, stimuleren zij daarmee andere partijen om hun normen over te nemen. Dit model vereist dat de vragende partijen hun wensen goed kunnen formuleren en ook bereid zijn om aanzienlijk te investeren. Op dit moment zijn de kaders voor een persoonlijke gezondheidsomgeving echter nog niet helder genoeg en kennen zorgaanbieders nog belemmeringen bij de uitwisseling ermee, waaronder juridische vraagstukken en andere zoals eerder genoemd.
3. Een model dat in het verleden veel is gehanteerd, is dat van centraal aangeboden voorzieningen. Door vanuit de overheid of andere dominante partijen zoals zorgverzekeraars een infrastructuur aan te bieden, worden veel keuzes op collectief niveau gemaakt en conformeren deelnemers zich als vanzelf. Voor persoonlijke gezondheidsomgevingen is dit model minder voor de hand liggend. Het concept van persoonlijke gezondheidsomgevingen is nog pril, en een duidelijke keuze voor een specifieke randvoorwaardelijke oplossing kan innovatie in de weg staan. Voor de aansluiting van zorgaanbieders geldt dat er al verschillende decentrale oplossingen bestaan. Een decentraal model sluit daarmee goed aan bij de ervaringen die de sector de afgelopen jaren heeft opgedaan met het ontsluiten van gezondheidsinformatie en maakt hergebruik van instituties en investeringen. Daarbovenop speelt dat er in de zorgsector weinig animo lijkt te zijn voor een centrale voorziening, mede vanwege politieke standpunten. Een keuze voor een centrale voorziening zal daarmee minder vertrouwen genieten, naast het feit dat met een dergelijke oplossing een potentieel single point of failure wordt geïntroduceerd.
4. De optie voor vrijwillige afspraken resteert. Deze afspraken zullen al snel de vorm krijgen van een afsprakenstelsel, omdat er tussen verschillende typen actoren verschillende typen afspraken nodig zijn. Vrijwillige afspraken hebben als kenmerk dat toe- en uittreding (onder voorwaarden) vrijwillig is. Wil een afsprakenstelsel effectief zijn, dan zal het zowel normstellend moeten zijn – in staat om de barrières te overwinnen – als aantrekkelijk genoeg voor partijen om zich aan te willen conformeren.

## Wat zijn kenmerken van een goed afsprakenstelsel?

Om tot een goed afsprakenstelsel voor gegevensuitwisseling met persoonlijke gezondheidsomgevingen te komen, loont het om naar voorbeelden in andere sectoren te kijken waar afspraken zijn gemaakt die barrières rond vertrouwen en interoperabiliteit wegnemen, onder waarborging van collectieve belangen. De afspraken hebben een wisselende mate van vrijwilligheid; veelal zijn afspraken eerst ontstaan in een vrijwillig kader en later verplichtend opgelegd. In onder andere de rechtspraak, het financiële systeem en rond elektronische identiteiten is veel ervaring opgedaan met stelsels van samenhangende afspraken. Enkele gemeenschappelijke kenmerken komen in al deze sectoren terug en kunnen als uitgangspunt dienen voor het MedMij Afsprakenstelsel.



De afspraken richten zich vrijwel altijd op professionele partijen, vaak intermediairs die optreden namens burgers of consumenten. De burgers zelf worden in hoge mate ontzorgd. Er is vaak sprake van professionele partijen die de interactie tussen twee partijen bevorderen. Een debiteur en een crediteur, een gedaagde en een eiser of een webwinkel en een klant maken gebruik van dienstverleners die de ingewikkelde uitvoering van de gewenste interactie mogelijk maken. Geld overmaken is voor de betaler en de ontvanger relatief gemakkelijk; banken handelen het ingewikkelde betalingsverkeer af voor hun klanten. Dat geldt ook voor het starten van een juridische procedure; advocaten en andere spelers in het rechtssysteem hanteren complexe procedures die gericht zijn op het bereiken van doelen voor hun cliënten. In deze sectoren is sprake van zakelijke dienstverlening door professionele partijen die onderling in een ander spel verwickeld zijn dan degenen die zij vertegenwoordigen. Ook bij persoonlijke gezondheidsomgevingen is een dergelijk model voorzienbaar; het zijn immers niet de persoon en de zorgaanbieder zelf die de daadwerkelijke informatie-uitwisseling op zich nemen, maar aanbieders van ict-oplossingen.

Afspraken die worden gemaakt in stelsels met intermediaire dienstverleners richten zich veelal op twee niveaus. Allereerst worden regels gesteld voor de relatie tussen de vertegenwoordiger (dienstverlener) en de vertegenwoordigde. Dit zijn tamelijk statische afspraken die zich richten op het waarborgen dat de vertegenwoordiger de belangen van de vertegenwoordigde voldoende kan dienen. Zij gaan over zaken als transparantie, het voorkomen van belangenverstrengeling, het voldoen aan professionele normen, klacht- en verhaalsmogelijkheden, de redelijkheid van commerciële bepalingen, vertrouwelijkheid en het kunnen overstappen naar concurrenten. Deze afspraken dragen bij aan het vertrouwen van de uiteindelijke gebruiker, die wordt gecompenseerd voor de kennisvoorsprong van de professionele dienstverlener. Het verlaagt ook de transactiekosten en draagt bij aan een gezonde mededinging.

Daarnaast bestaat een afspraken domein tussen de dienstverleners onderling. Dit zijn veel dynamischer afspraken die vooral gaan over de werkwijzen; dergelijke afspraken zijn dan ook niet technologie-neutraal. De professionele afspraken gaan over onderwerpen zoals procedures, informatieverplichtingen, de inhoud van professionele kwaliteitsnormen, certificering, technische en organisatorische toelatingseisen en onderlinge garantstelling. Ook deze afspraken zijn gericht op het verlagen van de transactiekosten, het bevorderen van de mededinging en dienen uiteindelijk het vertrouwen van de persoon. De inhoud van de afspraken is voor de afnemer van de diensten echter moeilijk toetsbaar; het is een discours van vakgenoten onderling.

Voor elk afsprakenstelsel geldt dat een goede besturing ervan op de inzet, doorontwikkeling, beheer en het controleren van de afspraken een randvoorwaarde is. Daarin dient een heldere vertegenwoordiging van de betrokken partijen geregeld te zijn en moet de inbreng en besluitvorming transparant en open toegankelijk zijn. Voor vertrouwen in het stelsel is duidelijk toezicht ook noodzakelijk. De overheid kan in de besturing en het toezicht verschillende rollen en mate van invloed uitoefenen.

## Waarom zou een partij toetreden tot een afsprakenstelsel?

Wanneer de normen tot stand komen in een vrijwillig stelsel, kunnen de professionele partijen (dienstverleners en eventueel zorgaanbieders) er zelf voor kiezen om wel of niet deel te nemen. Uiteraard is het wenselijk dat genoeg serieuze partijen deelnemen aan het afsprakenstelsel, omdat alleen dan een functionerende markt voor persoonlijke gezondheidsomgevingen zal ontstaan én het afsprakenstelsel dan niet gedomineerd kan worden door een handvol partijen. Deelnemende partijen zullen invloed moeten hebben op de afspraken, zodat er vertrouwen ontstaat in het realiteitsgehalte van de afspraken en het tempo van de doorontwikkeling. De kwaliteit en de continuïteit van de afspraken is daarbij ook van belang. Deelname moet ook voldoende voordelen bieden voor degenen die er moeite in steken; dit kan de vorm krijgen van kansen in de marketing, kennisvoordelen of in de operationele efficiëntie. Ook partijen die niet deelnemen aan het stelsel (free-riders) kunnen voordelen ondervinden van het ontstaan van een markt, maar het moet voor een serieuze partij aantrekkelijker blijven om wel te participeren in MedMij dan om alleen te profiteren van de beweging van anderen.

Om de deelname van partijen te bevorderen is het zowel nodig om de aard van de afspraken af te stemmen op de potentiële deelnemers, als om de governance zodanig in te richten dat de belangen van deelnemers doorlopend goed worden geborgd en er voorspelbaarheid en vertrouwen kunnen ontstaan.

## Doel en scope van het MedMij Afsprakenstelsel

Het MedMij Afsprakenstelsel draagt eraan bij dat persoonsgebonden, gevoelige en vertrouwelijke gegevens op een veilige en gebruiksvriendelijke wijze uitgewisseld kunnen worden tussen persoonlijke gezondheidsomgevingen enerzijds en anderzijds zorgaanbieders (in eerste instantie), overheden en andere partijen (in een latere fase) die over relevante gezondheidsgegevens beschikken. De uitwisseling geschiedt in twee richtingen; personen kunnen gegevens ophalen en delen.

MedMij streeft naar het realiseren van interoperabiliteit voor het uitwisselen van persoonlijke gezondheidsgegevens tussen personen en zorgaanbieders. Hiertoe wordt een afsprakenstelsel overeengekomen, bestaande uit afspraken op juridisch, organisatorisch, financieel, communicatief, semantisch en technisch gebied, zodat personen en zorgaanbieders op een veilige manier gegevens kunnen uitwisselen. Partijen die deelnemen aan het MedMij Afsprakenstelsel committeren zich aan de afspraken, en kunnen diensten aanbieden op basis van de reeds overeengekomen afspraken.

Het afsprakenstelsel gaat uit van *centraal vertrouwen en decentrale operatie*. Het afsprakenstelsel is een bewust gecreëerde verzameling instituties die waarborgen biedt voor een faire omgang met de belangen van de verschillende stakeholders. Bij de uitwisseling van gegevens via het MedMij-netwerk wordt echter uitgegaan van decentrale technische voorzieningen.

## De waarde van het MedMij Afsprakenstelsel voor de persoon en zijn of haar persoonlijke gezondheidsomgeving

Door een persoonlijke gezondheidsomgeving te gebruiken die het MedMij-label draagt, kan een persoon erop vertrouwen, dat deze deelneemt aan het MedMij-netwerk en op een veilige manier gegevens kan uitwisselen met zorgaanbieders. Voorwaarden opgelegd vanuit het MedMij Afsprakenstelsel borgen dat een persoonlijke gezondheidsomgeving met het MedMij-label op een veilige manier omgaat met gegevens. Het kan daarmee voorkomen dat er apps of omgevingen zijn die niet kunnen of mogen werken via het MedMij Afsprakenstelsel.

Een persoonlijke gezondheidsomgeving met het MedMij-label is een waarborg voor betrouwbare grip op je gezondheidsgegevens. En dat biedt toegevoegde waarde voor de persoon. MedMij zegt dus iets over integriteit, validiteit, actualiteit en interoperabiliteit, maar niet over de inhoudelijke functionaliteit. Het gebruik van aanvullende functionaliteit stelt mensen in staat om gezonder te leven en actiever bij te dragen aan een behandeling.

De inrichting van een persoonlijke gezondheidsomgeving zal net zo gepersonaliseerd zijn met aanvullende functionaliteiten als een smartphone dat is met apps. Mensen zullen zelf de functionaliteiten en apps gebruiken en kiezen die zij goed vinden. Op die manier wordt ingespeeld op de behoefte van de persoon via marktwerking. MedMij zegt om deze redenen niets over inhoudelijke functionaliteit en apps. Dat kan veranderen onder invloed van de verdere afspraken tussen persoon, zorgaanbieders, overheid en leveranciers over hetgeen pre concurrentieel en/of standaard gegarandeerd moet zijn voor de persoon in het MedMij Afsprakenstelsel.

## Criteria

### Doel

Criteria geven aan langs welke meetlat het succes van het afsprakenstelsel kan worden afgemeten. Criteria bestaan uit doelen (factoren waarbij gestreefd wordt naar een zo hoog mogelijke score, waarbij afwegingen tussen de doelen kunnen bestaan) en randvoorwaarden (niet-onderhandelbare eisen). De totstandkoming van het stelsel (het ontwerp- en beheerproces) en de inhoud van de afspraken zijn verweven; doelen kunnen dan ook betrekking hebben op beide aspecten. De nummering impliceert geen prioritering.

## Doelen

Nr.	Titel
<b>D1</b>	<b>Creëren van vertrouwen bij personen en zorgaanbieders in gegevensuitwisseling</b>
D1a	Vertrouwelijkheid van persoonsgegevens
D1b	Duidelijkheid over aansprakelijkheid voor gegevensverwerkingen
D1c	Transparantie over voldoen aan normen
D1d	Betrouwbare en veilige authenticatie
D1e	Duidelijkheid over toezicht en handhaving
D1f	Helderheid over de rol van de overheid
<b>D2</b>	<b>Interoperabiliteit van gegevensuitwisseling</b>
D2a	Beschikbaarheid van generieke authenticatie-oplossingen
D2b	Duidelijkheid van de voorgeschreven standaarden
D2c	Volledigheid van de voorgeschreven standaarden
D2d	Implementatiegemak van de voorgeschreven standaarden
D2e	Aanpasbaarheid van voorgeschreven standaarden in toekomst
D2f	Implementatiegemak bij aanpassingen in de toekomst
<b>D3</b>	<b>Creëren van een tweezijdige markt met de juiste innovatie- en kwaliteitsprikkel en voldoende keuzemogelijkheden</b>
D3a	Reële marktwerking voor dienstverlening in het persoonsdomein
D3b	Reële marktwerking voor dienstverlening in het zorgaanbiedersdomein
D3c	Vertrouwen in de toekomstbestendigheid van het afsprakenstelsel
D3d	Duidelijkheid over businessmodellen
<b>D4</b>	<b>Gebruiksvriendelijkheid</b>

D4a	Begrijpelijkheid en snelheid van de interacties rond gegevensuitwisseling
D4b	Begrijpelijkheid en snelheid van het initieel starten met MedMij voor de persoon
D4c	Universele toegankelijkheid van de interacties rond gegevensuitwisseling
<b>D5</b>	<b>Snelheid van implementatie door dienstverleners</b>
<b>D6</b>	<b>Toekomstvastheid van de oplossing</b>
D6a	Strategische flexibiliteit voor de uitwisseling met nieuwe domeinen
D6b	Strategische flexibiliteit voor het gebruik van nieuwe informatiestandaarden
D6c	Duidelijkheid over de governance op langere termijn
D6d	Schaalbaarheid bij grote aantallen gebruikers
D6e	Schaalbaarheid bij grote datavolumes
D6f	Schaalbaarheid bij hoogfrequente uitwisselingen
D6g	Schaalbaarheid bij grote aantallen deelnemers
<b>D7</b>	<b>Compatibiliteit met zoveel mogelijk gewenste kenmerken van een persoonlijke gezondheidsomgeving</b>
D7a	Mogelijkheden om de wettelijke vertegenwoordiger van de patiënt gegevens te laten verzamelen of delen via de persoonlijke gezondheidsomgeving
D7b	Mogelijkheden voor het verzamelen van relevante gezondheidsinformatie
D7c	Mogelijkheden voor het delen van relevante gezondheidsinformatie
D7d	Mogelijkheden voor het voeren van regie over gezondheid en zorg
D7e	Mogelijkheden voor het ondersteunen van zelfmanagement
<b>D8</b>	<b>Betaalbaarheid</b>

### Regie over gezondheid versus zelfmanagement

In doelstelling 7 wordt gesproken over zowel regie op gezondheid als over zelfmanagement. Deze begrippen hebben een verschillende betekenis.

*"Regie over gezondheid gaat in de eerste plaats over gezond blijven."*

Bron: Bierma, L. & Heldoorn, M. (2013), [Het persoonlijk gezondheidsdossier - De visie van patiëntenfederatie NPCF](#).

*"Het individuele vermogen om goed om te gaan met symptomen, behandeling, lichamelijke en sociale consequenties van de chronische aandoening en de bijbehorende aanpassingen in leefstijl. **Zelfmanagement** is effectief wanneer*

*mensen in staat zijn zelf hun gezondheidstoestand te monitoren en de cognitieve, gedragsmatige en emotionele reacties te vertonen die bijdragen aan een bevredigende kwaliteit van leven.”*

Bron: NPCF (2009), Zelfmanagement 2.0 - [over zelfmanagement van de patiënt en wat eHealth daaraan kan bijdragen.](#)

## Randvoorwaarden

Nr.	Titel	Toelichting
<b>R1</b>	<b>Voldoen aan actuele wet- en regelgeving</b>	De uitvoering van de afspraken zal op elk moment in lijn moeten zijn met de Nederlandse wet- en regelgeving. Daarom moet het afsprakenstelsel zo zijn opgezet dat partijen die betrokken zijn bij de uitvoering ervan in staat worden gesteld te voldoen aan deze wet- en regelgeving; dit betekent vooral dat een goede uitvoering van het afsprakenstelsel niet mag vereisen dat partijen afwijken van wet- en regelgeving.
R1a	Voldoen aan Algemene Verordening Gegevensbescherming	De opzet van het afsprakenstelsel dient aan te sluiten bij de Algemene Verordening Gegevensbescherming en daarvan afgeleide wet- en regelgeving.
R1b	Voldoen aan zorgwetgeving	De opzet van het afsprakenstelsel dient aan te sluiten bij gezondheidsrechtelijke wetgeving.
R1c	Voldoen aan mededingingswetgeving	De opzet van het afsprakenstelsel mag niet in strijd zijn met mededingingswetgeving. Dit behelst onder andere dat de toegang van deelnemers niet-discriminatoir moet zijn.
R1d	Voldoen aan overige wet- en regelgeving	De opzet van het afsprakenstelsel is conform overige relevante wet- en regelgeving.
<b>R2</b>	<b>Snelle oplevering van een eerste werkende versie van het afsprakenstelsel en het MedMij-netwerk</b>	Er is grote behoefte aan het mogelijk maken van gegevensuitwisseling tussen personen en zorgaanbieders. Wanneer het afsprakenstelsel niet snel genoeg beschikbaar is en baten kan opleveren, ontstaat het gevaar dat partijen alternatieve oplossingen kiezen waarmee fragmentatie ontstaat en een deel van de beoogde baten uitblijft.
<b>R3</b>	<b>Verbinden van meerdere domeinen</b>	<p>Gezondheid en gezondheidsgegevens betreft alle aspecten van het leven en gaat niet alleen over gezond zijn of ziek zijn. Gezondheid gaat ook over bewust leven, over het verkrijgen van hulp, over zelfmanagement, over mantelzorg en over langdurige zorg en ondersteuning bij het ouder worden en voor het leven met een handicap.</p> <p>Het verzamelen van relevante gezondheidsgegevens betekent dan ook meer voor een persoonlijke gezondheidsomgeving dan alleen gegevens verzamelen vanuit de professionele curatieve zorg.</p> <p>Het afsprakenstelsel hoeft niet vanaf de start meerdere domeinen te verbinden, maar de fundamentele keuzes moeten het wel mogelijk maken om in de toekomst meerdere domeinen te ondersteunen.</p>

R4	<b>Transparante en open besluitvorming over (door)ontwikkeling</b>	Voor zowel gebruikers, deelnemers als overige belanghebbenden geldt dat het vertrouwen in het afsprakenstelsel wordt ondersteund als de voortgang van de ontwikkeling ervan inzichtelijk is, en helder is hoe belangrijke afwegingen zijn gemaakt.
----	--	--

## Principes

### Doel

Principes zijn richtinggevende uitspraken over ontwerpkeuzes in het afsprakenstelsel. Zij gaan over de manier waarop de doelen zo goed mogelijk worden bereikt en recht wordt gedaan aan de randvoorwaarden. Principes op deze pagina betreffen algemene uitspraken. Daar waar principes betrekking hebben op een specifieke invalshoek (bijvoorbeeld juridica of architectuur) zijn zij te vinden bij de betreffende onderdelen van het afsprakenstelsel. Principes worden voorzien van een rationale, waarin de belangrijkste ontwerpafwegingen zijn opgenomen.

De principes zijn geordend in vier groepen:

- Neutraliteitsprincipes gaan over aspecten waarover het MedMij Afsprakenstelsel geen nadere beperkingen wil toevoegen aan wat in andere toepasselijke kaders al is voorzien. Daarmee bakenen deze principes het MedMij Afsprakenstelsel af op de aspecten waarover zij wel en niet wil gaan.
- Speelveldprincipes gaan over de centrale rol van dienstverleners in het MedMij Afsprakenstelsel.
- Informatieregieprincipes gaan over de aard van de regie die de persoon in het MedMij Afsprakenstelsel kan voeren, in relatie tot zorgaanbieders en gezondheidsinformatie.
- Ontwikkelingsprincipes gaan over hoe het MedMij Afsprakenstelsel zich ontwikkelt en hoe die ontwikkeling gestuurd wordt.

De onderstaande tabel kan worden gebruikt om de principes te sorteren op nummer of op groep.

Nummer	Titel	Groep
1	Het MedMij-netwerk is zoveel mogelijk gegevensneutraal	Neutraliteit
2	Dienstverleners zijn transparant over de gegevensdiensten	Speelveld
3	Dienstverleners concurreren op de functionaliteiten	Speelveld
4	Dienstverleners zijn aanspreekbaar door de gebruiker	Speelveld
5	De persoon wisselt gegevens uit met de zorgaanbieder	Informatieregie
6	MedMij spreekt alleen af wat nodig is	Neutraliteit
7	De persoon en de zorgaanbieder kiezen hun eigen dienstverlener	Speelveld
8	(vervallen)	-
9	De dienstverleners zijn deelnemers van het afsprakenstelsel	Speelveld
10	Alleen de dienstverleners oefenen macht uit over persoonsgegevens bij de uitwisseling	Speelveld
11	Stelselfuncties worden vanaf de start ingevuld	Ontwikkeling
12	Het afsprakenstelsel is een groeimodel	Ontwikkeling
13	Ontwikkeling geschiedt in een half-open proces met verschillende	Ontwikkeling

	stakeholders	
14	Uitwisseling is een keuze	Neutraliteit
15	Het MedMij-netwerk is gebruiksrechten-neutraal	Neutraliteit
16	De burger regisseert zijn gezondheidsinformatie als uitgever	Informatieregie
17	Aan de persoonlijke gezondheidsomgeving zelf worden eisen gesteld	Speelveld
18	Afspraken worden aantoonbaar nageleefd en gehandhaafd	Speelveld
19	Het afsprakenstelsel snijdt het gebruik van normen en standaarden op eigen maat	Neutraliteit

De principes worden hieronder per groep beschreven.

## Neutraliteit

### P1 - Het MedMij-netwerk is zoveel mogelijk gegevensneutraal

De dienstverleners vormen onderling een netwerk voor de uitwisseling van gegevens tussen het persoonsdomein en het zorgaanbiedersdomein. Dit netwerk bestaat uit alle dienstverleners die deelnemen aan het afsprakenstelsel. Via een dienstverlener in het ene domein kunnen alle dienstverleners in het andere domein bereikt worden. Een dienstverlener die deelneemt aan het netwerk is verplicht om te interacteren met andere dienstverleners wanneer de gebruiker daarom vraagt. Daarmee kan een gebruiker via een dienstverlener in potentie toegang krijgen tot alle gebruikers in het andere domein. Het MedMij-netwerk regelt de totstandkoming van gegevensuitwisselingen, inclusief het proces van adressering en authenticatie, en het feitelijke transport van de gegevens tussen de dienstverleners. De opzet van het netwerk is zoveel mogelijk neutraal met betrekking tot de structuur of de inhoud van de gegevens zelf. Deze kern van afspraken is gegevensdienstonafhankelijk. Daarbovenop kunnen specifieke afspraken gelden die van toepassing zijn voor een bepaalde gegevensdienst of verzameling van gegevensdiensten.

### P6 - MedMij spreekt alleen af wat nodig is

Onderwerpen die al geregeld zijn in wet- en regelgeving of de facto technisch geen barrière vormen, worden niet opgenomen in het afsprakenstelsel. Het stelsel richt zich op afspraken die nodig zijn om barrières te doorbreken en streeft geen volledigheid na. Op deze wijze wordt de kracht van bestaande normen ook zoveel mogelijk gebruikt en verbetert de onderhoudbaarheid van MedMij. Wijzigingen in wet- en regelgeving of generieke technische innovaties (mits zij de overige keuzes in het afsprakenstelsel niet raken) kunnen door deelnemers worden op- en nagevolgd zonder dat een wijziging van de formele afspraken noodzakelijk is.

### P14 - Uitwisseling is een keuze

Het afsprakenstelsel laat de persoon en de zorgaanbieder vrij om wel of niet een zekere uitwisseling aan te gaan met een zekere zorgaanbieder respectievelijk persoon. Elke uitwisseling in het kader van het MedMij Afsprakenstelsel vindt plaats met goedvinden van persoon en zorgaanbieder. De evidentie van dat goedvinden kan verschillen. Soms kan een partij dat goedvinden wettelijk niet weigeren. Soms is wettelijk geregeld dat voorafgaand aan de uitwisseling expliciete toestemming wordt verkregen. Maar ook in andere gevallen zal het afsprakenstelsel ervoor zorgdragen dat dat goedvinden wordt vastgesteld.

### P15 - Het MedMij-netwerk is gebruiksrechten-neutraal

Het afsprakenstelsel laat de persoon en de zorgaanbieder vrij in het gebruik van gezondheidsgegevens, in de betekenis en bedoeling die zij hebben. De gebruiksrechten van gezondheidsinformatie die omgaat in het kader van het MedMij Afsprakenstelsel volgen enkel uit de betekenis en bedoeling van die gegevens zelf en



uit wet- en regelgeving. Personen en Zorgaanbieders, en/of hun respectievelijke dienstverleners, verbinden via het MedMij-netwerk aan de gegevens geen nadere gebruiksbeperkingen jegens de ander, bijvoorbeeld door middel van aan die gegevens verbonden policy's. Zo worden Zorgaanbieders niet gehinderd in hun professionele praktijk en worden Personen in de gelegenheid gesteld regie te voeren over (de informatie over) hun gezondheid.

### **P19 - Het afsprakenstelsel snijdt het gebruik van normen en standaarden op eigen maat**

Vanwege principe P6 legt het MedMij Afsprakenstelsel een voorkeur aan de dag voor het gebruik van elders gespecificeerde normen en standaarden. Daarbij gelden voorkeuren voor:

- internationale boven nationale boven sectorale normen en standaarden, opdat de schaalbare interoperabiliteit en de gelijkheid in het MedMij-speelveld worden bevorderd;
- open boven half-open boven gesloten standaarden, opdat gelijkheid in het MedMij-speelveld wordt bevorderd en wordt voorkomen dat al te specifieke en niet-beïnvloedbare belangen de norm of standaard inhoudelijk gaan vervreemden van toepasbaarheid in MedMij-context;
- bewezen boven experimentele normen en standaarden, opdat de stabiliteit en kwaliteit van het MedMij Afsprakenstelsel worden bevorderd;
- standaarden en normen die ontwikkeld zijn vanuit contexten, principes en hoofdkeuzes die passen bij die van het MedMij Afsprakenstelsel, opdat het gebruik ervan voor het MedMij Afsprakenstelsel niet vroeg of laat tot ingrijpende discontinuïteit leidt en zo de duurzaamheid van het afsprakenstelsel bedreigt.

Daar waar het MedMij Afsprakenstelsel gebruik maakt van normen en standaarden, verwijst het ernaar louter als product, niet als ontwikkel-, beheer- of besturingsproces. De verwijzing geldt enkel specifieke versies van een norm of standaard, en dus geen andere versies, huidig of toekomstig. Het MedMij Afsprakenstelsel maakt voor zover nodig specifieke keuzes binnen de norm of standaard, om het gebruik te laten passen in MedMij-context.

## **Speelveld**

### **P2 - Dienstverleners zijn transparant over de gegevensdiensten**

De dienstverleners zijn naar elkaar en naar de gebruikers transparant over de gegevensdiensten die zij namens hun gebruikers kunnen aanbieden over het MedMij-netwerk. MedMij definieert welke gegevensdiensten over het MedMij-netwerk aangeboden mogen worden en biedt een faciliteit om het aanbod van de dienstverleners inzichtelijk te maken.

### **P3 - Dienstverleners concurreren op de functionaliteiten**

De dienstverleners bieden hun gebruikers functionaliteit in de vorm van een persoonlijke gezondheidsomgeving, koppelingen met zorginformatiesystemen, apps en dergelijke. De dienstverleners zijn vrij in het vormgeven van dit aanbod en concurreren met elkaar om de gunst van de gebruiker. De opzet van het MedMij-netwerk maakt het mogelijk dat een gebruiker meerdere dienstverleners heeft.

### **P4 - Dienstverleners zijn aanspreekbaar door de gebruiker**

Dienstverleners kunnen functionaliteiten zelf aanbieden, of de gegevens die zij namens de persoon hebben ontvangen op verzoek van de persoon beschikbaar stellen aan andere partijen die functionaliteit leveren in het persoonsdomein. Ook kunnen dienstverleners, in beide domeinen, ervoor kiezen de dienstverlening rond de gegevenslogistiek uit te besteden aan andere partijen. De MedMij-dienstverlener blijft echter altijd door de gebruiker aanspreekbaar op de correcte wijze van omgang met persoonsgegevens en de kwaliteit van de interactie via het MedMij-netwerk.

### **P7 - De persoon en de zorgaanbieder kiezen hun eigen dienstverlener**

De persoon en de zorgaanbieder kiezen elk hun eigen dienstverlener(s), door wie zij vertegenwoordigd worden in de gegevensuitwisseling. Het werken met één dienstverlener in het gehele stelsel is niet mogelijk, omdat er dan geen keuzevrijheid zou zijn en de facto een centrale voorziening in plaats van een afsprakenstelsel zou ontstaan. Dit betekent ook dat elke deelnemende dienstverlener zorgaanbieder alle deelnemende dienstverleners persoon op het MedMij Netwerk gelijk moet behandelen en dat elke deelnemende dienstverlener persoon alle deelnemende dienstverleners zorgaanbieder op het MedMij Netwerk gelijk moet behandelen. Interne ontwerpkeuzen van een dienstverlener in het ene domein dienen niet die in het andere domein te beïnvloeden.

### **P9 - De dienstverleners zijn deelnemers van het afsprakenstelsel**

Het afsprakenstelsel leidt tot afspraken tussen de dienstverleners. Gebruikers zijn niet rechtstreeks deelnemer in het stelsel; dit doen we om hen zo veel mogelijk te ontzorgen. De dienstverleners zijn deelnemers in het afsprakenstelsel en binden zich privaatrechtelijk en vrijwillig aan het geheel van de afspraken.

### **P10 - Alleen de dienstverleners oefenen macht uit over persoonsgegevens bij de uitwisseling**

De dienstverleners wisselen tussen de domeinen persoonsgegevens uit. Dienstverleners mogen gebruikmaken van derde partijen voor de uitoefening van taken maar blijven geheel verantwoordelijk voor en aanspreekbaar op het nakomen van de afspraken. Partijen die niet onder de volledige verantwoordelijkheid van een dienstverlener vallen, mogen niet in staat worden gesteld om macht uit te oefenen over de persoonsgegevens. Denk hierbij aan telecomproviders die connectiviteit aanbieden tussen de dienstverleners; zij kunnen een rol vervullen bij het transport van de gegevens maar alleen als zij op geen enkele manier kennis kunnen nemen van de inhoud van de uitwisseling. Met dit principe wordt gewaarborgd dat altijd helder is wie potentieel toegang hebben gehad tot persoonsgegevens, zonder dat voor gebruikers of toezichthouders een zoekplaatje ontstaat. Een decentrale oplossing voor gegevensuitwisseling zonder derde partijen tussen de dienstverleners is technisch en juridisch goed mogelijk. Vanuit het oogpunt van eenvoud is het daarom ook niet nodig om partijen te introduceren in het stelsel die niet onder de verantwoordelijkheid van dienstverleners vallen.

### **P17 - Aan de persoonlijke gezondheidsomgeving zelf worden eisen gesteld**

MedMij voorziet in afspraken over de relatie tussen de deelnemer en de gebruiker. De persoon behoeft hierbij een bijzondere bescherming. Anders dan de zorgaanbieder is hij geen professionele partij (het werken met gezondheidsgegevens is geen dagelijkse kost). Daarbij zijn de mogelijkheden van personen om volledig geïnformeerde afwegingen te maken in hun eigen belang onderling zeer verschillend en soms beperkt. Ook hebben personen een relatief grote vertrouwensdrempel te overwinnen omdat het gebruik van een persoonlijke gezondheidsomgeving volgens de MedMij-afspraken betrekking heeft op hun eigen gegevens (en niet die van een ander). Verder geldt dat door het gebruik van persoonlijke gezondheidsomgevingen nieuwe gegevensverzamelingen ontstaan, waarvoor minder specifieke regelgeving en ervaringen bestaan dan wanneer het gaat om gegevensverzamelingen in het zorgaanbiedersdomein. Denk daarbij aan het ontbreken van een patiëntgeheim, waar wel een medisch beroepsgeheim bestaat in het zorgaanbiedersdomein. Ten slotte zal de waarde van het merk MedMij en de mate waarin het erin slaagt om vertrouwensbarrières voor gegevensuitwisseling te overwinnen, mede afhankelijk zijn van de mate waarin personen vertrouwen hebben in persoonlijke gezondheidsomgevingen die uitwisselen via MedMij. Dat betekent dat er een stelselbelang is bij het waarborgen van de betrouwbaarheid van de persoonlijke gezondheidsomgevingen en de deelnemers die deze omgevingen aanbieden.

Dit leidt ertoe dat MedMij eisen stelt aan de Dienstverlener Persoon die niet alleen de uitwisseling met zorgaanbieders betreffen, en betrekking hebben op de persoonlijke gezondheidsomgeving zelf.

### **P18 - Afspraken worden aantoonbaar nageleefd en gehandhaafd**

Dienstverleners dienen aan te tonen dat zij zich houden aan afspraken uit het MedMij Afsprakenstelsel. Daarbij kan toetsing door derde partijen worden vereist. Enkel een intentie tot het volgen van of een

juridische binding aan de afspraken is niet voldoende. Toetsing kan ook vooraf plaatsvinden. Er wordt toezicht gehouden op de naleving door een van de deelnemers onafhankelijke partij, die over een proportioneel en effectief sanctie-instrumentarium beschikt. Op deze manier wordt het onaantrekkelijker voor partijen om bewust af te wijken van de afspraken in eigen voordeel, ontstaat een actievere omgang met de afspraken die een juiste interpretatie en suggesties voor doorontwikkeling tot gevolg heeft, en wordt bijgedragen aan het vertrouwen van alle betrokkenen.

## Informatieregie

### P5 - De persoon wisselt gegevens uit met de zorgaanbieder

Personen wisselen gezondheidsgegevens uit met zorgaanbieders. Veel van de gegevens zijn geregistreerd of worden gebruikt door individuele zorgverleners. De gegevens worden vaak echter bijgehouden in een informatiesysteem op het niveau van de organisatie. Denk hierbij aan een huisartsenpraktijk of een ziekenhuis die elektronische dossiers over patiënten bijhoudt, waarbij meerdere zorgverleners het medisch dossier bijwerken en raadplegen. Steeds vaker worden dossiers ook specialisme-overstijgend bijgehouden; de ontwikkeling van een kern dossier is hiervan een goed voorbeeld. Ook kan MedMij betrekking hebben op zorgadministratieve gegevens (zoals afspraken), die worden bijgehouden door anderen dan de zorgverleners zelf. Voor de uitwisseling van gegevens is het daarom passend om te spreken van een interactie tussen de persoon en de zorgaanbieder, waarbij de zorgaanbieder een organisatie is van een of meer zorgverleners. Wanneer we zouden uitgaan van de zorgverlener wordt het beschrijven van het afsprakenstelsel nodeloos ingewikkeld, omdat de zorgverlener dan vaak een relatie heeft met andere zorgverleners of met niet-medische medewerkers of organisaties. De zorgaanbieder is een logische partij om over het geheel dat nodig is voor de uitwisseling van gezondheidsgegevens met de patiënt namens de zorgverleners afspraken te maken met de dienstverlener in het MedMij-netwerk.

### P16 - De burger regisseert zijn gezondheidsinformatie als uitgever

MedMij wil iedereen meer regie op zijn gezondheid geven. Daarvoor is het nodig dat iedereen, door middel van een persoonlijke gezondheidsomgeving, inzicht in zijn eigen gezondheidsinformatie heeft, en op die gezondheidsinformatie regie kan voeren. Voor dat laatste zijn meerdere vormen denkbaar, die aanzienlijk verschillen in de kracht van de regie en in de eruit voortvloeiende verantwoordelijkheden en vrijheden voor alle betrokkenen. Ook verschillen zij sterk in hoe het informatieverkeer is ingericht, ook functioneel en technisch. Het MedMij afsprakenstelsel kiest voor een regiemodel waarin de burger zijn eigen gezondheidspublicaties samenstelt en uitgeeft, dat wil zeggen, deelt met lezers. Daartoe is het hem gegeven bronnen aan te boren. Bronnen en lezers zijn allereerst aanbieders van zorg- en gezondheidsdiensten. De uitgever is dus de hoofdrol in het persoonsdomein; bron en lezer zijn de twee hoofdrollen in het zorgaanbiedersdomein. Deze vorm van informatieregie legt het initiatief in hoge mate bij de burger (de uitgever) en is daarmee krachtiger dan het model waarin de burger alleen kan reageren - instemmend of afkeurend - op verkeer tussen zorgaanbieders. Anderzijds gaat de regievorm niet zover dat zij de burger het onverminderde economische eigendom toedicht over de gezondheidsinformatie, en het intellectuele eigendom evenmin. Achter deze vormen zouden nog geheel andere regiomodellen schuilgaan, met onwenselijke consequenties en risico's.

## Ontwikkeling

### P11 - Stelselfuncties worden vanaf de start ingevuld

Het functioneren van het MedMij-netwerk en het afsprakenstelsel is mede afhankelijk van de mate waarin het stelsel als geheel in staat is om in te spelen op ontwikkelingen in de omgeving of in de operatie, zowel positieve als negatieve. Daarbij zijn rollen nodig die zich richten op het belang van het stelsel, en niet op een specifieke deelnemer of een specifieke relatie tussen twee deelnemers daarin. Immers, er zijn vraagstukken (zoals doorontwikkeling, het beslechten van geschillen of het reageren op een beveiligingsincident) die het belang van een of twee deelnemers overstijgen. De belangrijkste stelselfuncties, waaronder ten minste ontwikkeling, toezicht en handhaving, worden vanaf de start van het afsprakenstelsel ingevuld. De diepgang van deze functies en de organisatie(s) die deze rollen vervullen kunnen in de loop van de tijd wijzigen.

### **P12 - Het afsprakenstelsel is een groeimodel**

Om snel een eerste versie van het afsprakenstelsel te kunnen krijgen én te kunnen leren van tussentijdse ervaringen, wordt het afsprakenstelsel opgezet als groeimodel. De belangrijkste barrières voor de uitwisselingen met de meeste potentiële baten worden als eerste opgepakt. Daarbij is ook de haalbaarheid van realisatie, waaronder de aansluiting op de huidige ontwikkelingen in de markt, een criterium. Daar waar duidelijkheid benodigd is in de afspraken die pas op termijn van kracht zijn maar die op enig moment nog niet haalbaar zijn, kan een groeipad worden afgesproken.

Het afsprakenstelsel start met de uitwisseling tussen de persoon en de zorgaanbieder. De opzet van het stelsel is echter wel zodanig dat een uitwisseling tussen de persoon en derden op termijn mogelijk is.

### **P13 - Ontwikkeling geschiedt in een half-open proces met verschillende stakeholders**

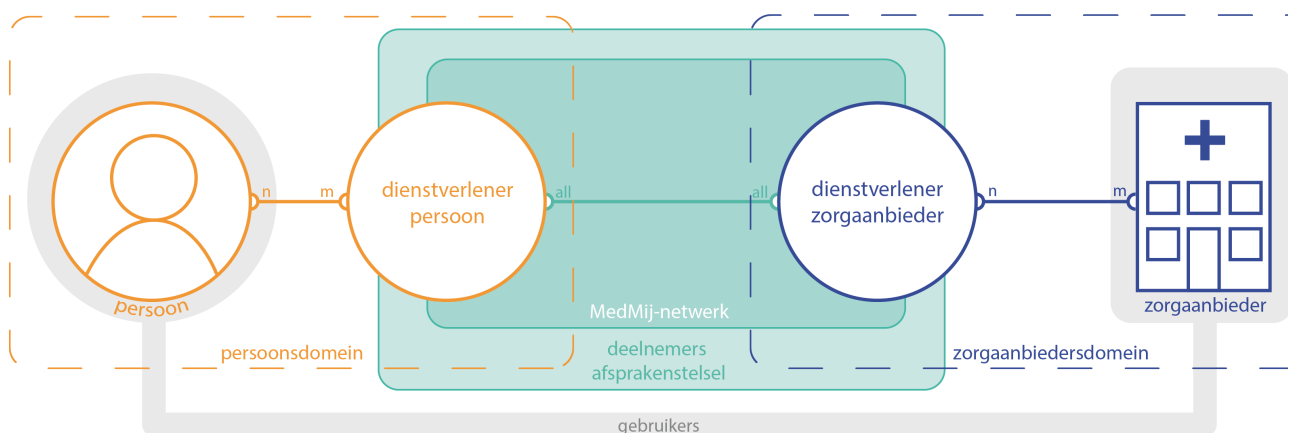
Het afsprakenstelsel wordt (door)ontwikkeld in samenspraak met de belangrijkste stakeholders, waaronder vertegenwoordigers van de deelnemers, de gebruikers en partijen met een belang bij het functioneren van het stelsel. Dit zorgt ervoor dat (door)ontwikkeling en gebruik zoveel mogelijk van elkaar profiteren, versnelling optreedt in de implementatie, en draagvlak wordt verworven bij de afnemers van het ontwikkelproces. Vanwege de gevraagde snelheid en de aansluiting op andere centraal gestuurde initiatieven vindt de ontwikkeling plaats in een half-open proces. Deelname is mogelijk voor iedere partij die zich afdoende kan kwalificeren op toegevoegde waarde; de kaders voor en de ritmiek van het ontwerpproces worden echter bepaald door het programma MedMij en later de Stichting MedMij.

## Opzet

### Doel

De opzet van het afsprakenstelsel geeft op het hoogst mogelijke niveau een overzicht van de rollen in de gegevensuitwisseling via het MedMij-netwerk, hun onderlinge relaties, de interacties tussen deze rollen en de belangrijkste begrippen die geassocieerd zijn met rollen en partijen.

## Rollen en relaties



We onderscheiden het Persoonsdomein en het Zorgaanbiedersdomein. Deze begrippen helpen om een onderscheid te kunnen maken tussen datgene dat zich afspeelt in de controlesfeer van de Persoon (door hemzelf of namens hem door zijn Dienstverlener persoon) en datgene dat zich afspeelt in de controlesfeer van de Zorgaanbieder (door hemzelf of namens hem door zijn Dienstverlener zorgaanbieder). Op beide domeinen is verschillende wetgeving van toepassing, en in beide domeinen kan de onderlinge verhouding tussen de Dienstverlener en de Gebruiker verschillend zijn.

De Persoon en de door hem of haar gekozen Dienstverleners persoon vormen het Persoonsdomein. Een Persoon kan gebruikmaken van een of meer Dienstverleners persoon. Een Dienstverlener persoon kan actief zijn voor een of meer Personen. In de afbeelding is dit weergegeven als een n-op-m-relatie.

De Zorgaanbieder en de door hem gekozen Dienstverlener zorgaanbieder vormen het Zorgaanbiedersdomein. De Zorgaanbieder kiest een of meer Dienstverleners zorgaanbieder. Een Dienstverlener zorgaanbieder kan actief zijn voor een of meer Zorgaanbieders. In de afbeelding is dit weergegeven als een n-op-m-relatie.

De Persoon en de Zorgaanbieder zijn Gebruiker van MedMij. De Dienstverlener persoon en de Dienstverlener zorgaanbieder zijn Deelnemer in het afsprakenstelsel. Alle Dienstverleners persoon en alle Dienstverleners zorgaanbieder vormen samen het MedMij-netwerk. Elke Dienstverlener persoon moet elke Dienstverlener zorgaanbieder kunnen bereiken, en vice versa. Daarom is een 'all-to-all'-relatie opgenomen in de afbeelding.

De Dienstverleners zijn voor de interactie via het MedMij-netwerk gehouden aan een set afspraken over het gewenste en toegestane gedrag op het netwerk. Het afsprakenstelsel bevat afspraken over de interacties via het netwerk, en een aantal aanvullende afspraken waaraan de Dienstverlener zich dient te houden vanuit het oogpunt van bescherming van de Gebruiker. De Dienstverleners leveren de Gebruiker daarnaast diensten waarover geen afspraken worden gemaakt via het afsprakenstelsel.

## Interacties tussen de rollen

In onderstaande tabel zijn op het hoogste niveau de gegevensuitwisselingen tussen de gebruikers van het MedMij-netwerk beschreven. Hierbij is aangegeven wat de kernverantwoordelijkheid is van de verschillende rollen in het afsprakenstelsel. Het interactie-overzicht gaat niet in op de wijze waarop dit wordt gerealiseerd (dat volgt uit onder andere de technische en juridische uitwerking), en ook niet op randvoorwaardelijke interacties of gegevensuitwisselingen tussen de partijen (zoals het aansluiten op het MedMij-netwerk).

Nr.	Beoogd resultaat	Interacties
1	De Persoon heeft de door hem of haar gevraagde gezondheidsgegevens verkregen, die de Zorgaanbieder digitaal over hem of haar beschikbaar heeft.	De Persoon verzoekt de Dienstverlener persoon om namens hem of haar de Dienstverlener zorgaanbieder te verzoeken de gevraagde gegevens zoals die bij de Zorgaanbieder bekend zijn te verzenden naar de Dienstverlener persoon.
2	De Persoon heeft de Zorgaanbieder gegevens over de gezondheid van de Persoon verstrekt.	<p>De Persoon verzoekt de Dienstverlener persoon om namens hem of haar aan de Dienstverlener zorgaanbieder een door de Persoon aan de Dienstverlener persoon beschikbaar gestelde gegevensset te verzenden.</p> <p>De Dienstverlener zorgaanbieder informeert de Zorgaanbieder over de nieuwe gegevens.</p>

## Begrippenlijst

### Doel

De begrippenlijst geeft een eenduidige definitie van de belangrijkste begrippen die in het afsprakenstelsel worden gebruikt.

Begrip	Domein	Definitie	Synoniemen
Abonnement	tussen Persoonsdomein en Zorgaanbiedersdomein	Overeenkomst tussen een <i>Zorgaanbieder</i> en een <i>Persoon</i> voor het (mogen) leveren van <i>Notificaties</i> door <i>Zorgaanbieder</i> aan <i>Dienstverlener persoon</i> . Deze release van het MedMij Afsprakenstelsel betreft enkel <i>Abonnementen</i> die betrekking hebben op <i>Gegevensdiensten</i> die zijn gebaseerd op de <i>UC Verzamelen</i> .	
Afsprakenstelsel	alle domeinen samen	Set van afspraken op juridisch, organisatorisch, financieel, semantisch en technisch gebied om alle partijen voldoende vertrouwen te geven in hetgeen het stelsel hen biedt. Partijen die deelnemen aan het MedMij Afsprakenstelsel committeren zich aan de afspraken, en kunnen op basis van de reeds overeengekomen afspraken, diensten aanbieden.	MedMij Afsprakenstelsel
Catalogus	alle domeinen samen	Verzameling van <i>Gegevensdiensten</i> die op enig moment door <i>Zorgaanbieders</i> aangeboden mogen (of mochten) worden op het MedMij-netwerk.	
Deelnemer	Persoonsdomein of Zorgaanbiedersdomein	Een partij die dienstverlening aanbiedt binnen het MedMij Afsprakenstelsel. De <i>Dienstverlener persoon</i> en de <i>Dienstverlener zorgaanbieder</i> zijn <i>Deelnemer</i> in het afsprakenstelsel en daarmee gebonden aan de afspraken,	

		bekrachtigd door het tekenen van een deelnemersovereenkomst.	
Dienstverlener persoon	Persoonsdomein	Dit betreft een rol in het MedMij Afsprakenstelsel. Levert een Persoonlijke gezondheidsomgeving, een dienst aan de Persoon voor de regie op zijn gezondheid die minimaal gegevensuitwisseling met de Zorgaanbieder mogelijk maakt middels het MedMij Afsprakenstelsel.	
Dienstverlener zorgaanbieder	Zorgaanbiedersdomein	Dit betreft een rol in het MedMij Afsprakenstelsel. Levert Diensten aan de Zorgaanbieder gerelateerd aan de uitwisseling tussen Persoon en Zorgaanbieder en committeert zich hiervoor aan de naleving van de afspraken van het MedMij Afsprakenstelsel.	
Gebruiker	Persoonsdomein of Zorgaanbiedersdomein	Een partij die gebruik maakt van dienstverlening van deelnemers aan het afsprakenstelsel. De Persoon en de Zorgaanbieder zijn Gebruiker van MedMij.	
Gegevensdienst	tussen Persoonsdomein en Zorgaanbiedersdomein	Een gestandaardiseerde dienst voor gegevensuitwisseling met waarde voor de Gebruiker die door een Dienstverlener kan worden aangeboden over het MedMij-netwerk. MedMij definieert welke gegevensdiensten over het MedMij-netwerk aangeboden mogen worden en biedt een faciliteit om het aanbod van de dienstverleners inzichtelijk te maken.	
Gezondheidsgegevens	tussen Persoonsdomein en Zorgaanbiedersdomein	Gegeven betreffende de geestelijke en/of lichamelijke gesteldheid van een persoon.	Persoonlijke gezondheidsinformatie, gezondheidsinformatie
MedMij-netwerk	tussen Persoonsdomein en Zorgaanbiedersdomein	Alle Dienstverleners persoon en alle Dienstverleners zorgaanbieder vormen samen	Netwerk



		het MedMij-netwerk. Elke Dienstverlener persoon moet elke Dienstverlener zorgaanbieder kunnen bereiken, en vice versa.	
Notificatie	tussen Persoonsdomein en Zorgaanbiedersdomein	<p>Kennisgeving, van <i>Zorgaanbieder</i> aan <i>Dienstverlener persoon</i>. Deze release van het MedMij Afsprakenstelsel betreft</p> <ul style="list-style-type: none"> <li>• notificaties van wijzigingen in (gezondheids)informatie met betrekking tot een <i>Persoon</i> en en <i>Gegevensdienst</i>, zoals beheerd bij de <i>Zorgaanbieder</i>. Dergelijke notificaties heten inhoudelijke notificaties of resource notifications.</li> <li>• notificaties van beperking of beëindigen van een <i>Abonnement</i> op initiatief van <i>Zorgaanbieder</i>. Deze notificaties heten abonnementsnotificaties of subscription notifications.</li> </ul>	
Persoon	Persoonsdomein	Degene, 16 jaar of ouder, op wie Gezondheidsgegevens betrekking hebben die via MedMij worden uitgewisseld en tevens de Gebruiker in het Persoonsdomein.	Betrokkene, burger, individu, gebruiker, patiënt, cliënt, zorgconsument, zorggebruiker
Persoonlijke gezondheidsomgeving	Persoonsdomein	Een Persoonlijke gezondheidsomgeving is een dienst aan de Persoon voor de regie op zijn gezondheid die minimaal gegevensuitwisseling met de Zorgaanbieder mogelijk maakt middels het MedMij Afsprakenstelsel.	PGO, persoonlijk gezondheidsplatform
Persoonsdomein	Persoonsdomein	Alle Personen en alle Dienstverleners personen vormen samen het Persoonsdomein.	
Rol	alle domeinen samen	Een samenhangende set van	

		verwachte en overeengekomen verantwoordelijkheden en interacties in het MedMij Afsprakenstelsel. Aan een Rol zijn afspraken gekoppeld zoals vastgelegd in het Afsprakenstelsel MedMij. Een rol kan worden vervuld door een natuurlijke persoon en/of organisatie.	
Zorgaanbieder	Zorgaanbiedersdomein	Een zorgverlener of een verband van zorgverleners die behandelingsovereenkomsten kunnen aangaan met patiënten op grond van art. 7: 446 BW en tevens de Gebruiker in het Zorgaanbiedersdomein.	Zorginstelling, zorgorganisatie, brondossierhouder
Zorgaanbiedersdomein	Zorgaanbiedersdomein	Alle Zorgaanbieders en alle Dienstverleners zorgaanbieder vormen samen het Zorgaanbiedersdomein.	
Zorginformatiesysteem	Zorgaanbiedersdomein	Het systeem of geheel van de systemen waarin de zorgaanbieder het medisch dossier van de persoon bijhoudt.	XIS

## Juridische context

De juridische context bestaat uit:

- Het [Juridisch kader](#), waarin de relevante wet- en regelgeving wordt geanalyseerd. De analyse biedt inzicht voor deelnemers en de beheerorganisatie aangaande de eisen die de wet aan hen stelt, en biedt tevens onderbouwing voor enkele nadere afspraken binnen het MedMij Afsprakenstelsel.
- Een beschrijving van het stelsel van [Overeenkomsten en rechtsrelaties](#) die gelden binnen het MedMij Afsprakenstelsel.
- Een analyse van de [verwerkingsverantwoordelijkheden](#) voor de gegevensuitwisseling via het MedMij Afsprakenstelsel. De analyse biedt inzicht voor deelnemers en de beheerorganisatie aangaande de eisen die de wet aan hen stelt, en biedt tevens onderbouwing voor en toelichting op enkele nadere afspraken binnen het MedMij Afsprakenstelsel.
- Een toelichting op de verantwoordelijkheden en [normen](#) voor deelnemers die voortvloeien uit de AVG. Daarbij is op onderdelen aangegeven wat het MedMij afsprakenstelsel hierop aanvullend of invullend vereist evenals eventuele opmerkingen of aandachtspunten voor deelnemers.

## Juridisch kader

Het juridisch kader geeft een overzicht van de relevante wet- en regelgeving voor deelnemers aan het MedMij Afsprakenstelsel. Deze wet- en regelgeving heeft betrekking op de dienstverlening die met behulp van het MedMij Afsprakenstelsel wordt uitgeoefend. Dit overzicht pretendeert niet volledig te zijn. Het is en blijft te allen tijde de verantwoordelijkheid van de betrokken partijen om aan de voor hen geldende (specifieke) wet- en regelgeving te voldoen. Voor de toepassing van de in het overzicht opgenomen wet- en regelgeving voor het MedMij Afsprakenstelsel is een toelichting opgenomen.

De privaatrechtelijke afspraken, op basis waarvan partijen gerechtigd zijn hun diensten in relatie tot het MedMij Afsprakenstelsel aan te bieden, zijn aanvullend op de geldende wet- en regelgeving en zijn opgenomen bij [Overeenkomsten en rechtsrelaties](#).

Wetgeving	Toelichting	Toepassing
<p><a href="#">Algemene Verordening Gegevensbescherming (AVG)</a></p> <p>(gepubliceerd 27-04-2016, geldend vanaf 25-05-2018)</p>	<p>MedMij-deelnemers verwerken persoonsgegevens. De Algemene Verordening Gegevensbescherming (AVG) is daarmee van toepassing. De AVG behelst de waarborgen voor een aantoonbare en controleerbare rechtmatige, behoorlijke en transparante verwerking van persoonsgegevens. Een belangrijk onderdeel hiervan zijn de rechten van betrokkenen, zoals het recht op informatie en inzage.</p> <p>Een aantoonbare en controleerbare verwerking van persoonsgegevens houdt in dat iedere organisatie die persoonsgegevens verwerkt actief en controleerbaar moet kunnen aantonen dat zij zich aan de beginselen van een rechtmatig, behoorlijke en transparante verwerking van persoonsgegevens houdt. Door aan deze beginselen te voldoen, wordt gewaarborgd dat de betrokkene zicht heeft op wie voor welke doeleinde(n) welke persoonsgegevens van hem /haar verwerkt en kan hij/zij ook controle uitoefenen over de verwerking van zijn persoonsgegevens.</p>	<p>Of een partij die met gebruikmaking van het MedMij Afsprakenstelsel verwerker of verwerkingsverantwoordelijke is, is voor de verwerking van persoonsgegevens in relatie tot het aanbieden van MedMij diensten of -gegevensdiensten, dus afhankelijk van de vraag:</p> <ul style="list-style-type: none"> <li>• welke partij(en) in de concrete situatie feitelijk (gezamenlijk) doel en middelen bepaalt (bepalen) van de verwerking van persoonsgegevens;</li> <li>• of er een partij is die voor de verwerkingsverantwoordelijke 'slechts' handelt volgens de vooraf door de verwerkingsverantwoordelijke opgestelde en schriftelijke instructies en geen zeggenschap heeft over de persoonsgegevens.</li> </ul> <p>Hieronder geven wij - gelet op de technische inrichting en werking van het MedMij Afsprakenstelsel en de daaruit voortvloeiende verwerking van persoonsgegevens - een zienswijze op de invulling van verwerkingsverantwoordelijke en verwerker. Zie voor een meer uitgebreide toelichting op de rechtsrelaties tussen de bij het MedMij Afsprakenstelsel betrokken partijen <a href="#">Overeenkomsten en rechtsrelaties</a>.</p> <p>Ten eerste wordt - voor wat betreft de verantwoordelijkheidsverdeling ten aanzien van de naleving van de wet- en</p>

Twee belangrijke begrippen uit de AVG zijn die van 'verwerkingsverantwoordelijke' en 'verwerker'. De verwerkingsverantwoordelijke heeft zeggenschap over de verwerking van persoonsgegevens en stelt het doel of de middelen voor de verwerking van persoonsgegevens vast. De verwerker verwerkt de persoonsgegevens in opdracht van en volgens schriftelijke instructie van de verwerkingsverantwoordelijke. Alhoewel de primaire verantwoordelijkheid voor de gegevensverwerking bij de verwerkingsverantwoordelijke ligt, is ook de verwerker aansprakelijk indien de verwerking van persoonsgegevens in strijd met de beginselen van de AVG plaatsvindt, dan wel wanneer bij de verwerking van de persoonsgegevens niet conform de rechtmatige instructies van de verwerkingsverantwoordelijke is gehandeld.

regelgeving in z'n algemeenheid - opgemerkt dat wettelijke verantwoordelijkheden en afspraken ten aanzien van bestaande eHealth toepassingen en/of initiatieven (tussen betrokken partijen) niet worden doorkruist door gebruikmaking van het MedMij Afsprakenstelsel.

Gebruikmaking van het MedMij Afsprakenstelsel betekent ook geen wijziging in de verantwoordelijkheid voor de naleving van wettelijke verplichtingen in relatie tot de uitwisseling van (persoons)gegevens en/of gezondheidsgegevens ten opzichte van de situatie zoals deze gelden op basis van de WGB0, de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en de AVG. Dit betekent dat voor een rechtmatige, behoorlijke en transparante verwerking van de (persoons)gegevens en gezondheidsinformatie via MedMij de actoren die een rol spelen in de gegevensuitwisseling via MedMij de volgende verantwoordelijkheid hebben:

1. De Zorgaanbieder als Gebruiker van Diensten van de Dienstverlener zorgaanbieder van het MedMij Afsprakenstelsel is gehouden tot naleving van de WGB0, de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg en is in deze hoedanigheid 'verwerkingsverantwoordelijke' voor de verwerking van persoonsgegevens in de zin van de AVG. In het geval de Zorgaanbieder als 'verwerkingsverantwoordelijke' de Dienstverlener Zorgaanbieder inschakelt om in opdracht van hem (bijzondere) persoonsgegevens met de Persoon (via het MedMij- netwerk) te verwerken, is de Zorgaanbieder voor deze verwerking van persoonsgegevens verplicht een verwerkersovereenkomst met de Dienstverlener Zorgaanbieder af te sluiten. Hiervan is bijvoorbeeld sprake bij authenticatie van de Persoon door de Zorgaanbieder als gevolg van de identificatieplicht voor de Zorgaanbieder overeenkomstig de

Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. Voor onder meer deze situatie wordt door het MedMij Afsprakenstelsel een [Modelverwerkersovereenkomst Zorgaanbieder - Dienstverlener zorgaanbieder](#) ter beschikking gesteld.

2. De Dienstverlener Zorgaanbieder is 'verwerker' van de Zorgaanbieder, voor zover de Dienstverlener in opdracht van en op basis van schriftelijke instructies van de Zorgaanbieder persoonsgegevens verwerkt. Van een dergelijke situatie is bijvoorbeeld sprake bij authenticatie - in opdracht van de Zorgaanbieder - van de Persoon die (via de Dienstverlener Persoon) informatie opvraagt bij zijn Zorgaanbieder. Zie ook punt 1.
3. De Dienstverlener Persoon is 'verwerkingsverantwoordelijke' voor de verwerking van persoonsgegevens voor Diensten en Gegevensdiensten die hij via het MedMij Afsprakenstelsel ten behoeve van de Persoon ontsluit.

In het MedMij Afsprakenstelsel wordt de persoon niet gezien als verwerkingsverantwoordelijke. De filosofie achter de AVG is om een persoon te beschermen tegen de macht van de overheden en bedrijven over hun persoonsgegevens. Als een persoon alle plichten van de verantwoordelijke op zich moet laden en niet meer de rechten heeft die hem in de zin van de AVG toekomen, dan is hij niet beschermd, moet hij zelf het informatiebeveiligingsbeleid opstellen, verwerkersovereenkomsten sluiten etc. Dat past niet bij de bedoelingen van het wettelijk kader ter bescherming van de betrokkene. De persoon heeft wel zeggenschap over de gegevens in een persoonlijke gezondheidsomgeving, maar niet de volledige macht hierover, inclusief de verantwoordelijkheden zoals hiervoor genoemd. Hij/ zij staat in die zin in ongelijke machtsverhouding ten opzichte van bedrijven, zorgaanbieders en overheden. De Dienstverlener persoon

		<p>wordt daarom gezien als zelfstandig verwerkingsverantwoordelijke binnen het afsprakenstelsel.</p> <p>Alleen in het geval dat Diensten en Gegevensdiensten via het MedMij Afsprakenstelsel worden geleverd, dient er dus een <a href="#">Deelnemersovereenkomst Dienstverlener Persoon</a> of een <a href="#">Deelnemersovereenkomst Dienstverlener Zorgaanbieder</a> met Stichting MedMij te worden afgesloten en kan het zijn dat eventuele bestaande overeenkomsten worden aangepast en /of uitgebreid ter waarborging van de naleving van de afspraken van het MedMij Afsprakenstelsel bij de levering van Diensten via MedMij. Zie voor een nadere uitwerking van de verwerkingsverantwoordelijkheid bij de Diensten en Gegevensdiensten <a href="#">Toelichting verwerkingsverantwoordelijkheid</a>.</p> <p>Gegevens die via MedMij worden uitgewisseld betreffen bijna altijd bijzondere persoonsgegevens. Deelnemers moeten hiervoor voldoen aan de normen die de AVG stelt met betrekking tot het verwerken van deze persoonsgegevens. Deelnemers zijn zelf verantwoordelijk voor de correcte implementatie van de wet. Vanwege het belang van een correcte uitvoering van deze wet door deelnemers aan het MedMij Afsprakenstelsel heeft MedMij een <a href="#">toelichting</a> op de verantwoordelijkheden en normen in de AVG opgenomen.</p> <p>De AP biedt <a href="#">ondersteuning bij de uitvoering van de AVG</a>. Daarnaast kan gebruik worden gemaakt van de 'Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming' van het Ministerie van Justitie en Veiligheid. De AP heeft tevens een <a href="#">praktijkgids</a> 'Patiëntgegevens in de cloud' uitgegeven . De AP heeft deze praktijkgids uitgegeven omdat het gebruik van de cloud risico's met zich meebrengt.</p>
	De Wet op de geneeskundige behandelingsovereenkomst	Zorgaanbieders dienen de wettelijke bepalingen te volgen voor

## Wet op de geneeskundige behandelingsovereenkomst (WGBO)

(geldend vanaf 01-02-2006)

(WGBO) beschrijft de rechten en plichten van patiënten in de zorg.

Er is sprake van een geneeskundige behandelingsovereenkomst wanneer een arts een patiënt onderzoekt of behandelt. De wet is bedoeld om de positie te versterken van patiënten die medische zorg nodig hebben.

De WGBO regelt onder andere het recht op informatie over de medische situatie, inzage in het medisch dossier, recht op privacy en geheimhouding van medische gegevens (beroepsgeheim).

dossiervorming. Een persoonlijke gezondheidsomgeving is juridisch gezien geen dossier dat valt onder deze dossierplicht. Een Persoon houdt in een persoonlijke gezondheidsomgeving, in aanvulling op het dossier van de zorgaanbieder, vrijwillig gezondheidsdata bij.

De Zorgaanbieder is verplicht bij het verstrekken van gegevens vanuit of het opnemen van gegevens in het medisch dossier de identiteit van de Persoon te verifiëren. Binnen het MedMij Afsprakenstelsel zal een derde partij, de Dienstverlener persoon, namens de persoon gegevens ophalen bij de Zorgaanbieder via de Dienstverlener zorgaanbieder. De Persoon zal in die gegevensuitwisseling de Zorgaanbieder toestemming moeten verlenen om de gegevens beschikbaar te stellen aan deze derde partij, de Dienstverlener persoon. De Dienstverlener zorgaanbieder registreert, in opdracht van en volgens instructie van de Zorgaanbieder, de verkregen toestemming van de Persoon om gegevens te delen met de Dienstverlener Persoon. Op grond van de WGBO mogen minderjarigen alleen rechtshandelingen verrichten met toestemming van hun wettelijk vertegenwoordiger. De leeftijdsgrens is in de WGBO op 16 jaar gesteld. Personen vanaf 16 jaar mogen dus zelfstandig beslissen over de medische behandeling.

Op het omgaan met de door de Persoon aangeleverde gegevens berusten de plichten van de zorgaanbieder conform 'goed hulpverlenerschap', die nader zijn gedefinieerd in de WGBO, evenals de bepalingen rond dossiervorming en medisch beroepsgeheim. Dat betekent dat de Zorgaanbieder bepaalt welke gegevens uiteindelijk worden opgenomen in het medisch dossier en welke actie hierop wordt ondernomen.

Bij een persoonlijke gezondheidsomgeving geniet de Persoon niet de bescherming van het medisch beroepsgeheim. In aanvulling



		<p>op de bestaande privacy wet- en regelgeving wordt daarom binnen het MedMij Afsprakenstelsel van belang geacht om de Persoon tevens bewust te laten zijn van de gevoeligheid van de gezondheidsgegevens. In de <a href="#">Gebruikersvoorlichting</a> zijn hiervoor ondersteunende teksten opgenomen.</p>
<p><a href="#">Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg</a></p> <p>(geldend vanaf 01-01-2018)</p>	<p>De wet aanvullende bepalingen verwerking persoonsgegevens in de zorg vervangt de wetten gebruik burgerservicenummer in de zorg en de wet cliëntenrechten bij elektronische verwerking van gegevens in de zorg.</p> <p>De wet introduceert rechten en waarborgen voor cliënten bij elektronische gegevensuitwisseling en het beschikbaar stellen van gegevens via elektronische uitwisselingssystemen. Daarnaast verplicht het zorgaanbieder het burgerservicenummer (BSN) van hun patiënten vast te leggen in hun administratie. Met het BSN kan de identiteit van de patiënt zeker worden gesteld. Ook bij het verstrekken van persoonsgegevens met betrekking tot de verlening van, indicatiestelling voor of verzekering van zorg aan andere zorgaanbieder, een indicatieorgaan of aan zorgverzekeraars moet de zorgaanbieder het burgerservicenummer gebruiken.</p> <p>Gebruik van het BSN is vastgelegd in een gesloten stelsel. Alleen als er wettelijke gronden zijn voor de verwerking van het BSN, is het gebruik van het BSN toegestaan. Verwerkingsverantwoordelijken bij de overheid en de zorg, inclusief zorgaanbieder, indicatieorganen en</p>	<p>De Zorgaanbieder, in het BSN-domein, is verplicht bij het verstrekken van gegevens vanuit of het opnemen van gegevens in het medisch dossier de identiteit van de Persoon te verifiëren aan de hand van het BSN. In Nederland wijst het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) de digitale identiteitsmiddelen aan die gebruikt kunnen worden voor deze verificatie. Binnen het MedMij Afsprakenstelsel gebruikt de Dienstverlener zorgaanbieder, onder verwerkingsrelatie van de Zorgaanbieder, in verband met de verplichting het BSN te gebruiken, deze hiertoe aangewezen middelen. De Zorgaanbieder is verantwoordelijk voor het bepalen van het betrouwbaarheidsniveau waartegen de identificatie plaatsvindt. Meer informatie voor het bepalen van het juiste betrouwbaarheidsniveau is te vinden in de Handreiking <a href="#">Betrouwbaarheidsniveaus voor digitale dienstverlening</a> en <a href="#">Onderzoek patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg</a>, <a href="#">PrivacyCare</a> en <a href="#">PBLQ, 2016</a>.</p> <p>Binnen het MedMij Afsprakenstelsel wordt gebruik gemaakt van een door BZK aangewezen authenticatiemiddel. Dit middel zorgt voor de verificatie van de identiteit van de Persoon door de Zorgaanbieder. Het gebruik van dit middel is momenteel door BZK niet aan leeftijd gebonden. Dit betekent personen onder de 16 jaar in de zin van de WGBO ook kunnen beschikken over een authenticatiemiddel. Voor personen onder de 16 jaar gelden echter specifieke wettelijke regels. Voor het verstrekken en delen van gegevens aan een minderjarige moet op grond van de WGBO toestemming of een machtiging tot toestemming worden verleend door</p>

zorgverzekeraars mogen – onder voorwaarden – het BSN verwerken. Er is een uitzondering voor verwerkers die optreden namens verwerkingsverantwoordelijken (AVG). Verwerkers mogen, in het kader van hun verwerkersrol, gegevens verwerken ten behoeve van de eerder genoemde verwerkingsverantwoordelijken, waaronder het BSN.

In de wet is de bepaling opgenomen dat voor beschikbaarstelling van gegevens via een elektronisch uitwisselingssysteem de Zorgaanbieder voorafgaande toestemming van de betreffende cliënt moet krijgen (art. 15a lid 1). Bij dit alles gaat het om zogenaamde ‘gespecificeerde toestemming’, dat wil zeggen toestemming voor het beschikbaar stellen van alle of bepaalde gegevens aan bepaalde door de cliënt aan te duiden Zorgaanbieders of categorieën van Zorgaanbieders. Alle (categorieën van) Zorgaanbieders die de Persoon niet expliciet heeft benoemd zijn automatisch uitgesloten om gegevens die beschikbaar zijn gesteld in een elektronisch uitwisselingssysteem, te raadplegen.

Ook biedt deze wet een recht op elektronische inzage.

Zowel het recht op gespecificeerde toestemming als het recht op elektronische inzage vergt nog dermate veel aanpassing in bestaande zorg-ict-systemen dat de wetgever vanaf de inwerkingtredingsdatum van deze wet op 1 juli 2017 nog drie jaar de tijd heeft gegeven

degene die de ouderlijke verantwoordelijkheid of de wettelijke verantwoordelijkheid voor het kind draagt. Het MedMij Afsprakenstelsel voorziet in het opvragen of delen van gegevens door de Persoon zelf en kent (nog) geen mogelijkheden om (digitaal) toestemming te verkrijgen van een wettelijk vertegenwoordiger of de ouderlijke verantwoordelijke. Er worden daarom voorlopig alleen gegevens en/of gezondheidsinformatie van personen van 16 jaar en ouder verstrekt door of gedeeld met de zorgaanbieder. Dit betekent dat personen jonger dan 16 jaar die inloggen door middel van het door BZK aangewezen middel geen gegevens en/of gezondheidsinformatie ontvangen of delen via het MedMij Afsprakenstelsel.

In het geval de Persoon zich voor het eerst tot een Zorgverlener wendt, moet de Zorgverlener bij het eerste fysieke contact het BSN verifiëren. Zie ook artikel 4 en 5 sub a Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg. Vervolgens valt de interactie tussen de Persoon en zijn Zorgverlener onder het vervolg van de verlening van zorg. Voor dit vervolg van de verlening van zorg mag het BSN worden verwerkt. Op grond van artikel 5 sub b Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg dient de Zorgverlener zich namelijk ook voor het vervolg van een goede zorgverlening zich ervan te vergewissen dat het burgerservicenummer betrekking heeft op de Persoon.

De gegevensuitwisseling met een persoonlijke gezondheidsomgeving van de Persoon en de Zorgaanbieder wordt beschouwd als het vervolg van een goede zorgverlening, waarvoor het redelijkerwijs nodig is dat het BSN wordt verwerkt door de Zorgaanbieder bij het verstrekken of opnemen van gegevens.

De Dienstverlener persoon heeft geen wettelijke grondslag om het BSN te mogen verwerken en heeft het BSN ter identificatie van de Persoon ook niet nodig. De Dienstverlener persoon is wel

	<p>om aan deze verplichtingen te voldoen.</p>	<p>verantwoordelijk voor een goede toegangsbeveiliging aan de kant van de Persoon. Wat de afspraken zijn binnen het MedMij Afsprakenstelsel over toegangsbeveiliging en digitale identificatie is toegelicht in <a href="#">Architectuur en technische specificaties</a> evenals in het <a href="#">Normenkader</a> informatiebeveiliging.</p> <p>Voor de uitwisseling van gegevens tussen Zorgaanbieder en de Persoon is geen gespecificeerde toestemming vereist, zoals bedoeld in deze wet. De persoon heeft het recht te mogen beschikken over de over hem/haar vastgelegde gegevens. Wel zal, voortkomend uit de AVG, toestemming moeten zijn verleend door de Persoon aan de Dienstverlener persoon om namens de Persoon gegevens te verwerken en voortkomend uit de WGBO toestemming aan de Zorgaanbieder voor het ophalen van gegevens van of het verstrekken van gegevens aan de Dienstverlener persoon, als derde partij in opdracht van de Persoon (zie eerder). Hoe het verlenen van deze toestemming plaatsvindt, is beschreven in <a href="#">Architectuur en technische specificaties</a>.</p> <p>N.B. de set van persoonsgegevens en informatie uit het medisch dossier die de Zorgaanbieder, nadat de Persoon is geïdentificeerd en de Persoon hiervoor zijn toestemming heeft verleend, verstrekt aan de Dienstverlener Persoon, zou mogelijk ook het BSN van de Persoon kunnen behelzen. De verstrekking van het BSN als onderdeel van deze rechtshandeling is niet toegestaan! De Dienstverlener Persoon is immers niet gerechtigd het BSN te verwerken. Het verdient derhalve aanbeveling dat de Zorgaanbieder bij de verstrekking van de gegevens controleert of het BSN uit de gegevensset is verwijderd.</p>
<p>Toezicht en controle op de naleving</p>	<p>Binnen het zorgaanbiedersdomein zijn verschillende instanties die wettelijk toezicht houden. Dit toezicht op de uitvoering van geldende wet- en regelgeving blijft onverminderd van kracht.</p>	<p>De Stichting MedMij is verantwoordelijk voor controle op de naleving van de verplichtingen van het MedMij Afsprakenstelsel door de deelnemers.</p>

Via het afsprakenstelsel wordt slechts aanvullend toezicht gedefinieerd op de specifieke afspraken binnen het MedMij Afsprakenstelsel.

De instanties die toezicht houden, zijn:

- [Autoriteit Persoonsgegevens \(AP\)](#) - De Autoriteit Persoonsgegevens houdt toezicht op de naleving van de wettelijke regels voor bescherming van persoonsgegevens en adviseert over nieuwe regelgeving;
- [Autoriteit Consument en Markt \(ACM\)](#) - De Autoriteit Consument en Markt houdt toezicht op de mededinging, een aantal specifieke sectoren en het consumentenrecht. De ACM zet zich in voor een gelijk speelveld met bedrijven die zich aan de regels houden, en goed geïnformeerde consumenten die voor hun recht opkomen;
- [Inspectie Gezondheidszorg en Jeugd \(IGJ\)](#) - De Inspectie Gezondheidszorg en Jeugd is onafhankelijk toezichthouder in de Nederlandse gezondheidszorg. Door toezicht, handhaving en opsporing van strafbare feiten bewaken en bevorderen zij de veiligheid en kwaliteit van zorg;
- [Nederlandse Zorgautoriteit \(NZa\)](#) - De Nederlandse Zorgautoriteit zet zich in voor goede en betaalbare zorg die beschikbaar is als je die nodig hebt. Vanuit dat perspectief maakt de NZa regels en

De Stichting MedMij zal niet toezien op de uitvoering van wet- en regelgeving door de deelnemers in het MedMij Afsprakenstelsel. Dit is de verantwoordelijkheid van de genoemde toezichthouders. Het MedMij Afsprakenstelsel betreffen aanvullende afspraken op wet- en regelgeving, vastgelegd in een privaatrechtelijke overeenkomst tussen de deelnemer en de Stichting MedMij. Overtredingen van de wet- en regelgeving kunnen wel gevolgen hebben voor de positie van de Deelnemer in het MedMij Afsprakenstelsel.

	<p>houdt zij toezicht op zorgaanbieders en zorgverzekeraars;</p> <ul style="list-style-type: none"> <li>• <a href="#">Working Party</a> op grond van artikel 29 van de Europese richtlijn (alle toezichthouders op persoonsgegevens in Europa gezamenlijk, in Nederland AP) - De Working Party geeft 'Opinions' hoe de wet geïnterpreteerd moet worden. Zoals de interpretatie van voorwaarden voor anonimiseren, certificeren en PIA's.</li> </ul>	
<p><a href="#">Verordening (EU) 2017/745 van het Europees parlement en de Raad betreffende medische hulpmiddelen</a></p> <p>(gepubliceerd 05-04-2017, geldend vanaf 26-05-2020)</p>	<p>Deze verordening heeft tot doel het soepel functioneren van de interne markt voor medische hulpmiddelen te garanderen, uitgaande van een hoog beschermingsniveau voor de gezondheid van patiënten en gebruikers, en rekening houdend met de kleine en middelgrote ondernemingen die in deze sector actief zijn.</p> <p>Tegelijkertijd stelt deze verordening hoge kwaliteits- en veiligheidseisen aan medische hulpmiddelen, teneinde tegemoet te komen aan gemeenschappelijke veiligheidsbezwaren ten aanzien van dergelijke producten.</p> <p>Beide doelstellingen worden gelijktijdig nagestreefd en zijn onlosmakelijk met elkaar verbonden waarbij de ene niet ondergeschikt is aan de andere.</p>	<p>De Inspectie Gezondheidszorg en Jeugd beschrijft op haar <a href="#">eigen website</a> de toepassing van de verordening. Daarbij geeft de IGJ aan dat "de nieuwe regelgeving omvat veel (met name technische) zaken die de komende tijd nog nader worden uitgewerkt door de Europese Commissie en de lidstaten van de EU".</p> <p>Vanuit het MedMij Afsprakenstelsel worden geen aanvullende zaken geregeld met betrekking tot medische hulpmiddelen. Deelnemers dienen zelf een afweging te maken met betrekking tot de toepassing van deze verordening voor hun eigen dienstverlening.</p>
<p><a href="#">Aanpassingswet richtlijn inzake elektronische handel</a></p> <p>(geldend vanaf 30-06-2014)</p>	<p>Met deze wet wordt de Richtlijn inzake elektronische handel geïmplementeerd. Deze richtlijn heeft tot doel om bij te dragen aan de goede werking van de interne markt door het vrije verkeer van diensten van</p>	<p>Vanuit het MedMij Afsprakenstelsel worden geen aanvullende zaken geregeld met betrekking tot deze aanpassingswet. Deelnemers dienen zelf een afweging te maken met betrekking tot de invulling van deze aanpassingswet voor hun eigen dienstverlening.</p>

	de informatiemaatschappij tussen de lidstaten te waarborgen. Dit wordt gerealiseerd door belemmeringen voor de elektronische handel weg te nemen.	
<p><b>Implementatiewet richtlijn consumentenrechten</b></p> <p>(geldend vanaf 13-06-2014)</p>	<p>Deze wet implementeert de richtlijn consumentenrechten. Met deze wet wordt consumenteninformatie voor verkoop in de winkel, op afstand (via onder andere internet en telefoon) en buiten verkooppromten (bijvoorbeeld colportage) geregeld.</p> <p>Ook wordt er voor verkoop op afstand en buiten verkooppromten het herroepingsrecht (bedenktijd voor de consument) geregeld.</p>	<p>Vanuit het MedMij Afsprakenstelsel worden geen aanvullende zaken geregeld met betrekking tot deze implementatiewet. Deelnemers dienen zelf een afweging te maken met betrekking tot de invulling van deze implementatiewet voor hun eigen dienstverlening.</p>
<p><b>Wet gelijke behandeling op grond van handicap en chronische ziekte (wgbh/cz)</b></p> <p>(geldend vanaf 03-04-2003)</p>	<p>De wet gelijke behandeling op grond van handicap en chronische ziekte (wgbh/cz) is ook van toepassing op digitale goederen en diensten. Dit houdt in dat aanbieders van goederen en diensten gehouden zijn om doeltreffende aanpassingen te verrichten (art. 2) en geleidelijk toe te werken naar algemene toegankelijkheid (art. 2a), mits dit geen onevenredige belasting vormt. Het Besluit Toegankelijkheid licht toe dat sectoren werk kunnen maken van de stap naar algemene toegankelijkheid via actieplannen.</p>	<p>Vanuit het MedMij Afsprakenstelsel worden geen aanvullende zaken geregeld met betrekking tot deze aanpassingswet. Deelnemers dienen zelf een afweging te maken met betrekking tot de invulling van deze wet voor hun eigen dienstverlening. Het advies in algemene zin is: ga als ontwikkelaar van digitale goederen en diensten, waaronder ook de deelnemers in het MedMij afsprakenstelsel vallen, vooral ook het gesprek aan met gebruikersgroepen waarin gebruikers met een beperking vertegenwoordigd zijn. Om in dialoog te bepalen welke ontwerpbevestigingen je kunt meenemen. Vaak kom je in die dialoog vanzelf ook tot de evenredige aanpassingen, die je bovendien dan vanaf de start kunt meenemen.</p> <p>Handvatten/concreet stappenplan voor uitvoering: <a href="https://www.digitoegankelijk.nl/onderwerpen/stappenplan-toegankelijkheid">https://www.digitoegankelijk.nl/onderwerpen/stappenplan-toegankelijkheid</a></p> <p>De verplicht te gebruiken schermen voor de toestemmings- en bevestigingsverklaring binnen het afsprakenstelsel in de usecases voor verzamelen en delen (<a href="#">architectuur en technische specificaties</a>) zijn toegankelijk</p>

		gemaakt conform de bepalingen in deze wet. Hetzelfde geldt voor de schermen van een door BZK aangewezen authenticatiemiddel.
Aansprakelijkheid	<p>Voor de aansprakelijkheid gelden de algemene regels van het Nederlands recht ten aanzien van de inhoud en omvang van wettelijke verplichtingen tot schadevergoeding.</p> <p>Aansprakelijkheid kan voortvloeien uit het niet nakomen van een wettelijke verplichting en/of het niet betrachten van de nodige zorgvuldigheid die gelet op de omstandigheden van het geval redelijkerwijs van de desbetreffende partij kan worden verwacht.</p> <ul style="list-style-type: none"> <li>• Bij het 'niet nakomen van een wettelijke verplichting' gaat het bijvoorbeeld om de niet naleving van de voor de deelnemer van toepassing zijnde (specifieke) wet- en regelgeving omtrent privacy en informatiebeveiliging.</li> <li>• Bij het 'betrachten van de nodige zorgvuldigheid' gaat het dan bijvoorbeeld om de inrichting van processen die ervoor zorgen dat aan de eisen die voor de deelnemer in het MedMij Afsprakenstelsel zijn opgenomen wordt voldaan en deze ook worden nageleefd.</li> </ul>	<p>Binnen het MedMij Afsprakenstelsel is iedere deelnemer aansprakelijk voor zijn eigen handelen en/of nalaten binnen de rol die hij vervult. De deelnemers mogen en kunnen niet afwijken van de algemene regels van het Nederlands recht. Hoe deze regels in een concreet geval uitwerken, is afhankelijk van de feiten en de omstandigheden van het geval.</p> <p>De aansprakelijkheid is voor Deelnemers in ieder geval uitdrukkelijk beperkt tot het eigen handelen van de Deelnemer. Hiermee wordt voorkomen dat een Deelnemer aansprakelijk zou worden gesteld voor gevallen waarbij schade optreedt die niet door hem is veroorzaakt of aan hem is toe te rekenen.</p>



## Overeenkomsten en rechtsrelaties

Het MedMij Afsprakenstelsel waarborgt dat binnen het MedMij-netwerk op een veilige en betrouwbare manier persoonsgegevens en/of gezondheidsinformatie tussen de Deelnemers worden uitgewisseld. Om dit te bewerkstelligen behelst het MedMij Afsprakenstelsel informatiestandaarden, technische, organisatorische en juridische afspraken. Als gevolg van het afsluiten van de Deelnemersovereenkomst met de Stichting MedMij - nadat hiertoe de toetredingsprocedure succesvol is doorlopen - worden de Dienstverleners Zorgaanbieders en Dienstverlener Personen Deelnemer van het MedMij Afsprakenstelsel. Iedere partij die aantoonbaar voldoet aan de afspraken van het MedMij Afsprakenstelsel kan toetreden en Deelnemer worden van het MedMij Afsprakenstelsel. Als onderdeel van het toetredingsproces zijn Deelnemers tevens gehouden de [Zelfverklaring integriteit](#) te overleggen.

Als Deelnemer van het MedMij Afsprakenstelsel committeren partijen zich aan de naleving van de verplichtingen en afspraken die voor hun rol uit het MedMij Afsprakenstelsel voortvloeien. Deelnemers mogen op basis van de Deelnemersovereenkomst hun Diensten leveren aan Gebruikers onder de merknaam MedMij. Om deze Diensten via het MedMij-netwerk te kunnen leveren zijn deze partijen toegetrokken tot het MedMij Afsprakenstelsel. De Persoon en de Zorgaanbieder zijn Gebruiker van Diensten van Deelnemers in het MedMij Afsprakenstelsel.

De Deelnemers zijn zelf verantwoordelijk voor het afsluiten van dienstverleningsovereenkomsten met hun Gebruikers. Deelnemers zijn immers ook zelf verantwoordelijk voor de veilige en betrouwbare werking van de Diensten die zij aanbieden. Om ervoor te zorgen dat dienstverleningsovereenkomsten tussen de Deelnemers en Gebruikers wel goed aansluiten op de Diensten, die met inzet van het MedMij-netwerk, worden geleverd, wordt vanuit het MedMij Afsprakenstelsel informatie ter beschikking gesteld die door de Deelnemer kan worden gebruikt bij het afsluiten van zijn dienstverleningsovereenkomst met de Gebruiker. Voorbeelden van informatie die via het MedMij Afsprakenstelsel voor Deelnemers ter beschikking wordt gesteld zijn de Gebruiksvoorlichting persoonsdomein, Gebruiksvoorlichting zorgdomein en de Modelverwerkersovereenkomst Zorgaanbieder - Dienstverlener Zorgaanbieder.

De Gebruiker bepaalt zelf of hij/zij gebruik wil maken van een persoonlijke gezondheidsomgeving. Zo ja, kiest hij/zij een persoonlijke gezondheidsomgeving en kan controleren of deze tevens Deelnemer is en Diensten aanbiedt conform het MedMij Afsprakenstelsel in de lijst van Deelnemers die op de website van het MedMij Afsprakenstelsel is gepubliceerd.

## Overzicht van partijen en rechtsrelaties

Bij de uitwisseling van (persoons)gegevens en gezondheidsinformatie tussen Gebruikers via het MedMij-netwerk worden verschillende partijen onderscheiden die zich weer in verschillende rechtsrelaties tot elkaar verhouden. In de architectuur en technische specificaties van het MedMij Afsprakenstelsel is uitgewerkt welke rollen deze partijen binnen de architectuur vervullen, de functies die zij op de verschillende netwerklagen vervullen, alsmede welke gegevens zij met elkaar uitwisselen.

Om de verantwoordelijkheden binnen het proces van de uitwisseling van gezondheidsgegevens binnen het MedMij Netwerk inzichtelijk te maken, is hieronder vanuit juridisch perspectief een overzicht van de rechtsrelaties tussen de verschillende partijen opgenomen die een rol spelen binnen het MedMij Afsprakenstelsel. Het gaat dan om de volgende actoren:

1. de Stichting MedMij als eindverantwoordelijke voor het MedMij Afsprakenstelsel;
2. de Beheerorganisatie en/of uitvoeringsorganisatie die in opdracht van de Stichting zorgdraagt voor het beheer van het MedMij Afsprakenstelsel;
3. de Deelnemer (Dienstverlener Zorgaanbieder) die binnen de kaders van het MedMij Afsprakenstelsel Diensten aanbiedt aan de Zorgaanbieder;
4. de Deelnemer (Dienstverlener Persoon) die binnen de kaders van het MedMij Afsprakenstelsel Diensten aanbiedt aan de Persoon;
5. de Zorgaanbieder als Gebruiker die Diensten afneemt van de Dienstverlener Zorgaanbieder, en



6. de Persoon als Gebruiker die Diensten afneemt van de Dienstverlener Persoon.

## Rechtsrelaties MedMij Afsprakenstelsel

Hieronder is het overzicht opgenomen van rechtsrelaties tussen de actoren waarop het MedMij Afsprakenstelsel van toepassing is met verwijzing naar de overeenkomsten in het MedMij Afsprakenstelsel.

Het uitgangspunt van het MedMij Afsprakenstelsel is dat Deelnemers (dus Dienstverlener Zorgaanbieder en Dienstverlener Persoon) als tussenpersoon voor hun Gebruikers fungeren. Er is sprake van vertegenwoordiging. Dit houdt in dat de Deelnemers in opdracht van respectievelijk de Persoon en de Zorgaanbieder de gegevensuitwisseling tussen de Persoon en de Zorgaanbieder verzorgen. De Diensten die in het kader van deze opdrachtverlening via het MedMij-netwerk worden geleverd bestrijken de contractuele relaties van het Afsprakenstelsel MedMij.

Rechtsrelaties binnen MedMij	Type overeenkomst
1. Stichting MedMij - Dienstverlener Persoon	Deelnemersovereenkomst Dienstverlener persoon
2. Stichting MedMij - Dienstverlener Zorgaanbieder	Deelnemersovereenkomst Dienstverlener zorgaanbieder

De [Deelnemersovereenkomst Dienstverlener persoon](#) en de [Deelnemersovereenkomst Dienstverlener zorgaanbieder](#) bevatten de basisafspraken tussen Stichting MedMij en de Dienstverlener persoon respectievelijk de Dienstverlener zorgaanbieder. De Deelnemersovereenkomst is voor alle Deelnemers in dezelfde rol gelijk en zorgt ervoor dat Deelnemers gehouden zijn de op hen rustende verantwoordelijkheden te nemen en verplichtingen en afspraken uit het MedMij Afsprakenstelsel zorgvuldig uit te voeren en aantoonbaar na te leven. Ook bindt de overeenkomst Deelnemers aan de besturingsafspraken die noodzakelijk zijn voor het borgen van het vertrouwen in MedMij. Deelnemers mogen binnen MedMij in hun rol alleen diensten verrichten indien zij een Deelnemersovereenkomst hebben gesloten met de Stichting MedMij. Het onderlinge vertrouwen tussen partijen bij het gebruik van MedMij is (mede) gebaseerd op de overeenkomsten die de Deelnemers en de Stichting MedMij binden aan het nakomen van de afspraken in het MedMij Afsprakenstelsel. De Deelnemers zijn verantwoordelijk voor de doorvertaling van de afspraken naar hun klanten en derden. De Deelnemers zijn, binnen de kaders van het MedMij Afsprakenstelsel, vrij om zelf in een overeenkomst met de Gebruiker nadere afspraken te maken over de inhoud en de omvang van hun dienstverlening.

## Overige rechtsrelaties

Hieronder is een overzicht opgenomen van rechtsrelaties die van wezenlijke invloed zijn op het vertrouwen in en een veilige en betrouwbare verwerking van en gegevensuitwisseling via het MedMij Afsprakenstelsel. Deze rechtsrelaties zijn van belang omdat in het technische ontwerp en de architectuur van het MedMij Netwerk componenten zijn opgenomen waarbij partijen in deze rechtsrelaties een uitvoerende verplichting hebben. Dat betekent dat afspraken tussen deze partijen ook randvoorwaardelijk zijn voor een veilige, interoperabele en betrouwbare gegevensuitwisseling tussen de persoonlijke gezondheidsomgeving MedMij en de informatiesystemen van de Zorgaanbieders.

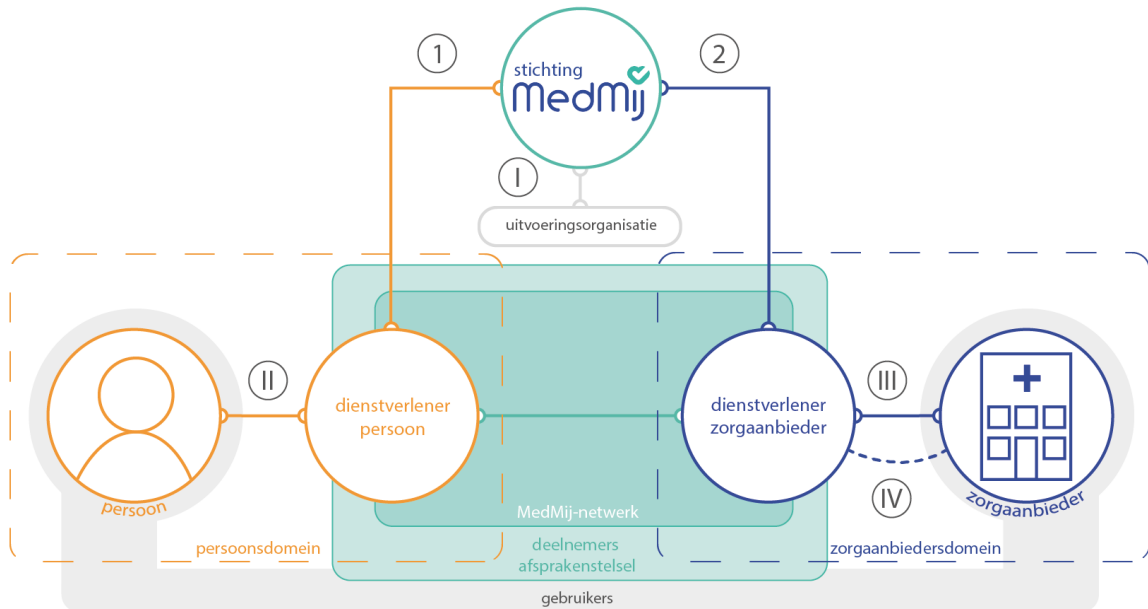
Rechtsrelaties die van belang zijn voor MedMij	Type overeenkomst

I. Stichting MedMij - Beheer /uitvoeringsorganisatie	Opdrachtverlening voor ondersteuning en uitvoering van taken van Stichting MedMij zoals: <ol style="list-style-type: none"> <li>1. De instandhouding van de goede technische werking van de gemeenschappelijke voorzieningen in het afsprakenstelsel.</li> <li>2. Het voeren van de regie over de werking van het Netwerk en het beheer van het MedMij Afsprakenstelsel.</li> </ol>
II. Dienstverlener Persoon - Gebruiker	Dienstverleningsovereenkomst Persoon.  Binnen het MedMij Afsprakenstelsel wordt voor deze rechtsrelatie de Gebruiksvoorlichting persoonsdomein ter beschikking gesteld.
III. Dienstverlener Zorgaanbieder - Gebruiker	Binnen het MedMij Afsprakenstelsel wordt voor deze rechtsrelatie de Gebruiksvoorlichting zorgdomein ter beschikking gesteld
IV. Zorgaanbieder – Dienstverlener Zorgaanbieder	Verwerkersovereenkomst

De rechtsrelaties genoemd onder I t/m IV vallen buiten de overeenkomsten die moeten worden afgesloten voor toetreding tot het MedMij Afsprakenstelsel maar dienen dus - voor het vertrouwen en een betrouwbare en veilige werking van het MedMij Afsprakenstelsel - wel degelijk tussen de betrokken partijen te worden afgesloten. Partijen zijn echter zelf verantwoordelijk voor het afsluiten van deze overeenkomsten.

De uitvoering van verwerkingen door een Verwerker dient geregeld te zijn in een schriftelijke overeenkomst tussen Verwerker en Verwerkingsverantwoordelijke. De meeste Dienstverleners zorgaanbieder zullen al een dergelijke verwerkersovereenkomst hebben met de Zorgaanbieder. Voor de specifieke MedMij-aspecten is de [Modelverwerkersovereenkomst](#) te gebruiken. In het geval er al een bestaande overeenkomst is afgesloten tussen Verwerker en Verwerkingsverantwoordelijke kunnen partijen ervoor kiezen de specifieke bepalingen in relatie tot de verwerking van persoonsgegevens voor MedMij uit de [Modelverwerkersovereenkomst](#) te integreren in de bestaande verwerkersovereenkomst. Hierbij is te denken aan zaken zoals het verwerken van burgerservicenummer ten behoeven van authenticatie, het verkrijgen van toestemming van de Persoon voor het verstrekken van gegevens aan een derde partij namelijk de Dienstverlener persoon, het verwerken van persoonsgegevens ten behoeve van de gegevensuitwisseling (zoals logging) en de verwerking van de betreffende persoonsgegevens zelf.

Alle rechtsrelaties zijn privaatrechtelijk van aard en alle deelnemers zijn gebonden aan Nederlands recht. De figuur hieronder geeft de verschillende rechtsrelaties weer.



# Toelichting verwerkingsverantwoordelijkheid

## Inleiding

Het MedMij Afsprakenstelsel onderscheidt om te beginnen twee use cases voor de gegevensuitwisseling tussen de *Persoon* en zijn *Zorgaanbieder*, namelijk de use case [Verzamelen](#) en de use case [Delen](#). Met de use case *Verzamelen* kan de *Persoon* zijn gegevens en gezondheidsinformatie in zijn PGO inkijken, opslaan en beheren. Met de use case *Delen* kan de *Persoon* gegevens en gezondheidsinformatie vanuit zijn PGO aan zijn *Zorgaanbieder* aanbieden, opdat de *Zorgaanbieder* deze informatie kan opnemen in zijn medisch dossier.

Daarnaast is er de use case [Abonneren](#), waarmee *Persoon* en *Zorgaanbieder* kunnen afspreken dat de *Zorgaanbieder* gedurende een zekere looptijd meldingen kan doen bij de PGO over wijzigingen in beschikbare gezondheidsgegevens. Die meldingen heten *Notificaties*. Na het afspreken van zo'n abonnement gebruiken partijen de use case [Notificeren](#) voor het uitwisselen van die meldingen.

In de uitvoering van de use case *Verzamelen* en de use case *Delen* zijn verschillende rollen betrokken. Hieronder wordt voor de voornoemde use cases uitgewerkt welke partij waar in het proces welke (verwerkings)verantwoordelijkheid heeft gelet op de (specifieke) privacy wet- en regelgeving die op betrokken partijen van toepassing is.

## Authenticatie

Voor de use cases *Verzamelen*, *Delen* en *Abonneren* geldt dat in het geval de *Persoon* gegevens en/of gezondheidsinformatie met zijn *Zorgaanbieder* wil uitwisselen, of een abonnement aangaat, de *Zorgaanbieder* de *Persoon* altijd eerst moet identificeren en authenticeren. Zoals ook in het [Juridisch kader](#) is aangegeven wordt hiervoor binnen het MedMij Afsprakenstelsel gebruik gemaakt van een door het ministerie van BZK aangewezen authenticatiemiddel. Het identificatie- en authenticatieproces geschiedt onder de verantwoordelijkheid van de *Zorgaanbieder*. De *Zorgaanbieder* is immers op grond van de artikelen 4, 5 en 6 van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg, in het kader van het verlenen van zorg, verplicht de identiteit van de patiënt vast te stellen. Hiervoor mag op basis van deze wet het BSN door de *Zorgaanbieder* worden verwerkt. De interactie tussen de *Persoon* en zijn *Zorgaanbieder* via het MedMij Afsprakenstelsel wordt beschouwd als een handeling die valt onder (het vervolg van) de verlening van zorg. Hiervoor mag dan ook het BSN worden verwerkt. In het licht van de AVG betekent dit dat het de *Zorgaanbieder* is toegestaan om het BSN te verwerken op grond van art. 87 AVG en 46 Uitvoeringswet AVG. De rechtmatigheidsgrondslag voor de verwerking van het BSN op grond van de AVG is hiermee de uitvoering van een wettelijke verplichting die op de *Zorgaanbieder* als verwerkingsverantwoordelijke rust (art. 6 lid 1 sub c AVG).

De *Zorgaanbieder* maakt in het authenticatieproces van de *Persoon* — die via MedMij gegevens /gezondheidsinformatie met zijn *Zorgaanbieder* wil delen — gebruik van een verwerker: de *Dienstverlener zorgaanbieder*. Deze *Dienstverlener zorgaanbieder* heeft enerzijds — om als *Deelnemer* in het MedMij Afsprakenstelsel zijn *Diensten* aan de *Zorgaanbieder* te mogen aanbieden — een *Deelnemersovereenkomst* met de Stichting MedMij gesloten. Anderzijds heeft deze *Dienstverlener zorgaanbieder* een [verwerkersovereenkomst](#) met de *Zorgaanbieder* gesloten. Op basis van deze verwerkersovereenkomst zorgt hij feitelijk voor, weliswaar namens, onder controle en in opdracht van de *Zorgaanbieder*, de authenticatie van de *Persoon*. Deze verwerkersovereenkomst rechtvaardigt de verwerking van de gegevens, gezondheidsinformatie en het BSN door de *Dienstverlener zorgaanbieder* in de rol van verwerker. De *Dienstverlener zorgaanbieder* wordt in zijn rol als verwerker beschouwd als de feitelijk beheerder van het medisch dossier die namens de *Zorgaanbieder* handelt en waarover de *Zorgaanbieder* als verwerkingsverantwoordelijke controle heeft (via de verwerkersovereenkomst). Voor deze situatie geldt het zogenoemde afgeleid beroepsgeheim. Dit houdt in dat de *Zorgaanbieder* aansprakelijk is als door de *Dienstverlener zorgaanbieder* in strijd met de geheimhoudingsplicht gegevens worden verwerkt. Vanwege het feit dat in de relatie tussen de *Dienstverlener zorgaanbieder* en de *Zorgaanbieder* het afgeleide

beroepsgeheim geldt en de verwerkingsverantwoordelijke hier op kan worden aangesproken wordt de *Dienstverlener zorgaanbieder* hiermee als rechtstreeks betrokkene in de zin van art. 7:457 BW beschouwd. Voor deze situatie hoeft op grond van art 7:457 BW geen toestemming door de patiënt te worden gegeven.

Met het oog op authenticatie handelt de *Persoon* dus rechtstreeks (via de *Dienstverlener zorgaanbieder* als verwerker) met de *Zorgaanbieder*. Als hij gegevens wenst uit te wisselen met zijn *Zorgaanbieder*, dient de *Persoon* zich eerst te authenticeren bij zijn *Zorgaanbieder*. Met deze rechtstreekse relatie wordt gewaarborgd dat de *Dienstverlener persoon* nimmer de beschikking heeft over het BSN en/of informatie ten behoeve van de authenticatie van de *Persoon*, anders dan de terugkoppeling van de *Zorgaanbieder* (via de *Dienstverlener zorgaanbieder*) dat de *Persoon* wel of geen gegevens kan uitwisselen met de desbetreffende *Zorgaanbieder*. Identificatie en authenticatie van de *Persoon* is derhalve een aparte rechtstreekse rechtshandeling tussen de *Zorgaanbieder* (via de *Dienstverlener zorgaanbieder*) en de *Persoon*. Zonder deze identificatie en authenticatie worden er geen gegevens uitgewisseld. Pas nadat de identificatie en authenticatie heeft plaatsgevonden, kan de gegevensuitwisseling in het kader van MedMij plaatsvinden. Deze gegevensuitwisseling die op het authenticatieproces volgt, is een rechtshandeling tussen enerzijds de *Dienstverlener persoon* en de *Persoon* en de *Dienstverlener persoon* en de *Zorgaanbieder* anderzijds. In deze rechtshandeling vindt de uitwisseling van de gegevens over de gezondheid plaats op basis van uitdrukkelijke toestemming van de *Persoon*. Zie hiervoor ook onderstaande paragraaf UC Verzamelen en UC Delen.

## UC Verzamelen en UC Delen

### Toestemming aan de *Dienstverlener persoon* voor verstrekking

Zowel voor de use case Delen als de use case Verzamelen dient de *Dienstverlener persoon* op basis van de AVG toestemming te hebben voor de verwerking van de gegevens over de gezondheid van de *Persoon*. Om ervoor te zorgen dat de *Persoon* met gebruik van zijn PGO via het MedMij-netwerk gegevens kan uitwisselen en zijn gegevens en gezondheidsinformatie in zijn PGO kan beheren, sluit de *Persoon* een overeenkomst met de *Dienstverlener persoon*. Deze *Dienstverlener persoon* handelt — nadat identificatie en authenticatie tussen de *Persoon* en de *Zorgaanbieder* heeft plaatsgevonden — op basis van deze dienstverleningsovereenkomst namens de *Persoon* bij de gegevensuitwisseling tussen de *Persoon* en de *Zorgaanbieder*. In het licht van de AVG is de *Dienstverlener persoon* hiermee de verwerkingsverantwoordelijke in de uitvoering van de dienstverleningsovereenkomst waarbij de *Persoon* via de PGO MedMij persoonsgegevens/gezondheidsinformatie deelt of uitwisselt met zijn *Zorgaanbieder*. De rechtmatigheidsgrondslag 'noodzakelijk voor de uitvoering van de overeenkomst' (art. 6 lid 1 sub b AVG) is van toepassing voor de verwerking van de gewone persoonsgegevens in relatie tot de dienstverleningsovereenkomst die tussen de *Dienstverlener persoon* en de *Persoon* wordt afgesloten. Daarnaast is de rechtmatigheidsgrondslag 'uitdrukkelijke toestemming' (art 9 lid 2 sub a AVG) van toepassing voor de verwerking van de gegevens over de gezondheid van *Persoon* (bijzonder persoonsgegeven) in relatie tot de PGO. Vorenstaande betekent dat de *Dienstverlener persoon* zowel in relatie tot de use case Verzamelen als de use case Delen als verwerkingsverantwoordelijke de expliciete toestemming van de *Persoon* moet hebben alvorens de *Persoon* gebruik maakt van zijn PGO.

Op grond van de artikelen 7 en 8 AVG moet de *Dienstverlener persoon* als verwerkingsverantwoordelijke in relatie tot 'toestemming' voor de gegevensuitwisseling via de PGO het volgende kunnen aantonen:

- a. dat en waarvoor de *Persoon* toestemming heeft verleend;
- b. dat de toestemming vrijelijk, specifiek, geïnformeerd en ondubbelzinnig is gegeven, en
- c. wie de verwerkingsverantwoordelijke is, wat de specifieke doeleinden/ het specifieke doel van de verwerking is, wie de ontvangers van de persoonsgegevens zijn en het recht om de toestemming te allen tijde in te trekken.

Om dit te kunnen aantonen, zal de *Dienstverlener persoon* een verklaring van toestemming moeten opstellen. Deze verklaring dient in een begrijpelijke, gemakkelijke, toegankelijke vorm en in duidelijke taal te worden opgesteld. Bij het geven van de toestemming moet om een actieve handeling van de *Persoon* gaan. De voornoemde informatie in relatie tot toestemming zal voorafgaand aan het daadwerkelijk geven van de toestemming moeten zijn verstrekt. Ook dit zal door de *Dienstverlener persoon* moeten kunnen worden aangetoond.

## Toestemming aan de *Zorgaanbieder* voor verstrekking

Zowel voor de use case Delen als de use case Verzamelen dient de *Persoon* voor een rechtmatige uitwisseling van gegevens over zijn gezondheid zijn toestemming ook aan de *Zorgaanbieder* te hebben verleend. Deze toestemming heeft betrekking op de situatie dat de *Dienstverlener persoon* de gegevens die hij — via het MedMij-netwerk (door middel van de *Dienstverlener zorgaanbieder*) en na de authenticatie van de *Persoon* door de *Zorgaanbieder* — over de *Persoon* van de *Zorgaanbieder* ontvangt ook rechtmatig verwerkt. Deze toestemming vloeit voort uit de WGBO. Op basis van artikel 7: 457 BW mogen gegevens uit het medisch dossier immers niet met 'anderen' worden gedeeld, tenzij de patiënt hiervoor zijn toestemming heeft gegeven. De *Dienstverlener persoon* aan wie de *Zorgaanbieder* gegevens over de *Persoon* verstrekt ten behoeve van de PGO wordt als een 'ander' in de zin van de WGBO beschouwd. Voor deze specifieke situatie is een [toestemmingsverklaring](#) in het MedMij Afsprakenstelsel opgenomen, en wel in de use cases Verzamelen en Abonneren. In het geval van de use case Abonneren zijn het *Notificaties* die de gezondheidsgegevens vormen.

## Rechtmatigheidsgrondslag *Zorgaanbieder* ontvangen

Tot slot nog de grondslag voor de *Zorgaanbieder* als verwerkingsverantwoordelijke om gezondheidsgegevens van de *Persoon* te ontvangen bij de use case Delen. Bij de use case Delen wordt op initiatief van de *Persoon* (door middel van de *Dienstverlener persoon*) persoonsgegevens en/of gegevens over de gezondheid van de *Persoon* (door middel van de *Dienstverlener zorgaanbieder*) aan de *Zorgaanbieder* aangeboden met het verzoek deze informatie op te nemen in het medisch dossier. De rechtmatigheidsgrondslag voor de verwerking van deze gegevens vloeit voort uit de behandelrelatie die de *Zorgaanbieder* met de *Persoon* heeft op grond van art. 7: 446 BW, alsmede de verplichting (op grond van art. 7: 454 BW) om een medisch dossier met betrekking tot de behandeling van de patiënt in te richten. In het licht van de AVG betekent dit dat het is toegestaan voor de *Zorgaanbieder* om persoonsgegevens te verwerken omdat dit noodzakelijk is voor de uitvoering van een overeenkomst (art. 6 lid 1 sub b AVG) en de uitvoering van een wettelijke verplichting (art. 6 lid 1 sub c AVG). Specifiek ten aanzien van de gezondheidsgegevens is het de *Zorgaanbieder* toegestaan om op grond van artikel 9 lid sub f AVG deze gegevens te verwerken.

Het is aan de *Zorgaanbieder* om te beoordelen of de gegevens en/of de gezondheidsinformatie die door de *Persoon* worden aangeboden ook relevant zijn voor het medisch dossier en in dit dossier worden opgenomen. Zie ook het [Juridisch kader](#). Alvorens een *Zorgaanbieder* dit beoordeelt dient eerst door de *Dienstverlener zorgaanbieder* (namens de *Zorgaanbieder*) te worden gecontroleerd of er inderdaad in ieder geval een behandelrelatie is met de desbetreffende *Persoon*. Op basis van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg is de *Zorgaanbieder* voor deze situatie ook gehouden de identiteit van de *Persoon* te verifiëren. Indien blijkt dat er inderdaad een behandelrelatie is en de *Zorgaanbieder* (door middel van de *Dienstverlener zorgaanbieder* en de *Dienstverlener zorgaanbieder* via de *Dienstverlener persoon*) aan de *Persoon* laat weten dat hij ontvankelijk is om de gegevens te ontvangen, wordt door de *Dienstverlener zorgaanbieder*, in de vorm van een controle vraag nog eens aan de *Persoon* gevraagd of hij inderdaad gegevens wil delen met zijn *Zorgaanbieder*. Hiervoor is in het MedMij Afsprakenstelsel een [bevestigingsverklaring](#) opgenomen. Op het moment dat de *Persoon* dit heeft bevestigd, stuurt de *Dienstverlener zorgaanbieder* een zogenaamd access token aan de *Dienstverlener persoon* van de *Persoon* op basis waarvan de *Dienstverlener persoon* kan afleiden dat de *Zorgaanbieder* ontvankelijk is voor het delen van gegevens door de desbetreffende *Persoon*. Met deze code kan de *Dienstverlener persoon* de



gegevens en/of de gezondheidsinformatie die de *Persoon* wenst te delen (via de *Dienstverlener zorgaanbieder*) doorzetten aan de *Zorgaanbieder*. Zoals eerder aangegeven, bepaalt de *Zorgaanbieder* vervolgens of hij deze informatie ook wenst op te nemen in het medisch dossier.

Door een access token te gebruiken bij de use case Delen wordt gewaarborgd dat de *Dienstverlener persoon* ook in de use case Delen geen BSN verwerkt. Gelet op het feit dat de *Dienstverlener persoon* wel een access token ontvangt, kan door de *Dienstverlener persoon* echter wel worden afgeleid dat er sprake is van een behandelrelatie. Dit gegeven kan als een 'gegeven over de gezondheid' in de zin van artikel 4 lid 15 AVG worden beschouwd waarvoor voor de rechtmatige verwerking hiervan door de *Dienstverlener persoon* op grond van artikel 9 lid 2 sub a AVG 'uitdrukkelijke toestemming' door de *Persoon* moet worden verleend. Dit betekent dat de *Dienstverlener persoon* in zijn verklaring van toestemming die hij op grond van artikel 7 en 8 AVG moet opstellen, ook informatie over deze verwerking dient op te nemen.

In het geval de *Zorgaanbieder* (via de *Dienstverlener zorgaanbieder*) aan de *Persoon* laat weten dat er geen behandelrelatie is met de desbetreffende *Persoon* ontvangt de *Dienstverlener persoon* (via de *Dienstverlener zorgaanbieder*) het bericht dat de *Zorgaanbieder* niet ontvankelijk is voor het delen van gegevens door de desbetreffende *Persoon*. In deze situatie dient de *Dienstverlener zorgaanbieder* de persoonsgegevens die in relatie tot de use case Delen zijn verwerkt, overeenkomstig het bepaalde in de [modelverwerkersovereenkomst](#), te verwijderen en/of te vernietigen. De rechtmatigheidsgrondslag voor de *Zorgaanbieder* en de *Dienstverlener zorgaanbieder* om in deze situatie wel het BSN te verwerken, is dat de *Zorgaanbieder* op grond van de Wet aanvullende bepalingen verwerking persoonsgegevens in het identificatieproces verplicht is het BSN te gebruiken.

## Toelichting AVG-normen

Gegevens die door deelnemers aan het MedMij Afsprakenstelsel worden uitgewisseld betreffen bijna altijd bijzondere persoonsgegevens. Deelnemers moeten hiervoor voldoen aan de normen die de AVG stelt met betrekking tot het verwerken van deze persoonsgegevens. Vanwege het belang van een correcte uitvoering van deze wet door deelnemers aan het MedMij Afsprakenstelsel, heeft MedMij hieronder een toelichting op de verantwoordelijkheden en normen in de AVG opgenomen. Indien aan de orde, is in een tweede kolom aangegeven of het MedMij Afsprakenstelsel een nadere invulling, dan wel een aanvulling heeft gedefinieerd op dat onderwerp. In een derde kolom is een eventuele opmerking of een aandachtspunt voor deelnemers opgenomen.

Onderstaande tabel is een hulpmiddel voor de deelnemer. De publicatie van deze tabel doet niets af aan de eigen verantwoordelijkheid van de verwerkingsverantwoordelijke om de AVG te implementeren. Deelnemers zijn zelf verantwoordelijk voor de correcte implementatie van de wet. Bij [Toetreding](#) tot het stelsel verklaart de deelnemer met de [Zelfverklaring integriteit](#) te voldoen aan de AVG.



Artikel AVG	Norm AVG	Aanvulling MedMij Afsprakenstelsel	Opmerking en/of aandachtspunt
<i>Toepassingsgebied AVG</i>			
<b>Artikel 2, 3</b>	<p>De AVG is van toepassing op:</p> <ul style="list-style-type: none"> <li>• verwerkingen die geheel of gedeeltelijk geautomatiseerd zijn, alsmede;</li> <li>• op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Onder 'bestand' wordt elk gestructureerd geheel van persoonsgegevens begrepen die volgens bepaalde criteria toegankelijk zijn.</li> </ul> <p>Verwerking van persoonsgegevens waarop de AVG van toepassing is moet plaatsvinden in het kader van activiteiten van een vestiging van een verwerkingsverantwoordelijke of een verwerker in de Europese Unie, ongeacht of de verwerking al dan niet plaatsvindt in de Europese Unie.</p> <p>De AVG is ook van toepassing op organisaties die buiten de Europese Unie zijn gevestigd, indien zij persoonsgegevens verwerken van betrokkenen in de Europese Unie óf indien zij het gedrag van betrokkenen in de Europese Unie monitoren.</p>	<p>Het MedMij Afsprakenstelsel bepaalt dat zijn deelnemers ingeschreven dienen te zijn in een handelsregister in de EU. Inschrijving in een handelsregister in de EU impliceert ofwel een vestiging in de EU, ofwel ondernemingsactiviteiten in de EU. Derhalve is de AVG van toepassing op deelnemers aan het afsprakenstelsel.</p>	

Algemene bepalingen en definities		
<b>Artikel 4, 9</b>	<p>Het begrip 'persoonsgegevens' betreft alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon.</p> <p>De AVG maakt een onderscheid tussen:</p> <p>1) persoonsgegevens, en</p> <p>2) bijzondere categorieën van persoonsgegevens.</p> <p>Bijzondere categorieën van persoonsgegevens, hierna bijzondere persoonsgegevens, betreffen gegevens waaruit ras of etnische afkomst, politieke opvattingen, religieuze of levensbeschouwelijke overtuigingen, of het lidmaatschap van een vakbond blijken, genetische gegevens, biometrische gegevens, gegevens over gezondheid, of gegevens met betrekking tot iemands seksueel gedrag of seksuele gerichtheid.</p> <p>Het zullen vooral bijzondere persoonsgegevens zijn die via het MedMij-netwerk uitgewisseld worden, aangezien de verwerking voornamelijk op gegevens betreffende de gezondheid van personen zal plaatsvinden.</p>	
<b>Artikel 4</b>	In de AVG worden twee rollen gedefinieerd:	Gelet op de rolomschrijvingen in het MedMij Afsprakenstelsel zullen de <i>Zorgaanbieder</i> en de

	<ul style="list-style-type: none"> <li>• verwerkingsverantwoordelijke,</li> <li>• verwerker.</li> </ul> <p>Een <b>verwerkingsverantwoordelijke</b> is degene die alleen, of samen met anderen, het doel van en de middelen voor de verwerking van persoonsgegevens vaststelt. Deze rol kan vervuld worden door een natuurlijk persoon, een rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan.</p> <p>Een <b>verwerker</b> is een natuurlijk persoon of rechtspersoon, een overheidsinstantie, een dienst of een ander orgaan die/dat ten behoeve van, en op instructie van, de verwerkingsverantwoordelijke persoonsgegevens verwerkt.</p> <p>Het is de feitelijke situatie waaruit afgeleid wordt welke partij welke rol vervult. Dit is contractueel niet af te spreken.</p>	<p><i>Dienstverlener Persoon</i> waarschijnlijk de rol van verwerkingsverantwoordelijke vervullen.</p> <p>De <i>Dienstverlener zorgaanbieder</i> zal, indien gegevens verwerkt worden in opdracht van de <i>Zorgaanbieder</i>, de rol aannemen van verwerker.</p> <p>Dit hangt echter wel altijd af van de feitelijke informatie en omstandigheden.</p> <p>Een toelichting is gegeven op de pagina <a href="#">Toelichting verwerkingsverantwoordelijkheden</a></p>	
<b>Artikel 4</b>	Verwerking van persoonsgegevens is een breed begrip. Het omvat in feite elke handeling die de gegevens betreft, waaronder eenvoudigweg het houden, ontvangen, verzamelen, bewerken, opslaan of verwijderen van die gegevens.		
<b>Artikel 5</b>	Persoonsgegevens die verwerkt worden dienen juist te zijn en zo nodig geactualiseerd te worden. Redelijke maatregelen moeten worden genomen door		<i>Zorgaanbieders</i> zijn zelf verantwoordelijk om te communiceren aan personen over de persoonsgegevens die zij verwerken.

	de verwerkingsverantwoordelijke om de persoonsgegevens die onjuist zijn, onverwijld te wissen of te wijzigen.		<i>Dienstverleners persoon</i> , als aanbieder van een PGO, dienen zich ervan bewust te zijn dat ze verantwoordelijk zijn om de persoonsgegevens die zij zelf verzamelen (en eventueel ook in een PGO aanwezig zijn) actueel te houden. De dienstverlener is niet verantwoordelijk voor de juistheid van de gegevens/ inhoud van de PGO die daarin zelf door de <i>Persoon</i> wordt opgenomen.
<b>Artikel 5</b>	<p>In beginsel mogen persoonsgegevens slechts voor:</p> <ul style="list-style-type: none"> <li>• welbepaalde,</li> <li>• uitdrukkelijk omschreven, en</li> <li>• gerechtvaardigde doeleinden</li> </ul> <p>verwerkt worden.</p> <p>Indien persoonsgegevens voor een ander, secundair, doeleinde verwerkt worden, is dit slechts mogelijk indien de betrokkene toestemming heeft gegeven voor deze verdere verwerking, of indien dit noodzakelijk is voor een specifiek wettelijk voorschrift ter waarborging van een belangrijke doelstelling van algemeen belang.</p> <p>Tot slot mogen persoonsgegevens niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkene te</p>	<p>In het MedMij Afsprakenstelsel is bepaald dat in het kader van de uitvoering van de Deelnemersovereenkomst met MedMij het doel van de verwerking van de persoonsgegevens de waarborging en realisering van een veilige, interoperabele en betrouwbare gegevensuitwisseling tussen de <i>Persoon</i> en <i>Zorgaanbieder</i> via de <i>Dienstverlener persoon</i> en de <i>Dienstverlener zorgaanbieder</i> overeenkomstig het bepaalde in het MedMij Afsprakenstelsel is.</p> <p>Deze bepaling is ook opgenomen in artikel 9 van de Modelverwerkersovereenkomst Zorgaanbieder – Dienstverlener zorgaanbieder.</p> <p>In het MedMij Afsprakenstelsel zijn bewaartermijnen gegeven voor de vereiste logging van de gegevensuitwisseling en de verwerking.</p>	<p>Aanvullend dienen de <i>Dienstverlener persoon</i> en de <i>Zorgaanbieder</i> de doeleinden voor (de verdere/eigen) verwerking van de persoonsgegevens specifiek te formuleren voor de <i>Persoon</i>, zodat duidelijk is waarom de verwerking van persoonsgegevens nodig is om dit doel te realiseren en ook in hoeverre de gegevens voor andere doeleinden kunnen worden verwerkt.</p> <p>Doordat het doel duidelijk geformuleerd is, wordt het ook snel duidelijk wanneer persoonsgegevens verwerkt zullen worden voor secundaire doeleinden.</p> <p>Voordat een <i>Persoon</i> zijn persoonlijke gezondheidsomgeving in gebruik neemt dient de <i>Dienstverlener persoon</i> een specifieke toestemming te verkrijgen van de <i>Persoon</i> voor het verwerken van persoonsgegevens.</p>

	identificeren dan noodzakelijk voor de verwezenlijking van de doeleinden waarvoor zij worden verzameld en verder verwerkt.		
<b>Artikel 5</b>	<p>Gegevensverwerkingen dienen te worden beperkt tot wat noodzakelijk is voor de verwerkingsdoeleinden. De gegevensverwerking moet derhalve vooraf getoetst worden aan de beginselen van proportionaliteit en subsidiariteit.</p> <p><b>Proportionaliteit</b> betekent dat moet worden beoordeeld of de inbreuk op de privacy van betrokkenen van de voorgenomen gegevensverwerking in een redelijke verhouding staat tot het doel. Daarbij zal moeten worden gekeken of de voorgenomen gegevensverwerking effectief is om het beoogde doel te bereiken en of de te verwerken persoonsgegevens relevant en toereikend zijn om het beoogde doel te bereiken.</p> <p>Bij <b>subsidiariteit</b> wordt bekeken of de verwerkingsdoeleinden met minder ingrijpende middelen kunnen worden bereikt.</p>	In het MedMij Afsprakenstelsel is onder andere in de <a href="#">Architectuur en technische specificaties</a> rekening gehouden met het proportionaliteits- en subsidiariteitsbeginsel. Op die manier is gestreefd naar afspraken waarbij niet meer gegevens worden verwerkt dan noodzakelijk is voor de gegevensuitwisseling (privacy by design en privacy bij default). Er vindt onafhankelijke toetsing daarvan plaats.	
<b>Artikel 5, 6</b>	Indien persoonsgegevens verstrekt worden aan derde partijen, moet de verwerking door deze derde partijen in lijn zijn met het doel waarvoor de persoonsgegevens oorspronkelijk zijn verzameld en verwerkt.	Deze bepaling is aanvullend op de AVG ook opgenomen in artikel 5.6 van de Deelnemersovereenkomst Dienstverlener persoon en Dienstverlener zorgaanbieder.	

Grondslagen & toestemming			
<b>Artikel 6, 7, 9</b>	<p>Persoonsgegevens mogen slechts verwerkt worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doelen, indien de verwerking plaatsvindt op een van de grondslagen die limitatief opgesomd zijn in de AVG. Dit betreft de volgende <b>grondslagen</b>:</p> <ol style="list-style-type: none"> <li>1) Toestemming van de betrokkene;</li> <li>2) De gegevens zijn noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene een partij is;</li> <li>3) De gegevens zijn noodzakelijk voor het volgen van een wettelijke verplichting;</li> <li>4) De gegevensverwerking is noodzakelijk om vitale belangen van de betrokkene of van een ander natuurlijk persoon te beschermen;</li> <li>5) De gegevensverwerking is noodzakelijk voor de vervulling van een taak van algemeen belang of van een taak in het kader van de uitoefening van het openbaar gezag;</li> <li>6) De gegevensverwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van u of van een</li> </ol>	<p><b>Algemeen:</b> In het afsprakenstelsel is bepaald dat in het kader van de uitvoering van de Deelnemersovereenkomst met MedMij het doel van de verwerking van de persoonsgegevens de waarborging en realisering van een veilige, interoperabele en betrouwbare gegevensuitwisseling tussen de <i>Persoon</i> en <i>Zorgaanbieder</i> via de <i>Dienstverlener persoon</i> en de <i>Dienstverlener zorgaanbieder</i> overeenkomstig het bepaalde in het MedMij Afsprakenstelsel is.</p> <p>In de overeenkomst met de deelnemer is bepaald dat: Voor zover de verwerking van persoonsgegevens door de Deelnemer wordt gebaseerd op de rechtmatigheidsgrondslag 'toestemming' in de zin van artikel 6 lid 1 AVG is de verwerking voor een ander doel dan genoemd in artikel 5.5 van deze Overeenkomst toegestaan, mits de beginselen van de AVG op deze verdere verwerking wordt toegepast, de <i>Persoon</i> over deze verdere verwerking wordt geïnformeerd alsmede over de rechten die de <i>Persoon</i> tegen deze verdere verwerking kan uitoefenen. Voor zover de verwerking van de persoonsgegevens wordt gebaseerd op de rechtmatigheidsgrondslag 'noodzakelijk voor de uitvoering van de overeenkomst' in de zin van artikel 6 lid 1 sub c AVG, is verdere verwerking van de persoonsgegevens door de Deelnemer alleen toegestaan indien de evenredigheidstoets van artikel 6 lid 4 AVG succesvol is doorlopen.</p>	<p><b>Algemeen:</b> Let goed op het verschil tussen toestemming en expliciete toestemming. Een grondslag voor de verwerking van bijzondere persoonsgegevens is uitdrukkelijke toestemming.</p> <p>Dit betreft een verzwaarde vorm van toestemming. De betrokkene moet nadrukkelijk uitdrukking hebben gegeven aan zijn wil om toestemming te verlenen voor het verwerken van zijn bijzondere persoonsgegevens. Impliciete toestemming is niet mogelijk.</p>

derde aan wie de gegevens worden verstrekt.

Bij verwerking van **bijzondere of strafrechtelijke persoonsgegevens** (zie de sectie Algemene bepalingen en definities bovenaan in deze tabel) dient één van de wettelijke uitzonderingen op het verwerkingsverbod van toepassing te zijn (art. 9 lid 2 AVG). Als geen van deze uitzonderingen van toepassing is, dan is de verwerking van dit type persoonsgegevens verboden.

Op bovengenoemd **verwerkingsverbod** gelden samengevat de volgende **uitzonderingen**:

1. de betrokkene heeft **uitdrukkelijke toestemming** gegeven;
2. de verwerking is noodzakelijk met het oog op de uitvoering van verplichtingen en de uitoefening van specifieke rechten op het gebied van arbeids- en sociaalzekerheidsrecht;
3. de verwerking is noodzakelijk ter bescherming van vitale belangen van de betrokkenen of een ander;
4. de verwerking wordt verricht door een instantie die op politiek, levensbeschouwelijk, godsdienstig of vakbondsgebied werkzaam is;

Meer informatie is ook te vinden op de [pagina Toelichting verwerkingsverantwoordelijkheden](#).

De Deelnemer verstrekt geen persoonsgegevens van de *Persoon* aan anderen dan degenen waaraan de Deelnemer uit hoofde van de Deelnemersovereenkomst gegevens mag verstrekken c.q. op grond van een wettelijke verplichting moet verstrekken. Het is de Deelnemer uitdrukkelijk verboden om data betreffende de *Persoon* te verkopen.

5. de verwerking betrekking heeft op persoonsgegevens die kennelijk door de betrokkene openbaar zijn gemaakt;
6. de verwerking noodzakelijk is voor de instelling, uitoefening of onderbouwing van een rechtsvordering;
7. de verwerking noodzakelijk is om redenen van zwaarwegend algemeen belang;
8. de verwerking noodzakelijk is voor preventieve en arbeidsgeneeskunde, voor de beoordeling van de arbeidsgeschiktheid, medische diagnoses, het verstrekken van gezondheidszorg of sociale diensten of behandelingen dan wel het beheren van gezondheidszorgstelsels en –diensten of sociale stelsel en diensten;
9. de verwerking noodzakelijk is om redenen van algemeen belang op het gebied van de volksgezondheid;
10. de verwerking noodzakelijk is met het oog op archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden.

Indien persoonsgegevens worden verwerkt op basis van gegeven **toestemming**, gelden er nog enkele specifieke **vereisten**:

- Aangetoond moet kunnen worden dat de betrokkene toestemming heeft gegeven voor de verwerking van zijn persoonsgegevens.



	<ul style="list-style-type: none"> <li>• De toestemming moet zijn gegeven door middel van een duidelijke actieve handeling.</li> <li>• De toestemming moet gevraagd zijn in een begrijpelijk en gemakkelijk toegankelijke vorm.</li> <li>• De toestemming moet vrijelijk gegeven kunnen worden.</li> <li>• De toestemmingsvraag moet in duidelijke en eenvoudige taal gepresenteerd worden.</li> <li>• De toestemming moet ten alle tijden ingetrokken kunnen worden.</li> </ul> <p>Indien een verdere verwerking niet verenigbaar is met het oorspronkelijke doel, dan zal de verwerkingsverantwoordelijke een specifieke wettelijke grondslag moeten hebben of</p> <p>toestemming moeten vragen van de betrokkene voor de verdere verwerking.</p> <p>Onder de AVG, anders dan onder de Wbp, is het BSN geen bijzonder persoonsgegeven meer, maar kent wel een specifieke bepaling in verband met de gegevensverwerking en opgenomen in art 87 AVG/46 Uitvoeringswet AVG.</p>	<p>Voor de rechtmatigheid van de verwerking van het BSN binnen de scope van het MedMij Afsprakenstelsel wordt verwezen naar het <a href="#">Juridisch kader</a> (wet aanvullende bepalingen verwerking persoonsgegevens in de zorg) en de <a href="#">Toelichting verwerkingsverantwoordelijkheid</a></p>	
<b>Artikel 8</b>	<p>Specifieke voorwaarden worden gesteld in de AVG voor toestemming van kinderen in het geval er sprake is van <b>diensten van de informatiemaatschappij</b>. Indien sprake is</p>	<p><b>Algemeen:</b> In het afsprakenstelsel is afgesproken dat voorlopig alleen gezondheidsgegevens van personen van 16 jaar en ouder uitgewisseld worden.</p>	<p><b>Let op:</b> Voor het verwerken van persoonsgegevens van kinderen gelden specifieke (strengere) eisen en eventueel de betrokkenheid van ouder of voogd.</p>

	<p>van een dergelijke situatie, dient de toestemming verleend te worden door de ouder of voogd.</p> <p>Het aanbieden van een PGO door een <i>Dienstverlener persoon</i> kan gekwalificeerd worden als het aanbieden van een dienst van de informatiemaatschappij zoals omschreven in artikel 3:15d lid 3 BW. Onder dienst van de informatiemaatschappij wordt namelijk verstaan elke dienst die gewoonlijk tegen vergoeding, langs elektronische weg, op afstand en op individueel verzoek van de afnemer van de dienst wordt verricht zonder dat partijen gelijktijdig op dezelfde plaats aanwezig zijn.</p>		<p>Bovendien is het momenteel niet mogelijk om gegevens van personen jonger dan 16 jaar via het MedMij Afsprakenstelsel te (laten) uitwisselen. Bekijk goed wat u wel/ niet toestaat in de registratie van personen jonger dan 16 jaar voor een PGO.</p>
Informatievoorziening			
<p><b>Artikel 12, 13, 14</b></p>	<p>Een verwerkingsverantwoordelijke is verantwoordelijk om betrokkenen te <b>informer</b>en over de verwerking van persoonsgegevens. Deze informatie dient zowel verschaft te worden indien de persoonsgegevens rechtstreeks bij de betrokkene worden verzameld, alsook wanneer de persoonsgegevens niet rechtstreeks bij de betrokkene worden verzameld.</p> <p>Indien persoonsgegevens rechtstreeks bij de betrokkene worden verzameld, dient de volgende informatie bij de verkrijging van</p>	<p><b>Algemeen:</b> De <i>Dienstverlener persoon</i> is aanvullend op de AVG ook op grond van de Deelnemersovereenkomst (artikel 4.1) verplicht verwerking van de persoonsgegevens overeenkomstig de privacywet- en -regelgeving uit te voeren. Specifiek voor de <i>Dienstverlener persoon</i> is nog opgenomen dat Gebruikers worden geïnformeerd over hoe de <i>Persoon</i> zijn rechten in deze bij de <i>Dienstverlener persoon</i> kan uitoefenen.</p> <p>.</p>	

de persoonsgegevens verstrekt te worden door de verwerkingsverantwoordelijke:

- De identiteit en contactgegevens van de verwerkingsverantwoordelijke, en indien van toepassing van de vertegenwoordiger;
- De contactgegevens van de functionaris voor gegevensbescherming indien aanwezig;
- De verwerkingsdoeleinden waarvoor de persoonsgegevens zijn bestemd;
- De grondslag voor de verwerking;
- Indien de gegevensverwerking noodzakelijk is voor de behartiging van het gerechtvaardigde belang van u of van een derde aan wie de gegevens worden verstrekt, dient informatie omtrent de gerechtvaardigde belangen verstrekt te worden;
- De ontvangers of categorieën van ontvangers van de persoonsgegevens indien van toepassing;
- Indien de verwerkingsverantwoordelijke het voornemen heeft de persoonsgegevens door te geven aan een derde land of een internationale organisatie dient aangegeven te worden of er een adequaatheidsbesluit van de Europese Commissie bestaat, of welke passende of geschikte waarborgen er zijn voor deze doorgifte;
- De periode gedurende welke de persoonsgegevens zullen worden

opgeslagen. Indien deze informatie niet verstrekt kan worden, dienen de criteria ter bepaling van die termijn verstrekt te worden;

- De rechten die betrokkenen toekomen;
- Of de verstrekking van persoonsgegevens een wettelijke of contractuele verplichting is dan wel een noodzakelijke voorwaarde om een overeenkomst te sluiten, en of de betrokkene verplicht is de persoonsgegevens te verstrekken en wat de mogelijke gevolgen zijn wanneer deze gegevens niet worden verstrekt;
- Het bestaan van eventuele geautomatiseerde besluitvorming en/of profilering.

Indien persoonsgegevens niet rechtstreeks van betrokkenen worden verkregen, dient in aanvulling op bovenstaande opsomming, door de verwerkingsverantwoordelijke ook informatie verstrekt te worden over:

- de betrokken categorieën van persoonsgegevens;
- de bron waar de persoonsgegevens vandaan komen en, in voorkomend geval, of zij afkomstig zijn van openbare bronnen.

De verwerkingsverantwoordelijke verstrekt in dit geval de informatie binnen een redelijke termijn, maar uiterlijk binnen één

	<p>maand na de verkrijging van de persoonsgegevens.</p> <p>Indien de persoonsgegevens zullen worden gebruikt voor communicatie met de betrokkene, dient de verwerkingsverantwoordelijke de informatie uiterlijk op het moment van het eerste contact met de betrokkene te verstrekken.</p>		
<i>Rechten van betrokkenen</i>			
<p><b>Artikel 15, 16, 17, 18, 20, 21, 22, 23</b></p>	<p><b>Betrokkenen</b> waarvan persoonsgegevens verwerkt worden komen verschillende <b>rechten</b> toe op grond van de AVG. De verwerkingsverantwoordelijke is degene die de uitoefening van deze rechten moet faciliteren. Daarnaast is de verwerkingsverantwoordelijke verantwoordelijk om iedere ontvanger aan wie de persoonsgegevens zijn verstrekt, in kennis te stellen van ieder verzoek tot rectificatie of wissing van persoonsgegevens, of verzoek tot beperking van de verwerking.</p> <p><b>Recht op inzage</b></p> <p>Betrokkenen hebben het recht om van de verwerkingsverantwoordelijke uitsluitend te verkrijgen over het al dan niet verwerken van hen betreffende persoonsgegevens. Indien dit het geval is, heeft de betrokkene het recht om inzage te verkrijgen van die</p>	<p><b>Algemeen:</b> Betrokkenen, <i>Personen</i> in termen van het MedMij Afsprakenstelsel, kunnen hun rechten uitoefenen jegens de <i>Dienstverlener persoon</i> voor de gegevens die verwerkt worden binnen de PGO.</p> <p>Verzoeken die gebaseerd zijn op een recht dat de betrokkene toekomt dienen daarom rechtstreeks aan de <i>Dienstverlener persoon</i> gericht te worden indien het gaat om persoonsgegevens die verwerkt worden in de PGO. In art. 4.1 van de Deelnemersovereenkomst hebben we opgenomen dat de deelnemers de verwerking van de persoonsgegevens overeenkomstig de privacywet- en -regelgeving uitvoeren. Specifiek voor de <i>Dienstverlener persoon</i> is nog opgenomen dat Gebruikers worden geïnformeerd over hoe de <i>Persoon</i> zijn rechten in deze bij de <i>Dienstverlener persoon</i> kan uitoefenen.</p> <p><b>Algemeen :</b> Betrokkenen, <i>Personen</i> in termen van het MedMij Afsprakenstelsel, kunnen daarnaast hun rechten uitoefenen jegens de <i>Zorgaanbieder</i> met betrekking tot de gegevens die verwerkt worden door de <i>Zorgaanbieder</i> in de uitoefening van zijn zorgtaken. De relatie <i>Persoon</i> –</p>	<p><b>Algemeen:</b> Zorg dat betrokkenen, <i>Personen</i>, de genoemde rechten kunnen uitoefenen en richt hiervoor processen in. Het is van belang dat de deelnemer kan aantonen dat dit gebeurt/is gebeurd. Indien mogelijk, richt dit dan zo in dat veel rechten, zoals hier genoemd, al automatisch uit te oefenen zijn in onder andere de PGO zelf.</p>

persoonsgegevens. Bovendien dient dan informatie omtrent de verwerking van persoonsgegevens verstrekt te worden, die ook verstrekt dient te worden indien de persoonsgegevens verzameld worden bij de betrokkenen.

Indien de betrokkene een verzoek tot inzage doet, verstrekt de verwerkingsverantwoordelijke een kopie van de persoonsgegevens die verwerkt worden aan de betrokkene.

#### **Recht op rectificatie**

Indien persoonsgegevens onjuist zijn, heeft de betrokkene het recht om van de verwerkingsverantwoordelijke onverwijld rectificatie van deze onjuiste persoonsgegevens te verkrijgen. Indien bepaalde persoonsgegevens onvolledig worden verwerkt, gelet op de doeleinden van de verwerking, heeft de betrokkene ook het recht om deze persoonsgegevens te vervolledigen.

#### **Recht op gegevenswissing**

Betrokkenen hebben het recht om van de verwerkingsverantwoordelijke, zonder onredelijke vertraging, wissing van hem betreffende persoonsgegevens te verkrijgen. De verwerkingsverantwoordelijke is in de

*Zorgaanbieder* valt buiten de scope van het Afsprakenstelsel MedMij. De *Dienstverlener zorgaanbieder* is de *Deelnemer*. Om ervoor te zorgen dat de *Zorgaanbieder* zijn verantwoordelijkheid kan nemen bij een verzoek om uitoefening van rechten van één van zijn patiënten die gebruik maakt van een PGO dat via MedMij-afspraken gegevens uitwisselt, is in art. 3.7 van de modelverwerkersovereenkomst tussen de *Dienstverlener zorgaanbieder* en de *Zorgaanbieder* opgenomen dat de *Dienstverlener zorgaanbieder* zijn medewerking verleent.

volgende gevallen verplicht om de persoonsgegevens te wissen:

1. indien de persoonsgegevens niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of verwerkt;
2. de betrokkene trekt gegeven toestemming in, en er is geen andere rechtsgrond voor de verwerking;
3. de betrokkene maakt bezwaar tegen de verwerking, waarbij er geen prevalerende dwingende gerechtvaardigde gronden voor de verwerking aanwezig zijn;
4. de persoonsgegevens zijn onrechtmatig verwerkt;
5. de persoonsgegevens moeten worden gewist om als verwerkingsverantwoordelijke te kunnen voldoen aan een wettelijke verplichting die op hem rust;
6. de persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij aan een kind jonger dan 16 jaar.

Een verwerkingsverantwoordelijke hoeft niet te voldoen aan een verzoek tot gegevenswissing indien de verwerking noodzakelijk is:

- voor het uitoefenen van het recht op vrijheid van meningsuiting en informatie;

- voor het nakomen van een wettelijke verwerkingsverplichting die op de verwerkingsverantwoordelijke rust;
- om redenen van algemeen belang op het gebied van volksgezondheid;
- met het oog op archivering in het algemeen belang, wetenschappelijke of historisch onderzoek of statistische doeleinden;
- voor de instelling, uitoefening of onderbouwing van een rechtsvordering.

#### **Recht op beperking van de verwerking**

Betrokkenen hebben het recht om de verwerking van hen betreffende persoonsgegevens te beperken (de gegevens mogen in dat geval alleen door de verwerkingsverantwoordelijke worden bewaard en alleen voor beperkte doeleinden worden gebruikt) indien:

- de nauwkeurigheid van de gegevens wordt betwist (en alleen zolang als nodig is om die nauwkeurigheid te verifiëren);
- de verwerking onrechtmatig is en de betrokkene verzoekt om beperking en zich verzet tegen het wissen van de persoonsgegevens;
- de verwerkingsverantwoordelijke de gegevens niet meer nodig heeft voor het oorspronkelijke doel, maar de betrokkene de gegevens nog wel nodig



heeft voor de instelling, uitoefening of onderbouwing van een rechtsvordering; of

- de betrokkene bezwaar heeft gemaakt tegen de verwerking, en in afwachting is van het antwoord op de vraag of de gerechtvaardigde gronden van de verwerkingsverantwoordelijke zwaarder wegen dan zijn eigen rechten.

### **Recht op overdraagbaarheid van gegevens**

Betrokkenen hebben het recht om:

- een kopie te ontvangen van hun betreffende persoonsgegevens in een gestructureerde, veelgebruikte, machineleesbare vorm die hergebruik ondersteunt;
- hen betreffende persoonsgegevens rechtstreeks van de ene verwerkingsverantwoordelijke naar de andere over te dragen.

### **Recht van bezwaar**

Betrokkenen hebben het recht om bezwaar te maken, vanwege met specifieke situatie verband houdende redenen, tegen de verwerking van persoonsgegevens indien die grondslag voor die verwerking is:

- noodzakelijkheid voor de vervulling van een taak van algemeen belang, of
- noodzakelijkheid voor de behartiging van de gerechtvaardigde belangen van de verwerkingsverantwoordelijke of van een derde.

De verwerkingsverantwoordelijke moet deze verwerking staken, tenzij de verantwoordelijke:

- aan kan tonen dat hij dwingende gerechtvaardigde gronden heeft voor de verwerking die prevaleren boven de belangen, rechten en vrijheden van de betrokkene, of
- er gerechtvaardigde gronden zijn die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering.

Daarnaast hebben betrokkenen het recht om bezwaar te maken tegen de verwerking van persoonsgegevens met het oog op direct marketing, inclusief profilering.

#### **Geautomatiseerde individuele besluitvorming, waaronder profilering**

Betrokkenen hebben tot slot het recht niet te worden onderworpen aan een besluit dat tot stand is gekomen door een uitsluitend geautomatiseerde verwerking of profilering.

	<p><b>NB</b> Er zijn uitzonderingen mogelijk op de uitoefening van de rechten van betrokkene, op voorwaarde dat de wezenlijke inhoud van de grondrechten en fundamentele vrijheden niet wordt aangetast en dat het gaat om noodzakelijke en evenredige maatregelen ter waarborging van enkele expliciet opgesomde belangrijke doelstellingen van algemeen belang. Uitzonderingen dienen altijd een wettelijke grondslag te hebben.</p>		
<p><i>Verplichtingen verwerkingsverantwoordelijken</i></p>			
<p><b>Artikel 5, 24 t/m 28, 30 t/m 36</b></p>	<p>Op partijen die de rol van <b>verwerkingsverantwoordelijke</b> vervullen rusten diverse <b>verplichtingen</b>.</p> <ol style="list-style-type: none"> <li>1. Allereerst is de verwerkingsverantwoordelijke verantwoordelijk voor, en moet hij in staat zijn om aan te tonen dat de gegevensbeschermingsbeginselen zoals neergelegd in de AVG worden nageleefd.</li> <li>2. De verwerkingsverantwoordelijke is verantwoordelijk voor het implementeren van passende <b>technische en organisatorische maatregelen</b> om te garanderen, en om aan te tonen, dat zijn verwerkingsactiviteiten voldoen aan de vereisten van de AVG. Deze maatregelen kunnen het implementeren van een passend gegevensbeschermingsbeleid</li> </ol>	<p><b>Algemeen:</b> Het afsprakenstelsel bepaalt dat de deelnemers aan het afsprakenstelsel ingeschreven dienen te zijn in een handelsregister in de EU.</p> <p>In het MedMij Afsprakenstelsel is onder andere in de <a href="#">architectuur en technische specificaties</a> rekening gehouden met het proportionaliteits- en subsidiariteitsbeginsel. Op die manier is gestreefd naar afspraken waarbij niet meer gegevens worden verwerkt dan noodzakelijk is voor de gegevensuitwisseling (privacy by design en privacy by default) en vindt onafhankelijke toetsing daarvan plaats.</p>	

omvatten. Het naleven van goedgekeurde gedragscodes kan een bewijs zijn van naleving.

3. Verwerkingsverantwoordelijken moeten ervoor zorgen dat zowel in de ontwerpfase van nieuwe verwerkingsactiviteiten, als in de implementatiefase van een nieuw product of dienst (bijvoorbeeld een nieuw ontwikkelde PGO), gegevensbeschermingsbeginselen en passende voorzorgsmaatregelen worden onderzocht en geïmplementeerd. Daarnaast dienen de nodige waarborgen in de verwerking ingebouwd te worden ter bescherming van de rechten van de betrokkenen. Dit wordt ook wel **gegevensbescherming door ontwerp** genoemd.

Daarnaast dienen passende technische en organisatorische maatregelen getroffen te worden om ervoor te zorgen dat in beginsel alleen persoonsgegevens worden verwerkt die noodzakelijk zijn voor elk specifiek doel van de verwerking. Dit wordt ook wel **gegevensbescherming door standaardinstellingen** genoemd.

4. Indien twee of meer verwerkingsverantwoordelijkheden gezamenlijk de doeleinden en de middelen van de verwerking bepalen, zijn zij **gezamenlijke**

**verwerkingsverantwoordelijken.** In dit geval dienen zij hun respectievelijke verantwoordelijkheden met betrekking tot de nakoming van de verplichtingen uit de AVG vast te stellen door middel van een onderlinge regeling. Betrokkenen kunnen in dit geval hun rechten uitoefenen jegens iedere verwerkingsverantwoordelijke afzonderlijk.

5. Een verwerkingsverantwoordelijke die buiten de EU is gevestigd, moet een vertegenwoordiger aanwijzen in een van de lidstaten waar de verwerkingsverantwoordelijke goederen of diensten aanbiedt of EU-ingezetenen monitort, tenzij de verwerking incidenteel en kleinschalig is en geen gevoelige persoonsgegevens bevat.

6. Verwerkingsverantwoordelijken kunnen verwerkers inschakelen om persoonsgegevens te verwerken op hun instructie, zoals een hostingbedrijf dat de PGO-gegevens moet hosten.

Slechts verwerkers die de naleving van de AVG garanderen mogen ingeschakeld worden. De verwerkingsverantwoordelijke dient een **verwerkersovereenkomst** af te sluiten met de verwerker. Er is een MedMij Modelverwerkersovereenkomst

**6. Verwerkersovereenkomst.** Aanvullend op de verplichtingen in de AVG wordt in het MedMij Afsprakenstelsel bepaald dat verwerkers van persoonsgegevens, die in opdracht van de verwerkingsverantwoordelijke werken, waaronder de *Dienstverlener zorgaanbieder* die de gegevensuitwisseling conform MedMij-afspraken regelt, een verwerkersovereenkomst af moeten sluiten. Hiervoor is een model verwerkersovereenkomst beschikbaar gesteld, waarin expliciet rekening is gehouden met de situatie die voortvloeit uit deelname aan het MedMij Afsprakenstelsel.

beschikbaar die gebruikt kan worden tussen de *Zorgaanbieder* en de *Dienstverlener zorgaanbieder*.

Indien er wordt gekozen voor een eigen verwerkersovereenkomst moet daarin informatie opgenomen te worden over:

- het onderwerp van de verwerking(en);
- de duur van de verwerking;
- de aard van het doel van de verwerking;
- het soort persoonsgegevens en de categorieën van betrokkenen;
- de rechten en verplichtingen van de verwerkingsverantwoordelijke.

In de verwerkersovereenkomst moet bovendien opgenomen worden dat de verwerker:

1. alleen persoonsgegevens mag verwerken op basis van gedocumenteerde instructies door de verwerkingsverantwoordelijke;
2. waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen;
3. de beveiliging van de persoonsgegevens die hij verwerkt moet garanderen;
4. aan regels is gebonden indien hij een sub-verwerker in wilt schakelen;

5. maatregelen implementeert om de verwerkingsverantwoordelijke te kunnen helpen bij de naleving van de rechten van betrokkenen;
6. de verwerkingsverantwoordelijke assisteert bij het verkrijgen van goedkeuring van een toezichthouder indien nodig;
7. na afloop van de verwerkingsdiensten, naargelang de keuze van de verwerkingsverantwoordelijke, alle persoonsgegevens wist of deze aan hem terugbezorgt;
8. alle informatie verstrekt aan de verwerkingsverantwoordelijke die noodzakelijk is om naleving van de AVG aan te kunnen tonen.

7. Een verwerkingsverantwoordelijke dient een register van de verwerkingsactiviteiten, ook wel **verwerkingsregister** genoemd, bij te houden. Dit register dient minimaal de volgende gegevens te bevatten:

- De naam en contactgegevens van:
  - de verwerkingsverantwoordelijke
  - indien van toepassing die van de gezamenlijke verwerkingsverantwoordelijken en/of vertegenwoordiger van de verwerkingsverantwoordelijke, en van de functionaris voor gegevensbescherming;
- De verwerkingsdoeleinden;

**7. Verwerkingsregister.** Een verwerkingsregister biedt ook een goed uitgangspunt voor een verwerkingsverantwoordelijke om de data die verzameld is goed in beeld te krijgen. Door de identificatie van alle data ontstaat ook een goed beeld over de stappen die ondernomen moeten worden op het gebied van beveiliging van de data. Voor een deelnemer is het dus belangrijk een dergelijk register bij te houden en hierin ook de verwerkingen op te nemen die het gevolg zijn van deelname aan het MedMij Afsprakenstelsel.

- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- De categorieën van ontvangers aan wie de persoonsgegevens zijn óf zullen worden verstrekt;
- Indien van toepassing: doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of internationale organisatie en de passende waarborgen;
- De van toepassing zijnde bewaartermijnen;
- Een omschrijving van de geïmplementeerde beveiligingsmaatregelen.

8. Een verwerkingsverantwoordelijke is, samen met de verwerker, verplicht om desgevraagd samen te werken met de toezichthoudende autoriteit bij het vervullen van haar taken.

9. De verwerkingsverantwoordelijke moet **passende technische en organisatorische beveiligingsmaatregelen** treffen om persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging of verlies, wijziging, ongeautoriseerde openbaarmaking of toegang. Afhankelijk

**9. Passende technische en organisatorische beveiligingsmaatregelen.** In het MedMij Afsprakenstelsel is een aanvullend normenkader informatiebeveiliging opgenomen. Op basis van een stelselrisicoanalyse en/of PIA worden maatregelen (her)overwogen en eventueel aanvullende privacy- en informatiebeveiligingsmaatregelen gedefinieerd. Dit kan resulteren in bijstelling van het [Normenkader informatiebeveiliging](#) en de [Architectuur en technische specificaties](#).

**10. Datalek.** Deelnemers aan het MedMij Afsprakenstelsel zijn zelf verantwoordelijk om eventuele datalekken te signaleren. Zie hiervoor ook de [Guidelines on Personal data breach notification](#) van de Europese privacytoezichthouders:



van de verwerkingsactiviteiten kunnen de beveiligingsmaatregelen het volgende omvatten:

- Pseudonimisering en versleuteling van persoonsgegevens;
- Doorlopende beoordelingen van de beveiligingsmaatregelen;
- Redundantie en back-up mogelijkheden;
- Regelmatig testen, beoordelen en evalueren van de beveiligingsmaatregelen.

Wat een passend niveau van beveiliging is, dient te worden getoetst aan de hand van de verwerkingsrisico's die met de verwerkingsactiviteit gepaard gaan.

10. De verwerkingsverantwoordelijke is verplicht om een inbreuk in verband met persoonsgegevens, ook wel **datalek** genoemd, zonder onredelijke vertraging en uiterlijk 72 uur nadat hij er kennis van heeft genomen te melden bij de bevoegde toezichthoudende autoriteit. (In Nederland is dit de Autoriteit Persoonsgegevens). De enige uitzondering hierop is wanneer beoordeeld is dat het niet waarschijnlijk is dat de inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van betrokkenen. De melding moet minimaal de volgende informatie bevatten:

<https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken>.

In het MedMij Afsprakenstelsel is in het [Normenkader informatiebeveiliging](#) opgenomen dat beveiligingsincidenten binnen 48 uur gemeld dienen te worden bij de beheerorganisatie. Hieronder vallen ook datalekken.

De beheerorganisatie is verantwoordelijk om een impact analyse te doen op het beveiligingslek en/of beveiligingsincident voor het stelsel als geheel, en dit te delen met andere partijen indien dit nodig wordt geacht.

1. Een omschrijving van de inbreuk in verband met persoonsgegevens, met inbegrip van het aantal betrokken betrokkenen en de getroffen categorieën van persoonsgegevens;
2. De naam en contactgegevens van de functionaris voor gegevensbescherming of een ander contactpunt waar meer informatie kan worden verkregen;
3. De waarschijnlijke gevolgen van de inbreuk;
4. De maatregelen die zijn getroffen om de inbreuk aan te pakken, waaronder maatregelen die de eventuele nadelige gevolgen van de inbreuk beperken.

De verwerkingsverantwoordelijke is bovendien verplicht om alle inbreuken in verband met persoonsgegevens te documenteren, inclusief informatie over de gevolgen daarvan en de genomen corrigerende maatregelen.

Indien een inbreuk in verband met persoonsgegevens een hoog risico oplevert voor betrokkenen, is de verwerkingsverantwoordelijke bovendien verplicht om de betrokkenen te informeren over deze inbreuk. Deze melding dient minimaal punt 2 t/m 4 van de verplichte informatie aan de toezichthoudende autoriteit te bevatten.

Een verwerkingsverantwoordelijke is uitgezonderd van deze meldingsplicht indien:

- Er passende technische en organisatorische beschermingsmaatregelen genomen zijn en deze maatregelen zijn toegepast op de persoonsgegevens waarop de inbreuk in verband met persoonsgegevens betrekking heeft, zoals bijvoorbeeld versleuteling van de data.
- Achteraf maatregelen genomen zijn om ervoor te zorgen dat de bedoelde hoge risico voor de rechten en vrijheden van betrokkenen zich waarschijnlijk niet meer zal voordoen.
- De mededeling onevenredige inspanningen zou vergen.

11. De verwerkingsverantwoordelijke dient in elk geval een functionaris voor gegevensbescherming aan te wijzen indien hij hoofdzakelijk is belast met grootschalige verwerking van bijzondere persoonsgegevens.

12. Indien een soort verwerking van persoonsgegevens, gelet op de aard, de omvang, de context en de doeleinden daarvan waarschijnlijk een hoog risico oplevert voor de rechten en vrijheden van

12. Formats voor gegevensbeschermingseffectbeoordelingen:

Van de ICO: <https://ico.org.uk/media/about-the-ico/consultations/2258461/dpia-template-v04-post-comms-review-20180308.pdf>

Van de CNIL: <https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-2-en-templates.pdf>

Het Rijksoverheid Model: <https://www.rijksoverheid.nl/documenten/rapporten/2017/09/29/model-gegevensbeschermingseffectbeoordeling-rijksdienst-pia>

betrokkenen, dient de verwerkingsverantwoordelijke vóór de verwerking een beoordeling uit te voeren van het effect van de beoogde verwerkingsactiviteiten op de bescherming van persoonsgegevens. Een dergelijke beoordeling wordt een **gegevensbeschermingseffectbeoordeling** genoemd. Dit is een degelijk instrument om vooraf privacyrisico's van de voorgenomen verwerkingsactiviteit(en) in kaart te brengen.

Een gegevensbeschermingseffectbeoordeling is in ieder geval vereist indien het een grootschalige verwerking van bijzondere persoonsgegevens betreft.

Een beoordeling bevat tenminste de volgende punten:

- een systematische beschrijving van de beoogde verwerkingen en de verwerkingsdoeleinden, waaronder, in voorkomend geval, de gerechtvaardigde belangen die door de verwerkingsverantwoordelijke worden behartigd;
- een beoordeling van de noodzaak en de evenredigheid van de verwerkingen met betrekking tot de doeleinden;
- een beoordeling van de risico's voor de rechten en vrijheden van betrokkenen;

	<ul style="list-style-type: none"> <li>• beoogde maatregelen om de risico's aan te pakken.</li> </ul> <p>Wanneer uit een gegevensbeschermingseffectbeoordeling blijkt dat de verwerking een hoog risico zou opleveren indien geen maatregelen genomen worden om het risico te beperken, dient de verwerkingsverantwoordelijke voorafgaand aan de verwerking de toezichthoudende autoriteit te raadplegen.</p>		
<i>Verplichtingen verwerker</i>			
<b>Artikel 28 t/m 33, 37</b>	<p>Op partijen die de rol van <b>verwerker</b> vervullen rusten diverse <b>verplichtingen</b>.</p> <ol style="list-style-type: none"> <li>1. Een verwerker mag alleen persoonsgegevens verwerken op basis van gedocumenteerde instructies van een verwerkingsverantwoordelijke. Tussen de verwerkingsverantwoordelijke en de verwerker dient een verwerkersovereenkomst afgesloten te worden.</li> <li>2. Een verwerker moet de beveiliging van de persoonsgegevens die hij verwerkt garanderen aan de verwerkingsverantwoordelijke.</li> <li>3. De verwerker moet ervoor zorgen dat alle persoonsgegevens die hij verwerkt vertrouwelijk worden behandeld. De</li> </ol>	In artikel 8 van de Deelnemersovereenkomst zijn, aanvullend op de AVG, verantwoordelijkheden van een deelnemer jegens derden, waaronder verwerkers van persoonsgegevens, opgenomen.	<p><b>Algemeen:</b> Ook voor verwerkers (bijvoorbeeld de <i>Dienstverlener zorgaanbieder</i> of subverwerkers van dienstverleners) is het belangrijk om in een verwerkersovereenkomst duidelijke afspraken te maken met een verwerkingsverantwoordelijke over de verwerkingen die zij uit zullen gaan voeren. Zij kunnen zelf het initiatief nemen om een verwerkersovereenkomst af te sluiten mocht de verwerkingsverantwoordelijke dit initiatief niet tonen.</p>

verwerkersovereenkomst tussen de verwerkingsverantwoordelijke en de verwerker moet van de verwerker eisen dat hij ervoor zorgt dat alle personen die gemachtigd zijn om de persoonsgegevens te verwerken, een passende geheimhoudingsplicht hebben.

4. Een verwerker mag slechts sub-verwerkers inschakelen indien de verwerkingsverantwoordelijke hier, vooraf, schriftelijk toestemming voor heeft gegeven. Wanneer de verwerkingsverantwoordelijke instemt met de aanstelling van sub-verwerkers, moeten die sub-verwerkers op dezelfde voorwaarden worden aangesteld als zijn vastgesteld in de verwerkersovereenkomst tussen de verwerkingsverantwoordelijke en de verwerker.

5. Een verwerker dient een register van de verwerkingsactiviteiten, ook wel **verwerkingsregister** genoemd, bij te houden. Dit register dient minimaal de volgende gegevens te bevatten:

- De naam en contactgegevens van:
  - de verwerkingsverantwoordelijke
  - indien van toepassing, de gezamenlijke verwerkingsverantwoordelijken en/of vertegenwoordiger van de verwerkingsverantwoordelijke, en

van de functionaris voor gegevensbescherming;

- De verwerkingsdoeleinden;
- Een beschrijving van de categorieën van betrokkenen en van de categorieën van persoonsgegevens;
- De categorieën van ontvangers aan wie de persoonsgegevens zijn óf zullen worden verstrekt;
- Indien van toepassing: doorgiften van persoonsgegevens aan een derde land of een internationale organisatie, met inbegrip van de vermelding van dat derde land of internationale organisatie en de passende waarborgen;
- De van toepassing zijnde bewaartermijnen;
- Een omschrijving van de geïmplementeerde beveiligingsmaatregelen.

6. Verwerkers (en hun vertegenwoordigers, indien aanwezig) zijn verplicht om op verzoek samen te werken met toezichthoudende autoriteiten bij de uitvoering van haar taken.

7. De verwerker moet **passende technische en organisatorische beveiligingsmaatregelen** treffen om persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging of verlies, wijziging, ongeautoriseerde openbaarmaking of toegang. Afhankelijk

## 7. Passende technische en organisatorische

**beveiligingsmaatregelen.** In het MedMij Afsprakenstelsel is een [Normenkader informatiebeveiliging](#) opgenomen waarin de informatiebeveiliging binnen het MedMij-netwerk uiteen is gezet. In de Deelnemersovereenkomst is aangegeven dat de Deelnemer de voor hem geldende afspraken uit het MedMij Afsprakenstelsel in dit kader doorvertaalt naar (sub)verwerkers. De Deelnemer staat er jegens de Stichting MedMij voor in dat de door hem ingeschakelde derde voor zijn Diensten en/of *Gegevensdiensten* alle verplichtingen uit de Deelnemersovereenkomst nakomt, onder andere dus de uitvoering van de afspraken in het MedMij Afsprakenstelsel, en is aansprakelijk voor het

van de verwerkingsactiviteiten kunnen de beveiligingsmaatregelen het volgende omvatten:

- pseudonimisering en versleuteling van persoonsgegevens;
- doorlopende beoordelingen van de beveiligingsmaatregelen;
- redundantie en back-up-mogelijkheden;
- regelmatig testen, beoordelen en evalueren van de beveiligingsmaatregelen.

Wat een passend niveau van beveiliging is, dient te worden getoetst aan de hand van de verwerkingsrisico's die met de verwerkingsactiviteit gepaard gaan.

8. De verwerker is verplicht om een inbreuk in verband met persoonsgegevens, ook wel **datalek** genoemd, zonder onredelijke vertraging te melden aan de verwerkingsverantwoordelijke.

9. Indien de verwerkingsverantwoordelijke waarvoor de verwerker persoonsgegevens verwerkt verplicht is om een **functionaris voor de gegevensbescherming** aan te stellen, werkt deze verplichting door op de verwerker.

**NB.** Indien een verwerker, in strijd met de AVG, zelf doeleinden en middelen van een verwerkingsactiviteit vaststelt, wordt de

handelen op grond van deze Overeenkomst van de door hem ingeschakelde derde.

**9. Functionaris voor de gegevensbescherming.** We raden verwerkers aan zelf te onderzoeken of zij een functionaris voor de gegevensbescherming aan moeten stellen doordat de verwerkingsverantwoordelijke hiertoe ook verplicht is.



verwerker met betrekking tot die verwerking als de verwerkingsverantwoordelijke beschouwd.		
--	--	--

## Architectuur en technische specificaties

### Toelichting

Een onmisbaar deel van het MedMij Afsprakenstelsel betreft de verantwoordelijkheden die de deelnemers in het afsprakenstelsel hebben, elk in zijn eigen rol, tijdens het feitelijk verzorgen van het informatieverkeer tussen het Persoonsdomein en het Zorgaanbiedersdomein. Deze verantwoordelijkheden zijn opgenomen in de architectuur en de technische specificaties van het MedMij Afsprakenstelsel, die in deze pagina's uiteen worden gezet. Deze verantwoordelijkheden zijn geordend in een aantal abstractieniveaus, geïnspireerd op het [interoperabiliteitsmodel van Nictiz](#).

Om te beginnen moeten deelnemers er samen voor zorgen dat zich zekere bedrijfsprocessen voltrekken tussen het Persoonsdomein en het Zorgaanbiedersdomein. Deze bedrijfsprocessen gaan over het verzamelen en delen van gezondheidsinformatie. Op dit abstractieniveau is nog geen sprake van geautomatiseerde afhandeling van deze processen, maar zijn de verantwoordelijkheden enkel nog geformuleerd in termen van de inhoud van die processen en van de gezondheidsinformatie die daarin omgaat. De proceslaag en de informatielaag uit het interoperabiliteitsmodel van Nictiz zijn gecombineerd in één laag: [Processen en Informatie](#).

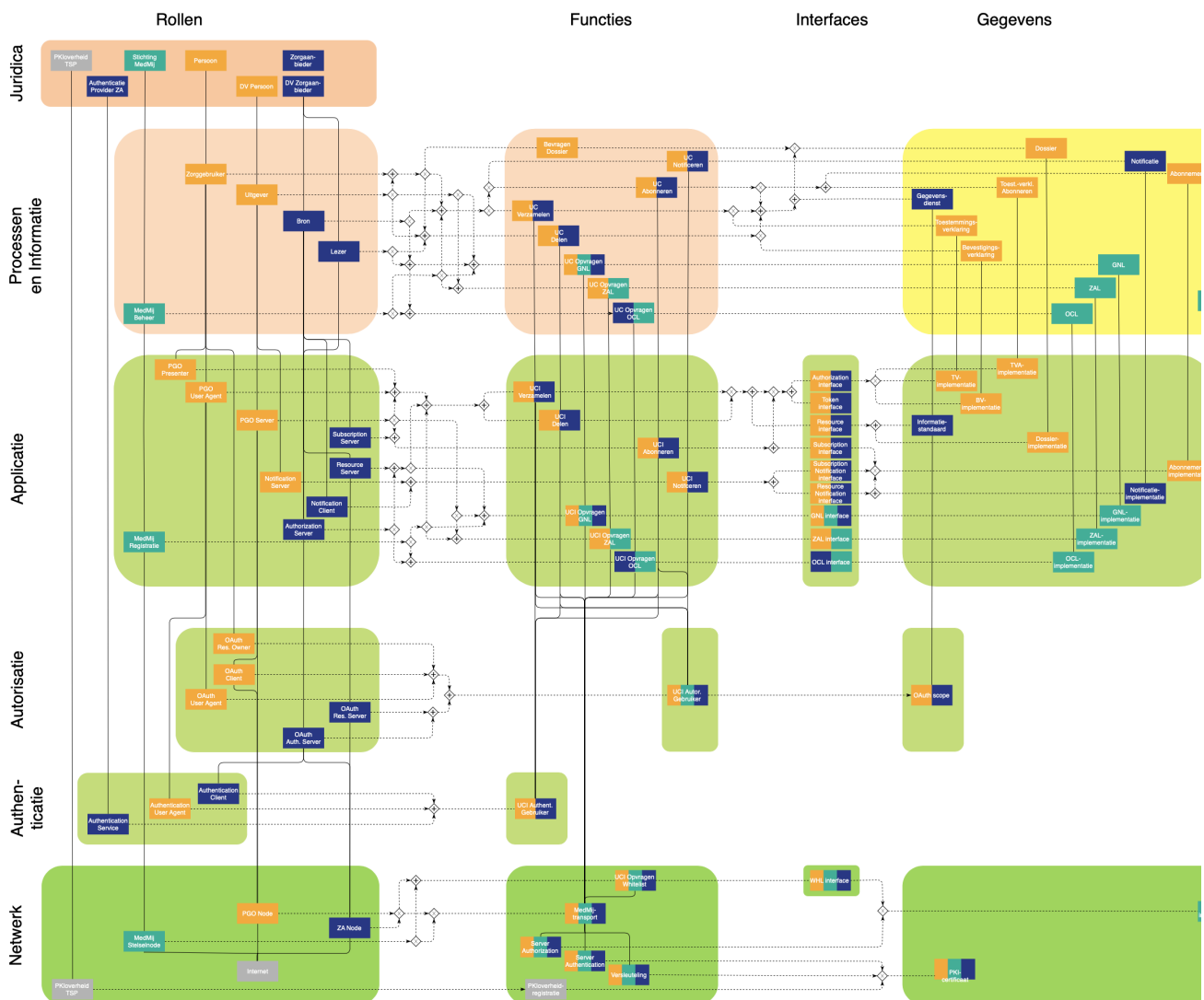
Op het volgende abstractieniveau, de [Applicatielaag](#), komt ter sprake dat, en hoe, deze bedrijfsprocessen met de erin omgaande gezondheidsinformatie, geautomatiseerd moeten worden uitgevoerd, in samenwerking tussen de rollen. Het is de meest complexe laag, die twee bijzondere deel-lagen heeft: één voor authenticatie van de *Persoon* en één voor diens autorisatie van het informatieverkeer.

Op het onderste abstractieniveau, de [Netwerk](#)-laag, zijn de verantwoordelijkheden opgenomen op het gebied van de netwerkinfrastructuur.

In onderstaand diagram zijn deze abstractieniveaus herkenbaar. Op elke laag worden de architectuurelementen aangegeven die nodig zijn op de betreffende laag, met hun onderlinge verbanden binnen en tussen de lagen. Het diagram op deze pagina is niet bedoeld om ineens de samenhang tussen alle details te specificeren. Dat gebeurt stap voor stap op de pagina's die bij de specificatielagen horen; op de pagina voor elke laag wordt de bij die laag passende uitsnede van het diagram herhaald en behandeld. Op deze pagina wil het diagram slechts twee rollen vervullen:

- een overzicht over de lagen (en kolommen) van de architectuur van het MedMij Afsprakenstelsel
- een index waarmee men bij een architectuurdetail snel de laag kan vinden waarop er op dat detail wordt ingegaan.

De toelichting onder het diagram bespreekt nog wat de kolommen, de kleuren en de lijntjes in het diagram betekenen en bereidt voor op lezing van de detailpagina's.



## Toelichting

In de architectuur is ook een vierdeling in kolommen aangebracht: rollen, functies, interfaces en gegevens. Interfaces zijn alleen aan de orde op de **Applicatie**-laag, waarvan zij de spil vormen. Op elke laag spelen voor die laag specifieke rollen, die voor die laag specifieke functies uitvoeren met behulp van voor die laag specifieke gegevens. Om precies die reden zijn de proceslaag en de informatielaag uit het interoperabiliteitsmodel van Nictiz gecombineerd in één laag, waaraan dus bovendien een rollenkolom is toegevoegd. Omdat het om een architectuur van een afsprakenstelsel gaat -- en nog niet om een architectuur van systemen en oplossingen -- speelt de rollenkolom een sleutelrol in de samenhang van de gehele architectuur. Rollen zijn bundels van verantwoordelijkheden. Die verantwoordelijkheden gaan over uit te voeren functies (tweede kolom), die op hun beurt gebruik maken van gegevens (vierde kolom). Een rol is dus geen individuele partij en geen systeem of component. Pas als individuele partijen de rol gaan vervullen, hebben zij daarvoor systemen en componenten nodig, als implementatie van de rollen.

De **Applicatielaag** heeft twee deellagen: een autorisatielaag en een authenticatielaag. Dat komt doordat voor deze twee kwesties standaarden worden gebruikt die hun eigen rollenstructuur hebben,

waarmee dus een expliciete binding moet worden aangebracht. Bovendien is het op deze manier mogelijk om de afspraken die specifiek voortvloeien uit het ontwerp van die standaarden een herkenbare en beheersbare plaats te geven.

Boven de [Processen-en-informatielaag](#) is een extra laag aangebracht: [Juridica](#). Deze laag kent alleen de rollen-kolom, niet de andere twee. Die laatste staan namelijk behandeld op de pagina [Overeenkomsten en rechtsrelaties](#). Deze laag is alleen bedoeld voor de koppeling, rollen-gewijs, van de architectuur met het juridische deel van het MedMij Afsprakenstelsel, zodat duidelijk wordt welke architecturale en technische verantwoordelijkheden verbonden zijn aan welke juridische rollen.

Op de authenticatielaag is het niet nodig nadere afspraken te maken over gegevens. Daarvoor kan geheel teruggevallen worden op de specificaties van het de koppelvlakken die door de *Authentication Provider ZA* worden geboden. Daarom ontbreekt die kolom in de architectuur.

De kleuren van de grote vlakken komen overeen met de kleuren die Nictiz aan de betreffende architectuuraspecten geeft in haar [interoperabiliteitsmodel](#). De kleuren van de architectuurelementen (de kleine rechthoeken) geven aan in welk domein het betreffende architectuurelement geplaatst is. Daarbij is allereerst de huisstijl van MedMij aangehouden, zodat:

- oranje staat voor het Persoonsdomein;
- blauw staat voor het Zorgaanbiedersdomein en
- groen staat voor het MedMij-domein.

De grijze kleur staat voor externe rollen waarvan het MedMij Afsprakenstelsel gebruik maakt. Waar meerdere kleuren zijn gecombineerd, geeft dat aan dat in het betreffende architectuurelement de domeinen samenwerken.

De verticale lijnen in de architectuur verbinden de rollen, functies en gegevens tussen de verschillende lagen.

De rollen in het MedMij Afsprakenstelsel zijn bijeen horende setjes verantwoordelijkheden. Ze komen voor op elke laag van de architectuur, van de [Juridische](#) laag, via de [Processen-en-Informatie](#)-laag en de [Applicatie](#)-laag tot en met de [Netwerk](#)-laag. Tussen twee aangrenzende architectuurlagen, zijn de rollen aan elkaar gekoppeld. Een rol op de ene laag gaat gepaard met een of meerdere rollen op de laag eronder. De rolbindingen vormen zo de ruggengraat van de architectuur van het MedMij Afsprakenstelsel.

Een rol is nadrukkelijk geen component of systeem. Menige rol wordt weliswaar door componenten en systemen gerealiseerd, maar hoe dat precies gebeurt, en hoeveel en welke componenten- of systeemarchitectuur daarvoor wordt gebruikt is aan de *Dienstverlener*, zolang deze zijn rollen, op alle lagen, naar behoren speelt, dat wil zeggen, de verantwoordelijkheden van die rollen draagt. Zo wordt aan *Dienstverleners*, in beide domeinen, volop ruimte geboden een businessmodel naar eigen inzicht te kiezen, waarin volop ruimte is voor onderaannemers, zolang de eindverantwoordelijkheid jegens het MedMij Afsprakenstelsel maar onvervreemdbaar bij de *Dienstverlener* blijft liggen.

Voor een *Dienstverlener* moet er verder maximale vrijheid zijn om één rol op het ene niveau in te richten met meerdere op de laag eronder. Het moet echter andersom wel duidelijk blijven, op alle lagen, dat er één *Dienstverlener* verantwoordelijk is voor elke rol. Meerdere rollen kunnen dus niet op één lagere worden afgebeeld. Het is wel mogelijk dat meerdere rollen door een gezamenlijk systeem gerealiseerd worden, zolang hun afzonderlijke eindverantwoordelijken maar intact blijven.

Dat wil zeggen dat één rol op de hogere architectuurlaag in het algemeen wordt ingevuld met één of meer verbonden rollen op de laag eronder. Andersom echter hoort één rol op de lagere architectuurlaag bij één verbonden rol op de hogere laag. Omdat de Nodes op [Netwerk](#)-niveau

worden geïdentificeerd met een hostname, kan zo altijd aan de logging op [Netwerk](#)-niveau afgelezen worden welke deelnemer verantwoordelijk is voor welke gebeurtenis.

Met de horizontale stippellijnen staat aangegeven welke rollen welke functies uitvoeren, respectievelijk welke functies welke gegevens gebruiken. Om te voorkomen dat er een onoverzichtelijke wirwar van stippellijnen ontstaat, maakt de figuur gebruik van joins en splits. Joins en splits zijn getekend als ruitjes. Een join (samenkomst) kenmerkt zich door meerdere inkomende pijlen en één uitgaande, een split (splitsing) juist door één inkomende en meerdere uitgaande pijlen.

Er komen twee tekens voor in de ruitjes.

- Een maaltteken staat voor exclusief, wat wil zeggen dat slechts één van de inkomende pijlen (bij joins) of uitgaande pijlen (bij splits) tegelijk aan de orde is.
- Een plusteken staat voor inclusief, wat wil zeggen dat altijd alle inkomende pijlen (bij joins) of uitgaande pijlen (bij splits) tegelijk aan de orde zijn.

Zo is bijvoorbeeld, op de laag *Processen en Informatie*, de rol *MedMij Beheer* betrokken:

- in drie use cases: *UC Opvragen ZAL*, *UC Opvragen OCL* en *UC Opvragen GNL* maar niet tegelijk (exclusief).
- in de use case *UC Opvragen ZAL* tegelijk (inclusief) met de rol *Uitgever*.

Voor elke laag staan de afspraken uitgewerkt op een aparte pagina:

- [Juridica](#)
- [Processen en Informatie](#)
- [Applicatie](#), inclusief Authenticatie en Autorisatie
- [Netwerk](#)

Elke pagina kan subpagina's hebben voor deelaspecten. Die afspraken bestaan steeds uit:

- de identificatie van de rollen op deze (deel)laag en de binding van die rollen aan de rollen op de laag erboven;
- de verantwoordelijkheden die de rollen op deze (deel)laag hebben in het uitvoeren van zekere functies met zekere gegevens.

Een aparte pagina [Informatiemodellen](#), met drie subpagina's, specificeert de conceptuele structuur van (een deel van) het begrippenapparaat van de architectuur van het MedMij Afsprakenstelsel en vertaalt die via logische modellen naar technische modellen van enkele componenten. Zo wordt tot op technisch niveau de interoperabiliteit op het MedMij-netwerk geborgd.

Vaak wordt er in de verantwoordelijkheden verwezen naar een specificatie. Dit kan een specifiek voor MedMij gespecificeerde use case zijn, bijvoorbeeld, maar is vaak ook een standaard, vooral voor informatie. De specificatie zal niet in de verantwoordelijkheid zelf staan uitgeschreven; er zal naar verwezen worden. Zo hoeft voor detailaanpassingen in de specificatie niet steeds de verantwoordelijkheid te worden aangepast. Dat zou, zeker bij standaardspecificaties, een ongewenste beheerlast van het afsprakenstelsel opleveren.

De rollen en verantwoordelijkheden zijn om te beginnen bondig en stellig als regel geformuleerd. Pas in tweede instantie zijn ze voorzien van toelichting. De opzet is dus niet die van een verhalende uiteenzetting van het stelsel, maar die van een setje afspraken, artikelsgewijs. Dat maakt de

architectuur geschikt om als verlengstuk van de deelnemersovereenkomst te worden gebruikt. De allereerste vraag is: *Wat is de afspraak?* In tweede instantie spelen vragen als: *Waarom is hiervoor gekozen?* en *Wat betekent die afspraak?*

Waar in de beschrijving van de architectuur, de daarin bevatte rollen en verantwoordelijkheden en de toelichtingen daarop, met een naam wordt gerefereerd aan architectuurcomponenten, zoals die voorkomen in het diagram hierboven, wordt de naam *italiek* en met Beginkapitaal geschreven. Dat geldt ook voor de pad-expressies in de invarianten bij de [Informatiemodellen](#). Variabelen in die pad-expressies staan ook *italiek*, maar beginnen met een kleine letter.

Sommige architectuurcomponenten worden ook vertegenwoordigd door een klasse, attribuut, element of type in de [Informatiemodellen](#). Omdat de spelling van de namen in de [Informatiemodellen](#) formeler is, kan de naamgeving daar iets afwijken van die in de rest van de architectuur, in het gebruik van spaties en hoofdletters. In de [Informatiemodellen](#) beginnen alle namen met een hoofdletter. Midden in de namen verschijnen bovendien hoofdletters wanneer, en alleen wanneer, het daar resterende deel van de naam ook als aparte naam voorkomt.

Technische code-fragmenten worden in `monospace` geciteerd.

## Rollen en hun getalsverhoudingen

De rollen in het MedMij Afsprakenstelsel zijn bijeen horende setjes verantwoordelijkheden. Ze komen voor op elke laag van de architectuur, van de [Juridische](#) laag, via de [Processen-en-Informatie](#)-laag en de [Applicatie](#)-laag tot de [Netwerk](#)-laag. Tussen twee aangrenzende architectuurlagen, zijn de rollen aan elkaar gekoppeld. Een rol op de ene laag gaat gepaard met een of meerdere rollen op de laag eronder. Een rol is dus geen component of systeem. Menige rol wordt weliswaar door componenten en systemen gerealiseerd, maar hoe dat precies gebeurt, en hoeveel en welke componenten- of systeemarchitectuur daarvoor wordt gebruikt is aan de *Dienstverlener*, zolang deze zijn rollen, op alle lagen, maar naar behoren speelt, dat wil zeggen, de verantwoordelijkheden van die rollen draagt.

Voor een *Dienstverlener* moet er maximale vrijheid zijn om één rol op het ene niveau in te richten met meerdere op de laag eronder. Het moet echter andersom wel duidelijk blijven, op alle lagen, dat er één *Dienstverlener* verantwoordelijk is voor elke rol. Meerdere rollen kunnen dus niet op één lagere worden afgebeeld. Het is wel mogelijk dat meerdere rollen door een gezamenlijk systeem gerealiseerd worden, zolang hun afzonderlijke eindverantwoordelijken maar intact blijven.

De *Nodes* op [Netwerk](#)-niveau worden geïdentificeerd met een hostname. Omdat dus ook elke *PGO Node* en *ZA Node* bij één *Dienstverlener* hoort, is aan de hostname de *Dienstverlener* te herkennen.

In het persoonsdomein geldt zo dat:

- één *Dienstverlener Persoon* één of meerdere *Uitgevers* verzorgt en elke *Uitgever* verzorgd wordt door één *Dienstverlener Persoon*;
- één *Uitgever* door één of meerdere *PGO Servers* wordt gerealiseerd en elke *PGO Server* één *Uitgever* realiseert;
- één *PGO Server* door één of meerdere *PGO Nodes* wordt ondersteund en elke *PGO Node* één *PGO Server* ondersteunt.

Zo kan dus ook in de *OAuth Clientlist* de hostname van een *PGO Node* geassocieerd worden met één (gebruikersvriendelijke naam van de) *PGO Server*.

In het zorgaanbiedersdomein geldt zo dat:

- één *Dienstverlener Zorgaanbieder* één of meerdere *Bronnen* en/of *Lezers* verzorgt en elke *Bron* en/of *Lezer* verzorgd wordt door één *Dienstverlener Zorgaanbieder*;
- één *Bron* en/of *Lezer* door één of meer combinaties van één *Authorization Server* en één *Resource Server* wordt gerealiseerd en elke combinatie van één *Authorization Server* en één *Resource Server* één *Bron* en/of *Lezer* realiseert;
- één *Authorization Server*, net als één *Resource Server*, door één of meerdere *ZA Nodes* wordt ondersteund;
- elke *ZA Node* hetzij één *Authorization Server* ondersteunt, hetzij één *Resource Server*, hetzij de combinatie van één *Authorization Server* en één *Resource Server* ondersteunt;
- elke *ZA Node* één of meerdere endpoints kent en elk endpoint hoort bij één *ZA Node*, zodanig dat de hostname in een endpoint-adres de hostname van die *ZA Node* is.

Het vierde punt staat het toe om een *Authorization Server* en een *Resource Server* te verdelen over verschillende *ZA Nodes*, maar ook te combineren op dezelfde. Het derde punt staat het zelfs toe dat *Authorization Server* en *Resource Server* elk apart op meerdere *ZA Nodes* worden geprojecteerd. Het kan dan voorkomen dat, bij de betreffende *ZorgaanbiederGegevensdiensten* in de *Zorgaanbiederslijst*, hostnames in de endpointadressen staan die verschillen tussen het authorization endpoint, het token endpoint en het resource endpoint, zelfs bij eenzelfde *Interfaceversie*. Een belangrijke eis blijft evenwel dat al deze hostnames bij *ZA Nodes* van eenzelfde *Dienstverlener Zorgaanbieder* horen. De hele flow behorend bij een zekere *ZorgaanbiederGegevensdienst* moet namelijk onder de eindverantwoordelijkheid van één zo'n *Dienstverlener* vallen, namelijk van de *Dienstverlener* die die *ZorgaanbiederGegevensdienst* ontsluit. Zo blijft die integrale eindverantwoordelijkheid ook op net-werk-niveau toetsbaar. Zie de drie (ingewikkelde) *invarianten* bij *ZorgaanbiederGegevensdienst* van het soort "niet-lokale afhankelijkheid".

Hoezeer ook alle eindverantwoordelijkheden gedragen worden door de *Dienstverleners* die deelnemer zijn in het MedMij Afsprakenstelsel, zij kunnen ervoor kiezen de uitvoering van die verantwoordelijkheden deels of zelfs geheel uit te besteden. In een mogelijke systeemarchitectuur maken meerdere *Resource Server*-systemen gebruik van een-zelf-de (al dan niet uitbesteed) *Authorization Server*-systeem. Het is mogelijk dat die *Resource Server*-systemen samen onder de eindverantwoordelijkheid van één *Dienstverlener Zorgaanbieder* vallen, met de uitvoering al dan niet uitbesteed. Het is ook mogelijk dat twee verschillende *Dienstverleners Zorgaanbieder* voor de *Authorization Server* gebruik maken van eenzelfde onderaannemer. De host-names in de adressen van de *Authorization Endpoints/Token Endpoints* zullen dan evengoed verschillen tussen die twee eindverantwoordelijke *Dienstverleners Zorgaanbieders*, zelfs al zou er het zelfde *Authorization Server*-systeem achter zitten. Voor de *ZorgaanbiederGegevensdiensten* waarvoor *Dienstverlener Zorgaanbieder A* verantwoordelijk is, moet dat de hostname van een *Node* van A zijn; voor de *Zorgaanbieder-Gegevensdiensten* waarvoor *Dienstverlener Zorgaanbieder B* verantwoordelijk is moet dat de hostname van een *Node* van B zijn.

De architectuur heeft zo maximale ruimte aan de eigen businessmodellen en architecturen van *Dienstverleners Zorgaanbieder* willen geven zonder daarbij de interoperabiliteit en strakke eindverantwoordelijkheden geweld aan te doen.



## Coördinatie, regie en uitwisseling

### Scheiding tussen Regie, Uitwisseling en Coördinatie

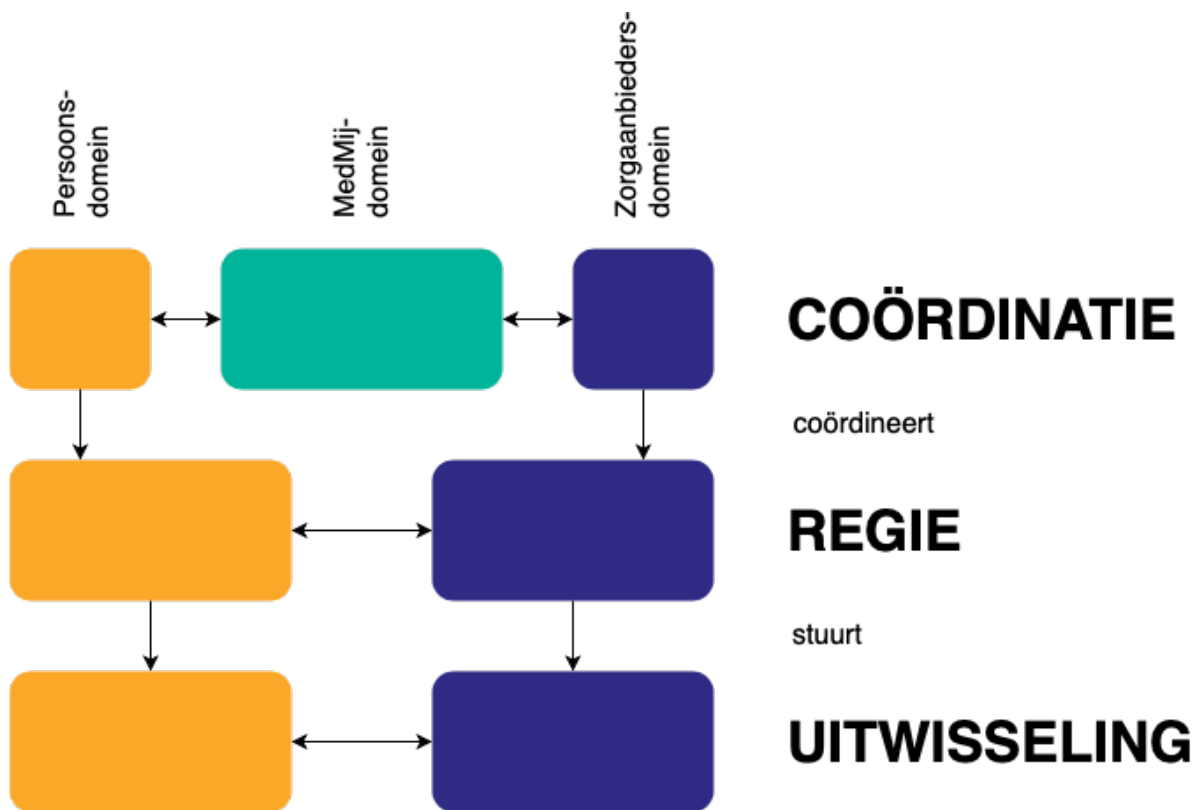
Het MedMij Afsprakenstelsel scheidt, op de [Processen-en-Informatie](#)-laag en op de [Applicatie](#)-laag, drie hoofdfuncties: *Regie*, *Uitwisseling* en *Coördinatie*. Al het gedrag van de betrokken rollen op deze lagen hoort bij één van deze drie hoofdfuncties. De hoofdfuncties hebben een onderlinge relatie. Aan de hoofdfuncties zijn beginselkeuzes verbonden (zie onder).

Centraal staat de *Regie*; hiermee voert de *Persoon* regie, in interactie met de *Zorgaanbieder*, over (de uitwisseling van) zijn gezondheidsinformatie. Dat doet hij als uitgever, conform [principe 16](#). Onder deze hoofdfunctie vallen bijvoorbeeld het geven van toestemming van de *Persoon* aan de *Zorgaanbieder*, het authenticeren van de *Persoon* door de *Zorgaanbieder*, het autoriseren van de PGO door de *Zorgaanbieder* en het aangaan, beëindigen en onderhouden van abonnementen. *Regie* leidt zo steeds tot overeenkomsten tussen *Persoon*, *Zorgaanbieder* en *Dienstverlener Persoon*, en is gebaseerd op vertrouwen in de identiteit van de anderen in de overeenkomst. De *Dienstverlener zorgaanbieder* is geen partij in deze overeenkomsten, omdat deze geen verwerkingsverantwoordelijke is zoals wel de *Dienstverlener Persoon*. De *Dienstverlener Zorgaanbieder* speelt wel een belangrijke uitvoerende rol in de totstandkoming van de overeenkomsten, als verwerker namens de *Zorgaanbieder*.

*Regie* stuurt *Uitwisseling*. *Uitwisseling* geeft uitvoering aan de *Regie*. Deze tweede hoofdfunctie voert het feitelijke verkeer van gezondheidsinformatie uit, van *Zorgaanbieder* naar PGO (*Verzamelen* en *Notificeren*) of andersom (*Delen*). Alle uitwisseling vindt plaats conform gestandaardiseerde *Gegevensdiensten* en in het kader van een *Regie*-overeenkomst. *Regie* en *Uitwisseling* worden, conform [principe 10](#), alleen uitgevoerd door partijen die onder de volledige verantwoordelijkheid vallen van een *Dienstverlener persoon* of *Dienstverlener zorgaanbieder*, en dus decentraal. MedMij is zelf niet betrokken in de uitvoering van *Regie* of *Uitwisseling*.

Toch is een voorbereidende rol van MedMij nodig om de partijen in staat te stellen de onderlinge *Regie* tot stand te brengen. *Coördinatie* is de derde hoofdfunctie, die zorgt voor het vertrouwen tussen het Persoonsdomein en het Zorgaanbiedersdomein, zodat deze van elkaar kunnen weten wat zij kunnen en mogen op het MedMij-netwerk. Deze functie wordt uitgevoerd met de *Catalogus*, die zegt welke *Gegevensdiensten* op enig moment op het MedMij-netwerk van kracht zijn, en vier lijsten (*Gegevensdienstnamenlijst*, *OAuthclientlist*, *Whitelist* en *Zorgaanbiederslijst*), die zeggen welke *Deelnemers* er zijn, en wat zij kunnen en mogen.





## Processen-en-Informatie-laag

Op deze laag zijn worden de drie hoofdfuncties door de volgende rollen uitgevoerd.

hoofdfunctie	Persoonsdomein	MedMij-domein	Zorgaanbiedersdomein
<b>Coördinatie</b>	<ul style="list-style-type: none"> <li>Uitgever</li> </ul>	<ul style="list-style-type: none"> <li>MedMij Beheer</li> </ul>	<ul style="list-style-type: none"> <li>Bron</li> <li>Lezer</li> </ul>
<b>Regie</b>	<ul style="list-style-type: none"> <li>Zorggebruiker</li> <li>Uitgever</li> </ul>	-	<ul style="list-style-type: none"> <li>Bron</li> <li>Lezer</li> </ul>
<b>Uitwisseling</b>	<ul style="list-style-type: none"> <li>Zorggebruiker</li> <li>Uitgever</li> </ul>	-	<ul style="list-style-type: none"> <li>Bron</li> <li>Lezer</li> </ul>

Op deze laag worden de drie hoofdfuncties in de volgende use cases uitgevoerd.

hoofdfunctie	Persoonsdomein	MedMij-domein	Zorgaanbiedersdomein
<b>Coördinatie</b>	<ul style="list-style-type: none"> <li>UC Opvragen GNL</li> </ul>		

	<ul style="list-style-type: none"> <li>• <a href="#">UC Opvragen ZAL</a></li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">UC Opvragen GNL</a></li> <li>• <a href="#">UC Opvragen ZAL</a></li> <li>• <a href="#">UC Opvragen OCL</a></li> </ul>	<ul style="list-style-type: none"> <li>• <a href="#">UC Opvragen GNL</a></li> <li>• <a href="#">UC Opvragen OCL</a></li> </ul>
<b>Regie</b>	<ul style="list-style-type: none"> <li>• <a href="#">UC Verzamelen</a> (authorization interface en token interface)</li> <li>• <a href="#">UC Delen</a> (authorization interface en token interface)</li> <li>• <a href="#">UC Abonneren</a></li> <li>• <a href="#">UC Notificeren</a> (voor abonnements-Notificaties)</li> <li>• <a href="#">UC Portabiliteitsrapport</a></li> </ul>	-	<ul style="list-style-type: none"> <li>• <a href="#">UC Verzamelen</a> (authorization interface en token interface), inclusief de beschikbaarheidsvoorwaarde</li> <li>• <a href="#">UC Delen</a> (authorization interface en token interface), inclusief de ontvankelijkheidsvoorwaarde</li> <li>• <a href="#">UC Abonneren</a></li> <li>• <a href="#">UC Notificeren</a> (voor abonnements-Notificaties)</li> </ul>
<b>Uitwisseling</b>	<ul style="list-style-type: none"> <li>• <a href="#">UC Verzamelen</a> (resource interface)</li> <li>• <a href="#">UC Delen</a> (resource interface)</li> <li>• <a href="#">UC Notificeren</a> (voor inhoudelijke Notificaties)</li> </ul>	-	<ul style="list-style-type: none"> <li>• <a href="#">UC Verzamelen</a> (laatste fase)</li> <li>• <a href="#">UC Delen</a> (resource interface)</li> <li>• <a href="#">UC Notificeren</a> (voor inhoudelijke Notificaties)</li> </ul>

## Applicatielaag

Op deze laag zijn worden de drie hoofdfuncties door de volgende rollen uitgevoerd.

hoofdfunctie	Persoonsdomein	MedMij-domein	Zorgaanbiedersdomein
<b>Coördinatie</b>	<ul style="list-style-type: none"> <li>• PGO Server</li> </ul>	<ul style="list-style-type: none"> <li>• MedMij Registratie</li> </ul>	<ul style="list-style-type: none"> <li>• Authorization Server</li> </ul>
<b>Regie</b>	<ul style="list-style-type: none"> <li>• PGO Gebruiker</li> <li>• PGO User Agent</li> <li>• PGO Server</li> <li>• Notification Server (voor subscription notifications)</li> <li>• OAuth Resource Owner</li> <li>• OAuth User Agent</li> </ul>		<ul style="list-style-type: none"> <li>• Authorization Server</li> <li>• Subscription Server</li> <li>• Notification Client (voor subscription notifications)</li> <li>• OAuth Authorization Server</li> <li>• Authentication Client</li> <li>• Authentication Service</li> </ul>

	<ul style="list-style-type: none"> <li>• <i>OAuth Client</i></li> <li>• <i>Authentication User Agent</i></li> </ul>		<ul style="list-style-type: none"> <li>• <i>Subscription Server</i></li> </ul>
<b>Uitwisseling</b>	<ul style="list-style-type: none"> <li>• <i>PGO Gebruiker</i></li> <li>• <i>PGO User Agent</i></li> <li>• <i>PGO Server</i></li> <li>• <i>Notification Server</i> (voor resource notifications)</li> <li>• <i>OAuth Resource Owner</i></li> <li>• <i>OAuth User Agent</i></li> <li>• <i>OAuth Client</i></li> </ul>		<ul style="list-style-type: none"> <li>• <i>Resource Server</i></li> <li>• <i>OAuth Resource Server</i></li> <li>• <i>Notification Client</i> (voor resource notifications)</li> </ul>

Op deze laag worden de drie hoofdfuncties op de volgende interfaces uitgevoerd. Elk interface hoort bij één hoofdfunctie.

hoofdfunctie	interface
<b>Coördinatie</b>	<ul style="list-style-type: none"> <li>• <a href="#">GNL interface</a></li> <li>• <a href="#">OCL interface</a></li> <li>• <a href="#">ZAL interface</a></li> </ul>
<b>Regie</b>	<ul style="list-style-type: none"> <li>• <a href="#">user interface (Verklaringen)</a></li> <li>• <a href="#">authorization interface</a></li> <li>• <a href="#">token interface</a></li> <li>• <a href="#">subscription interface</a></li> <li>• <a href="#">subscription notification interface</a></li> </ul>
<b>Uitwisseling</b>	<ul style="list-style-type: none"> <li>• <a href="#">resource interface</a></li> <li>• <a href="#">resource notification interface</a></li> </ul>

## Beginnelsen

De architectuur van het MedMij Afsprakenstelsel hanteert de volgende beginselen ten aanzien van de hoofdfuncties.

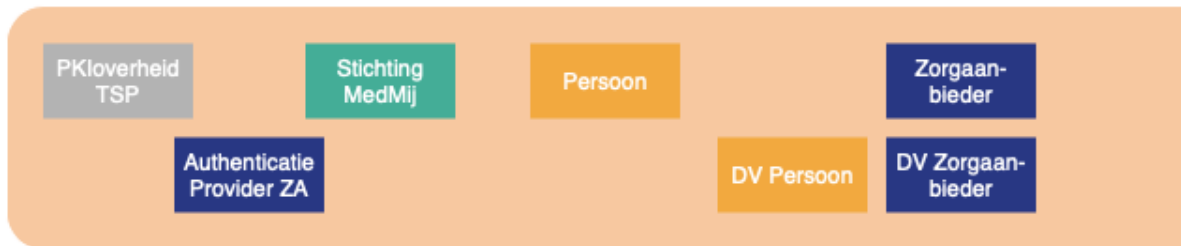
1. **Eén interface, één hoofdfunctie.** Een interface (op de [Applicatie](#)-laag) hoort bij precies één hoofdfunctie. Bij voorkeur horen ook een rol en een use case bij precies één hoofdfunctie. Deze voorkeur is sterker op de [Applicatie](#)-laag dan op de [Processen en informatie](#)-laag. Deze voorkeur is bovendien minder sterk bij de gebruikersrollen in beide domeinen.
2. **Decentrale regie en uitwisseling.** Noch *MedMij Beheer* noch enige andere partij heeft een centrale of intermediaire rol in *Regie* of *Uitwisseling* tussen het Persoonsdomein en het Zorgaanbiedersdomein. Die intermediaire rol is er voor MedMij Beheer wel in *Coördinatie*. Dit beginsel is een uitwerking van [principe 7](#).

3. **Geen sector-specifieke standaarden of oplossingen voor Coördinatie en Regie.** Voor *Coördinatie* en *Regie* gebruikt het MedMij Afsprakenstelsel geen sector-specifieke oplossingen of standaarden. Sector-specificiteit moet hier niet alleen qua inhoud begrepen worden, maar ook qua governance (van een standaard). Gezondheid houdt zich niet aan sectorale verkavelingen; de *Regie* erop moet niet sectoraal verkaveld worden, omdat dat de regie zou beperken. Voor *Uitwisseling* heeft sector-specificiteit evenmin de voorkeur, maar vraagt de realiteit erom sector-specifieke uitwisselstandaarden te gebruiken (zoals HL7 voor de zorgsector en bijvoorbeeld StUF voor het gemeentelijke veld). Verreweg de meeste informatie-inhoudelijke standaardisatie vindt binnen sectoren plaats. Dit beginsel laat [principe 19](#) onverlet.
4. **Geen uitwisseling zonder regie.** Er vindt geen *Uitwisseling* plaats waaraan geen *Regie*-overeenkomst ten grondslag ligt. Mochten er *Uitwisselingen* in het MedMij Afsprakenstelsel moeten worden opgenomen die een andere legitimatie vereisen dan waarin *Regie* op enig moment voorziet, moet die nieuwe legitimatie dus onder de hoofdfunctie *Regie* worden toegevoegd. *Regie* bieden aan *Personen* op hun gezondheid(sinformatie) is het hoofddoel van MedMij. *Coördinatie* voorziet slechts in wat noodzakelijk is om dat doel te bereiken.
5. **Uitwisseling gestandaardiseerd en gecoördineerd.** Al het verkeer in het kader van *Uitwisseling* vindt plaats op basis van gestandaardiseerde *Gegevensdiensten*, die in de *Catalogus* zijn opgenomen.
6. **Gegevensdienst als eenheid van Regie.** De eenheid van *Regie* tussen *Persoon* en *Zorgaanbieder* is een hele *Gegevensdienst*. Een *Uitwisseling*, bijvoorbeeld een *Notificatie*, kan echter een kleinere eenheid betreffen, maar wel altijd als onderdeel van één *Gegevensdienst*. Ook elk Abonnement betreft één *Gegevensdienst*.
7. **Eén taal voor Coördinatie.** Alle functionaliteit van de hoofdfunctie *Coördinatie* is gestoeld op één gezamenlijke set [informatiemodellen](#), die geordend zijn in drie lagen: conceptueel ([metamodel](#)), logisch ([logische modellen](#)) en technisch ([XML-schema's](#)). Deze informatiemodellen zijn onderdeel van het MedMij Afsprakenstelsel. Dat geldt niet voor de informatiestandaarden die voor de *Gegevensdiensten* gebruikt worden. Die zijn weliswaar per *Gegevensdienst* gestandaardiseerd, maar niet over alle *Gegevensdiensten* heen, op *Catalogus*-niveau, gestandaardiseerd, omdat dat MedMij zou invangen in één sector (zie beginsel 3).
8. **Toekomstvast scheiding.** De scheiding tussen de drie hoofdfuncties vertegenwoordigt een structureel aspect van het evoluerende MedMij Afsprakenstelsel. Dat betekent dat, ondanks de grote implementatievrijheid van *Deelnemers*, zij hun implementatielast van nieuwe releases kunnen beperken door deze scheiding ook in hun implementatie-architectuur aan te brengen. De scheiding tussen de hoofdfuncties maakt de evolutie van het afsprakenstelsel voor *Deelnemers* voorspelbaarder.

## Juridica

### Rollen

#### Juridica



#### Toelichting

In deze laag staan de juridische rollen, als juridische basis voor de rollen op andere lagen van de architectuur. De reden dat deze laag in deze architectuur is opgenomen is dat haar rollen voor de samenhang tussen de verschillende architectuurlagen zorgen en de architectuur geborgd moet zijn in de juridische rollen in het MedMij Afsprakenstelsel. Bij een juridische rol horen verplichtingen voor het spelen van rollen op verschillende architectuurlagen.

De rollen die we hier in de architectuur noemen vallen uiteen in twee groepen:

1. de juridische rollen die partij zijn in MedMij-deelnemersovereenkomsten: *Dienstverlener persoon*, *Dienstverlener zorgaanbieder* en *Stichting MedMij*.
2. de juridische rollen die geen partij zijn in MedMij-deelnemersovereenkomsten, maar niettemin een uitvoerende verplichting hebben in de architectuur. Dat betekent dat de toepasselijke deelnemersovereenkomst van een deelnemer zal eisen dat deze een juridische relatie aangaat met die juridische rol. Het gaat hier om:
  - *Persoon* en *Zorgaanbieder*, wiens onderlinge informatierelatie door MedMij-verkeer wordt bediend;
  - *Authenticatie Provider ZA*, die voor *Zorgaanbieders* de authenticatie verzorgt van *Personen* die zich bij de *Zorgaanbieder* aandienen;
  - *PKloverheid TSP*, die certificaten uitgeeft waarmee het verkeer op het MedMij-netwerk betrouwbaar gemaakt kan worden.

In de architectuur van het afsprakenstelsel heeft de *Persoon* een operationele rol bij authenticatie en autorisatie van het gegevensverkeer. De *Zorgaanbieder* wordt operationeel geheel vertegenwoordigd door de *Dienstverlener Zorgaanbieder*.



In het Persoonsdomein is er naast de rol *Uitgever* ook de rol *Zorggebruiker*. Hoewel *Uitgever* namens *Zorggebruiker* handelt, kan *Zorggebruiker* niet ongenoemd blijven (verborgen achter de rol *Uitgever*) in de afspraken op deze en onderliggende lagen. Dat komt doordat *Zorggebruiker* niet enkel de gebruiker van *Uitgever*, maar allereerst het onderwerp van de gezondheidsinformatie die *Bron* ter beschikking moet stellen en *Lezer* ter beschikking gesteld wordt; daarvoor is authenticatie nodig. In het Zorgaanbiedersdomein ligt dat anders. In deze release van het afsprakenstelsel volstaat het om de *Bron* en *Lezer* te zien als de rollen die samen volledig verantwoordelijk zijn voor wat een *Zorgaanbieder* operationeel zou moeten doen. De implementatie van die verantwoordelijkheid is aan de *Bron*, respectievelijk *Lezer*. Dat werkt door in de [Applicatielaag](#) en de [Netwerklag](#).

Omdat ook de *Stichting MedMij* operationele verantwoordelijkheden heeft, staat hier de functionele rol van *MedMij Beheer*.

## Verantwoordelijkheden

### Toelichting

De verantwoordelijkheden op deze laag zijn geordend in hoofdstukken en secties als volgt:

- Dossier
  - Use cases
  - *Gegevensdiensten*
  - Authenticatie
  - Autorisatie
- Lijsten
  - *Zorgaanbiederslijst*
  - *OAuth Client List*
  - *Gegevensdienstnamenlijst*
  - *Whitelist*
- Logging en portabiliteit

Op meerdere plaatsen komen daarbij use cases (op deze laag) en use case-implementaties (op de [Applicatie](#)-laag) aan de orde. Een use case-implementatie is de implementatie van de use case met dezelfde naam. In deze release van het MedMij Afsprakenstelsel zijn er negen use cases, waarvan er zich zeven afspelen tussen het Persoons- en het Zorgaanbiedersdomein. Van deze zeven maken, om de interoperabiliteit in het MedMij-netwerk te borgen, stroomdiagrammen deel uit van het MedMij Afsprakenstelsel. De andere twee spelen zich helemaal binnen het Persoonsdomein af. Hiervan eist het MedMij Afsprakenstelsel wel dat erin moet worden voorzien, maar niet of slechts deels hoe; dat wordt aan de vrijheid van de MedMij-deelnemers gelaten.

Het gaat om de volgende use cases:

Use case	Stroomdiagram	Hoofdfunctie(s)
<i>UC Verzamelen</i>	met	<i>Regie en Uitwisseling</i>
<i>UC Delen</i>	met	<i>Regie en Uitwisseling</i>
<i>UC Raadplegen dossier</i>	zonder	<i>Regie</i>
<i>UC Portabiliteitsrapport</i>	zonder	<i>Regie</i>
<i>UC Abonneren</i>	met	<i>Regie</i>

UC Notificeren	met	Regie en Uitwisseling
UC Opvragen ZAL	met	Coördinatie
UC Opvragen OCL	met	Coördinatie
UC Opvragen GNL	met	Coördinatie

Voor registratie van *Deelnemers* en de vanwege hun deelname belangrijke gegevens zijn vooralsnog geen separate use cases geïdentificeerd, omdat registratie als een secundair proces wordt gezien. Zie hiervoor de pagina [Operationele processen](#).

De interpretatie door een *Zorggebruiker* van zorg- en gezondheidsinformatie die hij heeft verzameld bij een *Zorgaanbieder*, en de interpretatie door een *Zorgaanbieder* van zulke informatie die met hem /haar gedeeld is door een *Zorggebruiker*, hangt niet alleen af van de inhoud van die informatie, maar ook van de partij die de betreffende informatie oorspronkelijk heeft geregistreerd. We gebruiken hiervoor niet zomaar de term *Bron*, omdat deze term in de zin van het MedMij Afsprakenstelsel niet per se de oorspronkelijke herkomst (de auteur) betekent, maar alleen de onmiddellijke herkomst, gezien vanuit de *Uitgever*. In het MedMij Afsprakenstelsel is de auteursrol geen [juridische rol](#). Dat betekent niet alleen dat er binnen de grenzen van het MedMij Afsprakenstelsel momenteel geen basis is om auteursauthenticiteit (met bijvoorbeeld certificaten) te arrangeren, maar het brengt ook met zich mee dat informatie over de auteur, hoe wezenlijk ook, voor het MedMij Afsprakenstelsel een *gegevens-inhoudelijke* aangelegenheid is. Die informatie wordt immers ook gebruikt voor de interpretatie van de gedeelde zorg- en gezondheidsinformatie. Omdat, conform [principe 1](#), het MedMij Afsprakenstelsel gegevensneutraal wil zijn, wordt de auteursinformatie een onderdeel geacht van de inhoud van een *Gegevensdienst*.

## Dossier

### Use cases

1a. *Uitgever* biedt *Zorggebruiker* de use case *UC Verzamelen* om bij *Bron* gezondheidsinformatie te verzamelen bij *Zorgaanbieder*, indien deze die informatie beschikbaar stelt, die op deze *Zorggebruiker* betrekking heeft en laat deze in een persoonlijk gezondheidsdossier (kortweg *Dossier*) van *Zorggebruiker* bewaren. Bij deze use case betrokken rollen gebruiken hiertoe het betreffende [stroomdiagram](#).

#### Toelichting

Deze verantwoordelijkheid introduceert ook de notie van een persoonlijk gezondheidsdossier. Voor het voldoen aan deze regel is het dus niet voldoende aan de *Zorggebruiker* alleen inkijk in gezondheidsinformatie te bieden. Hij/zij moet het ook kunnen opslaan en beheren. Omdat deze functie zich over verschillende functionele rollen uitstrekt, is om interoperabiliteitsredenen de specificatie van het stroomdiagram aangehaald.

1b. *Uitgever* biedt *Zorggebruiker* de use case *UC Delen* om bij *Lezer* ten behoeve van een *Zorgaanbieder*, indien deze daartoe ontvankelijk is, gezondheidsinformatie te plaatsen die op deze *Zorggebruiker* betrekking heeft en die afkomstig is uit het *Dossier*. Bij deze use case betrokken rollen gebruiken hiertoe het betreffende [stroomdiagram](#).

#### Toelichting



Voor een beschrijving van overeenkomsten en verschillen tussen *UC Verzamelen* en *UC Delen*, zie de pagina over [UC Delen](#).

1c. *Uitgever* draagt ervoor zorg dat in het *Dossier* bij alle bij *Bron* in het kader van een *Gegevensdienst* verzamelde informatie onlosmakelijk deze *Bron* en *Gegevensdienst* als bron en verzamelcontext worden aangetekend. *Uitgever* draagt ervoor zorg dat, in geval van het delen van informatie met een (andere) *Zorgaanbieder* deze bron- en context-informatie wordt meegeleverd aan de *Lezer*. Voor de benoeming van de *Bron* wordt daarbij gebruik gemaakt van de *Zorgaanbiedersnaam*. Voor de benoeming van de context wordt daarbij gebruik gemaakt van de betreffende *Gegevensdienstnaam* uit de [Gegevensdienstnamenlijst](#).

#### Toelichting

Hiermee wordt geborgd dat bij de uitgewisselde zorg- en gezondheidsinformatie altijd duidelijk is bij welke *Bron* en in welke context (*Gegevensdienst*) deze is verzameld. Een *Lezer* van deze informatie kan deze meta-informatie gebruiken voor een betere interpretatie van de betreffende informatie. Mochten hieruit alsnog interpretatievragen komen, kan de *Lezer* zich vervoegen bij betreffende *Bron*.

2a. *Uitgever* biedt *Zorggebruiker* de use case *UC Raadplegen dossier* om het persoonlijk gezondheidsdossier te raadplegen.

#### Toelichting

Zie onder 1. Omdat deze functie zich niet over meerdere domeinen uitstrekt, is zij niet nader gespecificeerd in een stroomdiagram. Het is aan de vrijheid van de *Deelnemer* om deze naar behoefte van haar klanten in te richten. Maar zij mag niet ontbreken, omdat dan de *Zorggebruiker* geen [Regie](#) over het dossier zou kunnen voeren.

2b. In het kader van de use case *UC Raadplegen dossier* zal *Zorggebruiker* te allen tijde moeten kunnen nagaan:

- welke inhoud van het *Dossier* wel, en welke niet, via MedMij-verkeer van *Bron* is betrokken van welke *Zorgaanbieder*, en sindsdien niet is veranderd;
- welke inhoud van het *Dossier* wel, en welke niet, via MedMij-verkeer bij *Lezer* is geplaatst ten behoeve van welke *Zorgaanbieder*.

#### Toelichting

Hiermee is het voor de *Zorggebruiker* duidelijk op welk deel van de inhoud van zijn dossier hij de aan het MedMij Afsprakenstelsel verbonden vertrouwen kan verbinden. Het is immers goed mogelijk dat een PGO alleen op bepaalde onderdelen deelneemt, en dus voldoet, aan het MedMij Afsprakenstelsel.

3a. Desgewenst biedt *Uitgever* aan *Zorggebruiker* de use case *UC Abonneren*. Daarmee kan *Zorggebruiker* een *Abonnement op Notificaties* aangaan, verlengen, verkorten of beëindigen bij een *Zorgaanbieder*, via *Bron*. Deze *Notificaties* hebben betrekking op een *Gegevensdienst*. Bij deze use case betrokken rollen gebruiken hiertoe het betreffende [stroomdiagram](#).

#### Abonnementen

*Abonnementen* horen bij de [hoofdfunctie Regie](#).

3b. Bij elke combinatie van *Zorggebruiker*, *Uitgever*, *Zorgaanbieder* en *Gegevensdienst* hoort op elk moment maximaal één *Abonnement*.

### Abonnementen

Nieuwe verzoeken tot *Abonnementen* vervangen eventueel bestaande.

3c. Een *Uitgever* of *Bron* die de use case *UC Abonneren* aanbiedt, biedt ook de use case *UC Notificeren* aan. Bij deze use case betrokken rollen gebruiken hiertoe het betreffende [stroomdiagram](#).

### Notificaties

Deze verantwoordelijkheid introduceert de notie van een *Notificatie*. Een *Notificatie* hoort altijd bij slechts één *Abonnement*. Er zijn twee soorten *Notificaties*:

- inhoudelijke *Notificaties* brengen *Uitgever* (en mogelijk *Zorggebruiker*) op de hoogte van de beschikbaarheid van nieuwe (gezondheids)informatie van *Zorgaanbieder* bij *Bron*, betreffende een *Gegevensdienst* waarop *Zorggebruiker* bij die *Zorgaanbieder* geabonneerd is;
- abonnements-*Notificaties* brengen *Uitgever* (en mogelijk *Zorggebruiker*) op de hoogte van het door de *Zorgaanbieder*, via *Bron*, beëindigen van een *Abonnement* (zie verantwoordelijkheid 3d).

3d. Een *Bron* die de use case *UC Abonneren* ondersteunt, beëindigt een *Abonnement* wanneer:

1. het daartoe een verzoek van de *Uitgever* ontvangt;
2. de *Bron* na het sturen van een *Notificatie* ontdekt dat *Uitgever* het betreffende *Abonnement* niet kent.
3. de looptijd van het *Abonnement* is verlopen;
4. de *Zorgaanbieder* de betreffende *Gegevensdienst* niet langer aanbiedt, of wanneer de *Bron* de betreffende *Gegevensdienst* niet langer ontsluit. In deze situatie beëindigt de *Bron* onverwijld alle betreffende *Abonnementen*.

### Beëindiging van Abonnementen

Er worden geen eisen gesteld omtrent het beëindigen van een *Abonnement* ingeval (gezondheids) informatie van een *Zorggebruiker* niet langer beschikbaar is bij een *Zorgaanbieder*, bijvoorbeeld na een dossieroverdracht, of na vernietiging van het dossier. Wanneer deze situatie zich voordoet, zullen simpelweg tot de einddatum van het *Abonnement* geen inhoudelijke *Notificaties* meer worden gegenereerd.

Het zou kunnen gebeuren dat een *Authorization Client* een *Notificatie* wenst te sturen, in het kader van een lopend *Abonnement*, maar de *OAuth Client List* aangeeft dat de betreffende *OAuth Client* hetzij geen *Notificaties* meer kan ontvangen of de betreffende *Gegevensdienst* niet (meer) ondersteunt. In die gevallen wordt de *Notificatie* niet verzonden, maar blijft het *Abonnement* in beginsel wel intact. Omdat er geen *Notificaties* worden verstuurd, bestaan er geen risico's om het *Abonnement* aan te houden. Mocht de *OAuth Client List* een administratieve fout bevatten, is dat nog geen reden voor ontbinding van het *Abonnement* tussen *Persoon* en *Zorgaanbieder*, als zo'n fout hersteld zou worden, kunnen er daarna weer *Notificaties* onder hetzelfde *Abonnement* verstuurd gaan worden. Mocht een *Notification Client* een dergelijke situatie aantreffen, is er wel aanleiding

voor de betreffende *Dienstverlener zorgaanbieder* om contact op te nemen met de betreffende *Dienstverlener persoon* en, waar dan nog nodig, met de MedMij-beheerorganisatie. Zie ook verantwoordelijkheid 3e.

Het vierde punt gaat ervan uit dat de *Dienstverlener zorgaanbieder* een eigen administratie bijhoudt van welke *Gegevensdiensten* hij voor welke *Zorgaanbieders* ontsluit, en daarvoor niet leunt op de *Zorgaanbiederslijst* of andere lijsten. Zijn verwerkersrelaties met *Zorgaanbieders* zijn immers de bron van die lijsten, niet andersom. Het kan zijn dat de *Dienstverlener zorgaanbieder* een fout in die eigen administratie maakt en dan, vanwege het vierde punt, de betreffende *Abonnementen* beëindigd. Het MedMij Afsprakenstelsel voorkomt dat niet, omdat die fout moet worden gezien als een fout van de *Dienstverlener zorgaanbieder* als verwerker voor de *Zorgaanbieder*, met andere woorden, in het kader van de *Dienstverleningsovereenkomst* tussen die twee, en niet op het MedMij-koppelvlak.

3e. Een *Uitgever* die voornemens is het voeren van een zekere *Gegevensdienst* te beëindigen, of het voeren van *Abonnementen* te beëindigen, informeert daarover zijn *Zorggebruikers* en laat, voor zover mogelijk, alle hierdoor getroffen lopende *Abonnementen* beëindigen.

3f. Indien een *Bron* bij een *Zorgaanbieder* een wijziging detecteert in gezondheidsinformatie die hoort bij een *Gegevensdienst* waarop een *Persoon* bij die *Zorgaanbieder* een op dat moment geldig *Abonnement* heeft, via een *Uitgever*, voorziet die *Bron* die *Uitgever* van een zogenoemde inhoudelijke *Notificatie*, door middel van de [UC Notificeren](#).

3g. Indien een *Bron* bij een *Zorgaanbieder* een wijziging detecteert in een op dat moment geldig *Abonnement* dat een *Persoon*, via een *Uitgever*, bij die *Zorgaanbieder* is aangegaan, voorziet die *Bron* die *Uitgever* van een zogenoemde abonnements-*Notificatie*, door middel van de [UC Notificeren](#).

3h. De in verantwoordelijkheid 3d bedoelde beëindiging leidt:

- niet tot een abonnements-*Notificatie* in het eerste en tweede geval;
- wel tot een abonnements-*Notificatie* in het derde en vierde geval.

3i. Een *Abonnement* heeft een duur, gerekend in hele dagen vanaf het moment van aangaan, verlengen of verkorten.

- De *Catalogus* geeft bij elke *Gegevensdienst* de maximale duur aan van een *Abonnement* op die *Gegevensdienst*; is die maximale duur 0, dan kunnen er op die *Gegevensdienst* geen *Abonnementen* worden aangegaan.
- De *Zorgaanbieder* heeft, binnen de door de *Catalogus* aangegeven grenzen, ruimte voor eigen beleid aangaande de (maximale) duur van een *Abonnement*, gegeven de *Gegevensdienst* in kwestie. Dit wordt aangegeven in de *Zorgaanbiederslijst*.
- De *Zorgaanbieder* heeft, binnen de in de *Zorgaanbiederslijst* aangegeven grenzen, ruimte voor eigen beleid aangaande de (maximale) duur van een *Abonnement*, gegeven de *Persoon* in kwestie. Dit beleid maakt deel uit van de beschikbaarheidsvoorwaarde.
- De door een *Persoon* via zijn *Uitgever* gevraagde duur van een *Abonnement* wordt gemaximeerd op de in de vorige drie punten bedoelde maximale durven.

## Gegevensdiensten

4. *Uitgever* laat *Zorggebruiker* met een *Gegevensdienst* uit de [Gegevensdienstnamenlijst](#) gezondheidsinformatie verzamelen bij een *Bron* of, ten behoeve van een *Zorgaanbieder*, plaatsen bij een *Lezer*.

### Toelichting

Een *Gegevensdienst* is een op een specifieke en gestandaardiseerde set gezondheidsinformatie gerichte dienst waarmee *Bron* zulke informatie ontsluit naar *Uitgever* in het kader van de *UC Verzamelen* of *Lezer* zulke informatie geplaatst krijgt ten behoeve van een *Zorgaanbieder*. In de [Gegevensdienstnamenlijst](#) zijn de *Gegevensdiensten* opgenomen die op enig moment worden aangeboden, maar de *Catalogus* is de autoriteit daarvoor.

5. Elke *Bron* ontsluit op elk moment minstens één *Gegevensdienst*. Elke *Lezer* ontsluit op elk moment minstens één *Gegevensdienst*.

#### Toelichting

Het ontsluiten van een *Gegevensdienst* is, in deze versie van het MedMij Afsprakenstelsel, hetzij het door een *Bron* bij zich laten verzamelen of het door een *Lezer* met zich laten delen van zekere gezondheidsinformatie. De term 'ontsluiten' wordt hier gebruikt in plaats van de term 'aanbieden', omdat als aanbieder van een *Gegevensdienst* de *Zorgaanbieder* wordt gezien, niet de *Deelnemer* (*Bron* of *Lezer*). De *Deelnemer* ontsluit de *Gegevensdienst* dus namens de *Zorgaanbieder* die die *Gegevensdienst* aanbiedt.

De termen 'aanbieden' en 'ontsluiten' vertegenwoordigen een tweedeling in de verantwoordelijkheid voor een geleverde *Gegevensdienst*. De *Zorgaanbieder* is, ook als verwerkingsverantwoordelijke in de zin der AVG, verantwoordelijk voor het aanbieden van een *Gegevensdienst* aan de *Uitgever*; de *Dienstverlener zorgaanbieder* is, ook als verwerker in de zin der AVG, verantwoordelijk voor het ontsluiten van diezelfde *Gegevensdienst* aan diezelfde *Uitgever*. Aanbieden en ontsluiten zijn dus niet achter elkaar geschakeld: de *Zorgaanbieder* biedt de *Gegevensdienst* niet zozeer aan de *Bron/Lezer* aan, maar aan de *Uitgever*. Aanbieden en ontsluiten zijn aspecten van eenzelfde geleverde *Gegevensdienst*: het eerste het verwerkingsverantwoordelijke, het tweede het verwerkende.

6. *MedMij Beheer* zal alleen in de *Zorgaanbiederslijst* opnemen dat een zekere *Gegevensdienst* door een zekere *Zorgaanbieder* via een zekere *Bron*, respectievelijk *Lezer*, wordt aangeboden, indien zij (*Stichting MedMij*) heeft vastgesteld dat de *Dienstverlener zorgaanbieder* die daarbij de *Bron*, respectievelijk *Lezer*, is, voldoet aan de specifiek op die *Gegevensdienst* toepas-selij-ke eisen.

#### Toelichting

Omdat er een indirectie speelt, via de *Dienstverlener zorgaanbieder* naar de *Zorgaanbieder*, moet gezegd worden dat één *Zorgaanbieder* genoeg is (die een bepaalde *Gegevensdienst* ontsluit) om ervoor te zorgen dat de *Dienstverlener zorgaanbieder* zich voor die *Informatiestandaard* moet kwalificeren in het MedMij Afsprakenstelsel.

7a. Voor elke *Gegevensdienst* waarvan de *Zorgaanbiederslijst* aan-geeft dat een zekere *Zorgaanbieder* deze aanbiedt, zal *Bron*, respectievelijk *Lezer*, ervoor zorgdragen dat die *Gegevensdienst* ook geleverd wordt. Daarbij wordt geen enkel onderscheid gemaakt tussen *Uitgevers*, tenzij het MedMij Afsprakenstelsel daartoe uitdrukkelijk verplicht. Dit geldt ook voor de mogelijke andere *Gegevensdienst(en)* die in de [Catalogus](#) staan genoemd als *Vereist* bij eerstgenoemde *Gegevensdienst*.

#### Toelichting

Net als verantwoordelijkheid 6, moet verantwoordelijkheid 7a rekening houden met de indirectie via *Dienstverlener zorgaanbieder* naar de *Zorgaanbieder* zelf. Deze regel legt het bij de *Dienstverlener*

*zorgaanbieder* om ervoor zorg te dragen dat de *Zorgaanbieder* met wie hij een dienstverleningsovereenkomst heeft, ook de *Gegevensdienst* levert die hij toegezegd heeft.

7b. Het is verantwoordelijkheid 7a bepaalde is ook van toepassing zolang de geldigheid van de toepasselijke vermelding in de *Zorgaanbiederslijst* niet langer dan één uur (3600 seconden) geleden is verstreken.

#### Toelichting

Zo wordt ervoor ruimte geboden dat na-ijlende sessies, die nog gebruik maken van de verstrijkende versie van de *Zorgaanbiederslijst*, nog kunnen worden afgemaakt.

### Autorisatie

8a. *Bron* vergewist zich ervan, elke keer opnieuw voordat hij *Zorggebruiker* gezondheidsinformatie van *Zorgaanbieder* laat verzamelen door middel van [UC Verzamelen](#), dat deze *Zorggebruiker* uitdrukkelijk *Toestemming* heeft gegeven aan *Zorgaanbieder* om de in de *Gegevensdienst* betrokken gezondheidsinformatie aan *Uitgever* ter beschikking te laten stellen. De vraag om *Toestemming* heeft een vaste formulering, die is opgenomen in de [UC Verzamelen](#). Deze *Toestemming* is slechts van kracht binnen deze doorloping van de use case.

#### Toelichting

Het is dus de *Bron* die de *Toestemming* ophaalt bij de *Zorggebruiker*. De tweede zin van deze verantwoordelijkheid maakt de toestemming functioneel zo eenvoudig mogelijk, omdat in deze release van het MedMij Afsprakenstelsel alleen met een eenmalige vraag gezondheidsinformatie verzameld kan worden. De toestemming, hoe expliciet ook, heeft precies dezelfde reikwijdte als die eenmalige vraag.

8b. *Lezer* vergewist zich ervan, elke keer opnieuw voordat hij *Zorggebruiker* gezondheidsinformatie ten behoeve van *Zorgaanbieder* laat plaatsen, dat deze *Zorggebruiker* uitdrukkelijk heeft bevestigd om de in de *Gegevensdienst* betrokken gezondheidsinformatie aan *Zorgaanbieder* ter beschikking te willen stellen. De vraag om *Bevestiging* heeft een vaste formulering, die is opgenomen in de [UC Delen](#). Deze bevestiging geldt niet buiten deze doorloping van de *UC Delen*.

#### Toelichting

Deze verantwoordelijkheid is welbewust niet geïntegreerd met verantwoordelijkheid 8a omdat de hier bedoelde bevestiging niet de juridische status heeft van de in verantwoordelijkheid 8a bedoelde *Toestemming*.

8c. *Bron* vergewist zich ervan, elke keer opnieuw voordat hij *Zorggebruiker* een *Abonnement* met *Zorgaanbieder* laat aangaan, dat deze *Zorggebruiker* uitdrukkelijk *Toestemming* heeft gegeven aan *Zorgaanbieder* om *Notificaties*, betreffende de in de *Gegevensdienst* betrokken (gezondheids)informatie, aan *Uitgever* ter beschikking te laten stellen. De vraag om *Toestemming* heeft een vaste formulering, die is opgenomen in de [UC Abonneren](#).

#### Toelichting

*Bron* handelt dus ook bij het beschikbaar kunnen stellen van *Notificaties* conform een *Toestemming* van de *Zorggebruiker*. Deze *Toestemming* wordt gegeven bij het aangaan van het *Abonnement* en blijft geldig voor de duur van het *Abonnement*.

## Authenticatie

9. *Bron* en *Lezer* dragen ervoor zorg dat de onder 7 bedoelde opvolging, en de onder 8a, 8b en 8c bedoelde vraag om *Toestemming*, respectievelijk bevestiging, slechts plaatsvinden wanneer hij de identiteit van de *Zorggebruiker* met passende zekerheid heeft vastgesteld.

### Toelichting

Op de *Applicatie*-laag wordt beschreven dat de identiteit van de *Zorggebruiker* uitgedrukt wordt door een BSN.

## Lijsten

### Vier lijsten

In het MedMij Afsprakenstelsel worden, ten behoeven van de hoofdfunctie *Coördinatie*, vier lijsten gebruikt voor de interoperabiliteit en het vertrouwen tussen het Persoonsdomein en het Zorgaanbiedersdomein.

lijst	afkorting	wordt opgehaald en gebruikt door	informatie-inhoud	
		<i>Uitgever</i>	<i>Bron/ Lezer</i>	
<i>Zorgaanbiederslijst</i>	ZAL	X		welke <i>Zorgaanbieders</i> welke <i>Gegevensdiensten</i> aanbieden, en eventueel ook <i>Abonnementen</i> daarop, en op welke adressen zij die laten laten ontsluiten, gegeven een zekere <i>Interfaceversie</i>
<i>OAuth Client List</i>	OCL		X	de namen van PGO's, welke <i>Gegevensdiensten</i> zij mogen gebruiken en naar welke adressen mogelijk <i>Notificaties</i> in het kader van <i>Abonnementen</i> op die <i>Gegevensdiensten</i> kunnen worden gestuurd, gegeven een zekere <i>Interfaceversie</i>
<i>Gegevensdienstnamenlijst</i>	GNL	X	X	de gebruiksvriendelijke namen van <i>Gegevensdiensten</i>
<i>Whitelist</i>	WHL	X	X	welke <i>Nodes</i> actief mogen zijn op het MedMij-netwerk

### Zorgaanbiederslijst



10. *MedMij Beheer* beheert en publiceert een *Zorgaanbiederslijst*, namens de deelnemende *Dienstverleners zorgaanbieder*. De gepubliceerde *Zorgaanbiederslijst* bevat steeds en slechts alle actuele entrees, en beschrijft van elke *Zorgaanbieder*:

- welke *Gegevensdiensten* deze momenteel aanbiedt via welke *Bron* en *Lezer*, en welke technische adressen daarvoor moeten worden aangesproken bij de *Dienstverlener zorgaanbieder*, gegeven een zekere *Interfaceversie*;
- voor welke *Gegevensdiensten* het mogelijk is om *Abonnementen* aan te gaan en via welke technische adressen dit kan worden gedaan, gegeven een zekere *Interfaceversie*. In deze release van het MedMij Afsprakenstelsel staat de *Catalogus* alleen *Abonnementen* toe op *Gegevensdiensten* die zijn gebaseerd op de [UC Verzamelen](#).

#### Toelichting

Deze afspraak wijst *MedMij Beheer* de verantwoordelijkheid toe om ten behoeve van alle *Dienstverleners persoon* een lijst te verspreiden van *Zorgaanbieders* en de door hen aangeboden *Gegevensdiensten* en *Abonnementen*. Zonder deze functie zou het stelsel niet functioneren.

In de *Catalogus* staat bij elke *Gegevensdienst* de maximale duur van een *Abonnement* op ( *Notificaties* van) die *Gegevensdienst*. Bij een *Gegevensdienst* gebaseerd op [UC Delen](#) zal hier vooralsnog altijd 0 als maximale duur staan, hetgeen betekent dat er geen *Abonnementen* mogelijk zijn op deze *Gegevensdienst*.

11. De *Zorgaanbiederslijst* voldoet aan wat over haar is bepaald in de [Informatiemodellen](#).

12. *MedMij Beheer* beheert en publiceert, in de *Zorgaanbiederslijst*, unieke en gebruikersvriendelijke namen van *Zorgaanbieders*, van het formaat <zorgaanbieder>@medmij. Daarop is [naamgevingsbeleid](#) van toepassing.

#### Toelichting

*Zorgaanbieders* kunnen in hun directe of indirecte contact met *Zorggebruikers* deze naam meegeven als hun "MedMij-naam". *MedMij Beheer* zorgt voor uniciteit en heeft het laatste woord bij het vaststellen ervan.

13. *MedMij Beheer* biedt aan *Uitgever* een use case (*UC Opvragen ZAL*) om de actuele versie van die *Zorgaanbiederslijst* op te vragen. Betrokken rollen gebruiken hiertoe het betreffende [stroomdiagram](#).

### OAuth Client List

14a. *MedMij Beheer* beheert en publiceert een actuele *OAuth Client List*, namens de deelnemende *Dienstverleners persoon*. De gepubliceerde *OAuth Client List* bevat steeds en slechts alle actuele entrees, en beschrijft van elke *OAuth Client*:

- wat de gebruikersvriendelijke namen zijn die voor de *Dienstverleners persoon* worden gebruikt in de [Toestemmingsverklaring](#), de [Bevestigingsverklaring](#) en de [Notificatie van Zorggebruiker](#);
- op welke *Gegevensdiensten* de *Dienstverlener persoon* het ontvangen van *Notificaties*, in het kader van een *Abonnement*, ondersteunt en op welke technische adressen deze *Notificaties* moeten worden afgeleverd, gegeven een zekere *Interfaceversie*. In deze release van het MedMij Afsprakenstelsel kunnen slechts *Abonnementen* worden aangegaan op *Gegevensdiensten* die zijn gebaseerd op de *UC Verzamelen*.

#### Toelichting

De *OAuth Client List* bevat dus geen namen voor *Dienstverleners zorgaanbieder*. Dat is niet nodig, omdat deze niet voorkomen in de [Toestemmingsverklaring](#).

14b. De *OAuth Client List* voldoet aan wat over haar is bepaald in de [Informatiemodellen](#).

15. *MedMij Beheer* biedt aan *Bron* een use case (*UC Opvragen OCL*) om de actuele versie van die *OAuth Client List* op te vragen. Betrokken rollen gebruiken hiertoe het betreffende [stroomdiagram](#).

#### Gegevensdienstnamenlijst

16. *MedMij Beheer* beheert en publiceert de *Gegevensdienstnamenlijst*. Deze beschrijft welke gebruikersvriendelijke namen horen bij welke *Gegevensdiensten*. De *Gegevensdienstnamenlijst* voldoet aan wat over haar is bepaald in de [Informatiemodellen](#).

17. *MedMij Beheer* biedt aan *Uitgever*, *Bron* en *Lezer* een use case (*UC Opvragen GNL*) om de actuele versie van die *Gegevensdienstnamenlijst* op te vragen. Betrokken rollen gebruiken hiertoe het betreffende [stroomdiagram](#).

#### Whitelist

18. *MedMij Beheer* beheert en publiceert een actuele *Whitelist*, namens de deelnemende *Dienstverleners zorgaanbieder* en *Dienstverleners persoon*. De *Whitelist* beschrijft welke *Nodes* in MedMij-verkeer mogen deelnemen. De *Whitelist* voldoet aan wat over haar is bepaald in de [Informatiemodellen](#).

#### Toelichting

Er bestaat op deze laag geen use case voor het opvragen van de *Whitelist*. De *Whitelist* wordt alleen gebruikt op de [Netwerk](#)-laag. Op die laag is er wel een use case-implementatie voor dit doel.

#### Logging en portabiliteit

19a. *Uitgever* zal het *Dossier* zo inrichten dat deze ook dienst kan doen als logbestand, zoals bedoeld in de [AVG](#) en [NEN 7513:2018](#), van de door enige *Zorggebruiker* bij enige *Bron* verzamelde persoonsgegevens en door enige *Zorggebruiker* bij enige *Lezer* geplaatste persoonsgegevens.

#### Toelichting

Met de logging wordt beoogd een betrouwbaar overzicht te kunnen leveren van de gebeurtenissen waarbij gezondheidsinformatie over een persoon zijn verwerkt. Die gebeurtenissen kunnen zich over verschillende plaatsen en tijden uitstrekken. Het beoogde overzicht is dus alleen mogelijk als de loggegevens uit verschillende bronnen kunnen worden gecombineerd. Ook zonder direct een virtueel wereldwijd en levenslang patiëntdossier als doel te stellen is duidelijk dat gestandaardiseerde logging een voorwaarde is om het overzicht voor de betreffende *Persoon* mogelijk te maken.

Op 18 mei 2018 is een revisie verschenen van de 2010-versie van NEN 7513. Deze norm, met het nummer [NEN 7513:2018](#), is onderdeel van het [Normenkader informatiebeveiliging](#) van het MedMij Afsprakenstelsel. In hoofdstuk 5 van de gereviseerde norm staan de informatiebehoeften, zowel de algemene als die vanuit het specifieke perspectief van cliënten, zorginstellingen en toezichthouders. Hoofdstuk 6 vertaalt deze behoeften naar een overzicht van te loggen gebeurtenissen en hoofdstuk 7 biedt een model van de te loggen gegevens. De voorgaande versie ([NEN 7513:2010](#)) is ingetrokken. De term *NEN 7513* in het [Besluit elektronische gegevensverwerking door zorgaanbieders](#) wordt daarom geacht naar de 2018-versie te verwijzen.



19b. *Uitgever* zal het *Dossier* zo inrichten dat deze ook dienst kan doen als logbestand van ontvangen *Notificaties* en *aangegeane Abonnementen*. *Bron* zal een logbestand bijhouden van verzonden *Notificaties* en *aangegeane Abonnementen*.

19c. De bewaartermijn van de logbestanden is ten minste 24 maanden en niet meer dan 36 maanden. Na de bewaartermijn van de logbestanden moeten deze vernietigd worden.

#### Toelichting

Het maximum van de bewaartermijn is bepaald voor logging binnen de scope van MedMij-verkeer ter voorkoming van onnodige opslag van gegevens en ter bescherming van de privacy van de gebruiker. Deze minimale en maximale bewaartermijnen van logbestanden passen binnen de uitersten die daartoe door NEN7513 (paragraaf 8.5) zijn bepaald.

20. *MedMij Beheer* onderhoudt een archief van alle ooit verspreide versies van de *Zorgaanbiederslijst*, de *OAuth Client List*, de *Whitelist* en de *Gegevensdienstnamenlijst*. De bewaartermijn, gerekend vanaf het einde van de geldigheid van de betreffende versie, is niet korter dan die van de logbestanden als bedoeld in verantwoordelijkheid 19.

21a. *Uitgever* biedt *Zorggebruiker* de use case *UC Portabiliteitsrapport*. Daarmee kan *Zorggebruiker* geautomatiseerd een lijst exporteren, genaamd het *Portabiliteitsrapport*, van alle keren, gedurende een zekere periode, dat *Zorggebruiker* deze *Uitgever* bij een *Zorgaanbieder* gezondheidsinformatie volgens een zekere *Gegevensdienst* heeft verzameld.

21b. *Uitgever* biedt *Zorggebruiker* pro-actief de export van een *Portabiliteitsrapport* aan:

- voordat *Uitgever*, om welke reden dan ook, haar dienstverlening aan *Zorggebruiker* staakt;
- voordat *Uitgever* de logbestanden zou verwijderen waaruit zij *Portabiliteitsrapporten* voor *Zorggebruiker* over een zekere periode zou samenstellen.

21c. *Uitgever* beperkt *Zorggebruiker* niet in het gebruik van de *Portabiliteitsrapport* in de relatie van *Zorggebruiker* met mogelijke andere en/of latere *Uitgevers*.

21d. Het *Portabiliteitsrapport* voldoet aan hetgeen daarover bepaald is in de [Informatiemodellen](#) en heeft de technische vorm van een XML-document, dat voldoet aan het XML-schema dat op de pagina [XML-schema's](#) te vinden is.

#### Portabiliteitsrapport

Met het *Portabiliteitsrapport* krijgt *Zorggebruiker* een middel in handen om een belangrijk deel van de gezondheidsinformatie die hij in het *Dossier* in zijn PGO heeft verzameld, naar believen ook in andere PGO's onder te brengen (portabiliteit, overdraagbaarheid). Ook dat draagt bij aan de [Regie](#) van de *Zorggebruiker* over zijn gezondheidsinformatie, aan zijn voortdurend vrije keuze tussen *Dienstverlener persoon* ([principe 7](#)) en aan het beperken van het nadeel dat hij zou ondervinden wanneer zijn *Dienstverlener persoon* haar activiteiten zou staken.

Er is geen garantie dat een *Portabiliteitsrapport* geautomatiseerd door een andere PGO dan die het rapport heeft gemaakt zou kunnen worden 'afgespeeld', al is het maar doordat niet alle gebruikte *Gegevensdiensten* nog als geldig in de *Catalogus* hoeven te staan. Het *Portabiliteitsrapport* geeft in dat soort gevallen nog steeds precieze en menselijkerwijs enigszins leesbare informatie waarmee de nieuwe PGO alsnog, desnoods, handmatig gevuld kan worden.

*Dienstverleners* *persoon* kunnen hun dienstverlening aan *Zorggebruikers* kracht bij zetten door een importfunctie voor *Portabiliteitsrapporten* aan te bieden. Dit is echter niet verplicht en moet gezien worden in het licht van [principe 3](#).

Een zwaarder middel voor portabiliteit zou een uitwisselstandaard tussen PGO's zijn. Dit zou echter een flinke complexiteit en kosten met zich meebrengen, niet in het minst doordat het rekening zou moeten houden met alle voormalige versies van het MedMij Afsprakenstelsel en met *Gegevensdiensten* die ondertussen niet meer als geldig in de *Catalogus* staan.

## UC Verzamelen

### Toelichting

In de platen hieronder staat het stroomdiagram van de use case *Verzamelen*, in vier perspectieven:

- het totaalperspectief;
- het perspectief van de *Uitgever*, die onder de hoede van de *Dienstverlener persoon* valt. Laatstgenoemde kan deze plaat lezen als zijn verplichte aandeel in de use case *Verzamelen*;
- het perspectief van de *Bron*, die onder de hoede van de *Dienstverlener zorgaanbieder* valt. Laatstgenoemde kan deze plaat lezen als zijn verplichte aandeel in de use case *Verzamelen*;
- het perspectief van de *Zorggebruiker*.

De stroomdiagrammen tonen allereerst de situatie waarin alle acties slagen tot en met het uiteindelijke verzamelen van de gezondheidsinformatie (de zogenaamde happy flow). De twee oranje banen horen, conform de MedMij-huisstijl, tot het Persoonsdomein, de blauwe tot het Zorgaanbiedersdomein. Menige actie in de stroomdiagrammen is gekleurd weergegeven. De lichtgrijs gekleurde acties vormen samen de autorisatieflow; de zachtgeel gekleurde acties vormen samen de authenticatieflow. In de stroomdiagrammen voor de specifieke perspectieven hebben alleen de acties in de bij dat perspectief horende baan namen. De acties in de andere banen zijn gecompriemd en anoniem weergegeven.

Tot slot bespreken we de uitzonderingen op de happy flow. Daarbij werken we alleen vanuit het totaalperspectief.

## Totaalperspectief (happy flow)

### Toelichting

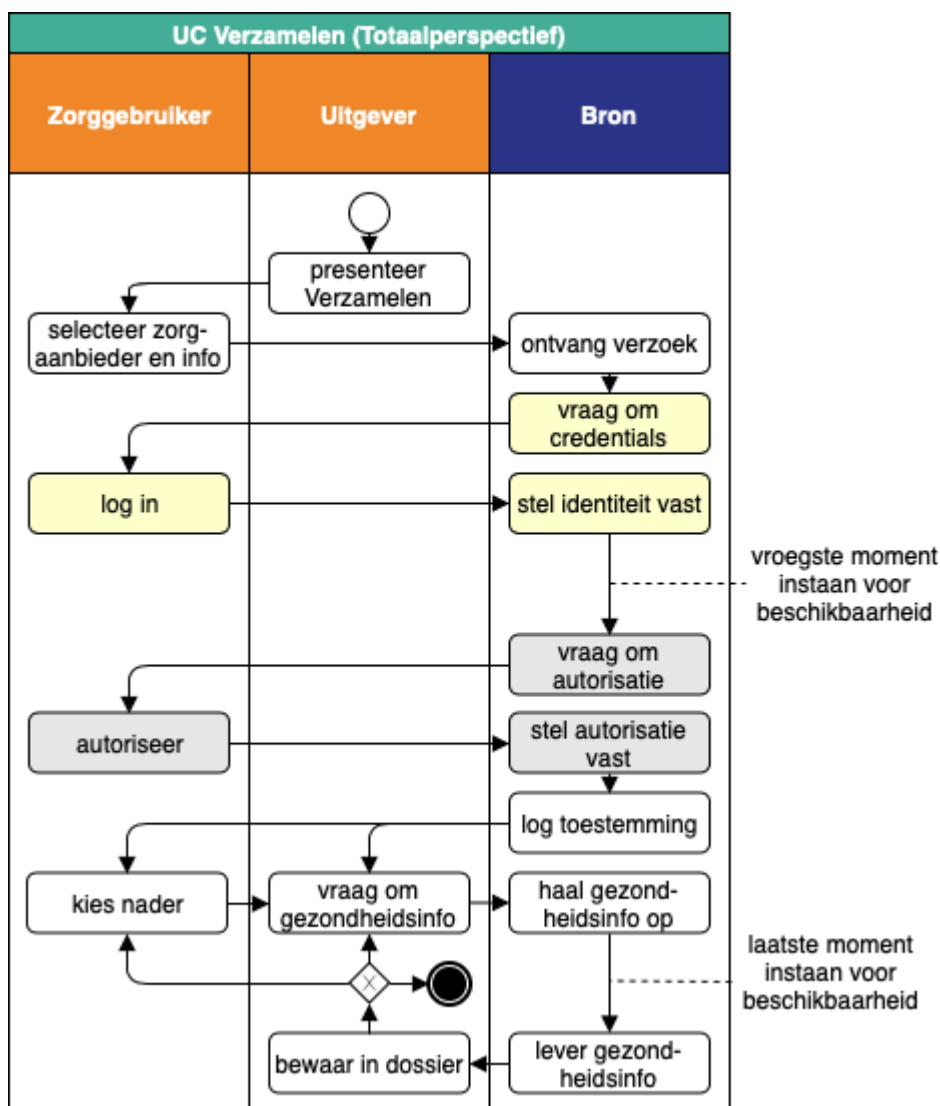
In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

De totale procesgang van de *UC Verzamelen* kent de volgende stappen:

- De *Uitgever* presenteert aan de *Zorggebruiker* de mogelijkheid om te verzamelen.
- De *Zorggebruiker* kiest expliciet de zorgaanbieder waarbij hij de informatie wenst te verzamelen en de specifieke *Gegevensdienst*. Daarvoor kunnen desgewenst de *Gegevensdienstnamen* worden gebruikt uit de *Gegevensdienstnamenlijst*. Het verzoek gaat naar de passende *Bron*.
- De *Bron* laat de *Zorggebruiker* zich authenticeren.
- Dan breekt het moment aan waarop de *Bron* op zijn vroegst ervoor instaat dat de *Zorgaanbieder* voor de betreffende *Gegevensdienst* überhaupt gezondheidsinformatie van die *Persoon* beschikbaar heeft, of anderszins de happy flow afbreekt. Het MedMij Afsprakenstelsel adviseert de beschikbaarheidsvoorwaarde op het vroegst aangegeven moment van kracht te laten zijn. In deze release staat het MedMij Afsprakenstelsel het toe die voorwaarde op een later moment van kracht te laten zijn, maar niet later dan het laatste in het figuur aangegeven moment.
- De *Bron* vraagt aan de *Zorggebruiker* of hij toestemming geeft tot het verstrekken van de gevraagde informatie aan de *Uitgever*. Deze vraag staat op de pagina [Toestemmingsverklaring](#).
- De *Bron* logt die toestemming en laat de *Uitgever* weten dat de toestemming gegeven is.
- Nu kan de *Uitgever* de *Bron* vragen om de gezondheidsinformatie.

- Uiterlijk na de ontvangst van het verzoek zal de *Bron* ervoor instaan dat de *Zorgaanbieder* voor de betreffende *Gegevensdienst* überhaupt gezondheidsinformatie van die *Persoon* beschikbaar heeft, of anders de happy flow afbreken.
- Bij ontvangst slaat de *Uitgever* die informatie op in het persoonlijke dossier.
- Mocht de *Gegevensdienst* waartoe de *Zorggebruiker* heeft geautoriseerd uit meerdere *Transacties* bestaan (zie hiervoor de [Catalogus](#)), bevraagt de *Uitgever* de *Bron* daarna mogelijk opnieuw voor de nog resterende *Transacties*, eventueel na nieuwe interactie met de *Zorggebruiker*.
- Bij de informatie wordt ook de meta-informatie opgeslagen die wordt bedoeld in verantwoordelijkheid 19 van de [Processen- en Informatielaag](#).

De beschikbaarheidsvoorwaarde hoort bij *Regie*, niet bij *Uitwisseling*. De voorwaarde geeft de *Zorgaanbieder* ruimte om deel te nemen in aan de *Persoon* gegeven *Regie*. Omdat echter bestaande implementatie-architecturen veelal uitwisseling centraal zetten, en niet *Regie*, hebben zij moeite de beschikbaarheidsvoorwaarde in de regiefase te implementeren. Daarom biedt het MedMij Afsprakenstelsel vooralsnog de gelegenheid om deze in de uitwisselingsfase te implementeren.



## Uitzonderingen (Totaalperspectief)

### Toelichting

In onderstaande tabel staan de uitzonderingssituaties beschreven. Alle worden door de *Bron* ontdekt. Om te voorkomen dat de *Uitgever* informatie over het bestaan van behandelrelaties verkrijgt zonder dat daarvoor (al) toestemming is gegeven, moet het onderscheid tussen de uitzonderingen 2, 3 en 4 niet te maken zijn door de *Uitgever*.

Op de Applicatielaag zullen, bij de [use case-implementatie Verzamelen](#), deze uitzonderingen opnieuw ter sprake komen, maar nu ook met hun precieze implementatie en formaat van de foutmeldingen.

Of de *Zorgaanbieder* de gevraagde gezondheidsinformatie beschikbaar stelt aan de *Persoon*, is om te beginnen een zaak tussen de *Zorgaanbieder* en *Persoon*, die daarvoor een behandelrelatie moeten hebben. Gegeven zo'n behandelrelatie is er wetgeving van toepassing op deze ter beschikkingstelling (zie [Juridisch kader](#)). Daarbinnen is eigen beslisruimte voor de *Zorgaanbieder*. Omdat *Zorgaanbieder* en *Persoon* evenwel geen *Deelnemers* in het MedMij Afsprakenstelsel zijn, specificeert het MedMij Afsprakenstelsel niet de exacte logica van de beslissing om de gezondheidsinformatie al dan niet ter beschikking te stellen. Om privacy-redenen vereist het MedMij Afsprakenstelsel echter wel dat er een behandelrelatie moet (hebben) bestaan waarbij de betreffende gezondheidsinformatie hoort én dat de *Persoon* minstens zestien jaar oud is (zie uitzondering UC Verzamelen 3).

Voor het verstrekken van gegevens aan een minder dan zestienjarige moet toestemming of een machtiging tot toestemming worden verleend door degene die de ouderlijke verantwoordelijkheid of de wettelijke verantwoordelijkheid voor de minder dan zestienjarige draagt. Omdat in dergelijke toestemmingen of machtigingen nog niet is voorzien in deze versie van het MedMij afsprakenstelsel, kan deze controle vooralsnog als onderdeel van de beschikbaarheidsvoorwaarde worden opgevat. Wanneer een toekomstige release van het MedMij afsprakenstelsel wel zulke toestemmingen of machtigingen omvat, zal de leeftijdsvoorwaarde gescheiden moeten worden van de beschikbaarheidsvoorwaarde.

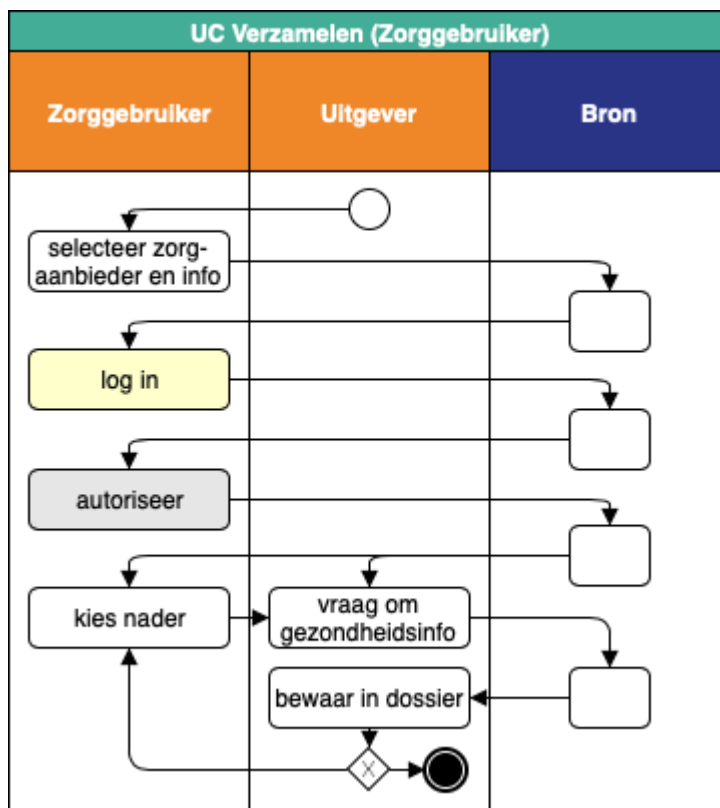
nr.	uitzondering	actie	vervolg
UC Verzamelen 1	<i>Bron</i> vindt het ontvangen verzoek ongeldig.	<i>Bron</i> informeert <i>Uitgever</i> over deze uitzondering. <i>Uitgever</i> informeert daarop <i>Zorggebruiker</i> hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Verzamelen 2	<i>Bron</i> kan de identiteit van de <i>Zorggebruiker</i> niet vaststellen.	<i>Bron</i> informeert <i>Uitgever</i> dat verzoek niet wordt ingewilligd.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Verzamelen 3	<i>Bron</i> stelt op enig moment vast dat van <i>Persoon</i> bij <i>Zorgaanbieder</i> geen gezondheidsinformatie voor die <i>Gegevensdienst</i> beschikbaar is. Hiervan is in elk geval sprake indien hetzij:		

	<ul style="list-style-type: none"> <li>er geen behandelrelatie is aan te wijzen als grondslag voor het verzamelen;</li> <li><i>Zorggebruiker</i> nog geen zestien jaar oud is.</li> </ul> <p>Zie de toelichting op <a href="#">Beschikbaarheids- en ontvankelijkheidsvoorwaarde</a>.</p>		
UC Verzamelen 4	De voorgelegde <a href="#">Toestemmingsverklaring</a> wordt niet afgegeven.		
UC Verzamelen 5	<i>Bron</i> kan het antwoord op de toestemmingsvraag niet vaststellen.	<i>Bron</i> informeert <i>Uitgever</i> over deze uitzondering. <i>Uitgever</i> informeert daarop <i>Zorggebruiker</i> hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Verzamelen 6	<i>Bron</i> kan, zelfs na toestemming, de gezondheidsinformatie alsnog niet ter beschikking stellen aan de <i>Uitgever</i> .	<i>Bron</i> informeert <i>Uitgever</i> over deze uitzondering. <i>Uitgever</i> informeert daarop <i>Zorggebruiker</i> hierover, met opgave van oorzaak.	Mocht de gezondheidsinformatie deels wel (geautoriseerd) ter beschikking staan, dan kan de flow dat nog verzorgen.

## Perspectief van de Zorggebruiker (happy flow)

### Toelichting

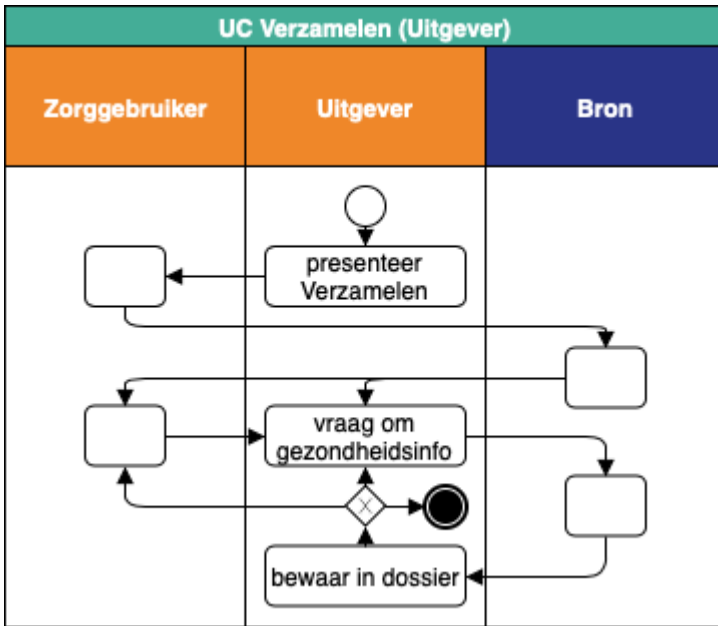
De *Zorggebruiker* moet drie stappen doorlopen: selectie van *Zorgaanbieder* en *Gegevensdienst*, inloggen en autoriseren. Als alles slaagt, slaat de *Uitgever* voor hem zowel de toestemming als de verkregen gezondheidsinformatie op.



## Perspectief van de Uitgever (happy flow)

### Toelichting

De *Uitgever* start de use case door aan de *Zorggebruiker* de mogelijkheid tot verzamelen te presenteren. Van de *Bron* krijgt hij na enige tijd het bericht dat de toestemming daarvoor is verleend, waarna hij die toestemming logt en de gezondheidsinformatie ophaalt bij de *Bron*, en opslaat.

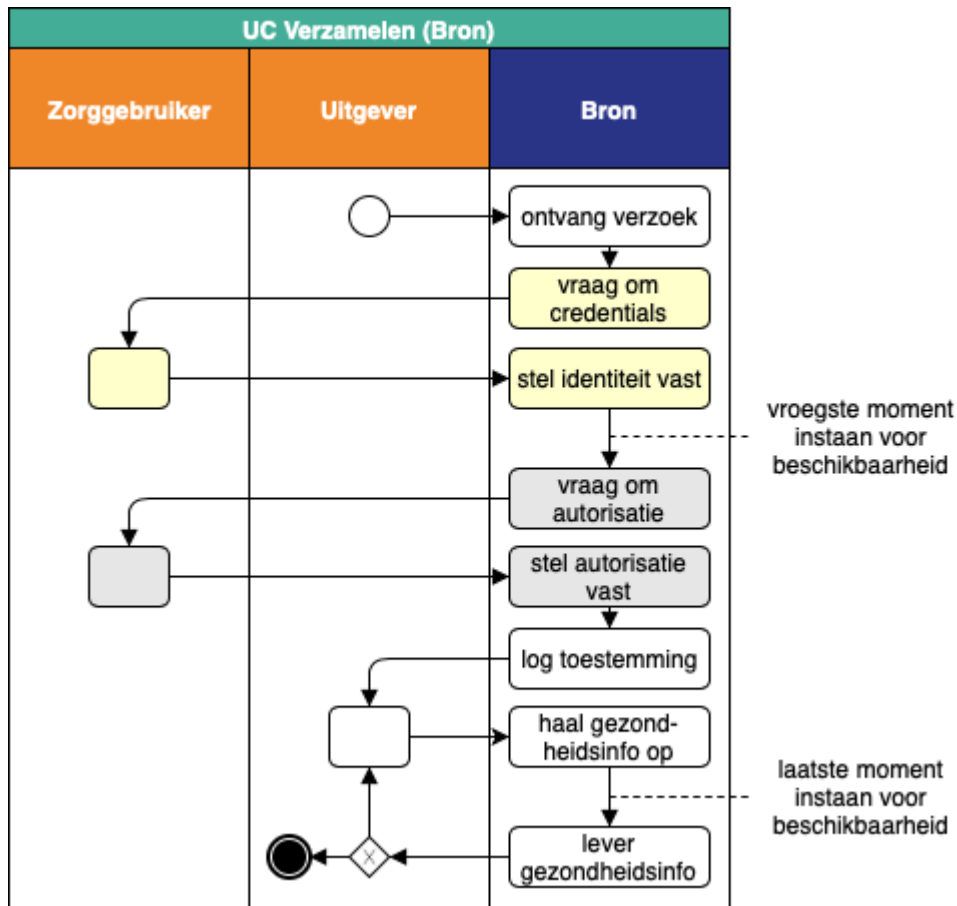


## Perspectief van de Bron (happy flow)

## Toelichting

De *Bron* regisseert, na ontvangst van het verzoek tot verzamelen, de authenticatie en de toestemming. Als die geslaagd zijn logt hij de toestemming en stuurt deze naar de *Uitgever*. Die zal uiteindelijk de bevraging terugsturen en het antwoord in ontvangst nemen.





## UC Delen

### Toelichting

Op deze pagina staan de stroomdiagrammen van de *UC Delen*. De use case is een spiegelbeeld van *UC Verzamelen*. Die spiegeling betekent echter niet dat de rollen van *Uitgever* en *Bron* nu omgekeerd worden belegd, dat wil zeggen bij respectievelijk *Dienstverlener zorgaanbieder* en *Dienstverlener persoon*. Een dergelijke omdraaiing zou een zwakkere, meer proces-logistiek-georiënteerde regievorm verraden en het initiatief bij de *Dienstverlener Persoon*, en dus bij de *Zorggebruiker*, wegnemen. Het MedMij Afsprakenstelsel ondersteunt een sterkere regievorm, waarbij ook in de *UC Delen* het initiatief bij de *Uitgever* ligt. In plaats van met een *Bron* vanwaar de *Uitgever* gezondheidsinformatie betreft, heeft hij nu echter te maken met een *Lezer* waaraan hij zulke informatie ter beschikking stelt. Net zoals de *Bron*-rol in *UC Verzamelen*, is de *Lezer*-rol in deze versie van het MedMij Afsprakenstelsel enkel nog verbonden aan de juridische rol van *Dienstverlener zorgaanbieder*.

Een tweede voordeel van deze keuze is dat de *UC Delen* in hoge mate dezelfde opzet kent als de *UC Verzamelen*. Dat geldt dientengevolge ook voor de respectievelijke use case-implementaties, die dus veel van elkaar kunnen hergebruiken. Dat laat onverlet dat er een aantal wezenlijke verschillen zijn. Op het niveau van *Processen en Informatie* zijn dat de volgende.

- Voor de start van de use case zou de *Zorggebruiker* moeten kunnen volstaan met het aanwijzen van die informatie in zijn *Dossier* die hij zou willen delen met een nader te benoemen *Zorgaanbieder*, en er daarbij vanuit mogen gaan dat de *Uitgever* daarbij weet welke *Gegevensdienst* daarbij aan de orde is.
- In tegenstelling tot in *UC Verzamelen* moet *Zorgaanbieder* in de gelegenheid worden gesteld om zich al dan niet open te stellen voor ontvangst van de betreffende informatie. De *Lezer* moet na authenticatie van de *Zorggebruiker* kunnen bepalen of de betreffende informatie welkom is bij de betreffende *Zorgaanbieder*. Deze controle op de ontvankelijkheid zal geautomatiseerd plaatsvinden, met het oog op de synchrone gebruikservaring, maar de wijze van implementatie wordt vrijgelaten.
- Juridisch gezien is er geen expliciete toestemming van de *Zorggebruiker* vereist aan de *Zorgaanbieder* voor het mogen ontvangen van de gezondheidsinformatie; die volgt uit de verstrekking door de *Zorggebruiker*. Er zijn wel toestemmingsvereisten in de relatie *Zorggebruiker-Uitgever* (inzake het mogen verstrekken van de gezondheidsinformatie), maar daarop ziet reguliere wet- en regelgeving toe. Niettemin wordt er, net als in *UC Verzamelen*, om een bevestiging gevraagd van de *Zorggebruiker*.
- Aan het eind van de use case wordt, indien de *Zorgaanbieder* ervoor ontvankelijk bleek, de betreffende informatie door de *Uitgever* geplaatst bij de *Zorgaanbieder*, via de *Lezer*. Net zoals in de *UC Verzamelen* geen nadere eisen worden gesteld aan hoe het ophalen van de informatie door de *Bron* bij de *Zorgaanbieder* geschiedt, geldt dat in de *UC Delen* ook voor de plaatsing. Van belang is slechts dat de *Zorggebruiker* ervan kan uitgaan dat de *Zorgaanbieder* kennis kan hebben genomen van de betreffende informatie. Hoe dat wordt geborgd is niet triviaal, maar wordt gelaten aan de voorzieningen die de *Dienstverlener zorgaanbieder* treft en de *Dienstverleningsovereenkomst* die hij dienaangaande aangaat met de *Zorgaanbieder*.

In de platen hieronder staat het stroomdiagram van de use case *Delen*, in vier perspectieven:

- het totaalperspectief;
- het perspectief van de *Zorggebruiker*;
- het perspectief van de *Uitgever*, die onder de hoede van de *Dienstverlener Persoon* valt. Laatstgenoemde kan deze plaat lezen als zijn verplichte aandeel in de use case *Delen*;
- het perspectief van de *Lezer*, die onder de hoede van de *Dienstverlener zorgaanbieder* valt. Laatstgenoemde kan deze plaat lezen als zijn verplichte aandeel in de use case *Delen*.

De stroomdiagrammen tonen allereerst de situatie waarin alle acties slagen tot en met het uiteindelijke delen van de gezondheidsinformatie (de zogenaamde happy flow). De twee oranje banen horen, conform de MedMij-huisstijl, tot het Persoonsdomein, de blauwe tot het Zorgaanbiedersdomein. Menige actie in de stroomdiagrammen is gekleurd weergegeven. De lichtgrijs gekleurde acties vormen samen de autorisatieflow; de zachtgeel gekleurde acties vormen samen de authenticatieflow. In de stroomdiagrammen voor de specifieke perspectieven hebben alleen de acties in de bij dat perspectief horende baan namen. De acties in de andere banen zijn gecomprimeerd en anoniem weergegeven.

Tot slot bespreken we de uitzonderingen op de happy flow. Daarbij werken we alleen vanuit het totaalperspectief.

## Totaalperspectief (happy flow)

### Toelichting

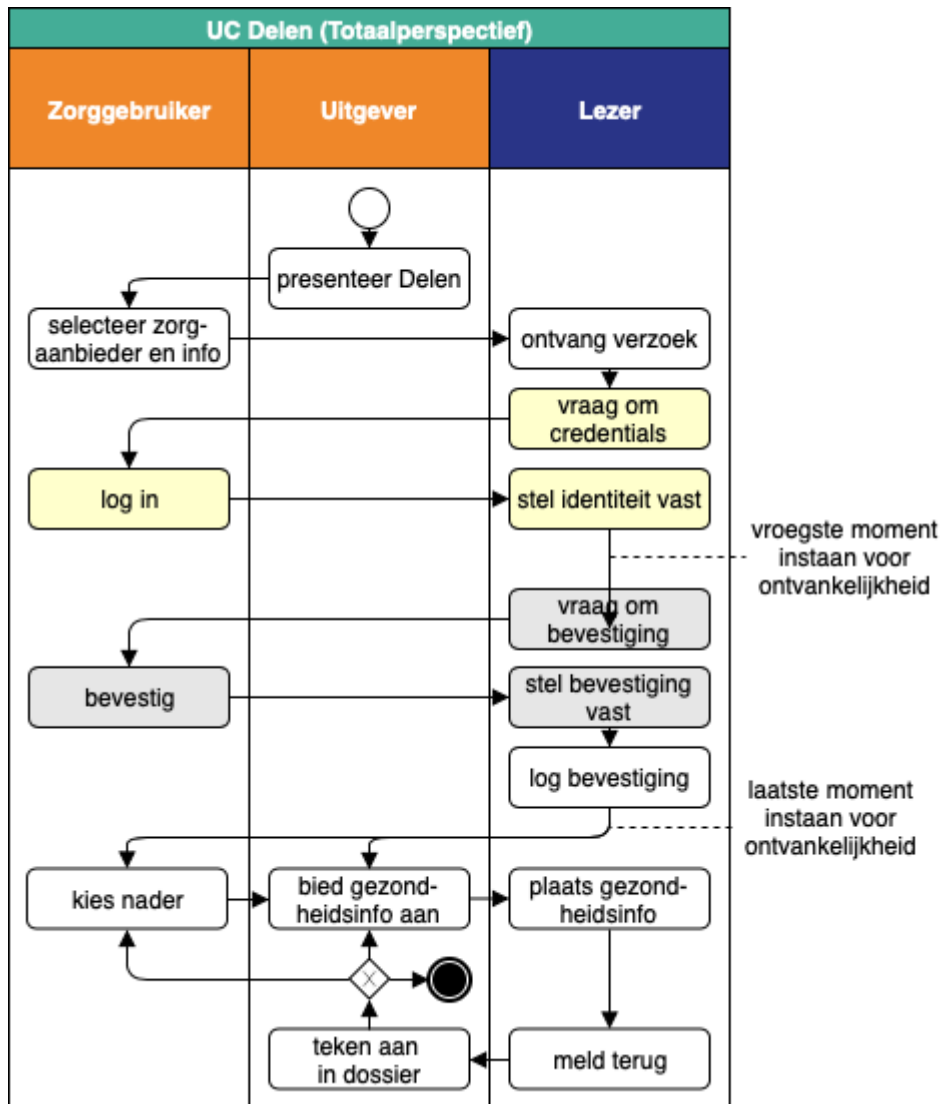
In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

De totale procesgang van de UC Delen kent de volgende stappen:

- De *Uitgever* presenteert aan de *Zorggebruiker* de mogelijkheid om te delen.
- De *Zorggebruiker* kiest de zorgaanbieder waarmee hij de informatie wenst te delen en de *Gegevensdienst*. Daarvoor kunnen desgewenst de *Gegevensdienstnamen* worden gebruikt uit de *Gegevensdienstnamenlijst*. Het verzoek gaat naar de passende *Lezer*.
- De *Lezer* laat de *Zorggebruiker* zich authenticeren.
- Dan breekt het moment aan waarop de *Lezer* op zijn vroegst ervoor instaat dat de *Zorgaanbieder* voor de betreffende *Gegevensdienst* überhaupt gezondheidsinformatie van die *Persoon* wenst te ontvangen, of anders de happy flow afbreekt. Het MedMij Afsprakenstelsel adviseert de ontvankelijkheidsvoorwaarde op het vroegst aangegeven moment van kracht te laten zijn. Vooralsnog staat het MedMij Afsprakenstelsel het toe die voorwaarde op een later moment van kracht te laten zijn, maar niet later dan het laatste in het figuur aangegeven moment.
- De *Lezer* vraagt aan de *Zorggebruiker* of hij de wens bevestigt de informatie te laten verstrekken aan de *Zorgaanbieder*. De vraag die aan de *Zorggebruiker* gesteld moet worden in de stap "bevestig" staat op de pagina [Bevestigingsverklaring](#).
- De *Lezer* logt die bevestiging en laat de *Uitgever* weten of die geslaagd is.
- Voordat de flow dan wordt overgegeven aan de *Uitgever* zal de *Lezer* ervoor instaan dat de *Zorgaanbieder* voor de betreffende *Gegevensdienst* überhaupt gezondheidsinformatie van die *Persoon* wenst te ontvangen, of anders de happy flow afbreken.
- Nu kan de *Uitgever* de gezondheidsinformatie plaatsen bij de *Lezer*.
- Mocht de *Gegevensdienst* waartoe de *Zorggebruiker* heeft geautoriseerd uit meerdere *Transacties* bestaan (zie hiervoor de [Catalogus](#)), plaatst de *Uitgever* daarna mogelijk opnieuw bij de *Lezer* voor de nog resterende *Transacties*, eventueel na nieuwe interactie met de *Zorggebruiker*.
- De *Uitgever* tekent bij de informatie ook de meta-informatie aan die wordt bedoeld in verantwoordelijkheid 19 van de [Processen- en Informatielaag](#).

Zie het toelichtingen-blok over regie en uitwisseling, onderaan de hoofdpagina van [Architectuur en technische specificaties](#). De ontvankelijkheidsvoorwaarde is een aspect van de regie, niet van de uitwisseling. De voorwaarde geeft de *Zorgaanbieder* ruimte om deel te nemen in aan de *Persoon* gegeven regie. Omdat echter bestaande implementatie-architecturen veelal uitwisseling centraal zetten, en niet regie, hebben zij moeite de beschikbaarheidsvoorwaarde in de regiefase te

implementeren. Daarom biedt het MedMij Afsprakenstelsel vooralsnog de gelegenheid om deze in de uitwisselingsfase te implementeren. *Deelnemers* wordt echter aangeraden om, met het oog op de toekomst, in hun implementatie-architecturen een passend onderscheid tussen regie en uitwisseling te maken en de eerste geleiding de tweede te laten sturen.



## Uitzonderingen (Totaalperspectief)

### Toelichting

In onderstaande tabel staan de uitzonderingssituaties beschreven. Alle worden door de *Lezer* ontdekt. Om te voorkomen dat de *Uitgever* informatie over het bestaan van behandelrelaties verkrijgt zonder dat (al) bevestiging is gegeven, moet het onderscheid tussen de uitzonderingen 2, 3 en 4 niet te maken zijn door de *Uitgever*.

Op de Applicatielaag zullen, bij de [use case-implementatie Delen](#), deze uitzonderingen opnieuw ter sprake komen, maar nu ook met hun precieze implementatie en formaat van de foutmeldingen.

Of de *Zorgaanbieder*, in de controle op ontvankelijkheid, zich ontvankelijk verklaart voor de door de *Persoon* aangeboden gezondheidsinformatie, is om te beginnen een zaak tussen de *Zorgaanbieder* en *Persoon*, die daarvoor een behandelrelatie moeten hebben. Gegeven zo'n behandelrelatie is er wetgeving van toepassing op deze ontvankelijkheid (zie [Juridisch kader](#)). Daarbinnen is eigen beslisruimte voor de *Zorgaanbieder*. Omdat *Zorgaanbieder* en *Persoon* evenwel geen *Deelnemers* in het MedMij Afsprakenstelsel zijn, specificeert het MedMij Afsprakenstelsel niet de exacte logica van de beslissing om al dan niet ontvankelijk te zijn voor de gezondheidsinformatie. Om privacy-redenen vereist het MedMij Afsprakenstelsel echter wel dat er een behandelrelatie moet (hebben) bestaan waarbij de betreffende gezondheidsinformatie hoort én dat de *Persoon* minstens zestien jaar oud is (zie uitzondering UC Delen 3).

Voor het laten delen van gegevens door een minder dan zestienjarige moet toestemming of een machtiging tot toestemming worden verleend door degene die de ouderlijke verantwoordelijkheid of de wettelijke verantwoordelijkheid voor de minder dan zestienjarige draagt. Omdat in dergelijke toestemmingen of machtigingen nog niet is voorzien in deze versie van het MedMij Afsprakenstelsel, kan deze controle vooralsnog als onderdeel van de ontvankelijkheidsvoorwaarde worden opgevat. Wanneer een toekomstige release van het MedMij Afsprakenstelsel wel zulke toestemmingen of machtigingen omvat, zal de leeftijdsvoorwaarde gescheiden moeten worden van de ontvankelijkheidsvoorwaarde.

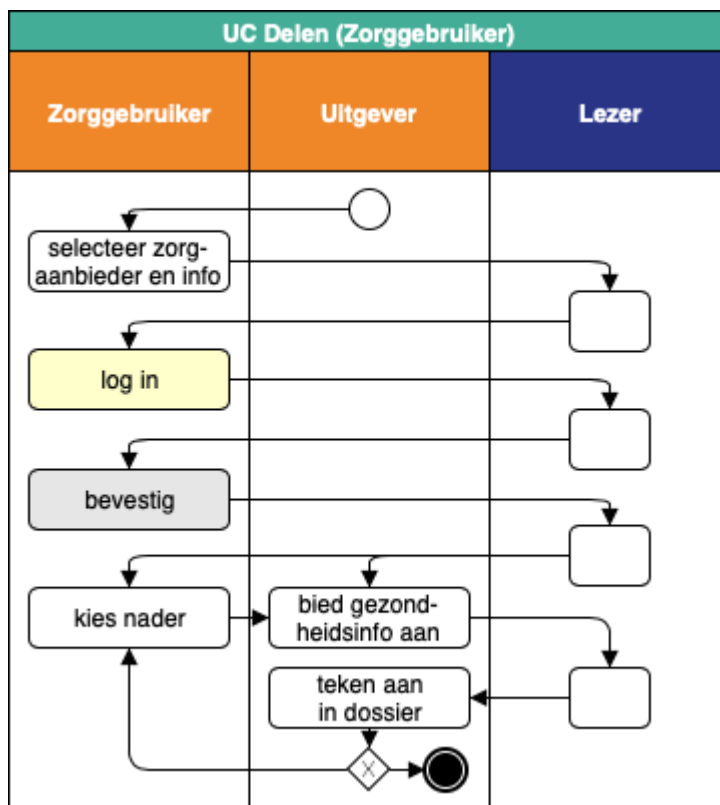
nr.	uitzondering	actie	vervolg
UC Delen 1	<i>Lezer</i> vindt het ontvangen verzoek ongeldig.	<i>Lezer</i> informeert <i>Uitgever</i> over deze uitzondering. <i>Uitgever</i> informeert daarop <i>Zorggebruiker</i> hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Delen 2	<i>Lezer</i> kan de identiteit van de <i>Zorggebruiker</i> niet vaststellen.	<i>Lezer</i> informeert <i>Uitgever</i> dat delen niet toegelaten wordt.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Delen 3	<p><i>Lezer</i> stelt op enig moment vast dat betreffende informatie van <i>Persoon</i> bij <i>Zorgaanbieder</i> niet welkom is. Hiervan is in elk geval sprake indien hetzij:</p> <ul style="list-style-type: none"> <li>er geen behandelrelatie is aan te wijzen als grondslag voor het delen;</li> <li><i>Zorggebruiker</i> nog geen zestien jaar oud is.</li> </ul> <p>Zie de toelichting op <a href="#">Beschikbaarheids- en ontvankelijkheidsvoorwaarde</a>.</p>		
UC Delen 4	De bevestiging wordt niet gegeven.		

UC Delen 5	<i>Lezer</i> kan het antwoord op de bevestigingsvraag niet vaststellen.	<i>Lezer</i> informeert <i>Uitgever</i> over deze uitzondering. <i>Uitgever</i> informeert daarop <i>Zorggebruiker</i> hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Delen 6	<i>Uitgever</i> kan, zelfs na bevestiging, de gezondheidsinformatie alsnog niet plaatsen bij <i>Lezer</i> .	<i>Uitgever</i> informeert daarop <i>Zorggebruiker</i> hierover, met opgave van oorzaak.	Mocht gezondheidsinformatie deels wel (geautoriseerd) geplaatst kunnen worden, dan kan de flow dat nog verzorgen.

## Perspectief van de *Zorggebruiker* (happy flow)

### Toelichting

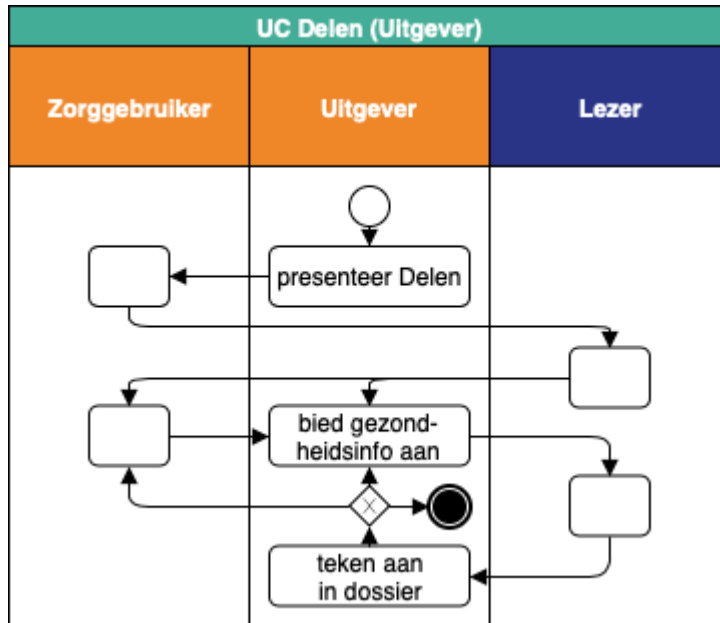
De *Zorggebruiker* moet om te beginnen drie stappen doorlopen: selectie van *Zorgaanbieder* en *Gegevensdienst*, inloggen en bevestigen. Eventueel kiest hij daarna voor nadere informatie om te laten plaatsen.



## Perspectief van de *Uitgever* (happy flow)

### Toelichting

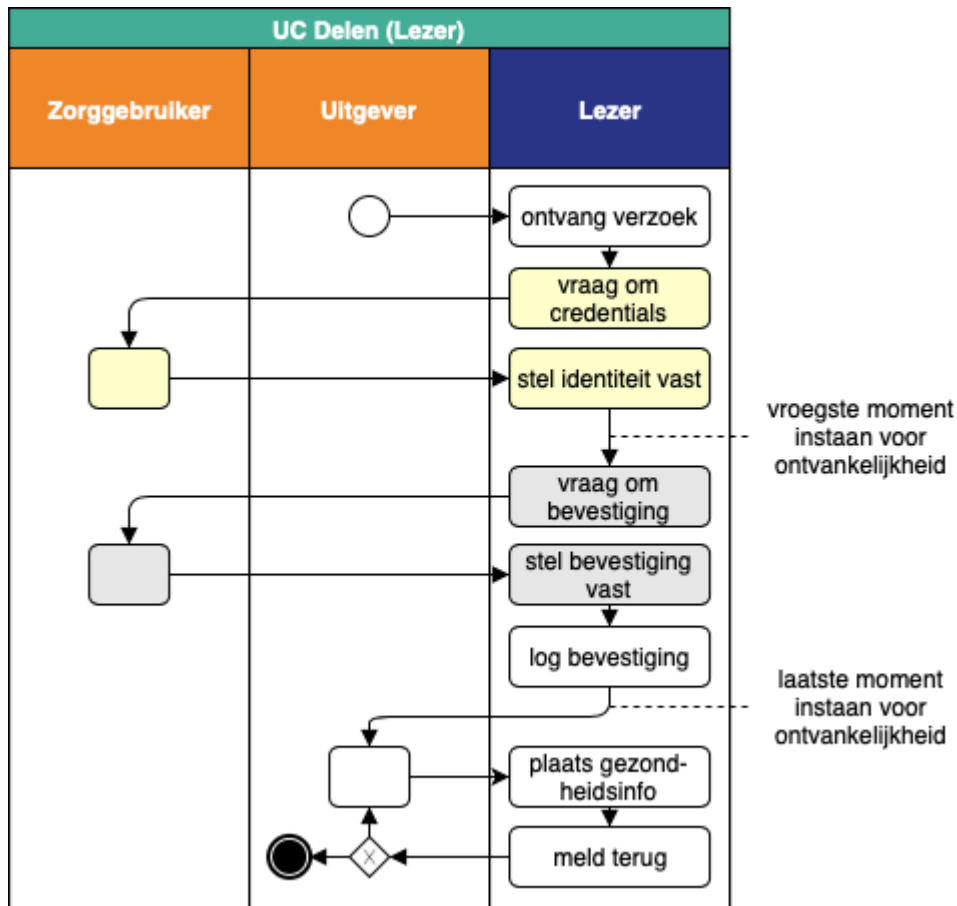
De *Uitgever* start de use case door aan de *Zorggebruiker* de mogelijkheid tot delen te presenteren. Van de *Lezer* krijgt hij na enige tijd het bericht dat de wens daartoe door *Zorggebruiker* is bevestigd, waarna hij de gezondheidsinformatie aanbiedt aan de *Lezer*. De reactie daarop tekent hij aan in het *Dossier*.



## Perspectief van de *Lezer* (happy flow)

### Toelichting

De *Lezer* regisseert, na ontvangst van het verzoek tot delen, de authenticatie en de bevestiging. Als die geslaagd zijn, logt hij de bevestiging. Uiteindelijk krijgt hij van de *Uitgever* de gezondheidsinformatie aangeboden ter plaatsing bij de *Zorgaanbieder*. De *Lezer* meldt het resultaat daarvan terug.





## UC Abonneren

### Toelichting

In de platen hieronder staat het stroomdiagram van de use case *Abonneren*, in vier perspectieven:

- het totaalperspectief;
- het perspectief van de *Uitgever*, die onder de hoede van de *Dienstverlener persoon* valt. Laatstgenoemde kan deze plaat lezen als zijn verplichte aandeel in de use case *Abonneren*;
- het perspectief van de *Bron*, die onder de hoede van de *Dienstverlener zorgaanbieder* valt. Laatstgenoemde kan deze plaat lezen als zijn verplichte aandeel in de use case *Abonneren*;
- het perspectief van de *Zorggebruiker*.

De use case *Abonneren* hoort geheel bij de hoofdfunctie *Regie*. Zij omvat het aangaan, het veranderen van de duur en het beëindigen van *Abonnementen*.

De stroomdiagrammen tonen allereerst de situatie waarin alle acties slagen tot en met het uiteindelijke afsluiten van een *Abonnement* (de zogenaamde happy flow). De twee oranje banen horen bij het Persoonsdomein, de blauwe bij het Zorgaanbiedersdomein. De lichtgrijs gekleurde acties vormen samen de autorisatieflow; de zachtgeel gekleurde acties vormen samen de authenticatieflow. In de stroomdiagrammen voor de specifieke perspectieven hebben alleen de acties in de bij dat perspectief horende baan namen. De acties in de andere banen zijn gecompriemd en anoniem weergegeven.

Tot slot bespreken we de uitzonderingen op de happy flow. Daarbij werken we alleen vanuit het totaalperspectief.

## Totaalperspectief (happy flow)

### Toelichting

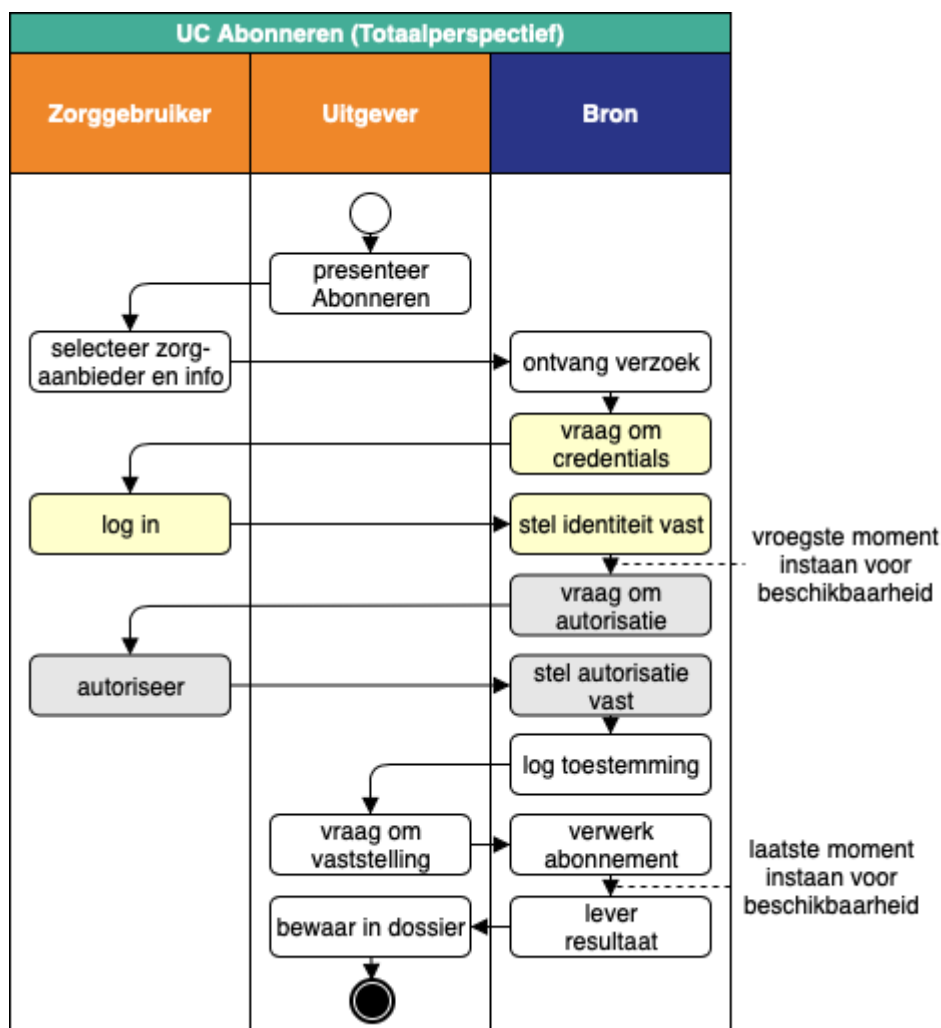
In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

De totale procesgang van de *UC Abonneren* kent de volgende stappen:

- De *Uitgever* presenteert aan de *Zorggebruiker* de mogelijkheid om *Abonnementen* aan te gaan, aan te passen of te beëindigen.
- De *Zorggebruiker* selecteert voor het aangaan van een *Abonnement* expliciet de *Zorgaanbieder* en de specifieke *Gegevensdienst*, en voor het aanpassen of beëindigen het betreffende *Abonnement*. Daarvoor kunnen desgewenst de *Gegevensdienstnamen* worden gebruikt uit de *Gegevensdienstnamenlijst*. Het verzoek gaat naar de passende *Bron*.
- De *Bron* laat de *Zorggebruiker* zich authenticeren.
- Indien het gaat om het aangaan of aanpassen van een *Abonnement*, breekt dan het moment aan waarop de *Bron* op zijn vroegst ervoor instaat dat de *Zorgaanbieder* voor de betreffende *Gegevensdienst* überhaupt gezondheidsinformatie van die *Persoon* beschikbaar heeft, of anders de happy flow afbreekt. Het MedMij Afsprakenstelsel adviseert de beschikbaarheidsvoorwaarde op het vroegst aangegeven moment van kracht te laten zijn. In deze release staat het MedMij Afsprakenstelsel het toe die voorwaarde op een later moment van kracht te laten zijn, maar niet later dan het laatste in het figuur aangegeven moment. Het beëindigen van een *Abonnement* mag de *Zorgaanbieder* niet weigeren.

- De *Bron* vraagt aan de *Zorggebruiker* of hij toestemming geeft tot het verstrekken van de gevraagde informatie aan de *Uitgever*. Deze vraag staat op de pagina [Toestemmingsverklaring Abonneren](#).
- De *Bron* logt die toestemming en laat de *Uitgever* weten dat de toestemming gegeven is.
- Nu kan de *Uitgever* de *Bron* vragen om diens vaststelling van het aangaan, aanpassen of beëindigen van het *Abonnement*.
- Indien het gaat om het aangaan of aanpassen van een *Abonnement*, zal uiterlijk na de ontvangst van het verzoek de *Bron* ervoor instaan dat de *Zorgaanbieder* voor de betreffende *Gegevensdienst* überhaupt gezondheidsinformatie van die *Persoon* beschikbaar heeft, of anders de happy flow afbreken.
- Bij ontvangst van het resultaat verwerkt de *Uitgever* het nieuwe, aangepaste of beëindigde *Abonnement* in het persoonlijke *Dossier*.
- Bij de informatie wordt ook de meta-informatie opgeslagen die wordt bedoeld in verantwoordelijkheid 19 van de [Processen- en Informatielaag](#).

De beschikbaarheidsvoorwaarde hoort bij [Regie](#), niet bij [Uitwisseling](#). De voorwaarde geeft de *Zorgaanbieder* ruimte om deel te nemen in aan de *Persoon* gegeven [Regie](#). Omdat echter bestaande implementatie-architecturen veelal uitwisseling centraal zetten, en niet [Regie](#), hebben zij moeite de beschikbaarheidsvoorwaarde in de regiefase te implementeren. Daarom biedt het MedMij Afsprakenstelsel vooralsnog de gelegenheid om deze in de uitwisselingsfase te implementeren.



## Uitzonderingen (Totaalperspectief)

### Toelichting

In onderstaande tabel staan de uitzonderingssituaties beschreven. Alle worden door de *Bron* ontdekt. Om te voorkomen dat de *Uitgever* informatie over het bestaan van behandelrelaties verkrijgt zonder dat daarvoor (al) toestemming is gegeven, moet het onderscheid tussen de uitzonderingen 2, 3 en 4 niet te maken zijn door de *Uitgever*.

Of de *Zorgaanbieder* de gevraagde gezondheidsinformatie beschikbaar stelt aan de *Persoon*, is om te beginnen een zaak tussen de *Zorgaanbieder* en *Persoon*, die daarvoor een behandelrelatie moeten hebben. Gegeven zo'n behandelrelatie is er wetgeving van toepassing op deze terbeschikkingstelling (zie [Juridisch kader](#)). Daarbinnen is eigen beslissruimte voor de *Zorgaanbieder*. Omdat *Zorgaanbieder* en *Persoon* evenwel geen *Deelnemers* in het MedMij Afsprakenstelsel zijn, specificeert het MedMij Afsprakenstelsel niet de exacte logica van de beslissing om de gezondheidsinformatie al dan niet ter beschikking te stellen. Om privacy-redenen vereist het MedMij Afsprakenstelsel echter wel dat er een behandelrelatie moet (hebben) bestaan waarbij de betreffende gezondheidsinformatie hoort én dat de *Persoon* minstens zestien jaar oud is (zie uitzondering UC Abonneren 3).

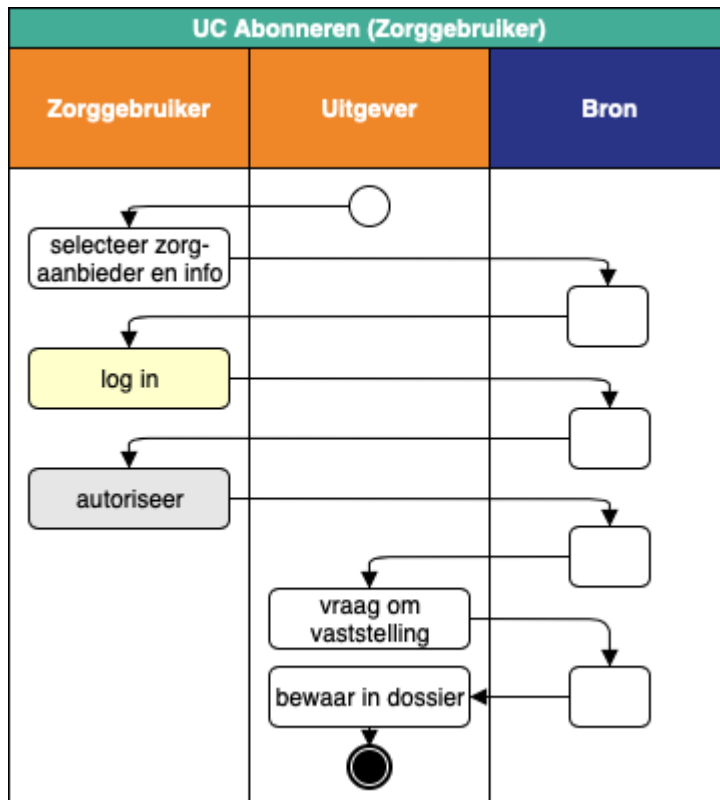
Voor het verstrekken van gegevens aan een minder dan zestienjarige moet toestemming of een machtiging tot toestemming worden verleend door degene die de ouderlijke verantwoordelijkheid of de wettelijke verantwoordelijkheid voor de minder dan zestienjarige draagt. Omdat in dergelijke toestemmingen of machtigingen nog niet is voorzien in deze versie van het MedMij afsprakenstelsel, kan deze controle vooralsnog als onderdeel van de beschikbaarheidsvoorwaarde worden opgevat. Wanneer een toekomstige release van het MedMij afsprakenstelsel wel zulke toestemmingen of machtigingen omvat, zal de leeftijdsvoorwaarde gescheiden moeten worden van de beschikbaarheidsvoorwaarde.

nr.	uitzondering	actie	vervolg
UC Abonneren 1	<i>Bron</i> vindt het ontvangen verzoek ongeldig.	<i>Bron</i> informeert <i>Uitgever</i> over deze uitzondering. <i>Uitgever</i> informeert daarop <i>Zorggebruiker</i> hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Abonneren 2	<i>Bron</i> kan de identiteit van de <i>Zorggebruiker</i> niet vaststellen.	<i>Bron</i> informeert <i>Uitgever</i> dat verzoek niet wordt ingewilligd.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Abonneren 3	<i>Bron</i> stelt op enig moment namens <i>Zorgaanbieder</i> vast dat niet wordt voldaan aan de beschikbaarheidsvoorwaarde. Hiervan is in elk geval sprake indien hetzij: <ul style="list-style-type: none"> <li>• er geen behandelrelatie is aan te wijzen als grondslag voor het verzamelen;</li> <li>• <i>Zorggebruiker</i> nog geen zestien jaar oud is.</li> </ul> Zie de toelichting op <a href="#">Beschikbaarheids- en ontvankelijkheidsvoorwaarde</a> .		
UC Abonneren 4	<i>Zorggebruiker</i> geeft geen <a href="#">Toestemmingsverklaring Abonneren</a> af.		
UC Abonneren 5	<i>Bron</i> kan het antwoord op de toestemmingsvraag niet vaststellen.	<i>Bron</i> informeert <i>Uitgever</i> over deze uitzondering. <i>Uitgever</i> informeert daarop <i>Zorggebruiker</i> hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Abonneren 6	<i>Bron</i> kan, zelfs na toestemming, de gezondheids- of <i>Abonnements</i> -informatie alsnog niet ter beschikking stellen aan de <i>Uitgever</i> .	<i>Bron</i> informeert <i>Uitgever</i> over deze uitzondering. <i>Uitgever</i> informeert daarop <i>Zorggebruiker</i> hierover, met opgave van oorzaak.	Mocht de gezondheidsinformatie deels wel (geautoriseerd) ter beschikking staan, dan kan de flow dat nog verzorgen.

## Perspectief van de *Zorggebruiker* (happy flow)

### Toelichting

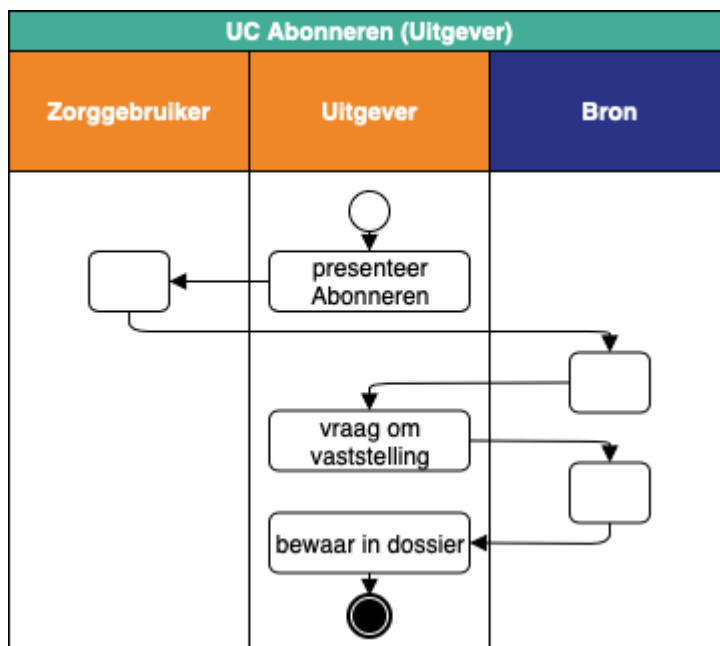
De *Zorggebruiker* moet drie stappen doorlopen: selectie van *Zorgaanbieder* en *Gegevensdienst*, inloggen en autoriseren. Als alles slaagt, slaat de *Uitgever* voor hem de vaststelling op.



## Perspectief van de *Uitgever* (happy flow)

### Toelichting

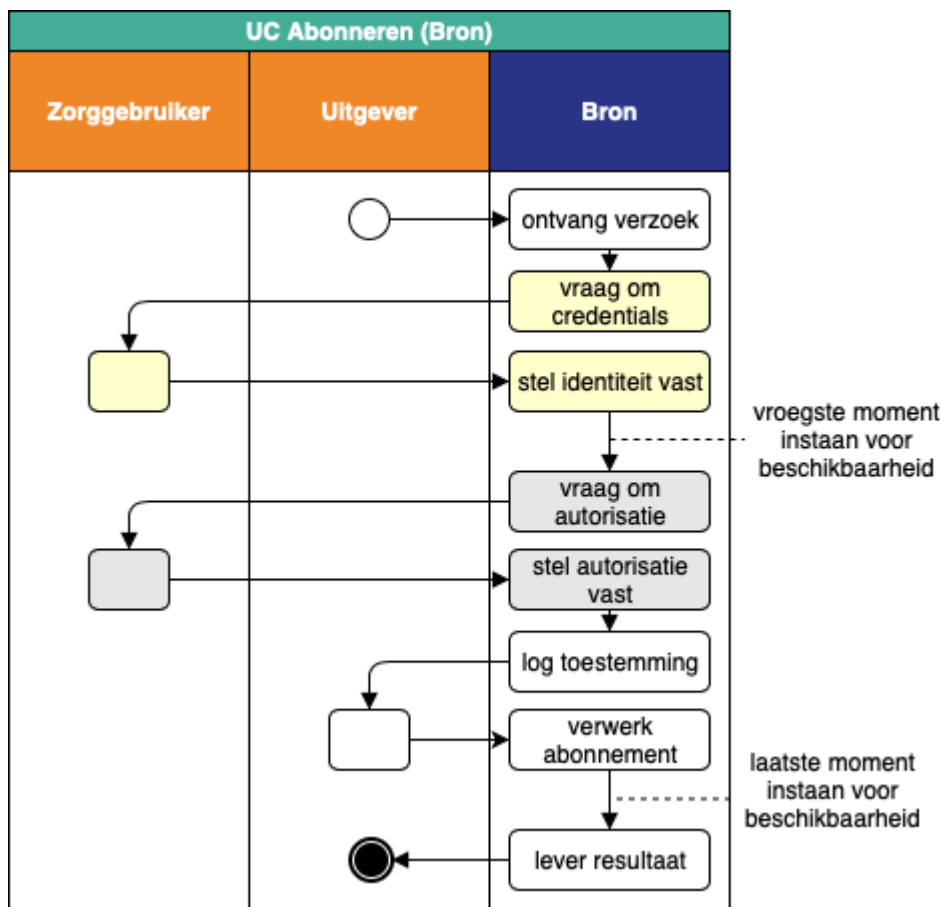
De *Uitgever* start de use case door aan de *Zorggebruiker* de mogelijkheid tot abonneren te presenteren. Van de *Bron* krijgt hij na enige tijd het bericht dat de toestemming daarvoor is verleend, waarna hij die toestemming logt en het abonneren laat vaststellen door de *Bron*, en opslaat.



## Perspectief van de *Bron* (happy flow)

### Toelichting

De *Bron* regisseert, na ontvangst van het verzoek, de authenticatie en de toestemming. Als die geslaagd zijn logt hij de toestemming en stuurt deze naar de *Uitgever*. Die zal uiteindelijk om vaststelling verzoeken en het antwoord in ontvangst nemen.



## UC Notificeren

### Toelichting

In de platen hieronder staat het stroomdiagram van de use case *Notificeren*, in vier perspectieven:

- het totaalperspectief;
- het perspectief van de *Zorggebruiker*;
- het perspectief van de *Uitgever*, die onder de hoede van de *Dienstverlener* persoon valt. Laatstgenoemde dient deze plaat te lezen als zijn verplichte aandeel in de use case *Notificeren*;
- het perspectief van de *Bron*, die onder de hoede van de *Dienstverlener* zorgaanbieder valt. Laatstgenoemde dient deze plaat te lezen als zijn verplichte aandeel in de use case *Notificeren*.

De stroomdiagrammen tonen allereerst de situatie waarin alle acties slagen (de zogenaamde happy flow). De oranje banen horen, conform de MedMij-huisstijl, tot het Persoonsdomein, de blauwe tot het Zorgaanbiedersdomein. In de stroomdiagrammen voor de specifieke perspectieven hebben alleen de acties in de bij dat perspectief horende baan namen. De acties in de andere banen zijn gecompriemd en anoniem weergegeven.

Tot slot bespreken we de uitzonderingen op de happy flow. Daarbij werken we alleen vanuit het totaalperspectief.

## Totaalperspectief (happy flow)

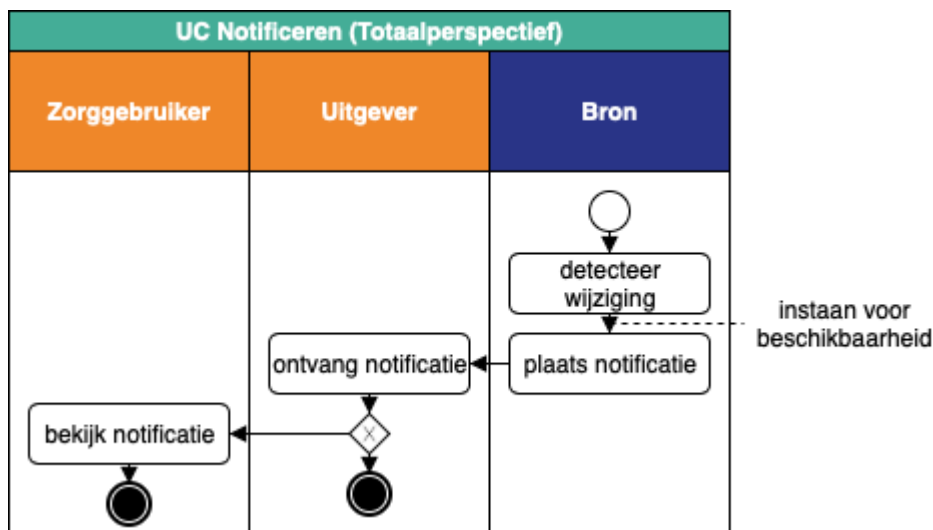
### Toelichting

In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

De totale procesgang van de *UC Notificeren* kent de volgende stappen:

- Hetzij de *Bron* detecteert een wijziging in (gezondheids)informatie waarop *Zorggebruiker* een *Abonnement* heeft genomen (een inhoudelijke wijziging) of de *Bron* beëindigt, op eigen initiatief, een specifiek *Abonnement* (een abonnementswijziging).
- Indien het een inhoudelijke wijziging betreft, wordt vastgesteld dat de *Zorgaanbieder* instaat voor de beschikbaarheid van de betreffende gezondheidsinformatie. De notie van beschikbaarheid is dezelfde als die in *UC Verzamelen*.
- De *Bron* plaatst een *Notificatie* bij de *Uitgever* en slaat de meta-informatie op die wordt bedoeld in verantwoordelijkheid 19b van de *Processen- en Informatielaag*.
- Bij ontvangst van een *Notificatie* slaat de *Uitgever* de meta-informatie op die wordt bedoeld in verantwoordelijkheid 19b van de *Processen- en Informatielaag*.
- Mogelijk stelt de *Uitgever* de *Zorggebruiker* op de hoogte van de *Notificatie*. Indien dat door middel van een tekstbericht gebeurd, worden hiervoor de teksten gebruikt die zijn opgenomen op de pagina *Notificatie van zorggebruiker*.

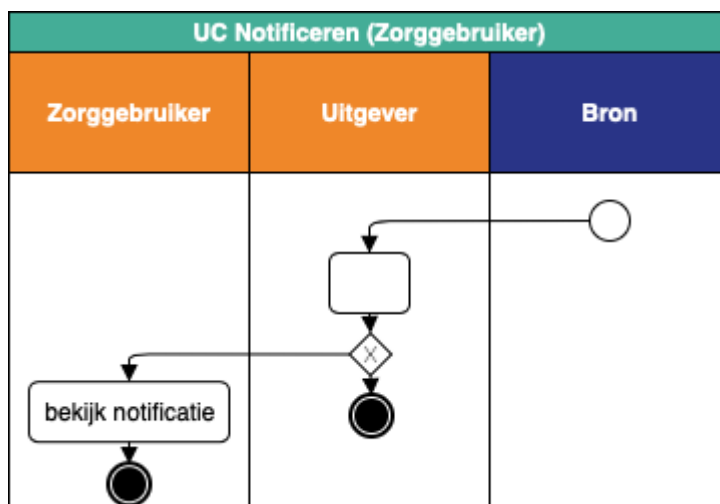




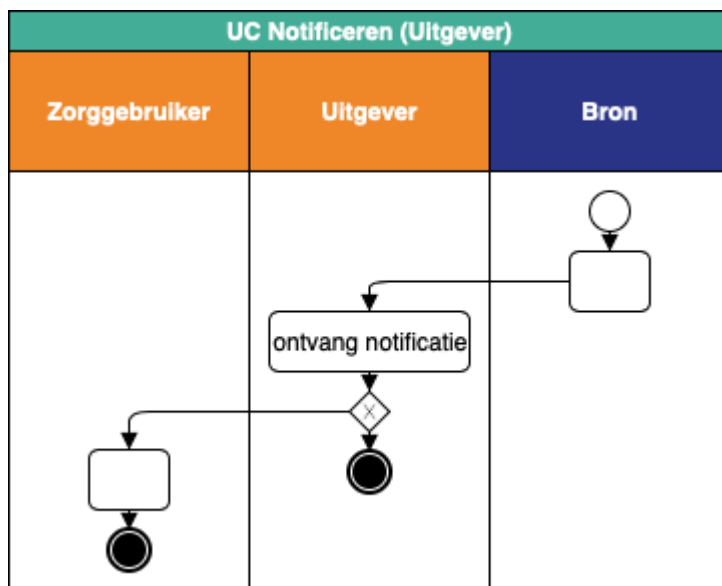
## Uitzonderingen (Totaalperspectief)

nr.	uitzondering	actie	vervolg
UC Notificeren 1	<i>Uitgever</i> vindt de ontvangen <i>Notificatie</i> ongeldig.	<i>Uitgever</i> informeert <i>Bron</i> over deze uitzondering.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Notificeren 2	<i>Uitgever</i> kan de <i>Notificatie</i> niet, niet geheel of niet tijdig verwerken.	<i>Uitgever</i> informeert <i>Bron</i> over deze uitzondering.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.

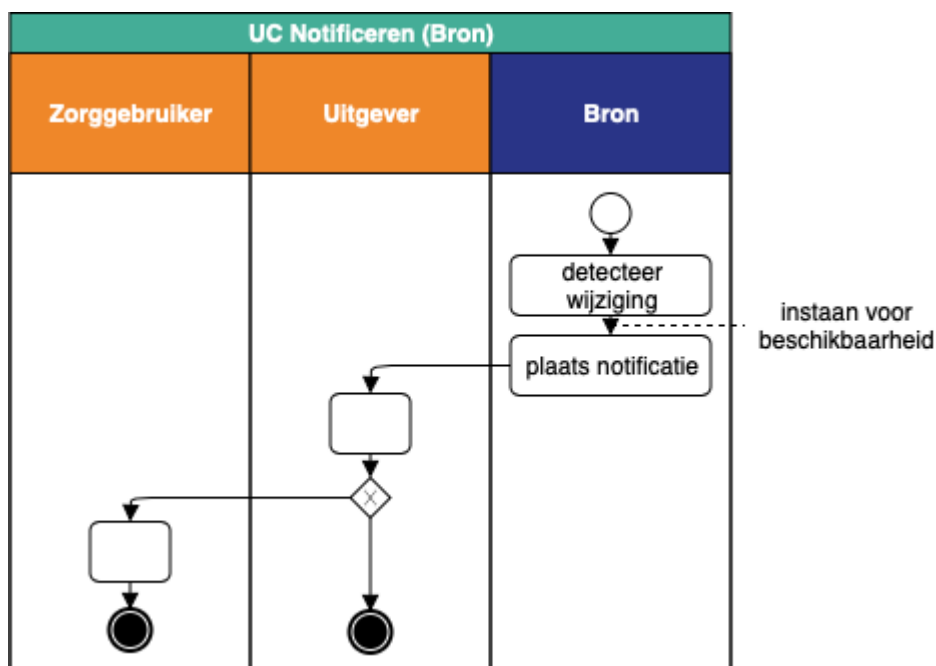
## Perspectief van de *Zorggebruiker* (happy flow)



## Perspectief van de *Uitgever* (happy flow)



Perspectief van de *Bron* (happy flow)

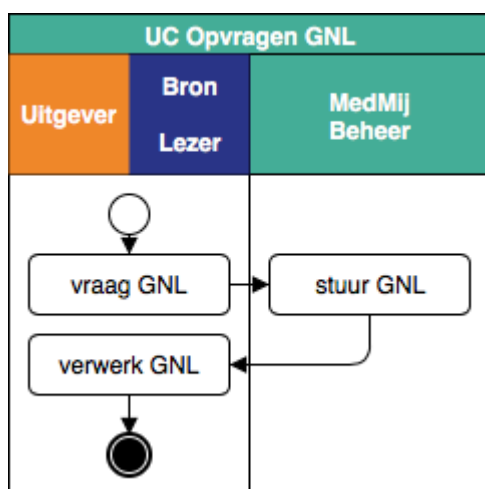


## UC Opvragen GNL

### Stroomdiagram

#### Toelichting

In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen. In de linkerbaan betekent dat: één *Uitgever* of één *Bron/Lezer*.

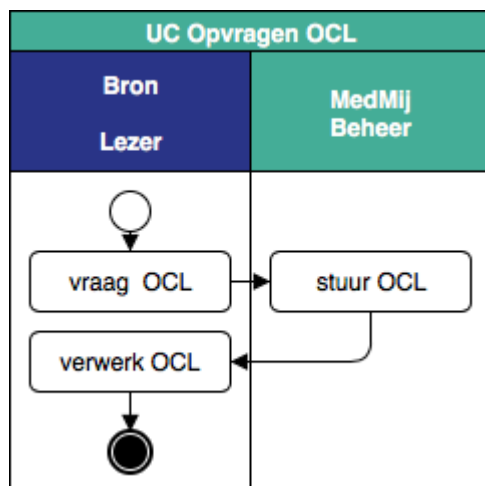


## UC Opvragen OCL

### Stroomdiagram

#### Toelichting

In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

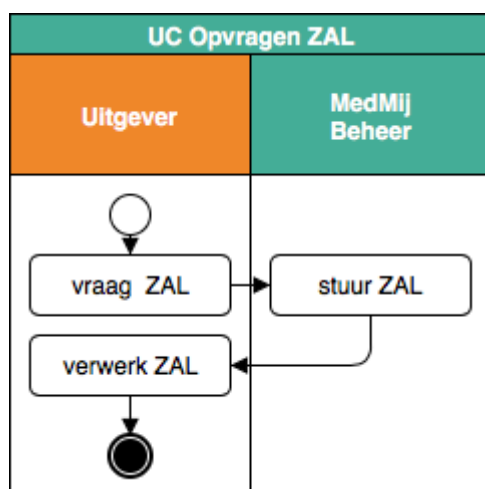


## UC Opvragen ZAL

### Stroomdiagram

#### Toelichting

In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.



## Beschikbaarheids- en ontvankelijkheidsvoorwaarde

### Verantwoordelijkheden

1a. De *Zorgaanbieder* voert beleid ten aanzien van het beschikbaar houden van gezondheidsinformatie (en *Abonnementen op Notificaties* daarover) voor, en ontvankelijk zijn voor gezondheidsinformatie van, zekere *Personen* op zekere *Gegevensdiensten*.

1b. De *Dienstverlener zorgaanbieder* voert, als verwerker voor elke verwerkingsverantwoordelijke *Zorgaanbieder*, diens in verantwoordelijkheid 1a bedoelde beleid uit in *UC/UCI Verzamelen*, *UC/UCI Abonneren*, *UC/UCI Delen* en *UC/UCI Notificeren*. De *Dienstverlener zorgaanbieder* voert in aanvulling op dat van de *Zorgaanbieders* geen eigen beleid dienaangaande.

1c. Het in verantwoordelijkheid 1a bedoelde beleid discrimineert op geen andere aspecten dan de *Persoon* en de *Gegevensdienst*. In het bijzonder is discriminatie op *Dienstverlener persoon* uitgesloten, tenzij dat door het MedMij Afsprakenstelsel wordt vereist.

#### Toelichting

Het instaan voor de beschikbaarheids- en de ontvankelijkheidsvoorwaarde is van kracht:

- ergens tussen de gebruikersauthenticatie en de uitwisseling van gezondheidsinformatie in *UC/UCI Verzamelen* en *UC/UCI Abonneren*, respectievelijk *UC/UCI Delen*;
- onmiddellijk bij het begin van *UC/UCI Notificeren*;

De bedoeling daarvan is tweeledig.

1. Het wil veilig stellen dat er zo snel mogelijk na de authenticatie van de *Persoon*, en in elk geval voordat er gezondheidsinformatie wordt uitgewisseld tussen *PGO Server* en *Resource Server*, uitgegaan mag worden van het vervuld zijn van twee voorwaarden voor het verzamelen of delen van de betreffende informatie: het bestaan van een (eventueel voorbijgaande) behandelrelatie als grondslag daarvoor en van een leeftijd van de persoon van minimaal zestien jaar. Het is de juridische eindverantwoordelijkheid van de *Zorgaanbieder* deze voorwaarden te (laten) verifiëren. Zie voor het leeftijdsaspect verder het *Juridisch kader*.
2. Zij geven de *Zorgaanbieder* de kans naar eigen bevinden extra beperkingen, structureel of incidenteel, op te leggen aan het laten verzamelen, laten abonneren op notificaties, of laten delen van informatie, bijvoorbeeld om technische redenen of vanwege bijzondere situaties, bijzondere patiënten of aangrijpende inhoud.

De *Dienstverlener zorgaanbieder* staat er bij het laten voortgaan van de procesgang dus voor in dat de behandelrelatie aanwezig is en dat de leeftijd voldoende is. Hoe de *Dienstverlener zorgaanbieder* dat (met de *Zorgaanbieder*) geborgd heeft is vrij. Aan die borging kunnen bijvoorbeeld bijdragen:

- juridische middelen, zoals bepalingen in de dienstverleningsovereenkomst tussen *Zorgaanbieder* en *Dienstverlener Zorgaanbieder*;
- organisatorische maatregelen in de wijze waarop *Zorgaanbieders* het dossier beheren, zodat aan de dossierinformatie, aan de ordening ervan, of zelfs aan de loutere aanwezigheid ervan, gezien kan worden of er een behandelrelatie aan ten grondslag ligt;
- geautomatiseerde logica, die voor een zekere *Persoon* en een zekere *Gegevensdienst* de ontvankelijkheid/beschikbaarheid bij een zekere *Zorgaanbieder* bepaalt, voortbouwend op organisatorische maatregelen.

Het MedMij Afsprakenstelsel verplicht er niet toe om leeftijdsgegevens en behandelrelatiegegevens expliciet te administreren. Waar het bestaan van een behandelrelatie of een toereikende leeftijd, op juridische en/of organisatorische gronden, geïmpliceerd wordt door andere gegevens, mogen

laatstgenoemde gegevens ook met die implicatie gebruikt worden. Het MedMij Afsprakenstelsel specificeert daarom geen logica voor de voorwaarden; het bepaalt slechts twee noodzakelijke onderdelen van hun post-conditie: een toereikende leeftijd van de *Persoon* en het (hebben) bestaan van een toepasselijke behandelrelatie.

Het niet-beschikbaar blijken zegt niets over de precieze reden. Daaruit kan zelfs niet worden geconcludeerd dat het-zij de behandelrelatie ontbreekt of de leeftijd ontoereikend is. De *Zorgaanbieder* kan ook an-dere redenen gehad hebben te weigeren.

Om redenen van dataminimalisatie en gebrui-ksvriendelijkheid zijn de beschikbaarheids- en ontvankelijkheidsvoorwaarden bij voorkeur zo snel mogelijk van kracht, dat wil zeggen, onmiddellijk na de authenticatie van de *Persoon*, nog voor de autorisatievraag (de vroege variant). De beschikbaarheids- en ontvankelijkheidsvoorwaarde behoren uit hun aard bij de [hoofd functie Regie](#), niet bij [Uitwisseling](#). Daartegenover wordt de implementatie van de voorwaarden voor sommige *Deelnemers* eenvoudiger als zij pas van kracht zouden hoeven te zijn wanneer de procesgang bij de *Resource Server* is aangekomen (de late variant).

Hieronder worden de vroege en de late variant vergeleken vanuit de perspectieven van dataminimalisatie en gebruiksvriendelijkheid. Beide aspecten moeten vanuit het perspectief van de gehele use case en alle betrokken rollen beschouwd worden: een keuze tussen de vroege en de late variant heeft effecten op meerdere plaatsen tegelijk. De afweging onderscheidt vier situaties, afhankelijk van twee vragen:

- Acht de *Zorgaanbieder* (zich voor) de informatie (uiteindelijk) beschikbaar/ontvankelijk?
- Geeft de *Persoon* (uiteindelijk) toestemming?

De late varianten verschillen overigens subtiel tussen zowel [UC/UCI Verzamelen](#) en [UC/UCI Delen](#). In [UC/UCI Delen](#) is de late variant in vergelijking nog een stap vroeger dan in [UC/UCI Verzamelen](#). Dat komt omdat anders een verwerking (namelijk: plaatsing) van gezondheidsinformatie zou gebeuren door de *Resource Server* nog voordat zou blijken dat de *Zorgaanbieder* hiervoor niet ontvankelijk is. In [UC/UCI Verzamelen](#) kan het een stapje later, omdat de te voorkomen actie pas de uitwisseling met de *PGO Server* is.

De twee varianten laten zich als volgt vergelijken inzake dataminimalisatie.

	(uiteindelijk) wel beschikbaar /ontvankelijk	(uiteindelijk) niet beschikbaar/ontvankelijk
(uiteindelijk) wel toestemming	<ul style="list-style-type: none"> <li>• Voor zover er aparte geautomatiseerde logica worden gebruikt voor een toets op beschikbaarheid of ontvankelijkheid vraagt de vroege variant extra verkeer ten opzichte van de late variant, namelijk tussen <i>Authorization Server</i> en de component(en) die zij voor het uitvoeren van die toets aanspreekt. Dat verkeer speelt zich wel geheel binnen de verantwoordelijkheid van een enkele verwerkingsverantwoordelijke</li> </ul>	<ul style="list-style-type: none"> <li>• In de late variant vindt, in tegenstelling tot in de vroege, al het verkeer na de authenticatie (de toestemmingsvraag, het uitdelen van authorisatie code en access token en het aanspreken van de <i>Resource Server</i>) onnodig plaats. Dit verkeer strekt zich uit over verantwoordelijkheidsgrenzen.</li> <li>• In de late variant krijgt de <i>PGO Server</i>, onnodig, meer over de beschikbaarheid /ontvankelijkheid, en dus over de <i>Persoon</i>, te weten van de <i>Resource Server</i> dan in de vroege variant van de <i>Authorization Server</i>. In de vroege variant kan de betreffende uitzondering immers, vanuit de <i>PGO Server</i> bezien,</li> </ul>

(uiteinde-lijk) geen toestemming	af; er vindt geen verstrekking plaats.	ook door falende authenticatie of weigering van toestemming veroorzaakt zijn. In de late variant komt de <i>PGO Server</i> echter wel te weten, door het ontvangen van de onnodige authorization code, dat er sprake is van zowel een behandelrelatie als een toereikende leeftijd.
	<ul style="list-style-type: none"> <li>De <i>Authorization Server</i> komt alleen in de vroege variant extra te weten dat behandelrelatie en leef-tijd in orde zijn. In de late variant komt alleen de <i>Resource Server</i> dat te weten. Dat laat onverlet dat beide onder dezelfde eindverantwoordelijke <i>Dienstverlener Zorgaanbieder</i> vallen.</li> </ul>	In de late variant vindt, in tegenstelling tot in de vroege, een overbodige toestemmingsvraag plaats. Dit verkeer vindt plaats over het relatief onveilige frontchannel.

De twee varianten laten zich als volgt vergelijken inzake gebruiksvriendelijkheid.

	(uiteindelijk) wel beschikbaar /ontvankelijk	(uiteindelijk) niet beschikbaar/ontvankelijk
(uiteindelijk) wel toestemming	geen verschil	<p>In de vroege variant is de <i>Persoon</i> onmiddellijk op de hoogte, zodat deze:</p> <ul style="list-style-type: none"> <li>geen onnodige en verwarrende handeling (betekenisloze toestemming) met rechtsgevolgen hoeft uit te voeren, zoals in de late variant;</li> <li>preciezer dan in de late variant op de hoogte raakt van waarom een uitwisseling faalt. In de late variant kan dat falen andere redenen hebben, zodat de <i>Persoon</i> voor opheldering op ondersteuningsvragen aangewezen zou zijn, die wellicht zelfs aan de <i>Zorgaanbieder</i> gericht worden. In de vroege variant zijn Uitzonderingen 2, 3 en 4 in <a href="#">UC/UCI Verzamelen</a>, <a href="#">UC/UCI Abonneren</a> en <a href="#">UC/UCI Delen</a> weliswaar samengenomen in één melding naar de <i>PGO Server</i>, zodat deze het onderscheid tussen falende authenticatie, falende autorisatie en falende beschikbaarheid/ontvankelijkheid niet kan maken. De <i>Persoon</i> zelf echter kent vanwege zijn/haar voorafgaande rechtstreekse interactie met de <i>Authorization Server</i> het resultaat van de authenticatie en de autorisatie wel, en kan dus alsnog uit deze gecombineerde melding, buiten medeweten van de <i>PGO Server</i>, afleiden of er sprake was van falende beschikbaarheid/toegankelijkheid.</li> </ul>
(uiteindelijk) geen toestemming		In de vroege variant is de persoon onmiddellijk op de hoogte en hoeft deze geen onnodige en verwarrende handeling (holle afwijzing) uit te voeren, zoals in de late variant.

De gevallen waarin de *Zorgaanbieder* (zich voor) de informatie beschikbaar/ontvankelijk acht zijn, uitgaande van redelijk gedrag van de *PGO Server*, waarschijnlijk talrijker dan die waarin dat niet het geval is. Anderzijds wegen de nadelen van de vroege variant voor eerstgenoemde gevallen licht, omdat het zorgaanbiedersdomein en de *Authorization Server* om andere redenen al afdoende beveiligd moeten zijn, al is het maar vanwege het gebruik van het BSN. Bovendien is er alleen



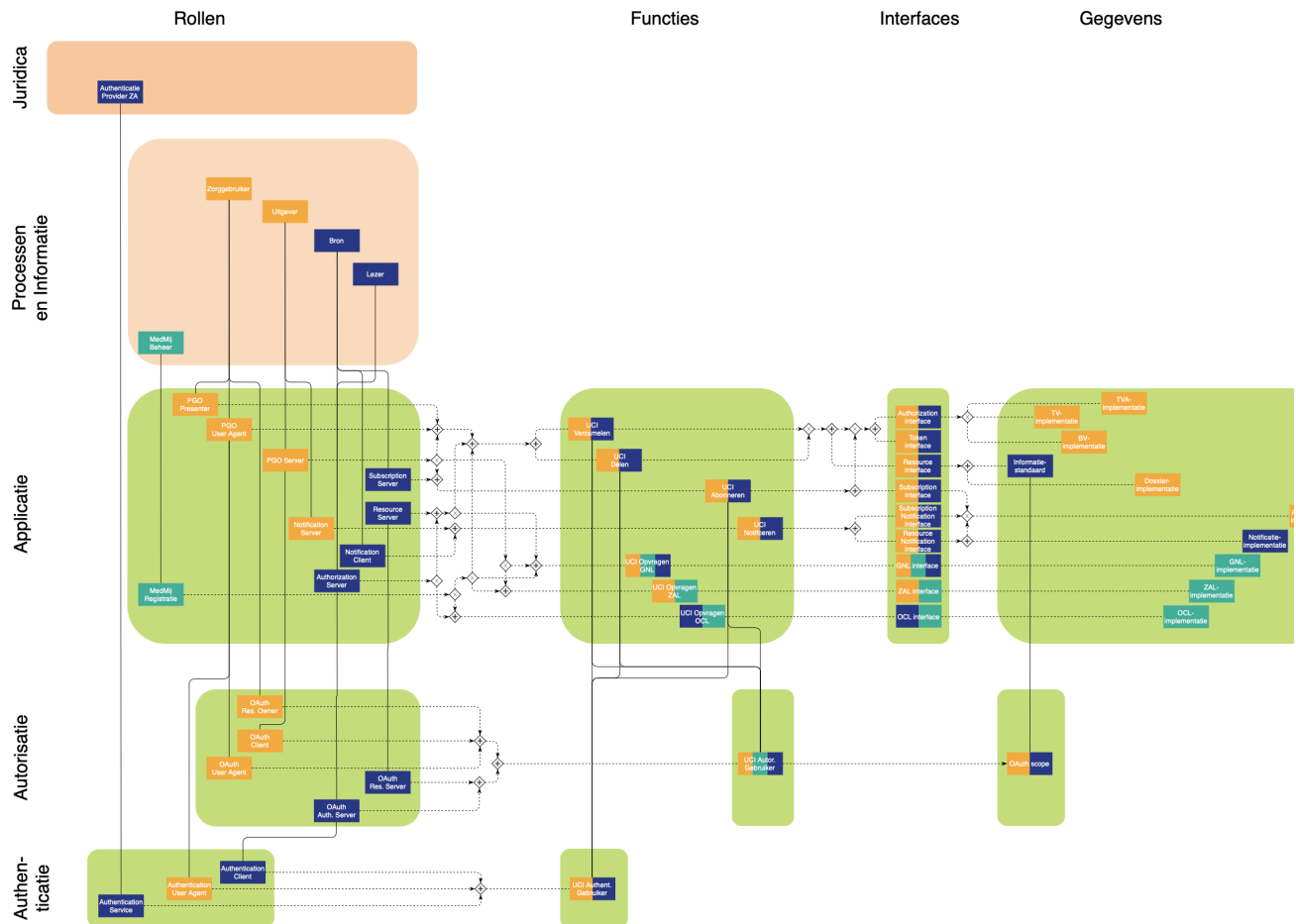
sprake van extra verkeer voor zo-ver geautomatiseerde logica wordt ingezet en daarvoor rollen anders dan de *Authorization Server*, en dus buiten het MedMij Afsprakenstelsel, worden aangesproken.

In deze release adviseert het MedMij Afsprakenstelsel daarom de vroege variant, vanwege bovengenoemde analyse. Het MedMij Afsprakenstelsel staat echter ook de late variant toe, om *Dienstverleners Zorgaanbieder* zowel de gelegenheid te geven snel aan te sluiten als de tijd om te overwegen hoe de vroege variant op termijn geïmplementeerd zou kunnen worden.

---

Verantwoordelijkheid 1c borgt het all-to-all-principe ([principe 7](#)) door te verbieden dat *Dienstverleners zorgaanbieder* bepaalde *Dienstverleners persoon* uitsluiten van (*Abonnementen op*) *Gegevensdiensten* die zij van enige *Zorgaanbieder* ontsluiten.

## Applicatie



### Inleiding

Voor een overzicht over alle lagen van de architectuur, en voor een toelichting van de betekenis van de symbolen en lijntjes, zie de [overzichtspagina](#).

De afkorting:

- BV staat voor *Bevestigingsverklaring*;
- GNL staat voor *Gegevensdienstnamenlijst*;
- OCL staat voor *OAuth Client List*;
- TV staat voor *Toestemmingsverklaring*;
- TVA staat voor *Toestemmingsverklaring Abonneren*;
- ZAL staat voor *Zorgaanbiederslijst*.

## Rollen

1. *Uitgever.*

- a. biedt aan *Zorggebruiker*, in het kader van de toepasselijke *Dienstverleningsovereenkomst*, een geautomatiseerde rol ter gebruik, hier genoemd: *PGO Server*. Eén *Uitgever* biedt één of meerdere *PGO Servers* en elke *PGO Server* wordt door één *Uitgever* geboden.
  - b. stelt, indien deze *UC Notificeren* aanbiedt, aan *Zorgaanbieder* een geautomatiseerde rol *Notification Server* ter beschikking, waarop de *Zorgaanbieder* *Notificaties* kan aanbieden. Eén zulke *Uitgever* één of meerdere *Notification Servers* en elke *Notification Server* wordt door één *Uitgever* geboden.
2. *Bron*:
- a. biedt, en *Lezer* biedt, een geautomatiseerde dienst, voor het namens *Zorgaanbieders* uitwisselen van gezondheidsinformatie met *PGO Server*, bestaande uit: *Authorization Server* en *Resource Server*. Eén *Bron* en/of *Lezer* biedt één of meer combinaties van één *Authorization Server* en één *Resource Server* en elke combinatie van één *Authorization Server* en één *Resource Server* wordt door één *Bron* en/of *Lezer* geboden.
  - b. biedt, indien deze *UC Abonneren* aanbiedt, een geautomatiseerde dienst voor het namens *Zorgaanbieders* aangaan van *Abonnementen*, bestaande uit *Authorization Server* en *Subscription Server*. Elke zulke *Bron* biedt één of meer combinaties van één *Authorization Server* en één *Subscription Server* en elke combinatie van één *Authorization Server* en één *Subscription Server* wordt door één *Bron* geboden.
  - c. biedt, indien deze *UC Notificeren* aanbiedt, een geautomatiseerde rol voor het namens *Zorgaanbieders* plaatsen van *Notificaties*, genaamd *Notification Client*. Elke zulke *Bron* biedt één of meer *Notification Clients* en elke *Notification Client* wordt door één *Bron* geboden.
3. *Zorggebruiker* gebruikt twee geautomatiseerde rollen voor toegang tot de functionaliteit van *PGO Server* en *Authorization Server*. *PGO Presenter* voor de presentatie van de functionaliteit aan *Zorggebruiker* en *PGO User Agent* voor het aanspreken van *PGO Server* en *Authorization Server*.
4. *MedMij Beheer* ontsluit ten behoeve van alle betrokkenen een geautomatiseerde dienst, hier genoemd: *MedMij Registratie*.
5. Ten behoeve van het authenticeren van *Zorggebruiker*, zal de betrokken *Authorization Server*, in de rol van *Authentication Client*, gebruikmaken van de *Authentication Service* van een *Authenticatie Provider* ZA.
6. Ten behoeve van het autoriseren van *PGO Server* voor toegang tot *Resource Server*, in het kader van *UCI Verzamelen* en *UCI Delen*, respectievelijk tot *Subscription Server* in het kader van *UCI Abonneren*, zullen de betrokken *PGO User Agent*, *PGO Server*, *Authorization Server* en *Resource Server*, respectievelijk *Subscription Server*, gebruik maken van *OAuth 2.0*, waarbij als grant type gebruik wordt gemaakt van *Authorization Code* en waarbij:
- a. de rol van *OAuth User Agent* wordt verzorgd door de *PGO User Agent*;
  - b. de rol van *OAuth Client* wordt verzorgd door de *PGO Server*;
  - c. de rol van *OAuth Resource Server* wordt verzorgd door de *Resource Server*, in het geval van *UCI Verzamelen* en *UCI Delen*, en door de *Subscription Server* in het geval van *UCI Abonneren*;
  - d. de rol van *OAuth Authorization Server* wordt verzorgd door de *Authorization Server*.
7. Als *MedMij-verkeer* is gedefinieerd: al het gegevensverkeer in het kader van enige use case-implementatie op deze laag of op de *Netwerk*-laag, onmiddellijk tussen twee verschillende van de vier volgende soorten rollen, namelijk:
- ten eerste *PGO Server* of *Notification Server*,
  - ten tweede *PGO User Agent*,
  - ten derde *Authorization Server*, *Resource Server*, *Subscription Server* of *Notification Client*, en
  - ten vierde *MedMij Registratie*,
- met dien verstande dat:
- in deze rollen telkens begrepen zijn de door hen eventueel verzorgde respectievelijke Autorisatie-rollen,
  - van deze rollen telkens uitgesloten zijn de door hen eventueel verzorgde Authenticatie-rollen, en
  - in deze rollen, met betrekking tot de use case-implementaties op de *Netwerk*-laag, telkens inbegrepen zijn de *Netwerk*-rollen waarop zij functioneren.
8. Al het *MedMij-verkeer*, voor zover daarin de *PGO User Agent*:

- betrokken is, heet *frontchannel-verkeer*;
- niet betrokken is, vormt het *backchannel-verkeer*.

### Toelichting

Hier worden de rollen van de [Processen-en-Informatie](#)-laag vertaald naar rollen op applicatieniveau. Voor de algemene uitgangspunten inzake de getalsverhoudingen tussen de rollen, zie de pagina [Architectuur en technische specificaties](#).

In het persoonsdomein zijn drie rollen onderscheiden: de *PGO Presenter*, *PGO User Agent* en de *PGO Server*. Dat is nodig om de verbinding te kunnen leggen met de rollen volgens OAuth. *PGO Presenter* en *PGO User Agent* zijn alle front-end-rollen voor de *PGO Server*, en kunnen bijvoorbeeld allebei in een browser zijn geïmplementeerd, maar voor een goede binding aan de *OAuth*- en *Authentication*-rollen en voor een goede beveiligingsmaatregelen is het nodig deze twee rollen te scheiden. Zoals ook elders in het MedMij Afsprakenstelsel gaat het hier om rollen, om setjes verantwoordelijkheden dus, niet om implementatiecomponenten.

In het Zorgaanbiedersdomein is zo'n scheiding niet nodig. Waar een *Persoon* zelf operationeel betrokken wordt in het informatieverkeer — namelijk om zich te laten authenticeren, en het verkeer te laten autoriseren — laat de *Zorgaanbieder* zich operationeel geheel vertegenwoordigen door zijn *Dienstverlener* en diens *Authorization Server* en *Resource Server*. Ook al zal in veel gevallen de gezondheidsinformatie uiteindelijk uit een achterliggend systeem worden betrokken, voor het MedMij Afsprakenstelsel is dat geen kwestie. Het is voldoende om bij de *Authorization Server* en *Resource Server* de eindverantwoordelijkheid neer te leggen (black box).

In lijn met keuzes op de [Proces- en Informatielaag](#), treden deze servers op namens alle eventuele achterliggende systemen in het Zorgaanbiedersdomein, zoals xIS'en. Die achterliggende complexiteit is een black box. Het is mogelijk dat een individuele xIS optreedt voor beide servers, maar dan moeten ook alle met deze rollen verbonden verantwoordelijkheden zijn ingevuld, zowel de direct verbonden verantwoordelijkheden (op de Applicatielaag) als de indirect verbonden verantwoordelijkheden (op de lagen erboven en eronder).

De keuze, in OAuth, voor de grant type Authorization Code past bij de typische software-architectuur die in MedMij in het Persoonsdomein wordt aangetroffen: toegang tot een PGO-dienst via componenten die niet onder controle van de *OAuth Client* vallen en als betrekkelijk onveilig moeten worden gezien. Op deze laag onderscheiden we bij deze toegang twee rollen: de rol *PGO Presenter* die zorgt voor de presentatie van de functionaliteit aan de *Zorggebruiker*, en de rol *PGO User Agent* die zorgt voor het aanspreken van de *PGO Server* en de *Authorization Server*. Het is de rol *PGO User Agent* die verbonden wordt met de rollen *OAuth User Agent* en *Authentication User Agent*. De *PGO User Agent* spreekt uiteindelijk dus ook de *Authentication Service* aan.

### Authorization Server, Resource Server en Subscription Server

De rollen *Authorization Server* en respectievelijk *Resource Server* (in [UCI Verzamelen](#) en [UCI Delen](#)) of *Subscription Server* (in [UCI Abonneren](#)) werken in het MedMij-afsprakenstelsel samen in eenzelfde ononderbroken sessie. Hun onderlinge relatie is een proceskoppeling. Dat wil zeggen, zij worden georkestreerd onder de hoede van één procesgang. Rollen in het MedMij Afsprakenstelsel zijn echter groepjes verantwoordelijkheden, geen implementatiecomponenten. Het is daarmee aan de *Dienstverlener zorgaanbieder* om in zijn implementatie, en business model, keuzes te maken over het scheiden of juist combineren van deze twee rollen. Als de rollen gescheiden zijn is het bovendien goed mogelijk om één *Authorization Server* of *Subscription Server* te laten samenwerken met meerdere *Resource Servers* en om één *Resource Server* zaken te laten doen met meerdere

*Authorization Servers of Subscription Servers.* Steeds echter zullen zij samen het gedrag moeten vertonen dat wordt geëist door het MedMij Afsprakenstelsel. Overigens maakt ook de OAuth-specificatie gewag van deze implementatievrijheid.

Omdat de sessiecoördinatie in het Zorgaanbiederdomein zich over het scheidsvlak tussen *Authorization Server* en *Resource Server of Subscription Server* uitstrekt, moet er in geval van gescheiden implementatie van *Authorization Server* en *Resource Server of Subscription Server* een interface worden gerealiseerd waarin die sessiecoördinatie in stand blijft. Bovendien moet, als de relatie tussen *Authorization Server* en *Resource Server of Subscription Server* niet één-op-één is, ervoor worden gezorgd dat de juiste twee elkaar vinden bij de communicatie over een specifiek access token.

Ondanks deze implementatievrijheid hebben de verantwoordelijkheden in het MedMij Afsprakenstelsel invloed op de implementatie-architectuur in het Zorgaanbiedersdomein. Met name vereist de adressering dat er voor één combinatie van *Zorgaanbieder*, *Gegevensdienst*, *Interfaceversie* (en *Systeemrol*) maar één authorization endpoint en één token endpoint (en één resource endpoint of subscription endpoint) kan zijn. Bovendien voorkomen beperkingen op de informatie-inhoud van authorization codes en access tokens dat het interface tussen *Authorization Server* en *Resource Server of Subscription Server* via het Persoonsdomein wordt gerealiseerd. Op enkele uitzonderingen na is dat interface een interne aangelegenheid van het Zorgaanbiedersdomein. Daarmee worden zowel principes P1 en P7 gediend, alsook dataminimalisatie, en dus de privacy. De belangrijkste uitzondering is dat de authorization code en het access token desgewenst een identificatie mogen bevatten van de service die het heeft uitgegeven. Daarmee kan de (voorzien) acceptant van de authorization code of het access token de *Authorization Server of Subscription Server* vinden waar de validatie van de authorization code of het access token moet plaatsvinden.

Zelfs als er sprake is van gescheiden implementatie, is het nog steeds één *Dienstverlener Zorgaanbieder* die eindverantwoordelijk is, jegens MedMij, voor het gezamenlijke gedrag van *Authorization Server* en *Resource Server of Subscription Server*. Dat betekent dat de interoperabiliteit tussen *Authorization Server* en *Resource Server of Subscription Server* moet vallen onder de overeenkomst die de betreffende *Dienstverlener zorgaanbieder* aangaat met eventuele onderaannemers, bijvoorbeeld als de *Dienstverlener zorgaanbieder* zelf de *Resource Server of Subscription Server* exploiteert maar een onderaannemer voor de *Authorization Server* contracteert. Zie ook de toelichting, onder de Rollen op de [Netwerk](#)-pagina, van hoe op netwerkniveau met *Nodes* wordt omgegaan indien een *Dienstverlener zorgaanbieder* gebruik zou maken van onderaannemers voor bijvoorbeeld *Authorization Server*- of *Subscription Server*-functionaliteit..

Het is denkbaar dat een community van dienstverleners in het Zorgaanbiedersdomein tot een afsprakenstelsel komt, aanpalend aan en voldoende aan het MedMij Afsprakenstelsel, waarin de interne architectuur van het Zorgaanbiedersdomein aan de orde is. Naast bovenbedoelde scheiding zouden daarin bijvoorbeeld ook architectuurkeuzes over de beschikbaarheids- en ontvankelijkheidstoets kunnen worden opgenomen.

### **Autorisatie versus authenticatie**

Het is van belang om een heldere scheiding te maken tussen autorisatie en authenticatie in het MedMij Afsprakenstelsel. Niet alleen zijn het verschillende functionaliteiten, authenticatie voor vaststelling van identiteit en autorisatie voor het beheren van toegangsrechten, de bijbehorende rollen kunnen in het MedMij Afsprakenstelsel niet zomaar worden gecombineerd. De *Authorization Server* heeft de rol om, namens de *Zorgaanbieder*, op verzoek van de *Persoon*, autorisaties uit te delen aan de *PGO Server*. Om dat betrouwbaar te kunnen doen, en om aan een wettelijke verplichting van de *Zorgaanbieder* invulling te geven, schakelt de *Authorization Server* de (externe) *Authentication Service* in.

Dat betekent echter niet dat de *Authorization Server* op haar beurt identiteitsdiensten gaat verlenen aan de *PGO Server*, door bijvoorbeeld een aan de BSN gekoppelde identiteit mee te geven met het acces token dat ze uitdeelt. Dat zou oneigenlijke verbreding zijn van haar authenticatierol, die begrensd zou moeten blijven tot de verantwoordelijkheden jegens de *Zorgaanbieder* en zich niet moet uitstrekken tot het bedienen van de *PGO Server*. Bovendien zou het een centrum van *Persoons*-identiteit creëren in het MedMij-landschap die, gezien de regiedoelstellingen van MedMij, bij voorkeur niet in het Zorgaanbiedersdomein ligt, maar in het Persoonsdomein, en daarbinnen bij voorkeur zo dicht mogelijk bij de *Persoon* zelf.

Daarom vindt er op het koppelvlak tussen *PGO Server* en *Authorization Server* geen uitwisseling van *Persoons*-identiteiten plaats, niet met bijvoorbeeld de standaard OpenID Connect, noch met een andere standaard met dat doel. Dat wil niet zeggen dat zulke standaarden niet op andere toekomstige koppelvlakken in het MedMij Afsprakenstelsel toegepast kunnen gaan worden, op koppelvlakken dus die juist wel voor identiteitsdienstverlening bedoeld zijn, in plaats van voor autorisatie.

De standaarden OAuth 2.0 en SAML 2.0 — als voorbeeld; de gekozen *Authentication Service* kan een ander koppelvlak gebruiken dan SAML — hebben dus verschillende doelen: OAuth voor autorisatie en SAML voor authenticatie. Dat zorgt er onder andere voor dat de rolstructuur anders is. In OAuth is er een gebruiker (*Resource Owner*) die via zijn browser of app (*User Agent*) aan de ene applicatie (*Client*) toegang verleent aan een andere (*Resource Server*), welke laatste zich daarvoor laat bijstaan door een *Authorization Server*. In SAML is er een gebruiker die via een browser of app (*User Agent*) inlogt bij een dienst (*Service Provider*), die zich daarvoor laat bijstaan door een *Identity Provider*.

Toch zitten er belangrijke overeenkomsten tussen de manieren waarop ze werken.

- Beide gaan ervan uit dat de eindgebruiker zich aandient via een betrekkelijk onveilig kanaal (de *User Agent*, het "front-channel"), terwijl er ook gevoeliger informatie moet worden uitgewisseld ("back-channel"), dat niet via dit kanaal verloopt.
- Bij beide moet de *User Agent* aan de hand worden genomen en heen- en teruggestuurd (redirect). Bij OAuth is dat van de *Client* naar de *Authorization Server* en terug. Bij SAML is dat van de *Service Provider* naar de *Identity Provider* en terug.
- Bij beide krijgt de *Client* (bij OAuth de *Client* en bij SAML de *Service Provider*) niet onmiddellijk de gewenste informatie (bij OAuth het access token en bij SAML de gebruikersidentiteit), maar via een ophaalbewijs (bij OAuth de authorization code, bij SAML het artefact). Het ophaalbewijs gaat voorlangs (via de *User Agent*), waarna achterlangs met het ophaalbewijs de gewenste informatie wordt opgehaald.

## MedMij-verkeer

In artikel 7 wordt het *MedMij-verkeer* afgebakend, met het oog op de [Netwerk](#)-laag. Al het *MedMij-verkeer* is over domeingrenzen. Bovendien maakt noch eventueel verkeer tussen *PGO Presenter* en *PGO User Agent*, noch eventueel verkeer tussen *Authorization Server* en *Resource Server* deel uit van *MedMij-verkeer*. Ook authenticatieverkeer is uitgesloten, omdat het MedMij Afsprakenstelsel geen eisen oplegt over welke (externe) *Authentication Service* wordt gebruikt. Het MedMij Afsprakenstelsel vereist dát er een passende authenticatie door *Zorgaanbieder* moet plaatsvinden, maar het verkeer dat daarvoor nodig is — tussen *Authorization Server*, *Authentication Service* en *PGO User Agent* — is geen MedMij-verkeer. Het is de *Zorgaanbieder* die niettemin als verwerkingsverantwoordelijke verantwoordelijk blijft voor een passende keuze van een *Authentication Service* en voor het laten inrichten van het authenticatieverkeer.

Deze afbakening is bovendien de opmaat voor punt 8 erna. Het daarin gemaakte onderscheid tussen frontchannel- en backchannelverkeer is nodig voor het formuleren van verantwoordelijkheden



over beveiliging (zie [Netwerk-laag](#)). In punt 7 moet ermee rekening gehouden worden dat er ook een use case-implementatie is op de [Netwerk-laag](#): *UCI Opvragen WHL*.

## Verantwoordelijkheden

### Use cases en Gegevensdiensten

#### Toelichting

Van de meeste use cases (zie de laag [Processen en Informatie](#)) wordt op deze (Applicatie)laag een use case-implementatie (UCI) voorgeschreven. Het gaat om de volgende.

use case-implementatie	Stroomdiagram	Hoofdfunctie
<i>UCI Verzamelen</i>	met	<i>Regie en Uitwisseling</i>
<i>UCI Delen</i>	met	<i>Regie en Uitwisseling</i>
<i>UCI Abonneren</i>	met	<i>Regie</i>
<i>UCI Notificeren</i>	met	<i>Regie of Uitwisseling</i>
<i>UCI Opvragen ZAL</i>	met	<i>Coördinatie</i>
<i>UCI Opvragen OCL</i>	met	<i>Coördinatie</i>
<i>UCI Opvragen GNL</i>	met	<i>Coördinatie</i>

1a. Bovengenoemde rollen implementeren de use case *UC Verzamelen* met de use case-implementatie *UCI Verzamelen*. Zij gebruiken hiertoe het betreffende [stroomdiagram](#). De gehele procesgang wordt ononderbroken uitgevoerd.

1b. Bovengenoemde rollen implementeren de use case *UC Delen* met de use case-implementatie *UCI Delen*. Zij gebruiken hiertoe het betreffende [stroomdiagram](#). De gehele procesgang wordt ononderbroken uitgevoerd.

1c. Voor zover de betreffende *Uitgever*, respectievelijk de betreffende *Bron*, *UC Abonneren* en *UC Notificeren* aanbieden, implementeren bovengenoemde rollen de *UC Abonneren* met de use case-implementatie *UCI Abonneren* en de *UC Notificeren* met de use case-implementatie *UCI Notificeren*. De gehele procesgang wordt ononderbroken uitgevoerd.

#### Toelichting

De gebruikersbeleving wordt het best bediend door de gehele procesgang ononderbroken te houden.

2. Als een *Uitgever* een zekere *Gegevensdienst* ontsluit ten behoeve van zijn *Zorggebruikers* en daartoe laat leveren door een *Bron* of *Lezer*, zullen de *PGO Server* van die *Uitgever* en de *Authorization Server* en *Resource Server* van die *Bron*, respectievelijk *Lezer*, daarvoor de bij de *Gegevensdienst* horende use case implementeren en de bij de *Gegevensdienst* horende *Informatiestandaarden* gebruiken, zoals deze in de *Catalogus* zijn opgenomen.

#### Toelichting

Zo wordt geborgd dat de juiste use case-implementaties en informatiestandaarden worden gebruikt.

### Autorisatie en OAuth

3. In de use case-implementaties [UCI Verzamelen](#), [UCI Delen](#) en [UCI Abonneren](#) handelen *PGO Server* enerzijds en *Authorization Server* en *Resource Server* of *Subscription Server* anderzijds, hun onderlinge verkeer af conform de standaard [OAuth 2.0](#).

#### Toelichting

Conform wettelijke verplichting geeft *Zorggebruiker*, in de [UC Verzamelen](#) en de [UC Abonneren](#), actief toestemming aan de *Zorgaanbieder*. In de [UC Delen](#) is deze verplichting niet aan de orde, maar vindt op dit moment evengoed een bevestiging door de *Zorggebruiker* plaats. De *PGO Presenter* presenteert een venster waarin de *Zorggebruiker* deze toestemming, respectievelijk bevestiging, kan geven. Aangezien in het persoonsdomein niet met BSN gewerkt mag worden, moet er een vervangende identificatie van de zorggebruiker gebruikt worden. Zie verantwoordelijkheid 5.

4. Van de vier soorten [authorization grants](#) die OAuth 2.0 biedt, beperken de OAuth-rollen zich tot [Authorization Code](#).

#### Toelichting

Met deze ene soort kunnen alle situaties die in het MedMij Afsprakenstelsel voorkomen worden bediend. Voor het maximaliseren van de interoperabiliteit kiest MedMij ervoor de andere drie soorten uit te sluiten.

5. De *OAuth Client* en *OAuth Resource Server* zullen slechts tokens van het type Bearer Token uitwisselen, conform [RFC6750](#).

#### Toelichting

De OAuth-standaard laat het (access) token type vrij. Token types verschillen in het vertrouwen waarmee de *Resource Server* aan de *Client* de gevraagde resources kan prijsgeven als laatstgenoemde het access token aan eerstgenoemde overlegt. Bij de eenvoudigste vorm (Bearer Token) geeft de *Resource Server* eenvoudigweg aan elke *Client* die een geldig access token overlegt, de resources die daarbij horen. "Aan toonder", net zoals een bank een cheque kan verzilveren aan toonder. Daaraan kleven evenwel veiligheidsrisico's, omdat het access token na uitgifte gestolen kan zijn, of anderszins vervreemd van de *Client* aan wie het uitgedeeld was. Andere token types kunnen daarom vragen om meer garanties, zoals een identiteit van de *Client* of een client secret. Bearer Token is echter het enige goed gestandaardiseerde en breed gebruikte token type. Het legt wel veel verantwoordelijkheid voor beheersing van de veiligheidsrisico's bij *Client* en *Authorization Server*. In [hoofdstuk 5 van de specificatie van de standaard RFC6750](#) is daarom expliciete aandacht voor die beveiligingsrisico's en maatregelen om die het hoofd te bieden. Zie hiervoor verantwoordelijkheid 18.

6. De *OAuth Client* maakt alleen gebruik van één scope tegelijk. De *OAuth Authorization Server* genereert authorization codes en access tokens met een enkelvoudige scope die geheel vervat moet zijn in de *Gegevensdienst* waarom de *OAuth Client* heeft gevraagd.

#### Toelichting



Bij het genereren van codes en tokens is de OAuth-scope meegenomen. Deze is gerelateerd aan de *Gegevensdienst*. Hoewel het technisch mogelijk is om meerdere scopes mee te geven is de scope beperkt tot één *Gegevensdienst* per keer.

7. De *OAuth Authorization Server* stelt van elke uitgegeven authorization code en elk uitgegeven access token de geldigheidsduur op exact 15 minuten (900 seconden). Zij geeft bovendien geen refresh tokens uit.

#### Toelichting

Dit is een maatregel tegen de beveiligingsrisico's 4.4.1.1 en 4.4.1.3 uit RFC 6819. Bovendien wordt de hele flow van *Verzamelen* ononderbroken uitgevoerd (zie onder 1). De 900 seconden moeten dan voldoende zijn voor de Client om het access token aan de *Authorization Server* aan te bieden. Een refresh token is dan niet nodig.

8a. De *OAuth Authorization Server* genereert authorization codes en access tokens zodanig, dat de kans op het raden ervan niet groter is dan  $2^{-128}$  en de daarvoor gebruikte random number generators cryptografisch veilig zijn.

8b. In de authorization codes en access tokens is het desgewenst toegestaan één of meer van de informatie-elementen uit de volgende limitatieve lijst op te nemen:

- een identifier van de authorization code, respectievelijk het access token, indien die identifier op zichzelf voldoet aan de in verantwoordelijkheid 8a genoemde eisen;
- een verloopmoment van de geldigheid van het token, onder de voorwaarden dat zowel:
  - de waarde daarvan in overeenstemming is met de verantwoordelijkheden in het MedMij Afsprakenstelsel en
  - uit het verstreken zijn daarvan wél de ongeldigheid van de authorization code of het access token mag worden geconcludeerd door de *Authorization Server* of de *Resource Server*, maar uit het nog niet verstreken zijn daarvan **niet** diens geldigheid, waarvoor namelijk een validatie van het gehele token tegen de interne administratie van de *Authorization Server* de enige autoriteit is;
- een identificatie van de service die het token heeft uitgegeven;
- de *scope* waarvoor de authorization code of het access token is uitgegeven, in de vorm van een kopie van de *scope*-parameter van de authorization request in antwoord waarop de authorization code of het access token is uitgegeven;
- de naam van het token-formaat;
- een digitale handtekening.

8c. Geen andere informatie dan de in verantwoordelijkheid 8b genoemde mag voorkomen in de authorization code of het access token, ook niet versleuteld. Er mogen t.a.v. informatie-inhoud van het token verschillende keuzes gemaakt worden tussen authorization code en access token. De *OAuth Client* mag de inhoud van het token niet interpreteren.

8d. Met betrekking tot zowel authorization codes als access tokens, draagt de *OAuth Authorization Server* die hen uitgeeft ervoor zorg, dat daarvan nooit twee dezelfde geldige in omloop zijn.

#### Toelichting

Dit is een maatregel tegen beveiligingsrisico 4.4.1.3 uit RFC 6819. Aan de in omloop gebrachte authorization codes en access tokens zijn twee belangrijke eisen te stellen: uniciteit en vertrouwelijkheid. De eis van vertrouwelijkheid weegt in het MedMij Afsprakenstelsel zwaar. Omdat de authorization code (indirect) en het access token (direct) toegang geven tot persoonlijke gezondheidsinformatie, kiest MedMij voor een formaat dat vrijwel betekenisloos is en alleen betekenis krijgt door confrontatie met lokale en goed beschermde administraties van de

*Authorization Server*. De maximale raadkans wordt geëist in [RFC6749, sectie 10.10](#). Er mag door vergelijking van meerdere authorization codes of access tokens niet doorschemeren hoe zij gegenereerd worden.

Wanneer een identifier is opgenomen in het access token, kan dat gebruikt worden als identificatie van de *Authorization Server*-sessie waarin het token werd uitgegeven, zodat de *Resource Server* deze sessie kan hervatten wanneer zij het access token aangeboden krijgt. Het is ook mogelijk dat een dergelijke identifier niet zozeer is opgenomen in de authorization code, respectievelijk het access token, maar geheel overeenkomt met de authorization code, respectievelijk het access token. Hoe dan ook, verantwoordelijkheid 8a blijft erop van kracht.

Wanneer een verloopmoment is opgenomen in het access token, wordt het mogelijk om de *Resource Server* te laten afzien van onnodige raadpleging van de *Authorization Server*, wanneer deze apart geïmplementeerd zouden zijn. De tweede voorwaarde bij deze mogelijkheid voorkomt dat een eventuele corruptering, in het *Persoonsdomein*, van de authorization code of het access token waarbij het verloopmoment verlaat zou worden, leidt tot onterechte toegang tot, of onterechte plaatsing van gezondheidsinformatie. Het accepteren van een authorization code of een access token gebeurt altijd in het licht van de interne administratie van de *Authorization Server*. Die corruptering kan het verloopmoment ook vervroegen, maar richt dan weinig schade aan. Overigens kan in de deze versie van het MedMij Afsprakenstelsel, waarin de geldigheidsduur een vaste waarde heeft, de *OAuth Client* zelf ook al uitrekenen wanneer het geen zin meer heeft een authorization code of access token nog aan te bieden. De meerwaarde van het opnemen van een verloopmoment in de authorization code of het access token zal dus hooguit in mogelijke toekomstige versies kunnen blijken.

De service die het token heeft uitgegeven is al wel in deze versie van het MedMij Afsprakenstelsel een nuttig informatie-element. In situaties waarin een *Resource Server* samenwerkt met meerdere van hem gescheiden geïmplementeerde *Authorization Servers*, moet deze bij een aangeboden access token kunnen bepalen welke *Authorization Server* moet worden aangesproken. Dat aanspreken kan bijvoorbeeld door middel van Token Introspection volgens [RFC7662](#). De geëigende bron voor die informatie is het access token zelf, dat weet heeft van zijn afkomst. Die afkomstinformatie levert geen extra privacyrisico's op, omdat de *OAuth Client* sowieso op de hoogte is van wie hij het access token heeft ontvangen.

Verder mag de *OAuth Authorization Server* ook een kopie van de *scope* opnemen in (de authorization code of) het access token, de *scope* die hij eerder in de authorization request heeft ontvangen van de *OAuth Client* (zie [Authorization interface](#), verantwoordelijkheid 1). Zo hoeft de *Resource Server* niet apart door de *PGO Server* van de *scope* op de hoogte gebracht te worden. De authorization code of het access token draagt zo weliswaar extra betekenis, maar de risico's daarvan wegen niet op tegen de risico's van het apart door de *PGO Server* laten sturen van de *scope*, die bijvoorbeeld zou kunnen afwijken van die waarvoor de authorization code of het access token is uitgegeven.

De lijst van toegestane informatie-elementen is limitatief. Geen andere informatie, ook niet versleuteld, mag in de authorization code of het access token zijn opgenomen. Daaronder vallen zeker ook:

- informatie over *Persoon*;
- informatie over *Zorgaanbieder of Gegevensdienst*, al dan niet in relatie tot *Persoon*, buiten de *scope*;
- benoeming van, en beperkingen aan, de beoogde acceptanten van de authorization code of het access token. Op dit punt is namelijk de *Zorgaanbiederslijst* de autoriteit: als de *OAuth Client* een access token heeft opgehaald op een plek die daartoe in de *Zorgaanbiederslijst* stond, dan moet hij dat access token kunnen aanbieden aan de plek die daartoe in de *Zorgaanbiederslijst* staat.

Het verbod op interpretatie door de *OAuth Client* van authorization code en access token zorgt ervoor dat er een minimale afhankelijkheid wordt gecreëerd tussen de dienstverleners in het Persoonsdomein enerzijds en die in het Zorgaanbiedersdomein anderzijds, zodat principes P1 en P7 maximaal worden nageleefd en interne complexiteit en implementatiekeuzes in het Zorgaanbiedersdomein niet doorschemeren in, of invloed uitoefenen op, de implementatie in het Persoonsdomein.

De beperkingen van betekenisdragendheid van de authorization code en het access token, zelfs indien versleuteld, bevorderen de privacy door middel van dataminimalisatie. Bovendien voorkomen zij nieuwe risico's op compromittering van die informatie-inhoud. Zulke compromittering zou moeilijk te ontdekken en te pareren zijn in het zorgaanbiedersdomein, ingeval men er daar toe besloten zou hebben van interne autorisatie-administratie af te zien omdat de informatie toch al meereist op de authorization code of het access token, via de *OAuth Client*.

9. Het OAuth-client type van de *OAuth Client* is confidential.

#### Toelichting

Om de privacy te kunnen borgen is het van belang dat de *OAuth Authorization Server* voldoende zekerheid heeft over de identiteit van de *OAuth Client*. Die zekerheid is afhankelijk van hoe goed de *OAuth Client* zijn credentials vertrouwelijk kan houden. Daartoe maakt de OAuth-specificatie onderscheid tussen twee client types: confidential en public. De eerste soort kan een voor de *Authorization Server* afdoende mate van vertrouwelijkheid van zijn credentials bieden, de tweede niet. Het is een hoofddoel van MedMij om zulk vertrouwen te borgen in een afsprakenstelsel en niet over te laten aan individuele spelers. Daarom verbindt het MedMij Afsprakenstelsel verantwoordelijkheden aan *Clients* ten behoeve van hun betrouwbaarheid jegens *Authorization Servers*. We verwachten dat een groot deel van de implementaties van de *OAuth Client* (van de *PGO Server* dus) deze vertrouwelijkheid sowieso kunnen bieden, omdat ze de architectuur hebben van wat de OAuth-specificatie *web application* noemt. Andersoortige *PGO Server*-architecturen, zoals die van een app, zijn ook mogelijk, maar alleen onder de voorwaarde dat de *OAuth Client* al het credentials-verkeer in de achtergrond op een server afhandelt, niet via het user device.

#### Lijsten

10a. *MedMij Registratie* en elke *PGO Server* implementeren de use case *UC Opvragen ZAL* met de use case-implementatie *UCI Opvragen ZAL*, door middel van het bepaalde inzake het ZAL interface op GNL-, OCL- en ZAL-interface. Zij gebruiken hiertoe het betreffende stroomdiagram.

10b. *PGO Server* betreft minstens elke vijftien minuten (900 seconden) de meest recente ZAL-implementatie van *MedMij Registratie*.

10c. *PGO Server* valideert elke nieuw verkregen ZAL-implementatie tegen het XML-schema van de *Zorgaanbiederslijst*. Dit XML-schema is een technische implementatie van het MedMij-metamodel.

11a. *MedMij Registratie*, *Authorization Server* en *Notification Client* implementeren de use case *UC Opvragen OCL* met de use case-implementatie *UCI Opvragen OCL*, door middel van het bepaalde inzake het OCL interface op GNL-, OCL- en ZAL-interface. Zij gebruiken hiervoor het betreffende stroomdiagram.

11b. *Authorization Server* en *Notification Client* betrekken minstens elke vijftien minuten (900 seconden) de meest recente OCL-implementatie van *MedMij Registratie*.

11c. *Authorization Server* en *Notification Client* valideren elke nieuwe verkregen *OCN-implementatie* tegen het [XML-schema van de OAuth Client List](#). Dit XML-schema is een technische implementatie van het [MedMij-metamodel](#).

12a. *MedMij Registratie*, *PGO Server* en *Authorization Server* implementeren de use case [UC Opvragen GNL](#) met de use case-implementatie [UCI Opvragen GNL](#), door middel van het bepaalde inzake het GNL interface op [GNL](#)-, [OCN](#)- en [ZAL](#)-interface. Zij gebruiken hiervoor het betreffende [stroomdiagram](#).

12b. *PGO Server* en *Authorization Server* betrekken minstens elke vijftien minuten (900 seconden) de meest recente *GNL-implementatie* van *MedMij Registratie*.

12c. *PGO Server* en *Authorization Server* valideren elke nieuwe verkregen *GNL-implementatie* tegen het [XML-schema van de GNL](#). Dit XML-schema is een technische implementatie van het [MedMij-metamodel](#).

## Beveiliging

13. In het gegevensverkeer voor [UCI Verzamelen](#), [UCI Delen](#), [UCI Abonneren](#), [UCI Notificeren](#), [UCI Opvragen ZAL](#), [UCI Opvragen OCN](#) en [UCI Opvragen GNL](#), maken betrokken rollen gebruik van de functies *Versleuteling*, *Server Authentication* en *Server Authorization*, volgens het bepaalde op de [Netwerklaag](#).

14. De *OAuth Client* en *OAuth Authorization Server* gebruiken voor al hun onderlinge verkeer [PKI-overheid](#)-certificaten, en wel servercertificaten, ten behoeve van de authenticatie van de andere server in een uitwisseling.

### Toelichting

Dit is een maatregel tegen beveiligingsrisico's [4.4.1.1](#), [4.4.1.3](#), [4.4.1.4](#) en [4.4.1.5](#) in [RFC 6819](#). De PKI-certificaten worden in deze release van het MedMij Afsprakenstelsel gebruik voor twee doelen op de [Netwerklaag](#): authenticatie van servers en versleuteling, waarmee de vertrouwelijkheid en integriteit van de inhoud van het gegevensverkeer wordt geborgd.

15. De *OAuth Client* realiseert de volgende beveiligingsmaatregelen, conform [RFC6819](#):

beveiligingsmaatregel	paragraaf in RFC6819	gemitigeerde risico('s)
Clients should use an appropriate protocol, such as OpenID or SAML to implement user login. Both support audience restrictions on clients.	4.4.1.13	4.4.1.13
All clients must indicate their client ids with every request to exchange an authorization "code" for an access token.		
Keep access tokens in transient memory and limit grants.	5.1.6	
Keep access tokens in private memory.	5.2.2	4.1.3
The "state" parameter should be used to link the authorization request with	5.3.5	4.4.1.8

the redirect URI used to deliver the access token.		
CSRF defense and the "state" parameter created with secure random codes should be deployed on the client side. The client should forward the authorization "code" to the authorization server only after both the CSRF token and the "state" parameter are validated.		4.4.1.12

16. De *OAuth Client* realiseert de volgende beveiligingsmaatregelen, conform [RFC6819](#):

beveiligingsmaatregel	paragraaf in <a href="#">RFC6819</a>	gemitigeerde risico('s)
Client applications should not collect authentication information directly from users and should instead delegate this task to a trusted system component, e.g., the system browser.	4.1.4	4.1.4
The client server may reload the target page of the redirect URI in order to automatically clean up the browser cache.	4.4.1.1	4.4.1.1
If the client authenticates the user, either through a single-sign-on protocol or through local authentication, the client should suspend the access by a user account if the number of invalid authorization "codes" submitted by this user exceeds a certain threshold.	4.4.1.12	4.4.1.12
Client developers and end users can be educated to not follow untrusted URLs.	4.4.1.8	4.4.1.8
For newer browsers, avoidance of iFrames during authorization can be enforced on the server side by using the X-FRAME-OPTIONS header. For older browsers, JavaScript frame-busting techniques can be used but may not be effective in all browsers.	5.2.2.6	4.4.1.9
Explain the scope (resources and the permissions) the user is about to grant in an understandable way	5.2.4.2	4.2.2

17. De *OAuth Authorization Server* realiseert de volgende beveiligingsmaatregelen, conform [RFC6819](#):

beveiligingsmaatregel	paragraaf in <a href="#">RFC6819</a>	gemitigeerde risico('s)
Authorization servers should consider such attacks: Password Phishing by Counterfeit Authorization Server	4.2.1	4.2.1
Authorization servers should attempt to educate users about the risks posed by phishing attacks and should provide mechanisms that make it easy for users to confirm the authenticity of their sites.		
Authorization servers should decide, based on an analysis of the risk associated with this threat, whether to detect and prevent this threat.	4.4.1.10	4.4.1.10
The authorization server may force a user interaction based on non-		

predictable input values as part of the user consent approval.		
The authorization server could make use of CAPTCHAs.		
The authorization server should consider limiting the number of access tokens granted per user.	4.4.1.11	4.4.1.11
The authorization server should send an error response to the client reporting an invalid authorization "code" and rate-limit or disallow connections from clients whose number of invalid requests exceeds a threshold.	4.4.1.12	4.4.1.12
Given that all clients must indicate their client ids with every request to exchange an authorization "code" for an access token, the authorization server must validate whether the particular authorization "code" has been issued to the particular client.	4.4.1.13	4.4.1.13
Best practices for credential storage protection should be employed.	5.1.4.1	4.4.1.2
Enforce system security measures.	5.1.4.1.1	4.3.2 en 4.4.1.2
Enforce standard SQL injection countermeasures.	5.1.4.1.2	
Store access token hashes only.	5.1.4.1.3	
The authorization server should enforce a one-time usage restriction.	5.1.5.4	4.4.1.1
If an authorization server observes multiple attempts to redeem an authorization "code", the authorization server may want to revoke all tokens granted based on the authorization "code".	5.2.1.1	
Bind the authorization "code" to the redirect URI.	5.2.4.5	4.4.1.3
the authorization server associates the authorization "code" with the redirect URI of a particular end-user authorization and validates this redirect URI with the redirect URI passed to the token's endpoint,		4.4.1.7

### Toelichting

Voor het opstellen van verantwoordelijkheden 15, 16 en 17 is gebruik gemaakt van [RFC 6819](#) van IETF, dat een uitgebreide inventarisatie van die risico's bevat, inclusief een reeks van maatregelen per risico. Waar het risico van toepassing is op het gebruik van OAuth binnen MedMij, en de maatregelen passen binnen de MedMij-principes, zijn zij opgenomen in het afsprakenstelsel.

Met betrekking tot het gestelde in [sectie 3.1 van RFC 6819](#) kan gesteld worden dat MedMij uitgaat van:

- handles i.p.v. assertions, zodat de *OAuth Resource Server* moet kunnen refereren aan data van de *OAuth Authorization Server*;
- bearer tokens i.p.v. proof tokens. Zie hiervoor verantwoordelijkheid 5 op deze laag.

In [hoofdstuk 4 van RFC 6819](#) staat een uitgebreide lijst van beveiligingsrisico's. Niet van toepassing zijn, voor de deze release van het afsprakenstelsel:



- bedreiging [4.1.2: Obtaining Refresh Tokens](#), omdat het afsprakenstelsel niet met refresh tokens werkt;
- bedreiging [4.2.3: Malicious Client Obtains Existing Authorization by Fraud](#), omdat in het afsprakenstelsel de autorisatie (vooralsnog) strikt eenmalig mag worden gebruikt;
- bedreiging [4.3.4: Obtaining Client Secret from Authorization Server Database](#), omdat authenticatie van *OAuth Clients* in MedMij werkt op basis van PKI-servercertificaten, niet op basis van client secrets;
- bedreiging [4.3.5: Obtaining Client Secret by Online Guessing](#), omdat authenticatie van *OAuth Clients* in MedMij op basis van PKI-servercertificaten wordt gedaan, niet op basis van client secrets.

Wel van toepassing zijn:

- bedreiging [4.1.3: Obtaining Access Tokens](#);
- bedreiging [4.1.4: End-user Credential Phished Using Comprised or Embedded Browser](#);
- bedreiging [4.1.5: Open Redirectors on Client](#);
- bedreiging [4.2.1: Password Phishing by Counterfeit Authorization Server](#);
- bedreiging [4.2.2: User Unintentionally Grants Too Much Access Scope](#);
- bedreiging [4.2.4: Open Redirector](#);
- bedreiging [4.3.1: Eavesdropping Access Tokens](#);
- bedreiging [4.3.2: Obtaining Access Tokens from Authorization Server Database](#);
- bedreiging [4.3.3: Disclosure of Client Credentials during Transmission](#);
- bedreiging [4.1.1: Obtaining Client Secrets](#);
- bedreiging [4.4.1.1: Eavesdropping or Leaking Authorization Code](#);
- bedreiging [4.4.1.2: Obtaining Authorization "codes" from Authorization Server Database](#);
- bedreiging [4.4.1.3: Online Guessing of Authorization "codes"](#);
- bedreiging [4.4.1.4: Malicious Client Obtains Authorization](#);
- bedreiging [4.4.1.5: Authorization "code" Phishing](#);
- bedreiging [4.4.1.6: User Session Impersonation](#);
- bedreiging [4.4.1.7: Authorization "code" Leakage through Counterfeit Client](#);
- bedreiging [4.4.1.8: CSRF against redirect-URI](#);
- bedreiging [4.4.1.9: Clickjacking Attack against Authorization](#);
- bedreiging [4.4.1.10: Resource Owner Impersonation](#);
- bedreiging [4.4.1.11: DoS Attacks That Exhaust Resources](#);
- bedreiging [4.4.1.12: DoS Using Manufactured Authorization "codes"](#);
- bedreiging [4.4.1.13: Code Substitution \(OAuth Login\)](#).

In relatie tot het MedMij Afsprakenstelsel vallen de maatregelen die getroffen moeten worden ter mitigatie van deze risico's uiteen in drie groepen:

- maatregelen waarin al is voorzien door één of meerdere verantwoordelijkheden in het MedMij-afsprakenstelsel, zoals bijvoorbeeld:
  - het gebruik van TLS ([Netwerk-laag](#));
  - het gebruik van een (externe) *Authentication Service* ([Applicatie-laag](#));
  - het beperken van de scope en de geldigheidsduur van authorization codes en access tokens ([Applicatie-laag](#));
  - verantwoordelijkheid 3 op het [Token interface](#);
- maatregelen die weliswaar door [RFC6819](#) worden gesuggereerd, maar niet worden overgenomen in het MedMij Afsprakenstelsel, omdat zij niet passen bij diens principes of bij andere verantwoordelijkheden in het stelsel;
- overige maatregelen, die alsnog getroffen dienen te worden door *PGO Server*, *OAuth Client* of *OAuth Authorization Server* en in verantwoordelijkheden 15-17 staan genoemd.

18. *OAuth Client*, *OAuth Authorization Server* en *OAuth Resource Server* implementeren de op deze respectievelijke rollen toepasselijke beveiligingsmaatregelen, volgens [paragraaf 5.3 van RFC6750](#).

**Toelichting**

Deze verantwoordelijkheid is opgenomen omdat met het bearer token informatie verkregen kan worden zonder dat nogmaals de identiteit wordt gecontroleerd. Daarom moeten maatregelen getroffen worden om te waarborgen dat het token alleen correct gebruikt kan worden.



## Interfaces

### Interfaces en use cases

Op deze pagina's staan de verantwoordelijkheden die horen bij de interfaces in het MedMij Afsprakenstelsel. In elke use case-implementatie wordt gebruik gemaakt van één of meer van deze interfaces. Onderstaande tabel laat zien welke use case-implementaties welk interface gebruiken.

hoofdfunctie	Regie						Uitwisseling
interface	user interface	authorization interface	token interface	subscription interface	subscription notification interface	resource notification interface	resource interface
geboden door rol	Authorization Server			Subscription Server		Notification Server	
UCI Verzamelen	X	X	X				
UCI Delen	X	X	X				
UCI Abonneren	X	X	X	X			
UCI Notificeren					X	X	
UCI Opvragen GNL							
UCI Opvragen OCL							
UCI Opvragen ZAL							

Verantwoordelijkheden over de adressering van deze interfaces komen hieronder aan de orde. Verantwoordelijkheden voor de specifieke interfaces zijn opgenomen in specifieke subpagina's, die klikbaar zijn in bovenstaande tabel.

### Adressering

#### Adressen en interfaces

Op de zes interfaces in de flows van [UCI Verzamelen](#), [UCI Delen](#), [UCI Abonneren](#) en [UCI Notificeren](#), adresseren Applicatie-rollen elkaar, op basis van een URI. Onderstaande tabel geeft een overzicht.

hoofdfunctie	interface	geadresseerde	bericht	kanaal
Regie	<a href="#">authorization interface</a>	Authorization Endpoint van de Authorization	authorization request	frontchannel

		Server		backchannel
		<i>OAuth Client (redirect_uri)</i>	authorization response	
	token interface	<i>Token Endpoint van de Authorization Server</i>	access token request	
	subscription interface	<i>Subscription Endpoint van de Subscription Server</i>	subscription request	
	subscription notification interface	<i>Subscription Notification Endpoint van de Notification Server</i>	subscription notification	
Uitwisseling	resource interface	<i>Resource Endpoint van de Resource Server</i>	resource request	
	resource notification interface	<i>Resource Notification Endpoint van de Notification Server</i>	resource notification	

In de nu volgende verantwoordelijkheden wordt bepaald hoe de URI's zijn opgebouwd waarmee de adresbepaler de adresgebruiker de geadresseerde laat adresseren, en hoe de parameters worden gevuld. De opbouw van het adres is steeds dezelfde, ook voor frontchannel en backchannel. Desondanks maken we in het [logische informatiemodel](#), in de *Zorgaanbiederslijst*, wel onderscheid tussen *Frontchanneluri* en *Backchanneluri*. Dat houdt dat model wendbaarder, mocht er ooit wel adresseringsverschillen tussen frontchannel en backchannel ontstaan.

1a. De *OAuth Client* stelt conform [RFC 3986](#) de URI samen waarmee hij zichzelf, de *Authorization Server*, de *Subscription Server* of de *Resource Server* adresseert. De *Notification Client* stelt conform [RFC 3986](#) de URI samen waarmee hij de *Notification Server* adresseert.

1b. De URI's bedoeld in verantwoordelijk 1a hebben een hostname die een fully-qualified domain name is, conform [RFC3696, sectie 2](#), en heeft het patroon `scheme://host path`, waarbij:

- `scheme` altijd `https` is, in lowercase;
- `host` een hostname is waarin
  - slechts de karakters [a-z], [0-9], "." (punt) en "-" (koppelteken) voorkomen;
  - elke punt twee opeenvolgende segmenten scheidt en van elk der gescheiden segmenten geen deel uitmaakt;
  - het eerste karakter van een segment geen koppelteken is;
  - elk segment minstens één karakter lang is;
  - het laatste segment minstens twee karakters lang is;
  - het laatste karakter geen koppelteken mag zijn;
  - maximaal 255 tekens voorkomen;
  - ten minste twee segmenten voorkomen;
- `path` de syntax heeft van `path-abempty` uit [sectie 3.3 van RFC 3986](#) (en dus leeg mag zijn), maar niet eindigt op een `/`.

### Toelichting

De eis dat `https` in lowercase staat volgt de canonical form zoals gespecificeerd in [sectie 3.1 van RFC 3986](#). De eisen aan de hostname zijn o.a. gebaseerd op [RFC 952](#) en [RFC 1123](#). Het laatste segment is het zogeheten top-level domain.

2a. In alle adressering op het [authorization interface](#), het [token interface](#), het [subscription interface](#), het [subscription notification interface](#), het [resource notification interface](#) en het [resource interface](#) is het gebruik van het voor `https` bedoelde poortnummer, zoals opgenomen in de [Service Name and Transport Protocol Port Number Registry](#) van IANA, verplicht.

### Toelichting

Dat geldt dus ook voor de `redirect_uri`.

In release 1.1.1 van het MedMij Afsprakenstelsel was deze verantwoordelijkheid alleen van toepassing op frontchannel-verkeer en had de *Dienstverlener Zorgaanbieder* voor backchannelverkeer de vrijheid om een ander poortnummer te kiezen dan dat conform de IANA-lijst bij `https` hoort (443). Dat zorgt echter voor een extra beveiligingsbeheerlast bij de *PGO Server* die rekening houden met meerdere bestemmingspoortnummers bij uitgaand verkeer. Die beheerst brengt indirect ook extra beveiligingsrisico's met zich mee. Daartegenover staat dat de in deze release aangebrachte aanscherping naar verwachting geen wezenlijke beperking voor *Dienstverleners Zorgaanbieder* zal zijn, omdat zij toch al gebruik maken van het voor `https` bedoelde poortnummer uit de IANA-lijst. Een mogelijke uitzondering vormt de situatie waarin de *Authorization Server* en/of *Resource Server* in een multi-tenant omgeving draaien.

2b. Voor het samenstellen van alle adressen van het authorization request, het token request, het subscription request en het resource request, betreft de *OAuth Client* de eerste onderdelen van de URI, namelijk `host` en `path`, uit de *Zorgaanbiederslijst*, op basis van de van toepassing zijnde *Zorgaanbieder* en hetzij *Gegevensdienst* (wanneer geadresseerde *Authorization Server* is) of *Systeemrol* (wanneer geadresseerde *Resource Server* is). Andere elementen van de algemene URI-syntax, zoals `user`, `password`, `query` en `fragment`, zijn afwezig in de adressen.

2c. De adressen voor de subscription notification en de resource notification betreft de *Notification Client* uit de *OAuth Client List*, op basis van de van toepassing zijnde *OAuth Client* en *Gegevensdienst*.

### Zorgaanbiederslijst en OAuth Client List

De *Zorgaanbiederslijst* wordt dus gebruikt door de *OAuth Client* om, gegeven een zekere *Interfaceversie*, het endpoint te kennen dat past bij de van toepassing zijnde *Zorgaanbieder*, *Gegevensdienst* en, voor het resource endpoint, *Systeemrol*. Net zo gebruikt de *Notification Client* de *OAuth Client List* om, gegeven een zekere *Interfaceversie*, het endpoint te kennen dat past bij de van toepassing zijnde *OAuth Client* en *Gegevensdienst*. Daarom moet er uit één zo'n setje één endpoint-adres volgen. Andersom echter is dat geen eis. Het is mogelijk om, in elke door de *Dienstverlener zorgaanbieder* gewenste combinatie, endpointadressen te hergebruiken voor meerdere van zulke setjes in de *Zorgaanbiederslijst*, respectievelijk door de *Dienstverlener persoon* in de *OAuth Client List*.

3. *MedMij Registratie* wordt in *UCI Opvragen ZAL*, *UCI Opvragen OCL* en *UCI Opvragen GNL* geadresseerd met de hostname [stelselnode.medmij.nl](https://stelselnode.medmij.nl).

## User interface (verklaringen)

### Toelichting

Het user interface hoort bij de [hoofdfunctie Regie](#).

1a. De vraag die aan de *Zorggebruiker* gesteld moet worden in de stap "autoriseer" in [UCI Verzamelen](#) staat gespecificeerd op de pagina [Toestemmingsverklaring](#). Daarbij geldt dat:

- de gebruikersvriendelijke weergave van de identiteit van de *Zorgaanbieder* (NaamZorgaanbieder) wordt bepaald door de betreffende *Dienstverlener Zorgaanbieder*, in haar dienstverleningsrelatie met de betreffende *Zorgaanbieder*;
- de gebruikersvriendelijke weergave van de *Gegevensdienst* (NaamGegevensdienst) wordt betrokken uit de scope die de *Authorization Server* in de allereerste stap van de flow heeft gekregen, die overeenkomt met de *Weergavenaam* die bij de betreffende *Gegevensdienst* in de *Gegevensdienstnamenlijst* is opgenomen;
- de gebruikersvriendelijke weergave van de identiteit van de *Uitgever* (NaamLeverancierPGO) wordt betrokken uit de *OAuth Client List*, op basis van de *redirect\_uri* (van OAuth) die in stap 1 is verkregen.

1b. De vraag die aan de *Zorggebruiker* gesteld moet worden in de stap "bevestig" in [UCI Delen](#) staat gespecificeerd op de pagina [Bevestigingsverklaring](#). Daarbij geldt dat:

- de gebruikersvriendelijke weergave van de identiteit van de *Zorgaanbieder* (NaamZorgaanbieder) wordt bepaald door de betreffende *Dienstverlener Zorgaanbieder*, in haar dienstverleningsrelatie met de betreffende *Zorgaanbieder*;
- de gebruikersvriendelijke weergave van de *Gegevensdienst* (NaamGegevensdienst) wordt betrokken uit de scope die de *Authorization Server* in de allereerste stap van de flow heeft gekregen, die overeenkomt met de *Weergavenaam* die bij de betreffende *Gegevensdienst* in de *Gegevensdienstnamenlijst* is opgenomen;
- de gebruikersvriendelijke weergave van de identiteit van de *Uitgever* (NaamLeverancierPGO) wordt betrokken uit de *OAuth Client List*, op basis van de *redirect\_uri* (van OAuth) die in stap 1 is verkregen.

1c. De vraag die aan de *Zorggebruiker* gesteld moet worden in de stap "autoriseer" in [UCI Abonneren](#) staat gespecificeerd op de pagina [Toestemmingsverklaring Abonneren](#). Daarbij geldt dat:

- de gebruikersvriendelijke weergave van de identiteit van de *Zorgaanbieder* (NaamZorgaanbieder) wordt bepaald door de betreffende *Dienstverlener Zorgaanbieder*, in haar dienstverleningsrelatie met de betreffende *Zorgaanbieder*;
- de aangeboden looptijd van het Abonnement (*Duur*) door de beleid van de *Zorgaanbieder* wordt bepaald, op basis van de door de *Persoon* gevraagde looptijd, en nooit langer dan de maximale looptijd die in de *Catalogus* bij de betreffende *Gegevensdienst* staat genoemd;
- de gebruikersvriendelijke weergave van de *Gegevensdienst* (NaamGegevensdienst) wordt betrokken uit de scope die de *Authorization Server* in de allereerste stap van de flow heeft gekregen, die overeenkomt met de *Weergavenaam* die bij de betreffende *Gegevensdienst* in de *Gegevensdienstnamenlijst* is opgenomen;
- de gebruikersvriendelijke weergave van de identiteit van de *Uitgever* (NaamLeverancierPGO) wordt betrokken uit de *OAuth Client List*, op basis van de *redirect\_uri* (van OAuth) die in stap 1 is verkregen.

### Toelichting

NaamZorgaanbieder, NaamGegevensdienst en NaamLeverancierPGO zijn placeholders, zoals opgenomen in de [Toestemmingsverklaring](#) en de [Bevestigingsverklaring](#).

Duur is een placeholder, zoals opgenomen in de [Toestemmingsverklaring Abonneren](#).

## Authorization interface

### Toelichting

Het authorization interface hoort bij de [hoofdfunctie Regie](#).

Op deze pagina staan alleen de verantwoordelijkheden inzake het authorization interface die nog niet genoemd staan in de [OAuth 2-specificatie](#).

1a. De parameters in de authorization request worden als volgt gevuld:

parameter	vulling	toelichting
response_type	letterlijke waarde code	Dit is het gevolg van verantwoordelijkheid 4 op de <a href="#">Applicatielaag</a> .
client_id	de hostname, die in de <i>OAuth Client List</i> is opgenomen, van de <i>Node</i> van de <i>OAuth Client</i> die de authorization request doet	
redirect_uri	<ol style="list-style-type: none"> <li>zodanig dat de erin opgenomen hostname gelijk is aan de <code>client_id</code> en er geen poortnummer is opgenomen</li> <li>de <code>redirect_uri</code> moet volledig zijn en verwijzen naar een <code>https</code>-beschermde endpoint</li> </ol>	<p>Zie verantwoordelijkheden 1 en 2a op de pagina <a href="#">Interfaces</a>.</p> <p>De tweede eis is een maatregel tegen beveiligingsrisico's <a href="#">4.1.5</a>, <a href="#">4.2.4</a>, <a href="#">4.4.1.1</a>, <a href="#">4.4.1.5</a> en <a href="#">4.4.1.6</a> in RFC 6819. Zie bovendien <a href="#">Token interface</a>, de toelichting onder verantwoordelijkheid 4.</p>
scope	<p>optioneel:</p> <ul style="list-style-type: none"> <li>de letterlijke waarde <code>subscribe</code></li> <li>gevolgd door een tilde ~</li> <li>gevolgd door een niet-negatief geheel getal, aangevende de gevraagde maximale duur van het <i>Abonnement</i></li> <li>gevolgd door een forward slash /</li> </ul> <p>gevolgd door, verplicht:</p> <ul style="list-style-type: none"> <li>de betreffende (één) <i>Zorgaanbiedernaam</i>,</li> </ul>	<p>De scope bestaat dus uit een optioneel deel gevolgd door twee verplichte onderdelen.</p> <p>Het optionele deel wordt gebruikt voor het aangaan, verlengen of beëindigen van een <i>Abonnement</i>. Als de gevraagde maximale duur van het <i>Abonnement</i> 0 is, betekent dat het verzoek om het beëindigen van het eventuele <i>Abonnement</i> op die <i>Gegevensdienst</i> bij die <i>Zorgaanbieder</i>.</p> <p>De twee verplichte delen volgen op het eventuele optionele deel en bestaat zelf uit twee, gescheiden door een tilde. Er mag in deze versie van het MedMij Afsprakenstelsel slechts sprake zijn van één van elk. Bij interpretatie van de <i>Zorgaanbiedernaam</i> door de ontvanger zal deze de suffix <code>@medmij</code> weer moeten toevoegen.</p>

	<p>ontdaan van de suffix @medmij, gevolgd door</p> <ul style="list-style-type: none"> <li>• een tilde (~), gevolgd door</li> <li>• het <i>GegevensdienstId</i> van de betreffende (één) <i>Gegevensdienst</i> uit de <i>Gegevensdienstnamenlijst</i>.</li> </ul>	<p>Er worden geen andere scopes of onderdelen van scopes opgenomen dan de hier genoemde.</p> <p>Voorbeelden van syntactisch juiste scopes zijn:</p> <ul style="list-style-type: none"> <li>• eenofanderezorgaanbieder~42, voor het eenmalig afnemen van <i>Gegevensdienst</i> 42 bij eenofanderezorgaanbieder@medmij;</li> <li>• subscribe~180 /eenofanderezorgaanbieder~42, voor het aangaan van een <i>Abonnement</i> op <i>Gegevensdienst</i> 42 bij eenofanderezorgaanbieder@medmij van maximaal 180 dagen, of het aanpassen van het <i>Abonnement</i> op <i>Gegevensdienst</i> 42 bij eenofanderezorgaanbieder@medmij naar maximaal 180 dagen vanaf vandaag;</li> <li>• subscribe~0 /eenofanderezorgaanbieder~42, voor het beëindigen van het <i>Abonnement</i> op <i>Gegevensdienst</i> 42 bij eenofanderezorgaanbieder@medmij.</li> </ul>
state	<ol style="list-style-type: none"> <li>1. conform <a href="#">sectie 4.1.1. van RFC 6749</a></li> <li>2. de waarde mag geen URI bevatten</li> </ol>	<p>Hiermee geeft de <i>OAuth Client</i> informatie mee aan de <i>OAuth Authorization Server</i>, waaraan eerstgenoemde later, bij de redirect, kan afleiden bij welk verzoek de authorization code hoort. Deze informatie is verder betekenisloos voor de <i>OAuth Authorization Server</i>.</p> <p>De tweede eis is een maatregel tegen beveiligingsrisico <a href="#">4.1.5</a>. De <i>state</i>-parameter mag niet bedoeld zijn om te worden toegevoegd aan, of anderszins verwerkt in de <i>redirect_uri</i>.</p>

1b. De *OAuth Client* zorgt ervoor dat voor het authorization request de http-methode GET wordt gebruikt, niet POST.

#### Toelichting

In de [OAuth-specificatie, sectie 3.1](#) wordt de Authorization Server verplicht gesteld GET te accepteren en wordt POST optioneel gehouden. Omdat GET de verreweg meest in het MedMij Afsprakenstelsel passende http-methode is voor de authorization request, geldt, om de *Authorization Server* niet voor onnodige implementatiekosten te plaatsen, deze verantwoordelijkheid. Hoewel deze verantwoordelijkheid een verantwoordelijkheid van de *OAuth Client* is, omdat deze onder de verantwoordelijkheid van een MedMij-deelnemer valt, wordt de request uiteindelijk door de *OAuth User Agent* uitgevoerd.

2. Na ontvangst van een authorization request met een zekere *client\_id* en met een zekere *Zorgaanbieder* en *GegevensdienstId* in de *scope*, verifieert de *Authorization Server* dat:



- deze *Gegevensdienst* voorkomt bij de betreffende `client_id` op de *OAuth Client List*,
- zij namens deze *Zorgaanbieder* deze *Gegevensdienst* ontsluit, blijkens de *Zorgaanbiederslijst*,
- indien in de scope ook `subscribe` voorkomt:
  - bij de betreffende `client_id` en *Gegevensdienst* op de *OAuth Client List* ook een subscription notification endpoint en een resource notification endpoint voorkomen;
  - zij namens deze *Zorgaanbieder* ook *Abonnementen* op deze *Gegevensdienst* ontsluit, blijkens de *Zorgaanbiederslijst*.

Slagen niet al deze verificaties, dan behandelt de *Authorization Server* dit als uitzondering 1b volgens verantwoordelijkheid 6.

#### Verificatie van erkenning op Gegevensdienst

Zo voorkomt de *Authorization Server* dat eigevoig wordt gegeven aan een verzoek dat blijkens de *OAuth Client List* of *Zorgaanbiederslijst* niet is toegestaan.

3. Tijdens de afhandeling van een authorization request laat de *Authorization Server*, in zijn rol als *Authentication Client*, voordat hij de *Zorggebruiker* om OAuth-autorisatie vraagt, de *Zorggebruiker* authenticeren door de *Authentication Service*.

#### Authenticatie

Conform [stroomdiagram](#) onder 1. De zorgaanbieder in het Zorgaanbieders- en dus BSN-domein is verplicht bij het verstrekken van gegevens vanuit een gezondheidsdossier de identiteit van de persoon te verifiëren aan de hand van het BSN.

Het MedMij Afsprakenstelsel brengt het gebruik van de *Authentication Service* onder in de OAuth-flow, onder operationele verantwoordelijkheid van de *Authorization Server*. Laatstgenoemde handelt in dezen onder verantwoordelijkheid van individuele *Zorgaanbieders*, want die zijn het waarvoor de *Persoon* zich authenticceert.

De directe interactie van de *Persoon* met de *Authorization Server* is bedoeld om de *PGO Server* te autoriseren om de *Resource Server* aan te spreken. Die levert de uiteindelijke *Gegevensdienst* pas.

4. Onmiddellijk na authenticatie van de *Zorggebruiker*, zoals bedoeld in verantwoordelijkheid 3, en alleen als deze slaagt, vraagt de *OAuth Authorization Server* de *Zorggebruiker* om een [Toestemmingsverklaring](#) (in het geval van [UCI Verzamelen](#) of [UCI Abonneren](#)) of een [Bevestigingsverklaring](#) (in het geval van [UCI Delen](#)), volgens het daaromtrent bepaalde op de pagina [User interface \(verklaringen\)](#), volgens de standaard [OAuth 2.0](#), op de wijze waarop deze in het MedMij Afsprakenstelsel wordt toegepast.

5. Voorafgaand aan uitgifte van een authorization code via de in de authorization request opgenomen `redirect_uri`, administreert de *OAuth Authorization Server* die authorization code en de daarvoor gebruikte `redirect_uri`.

#### Toelichting

Dit is een maatregel tegen beveiligingsrisico's [4.4.1.3](#), [4.4.1.5](#) en [4.4.1.7](#) uit RFC 6819 (zie [Applicatie-laag](#), verantwoordelijkheid 18). Zie verantwoordelijkheid 4 bij het [Token interface](#).

6. *Authorization Server* en *PGO Server* behandelen uitzonderingssituaties inzake het authorization interface af volgens onderstaande tabel.

Nummer	Implementeert uitzonderingen	Uitzondering	Actie	Melding
Authorization interface 1a	UC Verzamelen 1 UC Delen 1 UC Abonneren 1	<i>Authorization Server</i> ontvangt een authorization request zonder (geldige) <code>redirect_uri</code> en/of zonder een (geldige) <code>client_id</code> .	<i>Authorization Server</i> informeert <i>PGO Presenter</i> over deze uitzondering. <i>Authorization Server</i> voert geen redirect naar de <i>Client</i> uit, ook niet met een foutmelding.	conform <a href="#">OAuth 2.0-specificatie</a> , par. 4.1.2.1
Authorization interface 1b		<i>Authorization Server</i> ontvangt een ongeldige authorization request, anders dan uitzondering 1.	<i>Authorization Server</i> informeert <i>PGO Server</i> over deze uitzondering. <i>PGO Server</i> informeert <i>Zorggebruiker</i> daarover.	conform <a href="#">OAuth 2.0-specificatie</a> , par. 4.1.2.1, met de daar genoemde toepasselijke error code
Authorization interface 2	UC Verzamelen 2 UC Delen 2 UC Abonneren 2	<i>Authorization Server</i> kan de identiteit van de <i>Zorggebruiker</i> niet vaststellen.	<i>Authorization Server</i> informeert <i>PGO Server</i> over deze uitzondering. <i>PGO Server</i> informeert <i>Zorggebruiker</i> dat diens verzoek geen voortgang kan vinden, maar laat de oorzaak daarvan helemaal in het midden.	conform <a href="#">OAuth 2.0-specificatie</a> , par. 4.1.2.1, error code <code>access denied</code> , met in de error description "Access denied."
Authorization interface 3	UC Verzamelen 3 UC Delen 3 UC Abonneren 3	<i>Authorization Server</i> stelt tijdens de afhandeling van de authorization request vast dat: <ul style="list-style-type: none"> <li>in geval van <a href="#">UCI Verzamelen</a>: van <i>Persoon</i> bij <i>Zorgaanbieder</i> geen gezondheidsinformatie voor die <i>Gegevensdienst</i> beschikbaar is;</li> <li>in geval van <a href="#">UCI Delen</a>: <i>Zorgaanbieder</i> niet ontvankelijk is voor die <i>Gegevensdienst</i> van <i>Persoon</i>;</li> <li>in geval van <a href="#">UCI Abonneren</a>:</li> </ul>		

		<p><i>Zorgaanbieder geen Notificaties beschikbaar maakt voor Persoon op die Gegevensdienst.</i></p> <p>Zie de toelichting op <a href="#">Beschikbaarheids- en ontvankelijkheidsvoorwaarde</a>.</p>		
Authorization interface 4	UC Verzamelen 4  UC Delen 4  UC Abonneren 4	De autorisatievraag wordt ontkennend beantwoord.		
Authorization interface 5	UC Verzamelen 5  UC Delen 5  UC Abonneren 5	<i>Authorization Server</i> kan de autorisatie niet vaststellen.	<i>Authorization Server</i> informeert <i>PGO Server</i> over deze uitzondering. <i>PGO Server</i> informeert daarop <i>Zorggebruiker</i> hierover.	conform <a href="#">OAuth 2.0-specificatie</a> , par. 4.1.2.1, error code access denied, met in de error description "Authorization failed."

### Toelichting

De uitzonderingssituaties kunnen gezien worden als de implementatie-tegenhangers van de uitzonderingen van de [UC Verzamelen](#) en de [UC Delen](#). Op de Applicatielaag zijn deze echter per interface geordend. Alle uitzonderingen worden door de *Authorization Server* ontdekt. In deze versie van het MedMij Afsprakenstelsel is bepaald dat zij altijd leiden tot het zo snel mogelijk afbreken van de flow door alle betrokken rollen. Daartoe moeten echter eerst nog de andere rollen geïnformeerd worden. Om te voorkomen dat de *PGO Server* informatie over het bestaan van behandelrelaties verkrijgt zonder dat daarvoor (al) toestemming is gegeven, moet het onderscheid tussen de uitzonderingen 2, 3 en 4 niet te maken zijn door de *PGO Server*.

Deze tabel bevat alleen die uitzonderingssituaties ten aanzien waarvan het MedMij afsprakenstelsel eigen eisen stelt aan de implementatie. In de [specificatie van OAuth 2.0](#) staan daarnaast nog generiekere uitzonderingssituaties, zoals de situatie waarin de redirect URI ongeldig blijkt. Ook deze uitzonderingssituaties moeten geïmplementeerd worden.

## Token interface

### Inleiding

Op deze pagina staan alleen de verantwoordelijkheden inzake het token interface die nog niet genoemd staan in de [OAuth 2-specificatie](#).

1. De parameters in de access token request worden als volgt gevuld:

parameter	vulling	toelichting
grant_type	letterlijke waarde "authorization_code"	Dit is het gevolg van verantwoordelijkheid 4 op de <a href="#">Applicatielaag</a> .
code	conform verantwoordelijkheid 8a-d op de <a href="#">Applicatielaag</a>	Zie de toelichting bij verantwoordelijkheid 8a-d op de <a href="#">Applicatielaag</a> .
client_id	de hostname van de <i>Node</i> van de <i>OAuth Client</i> die de authorization request deed die de nu aangeboden authorization code opleverde	De <a href="#">OAuth 2.0-specificatie</a> stelt deze parameter niet verplicht indien de <i>OAuth Client</i> zich authenticceert, hetgeen in het MedMij Afsprakenstelsel gebeurt door middel van mutual TLS. En de noodzaak van het gebruik ervan wordt beperkt door verantwoordelijkheid 4 op deze pagina, die borgt dat het access token alleen wordt verstrekt aan de <i>OAuth Client</i> aan wie de <i>OAuth Resource Owner</i> toestemming heeft verleend. In <a href="#">hoofdstuk 2 van een Internet-Draft ter zake</a> wordt echter gesteld dat de <code>client_id</code> toch gebruikt moet worden ingeval mutual TLS wordt gebruikt. Dat laatste is het geval in het MedMij Afsprakenstelsel (zie <a href="#">Netwerk-laag</a> ).
redirect_uri	dezelfde waarde als in de voorafgaande authorization request	

2. De parameters in de [access token response](#) worden als volgt gevuld:

parameter	vulling	toelichting
access_token	Het hiermee uitgegeven access token.	
token_type	letterlijke waarde "Bearer"	
expires_in	900	Conform verantwoordelijkheid 7 op de <a href="#">Applicatie-laag</a> .
refresh_token	<b>niet gebruikt</b>	Conform verantwoordelijkheid

		7 op de <a href="#">Applicatie-laag</a> .
scope	<p>Conform <a href="#">sectie 5.1 van de OAuth 2.0-specificatie</a>.</p> <p>In toevoeging daarop: verplicht indien het authorization request verzocht om een <i>Abonnement</i>. In dat geval is de scope-parameter gelijk aan die in de betreffende <a href="#">authorization request</a>, maar met de <i>Abonnements-duur</i> gesteld op de door de <i>Authorization Server</i> toegekende, en dus mogelijk beperkte, waarde, in hele dagen vanaf vandaag. De toegekende duur van het <i>Abonnement</i> is:</p> <ul style="list-style-type: none"> <li>• niet hoger dan de in de authorization request gevraagde duur van het <i>Abonnement</i>;</li> <li>• niet hoger dan de maximale abonnementsduur die de Zorgaanbieder in de Zorgaanbiederslijst had opgenomen bij die <i>Gegevensdienst</i> en die <i>Interfaceversie</i>;</li> <li>• bij een gevraagde beëindiging gelijk aan 0.</li> </ul>	

#### Maximale duur

Omdat een *Zorgaanbieder* in de *Zorgaanbiederslijst* geen maximale abonnementsduur mag opnemen die de maximale abonnementsduur bij de betreffende *Gegevensdienst* in de [Catalogus](#) overschrijdt, kan in de scope dus ook geen feitelijke abonnementsduur verschijnen die de maximale abonnementsduur bij de betreffende *Gegevensdienst* in de [Catalogus](#) overschrijdt.

3. De *OAuth Client* biedt een zekere authorization code maximaal eenmaal aan aan de *Authorization Server* ter verkrijging van een access token. De *Authorization Server* voert een authorization code af, wanneer het eenmaal is aangeboden ter verkrijging voor een access token.

#### Toelichting

Dit is een maatregel tegen [beveiligingsrisico 4.1.1](#) uit RFC 6819 (zie [Applicatie-laag](#), toelichting bij verantwoordelijkheden 15-17). Het afvoeren van een authorization code houdt in dat de *Authorization Server* van een eenmaal uitgegeven authorization code bijhoudt of die al eens gebruikt is voor het verkrijgen van een access token. Mocht een authorization code voor een tweede of volgende keer worden aangeboden ter verkrijging van een access token, dan zal de *Authorization Server* dat weigeren en de flow afbreken. Als de *Client* aan wie die geweigerd wordt te kwader trouw was, is hiermee een gevaar afgewend. Was hij wel te goeder trouw en handelde hij conform het MedMij Afsprakenstelsel, dan was hij niet degene die al eerder dezelfde authorization code aanbood en blijkt er dus sprake geweest te zijn van een security breach.

4. De *OAuth Authorization Server* draagt geen access token over als in de token request geen `redirect_uri` is opgenomen, en evenmin als er in de token request wel een `redirect_uri` is opgenomen, maar deze niet identiek is aan de `redirect_uri` die de *OAuth Authorization Server*, bij uitreiking, verbonden heeft aan de authorization code die in de token request wordt aangeboden.

#### Toelichting

Dit is een maatregel tegen beveiligingsrisico's [4.4.1.3](#), [4.4.1.5](#) en [4.4.1.7](#) uit RFC 6819 (zie [Applicatie-laag, verantwoordelijkheid 18](#)).

Met het oog op de parameters `client_id` en `redirect_uri` in de authorization request en de access token request geldt dat:

- de `client_id` in de authorization request overeen moet komen met de hostname van de `redirect_uri` in diezelfde authorization request (verantwoordelijkheid 1 bij [Authorization interface](#));
- de `redirect_uri` in de access token request overeen moet komen met de `redirect_uri` in de authorization request (deze verantwoordelijkheid).

In de access token request speelt de `redirect_uri` dan niet de rol van adressering van de response, zoals in de authorization request wel, maar enkel als terugverwijzing naar de `redirect_uri` van het [Authorization interface](#). Bij de afhandeling van het [Token interface](#) wordt helemaal niet geredirect; die speelt zich geheel op het backchannel af.

5. Na ontvangst van een access token request, in *UCI Verzamelen* of *UCI Delen*, zal de *OAuth Authorization Server*, indien in antwoord daarop een access token dient te worden uitgegeven, na maximaal tien (10) seconden dit access token ter beschikking stellen aan de *OAuth Client*. Dit gedrag van de *OAuth Authorization Server* is gedurende minimaal 99,5% van de tijd beschikbaar.

6. *OAuth Authorization Server* en *OAuth Client* behandelen uitzonderingssituaties inzake het token interface volgens onderstaande tabel.

Nummer	Implementeert uitzondering	Uitzondering	Actie	Melding	Vervolg
Token interface 1	UC Verzamelen 6 UC Delen 6 UC Abonneren 6	<i>Authorization Server</i> moet vanwege één van de in de <a href="#">OAuth 2.0-specificatie</a> , par. 5.2, genoemde redenen de token request weigeren.	<i>Authorization Server</i> informeert <i>PGO Server</i> over deze uitzondering. <i>PGO Server</i> informeert daarop <i>Zorggebruiker</i> hierover.	met de conform <a href="#">OAuth 2.0-specificatie</a> , par. 5.2, toepasselijke error code	Allen stoppen de flow van de <i>UCI Verzamelen/UCI Delen</i> onmiddellijk na geïnformeerd te zijn over de uitzondering.
Token interface 2	UC Verzamelen 3 UC Delen 3 UC Abonneren 3	<i>Authorization Server</i> stelt tijdens de afhandeling van de token request vast dat: <ul style="list-style-type: none"> <li>• in geval van <i>UCI Verzamelen</i>: van <i>Persoon</i> bij <i>Zorgaanbieder</i> geen gezondheidsinformatie voor die <i>Gegevensdienst</i> beschikbaar is.</li> </ul>	<i>Authorization Server</i> informeert <i>PGO Server</i> over deze uitzondering. <i>PGO Server</i> informeert <i>Zorggebruiker</i> dat diens verzoek geen voortgang kan vinden,	conform <a href="#">OAuth 2.0-specificatie</a> , par. 4.1.2.1, error code <code>access denied</code> , met in de error description "Access denied."	

	<ul style="list-style-type: none"> <li>in geval van <i>UCI Delen</i>: <i>Zorgaanbieder</i> niet ontvankelijk is voor die <i>Gegevensdienst</i> van <i>Persoon</i>.</li> </ul> <p>Zie de toelichting op <a href="#">Beschikbaarheids- en ontvankelijkheidsvoorwaarde</a>.</p>	<p>maar laat de oorzaak daarvan helemaal in het midden.</p>	
--	--	---	--

### Toelichting

De uitzonderingssituaties kunnen gezien worden als de implementatie-tegenhangers van de uitzonderingen van de [UC Verzamelen](#) en de [UC Delen](#). Op de Applicatielaag zijn deze echter per interface geordend. Alle uitzonderingen worden door de *Authorization Server* ontdekt. In deze versie van het MedMij Afsprakenstelsel is bepaald dat zij altijd leiden tot het zo snel mogelijk afbreken van de flow door alle betrokken rollen. Daartoe moeten echter eerst nog de andere rollen geïnformeerd worden.

Deze tabel bevat alleen die uitzonderingssituaties ten aanzien waarvan het MedMij afsprakenstelsel eigen eisen stelt aan de implementatie. In de [specificatie van OAuth 2.0](#) staan daarnaast nog generiekere uitzonderingssituaties, zoals de situatie waarin de redirect URI ongeldig blijkt. Ook deze uitzonderingssituaties moeten geïmplementeerd worden.

## Resource interface

### Inleiding

Het resource interface hoort bij de [hoofdfunctie Uitwisseling](#).

Op deze pagina staan alleen de verantwoordelijkheden inzake het resource interface die nog niet genoemd staan in:

- de [OAuth 2-specificatie](#);
- de informatiestandaard van de *Gegevensdienst* die op het resource interface wordt aangesproken.

1. De *OAuth Client* gebruikt voor het sturen van het acces token, in de resource request, de methode `Authorization Request Header Field`, zoals beschreven in sectie 2.1 van RFC6750.

### Toelichting

De methode `Authorization Request Header Field` biedt de beste beveiliging.

2. Na ontvangst van een resource request, in *UCI Verzamelen* of *UCI Delen*, zal de *Resource Server*, indien in antwoord daarop een resource response dient te worden gedaan, na maximaal zestig (60) seconden dit resource response ter beschikking stellen aan de *PGO Server*. Dit gedrag van de *Resource Server* is gedurende minimaal 98,5% van de tijd beschikbaar.

3. Voor zover er in het verkeer tussen *PGO Server* en *Resource Server* in de use case-implementaties *UCI Verzamelen* en *UCI Delen* sprake is, in de stuurgegevens, van een gegevenselement dat tot de identiteit van de *Zorggebruiker* herleid kan worden, gebruiken zij daarvoor niets anders dan de OAuth-gegevens die zij in hun respectievelijke *OAuth Client* en *OAuth Resource Server* moeten uitwisselen. *PGO Server*, *Authorization Server* en *Resource Server* treffen goed beveiligde voorzieningen waarmee zij hieruit waar nodig zelf de identiteit van de *Zorggebruiker* kunnen vaststellen.

### Toelichting

Met het oog op het borgen van de privacy en het zo eenvoudig mogelijk houden van de architectuur van het MedMij Afsprakenstelsel, wordt ervoor gekozen de identifier voor de *Zorggebruiker* onderweg zo betekenisloos mogelijk te houden. Alle betekenis wordt er ter weerszijden aan verbonden door raadpleging van interne registraties. Omdat de *PGO Server*, *Authorization Server* en *Resource Server* samen een OAuth-flow afhandelen, beschikken zij (na authenticatie van de *Zorggebruiker*) over tokens die de identiteit van de *Zorggebruiker* vertegenwoordigen, namelijk (eerst) de authorization code en (later) het access token. Buiten deze hoeft en zal er geen identificerende gegevenselementen in het verkeer worden opgenomen. Het FHIR-gegevenselement *PatientID* wordt *niet* gebruikt.

4. *OAuth Resource Server* en *OAuth Client* behandelen uitzonderingssituaties inzake het resource interface af volgens onderstaande tabel.



Nummer	Implementeert uitzondering	Uitzondering	Actie	Melding	Vervolg
Resource interface 1	UC Verzamelen 6, UC Delen 6	De validatie van het access token door <i>Resource Server</i> faalt.	<i>Resource Server</i> informeert <i>PGO Server</i> over deze uitzondering. <i>PGO Server</i> informeert daarop <i>Zorggebruiker</i> hierover.	als <i>OperationOutcome</i> conform FHIR- specificatie, analoog aan uitzondering Resource interface 2, maar met issue type "security" of "suppressed".	Allen s de flow onmid na geïnf te zijn de uitzon
Resource interface 2	UC Verzamelen 5, UC Delen 5	<i>Resource Server</i> kan in de request niet, niet geheel of niet tijdig voorzien, om redenen anders dan uitzondering Resource interface 1.  Zie ook de toelichting op <a href="#">Beschikbaarheids- en ontvankelijkheidsvoorwaarde</a> .	<i>Resource Server</i> informeert <i>PGO Server</i> over deze uitzondering. <i>PGO Server</i> informeert daarop <i>Zorggebruiker</i> hierover.	conform de specificatie van de gebruikte <i>Informatiestandaard</i>	De flow worde voortg

## Subscription interface

### Inleiding

Het subscription interface hoort bij de [hoofdfunctie Regie](#).

Op deze pagina staan alleen de verantwoordelijkheden inzake het resource interface die nog niet genoemd staan in de [OAuth 2-specificatie](#).

1a. De subscription request is:

- als de *Persoon* via deze *Dienstverlener persoon* nog geen *Abonnement* heeft bij deze *Zorgaanbieder* op (*Notificaties over*) deze *Gegevensdienst*: een HTTP POST-request;
- als de *Persoon* via deze *Dienstverlener persoon* al een *Abonnement* heeft bij deze *Zorgaanbieder* op (*Notificaties over*) deze *Gegevensdienst*: een HTTP PUT-request.

### Subscription request

Met de subscription request biedt de *PGO Server* aan de *Subscription Server* een nieuwe *Abonnements*-resource aan, met daaraan verbonden de vooralsnog eenzijdige instemming van de *Persoon*. Hij verzoekt daarmee bovendien om een subscription response, waarmee ook de instemming van de *Zorgaanbieder* is verbonden. Zo ontstaat de overeenkomst. Ook een beëindiging van een Abonnement ontvangt zo de instemming van beide partijen, ook al kan de *Zorgaanbieder* zo'n beëindiging niet weigeren.

1b. De *OAuth Client* gebruikt voor het sturen van het acces token, in de subscription request, de methode `Authorization Request Header Field`, zoals beschreven in [sectie 2.1 van RFC6750](#).

### Toelichting

De methode `Authorization Request Header Field` biedt de beste beveiliging.

1c. De *OAuth Client* en de *Subscription Server* maken voor het uitwisselen van subscription requests en subscription responses gebruik van [JSON](#).

2. De parameters van de subscription request zijn als volgt gevuld:

parameter	vulling	toelichting
zorgaanbieder	verplicht, dezelfde waarde als voor de <i>Zorgaanbieder</i> in de scope van de voorafgaande token response	-
gegevensdienst	verplicht, dezelfde waarde als voor de <i>Gegevensdienst</i> in de scope van de voorafgaande token response	-
duration	verplicht, dezelfde waarde als die van de	-

	duration-parameter in de voorafgaande token response	
client_id	verplicht, dezelfde waarde als de client_id die gebruikt is in de voorafgaande authorization request	-
replaces	<ul style="list-style-type: none"> <li>afwezig, als de <i>Persoon</i> via deze <i>Dienstverlener persoon</i> nog geen <i>Abonnement</i> heeft bij deze <i>Zorgaanbieder</i> op (Notificaties over) deze <i>Gegevensdienst</i>;</li> <li>verplicht, als de <i>Persoon</i> via deze <i>Dienstverlener persoon</i> al een <i>Abonnement</i> heeft bij deze <i>Zorgaanbieder</i> op (Notificaties over) deze <i>Gegevensdienst</i>, en dan gevuld met de subscription_id van dat <i>Abonnement</i>.</li> </ul>	In het geval van <i>replaces</i> , identificeert het subscription_id het <i>Abonnement</i> dat door deze subscription request zal worden beëindigd (als duration=0) of aangepast (anders).

### Inleiding

Met de subscription request verzoekt de *PGO Server* aan de *Subscription Server* een *Abonnement* aan te maken, al dan niet ter vervanging van een bestaande, of te beëindigen. Daarbij geeft de *PGO Server* bovendien alvast aan dat deze wijziging de goedkeuring van de *Persoon* heeft.

3a. Na ontvangst van het subscription request verifieert de *Subscription Server* bij de *Authorization Server* dat het meegestuurd access token is uitgegeven in het kader van een *Abonnement* bij de betreffende *Zorgaanbieder*, op *Notificaties* van de betreffende *Gegevensdienst* en met de betreffende *duration*. Slagen niet al deze verificaties, dan behandelt de *Subscription Server* dit als uitzondering Subscription interface 1.

### Toelichting

Het access token moet dus een scope hebben die precies overeenkomt met de parameters van de subscription request.

3b. Als *replaces* een waarde heeft, verifieert de *Subscription Server* dat deze parameter een *Abonnement* identificeert van dezelfde *Persoon*, via dezelfde *Dienstverlener persoon*, op dezelfde *Gegevensdienst* bij dezelfde *Zorgaanbieder*. Slagen niet al deze verificaties, dan behandelt de *Subscription Server* dit als uitzondering Subscription interface 1.

### Toelichting

Hiermee controleert de *Subscription Server* dat de *PGO Server* het *Abonnement* kent dat hij met deze subscription request zou gaan beëindigen of aanpassen.

4. De enige parameter in de subscription response worden als volgt gevuld.

parameter	vulling	toelichting
subscription_id	identificatie waarmee de <i>Subscription Server</i> het <i>Abonnement</i> uniek voor deze <i>Persoon</i> en de <i>Dienstverlener</i> persoon identificeert	<p>Deze waarde gebruikt de <i>Notification Server</i> om bij een binnenkomende <i>Notificatie</i> het betreffende <i>Abonnement</i> te identificeren. Ook identificeert dit het <i>Abonnement</i> in logbestanden.</p> <p>Het subscription_id kan een integer waarde zijn, of een UUID, maar kan ook volgens een ander geldig identificatiepatroon worden gevuld.</p>

### Subscription response

Met de subscription response geeft de *Subscription Server* aan dat ook de *Zorgaanbieder* instemt met het *Abonnement*.

5. *Subscription Server* en *OAuth Client* handelen uitzonderingssituaties inzake het subscription interface af volgens onderstaande tabel.

Nummer	Implementeert uitzondering	Uitzondering	Actie	Melding	Vervolg
Subscription interface 1	UC Abonneren 6	De validatie van het access token door <i>Subscription Server</i> faalt, of er wordt niet voldaan aan de beschikbaarheidsvoorwaarde.  Zie ook de toelichting op <a href="#">Beschikbaarheids- en ontvankelijkheidsvoorwaarde</a> .	<i>Subscription Server</i> informeert <i>PGO Server</i> over deze uitzondering. <i>PGO Server</i> informeert daarop <i>Zorggebruiker</i> hierover.	Conform <a href="#">HTTP specificatie</a> met status code 401 "Niet geautoriseerd"	Allen stop de flow onmiddell na geïnform te zijn ove de uitzonderi
Subscription interface 2		<i>Subscription Server</i> ontvangt een ongeldig verzoek.		Conform <a href="#">HTTP specificatie</a> met status code 400 "Foute aanvraag"	
Subscription interface 3	UC Abonneren 3	<i>Subscription Server</i> kan in de request niet, niet geheel of niet tijdig uitvoeren, om redenen anders dan		Conform <a href="#">HTTP specificatie</a> met status code 500	

	uitzondering Subscription interface 1 of uitzondering Subscription interface 2.	"Interne serverfout"	
--	---	----------------------	--

6. Na ontvangst van een subscription request, in *UCI Abonneren*, zal de *Subscription Server*, indien in antwoord daarop een subscription response response dient te worden gedaan, na maximaal zestig (60) seconden dit resource response ter beschikking stellen aan de *PGO Server*. Dit gedrag van de *Subscription Server* is gedurende minimaal 98,5% van de tijd beschikbaar.

## Subscription notification interface

### Toelichting

Het subscription notification interface hoort bij de [hoofdfunctie Regie](#), terwijl het [resource notification interface](#) bij de [hoofdfunctie Uitwisseling](#) hoort.

1a. De *Notification Client* en de *Notification Server* maken op de subscription notification interface gebruik van HTTP 1.1.

1b. De *Notification Client* verstuurt de subscription notification middels een [HTTP POST](#) van een *Notification* op het in de *OAuth Client List* aangetroffen *Subscription Notification Endpoint*.

1c. Voor *Notificaties* en foutmeldingen op het subscription notification interface gebruiken *Notification Client* en de *Notification Server* het formaat [JSON](#).

2. De drie parameters in de subscription notification worden als volgt gevuld.

parameter	vulling	toelichting
subscription_id	De waarde waarmee de <i>Subscription Server</i> dit <i>Abonnement</i> in de <a href="#">subscription response</a> heeft geïdentificeerd.	Een gebeurtenis bij een <i>Zorgaanbieder</i> kan theoretisch leiden tot meerdere <i>Notificaties</i> . Iedere <i>Notificatie</i> hoort echter bij precies één <i>Abonnement</i> .
notification_type	De letterlijke waarde subscription.	Zo kan de <i>Notification Server</i> de subscription notification van de resource notification onderscheiden.
duration	De resterende duur van het <i>Abonnement</i> , gerekend in hele dagen.  Als deze waarde 0 is, is het <i>Abonnement</i> beëindigd door de <i>Zorgaanbieder</i> . In alle andere gevallen is deze waarde niet groter dan de resterende duur, op basis van de <i>Abonnementen</i> -administratie van de <i>Subscription Server</i> . De waarde kan wel kleiner zijn dan deze resterende duur, als het beleid van de <i>Zorgaanbieder</i> inzake de beschikbaarheidsvoorwaarde inkorting van het abonnement met zich meebrengt.	<i>Abonnementen</i> kunnen zowel door <i>Zorgaanbieder</i> als door <i>Uitgever</i> worden beëindigd. Beëindiging door <i>Uitgever</i> verloopt via de <a href="#">subscription interface</a> . Beëindiging door <i>Zorgaanbieder</i> verloopt via de subscription notification interface.  Met de mogelijkheid tot inkorting wordt de <i>Zorgaanbieder</i> in gelegenheid gesteld beschikbaarheidsbeleid

voortdurend te kunnen uitvoeren.

3. De enige parameter van de subscription notification response wordt als volgt gevuld.

parameter	vulling	toelichting
notification_id	identificatie waarmee de <i>Notification Server</i> de <i>Notificatie</i> uniek voor dit <i>Abonnement</i> identificeert	Dit kan bijvoorbeeld een integer waarde zijn, of een UUID, maar kan ook volgens een ander geldig ID-patroon worden gevuld.

4. Na ontvangst van een subscription notification, zal de *Notification Server*, indien in antwoord daarop een subscription notification response dient te worden gedaan, na maximaal tien (10) seconden dit antwoord ter beschikking stellen aan de *Notification Client*. Dit gedrag van de *Notification Server* is gedurende minimaal 98,5% van de tijd beschikbaar.

5. *Notification Server* en *Notification Client* handelen uitzonderingssituaties inzake het subscription notification interface af volgens onderstaande tabel.

Nummer	Implementeert uitzondering	Uitzondering	Actie	Melding	Vervolg
Subscription notification interface 1	UC Notificeren 1	<i>Notification Server</i> vindt de ontvangen <i>Notificatie</i> ongeldig.	<i>Notification Server</i> informeert <i>Notification Client</i> over deze uitzondering.	Conform <a href="#">HTTP specificatie</a> met met status code 400 "Foute aanvraag", en met in de body de van toepassing zijnde error code ("invalid_subscription_id", "invalid_notification_type" of "invalid_duration")	Allen sto onmidde te zijn ov  Wannee een erro invali " ontvang <i>Abonner</i> beëindig hiervoor subscrip sturen.
Subscription notification interface 2	UC Notificeren 2	<i>Notification Server</i> kan in de request niet, niet geheel of niet tijdig verwerken.	<i>Notification Server</i> informeert <i>Notification Client</i> over deze uitzondering.	Conform <a href="#">HTTP specificatie</a> met met status code 500 "Interne serverfout"	Allen sto onmidde te zijn ov

## Resource notification interface

### Toelichting

Het resource notification interface hoort de [hoofdfunctie Uitwisseling](#), terwijl het subscription notification interface bij de [hoofdfunctie Regie](#) hoort.

1a. De *Notification Client* en de *Notification Server* maken op het resource notification interface gebruik van HTTP 1.1.

1b. De *Notification Client* verstuurt de resource notification middels een [HTTP POST](#) van een *Notification* op het in de *OAuth Client List* aangetroffen *Subscription Notification Endpoint*.

1c. Voor *Notificaties* en foutmeldingen op het resource notification interface gebruiken *Notification Client* en de *Notification Server* het formaat [JSON](#).

2. De twee parameters in de resource notification worden als volgt gevuld.

parameter	vulling	toelichting
subscription_id	De waarde waarmee de <i>Subscription Server</i> dit <i>Abonnement</i> in de subscription response heeft geïdentificeerd.	Een gebeurtenis bij een <i>Zorgaanbieder</i> kan theoretisch leiden tot meerdere <i>Notificaties</i> . Iedere <i>Notificatie</i> hoort echter bij precies één <i>Abonnement</i> .
notification_type	De letterlijke waarde <code>resource</code> .	Zo kan de <i>Notification Server</i> de resource notification van de subscription notification onderscheiden.

### Toelichting

Hier is niet, zoals in de subscription notification, een `duration` opgenomen, omdat dat bij de [hoofdfunctie Regie](#) hoort. Communicatie over de *Abonnementen*-administratie vindt geheel plaats op het [subscription notification interface](#). Het resource notification interface is alleen voor inhoudelijke notificaties. Mogelijk zal in toekomstige releases van het MedMij Afsprakenstelsel in de resource notification ook een nadere indicatie worden opgenomen van het onderdeel van de *Gegevensdienst* waarop er nieuwe informatie beschikbaar is.

3. De enige parameter van de resource notification response wordt als volgt gevuld.

parameter	vulling	toelichting
notification_id	identificatie waarmee de <i>Notification Server</i> de <i>Notificatie</i> uniek voor dit <i>Abonnement</i> identificeert	Het id kan bijvoorbeeld een integer waarde zijn, of een UUID, maar kan ook volgens een ander geldig ID-patroon worden gevuld.



4a. Een *Notification Client* plaats **binnen één (1) uur** na het beschikbaar komen van nieuwe (gezondheids) informatie voor die *Zorggebruiker* betreffende die *Gegevensdienst*, een resource notification dienaangaande bij de betreffende *Notification Server*.

#### Notificaties

Als het tijdstip van beschikbaar komen van nieuwe (gezondheids)informatie wordt het moment gezien waarop betreffende informatie namens verwerkingsverantwoordelijke *Zorgaanbieder* (handmatig of automatisch) als "beschikbaar voor *Zorggebruiker*" wordt aangemerkt.

4b. Na ontvangst van een resource notification, zal de *Notification Server*, indien in antwoord daarop een resource notification response dient te worden gedaan, na maximaal tien (10) seconden dit antwoord ter beschikking stellen aan de *Notification Client*. Dit gedrag van de *Notification Server* is gedurende minimaal 98,5% van de tijd beschikbaar.

5. *Notification Server* en *Notification Client* handelen uitzonderingssituaties inzake het resource notification interface af volgens onderstaande tabel.

Nummer	Implementeert uitzondering	Uitzondering	Actie	Melding	Ver
Resource notification interface 1	UC Notificeren 1	<i>Notification Server</i> vindt de ontvangen resource notification ongeldig.	<i>Notification Server</i> informeert <i>Notification Client</i> over deze uitzondering.	Conform <a href="#">HTTP specificatie</a> met met status code 400 "Foute aanvraag", en met in de body de van toepassing zijnde error code ("invalid_subscription_id" of "invalid_notification_type")	Alle onr te z  Wa eer in " o Ab beë hie not
Resource notification interface 2	UC Notificeren 2	<i>Notification Server</i> kan in de request niet, niet geheel of niet tijdig verwerken.	<i>Notification Server</i> informeert <i>Notification Client</i> over deze uitzondering.	Conform <a href="#">HTTP specificatie</a> met met status code 500 "Interne serverfout"	Alle onr te z

## GNL-, OCL- en ZAL-interface

1. De URI van de:

- *Zorgaanbiederslijst* is [https://stelselnode.medmij.nl/MedMij\\_Zorgaanbiederslijst.xml?api=1.2.0](https://stelselnode.medmij.nl/MedMij_Zorgaanbiederslijst.xml?api=1.2.0)
- *OAuthclientlist* is [https://stelselnode.medmij.nl/MedMij\\_OAuthclientlist.xml?api=1.2.0](https://stelselnode.medmij.nl/MedMij_OAuthclientlist.xml?api=1.2.0)
- *Gegevensdienstnamenlijst* is [https://stelselnode.medmij.nl/MedMij\\_Gegevensdienstnamenlijst.xml?api=1.2.0](https://stelselnode.medmij.nl/MedMij_Gegevensdienstnamenlijst.xml?api=1.2.0)

### Versionering van de lijst-interfaces

Vanaf release 1.1.2 van het MedMij Afsprakenstelsel hebben de lijst-interfaces een versienummer. Dat maakt het mogelijk om meerdere versies van deze interfaces tegelijkertijd in productie te hebben. De versies worden, vanaf release 1.1.2, van elkaar onderscheiden door een query-parameter in de URI.

Het versienummer is identiek aan dat van de betreffende release. Opeenvolgende versies van de lijst-interfaces kunnen daarom inhoudelijk identiek zijn.

2. Het aandeel van *MedMij Registratie* in elk van de use case-implementaties *UCI Opvragen ZAL*, *UCI Opvragen OCL* en *UCI Opvragen GNL* is voor minstens 99,9% van de tijd beschikbaar. *MedMij Beheer* laat, na het niet beschikbaar raken van bedoelde aandeel, maximaal acht uren (480 minuten) verstrijken voordat het weer beschikbaar is.

3. *MedMij Beheer* brengt, in geval van zo'n incident, *Uitgevers*, *Bronnen* en *Lezers* op de hoogte van het optreden van het incident en van de verwachte down-time. *MedMij Beheer* brengt partijen op de hoogte van gepland onderhoud dat leidt tot tijdelijke onbeschikbaarheid.

4. Ingeval *MedMij Registratie* in *UCI Opvragen ZAL*, *UCI Opvragen OCL* en/of *UCI Opvragen GNL* onbeschikbaar is, mogen betreffende opvragers gedurende maximaal 10 uur gebruik maken van het meest recente exemplaar van de betreffende lijst in de cache.

## Use case-implementaties

### Inleiding

Deze pagina groepeert de pagina's van de verschillende use case-implementaties:

- [\*UCI Verzamelen\*](#)
- [\*UCI Delen\*](#)
- [\*UCI Abonneren\*](#)
- [\*UCI Notificeren\*](#)
- [\*UCI Opvragen GNL\*](#)
- [\*UCI Opvragen OCL\*](#)
- [\*UCI Opvragen ZAL\*](#)

## UCI Verzamelen

### Toelichting

In de platen hieronder staat het stroomdiagram van de use case-implementatie *Verzamelen*, in vier perspectieven:

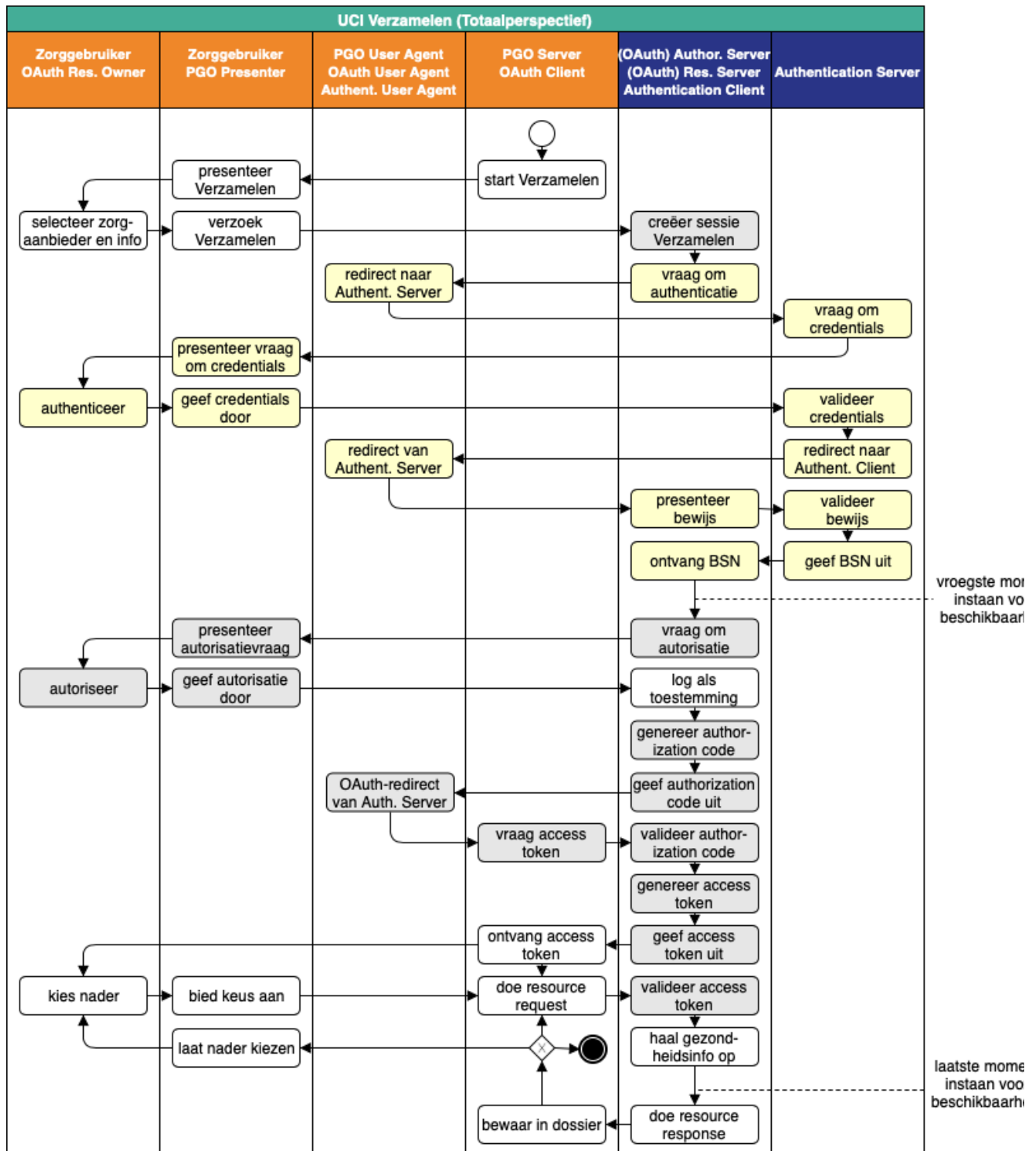
- het totaalperspectief, met zowel de happy flow als de uitzonderingen;
- het perspectief van de *PGO Server (= OAuth Client)*, die onder de hoede van de *Dienstverlener Persoon* valt. Laatstgenoemde kan deze plaat lezen als zijn verplichte aandeel in de use case-implementatie *Verzamelen*;
- het perspectief van de *(OAuth) Authorization Server/(OAuth) Resource Server/Authentication Client*, die onder de hoede van de *Dienstverlener Zorgaanbieder* valt. Laatstgenoemde kan deze plaat lezen als zijn verplichte aandeel in de use case-implementatie *Verzamelen*;
- het perspectief van de *Zorggebruiker (= OAuth Resource Owner)*.

De stroomdiagrammen tonen alleen de situatie waarin alle acties slagen tot en met het uiteindelijke verzamelen van de gezondheidsinformatie (de zogenaamde happy flow). De drie oranje banen horen, conform de MedMij-huisstijl tot het Persoonsdomein, de twee blauwe tot het Zorgaanbiedersdomein. Menige actie in de stroomdiagrammen is gekleurd weergegeven. De lichtgrijs gekleurde acties vormen samen de autorisatieflow volgens OAuth 2; de zachtgeel gekleurde acties vormen samen de authenticatieflow. Deze kleuren verwijzen dus alleen maar naar de gebruikte standaarden en zeggen niets over welke component de stap zou moeten uitvoeren. Authenticatie is dus ingebed in autorisatie. In de stroomdiagrammen voor de specifieke perspectieven hebben alleen de acties in de bij dat perspectief horende baan namen. De acties in de andere banen zijn gecombineerd en anoniem weergegeven.

Verantwoordelijkheden inzake uitzonderingen op de happy flow zijn opgenomen bij de respectievelijke interface, in tegenstelling tot op de [Processen & Informatie-laag](#), waar de uitzonderingen bij de use cases zijn genoemd.

## Totaalperspectief

### Happy flow



### Toelichting

In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

De flow kent de volgende stappen:

1. De *PGO Server* start de flow door in de *PGO Presenter* van de *Zorggebruiker* de mogelijkheid te presenteren om een bepaalde *Gegevensdienst* bij een zekere *Zorgaanbieder* te verzamelen. Het gaat altijd om precies één *Gegevensdienst* (één scope, in OAuth-termen). Uit de *Zorgaanbiederslijst* weet de *PGO Server* welke *Gegevensdiensten* door een *Zorgaanbieder* aangeboden worden. Desgewenst worden de *Gegevensdienstnamen* uit de *Gegevensdienstnamenlijst* gebruikt.
2. De *Zorggebruiker* maakt expliciet zijn selectie en laat de *OAuth User Agent* een verzamelverzoek sturen naar de *Authorization Server*. Het adres van het authorization endpoint komt uit de ZAL. De *redirect\_uri* geeft aan waarnaartoe de *Authorization Server* de *OAuth User Agent* verderop moet redirecten (met de authorization code).
3. Daarop begint de *Authorization Server* de OAuth-flow (in zijn rol als *OAuth Authorization Server*) door een sessie te creëren.
4. Dan start de *Authorization Server* (nu in de rol van *Authentication Client*) de authenticatieflow door de browser naar de *Authentication Server* te redirecten, onder meegeven van een *redirect\_uri*, die aangeeft waarnaartoe de *Authentication Server* straks de *OAuth User Agent* moet terugsturen, na het inloggen van de *Zorggebruiker*.
5. De *Authentication Server* vraagt van de *Zorggebruiker* via zijn *PGO Presenter* om inloggegevens.
6. Wanneer deze juist zijn, redirect de *Authentication Server* de *OAuth User Agent* terug naar de *Authorization Server*, onder meegeven van een ophaalbewijs.
7. Met dit ophaalbewijs haalt de *Authorization Server* rechtstreeks bij de *Authentication Server* het BSN op.
8. Dan breekt het vroegste moment aan waarop de *Authorization Server* ervoor instaat dat de *Zorgaanbieder* voor de betreffende *Gegevensdienst* überhaupt gezondheidsinformatie van die *Persoon* beschikbaar heeft, of anders de happy flow afbreekt. Daarvan maakt deel uit dat de *Persoon* daarvoor minstens 16 jaar oud moet zijn.
9. Zo ja, dan presenteert de *Authorization Server* via de *PGO Presenter* aan *Zorggebruiker* de vraag of laatstgenoemde hem toestaat de gevraagde persoonlijke gezondheidsinformatie aan de *PGO Server* (als *OAuth Client*) te sturen. Onder het flow-diagram staat gespecificeerd welke informatie, waarvandaan, de *OAuth Authorization Server* verwerkt in de aan *Zorggebruiker* voor te leggen [Toestemmingsverklaring](#).
10. Bij akkoord logt de *Authorization Server* dit als toestemming, genereert een authorization code en stuurt dit als ophaalbewijs, door middel van een browser redirect met de in stap 1 ontvangen *redirect\_uri*, naar de *PGO Server*. De *Authorization Server* stuurt daarbij de local state-informatie mee die hij in de eerste stap van de *PGO Server* heeft gekregen. Laatstgenoemde herkent daaraan het verzoek waarmee hij de authorization code moet associëren.
11. De *PGO Server* vat niet alleen deze authorization code op als ophaalbewijs, maar leidt er ook uit af dat de toestemming is gegeven en logt het verkrijgen van het ophaalbewijs.
12. Met dit ophaalbewijs wendt de *PGO Server* zich weer tot de *Authorization Server*, maar nu zonder tussenkomst van de *OAuth User Agent*, voor een access token.
13. Daarop genereert de *Authorization Server* een access token en stuurt deze naar de *PGO Server*.
14. Nu is de *PGO Server* gereed om het verzoek om de gezondheidsinformatie naar de *Resource Server* te sturen, nadat hij de gebruiker eventueel nog nadere keuzes heeft laten maken. Het adres van het resource endpoint haalt hij uit de ZAL. Hij plaatst het access token in het bericht en zorgt ervoor dat in het bericht geen BSN is opgenomen.
15. De *Resource Server* controleert of het ontvangen token recht geeft op de gevraagde resources, haalt deze (al dan niet) bij achterliggende bronnen op. Dan breekt het uiterste moment aan waarop de *Resource Server* ervoor moet instaan dat voor de betreffende *Gegevensdienst* de *Zorgaanbieder* de gezondheidsgegevens beschikbaar heeft. Is dat zo, dan verstuurt de *Resource Server* deze ze in een resource response naar de *PGO Server*. Is dat niet zo, dan breekt de *Resource Server* de happy flow af.

16. Deze bewaart de ontvangen gezondheidsinformatie in het persoonlijke dossier. Mocht de *Gegevensdienst* waartoe de *Zorggebruiker* heeft geautoriseerd uit meerdere *Transacties* bestaan (zie hiervoor de [Catalogus](#)), of mocht één *Transactie* volgens de betreffende *Informatiestandaard* uit meerdere requests bestaan, bevraagt de *PGO Server* de *Resource Server* daarna mogelijk opnieuw voor de nog resterende *Transacties*, eventueel na nieuwe interactie met de *Zorggebruiker*. Zolang het access token geldig is, kan dat.

In de regel worden bij een eenmalig gebruik van *UCI Verzamelen* het authorization interface, het token interface en het resource interface allemaal aangesproken, in die volgorde. Mocht de *PGO Server* echter nog beschikken over een nog niet verlopen access token voor de betreffende *Zorgaanbieder-Gegevensdienst*-combinatie, dan kan het onmiddellijk het resource interface aanspreken.

Het MedMij Afsprakenstelsel adviseert de beschikbaarheidsvoorwaarde op het vroegst aangegeven moment van kracht te laten zijn. Vooralsnog staat het MedMij Afsprakenstelsel toe die voorwaarde op een later moment van kracht te laten zijn, maar niet later dan het laatste in het figuur aangegeven moment.

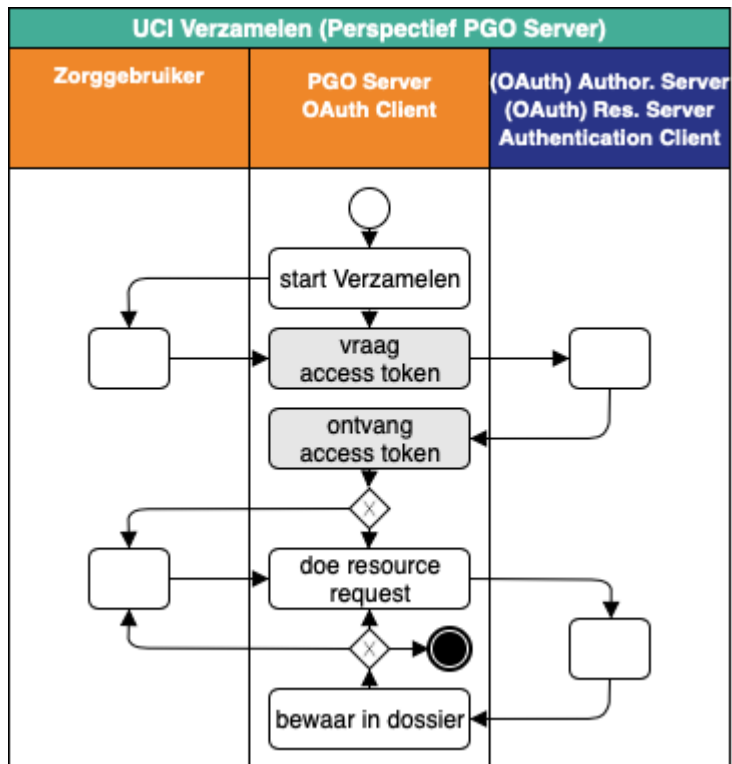
Bij de implementatie van de voorwaarde op beschikbaarheid bij de *Zorgaanbieder* voor de te verzamelen gezondheidsgegevens is het zaak rekening te houden met privacy-vereisten. Wanneer de *Dienstverlener Zorgaanbieder* ten behoeve van de beschikbaarheidsvoorwaarde nieuwe gegevensverzamelingen zou aanleggen, vindt een verwerking altijd onder de verantwoordelijkheid van één *Zorgaanbieder* plaats. Het combineren van verwerkingen of het onvoldoende segregeren moet worden vermeden. Afwijking hiervan is alleen mogelijk onder expliciete instructie van de *Zorgaanbieder(s)* en vereist een zorgvuldige voorafgaande afweging, vanwege de daaraan verbonden privacyrisico's.

## Specifieke perspectieven

### Perspectief PGO Server (happy flow)

#### Toelichting

Hieronder staat hetzelfde stroomdiagram, maar vanuit het perspectief van de *PGO Server*. Dat wil zeggen dat alle tussenliggende stappen die niet zichtbaar zijn voor de *PGO Server*, kortgesloten zijn. *Zorggebruiker* is "verborgen achter de browser" en de *Authentication Server* "achter de *Authorization Server*".

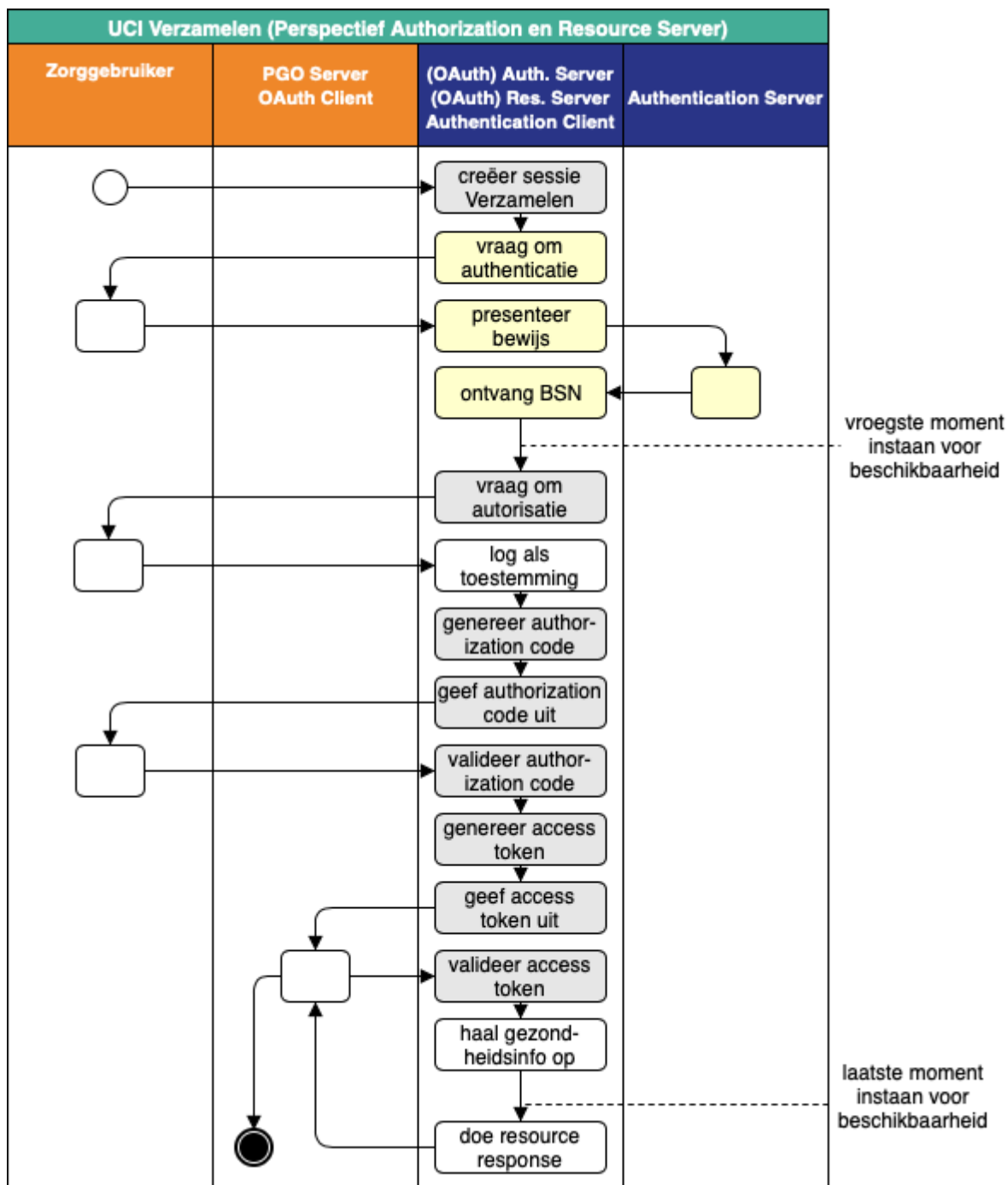


### Perspectief Authorization Server/Resource Server (happy flow)

#### Toelichting

Hieronder staat hetzelfde stroomdiagram, maar vanuit het perspectief van de *Authorization /Resource Server*. Dat wil zeggen dat alle tussenliggende stappen die niet zichtbaar zijn voor de *PGO Server*, kortgesloten zijn. *Zorggebruiker* is "verborgen achter de browser".

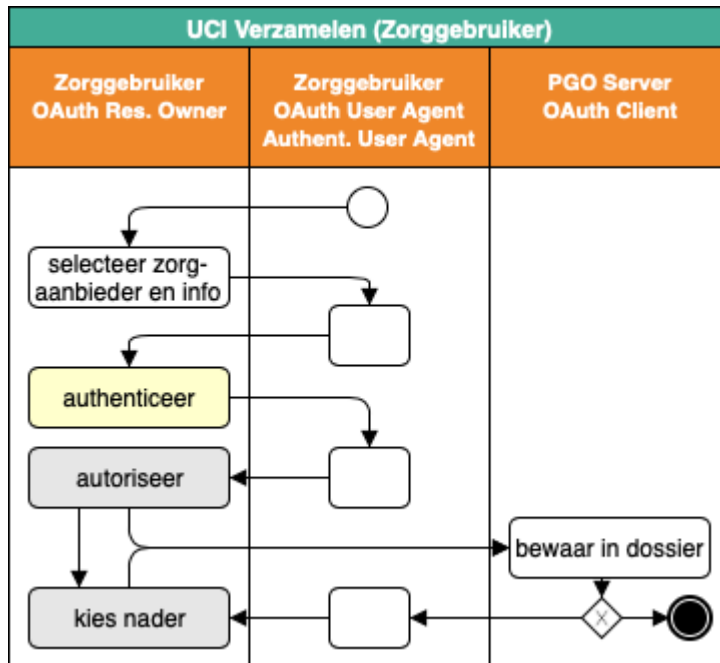




### Perspectief Zorggebruiker (happy flow)

#### Toelichting

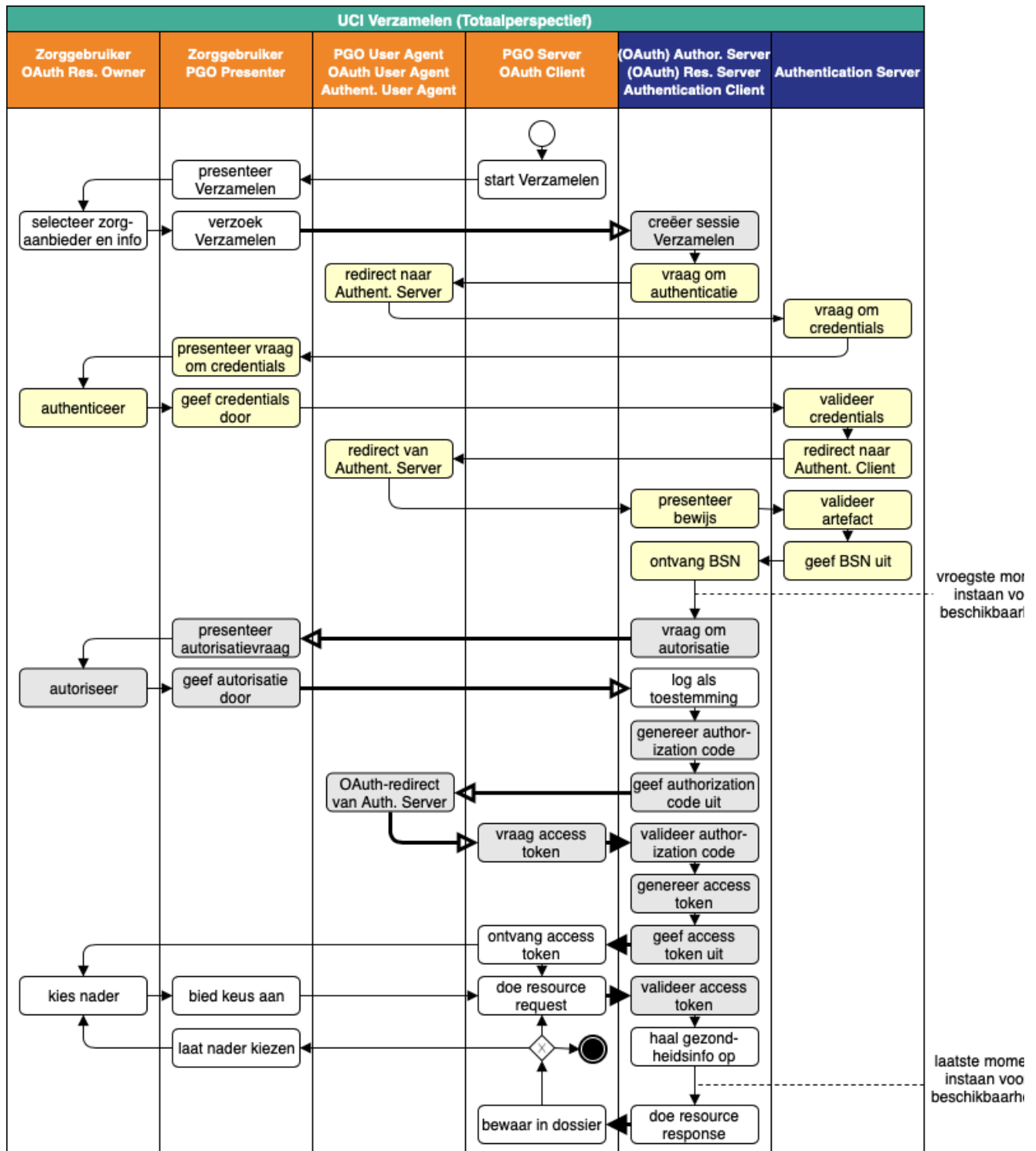
Hieronder staat hetzelfde stroomdiagram, maar vanuit het perspectief van de *Zorggebruiker*. Dat wil zeggen dat alle tussenliggende stappen die niet zichtbaar zijn voor de *Zorggebruiker*, kortgesloten zijn. Vrijwel alles is "verborgen achter de browser". We hebben alleen de laatste stap van *PGO Server* zichtbaar gehouden, omdat het bewaren van de verzamelde gezondheidsinformatie betekenis heeft voor de *Zorggebruiker*. Waarschijnlijk zal de *PGO Server* de *Zorggebruiker* laten weten dat het verzamelen geslaagd is, maar dat is niet verplicht.



## Frontchannel en backchannel

### Toelichting

In onderstaand stroomschema van UCI Verzamelen geven de dikke pijlen het *MedMij-verkeer* weer en zijn daarbinnen de vijf gevallen van frontchannel-verkeer (open pijlpunt) en vier gevallen van backchannel-verkeer (gesloten pijlpunt) aangegeven.



## UCI Delen

### Toelichting

In de platen hieronder staat het stroomdiagram van de use case-implementatie *Delen*, in vier perspectieven:

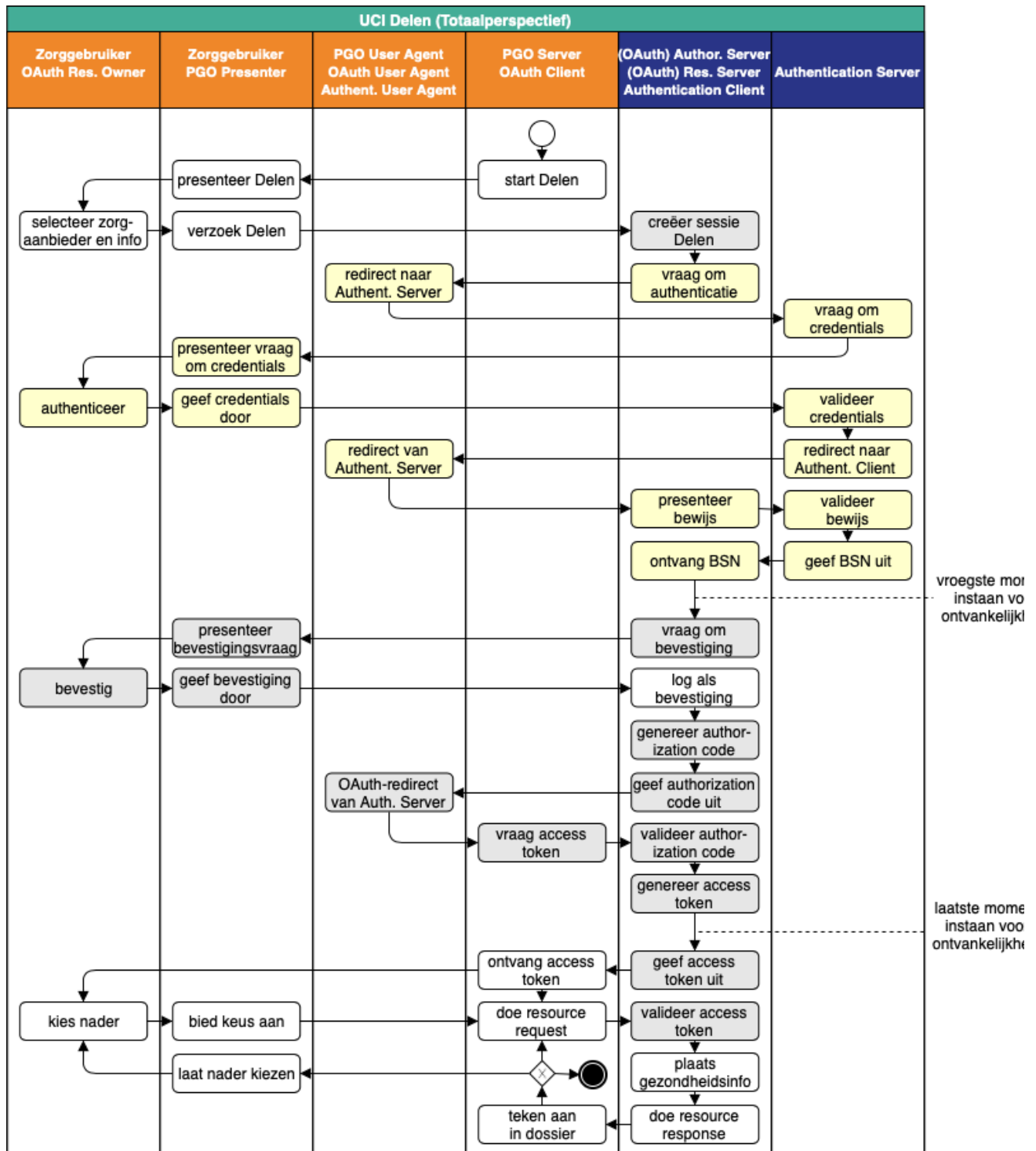
- het totaalperspectief, met zowel de happy flow als de uitzonderingen;
- het perspectief van de *PGO Server* (= *OAuth Client*), die onder de hoede van de *Dienstverlener Persoon* valt. Laatstgenoemde kan deze plaat lezen als zijn verplichte aandeel in de use case-implementatie *Delen*;
- het perspectief van de (*OAuth*) *Authorization Server*/*(OAuth) Resource Server/Authentication Client*, die onder de hoede van de *Dienstverlener Zorgaanbieder* valt. Laatstgenoemde kan deze plaat lezen als zijn verplichte aandeel in de use case-implementatie *Delen*;
- het perspectief van de *Zorggebruiker* (= *OAuth Resource Owner*).

De stroomdiagrammen tonen alleen de situatie waarin alle acties slagen tot en met het uiteindelijke delen van de gezondheidsinformatie (de zogenaamde happy flow). De drie oranje banen horen, conform de MedMij-huisstijl tot het Persoonsdomein, de twee blauwe tot het Zorgaanbiedersdomein. Menige actie in de stroomdiagrammen is gekleurd weergegeven. De lichtgrijs gekleurde acties vormen samen de autorisatieflow volgens OAuth 2; de zachtgeel gekleurde acties vormen samen de authenticatieflow. Deze kleuren verwijzen dus alleen maar naar de gebruikte standaarden en zeggen niets over welke component de stap zou moeten uitvoeren. Authenticatie is dus ingebed in autorisatie. In de stroomdiagrammen voor de specifieke perspectieven hebben alleen de acties in de bij dat perspectief horende baan namen. De acties in de andere banen zijn gecompriemd en anoniem weergegeven.

Verantwoordelijkheden inzake uitzonderingen op de happy flow zijn opgenomen bij de respectievelijke interface, in tegenstelling tot op de [Processen & Informatie-laag](#), waar de uitzonderingen bij de use cases zijn genoemd.

## Totaalperspectief

### Happy flow



### Toelichting

In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

De flow kent de volgende stappen:

1. De *PGO Server* start de flow door in de *PGO Presenter* van de *Zorggebruiker* de mogelijkheid te presenteren om een bepaalde *Gegevensdienst* met een zekere *Zorgaanbieder* te delen. Het gaat altijd om precies één *Gegevensdienst* (één scope, in OAuth-termen). Uit de *Zorgaanbiederslijst* weet de *PGO Server* welke *Gegevensdiensten* door een *Zorgaanbieder* aangeboden worden. Desgewenst worden de *Gegevensdienstnamen* uit de *Gegevensdienstnamenlijst* gebruikt.
2. De *Zorggebruiker* maakt expliciet zijn selectie en laat de *OAuth User Agent* een deel-verzoek sturen naar de *Authorization Server*. Het adres van het authorization endpoint komt uit de ZAL. De redirect URI geeft aan waarnaartoe de *Authorization Server* de *OAuth User Agent* verderop moet redirecten (met de authorization code).
3. Daarop begint de *Authorization Server* de OAuth-flow (in zijn rol als *OAuth Authorization Server*) door een sessie te creëren.
4. Dan start de *Authorization Server* (nu in de rol van *Authentication Client*) de authenticatieflow door de *OAuth User Agent* naar de *Authentication Server* te redirecten, onder meegeven van een redirect URI, die aangeeft waarnaartoe de *Authentication Server* straks de *OAuth User Agent* moet terugsturen, na het inloggen van de *Zorggebruiker*.
5. De *Authentication Server* vraagt van de *Zorggebruiker* via zijn *PGO Presenter* om inloggegevens.
6. Wanneer deze juist zijn, redirect de *Authentication Server* de *OAuth User Agent* terug naar de *Authorization Server*, onder meegeven van een ophaalbewijs.
7. Met dit ophaalbewijs haalt de *Authorization Server* rechtstreeks bij de *Authentication Server* het BSN op.
8. Dan breekt het vroegste moment aan waarop de *Authorization Server* ervoor instaat dat de *Zorgaanbieder* voor de betreffende *Gegevensdienst* überhaupt ontvankelijk is voor de gezondheidsinformatie van die *Persoon*, of anders de happy flow afbreekt. Daarvan maakt deel uit dat de *Persoon* daarvoor minstens 16 jaar oud moet zijn.
9. Zo ja, dan presenteert de *Authorization Server* via de *PGO Presenter* aan *Zorggebruiker* de vraag of laatstgenoemde bevestigt de gevraagde persoonlijke gezondheidsinformatie door de *PGO Server* (als *OAuth Client*) te laten aanbieden. Onder het stroomdiagram staat gespecificeerd welke informatie, waarvandaan, de *OAuth Authorization Server* verwerkt in de aan *Zorggebruiker* voor te leggen bevestigingsvraag.
10. Bij akkoord logt de *Authorization Server* dit als bevestiging, genereert een authorization code en stuurt dit als ophaalbewijs, door middel van een browser redirect met de in stap 1 ontvangen redirect URI, naar de *PGO Server*. De *Authorization Server* stuurt daarbij de local state-informatie mee die hij in de eerste stap van de *PGO Server* heeft gekregen. Laatstgenoemde herkent daaraan het verzoek waarmee hij de authorization code moet associëren.
11. De *PGO Server* vat niet alleen deze authorization code op als ophaalbewijs, maar leidt er ook uit af dat de bevestiging is gegeven en logt het verkrijgen van het ophaalbewijs.
12. Met dit ophaalbewijs wendt de *PGO Server* zich weer tot de *Authorization Server*, maar nu zonder tussenkomst van de *OAuth User Agent*, voor een access token.
13. Daarop genereert de *Authorization Server* een access token. Dan breekt het uiterste moment aan waarop de *Authorization Server* ervoor moet instaan dat voor de betreffende *Gegevensdienst* de *Zorgaanbieder* ontvankelijk is voor de gezondheidsgegevens van de betreffende *Persoon*. Is dat zo, dan verstuurt de *Authorization Server* het access token naar de *PGO Server*. Is dat niet zo, dan breekt de *Authorization Server* de happy flow af en stuurt zij geen access token naar de *PGO Server*.
14. Nu is de *PGO Server* gereed om de gezondheidsinformatie aan de *Resource Server* aan te bieden, nadat hij de gebruiker eventueel nog nadere keuzes heeft laten maken. Het adres van het resource endpoint haalt hij uit de ZAL. Hij plaatst het access token in het bericht en zorgt ervoor dat in het bericht geen BSN is opgenomen.

15. De *Resource Server* controleert of het ontvangen token recht geeft op het aanbieden van de informatie, plaatst deze (al dan niet) bij achterliggende bestemmingen en verstuurt een antwoord in een FHIR-response naar de *PGO Server*.
16. Deze maakt hierover een aantekeningen bij de aangeboden gezondheidsinformatie in het persoonlijke dossier. Mocht de *Gegevensdienst* waartoe de *Zorggebruiker* heeft geautoriseerd uit meerdere *Transacties* bestaan (zie hiervoor de [Catalogus](#)), plaatst de *PGO Server* daarna mogelijk opnieuw bij de *Resource Server* voor de nog resterende *Transacties*, eventueel na nieuwe interactie met de *Zorggebruiker*. Dat geldt ook voor de situatie waarin één *Transactie*, blijkens de betreffende *Informatiestandaard*, uit meerdere FHIR creates bestaat. Zolang het access token geldig is, kan dat.

---

In de regel worden bij een eenmalig gebruik van *UCI Delen* het authorization interface, het token interface en het resource interface allemaal aangesproken, in die volgorde. Mocht de *PGO Server* echter nog beschikken over een nog niet verlopen access token voor de betreffende *Zorgaanbieder-Gegevensdienst*-combinatie, dan kan het onmiddellijk het resource interface aanspreken.

---

Het MedMij Afsprakenstelsel adviseert de ontvankelijkheidsvoorwaarde op het vroegst aangegeven moment van kracht te laten zijn. In release 1.1.1 staat het MedMij Afsprakenstelsel toe die voorwaarde op een later moment van kracht te laten zijn, maar niet later dan het laatste in het figuur aangegeven moment.

Bij de implementatie van de toets op ontvankelijkheid van de *Zorgaanbieder* voor de te delen gezondheidsgegevens is het zaak rekening te houden met privacy-vereisten. Wanneer de *Dienstverlener Zorgaanbieder* ten behoeve van de ontvankelijkheidstoets nieuwe gegevensverzamelingen zou aanleggen, vindt een verwerking altijd onder de verantwoordelijkheid van één *Zorgaanbieder* plaats. Het combineren van verwerkingen of het onvoldoende segregeren moet worden vermeden. Afwijking hiervan is alleen mogelijk onder expliciete instructie van de *Zorgaanbieder(s)* en vereist een zorgvuldige voorafgaande afweging, vanwege de daaraan verbonden privacyrisico's.

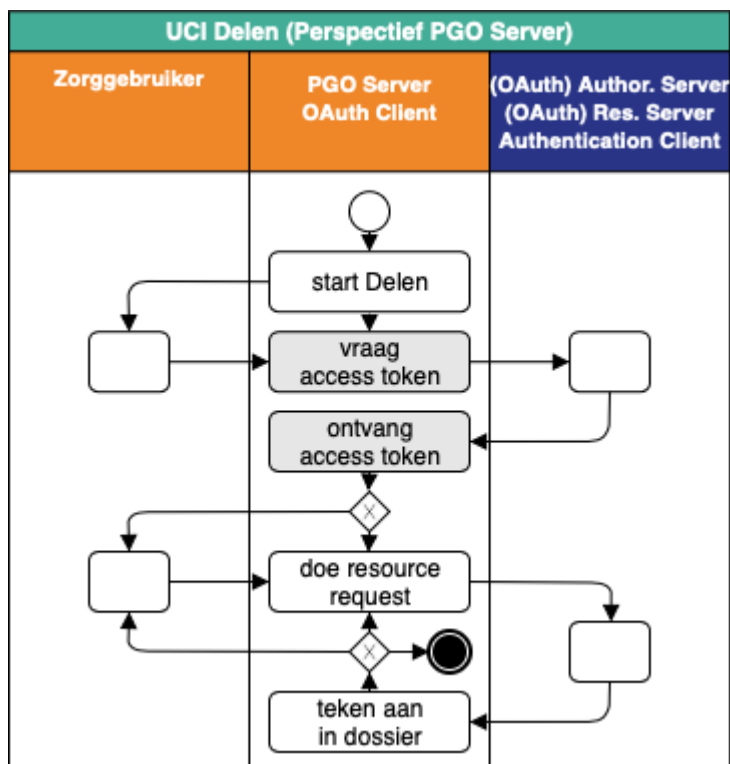
## Specifieke perspectieven



## Perspectief PGO Server (happy flow)

### Toelichting

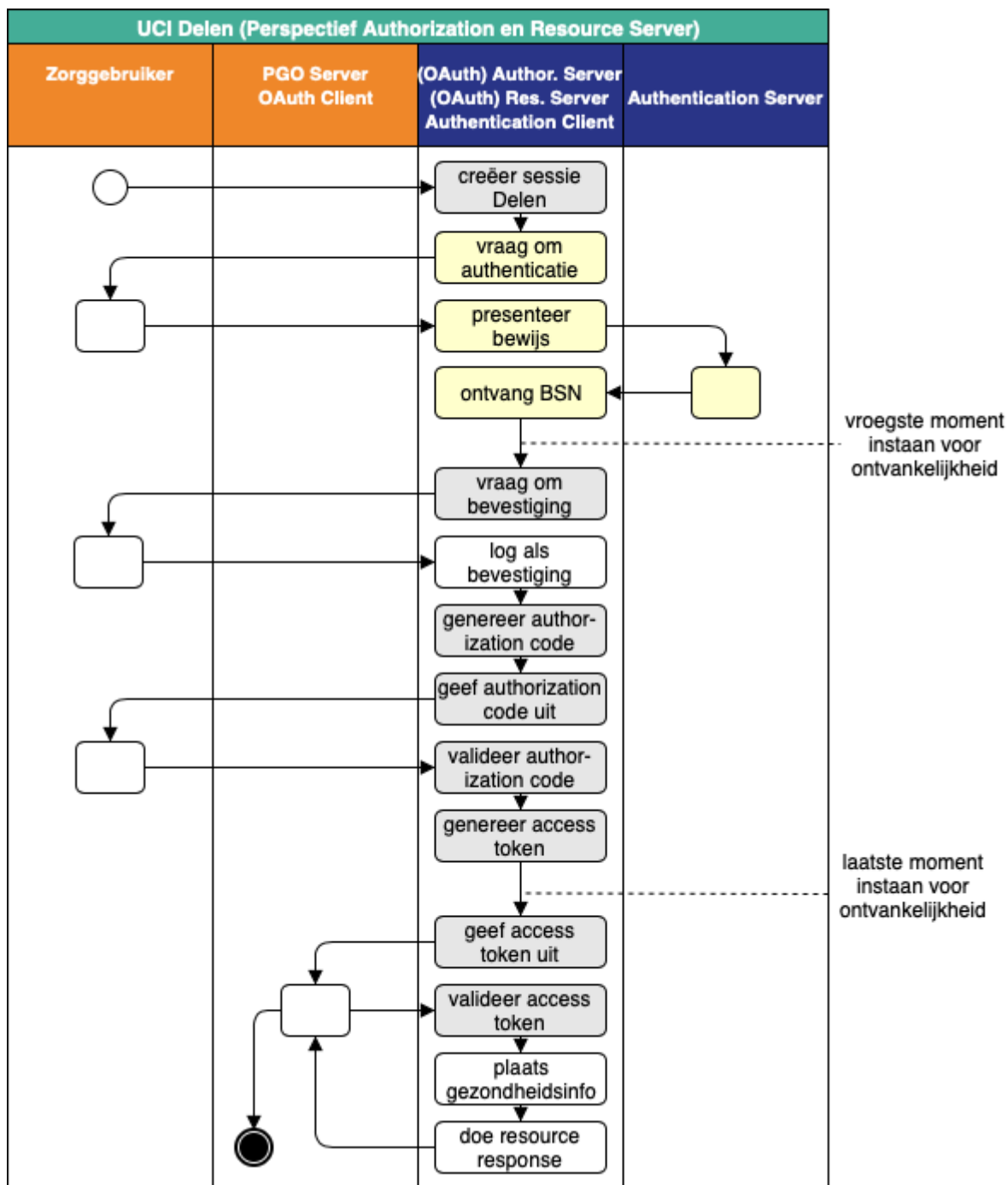
Hieronder staat hetzelfde stroomdiagram, maar vanuit het perspectief van de *PGO Server*. Dat wil zeggen dat alle tussenliggende stappen die niet zichtbaar zijn voor de *PGO Server*, kortgesloten zijn. *Zorggebruiker* is "verborgen achter de browser" en de *Authentication Server* "achter de *Authorization Server*".



## Perspectief Authorization Server/Resource Server (happy flow)

### Toelichting

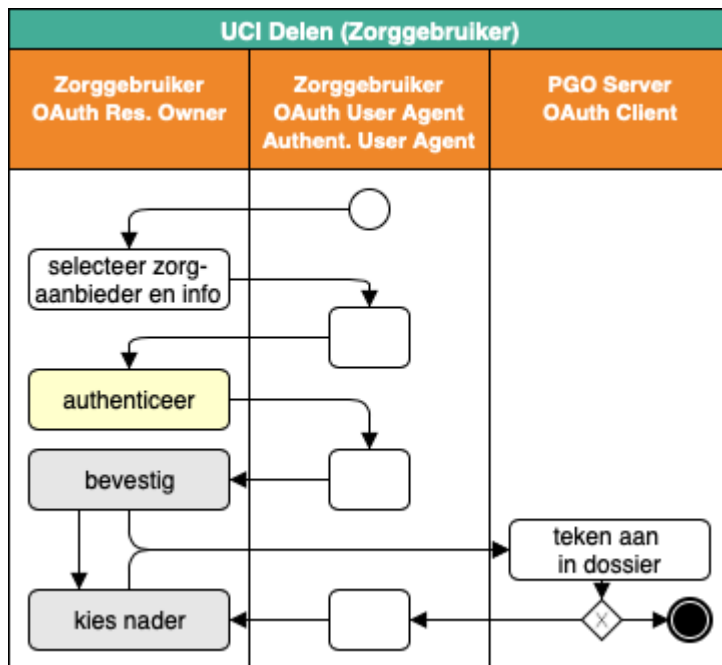
Hieronder staat hetzelfde stroomdiagram, maar vanuit het perspectief van de *Authorization /Resource Server*. Dat wil zeggen dat alle tussenliggende stappen die niet zichtbaar zijn voor de *PGO Server*, kortgesloten zijn. *Zorggebruiker* is "verborgen achter de browser".



## Perspectief Zorggebruiker (happy flow)

### Toelichting

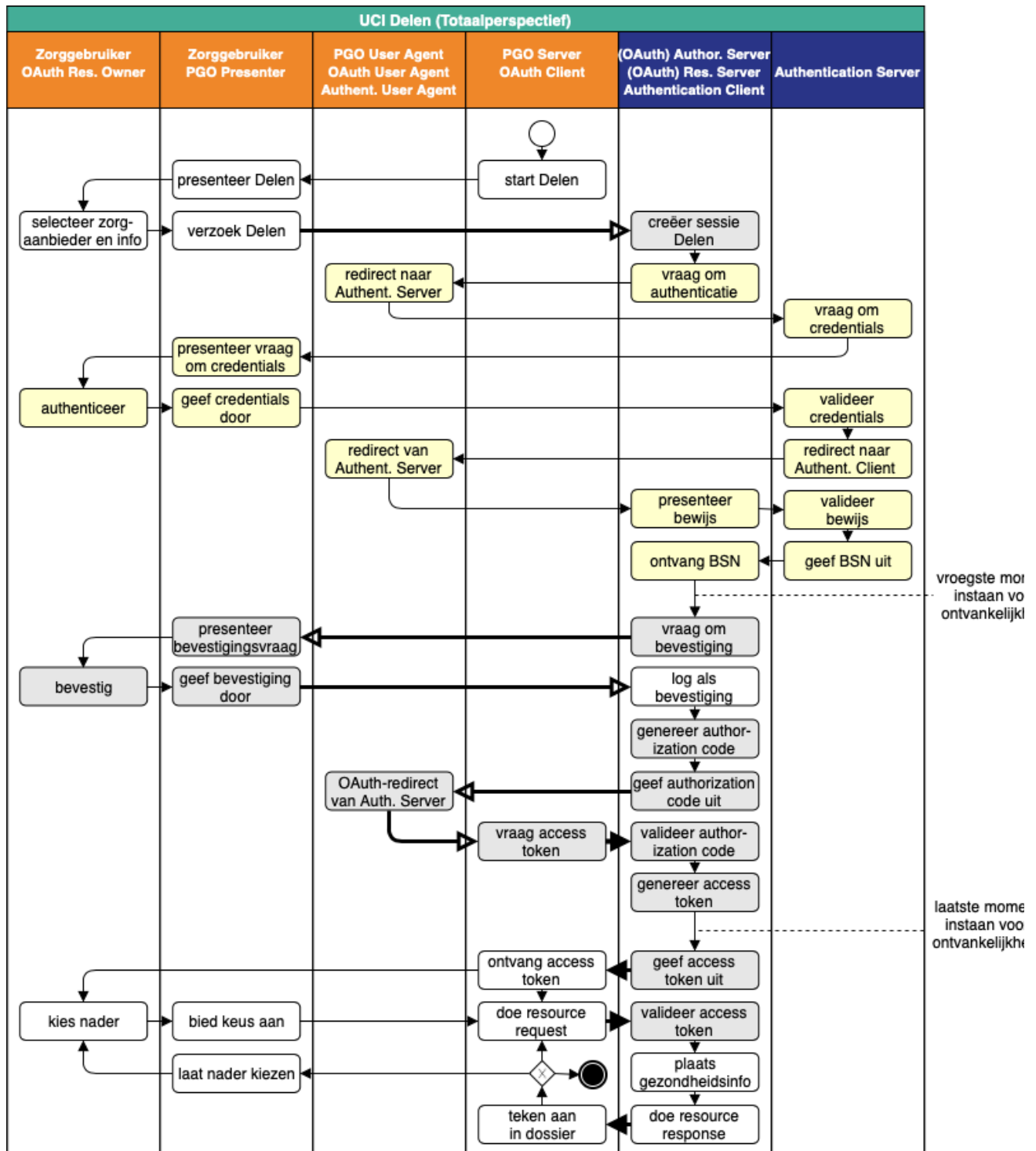
Hieronder staat hetzelfde stroomdiagram, maar vanuit het perspectief van de *Zorggebruiker*. Dat wil zeggen dat alle tussenliggende stappen die niet zichtbaar zijn voor de *Zorggebruiker*, kortgesloten zijn. Vrijwel alles is "verborgen achter de browser". We hebben alleen de laatste stap van *PGO Server* zichtbaar gehouden, omdat het markeren van de gedeelde gezondheidsinformatie betekenis heeft voor de *Zorggebruiker*. Waarschijnlijk zal de *PGO Server* de *Zorggebruiker* laten weten dat het delen geslaagd is, maar dat is niet verplicht.



## Frontchannel en backchannel

### Toelichting

In onderstaand stroomschema van UCI Delen geven de dikke pijlen het *MedMij-verkeer* weer en zijn daarbinnen de vijf gevallen van frontchannel-verkeer (open pijlpunt) en vier gevallen van backchannel-verkeer (gesloten pijlpunt) aangegeven.



## UCI Abonneren

### UCI Abonneren

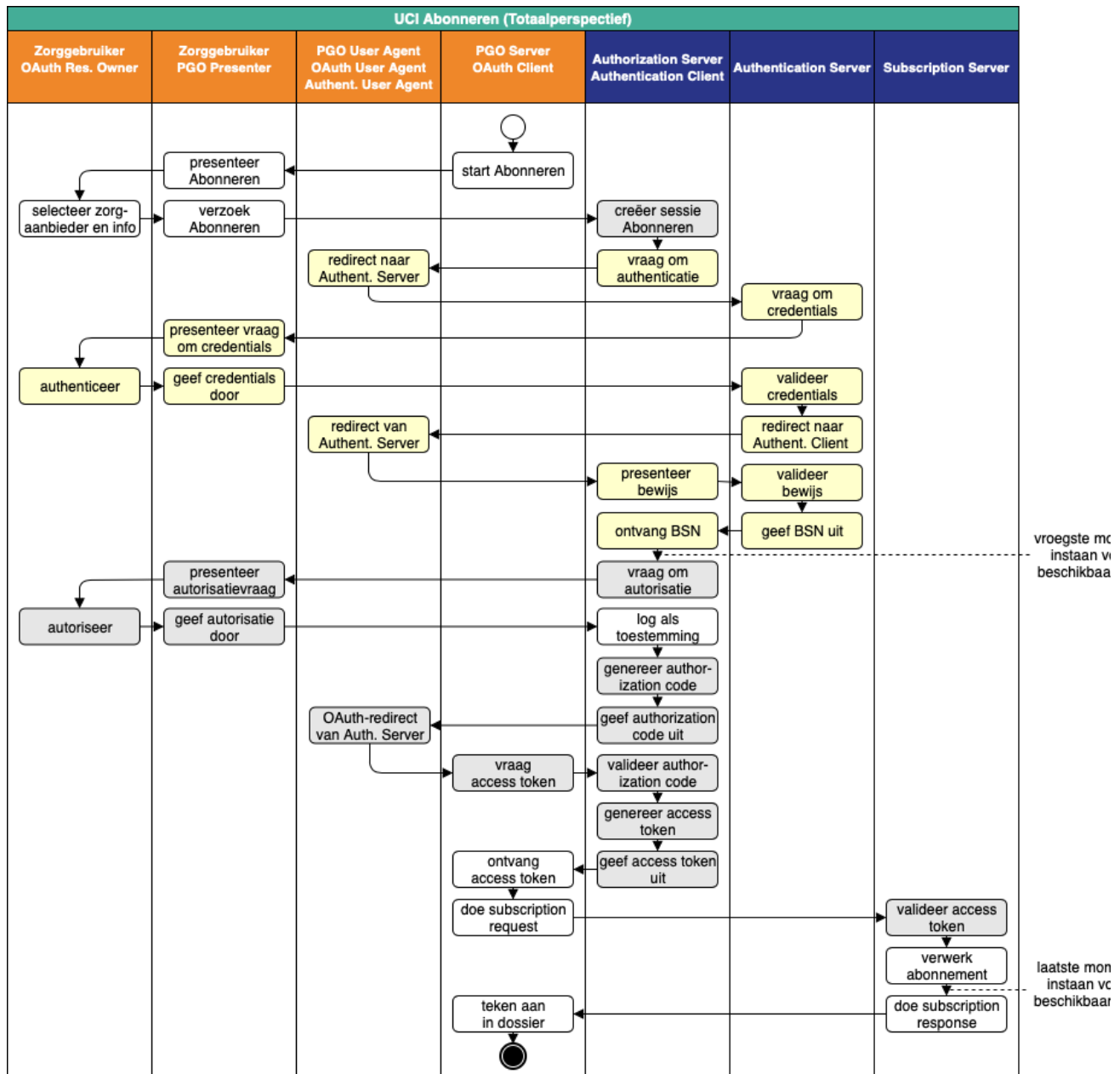
#### Toelichting

In de platen hieronder staat het stroomdiagram van de use case-implementatie UCI *Abonneren*, in vier perspectieven:

- het totaalperspectief, met zowel de happy flow als de uitzonderingen;
- het perspectief van de *PGO Server (= OAuth Client)*, die onder de hoede van de *Dienstverlener Persoon* valt. Laatstgenoemde kan deze plaat lezen als zijn verplichte aandeel in de use case-implementatie *Abonneren*;
- het perspectief van de *Authorization Server/Subscription Server/Authentication Client*, die onder de hoede van de *Dienstverlener zorgaanbieder* valt. Laatstgenoemde kan deze plaat lezen als zijn verplichte aandeel in de use case-implementatie *Abonneren*;
- het perspectief van de *Zorggebruiker (= OAuth Resource Owner)*.

De stroomdiagrammen tonen alleen de situatie waarin alle acties slagen tot en met het uiteindelijke aangaan van het *Abonnement* (de zogenaamde happy flow). De oranje banen horen, conform de MedMij-huisstijl tot het *Persoonsdomein*, de blauwe tot het *Zorgaanbiedersdomein*. Menige actie in de stroomdiagrammen is gekleurd weergegeven. De lichtgrijs gekleurde acties vormen samen de autorisatieflow volgens OAuth; de zachtgeel gekleurde acties vormen samen de authenticatieflow. Deze kleuren verwijzen dus alleen maar naar de gebruikte standaarden en zeggen niets over welke component de stap zou moeten uitvoeren. Authenticatie is dus ingebed in autorisatie. In de stroomdiagrammen voor de specifieke perspectieven hebben alleen de acties in de bij dat perspectief horende baan namen. De acties in de andere banen zijn gecomprimeerd en anoniem weergegeven.

Verantwoordelijkheden inzake uitzonderingen op de happy flow zijn opgenomen bij de respectievelijke interface, in tegenstelling tot op de [Processen & Informatie-laag](#), waar de uitzonderingen bij de use cases zijn genoemd.



## UCI Abonneren

In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

De flow kent de volgende stappen:

1. De *PGO Server* start de flow door in de *PGO Presenter* van de *Zorggebruiker* de mogelijkheid te presenteren om zich bij een zekere *Zorgaanbieder* te *Abonneren op Notificaties* voor een bepaalde *Gegevensdienst*. Het gaat altijd om precies één *Gegevensdienst*. Uit de *Zorgaanbiederslijst* weet de *PGO Server* op welke *Gegevensdiensten* een *Zorgaanbieder Abonnementen* aanbiedt worden. Desgewenst worden de *Gegevensdienstnamen* uit de *Gegevensdienstnamenlijst* gebruikt.

2. De *Zorggebruiker* maakt expliciet zijn selectie en laat de *OAuth User Agent* een abonneer-verzoek sturen naar de *Authorization Server*. Het adres van het authorization endpoint komt uit de ZAL. De `redirect_uri` geeft aan waarnaartoe de *Authorization Server* de *OAuth User Agent* verderop moet redirecten (met de authorization code).
3. Daarop begint de *Authorization Server* de OAuth-flow (in zijn rol als *OAuth Authorization Server*) door een sessie te creëren.
4. Dan start de *Authorization Server* (nu in de rol van *Authentication Client*) de authenticatieflow door de browser naar de *Authentication Server* te redirecten, onder meegeven van een `redirect_uri`, die aangeeft waarnaartoe de *Authentication Server* straks de *OAuth User Agent* moet terugsturen, na het inloggen van de *Zorggebruiker*.
5. De *Authentication Server* vraagt van de *Zorggebruiker* via zijn *PGO Presenter* om inloggegevens.
6. Wanneer deze juist zijn, redirect de *Authentication Server* de *OAuth User Agent* terug naar de *Authorization Server*, onder meegeven van een ophaalbewijs.
7. Met dit ophaalbewijs haalt de *Authorization Server* rechtstreeks bij de *Authentication Server* het BSN op.
8. Dan breekt het vroegste moment aan waarop de *Authorization Server* ervoor instaat dat de *Zorgaanbieder* voor de betreffende *Gegevensdienst* überhaupt gezondheidsinformatie van die *Persoon* beschikbaar heeft, of anders de happy flow afbreekt. Daarvan maakt deel uit dat de *Persoon* daarvoor minstens 16 jaar oud moet zijn.
9. Zo ja, dan presenteert de *Authorization Server* via de *PGO Presenter* aan *Zorggebruiker* de vraag of laatstgenoemde hem toestaat de gevraagde persoonlijke gezondheidsinformatie (*Notificaties*) aan de *PGO Server* (als *OAuth Client*) te sturen. Onder het flow-diagram staat gespecificeerd welke informatie, waarvandaan, de *OAuth Authorization Server* verwerkt in de aan *Zorggebruiker* voor te leggen [Toestemmingsverklaring Abonneren](#).
10. Bij akkoord logt de *Authorization Server* dit als toestemming, genereert een authorization code en stuurt dit als ophaalbewijs, door middel van een browser redirect met de in stap 1 ontvangen `redirect_uri`, naar de *PGO Server*. De *Authorization Server* stuurt daarbij de local state-informatie mee die hij in de eerste stap van de *PGO Server* heeft gekregen. Laatstgenoemde herkent daaraan het verzoek waarmee hij de authorization code moet associëren.
11. De *PGO Server* vat niet alleen deze authorization code op als ophaalbewijs, maar leidt er ook uit af dat de toestemming is gegeven en logt het verkrijgen van het ophaalbewijs.
12. Met dit ophaalbewijs wendt de *PGO Server* zich weer tot de *Authorization Server*, maar nu zonder tussenkomst van de *OAuth User Agent*, voor een access token.
13. Daarop genereert de *Authorization Server* een access token en stuurt deze naar de *PGO Server*.
14. Nu is de *PGO Server* gereed om het verzoek tot vaststelling van het *Abonnement* naar de *Subscription Server* te sturen. Het adres van het subscription endpoint haalt hij uit de ZAL. Hij plaatst het access token in het bericht en zorgt ervoor dat in het bericht geen BSN is opgenomen.
15. De *Subscription Server* controleert of het ontvangen token recht geeft op het gevraagde *Abonnement*. Dan breekt het uiterste moment aan waarop de *Subscription Server* ervoor moet instaan dat voor de betreffende *Gegevensdienst* de *Zorgaanbieder* de gezondheidsgegevens beschikbaar heeft. Is dat zo, dan verstuurt de *Subscription Server* deze ze in de subscription response naar de *PGO Server*. Is dat niet zo, dan breekt de *Subscription Server* de happy flow af.
16. Deze bewaart het vastgestelde *Abonnement* in het persoonlijke *Dossier*.

In de regel worden bij een eenmalig gebruik van *UCI Abonneren* het authorization interface, het token interface en het subscription interface allemaal aangesproken, in die volgorde. Mocht de *PGO Server* echter nog beschikken over een nog niet verlopen access token voor de betreffende *Zorgaanbieder-Gegevensdienst-Interfaceversie*-combinatie, dan kan het onmiddellijk het subscription interface aanspreken.

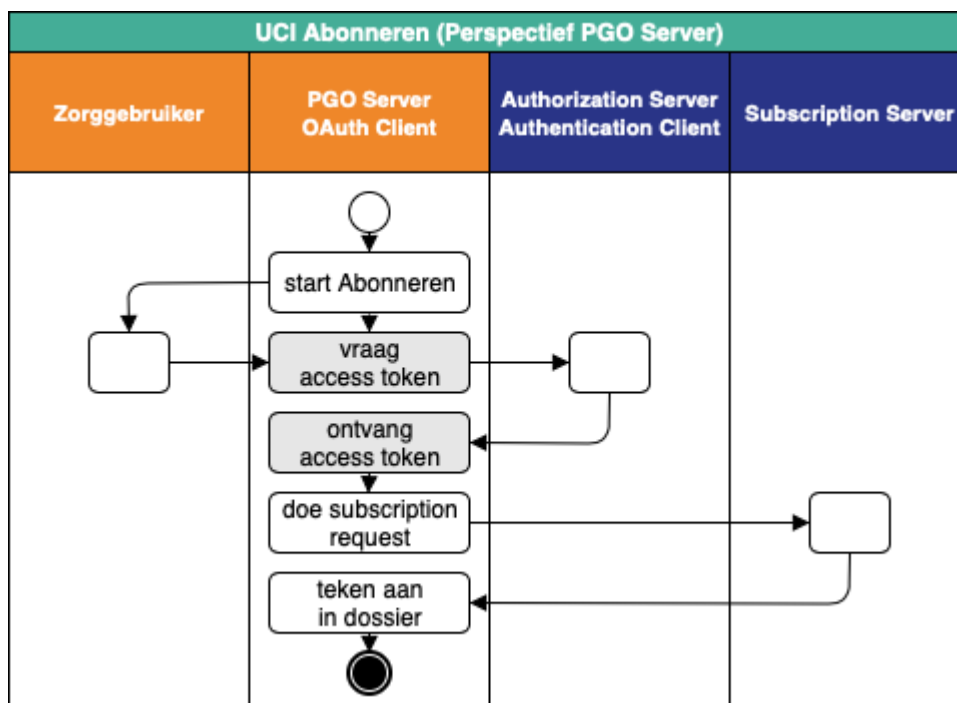
Het MedMij Afsprakenstelsel adviseert de beschikbaarheidsvoorwaarde op het vroegst aangegeven moment van kracht te laten zijn. Voorsnog staat het MedMij Afsprakenstelsel toe die voorwaarde op een later moment van kracht te laten zijn, maar niet later dan het laatste in het figuur aangegeven moment.

Bij de implementatie van de voorwaarde op beschikbaarheid bij de *Zorgaanbieder* voor de te verzamelen gezondheidsgegevens is het zaak rekening te houden met privacy-vereisten. Wanneer de *Dienstverlener zorgaanbieder* ten behoeve van de beschikbaarheidsvoorwaarde nieuwe gegevensverzamelingen zou aanleggen, vindt een verwerking altijd onder de verantwoordelijkheid van één *Zorgaanbieder* plaats. Het combineren van verwerkingen of het onvoldoende segregeren moet worden vermeden. Afwijking hiervan is alleen mogelijk onder expliciete instructie van de *Zorgaanbieder(s)* en vereist een zorgvuldige voorafgaande afweging, vanwege de daaraan verbonden privacyrisico's.

## Perspectief van de PGO Server

### Perspectief van de PGO Server

De *PGO Server* start de *UC Abonneren*. Via een redirect ontvangt hij een authorization code, waarmee hij een access token aanvraagt op het token interface. Na ontvangst van dat access token, spreekt hij de Subscription Server aan om de start, de wijziging of de beëindiging van het *Abonnement* te laten vaststellen.

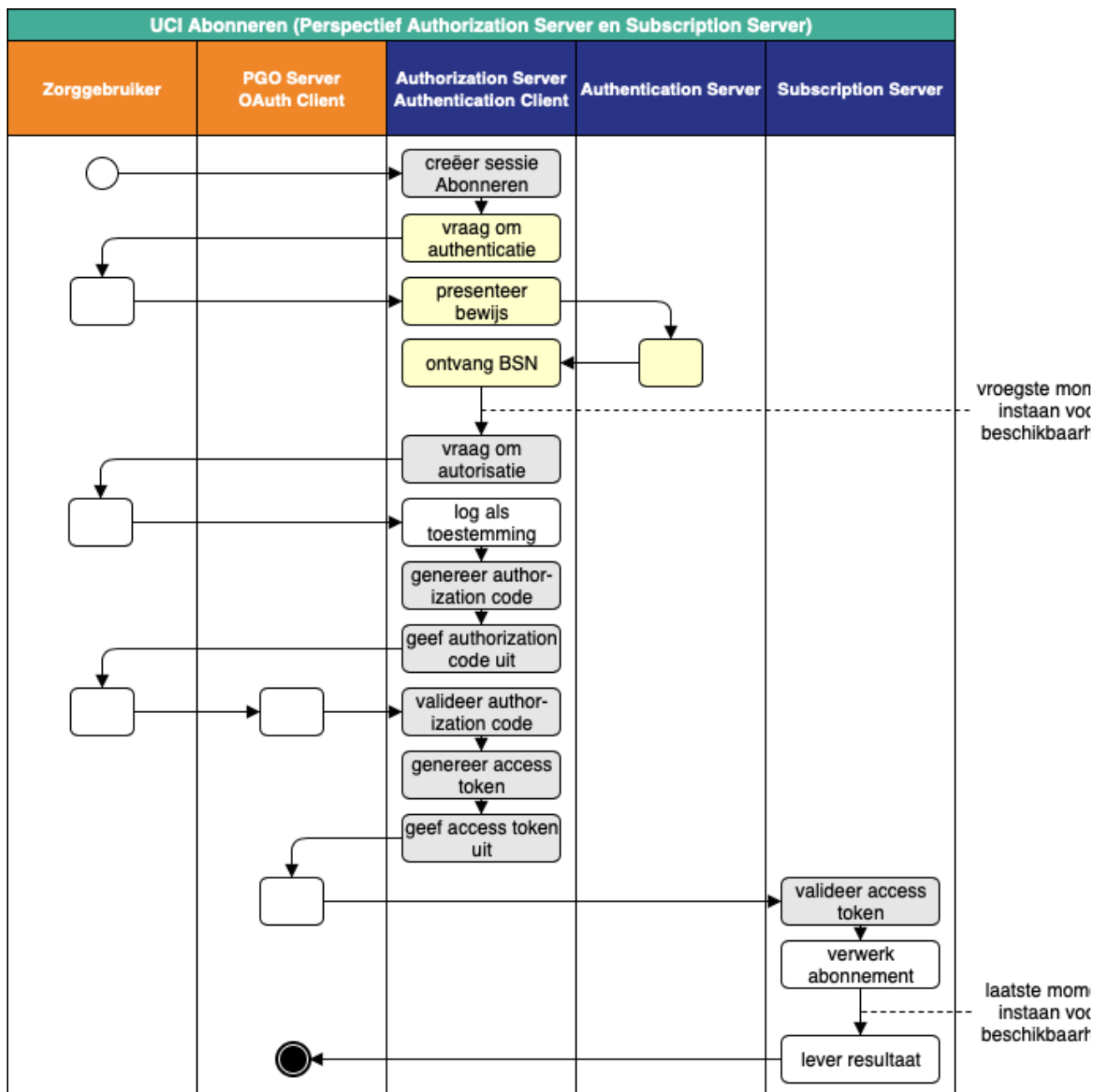


## Perspectief van de Authorization Server, Authentication Server en Subscription Server

### Perspectief van de Authorization en de Subscription Server



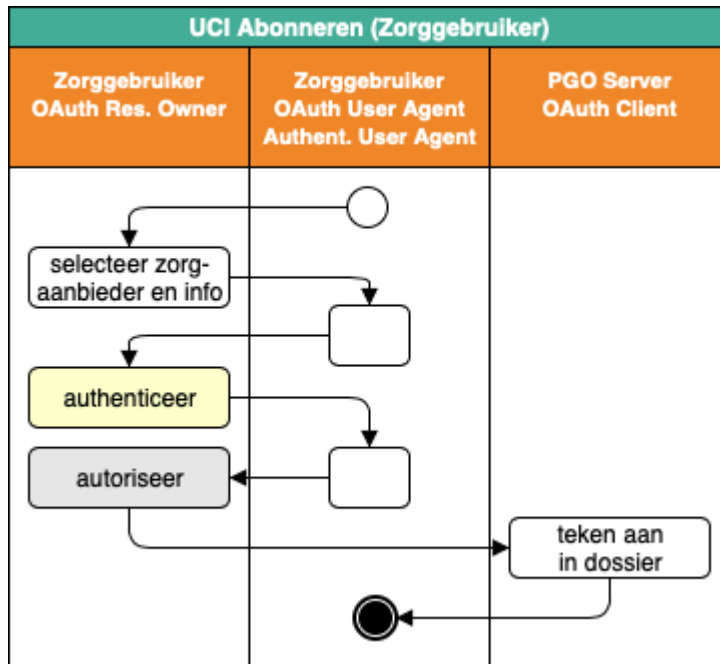
De *Authorization Server* creëert op verzoek van de *Zorggebruiker* een sessie voor *UC Abonneren* en doorloopt de gebruikelijke authenticatie- en autorisatiestappen. Via een redirect ontvangt hij een authorization code, waarmee hij een access token aanvraagt op het token interface. Na ontvangst van dat access token, spreekt hij de *Subscription Server* aan om de start, de wijziging of de beëindiging van het *Abonnement* te laten vaststellen.



### Perspectief van de *Zorggebruiker*

### Perspectief van de *Authorization* en de *Subscription Server*

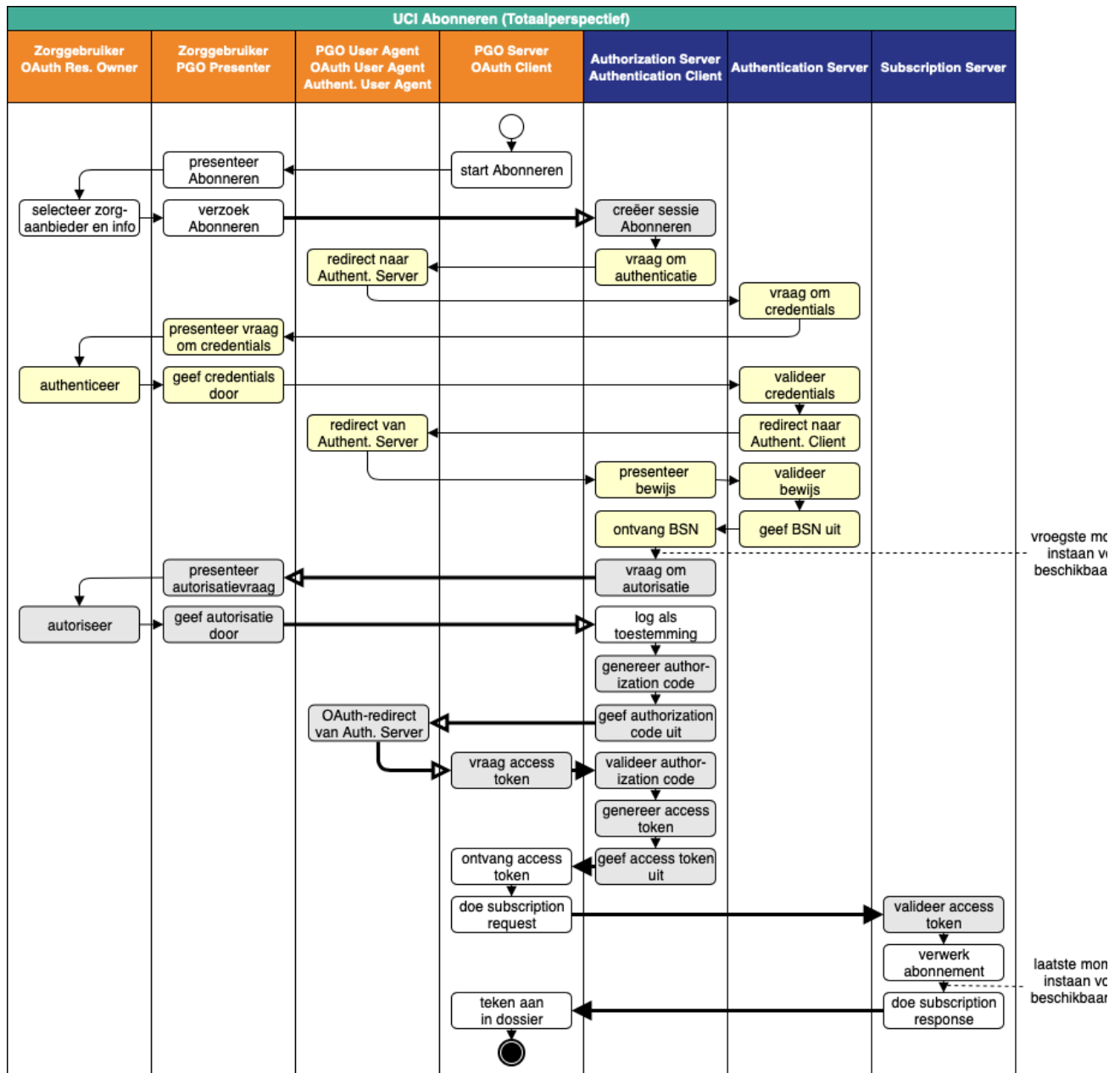
De *Zorggebruiker* selecteert de *Zorgaanbieder* en de *Gegevensdienst* waarop hij zich wenst te (her) abonneren, authenticceert zich en geeft Toestemming. Daarna tekent de PGO Server de abonnementswijziging (die hij heeft laten vaststellen door de *Subscription Server*) aan in het *Dossier*.



## Frontchannel en backchannel

### Frontchannel en backchannel

In onderstaand stroomschema van *UCI Abonneren* geven de dikke pijlen het *MedMij-verkeer* weer en zijn daarbinnen de vijf gevallen van frontchannel-verkeer (open pijlpunt) en vier gevallen van backchannel-verkeer (gesloten pijlpunt) aangegeven.



## UCI Notificeren

### UCI Notificeren

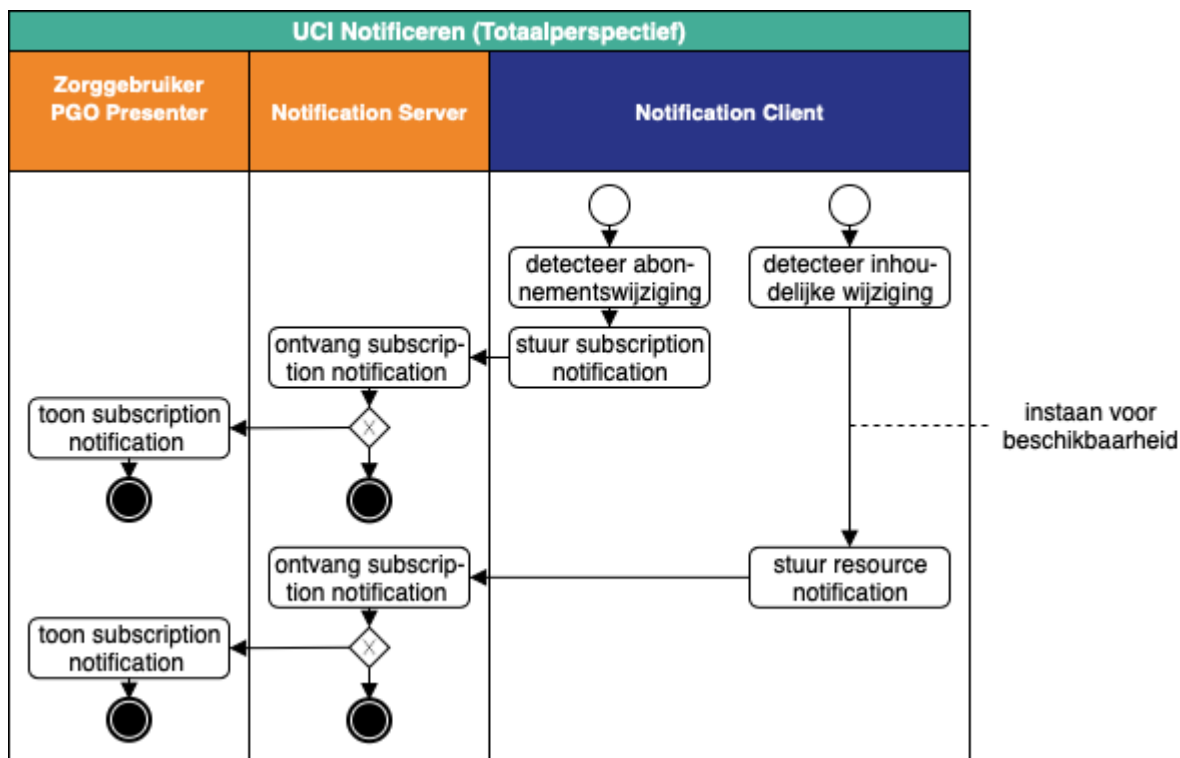
#### Toelichting

In de platen hieronder staat het stroomdiagram van de use case-implementatie *UCI Notificeren*, in vier perspectieven:

- het totaalperspectief, met zowel de happy flow als de uitzonderingen;
- het perspectief van de *Notification Server*, die onder de hoede van de *Dienstverlener persoon* valt. Laatstgenoemde kan deze plaat lezen als zijn verplichte aandeel in de use case-implementatie *Abonneren*;
- het perspectief van de *Notification Client*, die onder de hoede van de *Dienstverlener zorgaanbieder* valt. Laatstgenoemde kan deze plaat lezen als zijn verplichte aandeel in de use case-implementatie *Abonneren*;
- het perspectief van de *Zorggebruiker* (= *OAuth Resource Owner*).

De stroomdiagrammen tonen alleen de situatie waarin alle acties slagen tot en met het uiteindelijke aangaan van het *Abonnement* (de zogenaamde happy flow). De oranje banen horen, conform de MedMij-huisstijl tot het *Persoonsdomein*, de blauwe tot het *Zorgaanbiedersdomein*. Menige actie in de stroomdiagrammen is gekleurd weergegeven. De lichtgrijs gekleurde acties vormen samen de autorisatieflow volgens OAuth; de zachtgeel gekleurde acties vormen samen de authenticatieflow. Deze kleuren verwijzen dus alleen maar naar de gebruikte standaarden en zeggen niets over welke component de stap zou moeten uitvoeren. Authenticatie is dus ingebed in autorisatie. In de stroomdiagrammen voor de specifieke perspectieven hebben alleen de acties in de bij dat perspectief horende baan namen. De acties in de andere banen zijn gecomprimeerd en anoniem weergegeven.

Verantwoordelijkheden inzake uitzonderingen op de happy flow zijn opgenomen bij de respectievelijke interface, in tegenstelling tot op de [Processen & Informatie-laag](#), waar de uitzonderingen bij de use cases zijn genoemd.



## UCI Notificeren

### Toelichting

In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

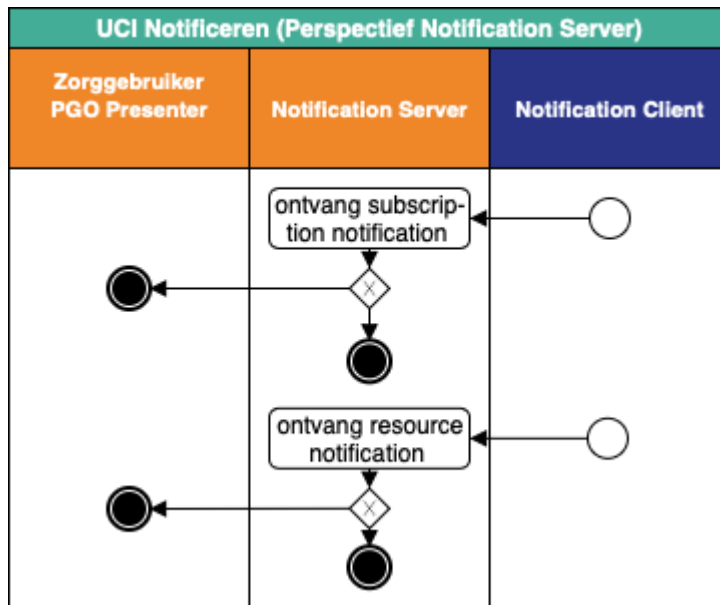
De flow kent de volgende stappen:

1. De *Notification Client* detecteert een inhoudelijke wijziging in de gezondheidsinformatie waarop *Zorggebruiker* een geldig *Abonnement* is aangegaan, respectievelijk de *Notification Client* detecteert dat de *Zorgaanbieder* een zeker abonnement beëindigt.
2. In beide gevallen bepaalt de *Notification Client*, o.b.v. de *client\_id* die werd gebruikt bij het aangaan van het *Abonnement*, in de *OAuth Client List* het juiste *Resource Notification Endpoint*, respectievelijk *Subscription Notification Endpoint*.
3. De *Notification Client* stuurt subscription notification, respectievelijk resource notification naar de *Notification Server*.
4. De *Notification Server* controleert de *Notificatie*, laat deze eventueel aan de *Zorggebruiker* tonen, en verstuurt een antwoord naar de *Notification Client*.

## Perspectief van de *Notification Server*

### Notification Server

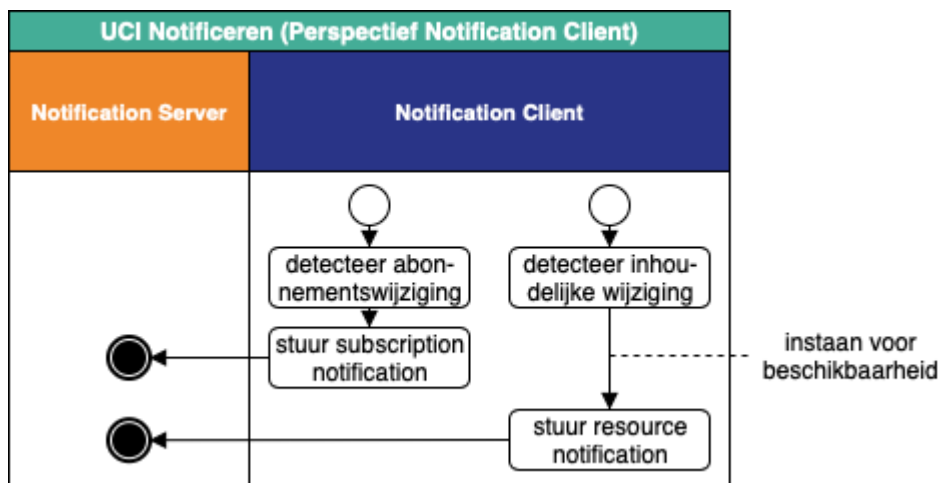
De *Notification Server* ontvangt een subscription notification of een resource notification en speelt deze mogelijk door aan de *Zorggebruiker* (*PGO Presenter*).



#### Perspectief van de *Notification Client*

##### Notification Client

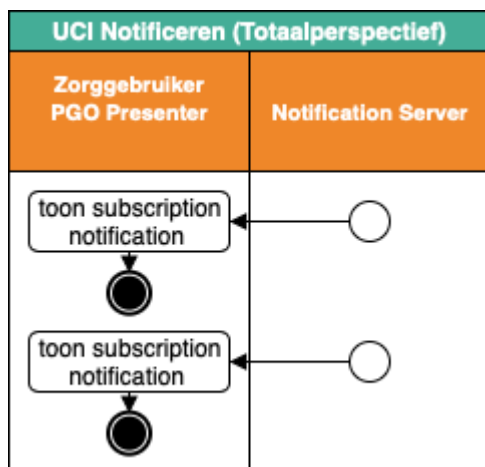
De *Notification Client* detecteert een inhoudelijke wijziging, respectievelijk een abonnementswijziging, en stuurt een subscription notification, respectievelijk een resource notification, naar de *Notification Server*.



#### Perspectief van de *Zorggebruiker*

##### Zorggebruiker

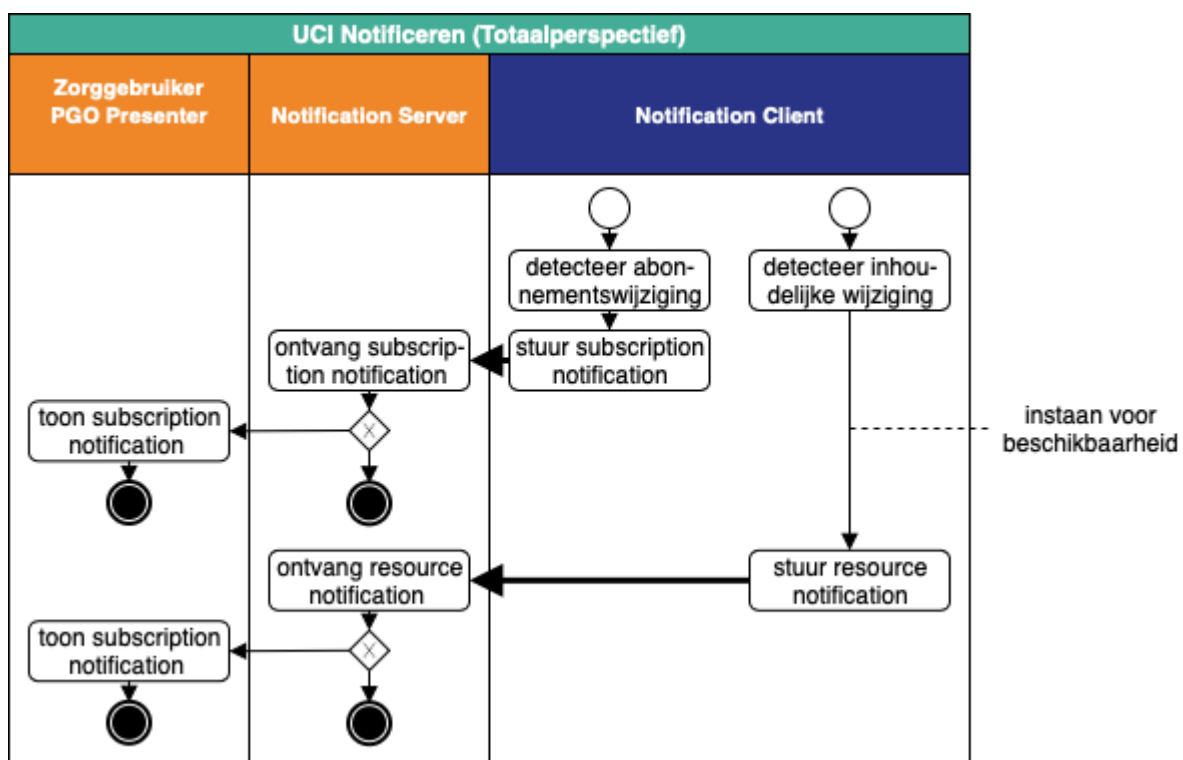
De *PGO Presenter* toont een subscription notification of een resource notification.



## Frontchannel en backchannel

### Frontchannel en backchannel

Beide soorten *Notificaties* betreffen backchannel-verkeer.



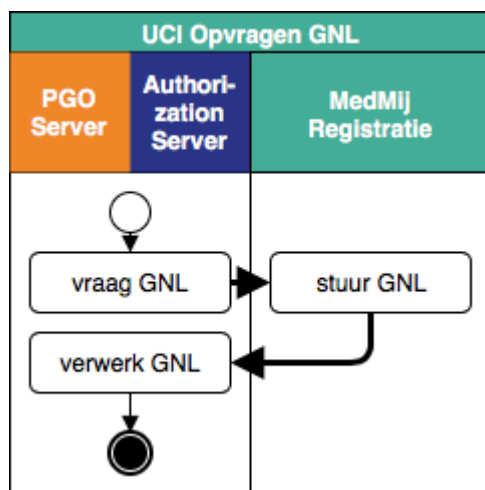
## UCI Opvragen GNL

### Stroomdiagram

#### Toelichting

In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen. In de linkerbaan betekent dat: één *PGO Server* of één *Authorization Server*.

Beide interacties met *MedMij Registratie* zijn backchannel-verkeer.





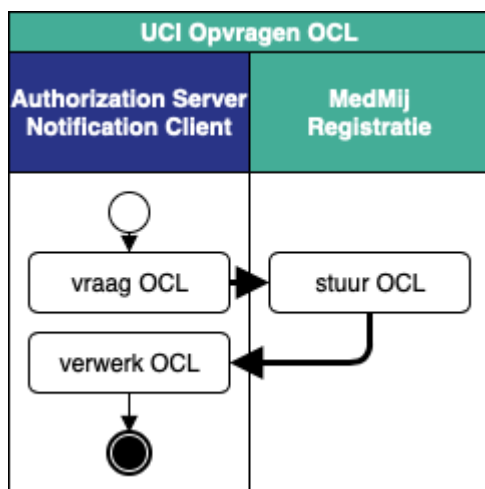
## UCI Opvragen OCL

### Stroomdiagram

#### Toelichting

In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

Beide interacties met *MedMij Registratie* zijn backchannel-verkeer.



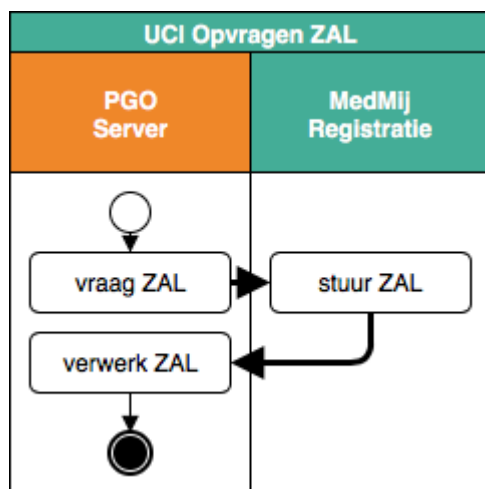
## UCI Opvragen ZAL

### Stroomdiagram

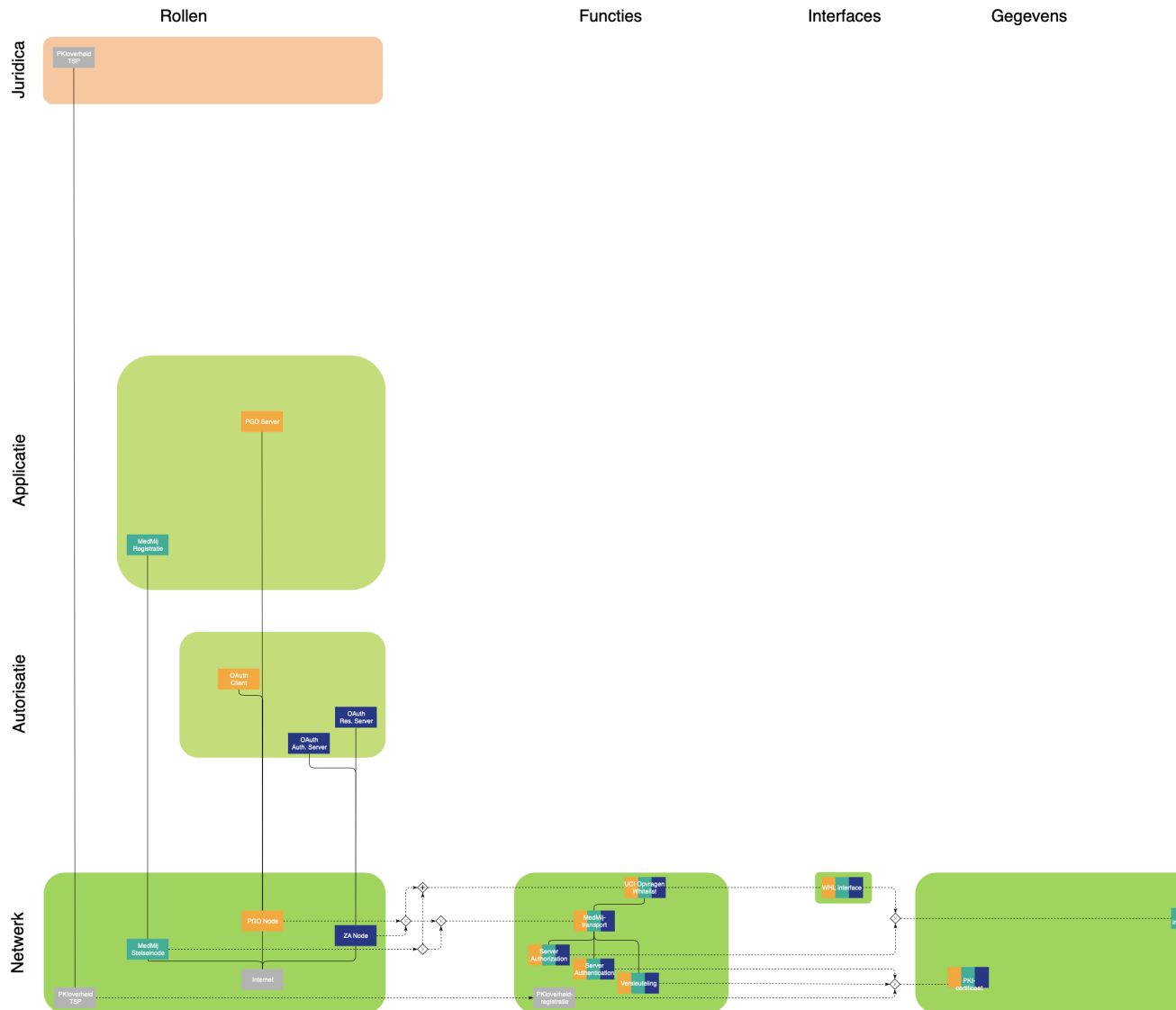
#### Toelichting

In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen.

Beide interacties met *MedMij Registratie* zijn backchannel-verkeer.



## Netwerk



### Inleiding

Op deze laag worden de infrastructurele rollen (*Nodes*) op het MedMij-netwerk bepaald en voorzien van verantwoordelijkheden op het gebied van versleuteling, authenticatie van *Nodes* en autorisatie van *Nodes*. Met dat laatste wordt bedoeld dat er steeds opnieuw moet worden vastgesteld dat een *Node* gerechtigd is zich te bewegen op het MedMij-netwerk. Voor versleuteling en authenticatie worden PKI-certificaten gebruikt.

Autorisatie zou op grofweg twee manieren in het MedMij Afsprakenstelsel kunnen worden opgenomen:

- via diezelfde PKI-certificaten, waarin aan de domeinnaam van de houder van het certificaat gezien kan worden of het om een *MedMij Node* gaat, door daarvan te eisen dat die domeinnaam de vorm `<dienstverlener>.medmij.nl` heeft;

- via een door MedMij-zelf beheerde lijst van geautoriseerde *MedMij Nodes* (een whitelist).

De voordelen van de eerste optie zouden zijn dat:

- er zo maximaal gebruik wordt gemaakt van afspraken die ook voor andere doeleinden al nodig zijn, namelijk het gebruik van PKI-certificaten;
- zo de mate van operationele centrale betrokkenheid van de Stichting MedMij wordt geminimaliseerd, en dus de kosten en risico's daarvan. In de tweede optie zou Stichting MedMij zelf een lijst moeten gaan beheren en ontsluiten naar alle servers om het operationele verkeer mogelijk te maken. In de eerste optie is alleen een name service nodig voor de [medmij.nl](https://medmij.nl)-domeinnamen. Dat laatste is een goed gestandaardiseerde, goed begrepen en goed uit te besteden service, die lagere kosten, lagere risico's en minder afhankelijkheid voor de deelnemers met zich mee zal brengen;
- MedMij zich zo maximaal houdt aan haar [architectuurprincipe P6](#): MedMij spreekt alleen af wat nodig is.

Toch is voor de tweede optie gekozen, omdat de voor de eerste optie benodigde controle over de hostnames en de certificaten alleen met ongewenste bijeffecten gepaard zou gaan. De volgende opties zijn daarbij verkend:

- De MedMij-beheerorganisatie wordt **Registration Authority (RA)** in PKI-overheid, jegens alle betrokken Certificate Authorities (CA's). PKI-overheid kent echter die mogelijkheid niet.
- De MedMij-beheerorganisatie geeft een **domeinverklaring** af, zodat deelnemers zelf een subdomein onder [.medmij.nl](https://medmij.nl) kunnen aanvragen bij een CA. Daarmee heeft de beheerorganisatie wel invloed op de uitgifte van een certificaat, maar laten intrekken is niet mogelijk, tenzij er sprake is van misbruik. Er is immers geen juridische relatie tussen de eigenaar van het domein (de beheerorganisatie) en de CA.
- Analooq aan de wijze waarop door sommigen beroepsgebonden certificaten worden uitgegeven, is een **maatwerk-certificeringsdienst** denkbaar. In de voorwaarden van het product (geldend vanaf de aanvraag van het certificaat) wordt dan expliciet geregeld dat wanneer de inschrijving in een extern register wegvallt, het certificaat door de CA wordt ingetrokken. Dat vereist dat de registerhouder (beheerorganisatie) wijzigingen doorgeeft aan alle CA's. Dit is economisch pas interessant bij een aanzienlijke hoeveelheid certificaathouders, waarvan in MedMij voorlopig geen sprake zal zijn.
- MedMij zou een **eigen PKI-omgeving** kunnen inrichten (afwijkend van PKI-Overheid). Dit is niet verder verkend, vanwege de complexiteit en verantwoordelijkheid die op de schouders van de beheerorganisatie zou rusten.
- De Stichting MedMij zou zelf **houder** kunnen zijn van alle certificaten, waarbij deelnemers gemandateerd worden voor beheerstaken rond hun eigen subset van certificaten. De Stichting kan certificaten intrekken. Identificatie van de dienstverlener naar de gebruiker is niet mogelijk, want de certificaten staan op naam van Stichting MedMij.
- Er zou een **custom field** gebruikt kunnen worden in certificaten. De MedMij Beheerorganisatie zou de controle kunnen krijgen over de wijze waarop met dit veld wordt omgegaan. Dit vereist waarschijnlijk afspraken met alle CA's. Dit geeft controle op het uitgeven van certificaten, maar geeft de beheerorganisatie geen mogelijkheden het certificaat te laten intrekken.

Onderstaande tabel vat samen hoe in de verantwoordelijkheden op deze laag de beveiligingsfuncties beveiliging, authenticatie en autorisatie worden ingericht. Het onderscheid, bij autorisatie, tussen inkomend en uitgaand verkeer is het gevolg van dat in deze twee gevallen de identificatie van de andere *Node* anders plaatsvindt.

frontchannel- verkeer	uitgaand backchannel- verkeer	inkomend backchannel-verkeer
--------------------------	----------------------------------	---------------------------------

versleuteling volgens TLS, met PKI-overheid-certificaat	altijd		
identificatie op basis van ...	redirect_uri of Zorgaanbiederslijst		PKI-overheid- certificaat
authenticatie, op basis van PKI-overheid-certificaat, van ...	alleen de TLS-server	TLS-client én TLS-server	
autorisatie op basis van controle tegen de <i>Whitelist</i>	niet	voorafgaand aan de TLS-handshake	zie verantwoordelijkheid 14a

## Rollen

### 1. In het *MedMij-netwerk* functioneert:

- elke *PGO Server*, met inbegrip van zijn *OAuth*-rol, op één of meerdere *PGO Nodes*. Voor al diens frontchannel-verkeer gebruikt elke *PGO Server* één *PGO Node*, en wel met een hostname die voor die *PGO Server* voorkomt op de *OAuth Client List*.
- elke *Authorization Server*, met inbegrip van zijn *OAuth*-rol, op één of meer *ZA Nodes*;
- elke *Subscription Server*, met inbegrip van zijn *OAuth*-rol, op één of meer *ZA Nodes*;
- elke *Notification Client* op één of meer *ZA Nodes*;
- elke *Notification Server* op één of meer *PGO Nodes*;
- elke *Resource Server*, met inbegrip van zijn *OAuth*-rol, op één of meer *ZA Nodes*;
- precies één *MedMij Stelselnode*, waarop *MedMij Registratie* functioneert.

#### Toelichting

Voor de algemene uitgangspunten inzake de getalsverhoudingen tussen de rollen, zie de pagina [Architectuur en technische specificaties](#).

De uitzondering daarop inzake het frontchannel-verkeer is noodzakelijk om de *OAuth Client List* te laten functioneren. Het is dus mogelijk voor een *PGO Server* om verschillende certificaten te hanteren voor frontchannel- en backchannel-verkeer, zolang op de *OAuth Client List* maar de hostname in het certificaat voor frontchannelverkeer voorkomt die tevens voorkomt in de redirect URI inzake *OAuth*.

Er is precies één *MedMij Stelselnode* in het *MedMij-netwerk*. Zonder die *MedMij Stelselnode* is er geen *MedMij-netwerk*.

In lijn met keuzes op de [Proces- en Informatielaag](#), treden in het zorgaanbiedersdomein alleen de *ZA Nodes* op in het *MedMij-netwerk*. Dat wil zeggen dat bijvoorbeeld achterliggende xLS'en niet over het *MedMij-netwerk* communiceren met de *ZA Node*. Dat verkeer is verborgen achter de *ZA Node*. Alle daarvoor benodigde routing wordt afgehandeld door de server-implementaties en speelt zich buiten het zicht van het *MedMij Afsprakenstelsel* af.

### 2. Op één:

- *PGO Node* functioneert hetzij één *PGO Server*, hetzij één *Notification Server*, hetzij de combinatie van één *PGO Server* en één *Notification Server*.

- *ZA Node* functioneert hetzij één *Authorization Server*, hetzij één *Resource Server*, hetzij één *Subscription Server*, hetzij één *Notification Client*, hetzij een combinatie van voorgaande rollen.

#### Toelichting

Voor de algemene uitgangspunten inzake de getalsverhoudingen tussen de rollen, zie de pagina [Architectuur en technische specificaties](#).

3. Een of meerdere *PKI-overheid TSP*s treden op als *PKI-overheid TSP*.

## Verantwoordelijkheden

### TLS en certificaten

- 1a. Al het verkeer over het *MedMij-netwerk* is beveiligd met [Transport Layer Security](#) (TLS).

1b. Er wordt enkel gebruik gemaakt van TLS-versies en -algoritmen die zijn geclassificeerd als "goed" in de [ICT-beveiligingsrichtlijnen voor Transport Layer Security \(TLS\), versie 2.0](#) van het NCSC. Een *Node* biedt alleen TLS 1.3 aan als hij ook TLS 1.2 aanbiedt.

#### Algoritmen

Het is niet verplicht om *alle* algoritmen aan te bieden die in de genoemde richtlijnen als "goed" zijn geclassificeerd.

- 1c. Gebruik van [TLS False Start](#) is verboden.

#### Toelichting

Gebruik van [TLS False Start](#) is verboden om te voorkomen dat er inhoudelijke verwerking plaatsvindt van uitgewisselde gegevens voordat voor de betreffende uitwisseling authenticatie en autorisatie geslaagd zijn (zie onder).

2. Om zich te kunnen authenticeren en autoriseren op het *MedMij-netwerk*, kunnen elke *PGO Node*, elke *ZA Node* en de *MedMij Stelselnode* een *PKI-overheid*-certificaat overleggen, en wel een server-certificaat van een *PKI-overheid TSP*.

3. Alle certificaathouders verbinden zich aan de op hen toepasselijke eisen van het *PKI-overheid*-stelsel. Een organisatie mag meerdere certificaten hebben.

#### Toelichting

De keuze voor de [PKI](#)-standaard past bij [principe](#) P19 van het MedMij Afsprakenstelsel. Er bestaan andere manieren voor, en ideeën over, het borgen van vertrouwen in een netwerk van geautomatiseerde systemen, maar deze zijn nog lang niet zo bewezen als PKI, dat wereldwijd wordt ondersteund, en wereldwijd is beproefd, door overheden en marktspelers.

Bij gebruik van de PKI-standaard doet zich de vraag voor van welk(e) PKI-stelsel(s) gebruik gemaakt kan of moet worden. Zo'n PKI-stelsel voorziet in een hiërarchie van organisaties die certificaten uitgeven, zodanig dat de betrouwbaarheid van de certificaten van zo'n organisatie leunt op de betrouwbaarheid van de eerst-hogere organisatie in die hiërarchie, doordat de certificaten van de lagere-in-hiërarchie een handtekening hebben van die van de hogere-in-hiërarchie. Aan de top van zo'n hiërarchie staat een zogenoemde root Certificate Authority (root CA) die zijn betrouwbaarheid

niet aan een hogere kan ontleen, zijn eigen (stam)certificaten tekent, en zo een steunpilaar is van het vertrouwen in het hele betreffende PKI-stelsel.

Het MedMij Afsprakenstelsel had ervoor kunnen kiezen een PKI-stelsel specifiek voor MedMij in te richten, maar de kosten daarvan, voor zichzelf en voor haar deelnemers, wegen niet op tegen de voordelen, onder de voorwaarde dat er een ander geschikt PKI-stelsel voorhanden is. Deelnemers zullen met hun services immers ook in andere afsprakenstelsels betrokken kunnen zijn dan dat van MedMij. Zo'n keuze past bovendien niet bij [principe P6](#).

Omdat het MedMij-netwerk een nationale en maatschappelijk kritische infrastructuur is, met hoge eisen aan betrouwbaarheid, kiest het MedMij Afsprakenstelsel voor het momenteel enige PKI-stelsel waarin de betrouwbaarheid uiteindelijk steunt op een Nederlandse publiekrechtelijke rechtspersoon: [PKloverheid](#) met de Staat der Nederlanden als root CA. Zo is de governance van de root CA transparant en toegankelijk belegd.

Het MedMij Afsprakenstelsel bouwt voor het door hem aan zijn deelnemers geboden vertrouwen dus mede op het PKloverheid-stelsel, op het door dat stelsel vastgestelde [programma van eisen](#) voor de in dat stelsel betrokken TSP's en op de [certificatiehiërarchie](#) van PKloverheid. Deelnemers in het MedMij Afsprakenstelsel zullen dus service-certificaten moeten betrekken bij een bij PKloverheid [aangesloten TSP](#) die bij haar past.

## Functie *Versleuteling*

4. Op het *MedMij-netwerk* wordt al het verkeer versleuteld volgens TLS, zoals bedoeld in verantwoordelijkheid 1.

## Functie *Server Authentication*

5. Tijdens de handshake van TLS, zoals bedoeld in verantwoordelijkheid 1, wordt door de TLS-server in de `server hello`-stap aan de TLS-client:

- in geval van backchannel-verkeer, altijd een verzoek om een certificaat gedaan. Indien de TLS-client daarop geen certificaat overlegt, wordt de handshake onmiddellijk afgebroken.
- in geval van frontchannel-verkeer, nooit een verzoek om een certificaat gedaan.

### Toelichting

Bij backchannel-verkeer vindt dus twee-wegauthenticatie plaats, bij frontchannel-verkeer een-wegauthenticatie.

6a. *ZA Node*, *PGO Node* en *MedMij Stelselnode* valideren tijdens de TLS-handshake aan het begin van een TLS-sessie of het een PKloverheid-certificaat is en controleren bij de *Certification Authority* of het ontvangen certificaat geldig is, op basis van [CRL](#) of [OCSP](#). In geval van het falen van één van deze controles wordt het certificaat niet geaccepteerd en de TLS-sessie niet gestart.

6b. In geval van het gebruik van [OCSP](#) in het kader van verantwoordelijkheid 6a mag de OCSP response vastgeniet zitten aan het certificaat ([OCSP Stapling](#)).

### Certificate revocation

Het laten vastnieten van een OCSP-antwoord aan het certificaat is toegestaan in het Afsprakenstelsel MedMij. De ontvanger mag dit OCSP-antwoord gebruiken maar kan de controle of het certificaat ingetrokken is ook op een andere manier uitvoeren. Wanneer ervoor gekozen is om de controle alleen via OCSP uit te voeren kan het voorkomen dat een OCSP responder geen of niet

tijdig een antwoord geeft. In dat geval kan ervoor gekozen worden om de TLS sessie toch op te zetten (soft-fail). Het primaire mechanisme binnen het MedMij Afsprakenstelsel om te bepalen of nodes elkaar mogen benaderen is de *Whitelist*-controle.

Voor alle eisen gerelateerd aan PKI-overheid-certificaten, zie <https://www.logius.nl/diensten/pkioverheid/aansluiten-als-tsp/pogramma-van-eisen>.

6c. Met inachtneming van verantwoordelijkheid 6a, accepteren *ZA Node*, *PGO Node* en *MedMij Stelselnode* PKI-overheid certificaten van elkaar door:

- alle root-certificaten te vertrouwen zoals gepubliceerd op <https://cert.pkioverheid.nl/>;
  - waarvan de geldigheidsdatum niet is verlopen en die NIET zijn ingetrokken;
  - met uitzondering van de onderstaande root certificaten (deze zijn NIET toegestaan):
    - de zogenaamde 'TEST' certificaten
    - Alle roots gemarkeerd met 'Persoon'
- deelnemers moeten alle valide domein en TSP certificaten onder PKI hiërarchie opnemen in de truststore; zie hiervoor <https://cert.pkioverheid.nl/>;
  - met uitzondering van (deze roots moeten NIET opgenomen worden):
    - Organisatie Persoon
    - Burger
    - Autonome apparaten
    - Private Personen
  - ook de zogenaamde intermediate-certificaten moeten worden opgenomen in de truststore.

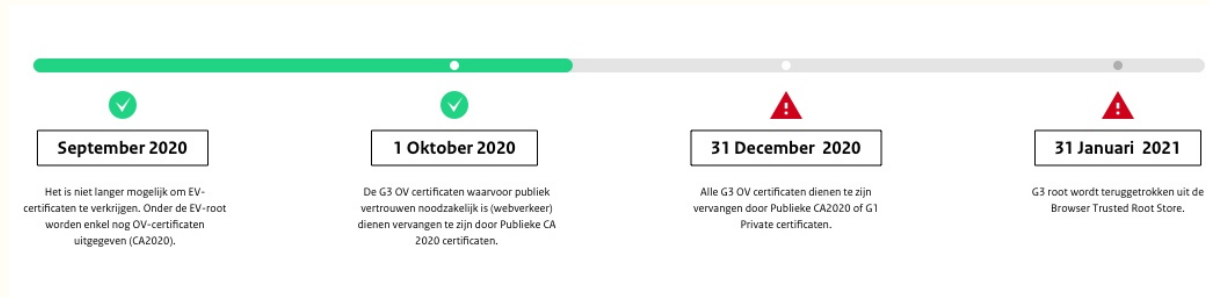
### Toelichting

- Voor alle frontchannel (internet-facing) verkeer moeten deelnemers een PKI-overheid-certificaat van het type 'publiek' toepassen, uitgegeven door de volgende keten en/of opvolgende generaties:
  - Stamcertificaat
    - Staat der Nederlanden EV Root CA
  - Intermediair Domein Server CA 2020
    - QuoVadis PKI-overheid Server CA 2020
    - Digidentity PKI-overheid Server CA 2020
    - KPN PKI-overheid Server CA 2020
- Voor alle backchannel verkeer (machine2machine) moeten deelnemers een PKI-overheid-certificaat van het type 'privaat' toepassen, uitgegeven door de volgende keten en/of opvolgende generaties:
  - Private Root CA (per medio 2020 de standaard voor m2m)
    - Stamcertificaat
      - Staat der Nederlanden Private Root CA - G1
    - Domein Private Services, maar alleen de volgende:
      - Staat der Nederlanden Private Services CA - G1
      - KPN PKI-overheid Private Services CA - G1
      - QuoVadis PKI-overheid Private Services CA - G1
      - Digidentity BV PKI-overheid Private Services CA - G1

Omdat het vastnieten van OCSP antwoorden (stapling) is toegestaan, zal iedere *Node* welke een certificaat moet controleren het vastnieten in zoverre moeten ondersteunen dat het alleen het feit dat er een vastgeniet OCSP antwoord gebruikt wordt niet mag leiden tot een foutmelding of het anderszins plots beëindigen van de TLS handshake of sessie.



## Let op: G3 ondersteuning tot 31 december 2020



Voorheen werd voor het backchannel verkeer gebruikgemaakt van zogenoemde G3 certificaten. Deze moeten vervangen worden door G1 certificaten. Logius heeft de uiterste datum voor het vervangen van G3 certificaten gezet op 31 december 2020. Tot die tijd moeten deze certificaten ondersteund blijven, zodat de verschillende systemen binnen het afsprakenstelsel met elkaar kunnen blijven communiceren. Het gaat hierbij om:

- Stamcertificaat
  - Staat der Nederlanden Root CA - G3
- Domein Organisatie Services - Server
  - Staat der Nederlanden Organisatie Services CA - G3
  - Digidentity BV PKIoverheid Organisatie Server CA - G3 (2018)
  - Digidentity BV PKIoverheid Organisatie Server CA - G3 (2019)
  - KPN BV PKIoverheid Organisatie Server CA - G3 (2016)
  - KPN BV PKIoverheid Organisatie Server CA - G3 (2019)
  - QuoVadis PKIoverheid Organisatie Server CA - G3 (2016)
  - QuoVadis PKIoverheid Organisatie Server CA - G3 (2019)

6d. PKIoverheid certificaten moeten (in ieder geval op productie en acceptatie omgevingen) als complete keten inclusief alle intermediate certificaten worden verstuurd en gecontroleerd. Een certificaat keten bestaat uit het certificaat zelf, aangevuld met alle intermediate certificaten die worden meegeleverd door de CSP, de uitgevende instantie van het betreffende certificaat. Het root certificaat moet niet meegeleverd worden (dit is al aanwezig in de truststore van de tegenpartij).

## Functie *Server Authorization*

### Verspreiding van de *Whitelist*

7. De *MedMij Stelselnode* biedt aan *PGO Node* en *ZA Node* een use case-implementatie (*UCI Opvragen WHL*) om de actuele versie van de *WHL-implementatie* op te vragen. Betrokken rollen gebruiken hiervoor het betreffende [stroomdiagram](#).

#### Toelichting

De *WHL-implementatie* is de implementatie van de *Whitelist* in XML.

8. Het aandeel van de *MedMij Stelselnode* in *UCI Opvragen WHL* is voor minstens 99,9% van de tijd beschikbaar. *MedMij Registratie* laat, na het niet beschikbaar raken van het aandeel van *MedMij Stelselnode* in de use case, maximaal acht uren (480 minuten) verstrijken voordat het weer beschikbaar is.

9. *PGO Nodes* en *ZA Nodes* betrekken minstens elke vijftien minuten (900 seconden) de meest recente *WHL-implementatie* van *MedMij Stelselnode*.

10. De *MedMij Stelselnode* heeft `stelselnode.medmij.nl` als hostname. De *MedMij Stelselnode* staat niet op de *WHL-implementatie*, maar wordt er voor de controle tegen de *Whitelist-implementatie* wel geacht op te staan.

#### Toelichting

Door op deze manier de *MedMij Stelselnode* te autoriseren voor MedMij-verkeer wordt ervoor gezorgd dat ook in foutsituaties of bootstrap-situaties een *PGO Node* of *ZA Node* de *MedMij Stelselnode* kan aanspreken om een *WHL-implementatie* op te halen.

11. *PGO Nodes* en *ZA Nodes* valideren elke nieuw verkregen *Whitelist* tegen het [XML-schema van de Whitelist](#). Dit XML-schema is een technische implementatie van het [MedMij-metamodel](#). Alle hostnames op de *Whitelist* zijn fully-qualified domain names, conform [RFC3696](#), [sectie 2](#)

12. Ten behoeve van de technische beveiliging van het gegevensverkeer dat zich voltrekt in het kader van *UCI Opvragen WHL* maken betrokken rollen gebruik van *Versleuteling*, *Server Authentication* en *Server Authorization*, volgens het bepaalde op deze [Netwerk-laag](#).

#### Gebruik van de *Whitelist*

13. *ZA Node*, *PGO Node* en *MedMij Stelselnode* laten, elk hunnerzijds, backchannel-verkeer over het *MedMij-netwerk* dan en alleen dan doorgang vinden, nadat zij hebben vastgesteld dat de hostname van de andere *Node*, waarmee verbinding gemaakt zou worden, op de meest actuele *Whitelist* voorkomt.

#### Toelichting

In geval van frontchannel-verkeer vindt er geen *Server Authorization* plaats.

14a. De *Node* die

- de TLS-client zou worden voert de in verantwoordelijkheid 13 bedoelde controle tegen de *Whitelist* uit voorafgaand aan de start van de TLS-handshake. Indien die controle niet kan worden uitgevoerd of een negatief resultaat oplevert, wordt de TLS-handshake niet gestart.
- de TLS-server is, voert de in verantwoordelijkheid 13 bedoelde controle tegen de *Whitelist* geheel uit voordat enige volgende stap wordt gezet door de *OAuth AuthorizationServer* of *OAuth Resource Server*, volgens de specificaties van [UCI Verzamelen](#), [UCI Delen](#), [UCI Abonneren](#) en [UCI Notificeren](#). Deze vereiste wordt volgordelijkheid genoemd. Indien de controle tegen de *Whitelist* niet kan worden uitgevoerd, of een negatief resultaat oplevert, wordt de procesgang onmiddellijk afgebroken en komt het niet tot een start van de uitvoering van die eerstvolgende stap. De controle tegen de *Whitelist* slaagt in dit geval dan en slechts dan als op de *Whitelist* tenminste een van de volgende namen uit het de door de TLS-client aangeboden certificaat voorkomen: de `Common Name` of een van de eventuele `Subject Alternative Names`

14b. Voor zover de *Dienstverlener Zorgaanbieder* ervoor kiest de controle tegen de *Whitelist* na afloop van de TLS-handshake uit te voeren, is deze controle logisch gescheiden van de bedoelde eerstvolgende stap. De vereiste volgordelijkheid kan worden aange-toond door middel van code-inspecties, penetratietesten en inspecties van logs.

#### Toelichting

In geval van uitgaand verkeer kan de voorziene TLS-client de controle tegen de *Whitelist* al uitvoeren voordat hij de TLS-handshake initieert, omdat hij de voorziene TLS-server al heeft geïdentificeerd, om te weten wie hij überhaupt moet aanspreken. In geval van inkomend verkeer echter, kan de TLS-server de zich aandienende TLS-client pas identificeren gedurende of na de TLS-handshake, aan de hand van het certificaat dat hij, conform verantwoordelijkheid 2, moet ontvangen. Daarop moet een hostname voorkomen die op de *Whitelist* is terug te vinden. Door toe te staan dat niet alleen de *Common Name* de voor MedMij geautoriseerde hostname mag bevatten, maar ook een *Subject Alternative Name*, biedt het MedMij Afsprakenstelsel aan deelnemers de mogelijkheid tot hergebruik van certificaten voor meerdere MedMij-nodes, of voor meerdere doelen dan alleen deelname in MedMij.

Het vroegste, en op het eerste gezicht dus meest veilige, moment om de controle tegen de *White-list* uit te voeren is in dat geval gedurende de TLS-handshake, tussen de ontvangst van het certificaat van de TLS-client en de voorziene verzending van de *Finished* message. Indien die controle niet kan worden uitgevoerd, of een negatief resultaat oplevert, wordt dan in plaats van de *Finished* message de uitzondering *access\_denied* verzonden. Hoewel sectie 7.2.2 van de [TLS-spectificatie](#) voorziet in deze mogelijkheid, voorzien veel standaardimplementaties er niet in. In-grepen in die standaard-implementaties zijn soms wel mogelijk, maar kunnen nieuwe beveiligingsrisico's met zich meebrengen, bijvoorbeeld vanwege de complexiteit van het beheren van maatwerk-aanpassingen aan standaardimplementaties.

Daarom wil het MedMij Afsprakenstelsel meer implementatievrijheid bieden, zonder evenwel het risico te accepteren dat er inhoudelijke informatie gaat worden verwerkt die afkomstig is van een TLS-client, voordat de controle tegen de *Whitelist* heeft verzekerd dat die TLS-client tot MedMij-verkeer geautoriseerd was. Omdat er meerdere manieren zijn om dat ook na afloop van de TLS-handshake te implementeren, vereist het MedMij Afsprakenstelsel hiervoor geen vaste architectuurvariant (zoals met een reverse proxy), maar stelt het de vereiste van veiligheid, naast een logische scheiding. Deze moeten kunnen worden aangetoond door middel van code-inspectie, penetratietesten en inspecties van logs.

15. Indien een *Whitelist*-controle, in het kader van verantwoordelijkheid 14, niet kan worden uitgevoerd, of een negatief resultaat oplevert, breekt dit de voortgang af van de uitvoering van de use case-implementatie en stellen de betrokken Applicatie-rollen elkaar hiervan niet op de hoogte.

#### Toelichting

Omdat het niet slagen van de *Whitelist*-controle duidt op een niet te vertrouwen tegenpartij, wordt deze daarvan niet op de hoogte gesteld.

## Domain Name System

16. *Dienstverleners persoon*, *Dienstverleners zorgaanbieder* en *MedMij Beheer* zijn, in hun rol als DNS Server of cliënt daarvan, ervoor verantwoordelijk dat de name records behorende bij de hostnames van *MedMij Nodes*, respectievelijk de *MedMij Stelselnode*, zijn ondertekend volgens DNSSEC.

17. De *MedMij Stelselnode* en elke *MedMij Node*, in zijn rol als DNS resolver in het Domain Name System, controleert of de ontvangen name records zijn voorzien van ondertekening volgens DNSSEC en valideert deze volgens DNSSEC. Indien deze controle en validatie niet beide slagen, ziet hij af van verbinding met de betreffende hostname.

#### Toelichting

Het gebruik van DNSSEC ([RFC 4033](#), [RFC 4034](#), [RFC 4035](#)) vermindert de kwetsbaarheid van het Domain Name System voor bijvoorbeeld [DNS spoofing](#).

## Samenstelling OAuth Client List

18. De *OAuth Client List* bevat voor elke *PGO Server* alleen die *PGO Node* waarmee de betreffende *PGO Server* het frontchannelverkeer afhandelt.

### Informatie

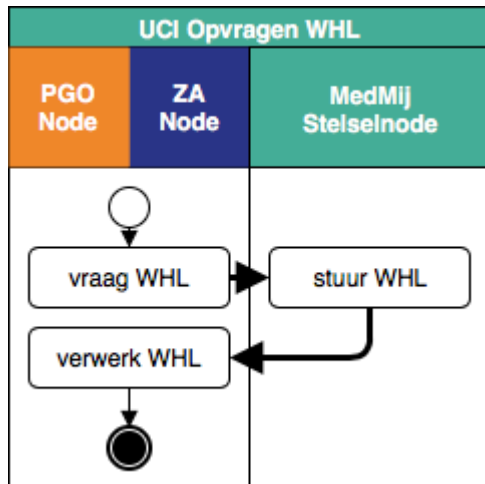
Conform het bepaalde onder punt 1 onder Rollen, mag een *PGO Server* meerdere *PGO Nodes* gebruiken, maar mag de *PGO Server* maar één *PGO Node* gebruiken voor al haar frontchannelverkeer, op het authorization interface dus. De inhoud van de *OAuth Client List* wordt alleen gebruikt op dat authorization interface, voor twee doelen:

- het kennisnemen van de *Gegevensdiensten* waarop de *PGO Server* is erkend, zodat de *Authorization Server* een authorization request kan weigeren wanneer de *PGO Server* niet is erkend op de *Gegevensdienst* waarvoor hij autorisatie vraagt;
- het kennisnemen van de naam van de *Dienstverlener persoon* die moet verschijnen in de [Toestemmingsverklaring](#) en de [Bevestigingsverklaring](#).

Daarom hoeft, voor een *PGO Server*, in de *OAuth Client List* alleen die ene *PGO Node* te worden opgenomen die deze *PGO Server* voor haar frontchannelverkeer gebruikt. Om geen overbodige gegevens te verspreiden, worden alle andere eventuele *PGO Nodes* van de *OAuth Client List* geweerd.

## Use case-implementatie Opvragen WHL

### Stroomdiagram



#### Toelichting

In elke voltrekking van de in het diagram beschreven flow is steeds sprake van één van elk van de bovenaan genoemde rollen. In de linkerbaan betekent dat: één *PGO Node* of één *ZA Node*.

Beide interacties met de *MedMij Stelselnode* zijn backchannel-verkeer.

## WHL-Interface

1. *MedMij Stelselnode* wordt in *UCI Opvragen WHL* wordt geadresseerd met de hostname `stelselnode.medmij.nl`. De URI van de *Whitelist* is `https://stelselnode.medmij.nl/MedMij_Whitelist.xml?api=1.2.0`

### Versionering van lijst-interfaces

Vanaf release 1.1.2 van het MedMij Afsprakenstelsel hebben de lijst-interfaces een versienummer. Dat maakt het mogelijk om meerdere versies van deze interfaces tegelijkertijd in productie te hebben. De versies worden, vanaf release 1.1.2, van elkaar onderscheiden door een query-parameter in de URI.

Het versienummer is identiek aan dat van de betreffende release. Opeenvolgende versies van de lijst-interfaces kunnen daarom inhoudelijk identiek zijn.

2. Het aandeel van *MedMij Stelselnode* in *UCI Opvragen WHL* is voor minstens 99,9% van de tijd beschikbaar. *MedMij Beheer* laat, na het niet beschikbaar raken van bedoelde aandeel, maximaal acht uren (480 minuten) verstrijken voordat het weer beschikbaar is.

3. *MedMij Beheer* brengt, in geval van zo'n incident, *Uitgevers*, *Bronnen* en *Lezers* op de hoogte van het optreden van het incident en van de verwachte down-time. *MedMij Beheer* brengt partijen op de hoogte van gepland onderhoud dat leidt tot tijdelijke onbeschikbaarheid.

4. Ingeval *MedMij Stelselnode* in *UCI Opvragen WHL* onbeschikbaar is, mogen betreffende opvragers gedurende maximaal 10 uur gebruik maken van het meest recente exemplaar van de betreffende lijst in de cache.

### Toelichting

De *Whitelist* is niet bedoeld voor het blokkeren van gecompromitteerde nodes. In die gevallen moet het betreffende certificaat worden ingetrokken, de systemen opgeschoond en een nieuw certificaat worden geïnstalleerd. Daarom is, in geval van de in deze verantwoordelijkheid bedoelde down-time, het gaan achterlopen van de inhoud van de *Whitelist*, geen beveiligingsrisico.

## Informatiemodellen

### Toelichting

Op de pagina's onder deze pagina zijn, op drie abstractieniveaus, modellen opgenomen van de informatie die een rol speelt in de architectuur van het MedMij Afsprakenstelsel, in de [hoofd functie Coördinatie](#). Het is de precieze "taal" van de hoofd functie *Coördinatie*. De drie abstractieniveaus verschillen in scope, stijl en structuur, maar bevatten allemaal dezelfde drie onderdelen:

- een modeldiagram met de structuur van de betrokken soorten informatie;
- een lijst met invarianten die extra eisen opleggen aan de instanties van het model;
- een lijst met zogenoemde basisklassen, dat wil zeggen, klassen waarvan de structuur in het diagram niet uitgewerkt staat, maar waarvan de waarden op zichzelf betekenis geacht worden te hebben.

De drie abstractieniveaus zijn:

- het conceptuele niveau met het [metamodel](#);
- het logische niveau met drie [logische modellen](#);
- het technische niveau met vier [XML-schema's](#) en een spreadsheet-tabelschema.

De scope van alle drie de niveaus beperkt zich in de deze versie van het MedMij Afsprakenstelsel tot de informatiesoorten die van belang zijn voor de vier door de MedMij-beheerorganisatie te publiceren lijsten en voor de *Catalogus*. Het [metamodel](#) bevat de relevante klassen vanuit het oogmerk van aanpasbaarheid en uitbreidbaarheid op de langere termijn. Binnen de grenzen van het object-georiënteerde denken, waarmee een groot deel van het publiek van deze modellen vertrouwd zal zijn, lukt dat het best met de systematische toepassing van associatieklassen. Dit staat nader toegelicht op de [metamodel](#)-pagina.

De [logische modellen](#) hebben samen dezelfde scope, maar maken een stap naar implementatie van de lijsten en de *Catalogus*. Daarom zijn ze hiërarchisch van opzet, en dus minder aanpasbaar en uitbreidbaar. Bovendien zijn er drie aparte logische modellen:

- één voor de vier lijsten, die gedurende de operatie van het MedMij-netwerk gepubliceerd worden;
- één voor de *Catalogus*, die bij het afsprakenstelsel gepubliceerd wordt op [deze pagina](#);
- één voor de *MedMijStelselNode*, die in het afsprakenstelsel zelf gepubliceerd wordt, op [deze pagina](#) (verantwoordelijkheid 3);
- één voor de twee soorten *rapporten*, waarmee *Deelnemers* moeten rapporteren over hun operatie op het MedMij-netwerk.

De [technische modellen](#) bouwen hier voort en zijn ook hiërarchisch, maar maken een verdere keuze voor technologie: XML en spreadsheet. Op dit niveau is er een apart model (XML-schema) voor elke lijst en elk rapport. Voor de *Catalogus* is de implementatietechnologie een tabel in een spreadsheet. Voor de *MedMijStelselNode* is er geen apart technisch model.

Lagere abstractieniveaus erven de relevante informatiesoorten, invarianten en basisklassen van hogere. Daarbij kan echter sprake zijn van structuur- en naamswijzigingen. Op de betreffende pagina's zijn deze abstractiestappen nader toegelicht. Zo wordt het proces van conceptuele specificatie naar technische implementatie zo controleerbaar en beheersbaar mogelijk.

## Metamodel

### Toelichting

Het metamodel ordent kernbegrippen uit het MedMij Afsprakenstelsel. Het is een conceptueel gegevensmodel, in de vorm van een UML-klassediagram. Het metamodel is gericht op het samenhangend beschrijven van begrippen en relaties die worden gebruikt in de [hoofd functie Coördinatie](#) van MedMij. Het metamodel is allereerst de basis voor de structuur van:

- de *Zorgaanbiederslijst*, waaraan de *OAuth Client* kan zien welke *Zorgaanbieders* momenteel welke *Gegevensdiensten* aanbieden en waarmee hij, gegeven een zekere *Interfaceversie*, de betrokken technische adressen (URI's) vindt van de *OAuth Authorization Server* (twee endpoints: het *Authorization Endpoint* en het *Token Endpoint*) en de *OAuth Resource Server* (het *Resource Endpoint*);
- de *Whitelist*, waarmee de *Nodes* elkaar accepteren als MedMij-nodes;
- de *OAuthclientlist*, waarin de *OAuth Authorization Server*:
  - een gebruikersvriendelijke naam van de *OAuth Client* kan vinden om te gebruiken in de [toestemmingsverklaring](#) danwel de [bevestigingsverklaring](#);
  - kan zien voor welke *Gegevensdiensten* de *OAuth Client* gekwalificeerd is;
- de *Gegevensdienstnamenlijst*, waaraan de *OAuth Client* kan zien welke *Weergavenamen* de *Gegevensdiensten* hebben die op enig moment beschikbaar zijn op het MedMij-netwerk.

Een vijfde lijst, de *Catalogus*, wordt door MedMij gepubliceerd als annex van het MedMij Afsprakenstelsel, op [deze pagina](#). Ten slotte is het metamodel de conceptuele basis voor twee rapportages die van Deelnemers worden verwacht:

- het *Beheerrapport*, waarmee elke *Deelnemer* de *Beheerorganisatie* periodiek inlicht over kentallen over het functioneren van het MedMij-netwerk;
- het *Portabiliteitsrapport*, waarmee de *Persoon* door diens *Dienstverlener Persoon* wordt ingelicht over welke gezondheidsinformatie die *Persoon* van *Zorgaanbieders* in zijn PGO heeft verzameld, zodat hij een eventuele andere of nieuwe PGO opnieuw met dezelfde verzamelacties zou kunnen vullen.

Voor alle zeven zijn logische modellen beschikbaar, op een [aparte pagina](#), die implementaties zijn van het metamodel.

Het metamodel is in een bepaalde stijl opgezet, met vooral associatieklassen. Het voordeel daarvan is dat het metamodel zo aanpasbaar en uitbreidbaar mogelijk blijft. Veel voorkomende constructies, zoals attributen en specialisatie zijn allemaal implementaties van associatieklassen. Implementatie willen we echter aan de [logische modellen](#) en de technische modellen (de [XML-schema's](#)) overlaten. Een tweede voordeel is dat bestaansafhankelijkheidsrelaties expliciet worden.

Bestaansafhankelijkheid wil zeggen dat de ene klasse betekenisloos is zonder de andere en dus dat eerstgenoemde klasse niet kan bestaan zonder laatstgenoemde. Bij een associatieklasse is die associatieklasse altijd bestaansafhankelijk van de twee klassen die het associeert.

Op enkele punten is afgeweken van deze modelleerstijl, door gebruik van:

- de uses-relatie, vooral in het *Informatiestandaarden*-domein, omdat dat domein niet onder beheer van MedMij valt;
- de aggregatie-relatie, idem;
- de objectgeoriënteerde specialisatie, namelijk waar we een opsommende definitie geven van *Deelnemersrol*, *Businessrol*, *Usecase* en *Bedrijfsrol*;

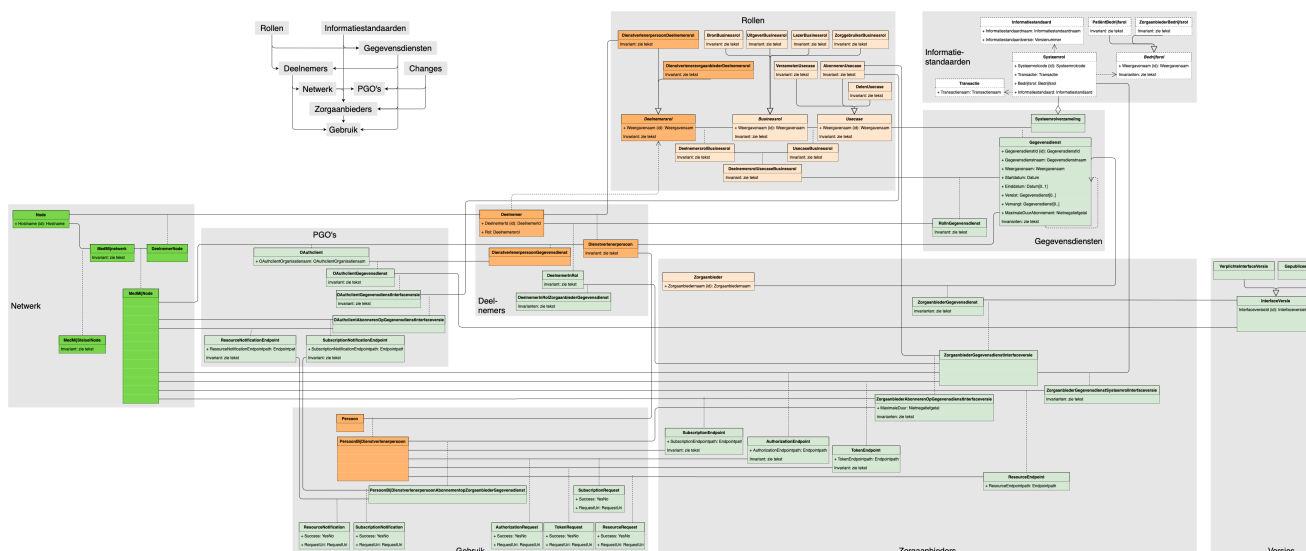


- attributen voor identificatie of omschrijving.

In al deze gevallen zouden ook associatieklassen gebruikt kunnen worden, maar zou dat de presentatie van het model onnodig compliceren.

Het metamodel is, voor het overzicht, geordend in negen modelgebieden: *Rollen*, *Deelnemers*, *PGO's*, *Zorgaanbieders*, *Gegevensdiensten*, *Informatiestandaarden*, *Netwerk*, *Changes* en *Gebruik*. Linksboven de plaat van het metamodel staat in een kaartje hoe de verschillende gebieden gebruik maken van concepten uit andere gebieden.

De namen van de klassen en de attributen beginnen allemaal met een hoofdletter. De rest van de namen bestaat uit enkel kleine letters, behalve daar waar de rest van de naam ook als aparte naam in het metamodel voorkomt, of er een eigenaam wordt gebruikt die anderszins eist. Het metamodel noteert dus *OAuthclient*, omdat de naam *OAuth* een eigenaam is waarin de *A* als hoofdletter wordt geschreven, en omdat de naam *Client* niet als aparte naam voorkomt in het metamodel. Het metamodel noteert *ZorgaanbiederGegevensdienst*, met een kapitale eerste *G*, omdat *Gegevensdienst* wel als aparte naam voorkomt.



## Toelichting

De MedMij-beheerorganisatie houdt bij welke *Organisaties*, door het aangaan van een *Deelnemersovereenkomst*, *Deelnemer* worden. *Deelnemers* zijn er in twee rollen: *DienstverlenerpersoonDeelnemersrol* en *DienstverlenerzorgaanbiederDeelnemersrol*. Deze komen overeen met de respectievelijke rollen *Dienstverlener Persoon* en *Dienstverlener Zorgaanbieder* op de [juridische laag](#).

*Organisaties* gebruiken *Nodes* waarvan zij de houder zijn. Als een *Organisatie* een *Deelnemer* is, zal zij zo'n *Node* als *DeelnemerNode* bij de MedMij-beheerorganisatie aanmelden. Op het *MedMijnetwerk* verschijnt zo'n *DeelnemerNode* als een *MedMijNode*. De *Hostnames* van deze *MedMijNodes* ontsluit de MedMij-beheerorganisatie over het *MedMijnetwerk*. De *MedMijNodes* gebruiken deze lijst als *Whitelist*, dat wil zeggen, om te bepalen of een *Node* die zich bij hen aandient, geautoriseerd is om op het *MedMijnetwerk* actief te zijn. Deze *Whitelist* verschijnt, als implementatiecomponent, pas in de [logische modellen](#). Dat geldt ook voor de *MedMijStelselNode*,

de Node via welke *MedMij Beheer* vier lijsten publiceert. De *MedMijStelselNode* staat niet expliciet op de *Whitelist*, maar is wel geautoriseerd deel te nemen op het *MedMijn* netwerk. Sterker, zonder de *MedMijStelselNode* kan het *MedMijn* netwerk niet werken.

Voor de *MedMijNodes* van *Deelnemers* die *Dienstverlenerpersoon* zijn (beter gezegd: voor de *OAuth Clients* op de *applicatielaag* gedurende de autorisatiefase van *UCI Verzamelen* en *UCI Delen*) bevat de *OAuthclientlist* gebruikersvriendelijke namen (*Organisatiennaam*), om gebruikt te worden in de *toestemmingsverklaring* en de *bevestigingsverklaring*. Ook de *OAuthclientlist* is een implementatiecomponent en verschijnt pas in de *logische modellen*. Wanneer een *OAuth Client* (een *PGO*) het gebruiken van *Abonnementen* mogelijk maakt voor de *Persoon*, moet zij endpoints aanbieden voor de twee soorten notificaties die de *Zorgaanbieder* in dat kader moet kunnen sturen: een *SubscriptionNotificationEndpoint* en een *ResourceNotificationEndpoint*.

In het *Rollen*-model domein verschijnen de *Deelnemerrollen*, *Businessrollen* en *Usecases* die in deze release van het *MedMij Afsprakenstelsel* bestaan, en hun toegestane combinaties. In het *Deelnemers*-model domein komen de *Deelnemers* in het *MedMij Afsprakenstelsel* aan de orde en voor welke *Zorgaanbieders* zij welke *Gegevensdiensten* ontsluiten.

*Gegevensdiensten* horen bij een *Usecase* en hebben een geldigheidsperiode. Bovendien wordt, door middel van het attribuut *Vereist*, van sommige *Gegevensdiensten* vereist dat, als een *Zorgaanbieder* die *Gegevensdienst* aanbiedt, hij ook zekere andere *Gegevensdiensten* moet aanbieden. Vaak zal die lijst leeg zijn, maar het heeft bijvoorbeeld weinig zin het *Delen* van een afspraakverzoek aan te bieden, zonder ook het *Verzamelen* van het antwoord daarop aan te bieden. De klasse *RollInGegevensdienst* wordt gebruikt om, via de *Deelnemer*, de *MedMij-rollen DienstverlenerpersoonDeelnemersrol* en *DienstverlenerzorgaanbiederDeelnemersrol* te verbinden met de dienovereenkomstige rollen die Nictiz in het Informatiestandaarden-domein heeft geformuleerd, namelijk respectievelijk *PatiëntBedrijfsrol* en *ZorgaanbiederBedrijfsrol*.

De klassen in het model domein *Informatiestandaarden*, inclusief hun namen, moeten begrepen worden in de zin waarin Nictiz ze gebruikt in het kader van de *Informatiestandaarden* die voor gebruik binnen *MedMij* zijn toegelaten. Daarom zijn de randen van deze klassen gestippeld. Een *Bedrijfsrol*, waarvan er twee zijn (*PatiëntBedrijfsrol* en *ZorgaanbiederBedrijfsrol*), wordt aangenomen door een *Systeemrol*. Bij elke *Systeemrol* hoort een *Informatiestandaard*. *Systeemrollen* worden gegroepeerd in *Systeemrolverzamelingen* die samen met een *Usecase* een *Gegevensdienst* vormen. Een actueel voorbeeld van een *Systeemrolverzameling* is een verzameling van vier *Systeemrollen* waarvan er twee (één voor elke betrokken *Bedrijfsrol*) een overzicht van beschikbare PDF-documenten uitwisselen en twee (opnieuw één voor elke betrokken *Bedrijfsrol*) een PDF-document uit dat overzicht uitwisselen. *Gegevensdiensten* worden als geheel (dat wil zeggen met hun gehele *Systeemrolverzameling*) aan *Zorggebruikers* aangeboden en die gebruikers zullen deze ook ineens autoriseren.

Onder in het model wordt het verband gelegd met de *Zorgaanbieders*. Dit model domein is de basis voor het *logische model* van de *Zorgaanbiederslijst*. Wanneer een *Zorgaanbieder* een zekere *Gegevensdienst* aanbiedt volgens een zekere *Interfaceversie*, hoort daarbij een *Zorgaanbieder GegevensdienstInterfaceversie*. Wanneer een *Zorgaanbieder* bovendien *Abonnementen* op deze *Gegevensdienst* aanbiedt, hoort daarbij een *ZorgaanbiederAbonnerenOpGegevensdienstInterfaceversie*. Deze klassen worden gebruikt om *Zorggebruikers* te informeren over wie van de *Zorgaanbieders* (*Abonnementen* op) welke *Gegevensdiensten* aanbieden. Binnen een *Gegevensdienst* zijn bovendien één of meerdere *Systeemrollen* aan de orde. Deze relatie is vervat in de klasse *ZorgaanbiederGegevensdienstSysteemrolInterfaceversie*.

Interfaces zijn geversioneerd: verschillende versies van interfaces kunnen tegelijkertijd op het *MedMij*-netwerk worden aangeboden. Daarom is er de klasse *Interfaceversie* in het model gebied *Changes*. Alle endpoints in de *Zorgaanbiederslijst* en *OAuth Client List* (zie onder) horen bij één *Interfaceversie*.

Een *Zorgaanbieder* kan de maximale abonnementsduur die hij aanbiedt voor een *Gegevensduur*, op een *Interfaceversie*, beperken. Daarbij moet hij echter blijven onder de maximale duur die MedMij voor die *Gegevensdienst* in de *Catalogus* heeft aangegeven. De maximale duur geeft de doorlooptijd aan in dagen waarbij de waarde 0 aangeeft dat een abonnement niet wordt ondersteund.

Bij een *ZorgaanbiederGegevensdienst* hoort één *AuthorizationEndpoint*, één *TokenEndpoint* en, indien daarop ook *Abonnementen* worden aangeboden, één *SubscriptionEndpoint*. Bij een *ZorgaanbiederGegevensdienstSysteemrol* hoort één *ResourceEndpoint*. Bij alle soorten endpoints noemt het metamodel het *Endpointpath*, het path in de URI waarmee de endpoints geadresseerd worden, en een *Interfaceversion*, waarmee gelijktijdig operationele versies van dezelfde endpoints kunnen worden onderscheiden. In deze versie van het MedMij Afsprakenstelsel worden op zowel frontchannel als backchannel de standaard IANA-poort voor `https` gebruikt. Er hoeven in de endpointadressen dus geen poortnummers te worden genoemd.

Deze onderdelen worden samen met de *Hostname* van de betreffende *MedMijNode* samengesteld tot een URI die geldt als het adres van het respectievelijke endpoint. Dat gebeurt in het *logische model* (met invarianten). De eisen aan al deze componenten en de wijzen van samenstellen tot de URI's staat beschreven op de *Interface*-pagina.

Eenzelfde *Zorgaanbieder* kan voor verschillende *Gegevensdiensten* van diensten van verschillende *Deelnemers* gebruik maken. Maar bij één *ZorgaanbiederGegevensdienst* hoort precies één *DeelnemerInRol*. Voor dit doel is in het metamodel de klasse *DeelnemerInRolZorgaanbiederGegevensdienst* opgenomen, in het *Deelnemers*-modeldomein.

Ten behoeve van het Beheerrapport en het Portabiliteitsrapport moet door *Deelnemers* informatie kunnen worden overlegd over wat er op het MedMij-netwerk gebeurt. Deze informatie wordt opgespannen door het modelgebied *Gebruik*. Deze informatie is hoofdzakelijk gestoeld op requests die worden gedaan over het MedMij-netwerk. Die zijn er in zes soorten. Van elke request moet bekend zijn wat de *RequestUri* was en of de request al dan niet succesvol was.

Invarianten, dat wil zeggen, beperkingen die te allen tijden aan de orde zijn, staan onderaan in een separate tabel opgenomen. Daarvan bestaan verschillende soorten, genoemd in de rechterkolom:

- Opsommingen stellen dat een zekere klasse een vast aantal expliciet benoemde instanties heeft.
- Getalsverhoudingen vereisen getalsmatige eisen aan het aantal instanties van een klasse, of de verhouding tussen de aantallen in meerdere klassen.
- Lokale afhankelijkheden stellen beperkingen aan de inhoudelijke verhoudingen tussen attributen van eenzelfde klasse.
- Niet-lokale afhankelijkheid stellen beperkingen aan de inhoudelijke verhoudingen tussen instanties van verschillende klassen.
- Rolbindingen beperken de rolcombinaties van verschillende rol-klassen. Zij komen overeen met onder andere de rolbindingen tussen de verschillende lagen.

De klassen in het metamodel horen bij de verschillende *lagen* in de architectuur van het afsprakenstelsel. De betreffende laag is aangegeven door de inkleuringen van de klassen. Alleen bij de Nictiz-klassen in het *Register van Informatiestandaarden* hebben we dit achterwege gelaten.

Uit dit metamodel wordt duidelijk hoe in het MedMij Afsprakenstelsel met adressering wordt omgegaan. De adresseringssystematiek bestaat uit drie onderdelen:

- MedMij-zorgaanbiedernamen voor *Zorgaanbieders*, zoals beschreven in verantwoordelijkheid 13 op de [Processen-en-Informatielaag](#);
- *Gegevensdiensten* met *Systeemrollen* zoals opgenomen in de *Catalogus*, respectievelijk het *Register van Informatiestandaarden*;
- Elke *Zorgaanbieder* kent bij elke *ZorgaanbiederGegevensdienst* (die hij aanbiedt via een *Dienstverlener Zorgaanbieder*) één *AuthorizationEndpoint* en één *TokenEndpoint* en bij elke *ZorgaanbiederGegevensdienstSysteemrol* daarbinnen één *ResourceEndpoint*. De endpoints hebben elk een URI als technisch adres.

Daar waar in het metamodel sprake is van periodes, begrensd door een start en een eind, moeten deze start en eind opgevat als beginmomenten. Als het om een startdatum en einddatum gaat, zoals in de attributen van *Gegevensdienst*, worden dus de beginmomenten van die data bedoeld, om 00h00m00. De start wordt opgevat als het begin van de geldigheid, het eind als het begin van de ongeldigheid. De geldigheid loopt daarom vanaf start tot eind (niet tot en met). Dit betekent ook dat, als het eind ontbreekt, de geldigheid zich voor onbepaalde tijd uitstrekt.

## Invarianten

Het diagram hierboven wordt geordend door (bestaans)afhankelijkheden tussen klassen. Binnen deze ordening bestaan er ook nog consistentie-eisen aan de instanties van deze klassen. Dit zijn de invarianten die in onderstaande tabel zijn opgenomen. Wat een invariant uitdrukt is dat een instantie van de betreffende klasse niet bestaat als zij niet aan de invariant voldoet. De tabel doet verder geen uitspraken over hoe de bewaking van deze consistentie wordt geïmplementeerd. In menige implementatie zullen tijdelijke inconsistenties worden toegestaan en pas later geweigerd of verholpen worden. Dat kan op vele manieren, maar het MedMij Afsprakenstelsel wil grote vrijheid laten in hoe de consistentie in registraties wordt geborgd.

De pad-expressies in de invarianten bestaan uit namen gescheiden door punten. Vanuit een zekere klasse wordt altijd een stap gemaakt naar een klasse waarvan eerstgenoemde onmiddellijk bestaansafhankelijk is. De naam van de zijde van de associatie waarover de stap wordt gemaakt wordt geacht de naam te dragen van de klasse aan het betreffende eindpunt van de associatie, de bestemming van de stap dus.

Betreft instanties van klasse ...	Invariant	Modeldomein	Toelichting
<i>AbonnerenUsecase</i>	Er is precies één instantie hiervan.	<i>Rollen</i>	Dit is een eenl
<i>AuthotizationEndpoint</i>	Voor elk <i>AuthorizationEndpoint</i> <i>a</i> en voor elke <i>DeelnemerInRolZorgaanbiederGegevensdienst</i> <i>d</i> , geldt:  ALS <i>d.ZorgaanbiederGegevensdienstInterfaceversie</i> = <i>a.ZorgaanbiederGegevensdienstInterfaceversie</i>  DAN <i>d.DeelnemerInRol.Deelnemer</i> = <i>a.MedMijNode.DeelnemerNode.Deelnemer</i>	<i>Zorgaanbieders</i>	Deze invariant authorization e <i>MedMijNode</i> <i>d</i> die ook de bet <i>Zorgaanbiede</i>
<i>Bedrijfsrol</i>	Elke <i>Bedrijfsrol</i> is hetzij <i>PatiëntBedrijfsrol</i> of <i>ZorgaanbiedersBedrijfsrol</i> .	<i>Informatiestandaarden</i>	Dit is een uitsl
<i>Bedrijfsrol</i>	Voor elke <i>Bedrijfsrol</i> <i>b</i> geldt: ALS( <i>b</i> : <i>PatiëntBedrijfsrol</i> DAN <i>b.Weergavenaam</i> = "Patiënt"; <i>b</i> : <i>ZorgaanbiedersBedrijfsrol</i> DAN <i>b.Weergavenaam</i> =	<i>Informatiestandaarden</i>	Dit koppelt de de weergaven

	"Zorgaanbieder"; ANDERS FOUT)		
<i>BronBusinessrol</i>	Er is precies één instantie hiervan.	<i>Deelnemers</i>	Dit is een eenl
<i>Businessrol</i>	Voor elke <i>Businessrol b</i> geldt: ALS( <i>b : BronBusinessrol</i> DAN <i>b.Weergavenaam = "Bron"</i> ; <i>b : LezerBusinessrol</i> DAN <i>b.Weergavenaam = "Lezer"</i> ; <i>b : UitgeverBusinessrol</i> DAN <i>b.Weergavenaam = "Uitgever"</i> ; ANDERS FOUT)	<i>Rollen</i>	Dit koppelt de de weergaven
<i>DeelnemerInRol</i>	Voor elke <i>DeelnemerInRol d</i> geldt: <i>d.Deelnemer.Deelnemersrol</i> en <i>d.RollInGegevensdienst</i> . <i>DeelnemersrolUsecaseBusinessrol.Deelnemersrol</i> zijn identiek.	<i>Deelnemers</i>	De betreffende aankomen vo <i>Catalogus</i> geb
<i>DeelnemerInRolZorgaanbiederGegevensdienst</i>	Voor elke <i>DeelnemerInRolZorgaanbiederGegevensdienst d</i> geldt: <i>d. ZorgaanbiederGegevensdienst.Gegevensdienst = d</i> . <i>DeelnemerInRol.RollInGegevensdienst.Gegevensdienst</i>	<i>Zorgaanbieders</i>	Een <i>Deelneme</i> over de opnan van een <i>Gege</i> <i>Zorgaanbiede</i> die <i>Gegevens</i>
<i>Dienstverlenerpersoon</i>	Er bestaat hooguit één instantie hiervan bij één <i>Deelnemer</i> , en precies één als de <i>Deelnemersrol</i> van laatstgenoemde van het type <i>DienstverlenerpersoonDeelnemersrol</i> is.	<i>Deelnemers</i>	Een <i>Deelneme</i> <i>Dienstverlene</i> hij de toepassi
<i>Deelnemersrol</i>	Voor elke <i>Deelnemersrol d</i> geldt: ALS( <i>d : DienstverlenerpersoonDeelnemersrol</i> DAN <i>d</i> . <i>Weergavenaam = "Dienstverlener persoon"</i> ; <i>d : DienstverlenerzorgaanbiederDeelnemersrol</i> DAN <i>d</i> . <i>Weergavenaam = "Dienstverlener zorgaanbieder"</i> ; ANDERS FOUT)	<i>Rollen</i>	Dit koppelt de de weergaven
<i>DeelnemersrolBusinessrol</i>	Er bestaan precies drie instanties hiervan, namelijk:	<i>Rollen</i>	Hier worden d

	<ul style="list-style-type: none"> <li>• één zodanig dat <i>DeelnemersrolBusinessrol</i>. <i>Deelnemersrol</i> : <i>DienstverlenerpersoonDeelnemersrol</i> en <i>DeelnemersrolBusiness.Businessrol</i> : <i>UitgeverBusinessrol</i>;</li> <li>• één zodanig dat <i>DeelnemersrolBusinessrol</i>. <i>Deelnemersrol</i> : <i>DienstverlenerzorgaanbiederDeelnemersrol</i> en <i>DeelnemersrolBusiness.Businessrol</i> : <i>BronBusinessrol</i>; en</li> <li>• één zodanig dat <i>DeelnemersrolBusinessrol</i>. <i>Deelnemersrol</i> : <i>DienstverlenerzorgaanbiederDeelnemersrol</i> en <i>DeelnemersrolBusiness.Businessrol</i> : <i>LezerBusinessrol</i>;</li> </ul>		<i>Dienstverlener</i> <i>Dienstverlener</i> <i>Businessroller</i>
<i>DeelnemersrolUsecaseBusinessRol</i>	Deze klasse bestaat uit precies één instantie voor elke combinatie van een instantie <i>d</i> van <i>DeelnemersrolBusinessrol</i> en een instantie <i>u</i> van <i>UsecaseBusinessrol</i> waarvoor geldt: <i>d.BusinessRol</i> = <i>u.BusinessRol</i> .	<i>Rollen</i>	Hier worden al combinaties g <i>Deelnemersro</i> <i>UsecaseBusin</i> <i>Dienstverlener</i> <i>Dienstverlener</i> <i>Dienstverlener</i> <i>/Verzamelen e</i> <i>/Lezer/Delen</i> .
<i>DelenUsecase</i>	Er is precies één instantie hiervan.	<i>Rollen</i>	Dit is een eenl
<i>DienstverlenerpersoonDeelnemersrol</i>	Er is precies één instantie hiervan.	<i>Rollen</i>	Dit is een eenl
<i>DienstverlenerzorgaanbiederDeelnemersrol</i>	Er is precies één instantie hiervan.	<i>Rollen</i>	Dit is een eenl
<i>Gegevensdienst</i>	Er zijn nul of meer <i>Gegevensdiensten</i> .	<i>Gegevensdiensten</i>	Er kunnen op <i>Gegevensdier</i> .
<i>Gegevensdienst</i>	Voor elke <i>Gegevensdienst g</i> geldt:	<i>Gegevensdiensten</i>	Anders heeft c

	<i>g.Startdatum</i> ligt voor <i>g.Einddatum</i> .		
<i>Gegevensdienst</i>	Voor elke <i>Gegevensdienst g1</i> en <i>g2</i> geldt: ALS <i>g2</i> voorkomt in <i>g1</i> . Vereist DAN ( <i>g2</i> staat als <i>Gegevensdienst</i> in <i>Catalogus EN</i> <i>g1.Startdatum</i> ligt niet voor <i>g2.Startdatum</i> EN <i>g1.Einddatum</i> ligt niet na <i>g2.Einddatum</i> )	<i>Gegevensdiensten</i>	Een geldige <i>G</i> onbestaande c vereisen. Een die is optionee tijd" en ligt na
<i>Gegevensdienst</i>	Voor elke <i>Gegevensdienst g</i> geldt:  <i>g.Gegevensdienstnaam</i> is een concatenatie van <i>g.Usecase</i> . <i>Weergavenaam</i> , <i>g.Weergavenaam</i> en de eerste twee cijferreeksen (voor zover aanwezig en met de scheidende punt) van <i>g.Systeemrol.Informatiestandaard</i> . <i>Informatiestandaardversie</i> , met een spatie als scheidingsteken.	<i>Gegevensdiensten</i>	Dit standaardi <i>Gegevensdier</i> . <i>Informatiestan</i> twee cijferree verdere cijferr bijvoorbeeld) v gezien.
<i>Gegevensdienst</i>	Voor elke twee verschillende <i>Gegevensdiensten g1</i> en <i>g2</i> geldt:  <i>g1.Gegevensdienstnaam</i> /= <i>g2.Gegevensdienstnaam</i>	<i>Gegevensdiensten</i>	Zo worden ver niet verward d
<i>GepubliceerdeInterfaceversie</i>	Er is precies één instantie hiervan.	<i>Changes</i>	Dit is een eenl
<i>LezerBusinessrol</i>	Er is precies één instantie hiervan.	<i>Rollen</i>	Dit is een eenl
<i>MedMijnnetwerk</i>	Er is precies één instantie hiervan.	<i>Netwerk</i>	Dit is een eenl
<i>MedMijStelselNode</i>	Er is precies één instantie hiervan.	<i>Netwerk</i>	Zonder <i>MedM</i> . <i>MedMijNetwer</i>
<i>Node</i>	De hostname van een Node bevat een domeinnaam die een fully-qualified domain name is, conform <a href="#">RFC3696</a> , sectie 2.	<i>Netwerk</i>	Dit is een maa RFC 6819.
<i>OAuthclient</i>	Voor elke <i>OAuthclient o</i> geldt: <i>o.OAuthclientOrganisatiennaam</i> voldoet aan het <a href="#">OAuthclient-</a>	<i>Applicatie</i>	Zie het <a href="#">OAuth</a>



	<a href="#">namenbeleid.</a>		
<i>OAuthClientAbonnerenOpGegevensdienstInterfaceversie</i>	Elke <i>OAuthClientAbonnerenOpGegevensdienstInterfaceversie</i> heeft precies één <i>ResourceNotificationEndpoint</i> .	PGO's	Zo kan de <i>Not</i> van een <i>OAuthClient</i> het <i>ResourceNotificationEndpoint</i> betreffende <i>OAuthClient</i> ondersteund.
<i>OAuthClientAbonnerenOpGegevensdienstInterfaceversie</i>	Elke <i>OAuthClientAbonnerenOpGegevensdienstInterfaceversie</i> heeft precies één <i>SubscriptionNotificationEndpoint</i> .	PGO's	Zo kan de <i>Not</i> van een <i>OAuthClient</i> het <i>SubscriptionNotificationEndpoint</i> in de <i>OAuthClient</i> de betre ondersteund.
<i>OAuthClientGegevensdienst</i>	<p>Voor elke <i>OAuthClientGegevensdienst</i> zg geldt:</p> <p>ALS er een <i>OAuthClientAbonnerenOpGegevensdienstInterfaceversie</i> <i>zagi1</i> is zodat:</p> <ul style="list-style-type: none"> <li>• <i>zagi1.OAuthClientGegevensdienstInterfaceversie.ZorgaanbiederGegevensdienst</i> = zg en</li> <li>• <i>zagi1.OAuthClientGegevensdienstInterfaceversie.Interfaceversie</i> is de <i>GepubliceerdeInterfaceversie</i></li> </ul> <p>DAN is er een <i>OAuthClientAbonnerenOpGegevensdienstInterfaceversie</i> <i>zagi2</i> zodat:</p> <ul style="list-style-type: none"> <li>• <i>zagi2.OAuthClientGegevensdienstInterfaceversie.ZorgaanbiederGegevensdienst</i> = zg en</li> <li>• <i>zagi2.OAuthClientGegevensdienstInterfaceversie.Interfaceversie</i> is de <i>VerplichteInterfaceversie</i></li> </ul>	Zorgaanbieders	Wanneer een <i>Gegevensdienst</i> gepubliceerde ook aanbieder . Zie <a href="#">Change-</a>

<i>ZorgaanbiederGegevensdienst</i>	Voor elke <i>ZorgaanbiederGegevensdienst.Gegevensdienst.TransactieVerzameling.Transactie.Systeemrol s</i> waarvoor geldt dat $s.Bedrijfsrol = ZorgaanbiederBedrijfsrol$ , geldt dat er een <i>ZorgaanbiederGegevensdienstSysteemrol z</i> is zodat $z.Systeemrol = s$ .	<i>Zorgaanbieders</i>	Als in de <i>Catalogus</i> <i>ZorgaanbiederGegevensdienst</i> zekere <i>ZorgaanbiederGegevensdienst</i> aangeboden.
<i>ZorgaanbiederGegevensdienst</i>	Elke <i>ZorgaanbiederGegevensdienst</i> heeft precies één <i>AuthorizationEndpoint</i> .	<i>Zorgaanbieders</i>	Zo kan de <i>OA</i> een <i>ZorgaanbiederGegevensdienst</i> het <i>AuthorizationEndpoint</i> .
<i>ResourceEndpoint</i>	Voor elk <i>ResourceEndpoint r</i> en voor elke <i>DeelnemerInRolZorgaanbiederGegevensdienst d</i> , geldt:  ALS $d.ZorgaanbiederGegevensdienstInterfaceversie = r.ZorgaanbiederGegevensdienstSysteemrolInterfaceversie$ . <i>ZorgaanbiederGegevensdienstInterfaceversie</i>  DAN $d.DeelnemerInRol.Deelnemer = r.MedMijNode.DeelnemerNode.Deelnemer$	<i>Zorgaanbieders</i>	Deze invariant resource endp die van dezelfde <i>ZorgaanbiederGegevensdienst</i> betreffende <i>ZorgaanbiederGegevensdienst</i> aanbiedt.
<i>ResourceEndpoint</i>	Voor elk <i>ResourceEndpoint r</i> geldt:  ALS $r.ZorgaanbiederGegevensdienstSysteemrolInterfaceversie = r.ZorgaanbiederGegevensdienstInterfaceversie$ . <i>ZorgaanbiederGegevensdienstInterfaceversie</i> . <i>ZorgaanbiederGegevensdienst.Gegevensdienst</i> is gebaseerd op een <i>Informatiestandaard</i> uit het <a href="#">Register Informatiestandaarden</a> ,  DAN is <i>r</i> gelijk aan wat in het technische ontwerp van de <i>Informatiestandaard [base]</i> heet.	<i>Zorgaanbieders</i>	Deze invariant voor de genoemde <i>Gegevensdienst</i> URL en andere resource.

<i>ResourceNotificationEndpoint</i>	<p>Voor elk <i>ResourceNotificationEndpoint</i> <i>s</i> geldt:</p> <p><i>s.MedMijNode.DeelnemerNode.Deelnemer</i> = <i>s.OAuthClientAbonnerenOpGegevensdienst.OAuthclient.MedMijNode.DeelnemerNode.Deelnemer</i></p>	PGO's	De <i>MedMijNode.ResourceNotificationEndpoint</i> als <i>OAuthClient</i> .
<i>RollInGegevensdienst</i>	<p>Deze klasse bestaat uit precies één instantie <i>r</i> voor elke combinatie van een instantie <i>d</i> van <i>r</i>.</p> <p><i>DeelnemersrolUsecaseBusinessrol</i> en een instantie <i>g</i> van <i>r</i>.</p> <p><i>Gegevensdienst</i> waarvoor geldt: <i>g.Usecase</i> = <i>d.UsecaseBusinessrol.Usecase</i></p>	<i>Deelnemers</i>	<p>Zo wordt ervoor bij de betrekking overeenkomt <i>r</i></p> <p><i>Deelnemersrol</i></p> <p>Voor elke keer een instantie.</p>
<i>SubscriptionEndpoint</i>	<p>Voor elk <i>SubscriptionEndpoint</i> <i>s</i> en voor elke <i>DeelnemerInRolZorgaanbiederGegevensdienst d</i>, geldt:</p> <p>ALS <i>d.ZorgaanbiederGegevensdienstInterfaceversie</i> = <i>s.ZorgaanbiederAbonnerenOpGegevensdienstInterfaceversie.ZorgaanbiederGegevensdienstInterfaceversie</i></p> <p>DAN <i>d.DeelnemerInRol.Deelnemer</i> = <i>s.MedMijNode.DeelnemerNode.Deelnemer</i></p>	<i>Zorgaanbieders</i>	Deze invariant subscription en <i>MedMijNode d</i> die ook de bet <i>Zorgaanbieder</i> .
<i>SubscriptionEndpoint</i>	<p>Voor elke <i>ZorgaanbiederGegevensdienst zg</i>, voor elke <i>ZorgaanbiederGegevensdienstInterfaceversie zgi</i> van <i>zg</i>, voor elke <i>ZorgaanbiederAbonnerenOpGegevensdienstInterfaceversie zag</i> van <i>zgi</i>, voor elk <i>ResourceEndpoint r</i> van <i>zagi</i> en voor elke <i>DeelnemerInRolZorgaanbiederGegevensdienst d</i> van <i>zg</i> geldt:</p>	<i>Zorgaanbieders</i>	<p>Deze invariant subscription en <i>MedMijNode d</i> die ook de bet <i>Zorgaanbieder</i>.</p> <p>Hoewel de inv. <i>SubscriptionEndpoint</i>.</p> <p><i>DeelnemerInRol</i> " zijn er van be elke</p>

	<i>r.MedMijNode.DeelnemerNode.Deelnemer = d. DeelnemerInRol.Deelnemer</i>		Zorgaanbiede. Dat wordt gere maar daarvan afhankelijk zijn
<i>SubscriptionNotificationEndpoint</i>	Voor elk <i>SubscriptionNotificationEndpoint s</i> geldt:  <i>s.MedMijNode.DeelnemerNode.Deelnemer = s. OAuthClientAbonnerenOpGegevensdienst. OAuthclient.MedMijNode.DeelnemerNode.Deelnemer</i>	<i>PGO's</i>	De <i>MedMijNode. SubscriptionN</i> dezelfde <i>Deeli</i> betreffende <i>O,</i>
<i>Systeemrol</i>	Voor elke <i>Systeemrol s</i> geldt: <i>ALS s.Bedrijfsrol : PatiëntBedrijfsrol</i> <i>DAN geldt voor alle RolInGegevensdienst r:</i> <i>(ALS s in r.Gegevensdienst.TransactieVerzameling</i> <i>DAN r.DeelnemersrolUsecaseBusinessrol.Deelnemersrol :</i> <i>DienstverlenerpersoonDeelnemersrol)</i>	<i>Deelnemers</i>	Dit koppelt de <i>Persoon</i> aan c
<i>Systeemrol</i>	Voor elke <i>Systeemrol s</i> geldt: <i>ALS s.Bedrijfsrol : ZorgaanbiederBedrijfsrol</i> <i>DAN geldt voor alle RolInGegevensdienst r:</i> <i>(ALS s in r.Gegevensdienst.TransactieVerzameling</i> <i>DAN r.DeelnemersrolUsecaseBusinessrol.Deelnemersrol :</i> <i>DienstverlenerzorgaanbiederDeelnemersrol)</i>	<i>Deelnemers</i>	Dit koppelt de <i>Zorgaanbiede.</i> .
<i>TokenEndpoint</i>	Voor elk <i>TokenEndpoint t</i> en voor elke <i>DeelnemerInRolZorgaanbiederGegevensdienst d,</i> geldt:  <i>ALS d.ZorgaanbiederGegevensdienstInterfaceversie =</i> <i>t.ZorgaanbiederGegevensdienstInterfaceversie</i>  <i>DAN d.DeelnemerInRol.Deelnemer = t.MedMijNode.</i> <i>DeelnemerNode.Deelnemer</i>	<i>Zorgaanbieders</i>	Deze invariant endpoint hoort dezelfde <i>Deeli</i> <i>Zorgaanbiede.</i>

<i>UitgeverBusinessrol</i>	Er is precies één instantie hiervan.	<i>Rollen</i>	Dit is een eenl
<i>Usecase</i>	Voor elke <i>Usecase u</i> geldt: ALS( <i>u : VerzamelenUsecase</i> DAN <i>u.Weergavenaam = "Verzamelen";</i> <i>u : DelenUsecase</i> DAN <i>u.Weergavenaam = "Delen";</i> ANDERS FOUT)	<i>Rollen</i>	Dit koppelt de de weergaven
<i>Usecase Businessrol</i>	Er zijn precies vier instanties hiervan, namelijk: <ul style="list-style-type: none"> <li>• één zodanig dat <i>UseCaseBusinessrol.Businessrol : UitgeverBusinessrol</i> en <i>UseCaseBusinessrol.Usecase : VerzamelenUsecase;</i></li> <li>• één zodanig dat <i>UseCaseBusinessrol.Businessrol : UitgeverBusinessrol</i> en <i>UseCaseBusinessrol.Usecase : DelenUsecase;</i> en</li> <li>• één zodanig dat <i>UseCaseBusinessrol.Businessrol : BronBusinessrol</i> en <i>UseCaseBusinessrol.Usecase : VerzamelenUsecase;</i> en</li> <li>• één zodanig dat <i>UseCaseBusinessrol.Businessrol : LezerBusinessrol</i> en <i>UseCaseBusinessrol.Usecase : DelenUsecase.</i></li> </ul>	<i>Rollen</i>	Hier wordt bep participeren in
<i>VerplichteInterfaceversie</i>	Er is precies één instantie hiervan.	<i>Changes</i>	Dit is een eenl
<i>VerzamelenUsecase</i>	Er is precies één instantie hiervan.	<i>Rollen</i>	Dit is een eenl
<i>ZorgaanbiedersBedrijfsrol</i>	Er is precies één instantie hiervan.	<i>Informatiestandaarden</i>	Dit is een eenl
<i>Zorgaanbieder</i>	Elke <i>Zorgaanbieder</i> heeft minstens één <i>ZorgaanbiederGegevensdienst</i>	<i>Zorgaanbieders</i>	Anders is de o de <i>Zorgaanbie</i>
<i>Zorgaanbieder</i>	Elke <i>Zorgaanbieder</i> heeft bij elke <i>Gegevensdienst</i> ten hoogste één <i>ZorgaanbiederGegevensdienst</i> .	<i>Zorgaanbieders</i>	Zo kan de OA een <i>Zorgaanb</i>

			het <i>Authorizati</i> vinden, in de <i>z</i>
<i>Zorgaanbieder</i>	Voor elke <i>ZorgaanbiederGegevensdienst zg1</i> en voor elke <i>Gegevensdienst g</i> in <i>zg1.Gegevensdienst</i> . Vereist geldt:  er een <i>ZorgaanbiederGegevensdienst zg2</i> , zodat $zg1.Zorgaanbieder = zg2.Zorgaanbieder$ en $zg1.Gegevensdienst = g$ .	<i>Zorgaanbieders</i>	Zo wordt ervoor <i>Zorgaanbiede</i> die een andere ook de andere
<i>Zorgaanbieder</i>	Voor elke <i>ZorgaanbiederGegevensdienst zg1</i> en voor elke <i>Gegevensdienst g</i> in <i>zg1.Gegevensdienst</i> . Vervangt geldt:  er zijn, anders dan <i>zg1</i> , <u>geen</u> <i>ZorgaanbiederGegevensdiensten zg2</i> , zodat $zg1.Zorgaanbieder = zg2.Zorgaanbieder$ en  hetzij <i>zg2.Gegevensdienst</i> volgt <i>g</i> op of <i>g</i> volgt <i>zg2.Gegevensdienst</i> op.  'Opvolgen' is daarbij als volgt (recursief) gedefinieerd: <i>Gegevensdienst h1</i> volgt <i>Gegevensdienst h2</i> op als hetzij $h1 = h2$ of <i>h2</i> volgt een <i>Gegevensdienst</i> in <i>h1</i> . Vervangt op.	<i>Zorgaanbieders</i>	Zo wordt ervoor <i>Zorgaanbiede</i> kan aanbieder (direct of indire indirectie is ee
<i>ZorgaanbiederAbonnerenOpGegevensdienst</i>	Voor elke <i>ZorgaanbiederGegevensdienst zg</i> , Voor elke <i>ZorgaanbiederAbonnerenOpGegevensdienst zaog</i> van <i>zg</i> , voor elk <i>SubscriptionEndpoint s</i> van <i>zaog</i> en voor elke <i>DeelnemerInRolZorgaanbiederGegevensdienst d</i> van <i>zg</i> geldt:  $s.MedMijNode.DeelnemerNode.Deelnemer = d$ . <i>DeelnemerInRol.Deelnemer</i>	<i>Zorgaanbieders</i>	Deze invariant endpoint hoort dezelfde <i>Deeli</i> <i>Zorgaanbiede</i> . Hoewel de inv. <i>SubscriptionE</i> . <i>DeelnemerInR</i> " zijn er van be <i>Zorgaanbiede</i> . geregeld door daarvan wil de

<i>ZorgaanbiederAbonnerenOpGegevensdienstInterfaceversie</i>	<p>Voor elke <i>ZorgaanbiederAbonnerenOpGegevensdienstInterfaceversie</i> <i>zgi</i> geldt:</p> <p><i>zgi.ZorgaanbiederGegevensdienstInterfaceversie.ZorgaanbiederGegevensdienst.Gegevensdienst.Usecase = VerzamelenUsecase</i></p>	<i>Zorgaanbieders</i>	Vooralsnog zij verzamelende
<i>ZorgaanbiederAbonnerenOpGegevensdienstInterfaceversie</i>	<p>Elke <i>ZorgaanbiederAbonnerenOpGegevensdienstInterfaceversie</i> heeft precies één <i>SubscriptionEndpoint</i>.</p>	<i>Zorgaanbieders</i>	Zo kan de OA die <i>Abonnement</i> biedt, per <i>InterfaceSubscriptionEndpoint</i> <i>Zorgaanbieder</i> .
<i>ZorgaanbiederAbonnerenOpGegevensdienstInterfaceversie</i>	<p>Voor elke <i>ZorgaanbiederAbonnerenOpGegevensdienstInterfaceversie</i> <i>zgi</i> geldt:</p> <p><i>zgi.MaximaleDuur &lt;= zgi.ZorgaanbiederGegevensdienstInterfaceversie.ZorgaanbiederGegevensdienst.Gegevensdienst.MaximaleDuur</i></p>	<i>Zorgaanbieders</i>	Een <i>Zorgaanbieder</i> abonnementsduur <i>Gegevensduur</i> beperken. Deze onder de maximale <i>Gegevensduur</i> aangegeven.
<i>ZorgaanbiederGegevensdienst</i>	<p>Voor elke <i>ZorgaanbiederGegevensdienst</i> <i>zg</i> geldt:</p> <p>ALS er een <i>ZorgaanbiederGegevensdienstInterfaceversie</i> <i>zgi1</i> is zodat:</p> <ul style="list-style-type: none"> <li><i>zgi1.ZorgaanbiederGegevensdienst = zg</i> en</li> <li><i>zgi1.Interfaceversie</i> is de <i>GepubliceerdeInterfaceversie</i></li> </ul> <p>DAN is er een <i>ZorgaanbiederGegevensdienstInterfaceversie</i> <i>zgi2</i> zodat:</p> <ul style="list-style-type: none"> <li><i>zgi2.ZorgaanbiederGegevensdienst = zg</i> en</li> </ul>	<i>Zorgaanbieders</i>	Wanneer een <i>Gegevensdier</i> gepubliceerde ook aanbieder. Zie <a href="#">Change-</a>

	<ul style="list-style-type: none"> <li>• <i>zgi2.Interfaceversie</i> is de <i>VerplichteInterfaceversie</i></li> </ul>		
<i>ZorgaanbiederGegevensdienst</i>	<p>Voor elke <i>ZorgaanbiederGegevensdienst</i> zg geldt:</p> <p>ALS er een <i>ZorgaanbidersAbonnerenOpGegevensdienstInterfaceversie zagi1</i> is zodat:</p> <ul style="list-style-type: none"> <li>• <i>zagi1.ZorgaanbiederGegevensdienstInterfaceversie.ZorgaanbiederGegevensdienst = zg</i> en</li> <li>• <i>zagi1.ZorgaanbiederGegevensdienstInterfaceversie.Interfaceversie</i> is de <i>GepubliceerdeInterfaceversie</i></li> </ul> <p>DAN is er een <i>ZorgaanbidersAbonnerenOpGegevensdienstInterfaceversie zagi2</i> zodat:</p> <ul style="list-style-type: none"> <li>• <i>zagi2.ZorgaanbiederGegevensdienstInterfaceversie.ZorgaanbiederGegevensdienst = zg</i> en</li> <li>• <i>zagi2.ZorgaanbiederGegevensdienstInterfaceversie.Interfaceversie</i> is de <i>VerplichteInterfaceversie</i></li> </ul>	<i>Zorgaanbiders</i>	<p>Wanneer een <i>Gegevens</i> gepubliceerde ook aanbieder <i>. Zie <a href="#">Change-</a></i></p>
<i>ZorgaanbiederGegevensdienst</i>	<p>Voor elke <i>ZorgaanbiederGegevensdienst.Gegevensdienst.TransactieVerzameling.Transactie.Systeemrol s</i> waarvoor geldt dat <i>s.Bedrijfsrol = ZorgaanbiederBedrijfsrol</i>, geldt dat er een <i>ZorgaanbiederGegevensdienstSysteemrol z</i> is zodat <i>z.Systeemrol = s</i>.</p>	<i>Zorgaanbiders</i>	<p>Als in de <i>Cata Zorgaanbiede</i>, zekere <i>Zorgaæ Gegevensdier</i>, <i>Zorgaanbiede</i>, aangeboden.</p>
<i>ZorgaanbiederGegevensdienst</i>	<p>Elke <i>ZorgaanbiederGegevensdienst</i> heeft precies één <i>AuthorizationEndpoint</i>.</p>	<i>Zorgaanbiders</i>	<p>Zo kan de <i>OAI</i> een <i>Zorgaanb</i>, het <i>Authorizat</i>, <i>Zorgaanbiede</i>.</p>



<i>ZorgaanbiederGegevensdienst</i>	Elke <i>ZorgaanbiederGegevensdienst</i> heeft precies één <i>TokenEndpoint</i> .	<i>Zorgaanbieders</i>	Zo kan de OA een <i>Zorgaanb.</i> het <i>TokenEnd</i> , <i>Zorgaanbiede</i> .
<i>ZorgaanbiederGegevensdienst</i>	Elke <i>ZorgaanbiederGegevensdienst</i> heeft precies één <i>DeelnemerInRolZorgaanbiederGegevensdienst d</i> , en wel zo dat <i>d.DeelnemerInRol.Deelnemer.Rol = DienstverlenerzorgaanbiederDeelnemersrol</i> .	<i>Zorgaanbieders</i>	Zo is duidelijk voor een <i>Zorg</i> dat dat een <i>Di</i> betreft.
<i>ZorgaanbiederGegevensdienstSysteemrolInterfaceversie</i>	Elke combinatie van een <i>ZorgaanbiederGegevensdienstInterfaceversie</i> en een <i>Systeemrol</i> heeft ten hoogste één <i>ZorgaanbiederGegevensdienstSysteemrolInterfaceversie</i> .	<i>Zorgaanbieders</i>	Zo kan de OA een <i>Zorgaanb.</i> een <i>Systeemr</i> vinden, in de <i>z</i>
<i>ZorgaanbiederGegevensdienstSysteemrolInterfaceversie</i>	<i>ZorgaanbiederGegevensdienstSysteemrolInterfaceversie.Systeemrol.Bedrijfsrol = ZorgaanbiederBedrijfsrol</i>	<i>Zorgaanbieders</i>	<i>Zorgaanbiede</i> , aanbieden die zijn.
<i>ZorgaanbiederGegevensdienstSysteemrolInterfaceversie</i>	Elke <i>ZorgaanbiederGegevensdienstSysteemrolInterfaceversie</i> heeft precies één <i>ResourceEndpoint</i> .	<i>Zorgaanbieders</i>	Zo kan de OA een <i>Zorgaanb.</i> een <i>Systeemr</i> vinden, in de <i>z</i>
<i>ZorggebruikerBusinessrol</i>	Er is precies één instantie hiervan.	<i>Rollen</i>	Dit is een eenl

## Basisklassen

Basisklasse	Definitie
<i>Datum</i>	Conform het type <code>xs:date</code> , zoals gespecificeerd in <a href="#">XML Schema 1.0</a> .
<i>DeelnemerId</i>	String van minimaal één en maximaal 30 tekens.

<i>Endpointpath</i>	Zie adresseringsverantwoordelijkheden op de <a href="#">Interfaces</a> -pagina.
<i>GegevensdienstId</i>	String van minimaal één en maximaal 30 tekens.
<i>Gegevensdienstnaam</i>	String van minimaal drie en maximaal 50 tekens.
<i>Hostname</i>	Zie adresseringsverantwoordelijkheden op de <a href="#">Interfaces</a> -pagina.
<i>Informatiestandaardnaam</i>	String van minimaal drie en maximaal 50 tekens.
<i>InterfaceversieId</i>	String van minimaal één en maximaal 30 tekens.
<i>Nietnegatiefgetal</i>	Conform het type <code>xs:nonNegativeInteger</code> , zoals gespecificeerd in <a href="#">XML Schema 1.0</a> .
<i>OAuthclientOrganisatienaam</i>	Conform toepasselijk <a href="#">OAuthclient-namenbeleid</a> .
<i>RequestUri</i>	String van minimaal twaalf en maximaal 2048 tekens.
<i>Systeemrolcode</i>	String van minimaal één en maximaal 30 tekens.
<i>Transactienaam</i>	String van minimaal drie en maximaal 50 tekens.
<i>Versienummer</i>	Eén of meer cijferreeksen, elk bestaand uit één of meer cijfers 0 tot en met 9, gescheiden door een punt
<i>Weergavenaam</i>	String van minimaal drie en maximaal 50 tekens.
<i>YesNo</i>	Conform het type <code>xs:boolean</code> , zoals gespecificeerd in <a href="#">XML Schema 1.0</a> .
<i>Zorgaanbiedernaam</i>	Conform toepasselijk <a href="#">Zorgaanbiedersnamenbeleid</a> .

## Logische modellen

### Toelichting

Er is één [metamodel](#), maar er zijn meerdere logische modellen. Logische modellen bereiden de implementatie voor van bepaalde onderdelen van het [metamodel](#). Deze versie van het MedMij Afsprakenstelsel kent drie logische modellen. Elk daarvan hoort bij een of enkele specifieke implementatie-component(en) in MedMij Afsprakenstelsel. Het gaat om de volgende componenten:

- de vier door *MedMij Registratie* gepubliceerde lijsten: *Gegevensdienstnamenlijst*, *OAuthclientlist*, *Whitelist* en *Zorgaanbiederslijst*;
- de in het MedMij Afsprakenstelsel te publiceren *Catalogus van Gegevensdiensten*;
- de in het MedMij Afsprakenstelsel te publiceren (*Hostname* van de) *MedMijStelselNode*;
- de twee van Deelnemers gevraagde rapportages: *Beheerrapport* en *Portabiliteitsrapport*.

De vier lijsten staan gecombineerd in één logisch model, onder de klasse *MedMijBeheerlijst*, omdat zij basiskennmerken delen. Iets dergelijks geldt voor de twee rapporten, onder de klasse *MedMijRapport*.

Logische modellen gehoorzamen het [metamodel](#), maar verbijzonderen dat. In de stap van [metamodel](#) naar logisch model kunnen er (logische) klassen, invarianten en basisklassen bijkomen. Maar de logische modellen bouwen vooral ook voort op het [metamodel](#) door klassen en attributen daarvan te gebruiken. In dat geval hebben logische klassen, waarde en basisklassen dus overeenkomstige klassen in het [metamodel](#). De overeenkomsten staan hieronder bij het logische model genoemd in een tabel. Waar de tabel bij een zekere logische klasse, waarde of basisklasse de overeenkomst met het [metamodel](#) niet noemt, is deze nieuw voor het logische niveau.

Logische klassen hebben minder of meer attributen dan de overeenkomstige klassen in het [metamodel](#). Waar het er minder zijn, hoeven de weggelaten attributen dus niet te worden opgenomen in de te implementeren component, bijvoorbeeld van een te publiceren lijst. Waar het er meer zijn, worden deze attributen overgeërfd van een klasse in het [metamodel](#) waarvan de overeenkomstige klasse in dat metamodel bestaansafhankelijk was. In het [metamodel](#) was laatstgenoemde klasse dus toegankelijk voor de bestaansafhankelijke klasse, maar in het specifieke logische model niet meer aanwezig en dus ook niet meer toegankelijk. Zou de betreffende klasse in het logische model het attribuut dus niet hebben overgenomen, zou deze verloren zijn.

Waar een invariant uit het [metamodel](#) past binnen de scope van het specifieke logische model, verschijnt deze ook als invariant bij het logische model, hoewel de formulering zal zijn aangepast aan de ordening en naamgeving in het logische model. Daarenboven kunnen op logisch niveau ook nieuwe invarianten verschijnen. De meeste daarvan zijn vervangen: in de stap van het [metamodel](#) naar een logisch model raken verbanden verbroken tussen klassen. Als die verbanden toch van belang zijn in het logische model worden er attributen uit het [metamodel](#) verorven van een bepaalde klasse in het [metamodel](#) naar een lagere klasse, waarvan wel een pendant voorkomt in het logische model. Met "lagere klasse" wordt bedoeld dat deze bestaansafhankelijk is van de andere (hogere) klasse. Zo'n vervangingsinvariant staat opgeschreven met een `.` Vóór dat pijltje staat het ervende attribuut van de *logische* klasse, erachter staat het pad *in het metamodel* naar de vervende klasse.

Ook de basisklassen uit het [metamodel](#) worden, waar van toepassing, overgenomen door het logische model. Op een enkele plek verschijnen in het logische model ook nieuwe basisklassen.

De logische modellen hebben een meer op implementatie toegespitste structuur dan het [metamodel](#). Dat [metamodel](#) is gestoeld op associatieklassen en bestaansafhankelijkheid, de logische modellen zijn meer hiërarchisch. Hiërarchie is een insnoering van associatieve bestaansafhankelijkheid, maar

past beter bij menige gangbare implementatietechnologie, waaronder zeker XML, waarin de vier lijsten geïmplementeerd worden. Die insnoering betekent wel dat de logische modellen minder duurzaam en minder uitbreidbaar zijn dan het [metamodel](#); wat voor het [metamodel](#) een eenvoudige uitbreiding is kan voor de logische modellen een stevige ingreep zijn. Dat is de prijs van hiërarchie.

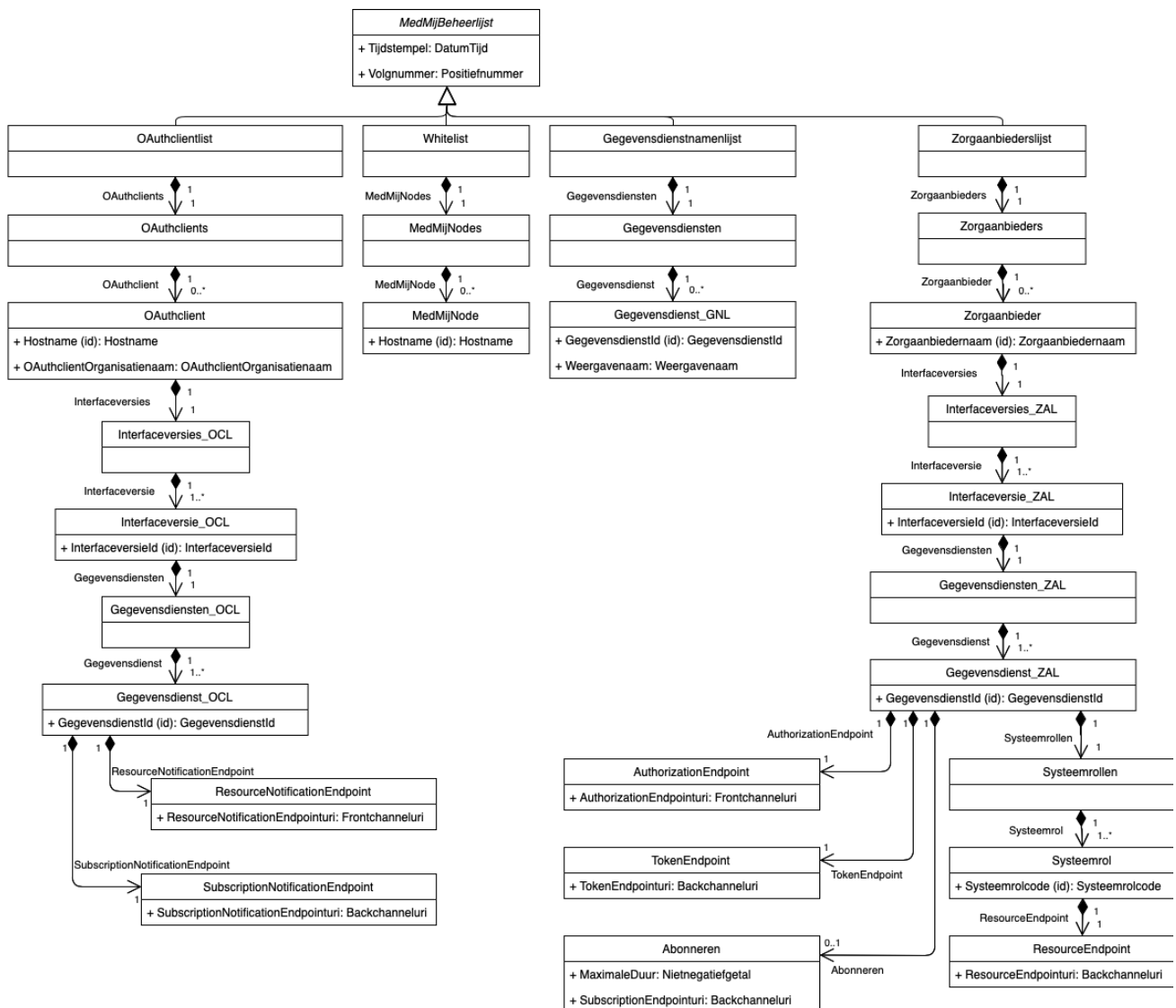
Bij de vertaling van de associativiteit van het [metamodel](#) naar de hiërarchie van de logische modellen is een aantal vuistregels gebruikt.

- De top van de hiërarchie van een logisch model wordt bepaald door de scope van de implementatiecomponent. De *Zorgaanbiederslijst*, bijvoorbeeld, somt allereerst de *Zorgaanbieders* op. Vanuit dat "logische centrum" wordt de hiërarchie van boven naar beneden afgelopen, zonder de scope van de implementatiecomponent te overschrijden. De stap naar beneden in de hiërarchie krijgt in het logische model typisch de vorm van een uses-relatie (de gestippelde pijl).
- Onderweg wordt een compositiehiërarchie aangelegd en in elke stap een selectie gemaakt uit de in het [metamodel](#) beschikbare attributen, op basis van de scope van de implementatiecomponent. Daarbij worden logische klassen niet gecombineerd tot een grofmaziger klasse, zelfs niet als er geen enkel attribuut overblijft. De klasse-granulariteit van het logische model is dus vergelijkbaar met die van het [metamodel](#).
- Bovendien worden, zoals hierboven beschreven, attributen die in het [metamodel](#) buiten de scope dreigen te vallen, maar wel nodig zijn, vererfd naar binnen de scope. Waar dat gebeurt, wordt de vererving gepreciseerd in de lijst van logische invarianten.
- Lagere klassen in de uses-hiërarchie vallen geheel binnen de logische scope van de hogere. Een hiërarchie creëert zo ook gesloten "name spaces". Dat betekent dat hun naamgeving eenvoudiger en korter kan dan in het [metamodel](#), waar alle contexten juist open zijn. In de logische modellen krijgen de namen van de klassen dus pas betekenis wanneer hogere klassen mee worden beschouwd. Maar dat vereenvoudigt de implementatie. In een aparte tabel bij elk logisch model wordt voorkomen dat door deze naamwijzigingen het verband met het [metamodel](#) verloren zou gaan.
- Een enkele keer heeft het vorige punt de consequentie dat er een homoniem dreigt te ontstaan binnen één logisch model (zoals *Gegevensdienst* en *Gegevensdiensten* in de logische model van de lijsten en de rapporten). In dat geval worden de namen uitgebreid zodat hun hiërarchische context zichtbaar wordt (namelijk met `_GNL`, `_OCL`, `_ZAL`, `_BR` en `_PR`).

Merk op dat de uses-hiërarchie de bestaansafhankelijkheidsrelatie ondersteboven zet. In de corresponderende klassen in het [metamodel](#) wordt in de uses-relatie de gebruikte klasse boven de gebruikende geplaatst, in de logische modellen juist andersom. Dit kenmerkt het doorslaggevende verschil tussen de conceptuele denkwijze van het [metamodel](#) en de bouw-gerichte denkwijze van de logische modellen. Voor de consistentie en duurzaamheid van het MedMij Afsprakenstelsel is het zaak om in het modelbeheer het [metamodel](#) centraal te plaatsen en vervolgens de logische modellen ermee in overeenstemming te houden. Het [metamodel](#) zorgt zo ook voor de duurzame consistentie tussen de verschillende logische modellen. Van die consistentie zijn de betrouwbaarheid en interoperabiliteit afhankelijk die door het MedMij Afsprakenstelsel geleverd moet worden.

## Lijsten

### Logisch model



## Logische invarianten

Betreft instanties van logische klasse ...	Invariant	Component	Toelichting	Aard	Herkomst
<i>Abonneren</i>	Voor elk <i>Abonneren a</i> geldt:  <i>a.MaximaleDuur</i> <= de maximale duur van <i>Abonnementen</i> op die <i>Gegevensdienst</i> zoals in de <i>Catalogus</i> aangegeven	<i>Zorgaanbiederslijst</i>	Een <i>Zorgaanbieder</i> kan de maximale abonnementsduur die hij aanbiedt voor een <i>Gegevensduur</i> , op een <i>Interfaceversie</i> , beperken. Daarbij moet hij echt blijven onder de maximale duur die MedMij voor die <i>Gegevensdienst</i> in de <i>Catalogus</i> heeft aangegeven.	niet-lokale afhankelijkheid	metamodel Zorgaanbie
<i>Abonneren</i>	Voor elk <i>Abonneren a</i> geldt:  <i>a.SubscriptionEndpointuri</i> combinatie van <i>s.MedMijNode.DeelnemerNode.Node.Hostname</i> en <i>s.AuthorizationEndpointpath</i> , conform de adresseringsverantwoordelijkheden op de <i>Interfaces</i> -pagina.	<i>Zorgaanbiederslijst</i>	Zie de <i>Interfaces</i> -pagina.	vererving	logisch moc
<i>AuthorizationEndpoint</i>	Voor elk <i>AuthorizationEndpoint a</i> geldt: <i>a.AuthorizationEndpointuri</i> combinatie van <i>a.MedMijNode.DeelnemerNode.Node.Hostname</i> en <i>a.AuthorizationEndpointpath</i> , conform de adresseringsverantwoordelijkheden op de <i>Interfaces</i> -pagina.	<i>Zorgaanbiederslijst</i>	Zie de <i>Interfaces</i> -pagina.	vererving	logisch moc

<i>Gegevensdienst_OCL</i>	Voor elke <i>Gegevensdienst_OCL</i> <i>g</i> met haar corresponderende <i>ZorgaanbiederGegevensdienst</i> <i>z</i> geldt: <i>g.GegevensdienstId</i> <i>z.Gegevensdienst.GegevensdienstId</i>	<i>Zorgaanbiederslijst</i>	Zo erft de <i>Zorgaanbiederslijst</i> de <i>GegevensdienstId</i> 's van de <i>Catalogus</i> .	vererving	logisch moc
<i>Gegevensdienst_ZAL</i>	Voor elke <i>Gegevensdienst_ZAL</i> <i>g</i> met haar corresponderende <i>ZorgaanbiederGegevensdienst</i> <i>z</i> geldt: <i>g.GegevensdienstId</i> <i>z.Gegevensdienst.GegevensdienstId</i>	<i>Zorgaanbiederslijst</i>	Zo erft de <i>Zorgaanbiederslijst</i> de <i>GegevensdienstId</i> 's van de <i>Catalogus</i> .	vererving	logisch moc
<i>Gegevensdienstnamenlijst</i>	Er is precies één instantie hiervan.	<i>Gegevensdienstnamenlijst</i>	Dit is een eenling in het model.	getalsverhouding	logisch moc
<i>Interfaceversies_ZAL</i>	Voor elke <i>Gegevensdienst_OCL</i> <i>g1</i> geldt dat:  ALS: <ul style="list-style-type: none"> <li><i>g1.Gegevensdiensten_OCL.Interfaceversie_OCL</i> is de gepubliceerde <i>Interfaceversie</i></li> <li>er is een <i>Abonneren a1</i> zodat <i>a1.Gegevensdienst_OCL = g1</i></li> </ul> DAN is er een <i>Gegevensdienst_ZAL</i> <i>g2</i> waarvoor geldt dat: <ul style="list-style-type: none"> <li><i>g2.GegevensdienstId = g1.GegevensdienstId</i></li> <li><i>g1.Gegevensdiensten_OCL.Interfaceversie_OCL</i> is de verplichte <i>Interfaceversie</i></li> </ul>	<i>Zorgaanbiederslijst</i>	Op <i>Gegevensdiensten</i> waarvoor door een <i>OAuthClient</i> onder de gepubliceerde <i>Interfaceversie Abonnementen</i> worden aangeboden, worden ook onder de verplichte <i>Interfaceversie Abonnementen</i> aangeboden.	niet-lokale afhankelijkheid	metamodel

	<ul style="list-style-type: none"> <li>er is een <i>Abonneren a2</i> zodat <i>a2</i>. <i>Gegevensdienst_OCL = g2</i></li> </ul>				
<i>Interfaceversies_ZAL</i>	<p>Voor elke <i>Interfaceversies_ZAL</i>, dienst verplichte <i>Interfaceversie_ZAL vi</i> en diens gepubliceerde <i>Interfaceversie_ZAL gi</i> geldt dat</p> <p>ALS er een <i>Gegevensdienst_ZAL g1</i> is waarvoor geldt dat <i>g1</i>. <i>Gegevensdiensten_ZAL</i>. <i>Interfaceversie_ZAL = gi</i></p> <p>DAN is er een <i>Gegevensdienst_ZAL g2</i> waarvoor geldt dat <i>g2</i>. <i>Gegevensdiensten_ZAL</i>. <i>Interfaceversie_ZAL = vi</i></p>	<i>Zorgaanbiederslijst</i>	<i>Gegevensdiensten</i> die door een <i>Zorgaanbieder</i> onder de gepubliceerde <i>Interfaceversie</i> worden aangeboden, worden ook onder de verplichte <i>Interfaceversie</i> aangeboden.	niet-lokale afhankelijkheid	metamodel
<i>Interfaceversies_ZAL</i>	<p>Voor elke <i>Gegevensdienst_ZAL g1</i> geldt dat:</p> <p>ALS:</p> <ul style="list-style-type: none"> <li><i>g1.Gegevensdiensten_ZAL</i>. <i>Interfaceversie_ZAL</i> is de gepubliceerde <i>Interfaceversie</i></li> <li>er is een <i>Abonneren a1</i> zodat <i>a1</i>. <i>Gegevensdienst_ZAL = g1</i></li> </ul> <p>DAN is er een <i>Gegevensdienst_ZAL g2</i> waarvoor geldt dat:</p> <ul style="list-style-type: none"> <li><i>g2.GegevensdienstId = g1</i>. <i>GegevensdienstId</i></li> </ul>	<i>Zorgaanbiederslijst</i>	Op <i>Gegevensdiensten</i> waarvoor door een <i>Zorgaanbieder</i> onder de gepubliceerde <i>Interfaceversie</i> <i>Abonnementen</i> worden aangeboden, worden ook onder de verplichte <i>Interfaceversie</i> <i>Abonnementen</i> aangeboden.	niet-lokale afhankelijkheid	metamodel



	<ul style="list-style-type: none"> <li>• <i>g1.Gegevensdiensten_ZAL.Interfaceversie_ZAL</i> is de verplichte <i>Interfaceversie</i></li> <li>• er is een <i>Abonneren a2</i> zodat <i>a2.Gegevensdienst_ZAL = g2</i></li> </ul>				
<i>MedMijNode</i>	Voor elke <i>MedMijNode m</i> geldt: <i>m.Hostname = m.DeelnemerNode.Node.Hostname</i>	<i>Whitelist</i>	Zo erft de <i>MedMijNode</i> de <i>Hostname</i> van de <i>Node</i> die het is.	vererving	logisch moc
<i>MedMijNode</i>	De <i>hostname</i> van een <i>MedMijNode</i> bevat een domeinnaam die een fully-qualified domain name is, conform <a href="#">RFC3696</a> , <a href="#">sectie 2</a> .	<i>Whitelist</i>	Dit is een maatregel tegen risico <a href="#">4.4.1.4</a> uit RFC 6819.	lokale afhankelijkheid	<a href="#">metamodel</a>
<i>OAuthclient</i>	Voor elke <i>OAuthclient o</i> : <i>o.OAuthclientOrganisatiennaam</i> voldoet aan het <a href="#">OAuthclient-namenbeleid</a> .	<i>Applicatie</i>	Zie het <a href="#">OAuthclient-namenbeleid</a> .	lokale afhankelijkheid	<a href="#">metamodel</a>
<i>OAuthclient</i>	Voor elke <i>OAuthclient o</i> geldt: <i>o.Hostname</i> <i>o.MedMijNode.Hostname</i> .	<i>OAuthclientlist</i>	Zo erft de <i>OAuthclientlist</i> de <i>Hostnames</i> van de <i>Nodes</i> .	vererving	logisch moc
<i>OAuthclientlist</i>	Er is precies één instantie hiervan.	<i>OAuthclientlist</i>	Dit is een eenling in het model.	getalsverhouding	logisch moc
<i>ResourceEndpoint</i>	Voor elk <i>ResourceEndpoint r</i> geldt: <i>r.ResourceEndpointuri</i> combinatie van <i>r.MedMijNode.DeelnemerNode.Node.Hostname</i> en <i>r</i> .	<i>Zorgaanbiederslijst</i>	Zie de <a href="#">Interfaces</a> -pagina.	vererving	logisch moc

	<i>ResourceEndpointpath</i> , conform de adresseringsverantwoordelijkheden op de <a href="#">Interfaces</a> -pagina.				
<i>ResourceNotificationEndpoint</i>	Voor elk <i>ResourceNotificationEndpoint r</i> geldt: <i>r.ResourceNotificationEndpointuri</i> combinatie van <i>r.MedMijNode.DeelnemerNode.Node.Hostname</i> en <i>r.AuthorizationEndpointpath</i> , conform de adresseringsverantwoordelijkheden op de <a href="#">Interfaces</a> -pagina.	<i>OAuthclientlist</i>	Zie de <a href="#">Interfaces</a> -pagina.	vererving	logisch moc
<i>SubscriptionNotificationEndpoint</i>	Voor elk <i>SubscriptionNotificationEndpoint s</i> geldt: <i>s.SubscriptionNotificationEndpointuri</i> combinatie van <i>s.MedMijNode.DeelnemerNode.Node.Hostname</i> en <i>s.AuthorizationEndpointpath</i> , conform de adresseringsverantwoordelijkheden op de <a href="#">Interfaces</a> -pagina.	<i>OAuthclientlist</i>	Zie de <a href="#">Interfaces</a> -pagina.	vererving	logisch moc
<i>Systeemrol</i>	Voor elke <i>Systeemrol s</i> met haar corresponderende <i>ZorgaanbiederGegevensdienstSysteemrol z</i> geldt: <i>s.Systeemrolcode z.Systeemrol.Systeemrolcode</i> .	<i>Zorgaanbiederslijst</i>	Zo erft de <i>Zorgaanbiederslijst</i> de <i>Systeemrolcodes</i> van het <i>Register van Informatiestandaarden</i> .	vererving	logisch moc
<i>TokenEndpoint</i>	Voor elk <i>TokenEndpoint t</i> geldt: <i>t.TokenEndpointuri</i> combinatie van <i>t.MedMijNode.DeelnemerNode.Node.Hostname</i> en <i>t.TokenEndpointpath</i> , conform de adresseringsverantwoordelijkheden op de <a href="#">Interfaces</a> -pagina.	<i>Zorgaanbiederslijst</i>	Zie de <a href="#">Interfaces</a> -pagina.	lokale afhankelijkheid	logisch moc

<i>Whitelist</i>	Er is precies één instantie hiervan.	<i>Whitelist</i>	Dit is een eenling in het model.	getalsverhouding	logisch mo
<i>Zorgaanbiederslijst</i>	Er is precies één instantie hiervan.	<i>Zorgaanbiederslijst</i>	Dit is een eenling in het model.	getalsverhouding	logisch mo

## Logische basisklassen

Basisklasse	Definitie	Herkomst
<i>Backchanneluri</i>	Zie adresseringsverantwoordelijkheden op de <a href="#">Interfaces</a> -pagina. De domeinnaam is een fully-qualified domain name, conform <a href="#">RFC3696</a> , <a href="#">sectie 2</a> .	logisch model
<i>DatumTijd</i>	Conform het type <code>xs:dateTime</code> , zoals gespecificeerd in <a href="#">XML Schema 1.0</a> en inclusief een tijdzone-indicatie.	logisch model
<i>Frontchanneluri</i>	Zie adresseringsverantwoordelijkheden op de <a href="#">Interfaces</a> -pagina. De domeinnaam is een fully-qualified domain name, conform <a href="#">RFC3696</a> , <a href="#">sectie 2</a> .	logisch model
<i>GegevensdienstId</i>	String van minimaal één teken en maximaal 30 tekens.	<a href="#">metamodel</a>
<i>Hostname</i>	Zie adresseringsverantwoordelijkheden op de <a href="#">Interfaces</a> -pagina.	<a href="#">metamodel</a>
<i>InterfaceversieId</i>	String van minimaal één en maximaal 30 tekens.	<a href="#">metamodel</a>
<i>OAuthclientOrganisatiennaam</i>	Conform toepasselijk <a href="#">OAuthclient-namenbeleid</a> .	<a href="#">metamodel</a>
<i>Positiefnummer</i>	Een geheel getal ongelijk 0.	logisch model
<i>Systeemrolcode</i>	String van minimaal één teken en maximaal 30 tekens.	<a href="#">metamodel</a>
<i>Weergavenaam</i>	String van minimaal drie en maximaal 50 tekens.	<a href="#">metamodel</a>
<i>Zorgaanbiedernaam</i>	Conform toepasselijk <a href="#">Zorgaanbiedersnamenbeleid</a> .	<a href="#">metamodel</a>

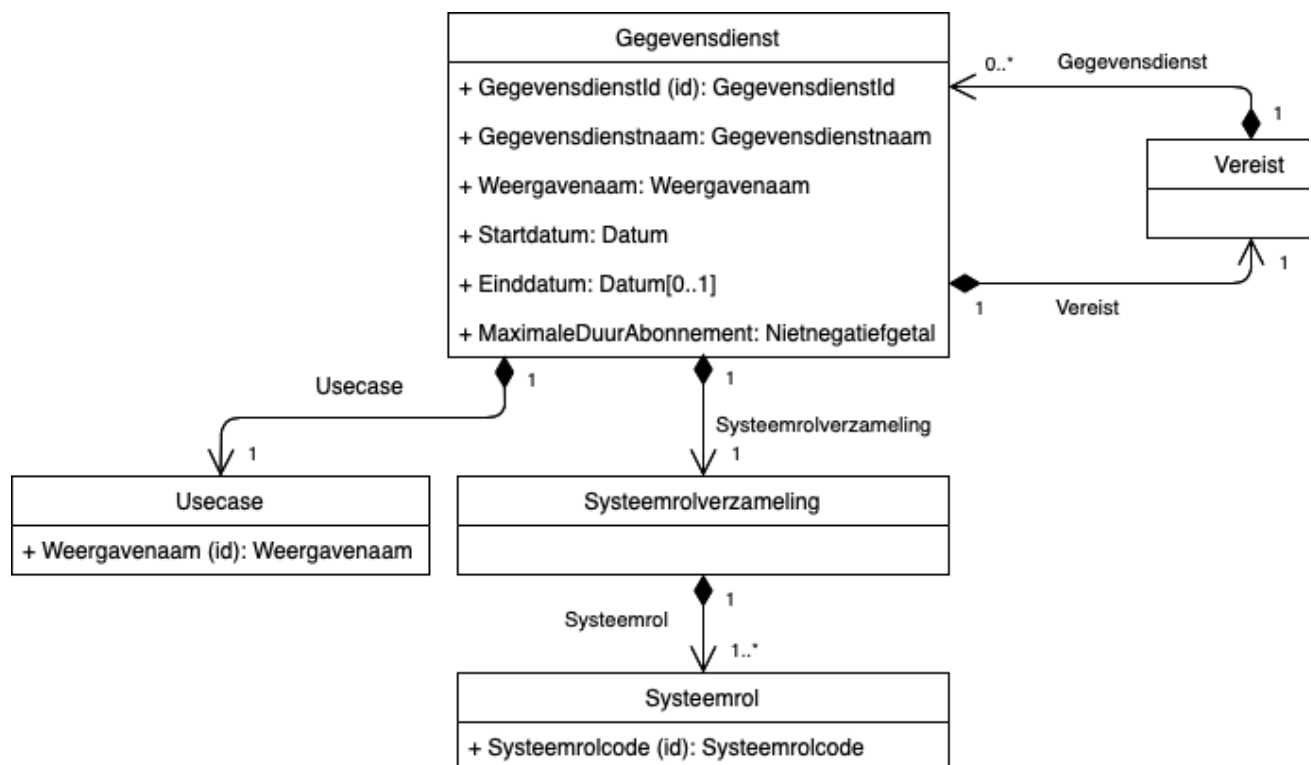
## Verband met metamodel

Klasse in logisch model	Herkomstklasse in metamodel
<i>Abonneren</i>	<i>ZorgaanbiederAbonnerenOpGegevensdienstInterfaceversie</i>
<i>AuthorizationEndpoint</i>	<i>AuthorizationEndpoint</i>
<i>Gegevensdienst_GNL</i>	<i>Gegevensdienst</i>
<i>Gegevensdienst_OCL</i>	<i>OAuthClientGegevensdienstInterfaceversie</i>
<i>Gegevensdienst_ZAL</i>	<i>ZorgaanbiederGegevensdienstInterfaceversie</i>
<i>Interfaceversie_OCL</i>	<i>Interfaceversie</i>
<i>Interfaceversie_ZAL</i>	<i>Interfaceversie</i>
<i>MedMijNode</i>	<i>MedMijNode</i>
<i>OAuthclient</i>	<i>OAuthclient</i>
<i>ResourceEndpoint</i>	<i>ResourceEndpoint</i>
<i>ResourceNotificationEndpoint</i>	<i>ResourceNotificationEndpoint</i>

<i>SubscriptionNotificationEndpoint</i>	<i>SubscriptionNotificationEndpoint</i>
<i>Systeemrol</i>	<i>ZorgaanbiederGegevensdienstSysteemrol</i>
<i>TokenEndpoint</i>	<i>TokenEndpoint</i>
<i>Zorgaanbieder</i>	<i>Zorgaanbieder</i>

## Catalogus

### Logisch model



## Logische invarianten

Betreft instanties van klasse ...	Invariant	Component	Toelichting	Aard	Herkomst
<i>Usecase</i>	Voor elke <i>Usecase</i> <i>u</i> geldt: <i>u.Weergavenaam</i> = "Verzamelen" OF <i>u.Weergavenaam</i> = "Delen"	<i>Catalogus</i>	Dit koppelt de namen van de subklassen aan de weergavenamen.	lokale afhankelijkheid	metamodel (bij <i>Usecase</i> )

## Logische basisklassen

Basisklasse	Definitie	Herkomst
<i>Datum</i>	Conform het type <code>xs:date</code> , zoals gespecificeerd in <a href="#">XML Schema 1.0</a> .	metamodel
<i>GegevensdienstId</i>	String van minimaal één teken en maximaal 30 tekens.	metamodel
<i>Gegevensdienstnaam</i>	String van minimaal drie en maximaal 50 tekens.	metamodel
<i>Nietnegatiefgetal</i>	Conform het type <code>xs:nonNegativeInteger</code> , zoals gespecificeerd in <a href="#">XML Schema 1.0</a> .	metamodel
<i>Systeemrolcode</i>	String van minimaal één teken en maximaal 30 tekens.	metamodel
<i>Weergavenaam</i>	String van minimaal drie en maximaal 50 tekens.	metamodel

## Verband met metamodel

Klasse/waarde in logisch model	Herkomstklasse in metamodel
<i>Gegevensdienst</i>	<i>Gegevensdienst</i>
<i>Usecase</i>	<i>Usecase</i> , <i>VerzamelenUsecase</i> en <i>DelenUsecase</i>

### Toelichting

De klasse *Usecase* is een abstracte klasse in het [metamodel](#). In het logische model zijn, in de compositiehiërarchie, echter concrete klassen nodig. In het kader van de *Catalogus* zijn we hier niet geïnteresseerd in de gehele semantiek van de conceptuele klassen *VerzamelenUsecase* en *DelenUsecase*, maar enkel in hun respectievelijke instanties, met de *Weergavenaam* die zij van de abstracte klasse *Usecase* krijgen, door middel van een invariant. Daarom gebruiken we in dit logische model een concrete klasse *Usecase*, die tot deze twee instantieert.

## MedMijStelselNode

### Logisch model

MedMijStelselNode
+ Hostname: Hostname

### Logische invarianten

Betreft instanties van klasse ...	Invariant	Component	Toelichting	Aard
<i>MedMijStelselNode</i>	Voor de <i>MedMijStelselNode</i> <i>m</i> geldt: <i>m.Hostname</i> <i>m.Node.Hostname</i>	<i>MedMijStelselNode</i>	Zo erft de <i>MedMijStelselNode</i> , van de <i>Node</i> die het is, de <i>Hostname</i> .	vererving

### Logische basisklassen

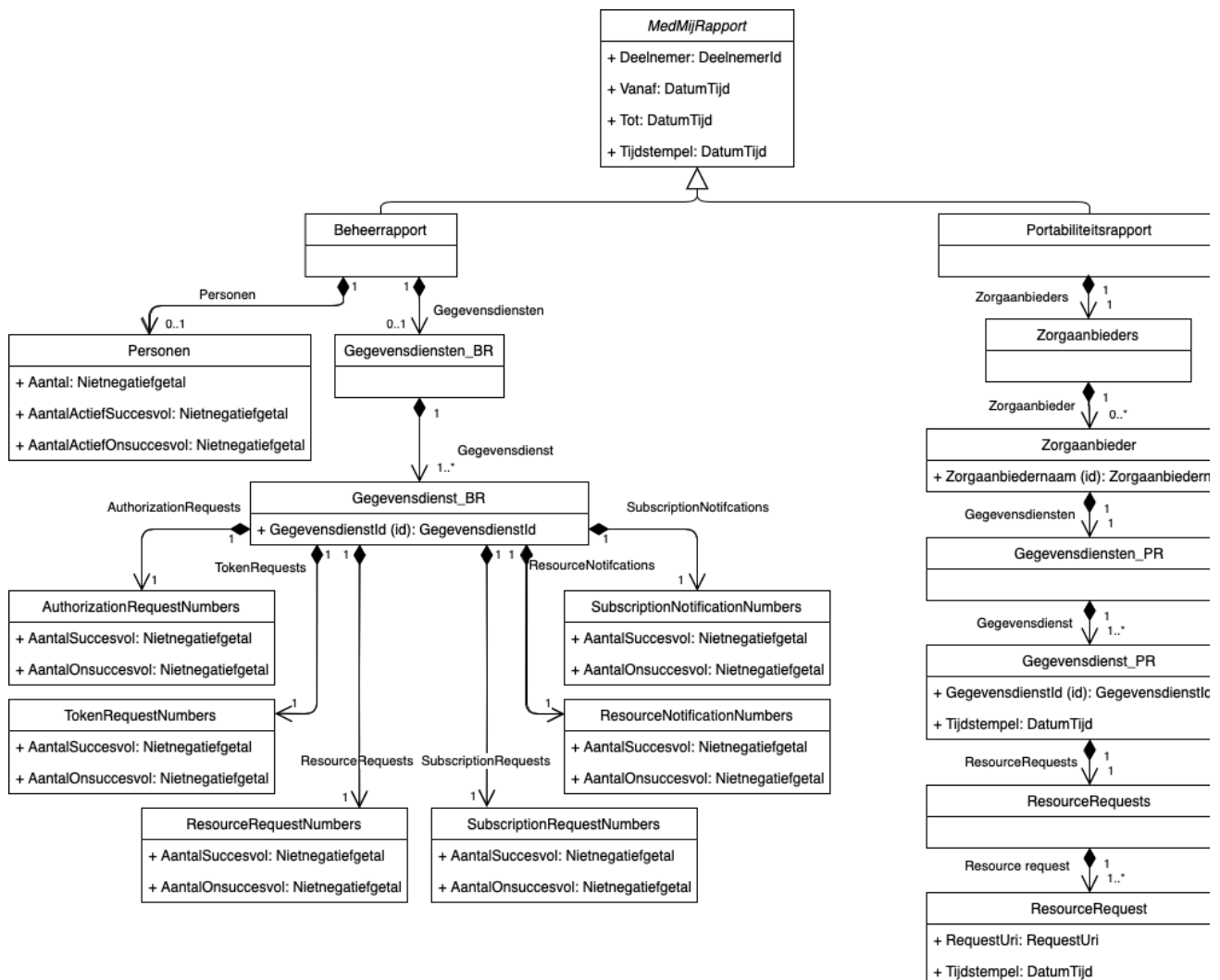
Basisklasse	Definitie	Herkomst
<i>Hostname</i>	Zie adresseringsverantwoordelijkheden op de Interfaces-pagina.	<a href="#">metamodel</a>

### Verband met metamodel

Klasse in logisch model	Herkomstklasse in metamodel
<i>MedMijStelselNode</i>	<i>MedMijStelselNode</i>

## Rapporten

### Logisch model



## Logische invarianten

Betreft instanties van logische klasse ...	Invariant	Component	Toelichting	Aard
<i>Beheerrapport</i>	Er is precies één instantie hiervan.	<i>Beheerrapport</i>	Dit is een eenling in het model.	getalsve
<i>Gegevensdienst_BR</i>	Voor elke <i>Gegevensdienst_BR</i> <i>g</i> met haar corresponderende <i>ZorgaanbiederGegevensdienst</i> <i>z</i> geldt: <i>g.GegevensdienstId</i> <i>z</i> . <i>Gegevensdienst</i> . <i>GegevensdienstId</i>	<i>Beheerrapport</i>	Zo erft het <i>Beheerrapport</i> de <i>GegevensdienstId</i> 's van de <i>Catalogus</i> .	verervin
<i>Gegevensdienst_PR</i>	Voor elke <i>Gegevensdienst_PR</i> <i>g</i> met haar corresponderende <i>ZorgaanbiederGegevensdienst</i> <i>z</i> geldt:	<i>Portabiliteitsrapport</i>	Zo erft het <i>Portabiliteitsrapport</i> de <i>GegevensdienstId</i>	verervin



	<i>g.GegevensdienstId</i> z. <i>Gegevensdienst</i> . <i>GegevensdienstId</i>		's van de <i>Catalogus</i> .	
<i>Portabiliteitsrapport</i>	Er is precies één instantie hiervan.	<i>Portabiliteitsrapport</i>	Dit is een eenling in het model.	getalsve

### Logische basisklassen

Basisklasse	Definitie	Herkomst
<i>DatumTijd</i>	Conform het type <code>xs:dateTime</code> , zoals gespecificeerd in <a href="#">XML Schema 1.0</a> en inclusief een tijdzone-indicatie.	logisch model
<i>DeelnemerId</i>	String van minimaal één en maximaal 30 tekens.	<a href="#">metamodel</a>
<i>GegevensdienstId</i>	String van minimaal één teken en maximaal 30 tekens.	<a href="#">metamodel</a>
<i>Nietnegatiefgetal</i>	Conform het type <code>xs:nonNegativeInteger</code> , zoals gespecificeerd in <a href="#">XML Schema 1.0</a> .	logisch model
<i>RequestUri</i>	String van minimaal twaalf en maximaal 2048 tekens.	<a href="#">metamodel</a>
<i>Zorgaanbiedernaam</i>	Conform toepasselijk <a href="#">Zorgaanbiedersnamenbeleid</a> .	<a href="#">metamodel</a>

### Verband met metamodel

Klasse in logisch model	Herkomstklasse in metamodel
<i>Gegevensdienst_BR</i>	<i>Gegevensdienst</i>
<i>Gegevensdienst_PR</i>	<i>Gegevensdienst</i>
<i>ResourceRequest</i>	<i>ResourceRequest</i>
<i>Zorgaanbieder</i>	<i>Zorgaanbieder</i>

## XML-schema's

### Toelichting

Op deze pagina staan de XML-schema's van:

- de lijsten die door *MedMij Beheer* aan *Bron* en *Uitgever* voor uiteenlopende doelen ter beschikking worden gesteld;
- de rapporten die door *Deelnemers* moeten kunnen worden opgeleverd.

De XML-schema's zijn een implementatie van de [logische modellen](#) van de lijsten in XML-syntax en vervullen daarom de rol van technisch model. XML past bij de hiërarchische structurering waarop al in de [logische modellen](#) is ingezet. Bovendien zijn XML-schema's en XML-bestanden serieel. Dat wil zeggen dat in de vertaling vanuit het [logische model](#) de klassen achter elkaar geplaatst moeten worden zonder hun diagrammatische ordening in het [logische model](#) te laten verdwijnen. Een compositierelatie in het logische model wordt een nesting in het XML-schema. Om de achter elkaar geplaatste modelelementen onderling te kunnen scheiden, zowel in het XML-schema als in de XML-instantie, en om de elementen te voorzien van meta-informatie, worden in XML tags gebruikt.

Net als op het conceptuele niveau van het [metamodel](#) en op het logisch niveau van het [logische model](#), verschijnen op het technische niveau ook invarianten. XML is zelfs in staat om sommige van die invarianten geautomatiseerd te controleren. In zulke XML-validatie wordt gecontroleerd of een zeker XML-bestand voldoet aan de structuur van een zeker XML-schema. Ook het MedMij Afsprakenstelsel maakt van deze gelegenheid gebruik door van ontvanger van de vier lijsten te eisen zo'n validatie uit te voeren. De XML-schema's daarvoor worden als onderdeel van het MedMij Afsprakenstelsel beschikbaar gesteld. Deze validatie biedt extra zekerheid over de juistheid van de verspreide lijsten en draagt zo bij aan de betrouwbaarheid van het functioneren van het MedMij-netwerk.

Toch zijn er nog verschillende manieren om het [logische model](#) van de lijsten in hun XML-schema's te vertalen. In het MedMij Afsprakenstelsel zijn daarbij de volgende afwegingen gebruikt:

- Alle typen en elementen die worden gebruikt voor een van de lijsten of rapporten, zijn in het XML-schema van de betreffende lijst of het betreffende rapport gedefinieerd. Er is dus geen gebruik gemaakt van een basisschema. Zo wordt de afhankelijkheid tussen de XML-schema's beperkt en wordt het gemakkelijker een van de schema's aan te passen zonder dat de andere schema's gewijzigd worden. De definities moeten echter blijven passen bij het [metamodel](#) en het [logische model](#); een aanpassing in een van deze modellen maakt aanpassing noodzakelijk van alle XML-schema's die door de wijziging geraakt worden.
- Bij het [logische model](#) van de lijsten en rapporten horen vier technische componenten. De hoogste klasse van elke component wordt het rootelement van het betreffende XML-schema. De attributen van de abstracte klassen bovenaan (*MedMijBeheerlijst* en *MedMijRapport*) worden over de technische modellen van de vier lijsten, respectievelijk de twee rapporten, verspreid. Er is dus voor elke lijst of rapport een apart XML-schema. Daardoor is de homonymie van *Gegevensdienst* en *Gegevensdiensten* geen probleem meer en kunnen in de namen de achtervoegsels *\_ZAL*, *\_GNL*, *\_OCL*, *\_BR* en *\_PR* achterwege blijven.
- Net als in de stap van het metamodel naar de logische modellen blijft de granulariteit van de klassen hetzelfde: er worden geen klassen samengenomen om een compacter schema te maken.
- Elk van de logische klassen, behalve de klasse die dienst doet als 'root', wordt afzonderlijk gedefinieerd als `complexType` in XML Schema, zodat hergebruik binnen het XML-schema mogelijk is.
- Elk van de basisklassen wordt afzonderlijk gedefinieerd als `simpleType` in XML Schema, zodat hergebruik binnen het XML-schema mogelijk is.

- Alle klassen en attributen uit het [logische model](#) zijn gemodelleerd als elementen in het XML-schema. Daarmee is een eenduidige vertaling mogelijk van het [logische model](#); er hoeft geen onderscheid tussen elementen en attributen te worden aangebracht. Elementen bieden meer mogelijkheden dan attributen en genieten daarom (als generieke keuze) de voorkeur.
- Daar waar in het [logische model](#) sprake is van identifiers, is in het XML-schema een 'uniqueness constraint' opgenomen.

## Schema's

Lijst of rapport	Bestandsnaam	Release	Versie bestand
<i>Zorgaanbiederslijst</i>	<a href="#">MedMij_Zorgaanbiederslijst.1.2.0.xsd</a>	3	9
<i>Whitelist</i>	<a href="#">MedMij_Whitelist.1.2.0.xsd</a>	2	10
<i>OAuthclientlist</i>	<a href="#">MedMij_OAuthclientlist.1.2.0.xsd</a>	4	8
<i>Gegevensdienstnamenlijst</i>	<a href="#">MedMij_Gegevensdienstnamenlijst.1.2.0.xsd</a>	1	8
<i>Beheerrapport</i>	<a href="#">MedMij_Beheerrapport.1.2.0.xsd</a>	2	4
<i>Portabiliteitsrapport</i>	<a href="#">MedMij_Portabiliteitsrapport.1.2.0.xsd</a>	1	4

Alleen de hierboven genoemde bestanden, met de aangegeven release en versie, mogen worden gebruikt in deze release van het MedMij Afsprakenstelsel.

### Voorbeeldbestanden (XML)

Van elke lijst is een voorbeeldbestand beschikbaar. Dit bestand maakt geen deel uit van de formele specificaties van het MedMij Afsprakenstelsel.

Lijst	Bestandsnaam	Versie voorbeeldbestand	Behorend bij XML-schema van de lijst met releasenummer
<i>Zorgaanbiederslijst</i>	<a href="#">MedMij_Zorgaanbiederslijst_example.xml</a>	6	3
<i>Whitelist</i>	<a href="#">MedMij_Whitelist_example.xml</a>	6	2
<i>OAuthclientlist</i>	<a href="#">MedMij_OAuthclientlist_example.xml</a>	8	4
<i>Gegevensdienstnamenlijst</i>	<a href="#">MedMij_Gegevensdienstnamenlijst_example.xml</a>	3	1
<i>Beheerrapport</i>	<a href="#">MedMij_Beheerrapport_example.xml</a>	7	2
<i>Portabiliteitsrapport</i>	<a href="#">MedMij_Portabiliteitsrapport_example.xml</a>	4	1

## Toelichting

### Tijdaspect

Het [metamodel](#) en de [logische modellen](#), met hun invarianten, werken "door de tijd". Zij beschrijven hoe de klassen samenhangen op elk moment. De XML-bestanden voor de lijsten zijn echter specifieke momentopnames van de instanties van de klassen. Er moet daarom een tijdslelement worden toegevoegd om lijsten die op verschillende momenten zijn gegenereerd, uit elkaar te kunnen houden, en om in retrospectief de geldigheidstermijn van een lijst te kunnen vaststellen.

- Elk XML-bestand kent een versie-aanduiding. Hiertoe wordt de combinatie van een `Volgnummer` en een `Tijdstempel` gebruikt. Hiermee wordt aan drie informatiebehoeften tegemoet gekomen:
  - Wanneer twee lijsten (van hetzelfde type) met opeenvolgende `Volgnummers` beschikbaar zijn, kan de geldigheidstermijn van de oudere lijst worden vastgesteld. Dat helpt bij de interpretatie van audit logs of foutopsporing.
  - Lijsten kunnen uniek worden geïdentificeerd. Dit kan aan de hand van `Volgnummer` of `Tijdstempel`, waarbij `Volgnummer` voor menselijke gebruikers vaak de meest intuïtieve zal zijn.
  - Per lijst kan worden nagegaan wanneer de laatste mutatie heeft plaatsgevonden. Dit zal in de regel een 'functionele' mutatie betreffen, geen fouterstel. Hieruit kan door vergelijking van opeenvolgende versies worden afgeleid wanneer de actuele lijst voor het laatst is gewijzigd; dat kan zinvol zijn bij het beoordelen van de effecten van changes of bij foutopsporing.
- `Tijdstempel` bestaat uit Datum, Tijd en Tijdzone-aanduiding, gebaseerd op `xs:dateTime`-type. Door voor een native XML-datatype te kiezen, wordt de implementatie vergemakkelijkt. Er geldt wel een restrictie op het element, dat afdwingt dat er altijd een Tijdzone-aanduiding wordt meegegeven.

### Releasebeheer

De bestandsnamen van de XML-schema's en XML-voorbeeldbestanden zijn zo gekozen dat zij niet wijzigen wanneer de inhoud van het XML-schema wijzigt. Dit vergemakkelijkt de implementatie van changes. Het is gebruikelijk om meta-informatie niet in de bestandsnaam op te nemen, maar in de XML-bestanden zelf (met name in de header). Daarom is het niet nodig om naast de informatie in het bestand, ook de bestandsnaam in te zetten voor versie-aanduiding.

Elk van de XML-schema's kent een eigen releasenummering. Zij kunnen daarmee onafhankelijk van elkaar worden aangepast. Daarmee wordt onnodige implementatielast bij een wijziging voorkomen. Het releasenummer is een geheel getal, om redenen van eenvoud. Altijd en alleen indien een XML-schema is gewijzigd, wordt het releasenummer met één opgehoogd.

De XML-schema's zijn integraal onderdeel van het afsprakenstelsel. Een wijziging van de XML-schema's leidt dan ook tot een nieuwe release van het afsprakenstelsel. Omgekeerd hoeft het niet zo te zijn dat een wijziging in de overige afspraken binnen het afsprakenstelsel, een wijziging van het XML-schema noodzakelijk maakt.

Omdat een wijziging in een XML-schema al snel tot incompatibiliteit met andere versies leidt (XML-bestanden die gebaseerd zijn op verschillende versies van het XML-schema zullen niet door het 'andere' XML-schema worden gevalideerd), is ervoor gekozen om het releasenummer op te nemen in de aanduiding van de namespace. Daarmee draagt een XML-bestand in de verwijzing naar de namespace tevens het releasenummer in zich. Zo wordt geborgd dat XML-bestanden niet met een verkeerde versie van het XML-schema worden gevalideerd.

De XML-schema's en de voorbeeld-XML-bestanden krijgen daarnaast een versienummer mee. Het versienummer is een geheel getal en wordt bij elke wijziging in het bestand met één opgehoogd. Met behulp van versienummering kunnen bestandsversies gedurende de ontwikkeling uit elkaar worden gehouden. Het nummer is ook aanwezig in productieveries; het is daarmee niet noodzakelijk om bij een statuswijziging van een release van het MedMij Afsprakenstelsel de XML-producten aan te passen, ook als die inhoudelijk niet gewijzigd zijn. Het versienummer wordt opgenomen als commentaar in het bestand, omdat dat niet machine-leesbaar hoeft te zijn en er op deze manier een eenduidige systematiek bestaat voor de XML-schema's en de XML-voorbeeldbestanden. Het commentaar heeft de vorm: `<!--File version: [versienummer]-->` en bevindt zich op de tweede regel van een bestand. De versienummering is, om redenen van eenvoud en duidelijkheid, onafhankelijk van de releasenummering van de XML-schema's.

## Namespaces

Voor de aanduiding van namespaces wordt gebruikgemaakt van een URL. Dit is de gemakkelijkste optie, omdat dit - anders dan bij een URN - geen namespaceregistratie bij IANA vereist. De namespace-URL kent de volgende opbouw: `xmlns://afsprakenstelsel.medmij.nl/[naamLijst|naamRapport]/release[releasenummer]`.

- Een namespace-URL gebruikt `xmlns://` als schema-aanduiding. Daarmee wordt duidelijk gemaakt dat het slechts een identificatie betreft, en dat de URL niet is bedoeld voor dereferencing (bijvoorbeeld om het XML-schema te downloaden).
- Het domein `afsprakenstelsel.medmij.nl` is een unieke hostname op het internet. Gebruik daarvan biedt zowel voldoende herkenbaarheid als uniciteit.
- De naamLijst kent één van de volgende waarden: `Whitelist`, `OAuthclientlist`, `Zorgaanbiederslijst` of `Gegevensdienstnamenlijst`.
- De naamRapport kent één van de volgende waarden: `Beheerrapport` of `Portabiliteitsrapport`.
- De aanduiding `release` is toegevoegd voor de menselijke leesbaarheid en daarmee duidelijkheid.

Waar het metamodel geen namen heeft gedefinieerd, kiezen we om redenen van consistentie en elegantie voor lowercase in de opbouw van de URL. Er wordt gebruikgemaakt van `elementFormDefault = "qualified"`. Dit vergroot de leesbaarheid van de XML-schema's omdat er geen prefixes nodig zijn bij het definiëren van elementen, en doet niet af aan enige functionaliteit. De prefixes voor de namespaces worden omwille van de leesbaarheid van de XML-schema's zo kort mogelijk gehouden, bestaan altijd uit drie letters en zijn geheel in lowercase. Onderstaande tabel geeft weer bij welke lijst of rapport welke prefix wordt gebruikt.

Lijst of rapport	Prefix
<i>Gegevensdienstnamenlijst</i>	gnl
<i>OAuthclientlist</i>	ocl
<i>Whitelist</i>	whl
<i>Zorgaanbiederslijst</i>	zal
<i>Beheerrapport</i>	bhr
<i>Portabiliteitsrapport</i>	pbr

## Syntactische keuzes

De XML-schema's gaan uit van [XML 1.0](#) en XML Schema 1.0 (opgebouwd uit specificaties aangaande [structuur](#) en [datatypes](#)). Deze versies bieden voldoende functionaliteit en kennen een zeer brede implementatie en ondersteuning.

De bestandsnaam van een XML-schema kent de opbouw `MedMij_[naamLijst].xsd`. De variabele `naamLijst` betreft één van de volgende waarden: `Whitelist`, `OAuthclientlist`, `Zorgaanbiederslijst` of `Gegevensdienstnamenlijst`.

De XML-schema's bevatten de XML Declaration `<?xml version="1.0" encoding="UTF-8"?>`. De aanwezigheid van een declaratie wordt aanbevolen door [XML 1.0](#). De encoding is optioneel bij het gebruik van UTF-8. De encoding is echter toch expliciet omdat dit mogelijke onzekerheid over de bedoeling of het correct volgen van de specificaties voorkomt. Er wordt geen gebruik gemaakt van het pseudo-attriboot `standalone`, omdat er gebruik gemaakt wordt van XML-schema's in plaats van DTD's.

Omwillen van de leesbaarheid zijn de XML-schema's pretty-printed; door het gebruik van regeleinden en inspringing wordt de leesbaarheid vergroot. Verder kent elk XML-schema een standaardvolgorde in haar opbouw:

- Het rootelement, voorafgegaan door de commentaartekst `<!--Rootelement-->`.
- De definitie van de logische klassen, voorafgegaan door de commentaartekst `<!--Logische klassen-->`.
- De definitie van de basisklassen, voorafgegaan door de commentaartekst `<!--Basisklassen-->`.

De volgorde waarin de klassen worden gedefinieerd is hierbinnen vrij.

Voor uniqueness constraints wordt gebruikgemaakt van `<xs:unique>`. De (verplichte) naam van uniqueness constraints in XML wordt opgebouwd volgens `Unieke_[naamKlasse]`. Zo vertaalt de eigenschap van het attribuut `Hostname` van de klasse `MedMijNode` uit het [logische model](#) waartoe de whitelist behoort zich in een uniqueness constraint met de naam `Unieke_MedMijNode`. Er kan worden volstaan met de naam van de klasse (zonder de hiërarchische context), omdat klassenamen op grond van het [logische model](#) uniek zijn. De naam van het attribuut hoeft niet te worden benoemd. Welke attributen tezamen de identiteit van een instantie van een klasse vormen is weergegeven in het [logische model](#). Binnen `<xs:unique>` wordt enkel `<xs:selector>` gebruikt voor de XPath-expressie; `<xs:field>` wordt opgenomen (conform de XML-specificatie) maar leeggelaten (kent de vulling `.` (punt)). Dit is een eenvoudiger keuze dan wanneer een criterium voor de splitsing van de XPath-expressie over `<xs:selector>` en `<xs:field>` zou moeten worden gegeven.

Er wordt gebruikgemaakt van `<xs:sequence>` binnen alle complexTypes, niet van `<xs:all>`, omdat het zo mogelijk is om elementen vaker dan eenmaal te gebruiken. Dat is een eigenschap waar veel gebruik van wordt gemaakt; het is inherent aan het karakter van de lijsten en is relevant bij veel van de compositierelaties (die geen maximum-omvang van de verzameling kennen).

De XML-schema's bevatten geen Byte Order Mark. Het gebruik van een Byte Order Mark is volgens [XML 1.0](#) optioneel bij UTF-8. [RFC 3629, hoofdstuk 6](#), stelt dat het Byte Order Mark verboden moet worden, daar waar UTF-8 verplicht wordt gesteld.

## Basisklassen

### Toelichting

De definitie van de basisklassen in het [logische model](#) is vertaald naar `simpleTypes` in XML-schema, die voortbouwen op een native XML-datatype en daar soms verdere restricties aan verbinden.

Merk op dat de patronen van *Backchanneluri* en *Frontchanneluri* identiek zijn.

Basisklasse	Basis (XML-datatype)	minLength	maxLength	pattern
<i>Backchanneluri</i>	<code>xs:string</code>			<code>https://([a-z0-9])([a-z0-9-])*(\.)+([a-z0-9])([a-z0-9-])*([a-z0-9])?(/[^\?#/\+])*</code>
<i>DatumTijd</i>	<code>xs:dateTime</code>			<code>.{20,}</code>
<i>Duur</i>	<code>xsd:duration</code>			
<i>Frontchanneluri</i>	<code>xs:string</code>			<code>https://([a-z0-9])([a-z0-9-])*(\.)+([a-z0-9])([a-z0-9-])*([a-z0-9])?(/[^\?#/\+])*</code>
<i>GegevensdienstId</i>	<code>xs:string</code>	1	30	
<i>Hostname</i>	<code>xs:string</code>			<code>(([a-z0-9])([a-z0-9-])*(\.)+([a-z0-9])([a-z0-9-])*([a-z0-9])?(/[^\?#/\+])*)</code>
<i>Nietnegatiefgetal</i>	<code>xs:nonNegativeInteger</code>			
<i>OAuthclientOrganisatienaam</i>	<code>xs:string</code>	3	50	
<i>Positiefnummer</i>	<code>xs:positiveInteger</code>			
<i>Systeemrolcode</i>	<code>xs:string</code>	1	30	
<i>Weergavenaam</i>	<code>xs:string</code>	3	50	
<i>Zorgaanbiedernaam</i>	<code>xs:string</code>	10	287	



## XML-bestanden voor lijsten

### Toelichting

De XML-bestanden waarmee MedMij Beheer de *Zorgaanbiederslijst*, de *Whitelist*, de *OAuth Client List* en de *Gegevensdienstnamenlijst* ontsluit voldoen aan enkele eisen, zodat *PGO Server*, *Authorization Server* en *MedMijNode* weten waarop zij kunnen rekenen voor de goede verwerking van deze lijsten.

1. Het XML-bestand van de *Zorgaanbiederslijst* heet `MedMij_Zorgaanbiederslijst.xml`. Het XML-bestand van de *Whitelist* heet `MedMij_Whitelist.xml`. Het XML-bestand van de *OAuth Client List* heet `MedMij_OAuthclientlist.xml`. Het XML-bestand van de *Gegevensdienstnamen* heet `MedMij_Gegevensdienstnamenlijst.xml`.

2. Bij een wijziging in een lijst die tot hernieuwde publicatie leidt, wordt het volgnummer van de lijst met één opgehoogd.

### Toelichting

De bestandsnamen van de lijsten zijn zo gekozen dat zij niet wijzigen wanneer de inhoud van het XML-schema wijzigt. Dit vergemakkelijkt de implementatie van changes. Het is gebruikelijk om meta-informatie niet uit de bestandsnaam te halen, maar uit de XML-bestanden zelf (met name uit de header). Daarom is het niet nodig om naast de informatie in het bestand, ook nog eens de bestandsnaam in te zetten voor versie-aanduiding.

3. De in verantwoordelijkheid 1 bedoelde XML-bestanden maken gebruik van een default namespace, zijnde de namespace waarin het bijpassende XML-schema is gedefinieerd, zonder prefix.

### Toelichting

De afwezigheid van (onnodige) prefixes komt de leesbaarheid ten goede en voorkomt dat bij de implementatie gebruik wordt gemaakt van namespace-aanduidingen en prefixes die in de toekomst mogelijk wijzigen.

4. De in verantwoordelijkheid 1 bedoelde XML-bestanden:

- voldoen aan [XML 1.0](#) en [XML Schema 1.0](#).
- zijn pretty-printed (verplicht gebruik van regeleinden en inspringing).
- bevatten de XML Declaration `<?xml version="1.0" encoding="UTF-8"?>`.
- bevatten geen Byte Order Mark.

### Toelichting

Deze vier eisen gelden ook voor de op de XML-bestanden van toepassing zijnde XML-schema's. Voor de toelichting ervan zij daarom verwezen naar die op de pagina over die [XML-schema's](#).

## Normenkader informatiebeveiliging

Alle deelnemers dienen in het bezit te zijn van een geldige NEN 7510-certificering, ongeacht hun grootte en of ze dienstverlener in het persoonsdomein of zorgaanbiedersdomein zijn. Ook de beheerorganisatie zal voor de uitvoering van haar diensten binnen het MedMij netwerk gebonden zijn aan de NEN 7510 norm. Gebruik van NEN 7510:2011 voor certificatie doeleinden onder accreditatie blijft mogelijk tot medio 2020, te weten 2 jaar na publicatie van het certificatieschema NCS 7510:2018. Dit nieuwe certificatieschema behorend bij NEN 7510-1:2017 is begin juni 2018 gepubliceerd. MedMij stelt de volgende eisen aan een NEN 7510-certificering voor deelnemers:

- De Dienstverlener zorgaanbieder moet de zorgaanbieders als belangrijke belanghebbenden hebben geïdentificeerd in het uitvoeren/herijken van de risicoanalyse (zie ook hetgeen over de de rollen en verantwoordelijkheden ten opzichte van de verwerking van persoonsgegevens is opgenomen in de [Juridische context](#));
- Bij de selectie van de van toepassing zijnde maatregelen dienen ten minste de maatregelen uit het normenkader informatiebeveiliging te zijn opgenomen;
- Indien de maatregel een implementatie voorschrijft, dient de maatregel op deze wijze te worden geïmplementeerd. De deelnemer heeft dit middels een self assessment gecontroleerd en onderbouwd. Hiervoor kan het format voor de onderbouwende rapportage als hulpmiddel dienen.

De deelnemer toont jaarlijks met een [Aanvullende auditverklaring en onderbouwende rapportage \(download hier\)](#) aan te voldoen aan het normenkader MedMij. Voor de onderbouwende rapportage bij de auditverklaring wordt door MedMij een format beschikbaar gesteld. Blijkt uit de aanvullende auditverklaring dat de deelnemer niet (meer) voldoet, dan beoordeelt de Stichting MedMij op basis van de onderbouwende rapportage of en op welke manier het [Nalevingsbeleid](#) moet worden toegepast.

De NEN 7510-certificering en de aanvullende auditverklaring met rapportage dienen te worden afgegeven door een Conformiteit Beoordelende Instelling (CBI), die NEN 7510 geaccrediteerd is door de Raad voor Accreditatie of een NEN 7510 licentieovereenkomst heeft met NEN. Aan de uitvoerend auditor die de verklaring afgeeft worden daarmee dus dezelfde eisen gesteld door de CBI als voor de afgifte van het NEN 7510 certificaat. Tevens dient het NEN 7510 certificaat te zijn opgenomen in het door NEN beheerde nationale certificatenregister NEN 7510. Voor het NEN 7510 certificaat gelden de door NEN aangehouden termijnen voor hercertificering. Voor vragen van CBI's over het normenkader kan contact worden opgenomen via [secmgt@medmij.nl](mailto:secmgt@medmij.nl).

## Normenkader

Beheersmaatregel	DVP	DVZA	BO	Implementatie
<a href="#">A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen</a>	✓	✓		Opgeslagen persoonlijke gezondheidsgegevens MOETEN beschermd worden door middel van disk-level en/of database-level encryptie. Hiervoor wordt verwezen naar de aanbevelingen die gelden voor 'near term protection' en 'long-term protection' in de ECRYPT-CSA aanbevelingen, zie hieronder.
<a href="#">A.12.1.2 (1) Wijzigingsbeheer</a>	✓	✓	✓	De IT-beheerprocessen MOETEN aansluiten op het MedMij Change- en releasebeleid.
<a href="#">A.12.1.2 (2) Wijzigingsbeheer</a>	✓	✓	✓	

Niet-standaard wijzigingen op de IT componenten die gebruikt worden binnen de scope van MedMij MOETEN op basis van het vier-ogen-principe worden uitgevoerd.

A.12.1.2 (3) Wijzigingsbeheer	✓	✓	✓	Indien er wijzigingen plaatsvinden die mogelijk significante impact hebben op de informatiebeveiliging, MOET de penetratietest zoals benoemd in <a href="#">A.18.2.3 (1) Beoordeling van technische naleving</a> voor deze componenten opnieuw uitgevoerd worden.
A.12.1.3 (1) Capaciteitsbeheer	✓	✓		Maatregelen MOETEN zijn gedocumenteerd en geïmplementeerd om te (kunnen) voldoen aan de beschikbaarheidseisen zoals vastgelegd in <a href="#">Token interface</a> en <a href="#">Resource interface</a> .
A.12.1.3 (2) Capaciteitsbeheer			✓	Maatregelen MOETEN zijn gedocumenteerd en geïmplementeerd om te (kunnen) voldoen aan de beschikbaarheidseisen zoals vastgelegd in <a href="#">GNL-, OCL- en ZAL-interface</a> .
A.12.3.1 Back-up van informatie	✓			Er MOETEN maatregelen zijn geïmplementeerd waardoor het gegevensverlies van persoonlijke gezondheidsinformatie maximaal 24 uur bedraagt. Daarnaast moet een herstelprocedure zijn ingericht waardoor de gegevens van een persoon binnen 24 uur terug kunnen worden geplaatst in geval van een incident. Deze herstelprocedure wordt minimaal jaarlijks getest.
A.12.4.1 Gebeurtenissen registreren	✓	✓		<p>Logging MOET plaatsvinden zoals gespecificeerd in het afsprakenstelsel (zie <a href="#">Processen en informatie</a> onder Logging)</p> <p>Daarnaast MOETEN de volgende acties ten minste 12 maanden onweerlegbaar en controleerbaar worden gelogd:</p> <ul style="list-style-type: none"> <li>• De actie waarbij de persoon via de DVP bij de DVZA gegevens wil opvragen</li> <li>• De acties waarbij de persoon toestemming geeft voor de uitwisseling conform de specificaties in het afsprakenstelsel (indien uitgevoerd onder verantwoordelijkheid van de DVZA)</li> </ul>
A.12.4.3 Logbestanden van beheerders en operators	✓	✓		<ol style="list-style-type: none"> <li>1. Het gebruik van toegangsrechten op IT-componenten waar persoonlijke gezondheidsgegevens worden verwerkt MOET worden gelogd;</li> <li>2. Deze logging MOET ten minste maandelijks worden gecontroleerd. Dit</li> </ol>

geldt ook voor eventuele  
onderaannemers;

3. Hierbij MOET functiescheiding  
gewaarborgd zijn;
4. Tijdens deze controle moet aandacht zijn  
voor onterecht/onnodig gebruik door  
medewerkers (met aantoonbare  
opvolging).

A.12.4.4 Kloksynchronisatie	✓	✓	✓	<p>De klokken van IT componenten die communiceren via MedMij en logging in het kader van MedMij bijhouden, MOETEN worden gesynchroniseerd met <a href="https://pool.ntp.org">pool.ntp.org</a>.</p> <p>Het is toegestaan te synchroniseren met een alternatieve NTP-server, wanneer maatregelen zijn getroffen om de afwijking met <a href="https://pool.ntp.org">pool.ntp.org</a> niet groter dan plus of min 500 ms te laten zijn.</p>
A.12.6.1 Beheer van technische kwetsbaarheden	✓	✓	✓	<p>De processen MOETEN aansluiten op de <a href="#">Operationele processen</a> in het MedMij Afsprakenstelsel ten aanzien van het beheer van technische kwetsbaarheden.</p> <p>Dit dient te omvatten:</p> <ul style="list-style-type: none"> <li>• Identificeren van kwetsbaarheden in de eigen technologie, onderzoeken van relevantie van door de beheerorganisatie geïdentificeerde kwetsbaarheden + terugkoppeling naar de beheerorganisatie hieromtrent;</li> <li>• Het patchen van systemen of anderszijds mitigeren van de kwetsbaarheid;</li> <li>• Het tijdig kunnen doorlopen van de gehele procedure bij hoog risico-kwetsbaarheden.</li> </ul>
A.14.2.1 Beleid voor beveiligd ontwikkelen	✓	✓	✓	<p>Bij het vaststellen voor het beleid voor beveiligd ontwikkelen MOETEN de ICT-beveiligingsrichtlijnen voor webapplicaties van het NCSC uit het "Uitvoeringsdomein" overwogen worden (<a href="https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties">https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties</a>).</p> <p>Voor mobiele applicaties MOETEN de Beveiligingsrichtlijnen voor mobiele applicaties van het NCSC overwogen worden (<a href="https://www.ncsc.nl/documenten/publicaties/2019/mei/01/beveiligingsrichtlijnen-voor-mobiele-apparaten">https://www.ncsc.nl/documenten/publicaties/2019/mei/01/beveiligingsrichtlijnen-voor-mobiele-apparaten</a>).</p>
A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten	✓	✓	✓	<p>Organisaties MOETEN relevante MedMij beheersmaatregelen contractueel beleggen bij hun leveranciers.</p>

A.15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers	✓	✓	✓	Organisaties MOETEN toezien op correcte naleving van de relevante MedMij beheersmaatregelen die bij een leverancier belegd zijn.
A.16.1.1 Verantwoordelijkheden en procedures	✓	✓	✓	De processen voor het behandelen van incidenten en calamiteiten moeten aansluiten op de <a href="#">Operationele processen</a> in het afsprakenstelsel.
A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging	✓	✓	✓	<p>Kwetsbaarheden en incidenten die betrekking hebben op persoonlijke gezondheidsgegevens of het functioneren van het MedMij stelsel MOETEN binnen 48 uur gemeld te worden bij het centrale incident management team. Zie <a href="#">Deelnemersovereenkomsten</a>.</p> <p>DVZA maken hierover zonodig afspraken met de aangesloten ZA's.</p>
A.16.1.7 Verzamelen van bewijsmateriaal	✓	✓	✓	<p>Medewerking MOET worden verleend aan (forensische) onderzoeken, door het aanleveren van gevraagde bewijsmaterialen, zulks op verzoek van de beheerorganisatie of bevoegde instanties.</p> <p>DVZA maken hierover zonodig afspraken met de aangesloten ZA's.</p>
A.18.2.3 (1) Beoordeling van technische naleving	✓	✓		<p>Tenminste jaarlijks MOET een whitebox applicatiepenetratietesten worden uitgevoerd op de externe koppelvlakken door een externe, onafhankelijke organisatie.</p> <p><b>Voor toetreding</b> heeft deze minimaal al één keer plaatsgevonden en MOETEN de hoog en middel risico bevindingen op externe MedMij koppelvlakken zijn opgelost.</p> <p>Voor penetratietesten die worden uitgevoerd <b>na toetreding</b>, dient een adequaat actieplan opgesteld te worden voor minimaal de hoge en midden risico's ten aanzien van de MedMij dienstverlening. Dit actieplan wordt gedeeld met de beheerorganisatie. De corrigerende maatregelen worden tijdig doorgevoerd.</p>
A.18.2.3 (2) Beoordeling van technische naleving			✓	<p>Tenminste jaarlijks MOET een blackbox infrastructuur penetratietesten worden uitgevoerd op de externe koppelvlakken van de deelnemers ten behoeve van het MedMij stelsel. Naar aanleiding van het resultaat wordt een</p>

adequaate actieplan opgesteld voor minimaal de hoge en midden risico's ten aanzien van de MedMij dienstverlening.

A. 5.1.1 Beleidsregels voor informatiebeveiliging	✓	✓	✓	De beleidsdocumenten MOETEN de beleidsmaatregelen die van toepassing zijn op MedMij (onder andere gespecificeerd in <a href="#">Privacy- en informatiebeveiligingsbeleid</a> ) specifiek benoemen.
A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging	✓	✓	✓	<p>De (eind)verantwoordelijkheid voor informatiebeveiliging MOET belegd zijn. Deze functionaris(sen) dient/dienen mandaat te hebben om bij (een dreiging van) een crisis spoedbesluiten te nemen ten aanzien van MedMij en deze besluiten met spoed te kunnen (laten) realiseren.</p> <p>De verantwoordelijke en operationele functionaris (sen) (inclusief eventuele onderaannemers) dient/ dienen hiervoor tijdens kantooruren binnen een uur beschikbaar te zijn en buiten kantooruren binnen drie uur.</p>
A. 7.2.2 (1) Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	✓	✓	✓	De verantwoordelijke functionaris(sen) zoals benoemd in <a href="#">A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging</a> MOET(EN) deelgenomen hebben aan de training over de algemene werking van het stelsel.
A. 7.2.2 (2) Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	✓	✓	✓	Overige medewerkers die werkzaamheden verrichten gerelateerd aan MedMij MOETEN een training hebben gevolgd over de algemene werking van het stelsel en op de voor hem/haar van toepassing zijnde beveiligingsmaatregelen.
A. 8.2.1 Classificatie van informatie	✓	✓	✓	De gegevens die binnen het stelsel worden verwerkt MOETEN worden behandeld conform het Informatieclassificatiebeleid (van MedMij).
A. 9.1.1 Beleid voor toegangsbeveiliging	✓	✓	✓	<p>Er MOETEN technische en organisatorische maatregelen worden genomen om inzage van persoonlijke gezondheidsgegevens door medewerkers te voorkomen. De organisatie dient minimaal elk halfjaar en na grote wijzigingen een self-assessment uit te voeren om vast te stellen dat deze maatregelen nog effectief zijn.</p> <p>In (zeer) uitzonderlijke gevallen is inzage in persoonlijke gezondheidsgegevens niet te voorkomen. Hiervoor dient de organisatie een (nood)procedure te documenteren. Deze procedure dient in te gaan op:</p>

- Functiescheiding tussen vragen van toestemming voor inzage en het geven van toestemming door een verantwoordelijke functionaris;
- Randvoorwaarden en maatregelen met als doel dat inzage plaatsvindt op een gecontroleerde en zo beperkt mogelijke (in tijd en hoeveelheid gegevens) wijze;
- Borging dat de deelnemer voldoet wordt aan wet- en regelgeving (AVG, Meldplicht Datalekken) en de geldende versie van het MedMij Afsprakenstelsel;
- Vastlegging en verantwoording van de getroffen acties.

#### A. 9.2.5 Beoordeling van toegangsrechten van gebruikers



1. Toegangsrechten die zijn verstrekt op IT-componenten waar persoonlijke gezondheidsgegevens worden worden verwerkt MOETEN ten minste maandelijks worden gecontroleerd.
2. Hierbij MOET functiescheiding gewaarborgd zijn.
3. Dit geldt ook voor eventuele onderaannemers.
4. Tijdens deze controle moet aandacht zijn voor medewerkers die geen gebruik (meer) maken van de toegangsrechten (met aantoonbare opvolging).

#### A. 9.4.1 Beperking toegang tot informatie



Authenticatie van personen (eindgebruikers) MOET plaatsvinden op basis van minimaal twee factoren. Na succesvolle authenticatie krijgen personen alleen toegang tot hun eigen persoonlijke gezondheidsgegevens.

#### Wijzigingen ten opzichte van release 1.1.1

Alle normen zijn tekstueel in lijn gebracht. Hierbij is het werkwoord "dienen" vervangen door "moeten", conform [RFC 2119](#). De verwijzing naar de *Deelnemer*-rol is uit de tekst gehaald; waar nodig wordt deze vervangen door de term "organisatie". Waar mogelijk zijn normen gesplitst per juridische rol: DVP, DVZA of BO.

De afzonderlijke normen zijn als volgt aangepast.

- A.5.1.1 is ook van toepassing geworden op de BO;
- A.7.2.2:
  - is gesplitst in twee normen;
  - is verduidelijkt om aan te geven om welke contactpersonen het hier gaat;
- A.9.2.5:
  - is gesplitst in aparte normen;

- is aangepast zodat de eis voor twee-factor-authenticatie is komen te vervallen, omdat de doelstelling van deze eis al wordt ingevuld door A.9.1.1 en de eis zelf in A.9.4.1 is opgenomen;
- is aangepast zodat de eis omtrent logging is verplaatst naar A.12.4.3;
- A.12.1.2 is gesplitst in twee aparte normen;
- A.12.1.3 is gesplitst in twee normen, voor elke rol één;
- A.12.3.1:
  - is niet meer van toepassing op de rol DVZA;
  - mag nu worden uitgesloten in bepaalde gevallen;
- A.12.4.1 is niet meer van toepassing op de rol BO;
- A.12.4.3 is toegevoegd, ten gevolge van de splitsing van A.9.2.5;
- A.12.4.4 is verduidelijkt; het is nu ook toegestaan met een andere NTP te synchroniseren;
- A.12.5.1 is ondergebracht in A.12.1.2 en als aparte norm verwijderd;
- A.12.6.1 is verduidelijkt; het gaat alleen om het melden van kwetsbaarheden in de eigen omgeving;
- A.14.2.1:
  - is verduidelijkt: de deelnemer hoeft deze maatregelen slechts in overweging te nemen;
  - is ontdaan van de nuancering inzake mobiele apps;
- A.15.1.2 is toegevoegd;
- A.15.2.1 is toegevoegd;
- A.16.1.3 is aangevuld: de DVZA maakt hierover zo nodig afspraken met zijn *Zorgaanbieders*;
- A.16.1.7 is aangevuld: de DVZA maakt hierover zo nodig afspraken met zijn *Zorgaanbieders*;
- A.18.2.3 is:
  - gesplitst in twee normen, per rol;
  - uitgebreid met een toelichting.

Verder:

- is het toetsingskader rechtstreeks opgenomen in het MedMij Afsprakenstelsel, zodat deze informatie toegankelijker is;
- wordt de aanvullende auditverklaring automatisch gegenereerd door Confluence, zodat deze altijd consistent blijft met het normenkader.

Hierdoor is de tabel met verwijzingen naar Word-documenten komen te vervallen.



## A. 5.1.1 Beleidsregels voor informatiebeveiliging

### Norm

<b>Rationale</b>	Deze maatregel borgt dat het Afsprakenstelsel wordt toegepast in beleid en maatregelen bij de deelnemers.
<b>Implementatie</b>	De beleidsdocumenten MOETEN de beleidsmaatregelen die van toepassing zijn op MedMij (onder andere gespecificeerd in <a href="#">Privacy- en informatiebeveiligingsbeleid</a> ) specifiek benoemen.
<b>NEN 7510-1: 2017</b>	A.5.1.1 Beleidsregels voor informatiebeveiliging
<b>NEN 7510: 2011</b>	A.5.1.1 Beleidsdocument voor informatiebeveiliging

### Beoordeling

<b>Auditmethode</b>	<ul style="list-style-type: none"> <li>• Stel vast dat in de beleidsdocumenten het privacy en informatiebeveiligingsbeleid van MedMij specifiek is opgenomen.</li> <li>• Stel vast dat dit beleid is uitgewerkt in maatregelen.</li> <li>• Stel minimaal door middel van interviews met de betrokken medewerkers vast of de maatregelen worden toegepast. Dit geldt ook voor eventuele onderaannemers.</li> </ul>
<b>Verificatie</b>	<ul style="list-style-type: none"> <li>• Welke beleidsdocumenten (incl. versienummer) zijn onderzocht.</li> <li>• Welke documenten zijn onderzocht die de maatregelen beschrijven.</li> <li>• Met wie gesproken is ter bevestiging van toepassing van de maatregelen.</li> </ul>

### Rollen

DVP	✓
DVZA	✓
BO	✓

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

## A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging

### Norm

<b>Rationale</b>	Deze maatregel borgt dat bij (dreiging van) calamiteiten door alle partijen daadkrachtig kan worden gereageerd. Zie ook <a href="#">A.12.4.1 Gebeurtenissen registreren</a> en <a href="#">A.16.1.1 Verantwoordelijkheden en procedures</a> .
<b>Implementatie</b>	<p>De (eind)verantwoordelijkheid voor informatiebeveiliging MOET belegd zijn. Deze functionaris(sen) dient/dienen mandaat te hebben om bij (een dreiging van) een crisis spoedbesluiten te nemen ten aanzien van MedMij en deze besluiten met spoed te kunnen (laten) realiseren.</p> <p>De verantwoordelijke en operationele functionaris(sen) (inclusief eventuele onderaannemers) dient/ dienen hiervoor tijdens kantooruren binnen een uur beschikbaar te zijn en buiten kantooruren binnen drie uur.</p>
<b>Toelichting</b>	Conform de betreffende <a href="#">Deelnemersovereenkomsten</a> .
<b>NEN 7510-1: 2017</b>	A.6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging
<b>NEN 7510: 2011</b>	<p>A.6.1.3 Toewijzing van verantwoordelijkheden voor informatiebeveiliging</p> <p>A.8.1.1 Rollen en verantwoordelijkheden</p>

### Beoordeling

<b>Auditmethode</b>	<ul style="list-style-type: none"> <li>• Stel op basis van evidence vast dat de genoemde functionaris(sen) is/zijn aangewezen.</li> <li>• Stel vast dat een procedure is ingericht zodat de genoemde beschikbaarheid, tijdens kantooruren binnen een uur en buiten kantooruren binnen drie uur, te allen tijde gegarandeerd is op dit onderwerp. Indien van toepassing dient deze procedure onderaannemers te omvatten.</li> <li>• De beschikbaarheid dient tevens gegarandeerd te zijn bij geplande en ongeplande afwezigheid.</li> <li>• Stel door middel van interviews vast dat de functionaris(sen) op de hoogte is/zijn van hun taken en verantwoordelijkheden t.a.v. de beschikbaarheid en het juiste mandaat hebben.</li> </ul>
<b>Verificatie</b>	<ul style="list-style-type: none"> <li>• In welke documentatie de verantwoordelijkheden en bevoegdheden zijn belegd.</li> <li>• Welke procedure (incl. versienummer) is ingezien m.b.t. de beschikbaarheid.</li> <li>• Met wie gesproken is ter bevestiging van de implementatie.</li> </ul>

### Rollen



DVP	✓
DVZA	✓
BO	✓

*DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie*

## A. 7.2.2 (1) Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

### Norm

<b>Rationale</b>	Deze maatregel borgt dat medewerkers zich bewust zijn van de werking van MedMij en de ketenverantwoordelijkheden.
<b>Implementatie</b>	De verantwoordelijke functionaris(sen) zoals benoemd in <a href="#">A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging</a> MOET(EN) deelgenomen hebben aan de training over de algemene werking van het stelsel.
<b>Toelichting</b>	Deze training wordt door de beheerorganisatie beheerd en gefaciliteerd.
<b>NEN 7510-1: 2017</b>	A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
<b>NEN 7510: 2011</b>	A.8.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

### Beoordeling

<b>Auditmethode</b>	Verkrijg een overzicht van verantwoordelijke functionarissen en stel op basis van het bewijs van deelname vast dat alle personen de training gegeven door de beheerorganisatie hebben gevolgd.
<b>Verificatie</b>	<ul style="list-style-type: none"> <li>• Het overzicht van contactpersonen.</li> <li>• Evidence m.b.t. de gevolgde training.</li> </ul>

### Rollen

DVP	✓
DVZA	✓
BO	✓

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

## A. 7.2.2 (2) Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

### Norm

<b>Rationale</b>	Deze maatregel borgt dat medewerkers zich bewust zijn van de werking van MedMij en de ketenverantwoordelijkheden.
<b>Implementatie</b>	Overige medewerkers die werkzaamheden verrichten gerelateerd aan MedMij MOETEN een training hebben gevolgd over de algemene werking van het stelsel en op de voor hem/haar van toepassing zijnde beveiligingsmaatregelen.
<b>Toelichting</b>	<ol style="list-style-type: none"> <li>1. Deze training mag door de deelnemer zelf beheerd en gefaciliteerd worden;</li> <li>2. Deze norm mag ook ingevuld worden doordat de medewerkers deelnemen aan de training gegeven door de beheerorganisatie.</li> </ol>
<b>Toetsing</b>	Stel vast dat de partij maatregelen heeft getroffen die borgen dat relevante medewerkers over de noodzakelijke kennis beschikken.
<b>NEN 7510: 2017</b>	A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
<b>NEN 7510: 2011</b>	A.8.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

### Beoordeling

<b>Auditmethode</b>	<ul style="list-style-type: none"> <li>• Verkrijg een overzicht van alle overige medewerkers die betrokken zijn bij MedMij gerelateerde werkzaamheden. Stel op basis van het bewijs van deelname vast dat deze personen ofwel de training hebben gevolgd die wordt gegeven door de beheerorganisatie, ofwel een training hebben gevolgd gegeven door de contactpersoon.</li> <li>• Stel vast dat de training gegeven door de contactpersoon de volgende aspecten voldoende behandelt: de werking van MedMij, de ketenverantwoordelijkheden en de voor de medewerker van toepassing zijnde beveiligingsmaatregelen.</li> </ul>
<b>Verificatie</b>	<ul style="list-style-type: none"> <li>• Het overzicht van overige medewerkers.</li> <li>• Evidence m.b.t. de gevolgde training.</li> </ul>

### Rollen

DVP	✓
DVZA	✓
BO	✓

*DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie*

## A. 8.2.1 Classificatie van informatie

### Norm

<b>Rationale</b>	Deze maatregel borgt dat informatie die binnen het stelsel wordt gebruikt, door deelnemers met dezelfde voorzichtigheid wordt behandeld.
<b>Implementatie</b>	De gegevens die binnen het stelsel worden verwerkt MOETEN worden behandeld conform het Informatieclassificatiebeleid (van MedMij).
<b>Toetsing</b>	Door middel van interviews en/of het tonen van evidence (zoals het informatieclassificatieschema of -beleid van de partij).
<b>NEN 7510-1: 2017</b>	A.8.2.1 Classificatie van informatie
<b>NEN 7510: 2011</b>	A.7.2.1 Richtlijnen voor classificatie

### Beoordeling

<b>Auditmethode</b>	<ul style="list-style-type: none"> <li>• Stel vast dat de classificatie van gegevens binnen de organisatie, voor de gegevens die binnen het stelsel worden uitgewisseld, overeenstemt met de classificatie zoals door MedMij benoemd in het Informatieclassificatiebeleid van MedMij</li> <li>• Stel vast dat de verwerking van de gegevens door de deelnemer daadwerkelijk plaatsvindt conform het Informatieclassificatiebeleid van MedMij. Hierbij ligt de focus op: gezondheidsgegevens, metagegevens, operationele gegevens, risicoanalyses, pentestrapporten en de whitelist. Dit geldt ook voor eventuele onderaannemers.</li> </ul>
<b>Verificatie</b>	Welk document (incl. versienummer) is ingezien.

### Rollen

DVP	✓
DVZA	✓
BO	✓

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

## A. 9.1.1 Beleid voor toegangsbeveiliging

### Norm

<b>Rationale</b>	Deze maatregel borgt dat persoonlijke gezondheidsgegevens alleen toegankelijk zijn voor de zorgaanbieder en de zorggebruiker (zie ook <a href="#">A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen</a> ).
<b>Implementatie</b>	<p>Er MOETEN technische en organisatorische maatregelen worden genomen om inzage van persoonlijke gezondheidsgegevens door medewerkers te voorkomen. De organisatie dient minimaal elk halfjaar en na grote wijzigingen een self-assessment uit te voeren om vast te stellen dat deze maatregelen nog effectief zijn.</p> <p>In (zeer) uitzonderlijke gevallen is inzage in persoonlijke gezondheidsgegevens niet te voorkomen. Hiervoor dient de organisatie een (nood)procedure te documenteren. Deze procedure dient in te gaan op:</p> <ul style="list-style-type: none"> <li>• Functiescheiding tussen vragen van toestemming voor inzage en het geven van toestemming door een verantwoordelijke functionaris;</li> <li>• Randvoorwaarden en maatregelen met als doel dat inzage plaatsvindt op een gecontroleerde en zo beperkt mogelijke (in tijd en hoeveelheid gegevens) wijze;</li> <li>• Borging dat de deelnemer voldoet wordt aan wet- en regelgeving (AVG, Meldplicht Datalekken) en de geldende versie van het MedMij Afsprakenstelsel;</li> <li>• Vastlegging en verantwoording van de getroffen acties.</li> </ul>
<b>NEN 7510: 2017</b>	A.9.1.1 Beleid voor toegangsbeveiliging
<b>NEN 7510: 2011</b>	A.11.1.1 Toegangsbeleid

### Beoordeling

<b>Auditmethode</b>	<ul style="list-style-type: none"> <li>• Stel vast dat het technisch onmogelijk is gemaakt dat (medewerkers van) partijen zich inzage kunnen verschaffen in persoonlijke gezondheidsgegevens. Dit geldt ook voor eventuele onderaannemers</li> <li>• Stel vast dat self assessment minimaal elk halfjaar en na grote wijzigingen is uitgevoerd.</li> <li>• Stel vast dat de (nood)procedure is opgesteld en effectief is (m.a.w. geen toegang is verkregen zonder toepassing van de procedure).</li> <li>• Indien inzage heeft plaatsgevonden: Controleer de vastlegging en verantwoording</li> </ul>
<b>Verificatie</b>	Welke documenten (incl. versienummers) zijn ingezien.

### Rollen

DVP	✓
DVZA	✓
BO	✓



*DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie*

## A. 9.2.5 Beoordeling van toegangsrechten van gebruikers

### Norm

<b>Rationale</b>	Deze maatregel borgt dat partijen regelmatig controleren of alleen gerechtigde gebruikers toegang hebben tot relevante IT-componenten (waaronder servers, databases en netwerkinfrastructuur).
<b>Implementatie</b>	<ol style="list-style-type: none"> <li>1. Toegangsrechten die zijn verstrekt op IT-componenten waar persoonlijke gezondheidsgegevens worden verwerkt MOETEN ten minste maandelijks worden gecontroleerd.</li> <li>2. Hierbij MOET functiescheiding gewaarborgd zijn.</li> <li>3. Dit geldt ook voor eventuele onderaannemers.</li> <li>4. Tijdens deze controle moet aandacht zijn voor medewerkers die geen gebruik (meer) maken van de toegangsrechten (met aantoonbare opvolging).</li> </ol>
<b>NEN 7510: 2017</b>	A.9.2.5 Beoordeling van toegangsrechten van gebruikers
<b>NEN 7510: 2011</b>	A.11.2.4 Beoordeling van toegangsrechten van gebruikers

### Beoordeling

<b>Auditmethode</b>	<ul style="list-style-type: none"> <li>• Stel op basis van de procedures vast dat toegangsrechten op servers, databases en netwerkinfrastructuur waar persoonlijke gezondheidsgegevens worden opgeslagen of worden verwerkt maandelijks gecontroleerd worden. Dit geldt ook voor eventuele onderaannemers.</li> <li>• Stel vast dat de functionaris(sen) die deze controle uitvoert/uitvoeren geen toegangsrechten verstrekken en/of zelf (beheer)toegang hebben tot de IT-componenten.</li> <li>• De controle van toegangsrechten mag ook geautomatiseerd plaatsvinden. Stel dan vast dat configureren van de geautomatiseerde controle(s) juist en volledig plaatsvindt</li> </ul>
<b>Verificatie</b>	Welke procedures (incl. versienummers) zijn ingezien.

### Rollen

DVP	✓
DVZA	✓
BO	✓

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

## A. 9.4.1 Beperking toegang tot informatie

### Norm

<b>Rationale</b>	Deze maatregel borgt dat authenticatie van personen en autorisatie tot hun persoonlijke gegevens betrouwbaar plaatsvindt.
<b>Implementatie</b>	Authenticatie van personen (eindgebruikers) MOET plaatsvinden op basis van minimaal twee factoren. Na succesvolle authenticatie krijgen personen alleen toegang tot hun eigen persoonlijke gezondheidsgegevens.
<b>NEN 7510: 2017</b>	A.9.4.1 Beperking toegang tot informatie
<b>NEN 7510: 2011</b>	A.11.5.2 Gebruikersidentificatie en -authenticatie

### Beoordeling

<b>Auditmethode</b>	<ul style="list-style-type: none"> <li>• Stel vast dat (minimaal) twee-factorauthenticatie van personen technisch afgedwongen wordt</li> <li>• Stel vast dat voldoende maatregelen zijn ingericht die waarborgen dat na succesvolle authenticatie de personen alleen toegang krijgen tot hun eigen persoonlijke gezondheidsgegevens. Ondersteunende evidence omvat bijvoorbeeld gedocumenteerde use-cases of het uitvoeren van een 'walk through' vanuit het perspectief van de eindgebruiker</li> </ul> <p>Ten aanzien van de in het eerste punt bedoelde twee factoren gelden de volgende twee richtlijnen.</p> <p>Ten eerste moeten de factoren uit verschillende van de volgende categorieën gebruikt worden.</p> <ul style="list-style-type: none"> <li>• drie categorieën van zogenoemde "authenticatiefactoren": factoren waarvan is bevestigd dat deze gebonden zijn aan een persoon. <ul style="list-style-type: none"> <li>• op <b>bezit</b> gebaseerde authenticatiefactoren: authenticatiefactoren waarvan de betrokkene moet aantonen dat deze in zijn bezit is;</li> <li>• op <b>kennis</b> gebaseerde authenticatiefactoren: authenticatiefactoren waarvan de betrokkene moet aantonen dat hij ervan kennis draagt;</li> <li>• <b>inherente</b> authenticatiefactoren: authenticatiefactoren die op een fysiek kenmerk van een natuurlijke persoon is gebaseerd en waarbij de betrokkene moet aantonen dat hij dat fysieke kenmerk bezit;</li> </ul> </li> <li>• dynamische authenticatie: een elektronisch proces, dat met gebruikmaking van cryptografie of een andere techniek de middelen biedt om op verzoek een elektronisch bewijs op te maken dat de betrokkene de controle heeft over of in het bezit is van de identificatiegegevens, en dat verandert telkens als authenticatie plaatsvindt tussen de betrokkene en het systeem dat diens identiteit verifieert;</li> </ul> <div style="border: 1px solid #ccc; padding: 10px; margin-top: 10px;"> <p><b>Twee factoren</b></p> <p>Bijvoorbeeld, wanneer er tijdens het inloggen zowel een TouchID als een FaceID gebruikt wordt, dan is er geen sprake van two-factor, omdat het beide inherente authenticatiefactoren zijn.</p> </div>
---------------------	---

Ten tweede moet het gebruik van beide factoren tijdens het inloggen achter elkaar plaatsvinden en in het inlog-proces onlosmakelijk aan elkaar verbonden zijn.

### Twee factoren

Bijvoorbeeld, wanneer FaceID gebruikt wordt om met de iCloud password manager een wachtwoord in te voeren is er geen sprake van twee-factorauthenticatie, omdat het wachtwoord ook handmatig ingevoerd kan worden.

Deze tabel toont voorbeelden van veelgebruikte authenticatiefactoren.

categorie	factor	beschrijving
bezit	kaart of pas	Bij de authenticatie is een fysieke, losse kaart betrokken bijvoorbeeld een bankkaart.
	SMS	Als onderdeel van de authenticatie wordt een dynamische SMS-code gecontroleerd. De SMS-code is voldoende lang en steeds een andere.
	push notifications	Als onderdeel van de authenticatie wordt er een melding ontvangen op de telefoon. De gebruiker bevestigt de melding.
	keychain	Deze controle is niet zichtbaar voor de gebruiker. Op de mobiele telefoon wordt een secure enclave of keychain gebruikt om bezit van de telefoon aan te tonen.
kennis	pincode	Als onderdeel van de authenticatie wordt een pincode ingevoerd. Een pincode is altijd verbonden aan een kaart of een app (licatie). Na een beperkt aantal foutpogingen wordt de kaart of app geblokkeerd.
	wachtwoord	Als onderdeel van de authenticatie wordt een wachtwoord ingevoerd. Voor de eisen aan het wachtwoord, de levensduur en het toegestane aantal foutpogingen is wachtwoordbeleid aanwezig.
inherent	vingerafdruk	Als onderdeel van de authenticatie wordt een vingerafdruk gecontroleerd, zoals TouchID.
	gezichtsherkenning	Als onderdeel van de authenticatie wordt het gezicht gecontroleerd, zoals FaceID.
	irisscan	Als onderdeel van de authenticatie wordt het oog gecontroleerd.

**Verificatie** Welke documenten (incl. versienummers) zijn ingezien.

## Rollen

DVP	<input checked="" type="checkbox"/>
DVZA	<input type="checkbox"/>
BO	<input type="checkbox"/>

*DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie*

## A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen

### Norm

<b>Rationale</b>	Deze maatregel borgt dat bij het versleutelen van persoonlijke gezondheidsgegevens gebruik wordt gemaakt van als veilig aangemerkte algoritmen.
<b>Implementatie</b>	Opgeslagen persoonlijke gezondheidsgegevens MOETEN beschermd worden door middel van disk-level en/of database-level encryptie. Hiervoor wordt verwezen naar de aanbevelingen die gelden voor 'near term protection' en 'long-term protection' in de ECRYPT-CSA aanbevelingen, zie hieronder.
<b>Toelichting</b>	<ol style="list-style-type: none"> <li>1. Deze maatregel mag uitgesloten worden indien DVZA onder zijn verantwoording geen persoonlijke gezondheidsgegevens opslaat.</li> <li>2. Een overzicht van publicaties is te vinden op <a href="https://www.keylength.com/">https://www.keylength.com/</a></li> <li>3. Er kan gebruik gemaakt worden van de ECRYPT-CSA aanbevelingen en/of die van het BSI</li> </ol>
<b>NEN 7510: 2017</b>	A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen
<b>NEN 7510: 2011</b>	A.12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen

### Beoordeling

<b>Auditmethode</b>	<ul style="list-style-type: none"> <li>• Stel op basis van de architectuurdiagrammen vast of er wordt voldaan aan de aanbevelingen die gelden voor 'near term protection' en 'long-term protection' volgens de ECRYPT-CSA aanbevelingen.</li> <li>• Stel op basis van een steekproef vast of aanbevelingen ook daadwerkelijk geïmplementeerd zijn.</li> </ul>
<b>Verificatie</b>	<ul style="list-style-type: none"> <li>• Welke versie van de aanbevelingen is gehanteerd.</li> <li>• Welke versie van de architectuurdiagrammen zijn ingezien.</li> <li>• Evidence m.b.t. de daadwerkelijke implementatie.</li> </ul>

### Rollen

DVP	✓
DVZA	✓
BO	

*DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie*

## A.12.1.2 (1) Wijzigingsbeheer

### Norm

<b>Rationale</b>	Deze maatregel borgt dat wijzigingen binnen de keten beheerst verlopen.
<b>Implementatie</b>	De IT-beheerprocessen MOETEN aansluiten op het MedMij Change- en releasebeleid.
<b>NEN 7510-1:2017</b>	A.12.1.2 Wijzigingsbeheer
<b>NEN 7510:2011</b>	A.10.1.2 Wijzigingsbeheer

### Beoordeling

<b>Auditmethode</b>	<ul style="list-style-type: none"> <li>• Stel vast dat IT-beheerprocessen van de organisatie aansluiten op het Change- en releasebeleid van MedMij.</li> <li>• Stel op basis van een steekproef vast dat de IT-beheerprocessen voor MedMij juist worden uitgevoerd.</li> </ul>
<b>Verificatie</b>	<ul style="list-style-type: none"> <li>• Welke procedures (incl. versienummers) zijn ingezien.</li> <li>• Evidence m.b.t. de daadwerkelijke implementatie.</li> </ul>

### Rollen

DVP	✓
DVZA	✓
BO	✓

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie



## A.12.1.2 (2) Wijzigingsbeheer

### Norm

<b>Rationale</b>	Deze maatregel borgt dat er altijd twee medewerkers betrokken zijn bij werkzaamheden aan systemen (configuratiewijzigingen, onderhoud, installatie van updates) die direct impact (kunnen) hebben op de beschikbaarheid, integriteit of vertrouwelijkheid van de keten. De maatregel vermindert het risico op onbeschikbaarheid van of kwetsbaarheden binnen de keten.
<b>Implementatie</b>	Niet-standaard wijzigingen op de IT componenten die gebruikt worden binnen de scope van MedMij MOETEN op basis van het vier-ogen-principe worden uitgevoerd.
<b>Toelichting</b>	Het gaat hier niet om achterliggende systemen (zoals EPD) maar om de aansluitende systemen en netwerkcomponenten (zoals firewalls).
<b>NEN 7510-1: 2017</b>	A.12.1.2 Wijzigingsbeheer
<b>NEN 7510: 2011</b>	A.10.1.2 Wijzigingsbeheer

### Beoordeling

<b>Auditmethode</b>	<ul style="list-style-type: none"> <li>• Stel vast dat een overzicht van standaard en niet-standaard wijzigingen is gedocumenteerd. Ga na of standaardwijzigingen geen midden/hoog risico hebben op de beschikbaarheid, integriteit of vertrouwelijkheid van de keten.</li> <li>• Stel vast dat vier-ogen-principe is ingericht voor niet-standaard wijzigingen.</li> <li>• Stel door middel van interview met de betrokken medewerkers vast of de procedures worden nageleefd.</li> </ul>
<b>Verificatie</b>	<ul style="list-style-type: none"> <li>• Welke procedures (incl. versienummers) zijn ingezien.</li> <li>• Met wie gesproken is ter bevestiging van de implementatie.</li> </ul>

### Rollen

DVP	✓
DVZA	✓
BO	✓

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

## A.12.1.2 (3) Wijzigingsbeheer

### Norm

<b>Rationale</b>	Deze maatregel borgt dat wijzigingen binnen de keten beheerst verlopen.
<b>Implementatie</b>	Indien er wijzigingen plaatsvinden die mogelijk significante impact hebben op de informatiebeveiliging, MOET de penetratietest zoals benoemd in <a href="#">A.18.2.3 (1) Beoordeling van technische naleving</a> voor deze componenten opnieuw uitgevoerd worden.
<b>NEN 7510-1: 2017</b>	A.12.1.2 Wijzigingsbeheer
<b>NEN 7510: 2011</b>	A.10.1.2 Wijzigingsbeheer

### Beoordeling

<b>Auditmethode</b>	Zie <a href="#">A.18.2.3 (1) Beoordeling van technische naleving</a>
<b>Verificatie</b>	Zie <a href="#">A.18.2.3 (1) Beoordeling van technische naleving</a>

### Rollen

DVP	✓
DVZA	✓
BO	✓

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

## A.12.1.3 (1) Capaciteitsbeheer

### Norm

<b>Rationale</b>	Deze maatregel borgt dat alle systemen in de keten voldoen aan de afgesproken eisen omtrent beschikbaarheid.
<b>Implementatie</b>	Maatregelen MOETEN zijn gedocumenteerd en geïmplementeerd om te (kunnen) voldoen aan de beschikbaarheidseisen zoals vastgelegd in <a href="#">Token interface</a> en <a href="#">Resource interface</a> .
<b>NEN 7510-1: 2017</b>	A.12.1.3 Capaciteitsbeheer
<b>NEN 7510: 2011</b>	A.10.3.1 Capaciteitsbeheer

### Beoordeling

<b>Auditmethode</b>	Stel op basis van IT-monitoring en/of service level rapportages vast dat over een periode van drie maanden voorafgaand aan de auditdatum voldaan is aan de beschikbaarheidseisen.
<b>Verificatie</b>	Evidence m.b.t. de rapportages.

### Rollen

DVP	✓
DVZA	✓
BO	

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

## A.12.1.3 (2) Capaciteitsbeheer

### Norm

<b>Rationale</b>	Deze maatregel borgt dat alle systemen in de keten voldoen aan de afgesproken eisen omtrent beschikbaarheid.
<b>Implementatie</b>	Maatregelen MOETEN zijn gedocumenteerd en geïmplementeerd om te (kunnen) voldoen aan de beschikbaarheidseisen zoals vastgelegd in <a href="#">GNL</a> -, <a href="#">OCL</a> - en <a href="#">ZAL</a> -interface.
<b>NEN 7510-1: 2017</b>	A.12.1.3 Capaciteitsbeheer
<b>NEN 7510: 2011</b>	A.10.3.1 Capaciteitsbeheer

### Beoordeling

<b>Auditmethode</b>	Stel op basis van IT-monitoring en/of service level rapportages vast dat over een periode van drie maanden voorafgaand aan de auditdatum voldaan is aan de beschikbaarheidseisen.
<b>Verificatie</b>	Evidence m.b.t. de rapportages.

### Rollen

DVP	<input type="checkbox"/>
DVZA	<input type="checkbox"/>
BO	<input checked="" type="checkbox"/>

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

## A.12.3.1 Back-up van informatie

### Norm

<b>Rationale</b>	Deze maatregel borgt dat deelnemers beschikken over een bruikbare back-up.
<b>Implementatie</b>	Er MOETEN maatregelen zijn geïmplementeerd waardoor het gegevensverlies van persoonlijke gezondheidsinformatie maximaal 24 uur bedraagt. Daarnaast moet een herstelprocedure zijn ingericht waardoor de gegevens van een persoon binnen 24 uur terug kunnen worden geplaatst in geval van een incident. Deze herstelprocedure wordt minimaal jaarlijks getest.
<b>Toelichting</b>	Deze maatregel MAG worden uitgesloten door een DVP indien de persoonlijke gezondheidsinformatie niet centraal wordt opgeslagen.
<b>NEN 7510-1: 2017</b>	A.12.3.1 Back-up van informatie
<b>NEN 7510: 2011</b>	A.10.5.1 Reservekopieën (back-ups)

### Beoordeling

<b>Auditmethode</b>	<ul style="list-style-type: none"> <li>• Stel vast dat de organisatie maatregelen heeft ingericht waardoor gegevensverlies is beperkt tot maximaal 24 uur. Dit zijn bijvoorbeeld back-ups en/of heet repliceren van gegevens.</li> <li>• Stel vast dat de herstelprocedure binnen 24u uitgevoerd kan worden en minimaal jaarlijks wordt getest.</li> <li>• Stel daarnaast via monitoring en rapportages vast dat de leverancier voldoet</li> </ul>
<b>Verificatie</b>	<ul style="list-style-type: none"> <li>• Welke procedures (incl. versienummers) zijn ingezien.</li> <li>• Evidence m.b.t. de (minimaal) jaarlijkse test.</li> </ul>

### Rollen

DVP	<input checked="" type="checkbox"/>
DVZA	<input type="checkbox"/>
BO	<input type="checkbox"/>

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

## A.12.4.1 Gebeurtenissen registreren

### Norm

<b>Rationale</b>	Deze maatregel borgt dat relevante security gebeurtenissen in systemen van de deelnemers en de beheerorganisatie (zoals het verlenen van toestemming aan zorgaanbieder door de zorggebruiker, het inzien of wijzigen van een PGO of het wijzigen aan loggen van gebruikers aan hun PGO) ten minste 12 maanden inzichtelijk blijven.
<b>Implementatie</b>	<p>Logging MOET plaatsvinden zoals gespecificeerd in het afsprakenstelsel (zie <a href="#">Processen en informatie</a> onder Logging)</p> <p>Daarnaast MOETEN de volgende acties ten minste 12 maanden onweerlegbaar en controleerbaar worden gelogd:</p> <ul style="list-style-type: none"> <li>• De actie waarbij de persoon via de DVP bij de DVZA gegevens wil opvragen</li> <li>• De acties waarbij de persoon toestemming geeft voor de uitwisseling conform de specificaties in het afsprakenstelsel (indien uitgevoerd onder verantwoordelijkheid van de DVZA)</li> </ul>
<b>NEN 7510-1: 2017</b>	A.12.4.1 Gebeurtenissen registreren
<b>NEN 7510: 2011</b>	<p>A.10.10.1 Aanmaken audit-logbestanden</p> <p>A.10.10.2 Controle van systeemgebruik</p>

### Beoordeling

<b>Auditmethode</b>	<ul style="list-style-type: none"> <li>• Stel vast of de logbestanden voldoen aan de voorwaarden van het afsprakenstelsel (zie <a href="#">Processen en informatie</a> onder Logging).</li> <li>• Stel vast hoe de onweerlegbaarheid en controleerbaarheid van de logs over personen is ingericht. Stel vast dat deze altijd minimaal 12 maanden beschikbaar blijven.</li> </ul>
<b>Verificatie</b>	<ul style="list-style-type: none"> <li>• Evidence m.b.t. de logbestanden.</li> <li>• Evidence m.b.t. aansluiting.</li> </ul>

### Rollen

DVP	✓
DVZA	✓
BO	

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

## A.12.4.3 Logbestanden van beheerders en operators

### Norm

<b>Rationale</b>	Deze maatregel borgt dat partijen regelmatig controleren of alleen gerechtigde gebruikers toegang hebben tot relevante IT-componenten (waaronder servers, databases en netwerkinfrastructuur).
<b>Implementatie</b>	<ol style="list-style-type: none"> <li>1. Het gebruik van toegangsrechten op IT-componenten waar persoonlijke gezondheidsgegevens worden verwerkt MOET worden gelogd;</li> <li>2. Deze logging MOET ten minste maandelijks worden gecontroleerd. Dit geldt ook voor eventuele onderaannemers;</li> <li>3. Hierbij MOET functiescheiding gewaarborgd zijn;</li> <li>4. Tijdens deze controle moet aandacht zijn voor onterecht/onnodig gebruik door medewerkers (met aantoonbare opvolging).</li> </ol>
<b>NEN 7510-1: 2017</b>	A.9.2.5 Beoordeling van toegangsrechten van gebruikers
<b>NEN 7510: 2011</b>	A.11.2.4 Beoordeling van toegangsrechten van gebruikers

### Beoordeling

<b>Auditmethode</b>	<ul style="list-style-type: none"> <li>• Stel op basis van de procedures vast dat de logging van servers, databases en netwerkinfrastructuur waar persoonlijke gezondheidsgegevens worden opgeslagen of worden verwerkt maandelijks gecontroleerd worden.</li> <li>• Stel vast dat de functionaris(sen) die deze controle uitvoert/uitvoeren geen toegangsrechten verstrekken en/of zelf (beheer)toegang hebben tot de IT-componenten.</li> <li>• De controle van logging mag ook geautomatiseerd plaatsvinden. Stel dan vast dat configureren van de geautomatiseerde controle(s) juist en volledig plaatsvindt.</li> </ul>
<b>Verificatie</b>	Welke documenten/registraties (incl. versienummers) zijn ingezien.

### Rollen

DVP	✓
DVZA	✓
BO	

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

## A.12.4.4 Kloksynchronisatie

### Norm

<b>Rationale</b>	Deze maatregel borgt dat tijdsvermeldingen in logbestanden gelijklopen, wanneer deze worden gebruikt om misbruik in de keten op te sporen. Zie ook <a href="#">A.16.1.7 Verzamelen van bewijsmateriaal</a> .
<b>Implementatie</b>	<p>De klokken van IT componenten die communiceren via MedMij en logging in het kader van MedMij bijhouden, MOETEN worden gesynchroniseerd met <a href="#">pool.ntp.org</a>.</p> <p>Het is toegestaan te synchroniseren met een alternatieve NTP-server, wanneer maatregelen zijn getroffen om de afwijking met <a href="#">pool.ntp.org</a> niet groter dan plus of min 500 ms te laten zijn.</p>
<b>NEN 7510-1: 2017</b>	A.12.4.4 Kloksynchronisatie
<b>NEN 7510: 2011</b>	A.10.10.6 Synchronisatie van systeemklokken

### Beoordeling

<b>Auditmethode</b>	Stel voor de relevante systemen voor het MedMij afsprakenstelsel vast via de logging*- en /of configuratie-instellingen dat de synchronisatie met <a href="#">pool.ntp.org</a> ten minste 1x per 24 uur plaats vindt. Dan wel middels een verklaring van een lokale NTP server over de synchronisatieprocedure met genoemde NTP-server.
<b>Verificatie</b>	Evidence m.b.t. de logbestanden en/ of configuratie instellingen.

### Rollen

DVP	✓
DVZA	✓
BO	✓

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie



## A.12.6.1 Beheer van technische kwetsbaarheden

### Norm

<b>Rationale</b>	Deze maatregel borgt dat deelnemers in staat zijn tijdig te reageren op meldingen van (vermeende) kwetsbaarheden in het MedMij stelsel.  Zie ook <a href="#">A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging</a> .
<b>Implementatie</b>	De processen MOETEN aansluiten op de <a href="#">Operationele processen</a> in het MedMij Afsprakenstelsel ten aanzien van het beheer van technische kwetsbaarheden.  Dit dient te omvatten: <ul style="list-style-type: none"> <li>• Identificeren van kwetsbaarheden in de eigen technologie, onderzoeken van relevantie van door de beheerorganisatie geïdentificeerde kwetsbaarheden + terugkoppeling naar de beheerorganisatie hieromtrent;</li> <li>• Het patchen van systemen of anderzijds mitigeren van de kwetsbaarheid;</li> <li>• Het tijdig kunnen doorlopen van de gehele procedure bij hoog risico-kwetsbaarheden.</li> </ul>
<b>NEN 7510-1: 2017</b>	A.12.6.1 Beheer van technische kwetsbaarheden
<b>NEN 7510: 2011</b>	A.12.6.1 Beheersing van technische kwetsbaarheden

### Beoordeling

<b>Auditmethode</b>	<ul style="list-style-type: none"> <li>• Stel vast dat de organisatie in haar procedures aansluit op het proces van beheren van technische kwetsbaarheden uit het afsprakenstelsel van MedMij.</li> <li>• Stel door middel van interview met de betrokken medewerkers vast of de procedures worden nageleefd.</li> </ul>
<b>Verificatie</b>	<ul style="list-style-type: none"> <li>• Welke procedures (incl. versienummers) zijn ingezien.</li> <li>• Met wie gesproken is ter bevestiging van de implementatie.</li> </ul>

### Rollen

DVP	✓
DVZA	✓
BO	✓

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

## A.14.2.1 Beleid voor beveiligd ontwikkelen

### Norm

<b>Rationale</b>	Deze maatregel borgt dat deelnemers en beheerorganisatie beveiligingsstandaarden toepassen bij het ontwikkelen van software en systemen die aan het internet gekoppeld worden. Dit voorkomt dat bekende programmeerfouten worden gemaakt.
<b>Implementatie</b>	<p>Bij het vaststellen voor het beleid voor beveiligd ontwikkelen MOETEN de ICT-beveiligingsrichtlijnen voor webapplicaties van het NCSC uit het "Uitvoeringsdomein" overwogen worden (<a href="https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties">https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties</a>).</p> <p>Voor mobiele applicaties MOETEN de Beveiligingsrichtlijnen voor mobiele applicaties van het NCSC overwogen worden (<a href="https://www.ncsc.nl/documenten/publicaties/2019/mei/01/beveiligingsrichtlijnen-voor-mobiele-apparaten">https://www.ncsc.nl/documenten/publicaties/2019/mei/01/beveiligingsrichtlijnen-voor-mobiele-apparaten</a>).</p>
<b>NEN 7510: 2011</b>	Deze maatregel bestond nog niet in NEN 7510:2011

### Beoordeling

<b>Auditmethode</b>	<ul style="list-style-type: none"> <li>• Stel vast dat de organisatie in haar beleid met betrekking tot de ontwikkeling, de door NCSC gedefinieerde minimale beveiligingsstandaarden ('Uitvoeringsdomein') in overweging heeft genomen.</li> <li>• Stel vast dat deze zijn toegepast.</li> </ul>
<b>Verificatie</b>	<ul style="list-style-type: none"> <li>• Welke procedures (incl. versienummers) zijn ingezien.</li> <li>• Met wie gesproken is ter bevestiging van de toepassing van de procedures.</li> </ul>

### Rollen

DVP	✓
DVZA	✓
BO	✓

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

## A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten

### Norm

<b>Rationale</b>	Deze maatregel borgt dat MedMij beheersmaatregelen die door een leverancier worden uitgevoerd contractueel vastgelegd worden.
<b>Implementatie</b>	Organisaties MOETEN relevante MedMij beheersmaatregelen contractueel beleggen bij hun leveranciers.
<b>Toelichting</b>	Deze maatregel mag worden uitgesloten indien er voor de MedMij-dienstverlening geen gebruik wordt gemaakt van externe leveranciers.
<b>NEN 7510-1: 2017</b>	A.15.1.2 Opnemen van beveiligingsaspecten in leveranciersovereenkomsten
<b>NEN 7510: 2011</b>	6.2.3 Beveiliging in overeenkomsten met een derde partij

### Beoordeling

<b>Auditmethode</b>	Stel vast dat de organisatie de uitbestede maatregelen contractueel heeft geborgd met de leverancier(s).
<b>Verificatie</b>	Welke documenten (incl. versienummers) zijn ingezien.

### Rollen

DVP	✓
DVZA	✓
BO	✓

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

## A.15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers

### Norm

<b>Rationale</b>	Deze maatregel borgt dat er controle plaatsvindt op de naleving van MedMij beheersmaatregelen die door een leverancier worden uitgevoerd.
<b>Implementatie</b>	Organisaties MOETEN toezien op correcte naleving van de relevante MedMij beheersmaatregelen die bij een leverancier belegd zijn.
<b>Toelichting</b>	Deze maatregel mag worden uitgesloten indien er voor de MedMij-dienstverlening geen gebruik wordt gemaakt van externe leveranciers.
<b>NEN 7510-1: 2017</b>	A.15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers
<b>NEN 7510: 2011</b>	10.2.2 Controle en beoordeling van dienstverlening door een derde partij.

### Beoordeling

<b>Auditmethode</b>	Stel vast (bijvoorbeeld door het inzien van auditrapportages of leveranciersbeoordelingen) dat de organisatie heeft vastgesteld dat de leverancier de relevante maatregelen naar behoren heeft geïmplementeerd/uitgevoerd.
<b>Verificatie</b>	Welke documenten (incl. versienummers) zijn ingezien.

### Rollen

DVP	✓
DVZA	✓
BO	✓

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

## A.16.1.1 Verantwoordelijkheden en procedures

### Norm

<b>Rationale</b>	Deze maatregel borgt dat deelnemers en beheerorganisatie volgens hetzelfde proces handelen in geval van incidenten en calamiteiten. Zie ook <a href="#">A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging</a> .
<b>Implementatie</b>	De processen voor het behandelen van incidenten en calamiteiten moeten aansluiten op de <a href="#">Operationele processen</a> in het afsprakenstelsel.
<b>NEN 7510-1: 2017</b>	A.16.1.1 Verantwoordelijkheden en procedures
<b>NEN 7510: 2011</b>	A.13.2.1 Verantwoordelijkheden en procedures

### Beoordeling

<b>Auditmethode</b>	<ul style="list-style-type: none"> <li>• Stel vast dat de organisatie in haar procedures aansluit op het proces van incidenten en calamiteiten uit het afsprakenstelsel van MedMij.</li> <li>• Stel vast de procedures worden nageleefd.</li> </ul>
<b>Verificatie</b>	<ul style="list-style-type: none"> <li>• Welke procedures (incl. versienummers) zijn ingezien.</li> <li>• Met wie gesproken is ter bevestiging van de implementatie.</li> <li>• Evidence m.b.t. de daadwerkelijke implementatie.</li> </ul>

### Rollen

DVP	✓
DVZA	✓
BO	✓

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

## A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging

### Norm

<b>Rationale</b>	Deze maatregel borgt dat alle partijen elkaar tijdig op de hoogte brengen wanneer zij kennis hebben over kwetsbaarheden, die relevant kan zijn voor het MedMij stelsel. Het kan hier bijvoorbeeld gaan om informatie verkregen via het NCSC, penetratietesten of een Responsible Disclosure-melding). Zie ook <a href="#">A.12.6.1 Beheer van technische kwetsbaarheden</a> .
<b>Implementatie</b>	Kwetsbaarheden en incidenten die betrekking hebben op persoonlijke gezondheidsgegevens of het functioneren van het MedMij stelsel MOETEN binnen 48 uur gemeld te worden bij het centrale incident management team. Zie <a href="#">Deelnemersovereenkomsten</a> .  DVZA maken hierover zonodig afspraken met de aangesloten ZA's.
<b>NEN 7510-1: 2017</b>	A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging
<b>NEN 7510: 2011</b>	A.13.1.2 Rapportage van zwakke plekken in de beveiliging

### Beoordeling

<b>Auditmethode</b>	<ul style="list-style-type: none"> <li>• Stel vast dat de organisatie in haar procedures aansluit op het proces van incidenten en calamiteiten en proces beheren technische kwetsbaarheden uit het afsprakenstelsel van MedMij.</li> <li>• Stel door middel van interview met de betrokken medewerkers en waar mogelijk onderbouwd met evidence vast of de procedures worden nageleefd.</li> <li>• Stel door middel van interview en evidence vast of de deelnemer alle ontdekte kwetsbaarheden tijdig heeft gemeld aan MedMij.</li> </ul>
<b>Verificatie</b>	<ul style="list-style-type: none"> <li>• Welke procedures (incl. versienummers) zijn ingezien.</li> <li>• Met wie gesproken is ter bevestiging van de implementatie.</li> <li>• Evidence m.b.t. ontdekte kwetsbaarheden en tijdige melding aan MedMij.</li> </ul>

### Rollen

DVP	✓
DVZA	✓
BO	✓

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

## A.16.1.7 Verzamelen van bewijsmateriaal

### Norm

<b>Rationale</b>	Deze maatregel borgt dat alle partijen moeten meewerken aan forensische onderzoeken, bijvoorbeeld in de nasleep van een stelselincident of fraude. Het zal meestal gaan om het opleveren van logfiles (zie <a href="#">A.12.4.1 Gebeurtenissen registreren</a> ).
<b>Implementatie</b>	Medewerking MOET worden verleend aan (forensische) onderzoeken, door het aanleveren van gevraagde bewijsmaterialen, zulks op verzoek van de beheerorganisatie of bevoegde instanties.  DVZA maken hierover zonodig afspraken met de aangesloten ZA's.
<b>NEN 7510-1: 2017</b>	A.16.1.7 Verzamelen van bewijsmateriaal
<b>NEN 7510: 2011</b>	A.13.2.3 Verzamelen van bewijsmateriaal

### Beoordeling

<b>Auditmethode</b>	<ul style="list-style-type: none"> <li>• Stel vast dat de organisatie in haar procedures het verlenen van medewerking aan (forensische) onderzoeken heeft opgenomen.</li> <li>• Stel vast dat de procedures worden nageleefd.</li> </ul>
<b>Verificatie</b>	<ul style="list-style-type: none"> <li>• Welke procedures (incl. versienummers) zijn ingezien.</li> <li>• Met wie gesproken is ter bevestiging van de implementatie.</li> <li>• Evidence m.b.t. de implementatie.</li> </ul>

### Rollen

DVP	✓
DVZA	✓
BO	✓

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

## A.18.2.3 (1) Beoordeling van technische naleving

### Norm

<b>Rationale</b>	Deze maatregel borgt dat deelnemers en de beheerorganisatie met regelmaat (en gebruikmakend van verschillende partijen) hun software, systemen en infrastructuur laten toetsen op bekende kwetsbaarheden.
<b>Implementatie</b>	<p>Tenminste jaarlijks MOET een whitebox applicatiepenetratietesten worden uitgevoerd op de externe koppelvlakken door een externe, onafhankelijke organisatie.</p> <p><b>Voor toetreding</b> heeft deze minimaal al één keer plaatsgevonden en MOETEN de hoog en middel risico bevindingen op externe MedMij koppelvlakken zijn opgelost.</p> <p>Voor penetratietesten die worden uitgevoerd <b>na toetreding</b>, dient een adequaat actieplan opgesteld te worden voor minimaal de hoge en midden risico's ten aanzien van de MedMij dienstverlening. Dit actieplan wordt gedeeld met de beheerorganisatie. De corrigerende maatregelen worden tijdig doorgevoerd.</p>
<b>Toelichting</b>	<p>Een whitebox penetratietest houdt in dat de penetratietester zoveel mogelijk inzicht heeft in de applicatie. Dit kan onder meer inhouden:</p> <ul style="list-style-type: none"> <li>• Toegang tot architectuur/ontwerpdocumentatie;</li> <li>• Toegang tot broncode;</li> <li>• Inloggegevens voor verschillende rollen.</li> </ul> <p>Het is niet nodig om een penetratietest uit te voeren op de gehele architectuur en/of alle programmacode. Het gaat met name om de beveiliging van de gegevens die over internet worden uitgewisseld, de focus moet dus liggen op de beveiliging van de externe koppelvlakken. Een app of een web portaal is ook een extern koppelvlak!</p>
<b>NEN 7510-1: 2017</b>	A.18.2.3 Beoordeling van technische naleving
<b>NEN 7510: 2011</b>	A.15.2.2 Controle op technische naleving

### Beoordeling

<b>Auditmethode</b>	Stel op basis van de meest recente rapportages vast of er wordt voldaan aan de jaarlijkse whitebox applicatiepenetratietesten op de externe koppelvlakken conform de architectuur en specificaties van MedMij (en louter binnen de scope van het MedMij afsprakenstelsel).
<b>Verificatie</b>	<ul style="list-style-type: none"> <li>• Evidence m.b.t. de uitgevoerde jaarlijkse testen.</li> <li>• Met wie gesproken is ter bevestiging van de implementatie.</li> <li>• Evidence m.b.t. het melden van kwetsbaarheden</li> </ul>

### Rollen

DVP	✓
DVZA	✓



BO

*DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie*

## A.18.2.3 (2) Beoordeling van technische naleving

### Norm

<b>Rationale</b>	Deze maatregel borgt dat deelnemers en de beheerorganisatie met regelmaat (en gebruikmakend van verschillende partijen) hun software, systemen en infrastructuur laten toetsen op bekende kwetsbaarheden.
<b>Implementatie</b>	Tenminste jaarlijks MOET een blackbox infrastructuur penetratietesten worden uitgevoerd op de externe koppelvlakken van de deelnemers ten behoeve van het MedMij stelsel. Naar aanleiding van het resultaat wordt een adequaat actieplan opgesteld voor minimaal de hoge en midden risico's ten aanzien van de MedMij dienstverlening.
<b>NEN 7510-1: 2017</b>	A.18.2.3 Beoordeling van technische naleving
<b>NEN 7510: 2011</b>	A.15.2.2 Controle op technische naleving

### Beoordeling

<b>Auditmethode</b>	Stel op basis van de meest recente rapportages vast of er wordt voldaan aan de jaarlijkse blackbox-applicatiepenetratietesten op de externe koppelvlakken conform de architectuur en specificaties van MedMij (en louter binnen de scope van het MedMij afsprakenstelsel).
<b>Verificatie</b>	<ul style="list-style-type: none"> <li>• Evidence m.b.t. de uitgevoerde jaarlijkse testen.</li> <li>• Met wie gesproken is ter bevestiging van de implementatie.</li> <li>• Evidence m.b.t. het melden van kwetsbaarheden</li> </ul>

### Rollen

DVP	
DVZA	
BO	✓

DVP = Dienstverlener persoon, DVZA = Dienstverlener zorgaanbieder, BO = Beheerorganisatie

# Aanvullende auditverklaring en onderbouwende rapportage

## Organisatiegegevens

De gegevens van de (aspirant) MedMij deelnemer.

Naam	
Adres	
Vertegenwoordigd door	
Rol	DVP/DVZA

## Certificatiegegevens

De gegevens van het onderliggende NEN 7510-certificaat.

Norm	NEN 7510-1:2017
Scope	
Certificaatnummer	
Vervaldatum	

## Auditgegevens

Gegevens over de audit.

CBI	
Bezochte locatie(s)	
Lead auditor	
Overige teamleden	

## Rapport

Gegevens over dit rapport.

Datum rapport	
Status rapport	Concept/Definitief
Bijlagen bij dit rapport	

## Onderbouwende rapportage

Beheersmaatregel	DVP	DVZA	BO	Implementatie	Voldoet
A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen	✓	✓		Opgeslagen persoonlijke gezondheidsgegevens MOETEN beschermd worden door middel van disk-level en/of database-level encryptie. Hiervoor wordt verwezen naar de aanbevelingen die gelden voor 'near term protection' en 'long-term protection' in de ECRYPT-CSA aanbevelingen, zie hieronder.	
A.12.1.2 (1) Wijzigingsbeheer	✓	✓	✓	De IT-beheerprocessen MOETEN aansluiten op het MedMij Change- en releasebeleid.	
A.12.1.2 (2) Wijzigingsbeheer	✓	✓	✓	Niet-standaard wijzigingen op de IT componenten die gebruikt worden binnen de scope van MedMij MOETEN op basis van het vier-ogen-principe worden uitgevoerd.	
A.12.1.2 (3) Wijzigingsbeheer	✓	✓	✓	Indien er wijzigingen plaatsvinden die mogelijk significante impact hebben op de informatiebeveiliging, MOET de penetratietest zoals benoemd in <a href="#">A.18.2.3 (1) Beoordeling van technische naleving</a> voor deze componenten opnieuw uitgevoerd worden.	
A.12.1.3 (1) Capaciteitsbeheer	✓	✓		Maatregelen MOETEN zijn gedocumenteerd en geïmplementeerd om te (kunnen) voldoen aan de beschikbaarheidseisen zoals vastgelegd in <a href="#">Token interface</a> en <a href="#">Resource interface</a> .	
A.12.1.3 (2) Capaciteitsbeheer			✓	Maatregelen MOETEN zijn gedocumenteerd en geïmplementeerd om te (kunnen) voldoen aan de beschikbaarheidseisen zoals vastgelegd in <a href="#">GNL</a> -, <a href="#">OCL</a> - en <a href="#">ZAL-interface</a> .	
A.12.3.1 Back-up van informatie	✓			Er MOETEN maatregelen zijn geïmplementeerd waardoor het gegevensverlies van persoonlijke gezondheidsinformatie maximaal 24 uur bedraagt. Daarnaast moet een herstelprocedure zijn ingericht waardoor de gegevens van een persoon binnen 24 uur terug	

kunnen worden geplaatst in geval van een incident. Deze herstelprocedure wordt minimaal jaarlijks getest.

#### A.12.4.1 Gebeurtenissen registreren



Logging MOET plaatsvinden zoals gespecificeerd in het afsprakenstelsel (zie [Processen en informatie](#) onder Logging)

Daarnaast MOETEN de volgende acties ten minste 12 maanden onweerlegbaar en controleerbaar worden gelogd:

- De actie waarbij de persoon via de DVP bij de DVZA gegevens wil opvragen
- De acties waarbij de persoon toestemming geeft voor de uitwisseling conform de specificaties in het afsprakenstelsel (indien uitgevoerd onder verantwoordelijkheid van de DVZA)

#### A.12.4.3 Logbestanden van beheerders en operators



1. Het gebruik van toegangsrechten op IT-componenten waar persoonlijke gezondheidsgegevens worden verwerkt MOET worden gelogd;
2. Deze logging MOET ten minste maandelijks worden gecontroleerd. Dit geldt ook voor eventuele onderaannemers;
3. Hierbij MOET functiescheiding gewaarborgd zijn;
4. Tijdens deze controle moet aandacht zijn voor onterecht /onnodig gebruik door medewerkers (met aantoonbare opvolging).

#### A.12.4.4 Kloksynchronisatie



De klokken van IT componenten die communiceren via MedMij en

logging in het kader van MedMij  
bijhouden, MOETEN worden  
gesynchroniseerd met [pool.ntp.org](https://pool.ntp.org).

Het is toegestaan te synchroniseren  
met een alternatieve NTP-server,  
wanneer maatregelen zijn getroffen  
om de afwijking met [pool.ntp.org](https://pool.ntp.org)  
niet groter dan plus of min 500 ms  
te laten zijn.

#### A.12.6.1 Beheer van technische kwetsbaarheden



De processen MOETEN aansluiten  
op de [Operationele processen](#) in  
het MedMij Afsprakenstelsel ten  
aanzien van het beheer van  
technische kwetsbaarheden.

Dit dient te omvatten:

- Identificeren van kwetsbaarheden  
in de eigen technologie,  
onderzoeken van relevantie van  
door de beheerorganisatie  
geïdentificeerde kwetsbaarheden  
+ terugkoppeling naar de  
beheerorganisatie hieromtrent;
- Het patchen van systemen of  
anderzijds mitigeren van de  
kwetsbaarheid;
- Het tijdig kunnen doorlopen van  
de gehele procedure bij hoog  
risico-kwetsbaarheden.

#### A.14.2.1 Beleid voor beveiligd ontwikkelen



Bij het vaststellen voor het beleid  
voor beveiligd ontwikkelen  
MOETEN de ICT-  
beveiligingsrichtlijnen voor  
webapplicaties van het NCSC uit  
het "Uitvoeringsdomein" overwogen  
worden (<https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties>).

Voor mobiele applicaties MOETEN  
de Beveiligingsrichtlijnen voor  
mobiele applicaties van het NCSC  
overwogen worden (<https://www.ncsc.nl/documenten/publicaties/2019/mei/01/beveiligingsrichtlijnen-voor-mobiele-apparaten>).

#### A.15.1.2 Opnemen van beveiligingsaspecten in



Organisaties MOETEN relevante  
MedMij beheersmaatregelen

leveranciersovereenkomsten				contractueel beleggen bij hun leveranciers.
A.15.2.1 Monitoring en beoordeling van dienstverlening van leveranciers	✓	✓	✓	Organisaties MOETEN toezien op correcte naleving van de relevante MedMij beheersmaatregelen die bij een leverancier belegd zijn.
A.16.1.1 Verantwoordelijkheden en procedures	✓	✓	✓	De processen voor het behandelen van incidenten en calamiteiten moeten aansluiten op de <a href="#">Operationele processen</a> in het afsprakenstelsel.
A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging	✓	✓	✓	<p>Kwetsbaarheden en incidenten die betrekking hebben op persoonlijke gezondheidsgegevens of het functioneren van het MedMij stelsel MOETEN binnen 48 uur gemeld te worden bij het centrale incident management team. Zie <a href="#">Deelnemersovereenkomsten</a>.</p> <p>DVZA maken hierover zonodig afspraken met de aangesloten ZA's.</p>
A.16.1.7 Verzamelen van bewijsmateriaal	✓	✓	✓	<p>Medewerking MOET worden verleend aan (forensische) onderzoeken, door het aanleveren van gevraagde bewijsmaterialen, zulks op verzoek van de beheerorganisatie of bevoegde instanties.</p> <p>DVZA maken hierover zonodig afspraken met de aangesloten ZA's.</p>
A.18.2.3 (1) Beoordeling van technische naleving	✓	✓		<p>Tenminste jaarlijks MOET een whitebox applicatiepenetratietesten worden uitgevoerd op de externe koppelvlakken door een externe, onafhankelijke organisatie.</p> <p><b>Voor toetreding</b> heeft deze minimaal al één keer plaatsgevonden en MOETEN de hoog en middel risico bevindingen op externe MedMij koppelvlakken zijn opgelost.</p> <p>Voor penetratietesten die worden uitgevoerd <b>na toetreding</b>, dient een adequaat actieplan opgesteld te worden voor minimaal de hoge en midden risico's ten aanzien van de MedMij dienstverlening. Dit</p>

				actieplan wordt gedeeld met de beheerorganisatie. De corrigerende maatregelen worden tijdig doorgevoerd.
A.18.2.3 (2) Beoordeling van technische naleving	✓			Tenminste jaarlijks MOET een blackbox infrastructuur penetratietesten worden uitgevoerd op de externe koppelvlakken van de deelnemers ten behoeve van het MedMij stelsel. Naar aanleiding van het resultaat wordt een adequaat actieplan opgesteld voor minimaal de hoge en midden risico's ten aanzien van de MedMij dienstverlening.
A. 5.1.1 Beleidsregels voor informatiebeveiliging	✓	✓	✓	De beleidsdocumenten MOETEN de beleidsmaatregelen die van toepassing zijn op MedMij (onder andere gespecificeerd in <a href="#">Privacy- en informatiebeveiligingsbeleid</a> ) specifiek benoemen.
A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging	✓	✓	✓	<p>De (eind)verantwoordelijkheid voor informatiebeveiliging MOET belegd zijn. Deze functionaris(sen) dient /dienen mandaat te hebben om bij (een dreiging van) een crisis spoedbesluiten te nemen ten aanzien van MedMij en deze besluiten met spoed te kunnen (laten) realiseren.</p> <p>De verantwoordelijke en operationele functionaris(sen) (inclusief eventuele onderaannemers) dient/ dienen hiervoor tijdens kantooruren binnen een uur beschikbaar te zijn en buiten kantooruren binnen drie uur.</p>
A. 7.2.2 (1) Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	✓	✓	✓	De verantwoordelijke functionaris (sen) zoals benoemd in <a href="#">A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging</a> MOET(EN) deelgenomen hebben aan de training over de algemene werking van het stelsel.
A. 7.2.2 (2) Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	✓	✓	✓	Overige medewerkers die werkzaamheden verrichten gerelateerd aan MedMij MOETEN een training hebben gevolgd over de algemene werking van het stelsel en op de voor hem/haar van



				toepassing zijnde beveiligingsmaatregelen.
A. 8.2.1 Classificatie van informatie	✓	✓	✓	De gegevens die binnen het stelsel worden verwerkt MOETEN worden behandeld conform het Informatieclassificatiebeleid (van MedMij).
A. 9.1.1 Beleid voor toegangsbeveiliging	✓	✓	✓	<p>Er MOETEN technische en organisatorische maatregelen worden genomen om inzage van persoonlijke gezondheidsgegevens door medewerkers te voorkomen. De organisatie dient minimaal elk halfjaar en na grote wijzigingen een self-assessment uit te voeren om vast te stellen dat deze maatregelen nog effectief zijn.</p> <p>In (zeer) uitzonderlijke gevallen is inzage in persoonlijke gezondheidsgegevens niet te voorkomen. Hiervoor dient de organisatie een (nood)procedure te documenteren. Deze procedure dient in te gaan op:</p> <ul style="list-style-type: none"> <li>• Functiescheiding tussen vragen van toestemming voor inzage en het geven van toestemming door een verantwoordelijke functionaris;</li> <li>• Randvoorwaarden en maatregelen met als doel dat inzage plaatsvindt op een gecontroleerde en zo beperkt mogelijke (in tijd en hoeveelheid gegevens) wijze;</li> <li>• Borging dat de deelnemer voldoet wordt aan wet- en regelgeving (AVG, Meldplicht Datalekken) en de geldende versie van het MedMij Afsprakenstelsel;</li> <li>• Vastlegging en verantwoording van de getroffen acties.</li> </ul>
A. 9.2.5 Beoordeling van toegangsrechten van gebruikers	✓	✓	✓	<ol style="list-style-type: none"> <li>1. Toegangsrechten die zijn verstrekt op IT-componenten waar persoonlijke gezondheidsgegevens worden worden verwerkt MOETEN ten minste maandelijks worden gecontroleerd.</li> </ol>

2. Hierbij MOET functiescheiding gewaarborgd zijn.
3. Dit geldt ook voor eventuele onderaannemers.
4. Tijdens deze controle moet aandacht zijn voor medewerkers die geen gebruik (meer) maken van de toegangsrechten (met aantoonbare opvolging).

#### A. 9.4.1 Beperking toegang tot informatie



Authenticatie van personen (eindgebruikers) MOET plaatsvinden op basis van minimaal twee factoren. Na succesvolle authenticatie krijgen personen alleen toegang tot hun eigen persoonlijke gezondheidsgegevens.

## Ondertekening

Hierbij verklaren ondergetekenden (auditor en vertegenwoordiger CBI) dat bovengenoemde Organisatie **wel** /**niet** voldoet aan het aanvullend normenkader informatiebeveiliging, release 1.2.0 MedMij Afsprakenstelsel, zoals door Stichting MedMij is uitgegeven.

---

(Naam auditor, datum, handtekening)

---

(Naam vertegenwoordiger CBI, datum, handtekening)

## Beleid

Het beleid gaat in op de vraag hoe Stichting MedMij omgaat met een aantal belangrijke besturingsthema's en vormt de basis voor de [Operationele processen](#). Het beleid is richtinggevend voor het optreden van Stichting MedMij. Het bevat tevens verantwoordelijkheden voor deelnemers. Indien de situatie daarom vraagt, mag Stichting MedMij na belangenafweging afwijken van het beleid.

## Beleid inzake gecontroleerde livegang

Stichting MedMij biedt *Deelnemers* de gelegenheid om, wanneer zij zich gekwalificeerd hebben voor een specifieke *Gegevensdienst*, gefaseerd live te gaan met die *Gegevensdienst* op het MedMij-netwerk. Gedurende een zogenoemde 'gecontroleerde livegang' wordt tijdelijk afgedongen op het principe dat, indien een zekere *Zorgaanbieder* een zekere *Gegevensdienst* aanbiedt op het MedMij-netwerk, alle daarvoor gekwalificeerde *Dienstverleners persoon* deze *Gegevensdienst* ook van deze *Zorgaanbieder* moeten kunnen afnemen. Tijdens een gecontroleerde livegang is een *Zorgaanbieder*, via diens *Dienstverlener zorgaanbieder*, in de gelegenheid om die toegang te beperken tot een beperkte groep *Dienstverleners persoon*.

Zo wordt weliswaar afgedongen op een cruciaal principe van MedMij, maar staat dit in dienst van datzelfde principe: gecontroleerde livegangen zijn tijdelijk en beogen de inbedding van betrokkenen in het MedMij-netwerk waarin het principe volop geldig is.

Een gecontroleerde livegang wordt gekarakteriseerd door:

- één *Gegevensdienst*;
- één of meer *Zorgaanbieders* die met deze *Gegevensdienst* gecontroleerd live willen gaan;
- één of meer *Dienstverleners zorgaanbieder* die deze *Gegevensdienst* voor deze *Zorgaanbieder(s)* ontsluiten;
- één of meer *Dienstverleners persoon* tot wie de toegang tot deze *Gegevensdienst* van deze *Zorgaanbieder(s)* beperkt wordt gedurende de gecontroleerde livegang. *Dienstverleners persoon* kunnen desgewenst een deel van hun gebruikerskring afzonderen voor de gecontroleerde livegang, maar de organisatie en implementatie daarvan valt geheel binnen hun eigen verantwoordelijkheid.

Gecontroleerde livegangen worden alleen toegestaan op de *Interfaceversie* die hoort bij de op dat moment verplichte release. Zie [Change- en releasebeleid](#). Bij het verouderen van een tot dan toe verplichte release stopt de gecontroleerde livegang. Het is daarom aanbevelenswaardig gecontroleerde livegangen te starten kort na een releasemoment.

Gedurende een gecontroleerde livegang kunnen *Zorgaanbieders*, *Dienstverleners zorgaanbieder* en *Dienstverleners persoon* toetreden tot en uitreden uit een gecontroleerde livegang. Wanneer de laatste *Zorgaanbieder*, de laatste *Dienstverlener zorgaanbieder* of de laatste *Dienstverlener persoon* zou uitreden, wordt de gecontroleerde livegang definitief beëindigd. Uittreding van een *Zorgaanbieder* kan gepaard gaan met een promotie, dat wil zeggen, met het opgaan van die *Zorgaanbieder* met de betreffende *Gegevensdienst* in het MedMij-netwerk, buiten die gecontroleerde livegang. Promotie van alle deelnemende *Zorgaanbieders* is het uiteindelijke doel van elke gecontroleerde livegang, maar geen verplichting. Promotie is een vrije keus van de betreffende *Zorgaanbieder* en vereist geen nadere kwalificatie of acceptatie.

Een gecontroleerde livegang wordt na drie maanden definitief beëindigd. Op gezamenlijk verzoek van betrokken partijen is hierop een eenmalig uitstel van één maand mogelijk. Een *Zorgaanbieder* mag op eenzelfde *Gegevensdienst* niet deelnemen in een gecontroleerde livegang wanneer hij minder dan drie maanden geleden ook al betrokken was bij een gecontroleerde livegang op die *Gegevensdienst*. Stichting MedMij behoudt zich het recht voor op te treden tegen situaties waarin een *Dienstverlener persoon* concurrentieel voordeel ontleent of beoogt te ontleen aan de tijdelijke exclusiviteit die hem gedurende een gecontroleerde livegang wordt gegund in het afnemen van de betreffende *Gegevensdienst* van een betrokken *Zorgaanbieder*.

Op een gecontroleerde livegang zijn onverminderd alle verantwoordelijkheden van toepassing die betrokken partijen dragen uit hoofde van hun deelname aan MedMij. Gecontroleerde livegangen worden langs geheel administratieve weg georganiseerd door de MedMij Beheerorganisatie. Van de betreffende *Gegevensdienst* wordt een kopie-*Gegevensdienst* gecreëerd en in de *Catalogus* opgenomen, waarop alleen bij de gecontroleerde livegang betrokken *Dienstverleners* erkend worden, onder de voorwaarde dat zij gekwalificeerd zijn op de originele *Gegevensdienst*. Een kopie-*Gegevensdienst* kan geen origineel zijn voor een volgende kopie. Er kunnen van één origineel-*Gegevensdienst* onbeperkt veel kopieën bestaan, na

elkaar of tegelijkertijd. Na beëindiging van de geldigheid van een kopie-*Gegevensdienst* wordt deze nooit opnieuw geldig.

De kopie-*Gegevensdienst* is alleen geldig gedurende de gecontroleerde livegang, maar nooit buiten de geldigheidsduur van de origineel-*Gegevensdienst*. In de *OAuth Client List* en de *Zorgaanbiederslijst* verschijnen de betrokken partijen met de kopie-*Gegevensdienst*, net zoals ze met de origineel-*Gegevensdienst* zouden verschijnen. Een gecontroleerde livegang is dus weliswaar besloten, maar niet geheim. Alle uitwisselingen in het kader van een gecontroleerde livegang worden net zo behandeld als alle andere MedMij-uitwisselingen.

Een gecontroleerde livegang is dus geen proef-deelname, maar in alle opzichten een deelname aan het MedMij-netwerk, waarin evenwel een *Gegevensdienst* voor een *Zorgaanbieder* gefaseerd live kan worden ontsloten naar alle daartoe gekwalificeerde *Dienstverleners* *persoon*.

## Change- en releasebeleid

Het MedMij Afsprakenstelsel evolueert voortdurend. Ontwikkelingen binnen en rondom MedMij kunnen aanleiding geven om afspraken uit het stelsel te wijzigen.

### Releasecyclus

De wijzigingen aan het stelsel vinden zoveel mogelijk plaats aan de hand van een vaste releasecyclus en een releaseplanning met release momenten in april en oktober. Stichting MedMij speelt hierbij een aanjagende en faciliterende rol met een aantal verantwoordelijkheden, namelijk: het samenstellen van samenhangende releases, het ophalen van input bij belanghebbenden, het uitvoeren van impactanalyses, het organiseren van de besluitvorming en de informatievoorziening eromheen en het bewaken van ontwikkelingen in de omgeving (bijvoorbeeld veranderende wetgeving). Ook is zij voortdurend attent op wijzigingen in gebruikte normen en standaarden en heroverweegt in voorkomend geval het hergebruik.

Jaarlijks stelt Stichting MedMij samen met de verschillende belanghebbenden een releaseplanning op. De releaseplanning bevat een overzicht van geplande releases voor de periode van een jaar, geeft aan wat de belangrijkste voorgenomen wijzigingen zijn per release en duidt per geplande release de mijlpalen van het ontwikkel- en implementatietraject aan. Wijzigingen betreffende de inhoud van het afsprakenstelsel moeten passen binnen deze releaseplanning. De releaseplanning moet op haar beurt weer passen binnen de strategische kaders. Het bestuur van Stichting MedMij stelt de releaseplanning vast.

### Dakpansgewijze releases

Om het ritme van de voortdurende ontwikkeling van het MedMij Afsprakenstelsel voor *Deelnemers* zo voorspelbaar mogelijk te maken, en *Deelnemers* daarbinnen ruimte te geven voor een proactief of reactief implementatiebeleid, zijn er op elk moment twee releases van het MedMij Afsprakenstelsel *actief*. Alleen actieve releases mogen actief zijn op het operationele MedMij-netwerk. Van die twee actieve releases is er altijd één *verplicht*. Dat wil zeggen dat alle *Deelnemers* op zijn minst deze verplichte versie moeten ondersteunen. De andere actieve release heet *gepubliceerd*. Implementatie daarvan is vooralsnog niet verplicht, maar wel toegestaan op het operationele MedMij-netwerk. Omdat de *Interfaces* in het MedMij Afsprakenstelsel geversioneerd zijn, kunnen deze tegelijkertijd actief zijn. De gepubliceerde release is de opvolger van de verplichte. Elke *Deelnemer* kan zelf kiezen wanneer hij de gepubliceerde versie implementeert, desgewenst naast de verplichte.

Wanneer een nieuwe release uitkomt van het MedMij Afsprakenstelsel, krijgt:

- de tot dan toe verplichte release de status *verouderd*, hetgeen wil zeggen dat deze release niet meer actief is;
- de tot dan toe gepubliceerde release de status *verplicht*. Deze release blijft dus actief, maar verliest haar optionele status;
- de nieuwe release de status *gepubliceerd*. Deze release wordt dus actief.

Steeds schuift dus de nieuwste release (de gepubliceerde) als een nieuwe dakpan half bovenop de (dan) verplichte. Alleen de bovenste twee dakpannen zijn actief. Hun overlap symboliseert het tegelijkertijd actief zijn op het MedMij-netwerk. Omdat MedMij een vast release-ritme hanteert (van eens per half jaar), is die overlap een halve dakpan groot. Onder de verplichte release liggen de verouderde releases, als inactieve geschiedenis van het MedMij Afsprakenstelsel.

### Totstandkoming releases

Alle belanghebbenden, waaronder in ieder geval de deelnemers, gebruikers en Stichting MedMij, kunnen invloed uitoefenen op (de totstandkoming van) wijzigingen in het afsprakenstelsel. Een Request For Change

(RFC) kan door een belanghebbende voorzien van motivatie worden ingediend voor behandeling. Stichting MedMij doet een eerste beoordeling van ingediende RFC's door deze te toetsen aan de vigerende wet- en regelgeving, architectuur en grondslagen, strategische koers, het jaarplan en de releasekalender. Hierbij wordt onder andere beoordeeld of het daadwerkelijk gaat om een wijziging, of de wijziging niet al eerder is ingediend en wat de urgentie is. Stichting MedMij zorgt, indien nodig, voor de nadere verkenning van RFC's door wijzigingsverzoeken te laten uitwerken, de benodigde expertise en vertegenwoordiging bij elkaar te brengen, de afstemming met partijen rondom het stelsel te kanaliseren, te zorgen dat de impact van een wijziging op het stelsel en de deelnemers wordt onderzocht en indien nodig een business case wordt opgesteld met betrokkenen. Ook controleert zij of de voorgestelde oplossing vrij en kosteloos voor de deelnemers te gebruiken is.

In principe mogen betrokkenen bij het ontwikkelproces ontwikkelinformatie vrij met elkaar delen zonder aanvullende bescherming. Alleen voor informatie over kwetsbaarheden geldt dat verspreiding beperkt is tot de direct betrokkenen en alleen mag plaatsvinden met extra bescherming (zie [Informatieclassificatiebeleid](#)). Mochten belanghebbenden gedurende het change- en releaseproces bijdragen aan de uitwerking van een wijziging, dan ziet Stichting MedMij erop toe dat zij over de juiste auteursrechten komt te beschikken om de documentatie te kunnen publiceren (zie [Intellectueel eigendomsbeleid](#)).

Het afsprakenstelsel bestaat uit een samenhangende set van producten (juridisch kader, overeenkomsten, architectuur en technische specificaties, etc.) met veel onderlinge afhankelijkheden. Aanpassing van een van de onderdelen vraagt altijd om een impactanalyse op de rest van de producten. Het afsprakenstelsel wordt daarom altijd in haar geheel gereleased. Deze releases bestaan uit een consistente set van RFC's en kunnen daarnaast verbeteringen van niet-inhoudelijke aard bevatten.

## Verschillende typen releases, en correcties

Releases voor het afsprakenstelsel worden als volgt aangeduid:

1. **Major releases:** releases met grotere (functionele) wijzigingen. Deze releases worden opgenomen in de releaseplanning;
2. **Minor releases:** releases met twee soorten correctief onderhoud:
  - a. Wijzigingen die nodig zijn om een onmiddellijke dreiging voor de continuïteit van of het vertrouwen in het MedMij Afsprakenstelsel/-netwerk af te wenden;
  - b. Verbeteringen waarvan de baten van spoedig doorvoeren significant groter zijn dan de implementatie-inspanningen, en die op breed draagvlak onder de deelnemers kunnen rekenen.

De aanduiding van releases is opgebouwd uit drie nummers, namelijk x.y.z (bijvoorbeeld 1.3.2). Bij een major release wordt de combinatie x.y opgehoogd. Daarbij zijn twee opties, ofwel y wordt met een verhoogd waarna z op 0 wordt gezet (bijvoorbeeld van 1.3.2 naar 1.4.0), ofwel x wordt met een verhoogd waarna y en z op 0 worden gezet (bijvoorbeeld van 1.3.2 naar 2.0.0). De keuze hiertussen is afhankelijk van aard en omvang van de release. Bij een minor release wordt z met een verhoogd (bijvoorbeeld van 1.3.2 naar 1.3.3).

Major release vinden twee maal per jaar plaats. De inhoud van een major release wordt samengesteld op basis van uitgewerkte wijzigingsvoorstellen (RFC's). Minor releases zijn niet bij voorbaat gepland; zij worden alleen indien nodig tussen major releases uitgebracht, op een datum die in overleg met *Deelnemers* wordt vastgesteld.

Daarnaast kunnen correcties op het MedMij Afsprakenstelsel worden aangebracht zonder dat deze leiden tot een nieuwe release. Deze doen bijvoorbeeld acute reparaties, verwijderen inconsistenties of passen voorbeeldberichten aan. Een correctie tast de juridische en technische strekking van het MedMij Afsprakenstelsel niet aan; waar dit wel het geval zou zijn, vereist de wijziging een nieuwe release. Correcties worden op een [aparte pagina](#) in het MedMij Afsprakenstelsel aangegeven.

## Besluitvorming releases

Bij major releases legt Stichting MedMij de release eerst voor aan de deelnemersraad, die hierover een zwaarwegend advies afgeeft. Het bestuur is niet gehouden aan dit advies, maar dient het advies van de raad wel serieus te nemen en een afwijking te onderbouwen. De besluitvorming over de release door het bestuur behoeft de goedkeuring van de eigenaarsraad. De eigenaarsraad dient hierbij geïnformeerd te worden over het advies van de deelnemersraad en eventueel over de motivatie van het bestuur om van dit advies af te wijken.

Indien het bestuur van Stichting MedMij wijzigingen eerder wil laten implementeren dan in de releaseplanning mogelijk is, dan kan worden besloten tot invoering middels een minor release. Er wordt dan een tussentijdse release van het afsprakenstelsel gecreëerd die niet eerder was gepland. Bij minor releases is het aan het bestuur of en op welke wijze belanghebbenden worden betrokken bij de totstandkoming. Goedkeuring van de eigenaarsraad en advisering van de deelnemersraad zijn bij een minor release niet noodzakelijk.

## Implementatie releases

Zodra het besluit over een release van het afsprakenstelsel is genomen, bepaalt Stichting MedMij in overleg met de deelnemers en eigenaren welke aanpak de minste impact en verstoringen veroorzaakt. Ook maakt de stichting de afweging of releases in productie naast elkaar kunnen bestaan en of deelnemers op enig moment meerdere releases moeten ondersteunen. Voor de implementatie van de release zijn de data in de implementatieplanning bij de release leidend. Afhankelijk van het soort release kan een implementatietermijn van toepassing zijn.

Stichting MedMij is ervoor verantwoordelijk dat het change- en releaseproces volgens afspraak wordt uitgevoerd, de planning te monitoren op risico's voor de afgesproken ingebruiknamemomenten, en waar nodig te escaleren op het juiste niveau. Ook zorgt zij voor een gestructureerde doorvoering van aanpassingen in de documentatie en het publiceren van een nieuwe release van het afsprakenstelsel ( minimaal in de vorm van een pdf voor de administratie van deelnemers).



## Dienstverleningsoverdrachtsbeleid

Een Dienstverlener zorgaanbieder kan, op verzoek van de Zorgaanbieder, het ontsluiten van een Gegevensdienst namens die Zorgaanbieder van een andere Dienstverlener zorgaanbieder overnemen. Deze overnemende Dienstverlener zorgaanbieder moet in dat geval erkend zijn als ontsluiter van die gegevensdienst en bij Stichting MedMij aan kunnen tonen de overname met de latende deelnemer te hebben afgestemd. Uit de afstemming moet minimaal blijken dat het moment van overname is afgestemd, zodat de continuïteit van dienstverlening zo hoog mogelijk blijft.

## Gegevensdienstenbeleid

### Gegevensdiensten en de Catalogus

*Deelnemers* ontsluiten via MedMij gestandaardiseerde diensten voor gegevensuitwisseling aan, de zogeheten *Gegevensdiensten*. Deze *Gegevensdiensten* worden uitgewisseld via bijbehorende use cases uit de architectuur van het MedMij Afsprakenstelsel. De *Gegevensdiensten* die zijn toegestaan binnen MedMij worden opgenomen in de *Catalogus*. Zolang nieuwe *Gegevensdiensten* passen binnen de bestaande use cases, kunnen ze onafhankelijk van een release worden toegevoegd aan de *Catalogus*. Mocht voor een *Gegevensdienst* (een) nieuwe use case nodig zijn, dan dient eerst deze nieuwe use case te worden toegevoegd volgens het reguliere change- en releaseproces. Pas daarna kan ook deze nieuwe *Gegevensdienst* worden toegevoegd aan de *Catalogus*.

### Het Register van Informatiestandaarden

Een *Gegevensdienst* bestaat uit een verzameling *Systeemrollen* uit een *Informatiestandaard*. Nictiz beheert voor MedMij het *Register van Informatiestandaarden* met daarin de *Informatiestandaarden* die binnen MedMij gebruikt worden. Partijen kunnen informatiestandaarden indienen voor toepassing binnen MedMij. Zie [www.medmij.nl](http://www.medmij.nl) voor het proces van toelating en de bijbehorende eisen. Besluiten over toelating van een *Informatiestandaard* tot het register worden genomen door het bestuur van Stichting MedMij.

Om de *Informatiestandaard* ook te kunnen toepassen, worden *Gegevensdiensten* gedefinieerd die bestaan uit een verzameling *Systeemrollen* uit de *Informatiestandaard*. Stichting MedMij doet een voorstel voor de definitie van een of meer *Gegevensdiensten* (de naamgeving, de relatie met de use cases, de verzamelingen *Systeemrollen* en of de ondersteuning van andere *Gegevensdiensten* wordt vereist) en de datum vanaf wanneer de *Gegevensdienst* op het MedMij-netwerk gebruikt kan worden. Het bestuur van de Stichting besluit over aanpassingen aan de *Catalogus*.

### Erkenning van *Deelnemer* als ontsluiter van een *Gegevensdienst*

*Deelnemers* ontsluiten *Gegevensdiensten* via het MedMij-netwerk voor en namens gebruikers. Voordat een *Deelnemer* in deze rol wordt erkend, dient zij aan te tonen de *Gegevensdienst* op de juiste manier te ondersteunen. In de *Catalogus* staat per *Gegevensdienst* beschreven welke relevante *Systeemrollen* uit de bijbehorende *Informatiestandaard* en welke use case uit de *Architectuur en technische specificaties* ondersteund dienen te worden. Ook geeft de *Catalogus* aan welke andere *Gegevensdiensten* vereist zijn (bijvoorbeeld: Delen Afspraken kan niet zonder Verzamelen Afspraken). Indien een *Deelnemer* nog niet over een erkenning voor een vereiste *Gegevensdienst* beschikt, dan dient deze partij eerst deze erkenning te behalen. In het *Testbeleid* staat verder beschreven hoe de ondersteuning van de *Gegevensdienst* en, indien nodig, de use case, kan worden aangetoond. Stichting MedMij ziet erop toe dat aan alle voorwaarden wordt voldaan, alvorens erkenningen wordt afgegeven.

### Gegevensdiensten die elkaar vereisen of vervangen

Stichting MedMij kan in de *Catalogus* aangeven dat de ene *Gegevensdienst* de andere vereist wanneer *Zorgaanbieders* die de ene *Gegevensdienst* aanbieden, verplicht worden om ook de andere aan te bieden. Dit is vaak het geval als de *Gegevensdiensten* samen een proces vormen, zoals het verzamelen en delen van gegevens. Vereisen hoeft geen wederzijdse relatie te zijn, maar dat kan wel.

In de *Catalogus* kan worden aangegeven dat de ene *Gegevensdienst* de andere vervangt. Hier-van is sprake als de ene *Gegevensdienst* een opvolger is van de andere, zoals typisch bij een nieuwe versie. Elke *Zorgaanbieder* kan zelf kiezen wanneer hij overgaat van de voorganger naar de opvolger, zolang dat maar niet later is dan de einddatum van de voorganger en niet vroe-ger dan de startdatum van de opvolger. *Zorgaanbieders* mogen niet tegelijk een opvolger en diens voorganger(s) aanbieden; per *Zorgaanbieder* sluiten die elkaar uit.

Het is ook mogelijk dat de ene *Gegevensdienst* meerdere andere opvolgt, of voorgaat. Mocht er één opvolger zijn bij één voorganger, wordt bij voorkeur de weergavenaam van deze twee identiek gehouden, om de persoon niet onnodig te belasten met de wijziging. Vervangen is in het algemeen geen wederzijdse relatie, maar wederkerigheid is strikt gezien wel mogelijk.

## Mutaties van *Gegevensdiensten*

De volgende mutaties zijn toegestaan binnen bestaande *Gegevensdiensten*:

1. Wijzigingen in de *Gegevensdienstnaam* of *Weergavenaam*;
2. Wijzigingen in de verzameling andere *Gegevensdiensten* die door de *Gegevensdienst* vereist worden of door haar vervangen worden;
3. Wijzigingen door het instellen van een *Einddatum* of het wijzigen van een geldigheidsperiode;
4. Wijzigingen aan de *Systeemrolverzameling* of de systeemrolspecificaties van een *Gegevensdienst* die niet van invloed zijn op de interoperabiliteit (patches).

Bij mutaties van de eerste drie types wordt aanvullende informatie bij publicatie van een nieuwe versie van de *Catalogus* opgenomen. Bij mutaties van het vierde type wordt aanvullende informatie opgenomen via het [Register van Informatiestandaarden](#).

Wijzigingen in de *Systeemrolverzameling* van een *Gegevensdienst* die van invloed zijn op de interoperabiliteit, leiden altijd tot een nieuwe *Gegevensdienst*. Er moet dan bepaald worden wanneer de oude *Gegevensdienst* wordt uitgefaseerd. Kleinere en grotere wijzigingen aan een *Informatiestandaard* zullen daartoe aanleiding geven. Wijzigingen anders dan patches worden voor akkoord voorgelegd aan het bestuur van Stichting MedMij.

## Uitfasen van *Gegevensdiensten*

De volgende triggers kunnen leiden tot het uitfasen van *Gegevensdiensten*:

- Wijzigingen aan een *Systeemrolverzameling* of de specificaties van een *Systeemrol* van een *Gegevensdienst* (zie mutaties van *Gegevensdiensten*);
- Het anders vormgeven van *Gegevensdiensten* (herindelen van *Systeemrollen-Gegevensdiensten*);
- Het schrappen van een *Informatiestandaard* uit het [Register van Informatiestandaarden](#).

Hoe lang de oude *Gegevensdienst(en)* nog bruikbaar is/zijn, wordt besloten door het bestuur van Stichting MedMij. Bij dit besluit houdt het bestuur rekening met het perspectief van de *Deelnemers*.

## Informatieclassificatiebeleid

Het informatieclassificatiebeleid beschrijft de manier waarop Stichting MedMij en de deelnemers informatie classificeren, zodat deze informatie passend kan worden behandeld vanuit het oogpunt van informatiebeveiliging. Dat betekent dat de omgang met de informatie (en de bijbehorende maatregelen rond onder meer beveiliging toegang) moet aansluiten bij het vereiste zekerheidsniveau in termen van beschikbaarheid, integriteit en vertrouwelijkheid.

Om deze aansluiting praktisch hanteerbaar te maken, hanteert MedMij een beperkt aantal classificatieniveaus en een eenvoudige wijze van het koppelen van een niveau aan informatie. Daarmee hoeft niet voor elk afzonderlijk informatie-element een afzonderlijke inschatting op de zekerheidsaspecten, noch een afzonderlijke afweging over de bijpassende informatiebeveiligingsmaatregelen gemaakt te worden.

### Classificaties

In onderstaande tabel zijn de gehanteerde classificaties opgesomd. Voor de classificatie van de zekerheidsaspecten is aangesloten bij NEN7512:2015.

MedMij- classificatie	Type informatie	Classificatie van zekerheidsaspecten		
		Beschikbaarheid	Integriteit	Vertrouwelijkheid
Gezondheid	Gegevens waaruit direct of indirect informatie over de gezondheid van een persoon uit kan worden afgeleid.	Midden	Hoog	Zeer hoog
Operationele kern	Gegevens die operationeel noodzakelijk zijn voor de gegevensuitwisseling via het MedMij-netwerk.	Midden	Hoog	Laag
Samenwerking en ontwikkeling	Gegevens die betrekking hebben op de communicatie van partijen over de huidige of toekomstige inhoud van het MedMij Afsprakenstelsel en de afsprakenstelsel.	Laag	Midden	Laag
Kwetsbaarheid	Niet algemeen bekende gegevens over een (mogelijke) kwetsbaarheid bij een of meerdere deelnemers of de beheerorganisatie, al dan niet voortkomend uit de afsprakenstelsel, waarmee een kwaadwillende partij inbreuk op de informatiebeveiliging van het MedMij-netwerk zou kunnen maken.	Laag	Midden	Hoog

### Labeling

In onderstaande tabel is aangegeven welke typen informatie of informatieproducten volgens welke MedMij-classificatie behandeld moeten worden. De informatie zelf wordt niet afzonderlijk voorzien van een 'label'; op grond van dit beleid moet deze informatie worden behandeld conform de bijbehorende classificatie.

Voor informatieproducten die niet in deze tabel voorkomen moet na analyse ofwel

- een passende MedMij-classificatie, worden gekozen en is labeling noodzakelijk om duidelijk te maken wat de MedMij-classificatie van de informatie is; ofwel
- wanneer geen passende MedMij-classificatie voorhanden is, een afzonderlijke behandeling plaatsvinden. De drie zekerheidsaspecten moeten worden geclassificeerd, de noodzakelijke informatiebeveiligingsmaatregelen moeten worden bepaald en het moet voor degenen die toegang hebben tot de informatie duidelijk zijn hoe die informatie behandeld moet worden. Dat kan door de informatie te voorzien van een label of andere aanduiding, dan wel door langs andere weg duidelijkheid te verschaffen over de regels rond de omgang met de betreffende informatie.

Type informatie	MedMij-classificatie
Functionele logging op grond van de afspraken onder <a href="#">Processen en informatie</a>	Gezondheid
Alle gegevens verkregen of verstrekt in het kader van een van de interacties in het kader van de use cases uit de <a href="#">Architectuur en technische specificaties</a>	Gezondheid
Zorgaanbiederslijst	Operationele kern
Whitelist	Operationele kern
OAuthclientlist	Operationele kern
Gegevensdienstnamenlijst	Operationele kern
Inhoud van het MedMij Afsprakenstelsel	Samenwerking en ontwikkeling
Informatie ten behoeve van of aangaande doorontwikkeling	Samenwerking en ontwikkeling
Kwetsbaarheden	Kwetsbaarheid
Risicoanalyse op stelselniveau	Kwetsbaarheid
Gegevens in het kader van forensisch onderzoek, indien deze geen persoonsgegevens bevatten	Kwetsbaarheid
Gegevens in het kader van forensisch onderzoek, indien deze wel persoonsgegevens bevatten	Gezondheid
Verklaringen van auditors over de toepassing van NEN7510 en het <a href="#">Normenkader informatiebeveiliging</a> , voor zover daarin opmerkingen zijn opgenomen aangaande niet-volledige compliance	Kwetsbaarheid
Rapporten van penetratietesten	Kwetsbaarheid

## Maatregelen

In onderstaande tabel is indicatief (zonder de pretentie volledig te zijn) aangegeven waar de maatregelen te vinden zijn die van toepassing zijn op informatie die is gelabeld met een bepaalde MedMij-classificatie. Deze maatregelen betreffen veelal de omgang in het kader van de uitwisseling tussen partijen. Deelnemers en de beheerorganisatie zijn daarnaast op grond van het [Normenkader informatiebeveiliging](#) (maatregel [A.8.2.1 Classificatie van informatie](#)) verplicht om ook hun interne informatiebeveiliging te laten aansluiten bij de MedMij-classificatie. Dat betekent dat zij de informatie van een interne classificatie moeten voorzien die op geen van de drie zekerheidsaspecten (betrouwbaarheid, integriteit, vertrouwelijkheid) lager is dan die van de MedMij-classificatie die verbonden is aan de informatie.

MedMij-classificatie	Maatregelen
Gezondheid	<p><a href="#">Architectuur en technische specificaties</a>: beschrijft de maatregelen om de uitwisseling van gezondheidsgegevens veilig en betrouwbaar te laten plaatsvinden.</p> <p><a href="#">Normenkader informatiebeveiliging</a>: beschrijft de aanvullende maatregelen die deelnemers minimaal moeten treffen om ook in het eigen domein op veilige en betrouwbare manier met gezondheidsgegevens om te gaan.</p> <p><a href="#">Deelnemersovereenkomsten</a>: beschrijft de juridische bepalingen tussen Stichting MedMij en de deelnemers gericht op de privacy en (informatie)beveiliging van gezondheidsgegevens (artikel 5).</p>
Operationele kern	<p><a href="#">Architectuur en technische specificaties</a>: beschrijft de maatregelen om op veilige en betrouwbare wijze om te gaan met de operationele uitwisselgegevens.</p> <p><a href="#">Normenkader informatiebeveiliging</a>: beschrijft de aanvullende maatregelen die deelnemers minimaal moeten treffen om ook in het eigen domein op veilige en betrouwbare manier met de operationele uitwisselgegevens om te gaan.</p>
Samenwerking en ontwikkeling	<p><a href="#">Change- en releasebeleid</a>: beschrijft hoe met ontwikkelinformatie moet worden omgegaan bij de doorontwikkeling van het MedMij Afsprakenstelsel.</p> <p><a href="#">Samenwerkings- en escalatiebeleid</a>: beschrijft de onderlinge samenwerking en communicatie van partijen rondom het afsprakenstelsel.</p>
Kwetsbaarheid	<p><a href="#">Privacy- en informatiebeveiligingsbeleid</a>: beschrijft welke maatregelen zijn ingericht om de privacy- en informatiebeveiliging van het stelsel te borgen.</p> <p><a href="#">Operationele processen</a>: beschrijft met het Proces beheren technische kwetsbaarheden hoe met kwetsbaarheden wordt omgegaan.</p>

## Intellectueel eigendomsbeleid

Het merk MedMij en het Afsprakenstelsel MedMij zijn intellectueel eigendom van Stichting MedMij. Dit geldt niet voor de implementaties bij deelnemers, standaarden waarnaar wordt verwezen in het afsprakenstelsel en de generieke voorzieningen, voor zover niet door of in opdracht van Stichting MedMij ontwikkeld.

### Merkenrecht

Het merk MedMij is geregistreerd om op te kunnen treden tegen merkinbreuk of onrechtmatig gebruik van het merk door andere partijen. Een deelnemer aan het stelsel mag het merk MedMij, zowel woord- als beeldmerk, hanteren conform de aanwijzingen voor juist merkgebruik zoals opgenomen bij [Communicatie](#).

Gebruik van het merk buiten de vastgelegde afspraken is niet toegestaan. Deelnemers mogen alleen gebruik maken van het merk als en zolang zij deelnemer zijn. Zij worden gebonden aan deze afspraken via de deelnemersovereenkomst met Stichting MedMij. Zij zullen niets doen/nalaten waardoor de rechten van het merk kunnen worden aangetast en/of de opgebouwde goodwill negatief kan worden beïnvloed. Gebruik van het merk en beeld door andere partijen dan de deelnemers, is alleen toegestaan onder verantwoordelijkheid van een deelnemer of indien hiervoor van tevoren toestemming is verkregen van Stichting MedMij.

[Communicatie](#) bevat aanwijzingen voor het naam en merkgebruik, huisstijlafspraken en communicatierichtlijnen voor het merk MedMij. Stichting MedMij is verantwoordelijk voor het aanleveren van deze richtlijnen, standaard tekst- en beeldmateriaal en andere tools die de deelnemers bij hun dienstverlening dienen te gebruiken.

### Auteursrecht

De inhoud van het MedMij Afsprakenstelsel heeft, vanuit het perspectief van de auteurswet, per definitie een auteur en rechthebbende. Zonder aanvullende afspraken hierover heeft de maker van het werk het auteursrecht. Andere partijen moeten expliciet toestemming krijgen voor het gebruik en de verspreiding van het desbetreffende werk. Gezien de aard van het afsprakenstelsel en de pre concurrentiële wijze van totstandkoming, is dit niet gepast en maakt Stichting MedMij hier aanvullende afspraken over.

Stichting MedMij dient het auteursrecht van de documentatie voor het MedMij Afsprakenstelsel te verkrijgen voorafgaand aan het maken of de doorontwikkeling. Partijen die bijdragen aan de totstandkoming van de documentatie (ook betaalde opdrachtnemers, zoals adviseurs en ontwikkelaars), dragen schriftelijk het intellectueel eigendom op hun bijdrages over aan Stichting MedMij. Voor deelnemers wordt de overdracht van het intellectueel eigendom over hun bijdrages aan de documentatie geregeld via de [Deelnemersovereenkomsten](#). Indien bijdrages aan de documentatie van het stelsel niet door of in opdracht van Stichting MedMij worden gemaakt, dan moet het auteursrecht eerst aan de stichting worden overgedragen, alvorens het materiaal gebruikt wordt. Stichting MedMij ziet toe op de overdracht van het intellectueel eigendom/het gebruiksrecht. Deelnemers dienen zich te onthouden van inbreuken op de Intellectuele Eigendomsrechten van zaken die door, voor of namens Stichting MedMij zijn ontwikkeld.

### Creative Commons-licentie

Stichting MedMij regelt de toestemming voor het gebruik en de verspreiding van het MedMij Afsprakenstelsel door de documentatie te publiceren onder de Creative Commons-licentie **Naamsvermelding-GeenAfgeleideWerken 4.0 Internationaal (CC BY-ND 4.0)**. Deze Creative Commons-licentie stelt twee voorwaarden aan het gebruik en de verspreiding:

- **Naamsvermelding.** Anderen mogen het MedMij Afsprakenstelsel kopiëren, distribueren, vertonen en opvoeren, maar uitsluitend als MedMij wordt vermeld als maker.

- **GeenAfgeleideWerken.** Anderen mogen het MedMij Afsprakenstelsel kopiëren, distribueren, vertonen en opvoeren mits het werk in de originele staat blijft. Het is niet toegestaan dat anderen het stelsel gebruiken als basis voor nieuw materiaal en/of het stelsel in aangepaste vorm verspreiden.



## Klachten- en geschillenbeleid

Een klacht is een uiting van ongenoegen, gericht aan Stichting MedMij over de dienstverlening van een deelnemer of Stichting MedMij. Een geschil is een onenigheid tussen twee of meer partijen naar aanleiding van de uitvoering van een MedMij-dienst. Binnen MedMij kan sprake zijn van drie soorten klachten en geschillen:

1. Tussen de deelnemers onderling;
2. Tussen de deelnemers en Stichting MedMij.

De ambitie is om klachten en geschillen op te lossen binnen het stelsel. Wanneer betrokken partijen in onderling overleg zelf niet tot een oplossing komen, kunnen zij klachten en geschillen voorleggen aan Stichting MedMij (zie [Samenwerkings- en escalatiebeleid](#)). De klachten en geschillen moeten gerelateerd zijn aan het niet-nakomen van de afspraken/deelnemersovereenkomst door een deelnemer en/of Stichting MedMij. Stichting MedMij doet geen uitspraken over de dienstverlening van een deelnemer aan een gebruiker. De rechtsrelatie tussen de deelnemer en haar gebruikers valt buiten de scope van het MedMij Afsprakenstelsel (zie ook [Overeenkomsten en rechtsrelaties](#)).

Mocht het onverhoopt niet lukken om klachten en/of geschillen onderling tussen partijen op te lossen, dan zijn er buiten het stelsel twee routes om conflicten te beslechten. Dit zijn 1) de betrokken partijen komen een vorm van alternatieve geschillenbeslechting overeen of 2) de betrokken partijen stappen naar de rechter. Partijen wordt aangeraden om zich telkens te beraden op de mogelijkheden voor alternatieve geschillenbeslechting.

Indien gebruikers klachten hebben over de naleving van de MedMij-afspraken door een deelnemer, dan kunnen zij deze richten aan het klachtenloket van de uitvoeringsorganisatie. Stichting MedMij zal de klacht onderzoeken en de deelnemer erop aanspreken, mocht deze zich inderdaad niet aan de regels houden. De deelnemer dient daarnaast te allen tijde zelf processen ingericht te hebben om te voorkomen dat klachten die niet-gerelateerd zijn aan de MedMij-afspraken worden gericht aan Stichting MedMij.

## Nalevingsbeleid

Een goede naleving van het afsprakenstelsel is onontbeerlijk voor het vertrouwen in het stelsel. Zowel deelnemers, Stichting MedMij, als indirect de wettelijke toezichthouders hebben een rol bij de instandhouding van het netwerk en de borging van het naleven van het afsprakenstelsel. In eerste instantie gebeurt de naleving zo veel mogelijk vanuit een zelfregulerend systeem en in goed onderling overleg tussen partijen in het afsprakenstelsel (zie [Samenwerkings- en escalatiebeleid](#)). In tweede instantie kan het echter noodzakelijk zijn een correcte naleving te bewerkstelligen door middel van een interventie.

De afspraken uit het MedMij Afsprakenstelsel kennen een privaatrechtelijk karakter. Het bestuur van Stichting MedMij is daarom zelf verantwoordelijk voor de controle op de naleving van deze afspraken. Deelnemers hebben zich via de ondertekende deelnemersovereenkomst verplicht tot het naleven van de stelselafspraken voor hun specifieke rol. Bij toetreding tonen deelnemers aan dat zij aan de afspraken voldoen. Ook tijdens deelname moeten *Deelnemers* aan de afspraken blijven voldoen. Daartoe kennen de testresultaten van een *Deelnemer*, waarop diens toetreding is gebaseerd, een geldigheidsduur die gemaximeerd is op 365 dagen.

Signalen over het niet naleven van de afspraken door deelnemers komen via meerdere routes bij de beheerorganisatie binnen, waaronder bij:

- Een bemiddeling door Stichting MedMij bij een escalatie in de samenwerking (zie [Samenwerkings- en escalatiebeleid](#));
- Verzoeken tot handhaving, meldingen van misstanden of afwijkingen en klachten ([Klachten- en geschillenbeleid](#));
- De test bij de erkenning van een deelnemer als ontsluiter van een gegevensdienst (zie [Testbeleid](#));
- Bij de implementatie van een nieuwe release van het stelsel (zie [Change- en releasebeleid](#));
- De jaarlijkse aanlevering van bewijsmateriaal voor de NEN 7510-certificering en de toepassing voor MedMij (zie [Normenkader informatiebeveiliging](#)).

Het handhaven van de afspraken verloopt langs privaatrechtelijke lijnen. Bij signalering van niet-naleving worden daarom de volgende stappen doorlopen:

1. **Constatering en vastlegging.** Stichting MedMij beschrijft zo concreet mogelijk welke verplichting van het MedMij Afsprakenstelsel het betreft, alsmede wat de concrete omstandigheden van het geval zijn. Voorbeelden van aanleidingen voor constatering zijn:
  - a. het verlopen van de geldigheidsduur van de testresultaten van de *Deelnemer*;
  - b. het aanmelden van een entry voor op de *OAuthClientList* in relatie waarmee de *Dienstverlener* persoon niet (geheel) erkend is;
  - c. het aanmelden van een entry voor op de *Zorgaanbiederslijst* in relatie waarmee de *Dienstverlener* zorgaanbieder niet (geheel) erkend is;
2. **Verificatie en verzoek om nadere toelichting.** De constatering van de niet-naleving wordt schriftelijk voorgelegd aan de desbetreffende deelnemer. De deelnemer dient hierop te reageren en aan te geven welke maatregelen binnen welke termijn worden getroffen om de niet-naleving op te lossen;
3. **Beoordeling nadere toelichting van deelnemer en communicatie besluit.** Op basis van de ontvangen informatie beoordeelt Stichting MedMij of, gelet op de aard en de ernst van de verplichting die niet wordt nageleefd, de door de deelnemer voorgestelde maatregelen en het benodigde tijdbestek passend zijn. Hierbij worden de criteria gehanteerd die ook worden gehanteerd bij het bepalen van de redelijke termijn bij een formele ingebrekestelling (zie hieronder). Indien de niet-naleving de veilige en betrouwbare werking van het netwerk in het geding brengen, dan kan Stichting MedMij beslissen om de overeenkomst tijdelijk op te schorten (zoals overeengekomen in artikel 7.3 van de deelnemersovereenkomst). De deelnemer wordt schriftelijk geïnformeerd over de beoordeling;
4. **Formele ingebrekestelling.** De formele ingebrekestelling is de laatste aanmaning om te voldoen aan de niet-naleving en geschiedt schriftelijk;

5. **Formele beëindiging deelnemersovereenkomst.** Nadat de termijn is verstreken die in de ingebrekestelling is opgenomen, is de deelnemer in verzuim. Op dat moment kan de deelnemersovereenkomst door Stichting MedMij worden ontbonden.

Tijdens elk van deze stappen kan door Stichting MedMij worden geconstateerd dat er ofwel geen sprake (meer) is van niet-naleving, ofwel dat er voldoende zicht is op naleving. Indien er geen sprake (meer) is van niet-naleving, dan wordt de procedure beëindigd. Bij voldoende zicht op naleving, wordt nog vinger aan de pols gehouden.

De tenuitvoerlegging van het nalevingsbeleid is een zaak van Stichting MedMij. Besluiten over opschorting of uitsluiting van deelname lopen via Stichting MedMij.

Stichting MedMij gaat vertrouwelijk om met dossiers aangaande lopende en afgesloten nalevingszaken. Besluiten over opschorting en uitsluiting van deelname zijn daarentegen openbaar.

## Formele ingebrekestelling

De ingebrekestelling is een schriftelijke sommatie waarin de deelnemer door Stichting MedMij wordt gesommeerd een voor hem geldende verplichting uit het MedMij Afsprakenstelsel, binnen een bepaalde termijn, na te komen. De ingebrekestelling is de laatste mogelijkheid die de deelnemer wordt geboden om de niet-naleving op te heffen. Indien de gestelde termijn wordt overschreden is de deelnemer in verzuim. Op het moment dat de deelnemer in verzuim is, kan de overeenkomst door Stichting MedMij worden ontbonden.

In de wet is niet aangegeven wat onder een redelijke termijn wordt verstaan, alleen dat een redelijke termijn moet worden gesteld. Of een bepaalde termijn redelijk is, wordt uiteindelijk bepaald door de rechter, gelet op de concrete omstandigheden van het geval. Voor Stichting MedMij betekent dit dat per geval voor de desbetreffende deelnemer, gelet op de verplichting die hij niet nakomt, moet worden bepaald wat een haalbare termijn is om de desbetreffende verplichting alsnog na te komen. De criteria die Stichting MedMij hanteert in haar afweging bij het bepalen van een redelijke termijn zijn:

- de kans dat het vertrouwen in het merk MedMij wordt geschaad;
- de kans dat de niet-naleving (imago)schade voor het merk MedMij oplevert;
- de kans dat de niet-naleving (imago)schade voor de overige deelnemers in het MedMij Afsprakenstelsel oplevert;
- de kans dat het afsprakenstelsel MedMij als geheel beveiligingsrisico's loopt;
- de gangbare doorlooptijd voor een bepaalde actie;
- of, en zo ja, welke ((inter)nationale) afspraken er worden gehanteerd voor de invoering /implementatie van een bepaalde actie.

## OAuthclient-namenbeleid

Binnen de OAuth-flow wordt aan de Persoon toestemming gevraagd voor de gegevensuitwisseling tussen een Zorgaanbieder en de OAuthclient van de Dienstverlener persoon (zie [Toestemmingsverklaring](#)). Om in de bijbehorende toestemmingsverklaring een gebruiksvriendelijke naam voor de OAuthclient te kunnen presenteren, is de OAuth Client List in het leven geroepen. Met deze lijst kan de Dienstverlener zorgaanbieder de gebruiksvriendelijke naam van de OAuthclient vinden en gebruiken in de toestemmingsverklaring.

Het OAuthclient-namenbeleid beschrijft hoe een Dienstverlener persoon een voor de persoon herkenbare naam kiest, zonder dat door een te grote variëteit aan namen voor de Persoon onduidelijkheid ontstaat over de toestemming.

### Wie kiest de OAuthclient-naam?

De Dienstverlener persoon bepaalt de gekozen naam en geeft deze door aan Stichting MedMij. Stichting MedMij stelt de naam vast.

### Waar moet de OAuthclient-naam aan voldoen?

1. De naam moet gelijk zijn aan een handelsnaam van de Dienstverlener persoon, zoals opgenomen in het handelsregister;
2. De naam is minimaal drie en maximaal 50 karakters lang;
3. De naam mag niet te herleiden zijn tot een persoon;
4. De naam mag het merk MedMij niet negatief beïnvloeden.

## Performancebeleid

De totale performance van het MedMij-netwerk hangt af van de individuele prestaties van deelnemers en *MedMij Registratie*. Aangezien de persoon binnen MedMij de regie voert over de uitwisseling van gegevens, initieert de *Dienstverlener persoon* bij de use cases [UC Verzamelen](#) en [UC Delen](#) de interacties en reageert de Dienstverlener zorgaanbieder. Om die reden zijn er afspraken opgenomen over de beschikbaarheid en reactietijd van Dienstverleners zorgaanbieder (zie [Token interface](#) en [Resource interface](#)). Bij de overige use cases voor het opvragen van de lijsten initiëren deelnemers en reageert MedMij Registratie. Er zijn daarom ook afspraken opgenomen over de beschikbaarheid van MedMij Registratie (zie [GNL-](#), [OCL-](#) en [ZAL-interface](#)).

Mochten deelnemers bij elkaar constateren dat de performance achterblijft of dat er fouten ontstaan in de onderlinge interacties, dan wordt van hen naar redelijkheid verwacht dat ze inspanning verrichten om dit onderling aanhangig te maken en te kijken of het daarmee opgelost kan worden. Stichting MedMij kan hierbij faciliteren en mediëren (zie ook [Samenwerkings- en escalatiebeleid](#)). Deelnemers gebruiken alle aanwezige logging, tevens naar redelijkheid, om een probleem te helpen oplossen.

### Toelichting

Om fouten in de eerste productieversie van het stelsel tijdig op te sporen, organiseert Stichting MedMij een platform om fouten op te sporen en op te lossen. Deelnemers leveren hieraan actief een bijdrage.

Mochten de prestaties van een deelnemer achterblijven en/of een deelnemer toont onvoldoende inzet om problemen op te lossen, dan treedt het [Nalevingsbeleid](#) in werking.

## Privacy- en informatiebeveiligingsbeleid

Aangezien gezondheidsgegevens van personen erg privacygevoelige gegevens zijn, zijn privacy en informatiebeveiliging belangrijke thema's binnen MedMij. De privacy en informatieveiligheid is, in aanvulling op de wet- en regelgeving die per definitie van toepassing is op de deelnemer, op drie manieren geborgd in het stelsel:

- Door de gegevensuitwisseling tussen deelnemers in hoge mate van detail te beschrijven en belangrijke maatregelen op het gebied van privacy en informatiebeveiliging hierin op te nemen (zie de [Architectuur en technische specificaties](#));
- Door strenge eisen te stellen aan de privacy en informatiebeveiliging van deelnemers in het eigen domein (zie het [Normenkader informatiebeveiliging](#));
- Door onder verantwoordelijkheid van Stichting MedMij aanvullende procedures in te richten, zoals de toetsing van deelnemers op het nakomen van de (privacy- en informatiebeveiligings)afspraken bij toetreding en gedurende deelname (zie onder andere [Toetredingsbeleid](#) en [Nalevingsbeleid](#)).

Stichting MedMij voert de regie over het in kaart brengen van privacy- en informatiebeveiligingsrisico's die individuele deelnemers overstijgen (stelselrisico's) en doet voorstellen voor maatregelen. Hiervoor vindt jaarlijks een [Risicoanalyse](#) plaats. Ook wordt, indien de aard, omvang of context van de gegevensuitwisselingen over het MedMij-netwerk of direct daaraan gerelateerde verwerkingen significant verandert, opnieuw een Privacy Impact Assessment (PIA) uitgevoerd. Op basis van deze risicoanalyse en/of PIA worden maatregelen heroverwogen en eventueel aanvullende privacy- en informatiebeveiligingsmaatregelen gedefinieerd. Dit kan resulteren in bijstelling van het [Normenkader informatiebeveiliging](#) en de [Architectuur en technische specificaties](#). Er wordt getracht (nieuwe) afspraken zoveel mogelijk aan te laten sluiten bij eisen van andere stelsels en hergebruik van bestaande certificeringen mogelijk te maken om de implementatie-, financiële en administratieve lasten voor deelnemers zoveel mogelijk beperkt te houden.

Samen met de deelnemers wordt ook op andere wijze toegezien op de privacy en informatiebeveiliging van het stelsel. Stichting MedMij en elke afzonderlijke deelnemer wijzen ieder een verantwoordelijke voor privacy en informatiebeveiliging aan (zie [Normenkader informatiebeveiliging](#) en tussen deze verantwoordelijken is minimaal vier keer per jaar overleg. Hieromheen is een incidenten- en calamiteitenprocedure en een proces beheren technische kwetsbaarheden ingericht, zodat duidelijk is wat er van de verschillende partijen wordt verwacht in noodsituaties (zie [Operationele processen](#)). Deelnemers zijn verantwoordelijk voor het doorgeven van de juiste contactpersoon en informeren Stichting MedMij bij wijzigingen.

Ten slotte zorgt Stichting MedMij verder voor afstemming over privacy en veiligheid met bestaande partijen en ontwikkelingen in de zorg en worden de belangrijkste ontwikkelingen in de wereld op dit gebied gevolgd.

## Risicoanalyse

Stichting MedMij voert elk jaar in samenspraak met deelnemers aan het MedMij Afsprakenstelsel een risicoanalyse uit. De risicoanalyse richt zich op informatieveiligheidsrisico's. Dit zijn risico's die kunnen leiden tot inbreuken op de beschikbaarheid, integriteit of vertrouwelijkheid van informatie. Compliance aan wet- en regelgeving is geen onderdeel van deze risicoanalyse (bijv. compliance m.b.t. NEN7512). Het betreft hier een risicoanalyse op stelselniveau, dat wil zeggen dat het de risico's betreft in de onderlinge relatie tussen de betrokken partijen en niet de specifieke analyse bij een betrokken partij. Het onderwerp van de risicoanalyse betreft daarmee wel alle onderdelen van het MedMij Afsprakenstelsel. Dit houdt in dat de maatregelen voortkomend uit de analyse betrekking (kunnen) hebben op de Dienstverlener persoon, Dienstverlener zorgaanbieder en Stichting MedMij. Personen en zorgaanbieders (de gebruikers) zijn geen onderdeel van het afsprakenstelsel en vallen buiten de scope van de risicoanalyse. Er kunnen wel maatregelen voor de risico's worden voorgesteld aan de Dienstverlener persoon of de Dienstverlener zorgaanbieder die van invloed kunnen zijn op de Persoon of Zorgaanbieder.

De risicoanalyse wordt, op grond van het [Informatieclassificatiebeleid](#), niet publiekelijk beschikbaar gesteld.

### Uitgangspunten bij de risicoanalyse

1. De scope van de risicoanalyse wordt voor het belangrijkste gedeelte bepaald door de [Grondslagen](#), met name in de [Criteria](#) en de [Principes](#). Op basis hiervan worden uitspraken gedaan over beschikbaarheid, vertrouwelijkheid en integriteit van de informatie binnen scope van het afsprakenstelsel;
2. De risicoanalyse wordt uitgevoerd op basis van de ten tijde van uitvoering laatst gepubliceerde release van het MedMij Afsprakenstelsel. Nieuwe of aangepaste maatregelen worden meegenomen in een nieuwe release van het afsprakenstelsel;
3. In de analyse is een vertegenwoordiging van alle rollen in het afsprakenstelsel en de governance betrokken;
4. Voldoen aan geldende wet- en regelgeving is een startpunt voor alle partijen en een vereiste in de definitie van maatregelen;
5. Het bestuur van Stichting MedMij streeft naar een voor de betrokken partijen aanvaardbaar risiconiveau aan de hand van de impact op de volgende onderwerpen: gezondheid, privacy, financieel, imago en vertrouwen. Stichting MedMij bepaalt met betrokken wat dit aanvaardbare risiconiveau is. De risicoanalyse, de risicotolerantie en beveiligingsmaatregelen worden vastgesteld door Stichting MedMij.

## Maatregelen

De risicoanalyse leidt tot het formuleren van drie typen maatregelen:

1. Maatregelen die direct betrekking hebben op risico's voor de werking en veiligheid van het stelsel en daarom uniform dienen te worden vastgesteld (bijv. onderlinge autorisatieprotocollen);
2. Maatregelen voor risico's die kunnen leiden tot stelselrisico's (een gebeurtenis bij een deelnemer die schade toebrengt aan andere deelnemers of Stichting MedMij). Deze zijn gespecificeerd in het stelsel om eenduidige interpretatie af te dwingen (bijv. toegang tot persoonlijke gezondheidsgegevens);
3. Maatregelen die vanuit efficiëntieoogpunt zijn opgenomen in het stelsel zodat niet iedere partij deze afzonderlijk hoeft te definiëren.

De geformuleerde maatregelen kunnen op verschillende manieren worden opgenomen in het afsprakenstelsel. Er kunnen [technische specificaties](#) worden geformuleerd voor deelnemers, [Beleid](#) en [Operationele processen](#) worden vormgegeven, dan wel normen in het [Normenkader informatiebeveiliging](#) worden opgenomen.

## Verwerking in de afsprakenset

Uit de overkoepelende risicoanalyse op het afsprakenstelsel die is uitgevoerd op release 1.0, is geconcludeerd dat een NEN 7510-certificering voor deelnemers en beheerorganisatie in samenhang met de overige onderdelen van het toetredingsproces, zoals kwalificatie en acceptatie, de belangrijkste informatiebeveiligingsrisico's voor het stelsel afdekt. Op een aantal onderwerpen zijn maatregelen uit de NEN 7510-norm meer specifiek ingevuld voor MedMij of zijn er aanvullende maatregelen voorgesteld. Het betreft onderwerpen waarbij is geconcludeerd dat een ingeschat risico het beste afgedekt kan worden door voor alle partijen een uniforme maatregel te treffen, in plaats van zelfstandig maatregelen te kiezen op basis van een eigen risico inschatting. Of het gaat om onderwerpen waarbij de individuele inschatting gevolgen kan hebben voor andere partijen in het netwerk. Deze maatregelen zijn opgenomen in het [Normenkader informatiebeveiliging](#). Daarnaast zijn maatregelen uit de risicoanalyse op stelselniveau opgenomen in de architectuur en technische specificaties of het beleid en operationele processen. De uitvoering van deze maatregelen wordt getoetst via onder andere het toetredingsproces.

NEN 7510-certificering is gangbaar en wettelijk verplicht bij de gegevensuitwisseling in het zorgaanbiedersdomein. Om voor de uitwisseling met dienstverleners in het persoonsdomein zoveel mogelijk aan te sluiten bij de bestaande gebruiken en certificeringen, is gekozen de NEN 7510 ook verplicht te stellen voor de Dienstverlener persoon. De NEN 7510 kent het vertrouwen van partijen in het zorgaanbiedersdomein en draagt zo bij aan de acceptatie van het stelsel. Het bezitten van een ISO 27001-certificering, de internationale standaard waarop de NEN 7510 is gebaseerd, is voor deelname aan het MedMij Afsprakenstelsel onvoldoende.

## Herijking risicoanalyse

De risicoanalyse is een product dat jaarlijks dient te worden herijkt, maar ook wanneer er bepaalde wijzigingen plaatsvinden. De risicoanalyse dient te worden herijkt op het moment dat:

- wijzigingen in het afsprakenstelsel worden gemaakt die van invloed kunnen zijn op de risicoanalyse;
- wanneer zich incidenten met aanzienlijke impact hebben voorgedaan;
- er bekende wijzigingen zijn in het dreigingslandschap voor MedMij;
- er significante technische wijzigingen zijn in de werking van het stelsel;
- er wijziging is van wetgeving waar MedMij aan moet voldoen;
- een van de uitgangspunten (zie hieronder) wordt gewijzigd.



## Samenwerkings- en escalatiebeleid

Deelnemers vormen met elkaar het MedMij-netwerk. Om een optimale beschikbaarheid van dit netwerk te kunnen waarborgen, zijn deelnemers van elkaar afhankelijk. Van deelnemers wordt daarom verwacht dat zij onderling samenwerken.

Om deze samenwerking te faciliteren, vullen deelnemers en Stichting MedMij (voor de dienst MedMij Registratie) de volgende rollen in:

- Een servicemanager als eindverantwoordelijke voor de dienstverlening voor MedMij;
- Een servicedesk bestaande uit minimaal één persoon als dagelijks aanspreekpunt voor de beheerorganisatie en andere deelnemers.

Om daarnaast te voorkomen dat vragen van gebruikers onnodig bij andere deelnemers, Stichting MedMij of zorgaanbieders terecht komen, dienen deelnemers ook de volgende rol in te vullen:

- Een gebruikers-helpdesk bestaande uit minimaal één persoon als dagelijks aanspreekpunt voor gebruikers.

Deelnemers maken bij Stichting MedMij kenbaar hoe de servicedesk, de servicemanager en de gebruikers-helpdesk te bereiken zijn. Deelnemers en Stichting MedMij registreren en publiceren deze contactgegevens, voor de eerste maal tijdens het toetredingsproces, in een online samenwerkingsplatform.

Servicedeskmedewerkers van de verschillende deelnemers mogen in de dagelijkse operatie een beroep op elkaar doen. Korte lijnen moeten ervoor zorgen dat verstoringen en/of problemen bij de dienstverlening van een deelnemer of bij de dienst MedMij Registratie zo snel mogelijk bij de servicedesk van de betreffende partij bekend zijn en de dienstverlening zo spoedig mogelijk kan worden hersteld.

Mochten er problemen ontstaan in de onderlinge samenwerking, dan kunnen servicedeskmedewerkers escaleren naar hun eigen servicemanager. Deze servicemanager bemiddelt vervolgens met de overige betrokken servicemanagers. Samen beslissen zij hoe de escalatie opgeheven wordt en de normale procesgang wordt hervat.

Indien de servicemanagers er onderling niet uitkomen, dan biedt Stichting MedMij het escalatiekanaal. Namens en samen met de escalerende partijen zal zij bemiddelen om een oplossing te vinden en tijdelijk toezien op de procesgang (totdat het normale proces kan worden hervat). Mocht ook deze bemiddeling niet slagen, dan beschrijft het [Klachten- en geschillenbeleid](#) de escalatieroutes buiten het stelsel.

## Testbeleid

Om de interoperabiliteit en het vertrouwen in het stelsel te borgen, dienen deelnemers aan te tonen de [Architectuur en technische specificaties](#) en de *Gegevensdiensten* die zij ontsluiten op de juiste manier te ondersteunen. De deelnemer doorloopt bij toetreding en tijdens deelname testen. De testen bepalen of de deelnemer voldoende geëquipeerd is om de afspraken uit de architectuur en technische specificaties waar te maken en de gegevensdiensten op de juiste manier te gebruiken. Stichting MedMij toetst niet de volledige implementatie, maar richt zich op risico's, interoperabiliteit tussen deelnemers en cruciale maatregelen voor het vertrouwen in MedMij.

De testresultaten hebben een beperkte geldigheidsduur van 365 dagen vanaf het positief doorlopen van de test.

Bij het aanvragen en inplannen van de hernieuwde test stelt de *Deelnemer* in overleg met de beheerorganisatie vast tegen welke actieve versie van het MedMij Afsprakenstelsel de test zal worden uitgevoerd (zie [Change- en releasebeleid](#)).

Wanneer moet er getest worden? We onderscheiden de volgende situaties:

1. De *Deelnemer* wil erkend worden als ontsluiter van een *Gegevensdienst*;
2. Hertest op initiatief van de *Deelnemer*, omdat de geldigheidsduur van diens testresultaten dreigt te verlopen.
3. Twijfel over de naleving van de afspraken;
4. Hertoeetreding als bedoeld in artikel 14.3 van de Deelnemersovereenkomst.

### Situatie 1: De deelnemer wil erkend worden als ontsluiter van een gegevensdienst

In situatie 1 moet op grond van het [Gegevensdienstenbeleid](#) worden aangetoond dat: (A) de relevante use cases uit de Architectuur en technische specificaties, (B) de algemene verantwoordelijkheden uit de Architectuur en technische specificaties en (C) de systeemrollen uit de *Gegevensdienst* goed worden ondersteund.

Voor (A) geldt het volgende schema:

Usecase(s) behorende bij de <i>Gegevensdienst</i>	Scope van de test (relevante use cases)	
	<i>Dienstverlener</i> persoon	<i>Dienstverlener</i> zorgaanbieder
Verzamelen	<a href="#">UCI Verzamelen</a> <a href="#">UCI Opvragen ZAL</a> <a href="#">UCI Opvragen GNL</a>	<a href="#">UCI Verzamelen</a> <a href="#">UCI Opvragen OCL</a> <a href="#">UCI Opvragen GNL</a>
Delen	<a href="#">UCI Delen</a> <a href="#">UCI Opvragen ZAL</a> <a href="#">UCI Opvragen GNL</a>	<a href="#">UCI Delen</a> <a href="#">UCI Opvragen OCL</a> <a href="#">UCI Opvragen GNL</a>
Abonneren	<a href="#">UCI Abonneren</a>	<a href="#">UCI Abonneren</a>

De UCI's moeten worden beschouwd inclusief de bijbehorende verantwoordelijkheden op de [Processen en informatie](#)-laag, de overige relevante verantwoordelijkheden op de [Applicatie](#)-laag, de bijbehorende verantwoordelijkheden op de [Netwerk](#)-laag en de formele regels in de relevante [Informatiemodellen](#).

Onder (B) wordt verstaan: de verantwoordelijkheden op de [Netwerk](#)-laag, inclusief de [UCI Opvragen WHL](#).

Voor (C) geldt dat in de [Catalogus](#) te vinden is welke Informatiestandaard bij een *Gegevensdienst* hoort en in het Register van Informatiestandaarden bij de *Informatiestandaard* vervolgens is opgenomen waar de ondersteuning van de *Systeemrollen* kan worden aangetoond. De test op de *Systeemrollen* vindt plaats in een opstelling die afwijkt van de productiesituatie. Het streven is om de toets in deze opstelling met zo min mogelijk aanvullende inspanningen van de deelnemer te kunnen doen. Aanvullende technische inspanning blijft echter nodig. Deelnemers committeren zich via hun deelname aan het afsprakenstelsel aan deze inspanningen. [Informatie over kwalificatie](#) kan worden gevonden bij de beheerder van de betreffende informatiestandaard.

De deelnemer kan zich voorbereiden op testen (A) en (B) in een testomgeving aangeboden door Stichting MedMij. Voor test (C) kan de deelnemer zich voorbereiden in de testomgeving van de partij die deze toets verzorgt. Voor (A) en (B) geldt verder dat eerdere positieve testen voor een UCI of de algemene verantwoordelijkheden niet opnieuw behoeven te worden uitgevoerd als de deelnemer erkend wil worden als ontsluiter van een nieuwe gegevensdienst.

## Situatie 2

De beperking van de geldigheidsduur van de testresultaten wordt begrepen als onderdeel van het [Nalevingsbeleid](#). Wanneer de geldigheid van de testresultaten verloopt, dreigt opschorting van de Deelnemersovereenkomst, in het kader van artikel 7, lid 3. Het verlopen van de testresultaten wordt gezien als één van de wijzen waarop niet-naleving geconstateerd wordt.

*Deelnemers* zijn zelf verantwoordelijk voor het laten plannen van de testen voor het herbevestigen van de geldigheid van hun implementatie, voordat de geldigheid van bestaande testresultaten verloopt. Daarbij stelt de *Deelnemer* in overleg met de beheerorganisatie vast tegen welke actieve versie van het MedMij Afsprakenstelsel de test zal worden uitgevoerd (zie [Change- en releasebeleid](#)).

Bij het succesvol doorlopen van de hertest zijn de nieuwe testresultaten opnieuw 365 dagen geldig.

### Situatie 2

Het testbeleid wil eraan bijdragen dat *Deelnemers* een voorspelbare ontwikkelkalender voor hun implementatie kunnen hanteren, afgestemd op de regelmatige releasemomenten van het MedMij Afsprakenstelsel (zie [Change- en releasebeleid](#)) en de hertesten.

## Situaties 3 en 4

In situaties 3 en 4 wordt per geval bekeken wat er opnieuw getest moet worden. De geldigheid van eerdere positieve testresultaten kunnen in deze situaties vervallen.

## Zorgaanbiedersnamenbeleid

*Zorgaanbieders* kunnen hun deelname en de manier waarop ze via MedMij te bereiken zijn aan *Personen* kenbaar maken via een *Zorgaanbiedersnaam* (*zorgaanbiedersnaam@medmij*). Het zorgaanbiedersnamenbeleid beschrijft hoe een *Zorgaanbieder* een voor de *Persoon* herkenbare naam kan kiezen, zonder in de toekomst de mogelijkheden van andere *Zorgaanbieders* om een herkenbare naam te kiezen te veel te beperken.

Het is de *Zorgaanbieder* die zijn *Zorgaanbiedersnaam* kiest, maar de *Dienstverlener zorgaanbieder* die de *Zorgaanbiedersnaam* aanreikt aan de MedMij Beheerorganisatie voor gebruik in de *Zorgaanbiederslijst*. Daarbij moet de *Dienstverlener zorgaanbieder* een verklaring van de *Zorgaanbieder* kunnen overleggen. Deze verklaring is opgenomen onder het Registratieproces *Zorgaanbiederslijst* op de pagina [Operationele processen](#).

## Rollen inzake de *Zorgaanbiedersnaam*

De *Zorgaanbiedersnaam*:

- wordt gekozen door de *Zorgaanbieder*, als verwerkingsverantwoordelijke, voor het specifieke doel om *Gegevensdiensten* aan te bieden over het MedMij-netwerk;
- wordt vastgesteld door de Stichting MedMij, die daartoe onderstaande kwaliteitseisen verifieert;
- wordt door MedMij niet gebonden aan enige *Gegevensdienst*, maar het is betreffende *Zorgaanbieder* gegeven dat wel te doen;
- is niet gebonden aan de *Dienstverlener zorgaanbieder*. De *Dienstverlener zorgaanbieder* informeert *Zorgaanbieders* wel over de context, het doel en het beleid inzake *Zorgaanbiedersnamen* in MedMij;
- wordt door een *Dienstverlener zorgaanbieder* verwerkt en, in het bijzonder, gehanteerd wanneer hij in opdracht van een *Zorgaanbieder* een *Gegevensdienst* wil laten opnemen op, of afvoeren van, de *Zorgaanbiederslijst*;
- wordt op het MedMij-netwerk niet verbonden aan enig ander kenmerk, adres of identificatie van de *Zorgaanbieder*. De verantwoordelijkheid voor zijn portfolio aan adressen (voor verschillende communicatiekanalen) en identificaties (voor verschillende doelen) ligt bij de *Zorgaanbieder* zelf.

## Eisen aan de *Zorgaanbiedersnaam*

1. De naam moet gekoppeld zijn aan de naam die de zorgaanbieder in andere communicatie gebruikt (niet: *stichtingtersamenwerkinghuisartsenoegstgeest@medmij*, wel: *huisartsensamenwerkingoegstgeest@medmij*);
2. De naam mag niet al voorkomen of sterk lijken op een naam die al geregistreerd is;
3. De naam mag niet ambigu zijn en op veel verschillende zorgaanbieders kunnen slaan (niet: *huisartshaarlem@medmij*, wel: *huisartswestergrachthaarlem@medmij*);
4. De naam mag niet de naam van een deelnemer bevatten of anderszins aan een specifieke deelnemer gekoppeld zijn;
5. De naam eindigt altijd op @medmij;
6. De naam is minimaal drie en maximaal 280 karakters lang (exclusief @medmij);
7. De naam wordt geregistreerd (ook in de *Zorgaanbiederslijst*) in het volgende formaat:
  - a. een reeks van één of meer segmenten, gescheiden door
    - i. hetzij één koppelteken,
    - ii. hetzij één ampersand,
    - iii. hetzij één punt;
  - b. gevolgd door @medmij, waarin
  - c. elk segment een reeks van één of meer fragmenten is, zodanig dat
  - d. elk fragment bestaat uit een reeks, met een minimale lengte van één karakter, van
    - i. kleine letters uit het Nederlandse alfabet (bestaande uit de zesentwintig letters a . . z) en /of

- ii. Arabische cijfers (0 . . 9).
- 8. Van de naam mogen, buiten de registratie, varianten voorkomen waarin een kleine letter is vervangen door de corresponderende hoofdletter en/of diakritische varianten van letters voorkomen. Deze lettervarianten worden echter als identiek gezien aan de kleine basisletter. De naam is dus niet hoofdletter-gevoelig en evenmin diacriet-gevoelig.
- 9. De naam mag niet te herleiden zijn tot een persoon;
- 10. De naam mag in het verleden niet door een andere zorgaanbieder gebruikt zijn;
- 11. De naam mag het merk MedMij niet negatief beïnvloeden.

### Het formaat van de Zorgaanbiedersnaam

Het formaat van de *Zorgaanbiedersnaam* benadert dat van de handelsnaam uit het Handels-register. Dat is nastrevenswaardig omdat doel en aard van de *Zorgaan-bie-dersnaam*tijken op die van de handelsnaam.

Met betrekking tot de diakritische tekens is niet zozeer het voorkomen ervan een probleem, maar wel het onderscheidend vermogen tussen verschillende accenten op, aan of onder dezelfde basisletter. Het is geautomatiseerde systemen weliswaar gegeven om woltgens van wöltgens te onderscheiden, mondhygiënist van mondhygienist en hélène van helène, maar dat geldt niet voor (vooral PGO-)gebruikers die *Zorgaanbiedersnamen* handmatig zullen willen intypen. Dat laatste moet mogelijk zijn, omdat een arts bijvoorbeeld op een kaartje of een kladje zijn *Zorgaanbiedersnaam* aan een patiënt zou kunnen meege-ven. In die zin lijkt een *Zorgaanbiedersnaam* op een e-mailadres. Een snel gemaakte fout met een diakritisch teken moet niet even snel tot de adressering van een onbedoelde *Zorgaanbieder* leiden.

Met betrekking tot cijfers is het om vergelijkbare redenen zaak te voorkomen dat te lange reek-sen (volg)nummers ontstaan. Daarom mogen er maximaal vier achtereenvolgende cijfers voorkomen.

Het koppelteken, de ampersand en de punt kunnen een belangrijke functie vervullen in de herken-baar-heid van de *Zorgaanbiedersnaam*, maar een reeks van dergelijke tekens achter elkaar amper.

*Zorgaanbiedersnamen* worden dus in kleine letters en zonder diakritische tekens geregistreerd en in de *Zorgaanbiederslijst* opgenomen, maar mogen in wíLlëKrîgE diakri-tische en hoofdlettervarianten worden aangegeven.

Zie voor de reguliere expressie van de basisklasse *Zorgaanbiedersnaam* de pagina over de [XML-schema's](#).

## Operationele processen

### Doel

Naast de use cases, zijn ook een aantal operationele processen in het afsprakenstelsel opgenomen. Deze processen spelen niet direct een rol in de gegevensuitwisseling, maar zijn wel nodig voor een goede operationele werking van het stelsel. Operationele processen geeft op hoofdlijnen een overzicht van de belangrijkste beheerprocessen waarbij deelnemers een rol spelen. Het overzicht is niet uitputtend. Detailuitwerkingen van deze processen zijn beschikbaar voor (potentiële) deelnemers.

## Incidenten- en calamiteitenproces

- **Doel:** Het incidenten- en calamiteitenproces heeft als doel MedMij-gerelateerde incidenten en calamiteiten op gestructureerde wijze af te handelen. Daarbij dient de dienstverlening zo min mogelijk te worden verstoord.
- **Initiatie:** Deelnemer en/of Stichting MedMij constateert een incident/calamiteit.
- **Afspraken over het proces:**
  - In de nadere uitwerking van het proces wordt gedefinieerd wat een incident en calamiteit is in het kader van MedMij. De procesafspraken hebben hier betrekking op.
  - Deelnemers en Stichting MedMij zijn verplicht elkaar te informeren over alle incidenten en calamiteiten die de operationele werking van het netwerk beïnvloeden ([Deelnemersovereenkomsten](#), artikel 5: privacy en (informatie)beveiliging).
  - Deelnemers en Stichting MedMij dienen zo spoedig mogelijk de benodigde acties uit te zetten om een incident of calamiteit op te lossen.
  - Stichting MedMij kan bij calamiteiten besluiten een operationeel team samen te stellen en de deelnemer vragen onderdeel te worden van dit team. Deelnemers dienen hieraan mee te werken.
  - Deelnemers en Stichting MedMij hebben allen één persoon binnen de eigen organisatie aangewezen als eindverantwoordelijke en centraal contactpersoon voor informatiebeveiligingsincidenten en -calamiteiten (zie [A. 6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging](#)).
  - Communicatie van de deelnemer over incidenten en calamiteiten in het kader van MedMij worden afgestemd met Stichting MedMij (waar dit niet de wettelijke verplichting betreft).
- **Resultaat:** Incident en/of calamiteit is opgelost door de betrokkenen.
- **Uitzonderingen:** -

## Proces beheren technische kwetsbaarheden

- **Doel:** Het proces beheren technische kwetsbaarheden heeft als doel om kwetsbaarheden in het stelsel tijdig te identificeren en op te lossen.
- **Initiatie:** *Deelnemer* en/of Stichting MedMij constateert een kwetsbaarheid.
- **Afspraken over het proces:**
  - *Deelnemers* en Stichting MedMij zijn verplicht elkaar te informeren over voor MedMij relevante kwetsbaarheden.
  - Stichting MedMij draagt zorg voor een centraal proces voor het signaleren en delen van kwetsbaarheden. In het proces zijn termijnen verbonden aan het oplossen van de kwetsbaarheden.
  - Uitwisseling van informatie over kwetsbaarheden vindt plaats met extra bescherming (zie [Informatieclassificatiebeleid](#)).
  - *Deelnemers* dienen in staat te zijn tijdig te reageren op meldingen van kwetsbaarheden in het MedMij Afsprakenstelsel ([A.12.6.1 Beheer van technische kwetsbaarheden](#)).

- **Resultaat:** Kwetsbaarheid is onderzocht en, waar nodig, verholpen door de betrokkenen.
- **Uitzonderingen:** -

## Proces erkenning van *Deelnemer* als ontsluiter van *Gegevensdienst*

- **Doel:** Het proces erkenning van *Deelnemer* als ontsluiter van *Gegevensdienst* heeft als doel te toetsen of de *Deelnemer* een *Gegevensdienst* op de juiste wijze ondersteunt.
- **Initiatie:** *Deelnemer* wil een *Gegevensdienst* ontsluiten.
- **Afspraken over het proces:**
  - *Deelnemer* levert bewijs aan voor het succesvol doorlopen van toetsing op de relevante *Systeemrollen* uit de bij de *Gegevensdienst* horende *Informatiestandaard* (zie [Testbeleid](#) en [Catalogus](#)).
  - Stichting MedMij bepaalt of aanvullende toetsing op functionaliteit uit de [Architectuur en technische specificaties](#) benodigd is. Indien het geval, dan dient de *Deelnemer* de ondersteuning van de aanvullende functionaliteit middels een toets te laten zien (zie [Testbeleid](#)).
  - Stichting MedMij bepaalt of *Deelnemer* eerst erkend moet worden als ontsluiter van andere *Gegevensdiensten*, omdat de *Gegevensdienst* dit vereist (zie [Gegevensdienstenbeleid](#)). Indien het geval, dan dient eerst de erkenning als ontsluiter van de vereiste *Gegevensdienst* behaald te worden.
- **Resultaat:** *Deelnemer* is erkend als ontsluiter van een *Gegevensdienst*. Stichting MedMij initieert het Registratieproces ontsluiting *Gegevensdiensten* door deelnemer.
- **Uitzonderingen:** *Deelnemer* voldoet niet aan de vereisten voor de *Gegevensdienst* en wordt niet erkend als ontsluiter.

## Proces vernieuwing erkenning van *Deelnemer*

- **Doel:** Het proces vernieuwing erkenning van *Deelnemer* heeft als doel om periodiek te herbevestigen dat de implementatie van een *Deelnemer* nog steeds aan het MedMij Afsprakenstelsel voldoet.
- **Initiatie:**
  - De geldigheidsduur van de testresultaten van een *Deelnemer* dreigt te verlopen.
  - *Deelnemer* draagt een entry aan voor opname op de *OAuthClientList* of *Zorgaanbiederslijst* in relatie waarmee *Deelnemer* nog niet (geheel) erkend is.
- **Afspraken over het proces:**
  - Stichting MedMij bepaalt, in overleg met *Deelnemer*, op welke onderdelen van het MedMij Afsprakenstelsel *Deelnemer* een hernieuwde test moet ondergaan. Het doel daarbij is om *Deelnemer* ten minste te laten voldoen aan de verplichte (zie [Change- en releasebeleid](#)) release van het MedMij Afsprakenstelsel.
  - Wanneer *Deelnemer* de hertest met goed gevolg doorstaat, zijn de testresultaten opnieuw 365 dagen geldig.
  - Wanneer *Deelnemer* de hertest niet doorstaat, bepaalt Stichting MedMij of daarom ontbinding of opschorting van de *Deelnemersovereenkomst* aan de orde is.
  - Stichting MedMij is verantwoordelijk voor het doorvoeren van de benodigde mutaties in het deelnemersregister, naar aanleiding van de resultaten van de hertest.
- **Afspraken over het proces:** Voorzover *Deelnemer* voldoet aan het MedMij Afsprakenstelsel, is diens deelname voor de komende 365 dagen bestendig.
- **Uitzonderingen:** -

## Registratieproces ontsluiting *Gegevensdiensten* door *Deelnemer*

- **Doel:** Het registratieproces ontsluiting *Gegevensdiensten* door *Deelnemer* heeft als doel de juiste informatie vast te leggen over de ontsluiting van *Gegevensdiensten* door de *Deelnemer*.
- **Initiatie:**
  - *Deelnemer* is erkend voor een *Gegevensdienst* en mag deze aanbieden.



- *Deelnemer* wil een *Gegevensdienst* niet meer ontsluiten.
- *Deelnemer* mag een *Gegevensdienst* niet meer ontsluiten op grond van falende herkwalificatie of -acceptatie.
- **Afspraken over het proces:**
  - Stichting MedMij is verantwoordelijk voor het doorvoeren van de benodigde mutaties in het deelnemersregister.
  - Mutaties zijn gebonden aan de verantwoordelijkheden en regels zoals gespecificeerd in de [Architectuur en technische specificaties](#).
- **Resultaat:** Stichting MedMij heeft het deelnemersregister en de overige relevante lijsten aangepast. De *Deelnemer* wordt geïnformeerd over de doorgevoerde wijziging.
- **Uitzonderingen:** -

## Registratieprocessen *Zorgaanbiederslijst*, *Whitelist* en *OAuthclientlist*

- **Doel:** De registratieprocessen voor de *Zorgaanbiederslijst*, *Whitelist* en *OAuthclientlist* hebben als doel de juiste informatie te verzamelen benodigd voor een goede operationele werking van het stelsel.
- **Initiatie:**
  - *Deelnemer* dient een verzoek in bij Stichting MedMij om een entry in de *Zorgaanbiederslijst*, *Whitelist* of *OAuthclientlist* aan te maken, te wijzigen of te verwijderen.
  - Triggers voor wijzigingen zijn per lijst verschillend:
    - *Zorgaanbiederslijst:*
      - *Dienstverlener zorgaanbieder* wil in het MedMij-netwerk kenbaar maken een *Gegevensdienst* namens een *Zorgaanbieder* te ontsluiten.
      - *Dienstverlener zorgaanbieder* wil in het MedMij-netwerk kenbaar maken een *Gegevensdienst* namens een *Zorgaanbieder* niet meer te ontsluiten.
      - *Dienstverlener zorgaanbieder* wil een endpoints bij een *ZorgaanbiederGegevensdienst* wijzigen.
    - *Whitelist:*
      - *Deelnemer* wil een node op het MedMij-netwerk gebruiken.
      - *Deelnemer* wil een van haar eigen nodes niet meer op het MedMij-netwerk gebruiken.
    - *OAuthclientlist:*
      - *Dienstverlener persoon* wil een *OAuthclient* toevoegen.
      - *Dienstverlener persoon* wil een *OAuthclient* verwijderen.
- **Afspraken over het proces:**
  - *Deelnemer* is verantwoordelijk voor het aanleveren van mutaties voor de *Zorgaanbiederslijst*, *WhiteList* en *OAuthclientlist*.
  - Bij het kenbaar maken van het ontsluiten van een *Gegevensdienst* voor een *Zorgaanbieder* overlegt de *Dienstverlener zorgaanbieder* de volgende verklaring van de *Zorgaanbieder*:  
"Ik, [*Zorgaanbieder*], verklaar onder de *Zorgaanbiedersnaam* [*Zorgaanbiedersnaam*] *Gegevensdienst* [*GegevensdienstId*] aan te willen bieden op het MedMij-netwerk, vanaf [*ingangsdatum*] en deze te laten ontsluiten door [*Dienstverlener zorgaanbieder*]."
  - Mutaties zijn gebonden aan de verantwoordelijkheden en regels zoals gespecificeerd in de [Architectuur en technische specificaties](#), het [Zorgaanbiedersnamenbeleid](#) en [OAuthclient-namenbeleid](#).
  - Stichting MedMij neemt het verzoek in behandeling en is verantwoordelijk voor een check op integriteit.
  - Valide mutaties worden in 95 procent van de gevallen door Stichting MedMij binnen 2 werkdagen verwerkt. Urgente mutaties krijgen daarbij voorrang. De mutatietijd voor urgente mutaties wordt in overleg met Stichting MedMij bepaald. Bij verwachte overschrijding van de (overeengekomen) verwerkingstijd, informeert Stichting MedMij de deelnemer hierover.
- **Resultaat:** Stichting MedMij heeft het betreffende register aangepast. De deelnemer wordt geïnformeerd over de doorgevoerde wijziging.
- **Uitzonderingen:** Een van de verantwoordelijkheden en regels in de [Architectuur en technische specificaties](#) wordt overtreden. Stichting MedMij vraagt de deelnemer om het verzoek aan te passen.



## Actualiseren van *Zorgaanbiederslijst* en de *OAuthClientList* bij publicatie nieuwe release

- **Doel:** Borgen dat in de *Zorgaanbiederslijst* en de *OAuthclientlist* alleen *Interfaceversies* voorkomen van actieve releases van het MedMij Afsprakenstelsel.
- **Initiatie:**
  - Er komt een nieuwe release uit van het MedMij Afsprakenstelsel. Dat wil zeggen dat de tot dan toe verplichte release de status *verouderd* krijg.
- **Afspraken over het proces:**
  - *MedMij Beheer* is verantwoordelijk voor het verwijderen van alle entries in de *Zorgaanbiederslijst* en de *OAuthClientList* die horen bij een (zou) verouderde *Interfaceversie*.
- **Resultaat:** Stichting MedMij heeft de betreffende lijsten aangepast.
- **Uitzondering:** Geen.

## Managementinformatieproces

- **Doel:** Het managementinformatieproces heeft als doel de verschillende stakeholders van informatie te voorzien over het gebruik van MedMij.
- **Initiatie:** Proces wordt geïnitieerd door de klok.
- **Afspraken over het proces:**
  - *Deelnemers* zijn verantwoordelijk voor het aanleveren van [Managementinformatie](#).
  - Stichting MedMij zorgt voor de verwerking van de gegevens tot een geaggregeerde rapportage. Concurrentiegevoelige informatie wordt hierbij zoveel mogelijk verborgen.
- **Resultaat:** Een geaggregeerde rapportage voor de betrokkenen.
- **Uitzonderingen:** *Deelnemer* levert de benodigde managementinformatie niet aan. Stichting MedMij verzoekt de *Deelnemer* alsnog de benodigde informatie aan te leveren. Mocht een *Deelnemer* (herhaaldelijk) in gebreke blijven, dan treedt het [Nalevingsbeleid](#) in werking.

## Uittredingsproces

- **Doel:** Het uittredingsproces heeft als doel een deelnemer op gestructureerde wijze en met oog voor de belangen van de verschillende stakeholders uit te laten treden.
- **Initiatie:**
  - Deelnemer wil uittreden uit het afsprakenstelsel.
  - *Deelnemer* dient uit te treden uit het afsprakenstelsel.
- **Afspraken over het proces:**
  - De belangrijkste verwachtingen van *Deelnemers* bij uittreding staan beschreven in de [Deelnemersovereenkomsten](#) (Artikel 7: Opschorting en beëindiging).
  - Stichting MedMij voert de benodigde mutaties door in het deelnemersregister en de relevante lijsten.
- **Resultaat:** *Deelnemer* is uitgetreden uit het afsprakenstelsel.
- **Uitzonderingen:** -

## Processen inzake gecontroleerde livegang

### Start van een gecontroleerde livegang

- **Doel:** Het in de gelegenheid stellen van een groep *Deelnemers* tot het uitvoeren van een gecontroleerde livegang conform [Beleid inzake gecontroleerde livegang](#).
- **Initiatie:** Minstens één *Zorgaanbieder*, minstens één *Dienstverlener zorgaanbieder* en minstens één *Dienstverlener persoon* willen samen een gecontroleerde livegang uitvoeren voor één *Gegevensdienst*. De bedoelde *Dienstverleners* moeten gekwalificeerd zijn voor die *Gegevensdienst*.

- **Afspraken over het proces:**
  - Gecontroleerde livegangen mogen alleen worden uitgevoerd op de dan verplichte release en bijbehorende *Interfaceversie*. Dit kan de looptijd van de gecontroleerde livegang beperken tot het eerstvolgende releasemoment van het MedMij Afsprakenstelsel.
  - De MedMij Beheerorganisatie creëert een kopie-*Gegevensdienst* van de beoogde *Gegevensdienst* en voegt deze toe aan de *Catalogus* met een geldigheidstermijn zoals gewenst door de betrokkenen, maar voldoende aan het [Beleid inzake gecontroleerde livegang](#).
  - De MedMij Beheerorganisatie voegt de kopie-*Gegevensdienst* toe aan de *Gegevensdienstnamenlijst*, onder dezelfde *Weergavenaam* als de origineel-*Gegevensdienst*.
  - Voor elk van de betrokken *Zorgaanbieders* en *Dienstverleners* persoon wordt het proces 'Toetreding tot een gecontroleerde livegang' uitgevoerd.
- **Resultaat:** De gecontroleerde livegang is operationeel, tenzij gedurende de uitvoering van het proces en zijn deelprocessen niet aan eisen blijkt te zijn voldaan.
- **Uitzonderingen:** -

### Toetreding tot een gecontroleerde livegang

- **Doel:** Het in de gelegenheid stellen van een *Zorgaanbieder* (desgewenst met diens *Dienstverlener zorgaanbieder*) of *Dienstverlener* persoon toe te treden tot een bestaande gecontroleerde livegang conform [Beleid inzake gecontroleerde livegang](#).
- **Initiatie:** Een *Zorgaanbieder* (desgewenst met diens *Dienstverlener zorgaanbieder*) of *Dienstverlener* persoon wenst toe te treden tot een gecontroleerde livegang. De betreffende *Dienstverlener* moet gekwalificeerd zijn voor de origineel-*Gegevensdienst* van de gecontroleerde livegang. De *Zorgaanbieder* mag in de afgelopen drie maanden niet al betrokken zijn geweest bij een gecontroleerde livegang op deze origineel-*Gegevensdienst*.
- **Afspraken over het proces:**
  - De MedMij Beheerorganisatie erkent de betreffende *Dienstverlener* op de kopie-*Gegevensdienst*, indien deze is gekwalificeerd op de origineel-*Gegevensdienst*.
  - Betrokken *Dienstverlener* laat zich inzake de kopie-*Gegevensdienst* op gebruikelijke wijze registreren in de *Zorgaanbiederslijst*, de *OAuth Client List* en de *Whitelist*.
- **Resultaat:** De betreffende partij is operationeel in de gecontroleerde livegang, tenzij niet aan de toepasselijke eisen is voldaan.
- **Uitzonderingen:** -

### Uittreding uit een gecontroleerde livegang

- **Doel:** Het in de gelegenheid stellen van een *Zorgaanbieder* (desgewenst met diens *Dienstverlener zorgaanbieder*) of *Dienstverlener* persoon uit te treden uit een bestaande gecontroleerde livegang conform [Beleid inzake gecontroleerde livegang](#).
- **Initiatie:** Een *Zorgaanbieder* (desgewenst met diens *Dienstverlener zorgaanbieder*) of *Dienstverlener* persoon wenst uit te treden uit een gecontroleerde livegang. Bij een *Zorgaanbieder* kan dat gepaard gaan met een wens tot promotie tot het gewone live MedMij-netwerk.
- **Afspraken over het proces:**
  - De MedMij Beheerorganisatie beëindigt de erkenning van betreffende *Dienstverlener* op de kopie-*Gegevensdienst*.
  - De MedMij Beheerorganisatie verwijdert de op de betreffende partij betrekking hebbende elementen uit de *Zorgaanbiederslijst*, de *OAuth Client List* en de *Whitelist*.
  - Indien het een *Zorgaanbieder* betreft die wens te promoveren, start de MedMij Beheerorganisatie het proces 'Promotie uit een gecontroleerde livegang'.
  - Mocht de uitreder de laatste *Zorgaanbieder*, *Dienstverlener zorgaanbieder* of *Dienstverlener* persoon zijn in de gecontroleerde livegang, start hij het proces 'Beëindiging van een gecontroleerde livegang'.
- **Resultaat:** De betreffende partij is niet meer operationeel in de gecontroleerde livegang.
- **Uitzonderingen:** -

## Promotie uit een gecontroleerde livegang

- **Doel:** Het live gaan van een *Zorgaanbieder*, met diens *Dienstverlener zorgaanbieder*, in het MedMij-netwerk, vanuit een gecontroleerde livegang, conform [Beleid inzake gecontroleerde livegang](#).
- **Initiatie:** Een *Zorgaanbieder* (met diens *Dienstverlener zorgaanbieder*) geven bij uitreding uit de gecontroleerde livegang aan te willen promoveren.
- **Afspraken over het proces:**
  - De MedMij Beheerorganisatie vervangt in de *Zorgaanbiederslijst* die elementen die betrekking hebben op de betreffende *Zorgaanbieder*-kopie-*Gegevensdienst*-combinaties de kopie-*Gegevensdienst* door de origineel-*Gegevensdienst*.
- **Resultaat:** De betreffende *Zorgaanbieder* is live met de betreffende *Gegevensdienst*.
- **Uitzonderingen:** -

## Beëindiging van een gecontroleerde livegang

- **Doel:** Het beëindigen van de gelegenheid van een groep *Deelnemers* tot het uitvoeren van een gecontroleerde livegang conform [Beleid inzake gecontroleerde livegang](#).
- **Initiatie:** Wanneer één van de volgende gebeurtenissen zich voordoet:
  - de looptijd van de kopie-*Gegevensdienst* verstrijkt, al dan niet na een eenmalige verlenging;
  - de laatste *Zorgaanbieder*, *Dienstverlener zorgaanbieder* of *Dienstverlener persoon* treedt uit uit de gecontroleerde livegang;
  - Stichting MedMij oordeelt dat enige bij de gecontroleerde livegang betrokken partij voordelen ontleent of beoogt te ontfangen aan de gecontroleerde livegang die niet in overeenstemming zijn met de bedoeling van gecontroleerde livegangen.
- **Afspraken over het proces:**
  - De MedMij Beheerorganisatie beëindigt de geldigheid van de kopie-*Gegevensdienst*.
  - De MedMij Beheerorganisatie verwijdert de kopie-*Gegevensdienst* uit de *Gegevensdienstnamenlijst*. De kopie-*Gegevensdienst* wordt nooit meer opnieuw gebruikt.
  - De MedMij Beheerorganisatie verwijdert de erkenning van betrokken *Dienstverleners* op de kopie-*Gegevensdienst*.
  - De MedMij Beheerorganisatie verwijdert op betrokken kopie-*Gegevensdienst* betrekking hebbende elementen uit de *Zorgaanbiederslijst* en de *OAuth Client List*.
  - Betrokken partijen verwijderen eventuele op hen betrekking hebbende elementen uit de *Whitelist*, voor zover zij die niet ook gebruiken buiten deze gecontroleerde livegang.
- **Resultaat:** De gecontroleerde livegang is niet meer operationeel.
- **Uitzonderingen:** -

## Communicatie

Communicatie beschrijft de afspraken over het [Merkgebruik](#) en het hanteren van de verplichte [Gebruikersvoorlichting](#), [Toestemmingsverklaring](#) en [Bevestigingsverklaring](#).

## Merkgebruik

Persoonlijke gezondheidsomgevingen en zorginformatiesystemen kennen vele vormen. De afspraken set houdt rekening met deze diversiteit en maakt het mogelijk om met een relatief beperkte afspraken set uitwisseling tussen deze systemen vorm te geven. MedMij heeft niet als doel om met de afspraken set uniformiteit van deze systemen te realiseren. Integendeel zelfs, MedMij omarmt de diversiteit en gelooft dat alleen zo de verschillende gebruikers goed kunnen worden bediend.

Dit uitgangspunt heeft consequenties voor de betekenis van het merk. MedMij staat vooral symbool voor de veilige en betrouwbare gegevensuitwisseling van gezondheidsgegevens tussen deelnemers aan het stelsel. Het merk is geen keurmerk voor de volledige functionaliteit of dienstverlening van een PGO of aan een zorgaanbieder. Gebruikers in de verschillende domeinen weten door de toepassing van het merk dat ze de gegevensuitwisseling tussen deelnemers kunnen vertrouwen en dat gegevens op een plek terecht komen waar de privacy en informatiebeveiliging voldoende is gewaarborgd.

Het gebruik van het merk kent in praktijk drie doelen, namelijk:

1. Herkenbaarheid voor de persoon;
2. Profilerings van de deelnemer (waaronder herkenbaarheid voor de zorgaanbieder);
3. Herkenbaarheid communicatie vanuit MedMij.

Het gebruik van het merk bij deze doelen wordt hieronder nader uitgewerkt.

### Doel 1: Herkenbaarheid voor de persoon

Het merk MedMij speelt voor de persoon een belangrijke rol bij het herkennen van partijen waarmee gezondheidsgegevens op een veilige en betrouwbare wijze kunnen worden uitgewisseld. De persoon moet bijvoorbeeld een Dienstverlener persoon kunnen uitzoeken die aan de MedMij-afspraken voldoet en ook zijn /haar zorgaanbieder moet kunnen laten weten uitwisseling via MedMij te ondersteunen. Het merk MedMij mag dan ook voor dit doeleinde worden gebruikt door de Dienstverlener persoon en door Zorgaanbieders (waarvoor Dienstverleners zorgaanbieder ZorgaanbiederGegevensdiensten ontsluiten).

De Dienstverlener persoon mag zowel in de persoonlijke gezondheidsomgeving zelf als in de communicatie daaromheen het merk gebruiken. In het systeem moet in ieder geval voor de persoon zichtbaar zijn wanneer sprake is van gegevens(uitwisseling) via MedMij. Het merk moet daarom aan de eindgebruiker gepresenteerd worden bij:

- Het tonen van de mogelijkheid om gegevens uit te wisselen via MedMij;
- Het tonen van de gezondheidsgegevens verkregen via MedMij.

Het recht om als aangesloten zorgaanbieder het merk te mogen voeren, volgt niet uit de rechtsrelaties in het stelsel. Dit wordt daarom geregeld met een licentietekst op de [MedMij-website](#).

### Doel 2: Profilerings van de deelnemer

Deelnemers mogen het merk hanteren om naar anderen te laten zien te voldoen aan de afspraken. Zo kan de Dienstverlener zorgaanbieder bijvoorbeeld met het merk aan de Zorgaanbieder kenbaar maken gegevensuitwisseling via MedMij aan te bieden.

### Doel 3: Herkenbaarheid communicatie vanuit MedMij

De beheerorganisatie gebruikt het merk voor de herkenbaarheid van de eigen communicatie. Ook gebruikt zij het merk bij communicatieproducten waarvan zij uitgever is, zoals bij de gebruikersvoorlichting.

## Uitingsvormen van het merk

Een consistente toepassing van het merk draagt bij aan de waarde hiervan. Deelnemers en Zorgaanbieders mogen het merk uiten met het MedMij-label of met een tekstuele verwijzing naar MedMij. Er zijn twee versies van het MedMij-label:



In principe maken Deelnemers en Zorgaanbieders gebruik van het MedMij-label met payoff. Mocht de payoff onleesbaar worden door het design, dan mag gebruik worden gemaakt van het MedMij-label zonder payoff.

Voor de herkenbaarheid van de communicatie vanuit MedMij, is verdergaand gebruik van de huisstijl in principe voorbehouden aan de beheerorganisatie. Dit geldt ook voor het MedMij-logo, zoals gebruikt door Stichting MedMij en de uitvoeringsorganisatie. Mocht een deelnemer communicatie nader willen laten aansluiten bij deze MedMij-huisstijl, dan vindt hierover altijd afstemming plaats met de beheerorganisatie. Geeft de beheerorganisatie toestemming voor verdergaand gebruik, dan is er een huisstijlhandleiding beschikbaar met daarin onder meer afspraken over kleurgebruik en opmaak.

Voor de waarde van het merk MedMij is het verder belangrijk dat partijen op een zelfde wijze communiceren over de boodschap van dit merk. Hiervoor zijn basistekstelementen beschikbaar bij de beheerorganisatie. Deze dienen ter inspiratie en mogen worden gebruikt in de eigen communicatie.

## Gebruikersvoorlichting

De Gebruikersvoorlichting bevat antwoorden op een aantal veelgestelde vragen die belangrijk zijn voor het vertrouwen in MedMij. De gebruikersvoorlichting heeft als doel het vertrouwen van zowel personen als zorgaanbieders in de digitale gegevensuitwisseling via MedMij te vergroten. Richting de Persoon wordt de Gebruikersvoorlichting persoonsdomein en richting de Zorgaanbieder de Gebruikersvoorlichting zorgaanbiedersdomein gehanteerd. Deelnemers aan het MedMij Afsprakenstelsel zijn middels de [Deelnemersovereenkomsten](#) verplicht om de MedMij-gebruikersvoorlichting aan hun gebruikers voor te leggen. Ook dienen zij bij nieuwe versies de gebruikersvoorlichting opnieuw aan hun gebruikers voor te leggen.

De gebruikersvoorlichting is vormgegeven in de MedMij-huisstijl en dient door deelnemers in deze vorm aan de gebruiker te worden voorgelegd. Het is toegestaan de gebruikersvoorlichting zowel in papieren als digitale vorm met de gebruiker te delen. De gebruikersvoorlichting moet tevens via de website van de deelnemer te vinden zijn door een link op te nemen naar de gebruikersvoorlichting op de MedMij-website. De bestanden met de gebruikersvoorlichting worden bij toetreding tot het stelsel en bij wijziging van de voorlichting met de deelnemer gedeeld.

## Toestemmingsverklaring

De toestemmingsverklaring en de toelichting daarop zijn verplichte teksten die de *Dienstverlener zorgaanbieder* dient voor te leggen aan de *Persoon* bij het ophalen van gezondheidsgegevens bij de *Zorgaanbieder*. Deze toestemmingsverklaring heeft betrekking op die gegevensuitwisseling. De verplichte toestemmingsverklaring volgt uit de Wet geneeskundige behandelingsovereenkomst (WGBO). De *Zorgaanbieder* is verplicht ervoor te zorgen dat 'anderen' dan de patiënt geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van het medisch dossier, tenzij hiervoor toestemming is verleend. Binnen de MedMij afspraken verstrekt de *Zorgaanbieder* via de *Dienstverlener zorgaanbieder* gegevens aan de *Dienstverlener persoon*. Aangezien dit een 'andere' is dan de *Persoon* zelf, moet de *Zorgaanbieder* weten dat de persoon hiervoor toestemming heeft verleend. Bij de [UC Verzamelen](#) en de [UC Abonneren](#) staat beschreven hoe het proces rondom het geven van toestemming eruit ziet. De *Dienstverlener zorgaanbieder* implementeert de toestemmingsverklaring en toont deze aan de *Persoon*.

### Toestemmingsverklaring

U geeft hierbij NaamZorgaanbieder toestemming om NaamGegevensdienst uit te wisselen met NaamLeverancierPGO voor het doel deze persoons- en gezondheidsgegevens op te nemen in uw persoonlijke gezondheidsomgeving.

### Toelichting op de toestemmingsverklaring

Het doel van het MedMij Afsprakenstelsel is dat eenieder die dat wil, kan beschikken over een Persoonlijke Gezondheidsomgeving (PGO) waarin - onder uw eigen regie - (persoons)gegevens en/of informatie over uw gezondheid wordt opgenomen. Om de PGO te voorzien van de door u gewenste (persoons)gegevens en/of gezondheidsinformatie zijn in het MedMij Afsprakenstelsel afspraken gemaakt over de uitwisseling van deze gegevens. Het uitwisselen van gegevens tussen de zorgaanbieder en uw PGO verloopt zodoende via partijen die voldoen aan deze MedMij-afspraken.

Op grond van de Wet geneeskundige behandelingsovereenkomst (WGBO) is de zorgaanbieder verplicht ervoor te zorgen dat 'anderen' dan de patiënt (lees: u) geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van uw medisch dossier, *tenzij u hiervoor toestemming heeft verleend*.

Aangezien uw PGO (en eventuele achterliggende partij die werkt volgens de MedMij-afspraken) een zogenaamde 'andere' is (in de zin van de WGBO) dient u de zorgaanbieder voor deze gegevensuitwisseling toestemming te verlenen. Deze toestemming heeft specifiek betrekking op de set van (persoons) gegevens en gezondheidsinformatie die, op uw verzoek, door de zorgaanbieder - overeenkomstig de afspraken in het MedMij Afsprakenstelsel - worden uitgewisseld met uw PGO.

## Verplicht toestemmingsscherm

De toestemmingsverklaring en de toelichting zijn onderdeel van onderstaand verplichte toestemmingsscherm. De *Dienstverlener zorgaanbieder* dient de variabelen op dit scherm te vullen volgens verantwoordelijkheid 1a op de pagina [User interface \(verklaringen\)](#). De HTML- en CSS-bestanden om het scherm te kunnen gebruiken, zijn als bijlage toegevoegd aan deze pagina ([medmij-toestemmingen-en-bevestiging.zip](#)). Deze bestanden beschrijven enkel de tekst en vormgeving van het scherm. De *Dienstverlener zorgaanbieder* blijft verantwoordelijk voor alle overige aspecten, zoals beveiliging van de webpagina. Het is toegestaan zinnen of elementen toe te voegen aan het scherm om te voldoen aan eventuele voorwaarden van een Authenticatieprovider. Dit mag niet ten koste gaan van de focus op de toestemming.





U geeft hierbij **NaamZorgaanbieder** toestemming om  
**NaamGegevensdienst** uit te wisselen met  
**NaamLeverancierPGO** voor het doel deze persoons- en  
gezondheidsgegevens op te nemen in uw persoonlijke  
gezondheidsomgeving.

✓ Ja, ik geef toestemming

Nee, ik geef geen toestemming

☐ Toon toelichting



U geeft hierbij **NaamZorgaanbieder** toestemming om  
**NaamGegevensdienst** uit te wisselen met  
**NaamLeverancierPGO** voor het doel deze persoons- en  
gezondheidsgegevens op te nemen in uw persoonlijke  
gezondheidsomgeving.

✓ Ja, ik geef toestemming

Nee, ik geef geen toestemming

☒ Toon toelichting

Het doel van het MedMij Afsprakenstelsel is dat eenieder die dat wil, kan beschikken over een Persoonlijke Gezondheidsomgeving (PGO) waarin - onder uw eigen regie - (persoons)gegevens en/of informatie over uw gezondheid wordt opgenomen. Om de PGO te voorzien van de door u gewenste (persoons)gegevens en/of gezondheidsinformatie zijn in het MedMij Afsprakenstelsel afspraken gemaakt over de uitwisseling van deze gegevens. Het uitwisselen van gegevens tussen de zorgaanbieder en uw PGO verloopt zodoende via partijen die voldoen aan deze MedMij-afspraken.

## Toestemmingsverklaring Abonneren

Deze toestemmingsverklaring en de toelichting daarop zijn verplichte teksten die de *Dienstverlener zorgaanbieder* dient voor te leggen aan de *Persoon* bij het tot stand brengen van een *Abonnement* op gezondheidsgegevens (*Notificaties*) bij de *Zorgaanbieder*. Deze toestemmingsverklaring heeft betrekking op die gegevensuitwisseling. De verplichte toestemmingsverklaring volgt uit de Wet geneeskundige behandelingsovereenkomst (WGBO). De *Zorgaanbieder* is verplicht ervoor te zorgen dat 'anderen' dan de patiënt geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van het medisch dossier, tenzij hiervoor toestemming is verleend. Binnen het MedMij Afsprakenstelsel verstrekt de *Zorgaanbieder* door middel van de *Dienstverlener zorgaanbieder* gegevens aan de *Dienstverlener persoon*. Aangezien dit een 'andere' is dan de *Persoon* zelf, moet de *Zorgaanbieder* weten dat de persoon hiervoor toestemming heeft verleend. Bij de [UC Abonneren](#) staat beschreven hoe het proces rondom het geven van toestemming eruit ziet. De *Dienstverlener zorgaanbieder* implementeert de toestemmingsverklaring en toont deze aan de *Persoon*.

### Toestemmingsverklaring

U geeft hierbij NaamZorgaanbieder toestemming om, gedurende ten hoogste Duur dagen, meldingen over NaamGegevensdienst te doen bij NaamLeverancierPGO voor het doel deze persoons- en gezondheidsgegevens op te nemen in uw persoonlijke gezondheidsomgeving.

De looptijd is mogelijk beperkt door NaamZorgaanbieder.

### Toelichting op de toestemmingsverklaring

Het doel van het MedMij Afsprakenstelsel is dat eenieder die dat wil, kan beschikken over een Persoonlijke Gezondheidsomgeving (PGO) waarin - onder uw eigen regie - (persoons)gegevens en/of informatie over uw gezondheid wordt opgenomen. Om de PGO te voorzien van de door u gewenste (persoons)gegevens en/of gezondheidsinformatie zijn in het MedMij Afsprakenstelsel afspraken gemaakt over de uitwisseling van deze gegevens. Het uitwisselen van gegevens tussen de zorgaanbieder en uw PGO verloopt zodoende via partijen die voldoen aan deze MedMij-afspraken.

Op grond van de Wet geneeskundige behandelingsovereenkomst (WGBO) is de zorgaanbieder verplicht ervoor te zorgen dat 'anderen' dan de patiënt (lees: u) geen inlichtingen hebben over, inzage hebben in of een afschrift hebben van uw medisch dossier, *tenzij u hiervoor toestemming heeft verleend*.

Aangezien uw PGO (en eventuele achterliggende partij die werkt volgens de MedMij-afspraken) een zogenaamde 'andere' is (in de zin van de WGBO) dient u de zorgaanbieder voor deze gegevensuitwisseling toestemming te verlenen. Deze toestemming heeft specifiek betrekking op de set van (persoons) gegevens en gezondheidsinformatie die, op uw verzoek, door de zorgaanbieder - overeenkomstig de afspraken in het MedMij Afsprakenstelsel - worden uitgewisseld met uw PGO.

## Verplicht toestemmingsscherm

De toestemmingsverklaring en de toelichting zijn onderdeel van onderstaand verplichte toestemmingsscherm. De *Dienstverlener zorgaanbieder* dient de variabelen op dit scherm te vullen volgens verantwoordelijkheid 1a op de pagina [User interface \(verklaringen\)](#). De HTML- en CSS-bestanden om het scherm te kunnen gebruiken, zijn als bijlage toegevoegd aan deze pagina ([medmij-toestemmingen-en-bevestiging.zip](#)). Deze bestanden beschrijven enkel de tekst en vormgeving van het scherm. De *Dienstverlener zorgaanbieder* blijft verantwoordelijk voor alle overige aspecten, zoals beveiliging van de webpagina. Het is toegestaan zinnen of elementen toe te voegen aan het scherm om te voldoen aan eventuele voorwaarden van een Authenticatieprovider. Dit mag niet ten koste gaan van de focus op de toestemming.



U geeft hierbij **NaamZorgaanbieder** toestemming om, gedurende ten hoogste **Duur** dagen, meldingen over **NaamGegevensdienst** te doen bij **NaamLeverancierPGO** voor het doel deze persoons- en gezondheidsgegevens op te nemen in uw persoonlijke gezondheidsomgeving.

De looptijd is mogelijk beperkt door **NaamZorgaanbieder**.

✓ Ja, ik geef toestemming

Nee, ik geef geen toestemming

☐ Toon toelichting



U geeft hierbij **NaamZorgaanbieder** toestemming om, gedurende ten hoogste **Duur** dagen, meldingen over **NaamGegevensdienst** te doen bij **NaamLeverancierPGO** voor het doel deze persoons- en gezondheidsgegevens op te nemen in uw persoonlijke gezondheidsomgeving.

De looptijd is mogelijk beperkt door **NaamZorgaanbieder**.

✓ Ja, ik geef toestemming

Nee, ik geef geen toestemming

☒ Toon toelichting

Het doel van het MedMij Afsprakenstelsel is dat eenieder die dat wil, kan beschikken over een Persoonlijke Gezondheidsomgeving (PGO) waarin - onder uw eigen regie - (persoons)gegevens en/of informatie over uw gezondheid wordt opgenomen. Om de PGO te voorzien van de door u gewenste (persoons)gegevens en/of gezondheidsinformatie zijn in het MedMij Afsprakenstelsel afspraken gemaakt over de uitwisseling van deze gegevens. Het uitwisselen van gegevens tussen de zorgaanbieder en uw PGO verloopt zodoende via partijen die voldoen aan deze MedMij-afspraken.

## Bevestigingsverklaring

De bevestigingsverklaring en de toelichting daarop zijn verplichte teksten die de *Dienstverlener zorgaanbieder* dient voor te leggen aan de *Persoon* bij het delen van gezondheidsgegevens met de *Zorgaanbieder*. Deze bevestigingsverklaring heeft betrekking op die gegevensuitwisseling. De verklaring is erop gericht om de *Persoon* te informeren over de voorgenomen uitwisseling van gegevens, en vast te stellen dat deze in overeenstemming met de wil van de *Persoon* plaatsvindt. Daarmee controleert de *Persoon* het verzoek dat de *Dienstverlener persoon* namens hem heeft gedaan voor het delen van een bepaald type gegevens (binnen een *Gegevensdienst*) met een specifieke *Zorgaanbieder*, voordat de *Dienstverlener zorgaanbieder* overgaat tot het autoriseren van de *Dienstverlener persoon* voor deze gegevensuitwisseling.

Bij de [UC Delen](#) staat beschreven hoe het proces rondom de bevestiging eruit ziet. De *Dienstverlener zorgaanbieder* implementeert de bevestigingsverklaring en toont deze aan de *Persoon*.

### Bevestigingsverklaring

U bevestigt hierbij dat `NaamLeverancierPGO` `NaamGegevensdienst` mag delen met `NaamZorgaanbieder`. De zorgaanbieder beoordeelt of hij deze informatie opneemt in uw medisch dossier en/of gebruikt voor uw behandeling.

### Toelichting op de bevestigingsverklaring

U heeft aangegeven uw persoonsgegevens en/of informatie over uw gezondheid met uw zorgaanbieder `NaamZorgaanbieder` te willen uitwisselen.

`NaamZorgaanbieder` verzoekt u te bevestigen dat u uw persoonsgegevens en/of gezondheidsinformatie van het type `NaamGegevensdienst` met hem wenst te delen. Na uw bevestiging stuurt uw zorgaanbieder een bericht naar de leverancier van uw persoonlijke gezondheidsomgeving (`NaamLeverancierPGO`). Hij zorgt er dan voor dat de informatie die u wenst te delen vanuit uw persoonlijke gezondheidsomgeving via MedMij aan uw zorgaanbieder wordt toegezonden. Het is aan `NaamZorgaanbieder` om te beoordelen of hij de informatie die u met hem deelt ook opneemt in uw medisch dossier.

## Verplicht bevestigingsscherm

De bevestigingsverklaring en de toelichting zijn onderdeel van een verplicht bevestigingsscherm. De *Dienstverlener zorgaanbieder* dient de variabelen op dit scherm te vullen volgens verantwoordelijkheid 1b op de pagina [User interface \(verklaringen\)](#). De HTML- en CSS-bestanden om het scherm te kunnen gebruiken, zijn als bijlage toegevoegd aan deze pagina ([medmij-toestemmingen-en-bevestiging.zip](#)). Deze bestanden beschrijven enkel de tekst en vormgeving van het scherm. De *Dienstverlener zorgaanbieder* blijft verantwoordelijk voor alle overige aspecten, zoals beveiliging van de webpagina. Het is toegestaan zinnen of elementen toe te voegen aan het scherm om te voldoen aan eventuele voorwaarden van een Authenticatieprovider. Dit mag niet ten koste gaan van de focus op de bevestiging.



U bevestigt hierbij dat **NaamLeverancierPGO**  
**NaamGegevensdienst** mag delen met **NaamZorgaanbieder**. De  
zorgaanbieder beoordeelt of hij deze informatie opneemt in uw  
medisch dossier en/of gebruikt voor uw behandeling.

✓ Ja, ik bevestig

Nee, ik bevestig niet

☐ Toon toelichting



U bevestigt hierbij dat **NaamLeverancierPGO**  
**NaamGegevensdienst** mag delen met **NaamZorgaanbieder**. De  
zorgaanbieder beoordeelt of hij deze informatie opneemt in uw  
medisch dossier en/of gebruikt voor uw behandeling.

✓ Ja, ik bevestig

Nee, ik bevestig niet

☒ Toon toelichting

U heeft aangegeven uw persoonsgegevens en/of informatie over uw gezondheid met uw zorgaanbieder  
**NaamZorgaanbieder** te willen uitwisselen.

**NaamZorgaanbieder** verzoekt u te bevestigen dat u uw persoonsgegevens en/of gezondheidsinformatie van  
het type **NaamGegevensdienst** met hem wenst te delen. Na uw bevestiging stuurt uw zorgaanbieder een  
bericht naar de leverancier van uw persoonlijke gezondheidsomgeving (**NaamLeverancierPGO**). Hij zorgt er  
dan voor dat de informatie die u wenst te delen vanuit uw **FaceTime** gezondheidsomgeving via MedMij aan  
uw zorgaanbieder wordt toegezonden. Het is aan **NaamZorgaanbieder** om te beoordelen of hij de

## Notificatie van Zorggebruiker

Deze pagina bevat teksten die de *Dienstverlener persoon* dient voor te leggen aan de *Zorggebruiker* wanneer zij *Zorggebruiker* tekstueel op de hoogte stelt van de ontvangst van een *Notificatie* van de *Dienstverlener zorgaanbieder*, in het kader van [UC Notificeren](#).

Deze release van het afsprakenstelsel kent twee typen *Notificatie*:

1. inhoudelijke *Notificaties*, waarmee wordt aangegeven dat er nieuwe (gezondheids)informatie beschikbaar is gekomen bij een *Zorgaanbieder*. Deze *Notificaties* horen bij de hoofdfunctie [Uitwisseling](#);
2. abonnements-*Notificaties*, waarmee een bestaand *Abonnement* namens de *Zorgaanbieder* wordt beëindigd. Deze *Notificaties* horen bij de hoofdfunctie [Regie](#).

### Verplichte tekst voor inhoudelijke *Notificaties* — uitgebreide versie

Vanwege uw abonnement bij `NaamZorgaanbieder` op `NaamGegevensdienst`, zijn nieuwe gegevens voor u beschikbaar bij `NaamLeverancierPGO`.

### Verplichte tekst voor abonnements-*Notificaties* — uitgebreide versie

`NaamZorgaanbieder` heeft uw abonnement op `NaamGegevensdienst` via `NaamLeverancierPGO` beëindigd.

Wanneer de *Zorggebruiker* tekstueel wordt ingelicht over de *Notificatie*, wordt daarbij per default deze uitgebreide versies gebruikt, tenzij de kanalen via welke de *Notificatie* de *Zorggebruiker* bereikt onvoldoende veilig zijn om `NaamZorgaanbieder` en `NaamGegevensdienst` over te communiceren. Indien en alleen indien die veiligheid onvoldoende gewaarborgd is, worden de volgende korte versies gebruikt.

### Verplichte tekst voor inhoudelijke *Notificaties* — korte versie

Er zijn nieuwe gegevens voor u beschikbaar bij `NaamLeverancierPGO`.

### Verplichte tekst voor abonnements-*Notificaties* — korte versie

Eén van uw abonnementen via `NaamLeverancierPGO` is beëindigd.

## Managementinformatie

Om het gebruik van MedMij inzichtelijk te maken, leveren de *Dienstverleners persoon* en *Dienstverleners zorgaanbieder* maandelijks een *Beheerrapport* op aan bij Stichting MedMij. De informatie uit deze rapporten wordt geaggregeerd tot een managementrapportage voor de Stichting MedMij en de *Deelnemers*. Concurrentiegevoelige informatie wordt hierbij zoveel mogelijk weggehaald.

Aan de met de *Beheerrapporten* ontvangen informatie voegt Stichting MedMij informatie toe over het gebruik door *Zorgaanbieders*. Deze informatie wordt betrokken uit MedMij Registratie.

De betreffende informatie in opgenomen in het *metamodel* en een *logisch model* en wordt door de *Dienstverlener persoon* en *Dienstverlener zorgaanbieder* aangeleverd als XML-document conform het XML-schema zoals gespecificeerd op de pagina *XML-schema's*. Het betreft de volgende informatie.

	naam in het logische model	definitie voor de <i>Dienstverlener persoon</i>	definitie voor de <i>Dienstverlener zorgaanbieder</i>
algemeen	MedMijRapport.Deelnemer	de identificatie van de <i>Dienstverlener persoon</i>	de identificatie van de <i>Dienstverlener zorgaanbieder</i>
	MedMijRapport.Vanaf	begindatum en -tijdstip van de periode die de rapportage beslaat: altijd 00h00m00s van de eerste van een kalendermaand	begindatum en -tijdstip van de periode die de rapportage beslaat: altijd 00h00m00s van de eerste van een kalendermaand
	MedMijRapport.Tot	einddatum en -tijdstip van de periode die de rapportage beslaat: altijd 00h00m00s van de eerste van de kalendermaand die volgt op MedMijRapport.Vanaf	einddatum en -tijdstip van de periode die de rapportage beslaat: altijd 00h00m00s van de eerste van de kalendermaand die volgt op MedMijRapport.Vanaf
	MedMijRapport.Tijdstempel	datum en tijdstip van het moment waarop het rapport is aangemaakt	datum en tijdstip van het moment waarop het rapport is aangemaakt
personen	MedMijRapport.Beheerrapport.Personen.Aantal	het aantal unieke gebruikers (accounts) van de PGO van die <i>Dienstverlener persoon</i> ,	Dit element dient <b>niet</b> te worden aangeleverd.

		gedurende de rapportageperiode	
	MedMijRapport.Beheerrapport. Personen.AantalActiefSuccesvol	Aantal unieke gebruikers (Accounts) die in deze periode minimaal één request op een resource interface hebben verstuurd waarop een succesvolle resource respons werd ontvangen	Dit element dient <b>niet</b> te worden aangeleverd.
	MedMijRapport.Beheerrapport. Personen.AantalActiefOnsuccesvol	Aantal unieke gebruikers (Accounts) die in deze periode minimaal één request op een resource interface hebben verstuurd waarop een niet-succesvolle resource respons werd ontvangen	Dit element dient <b>niet</b> te worden aangeleverd.
per Gegevensdienst :	AuthorizationRequestNumbers. AantalSuccesvol	het aantal keren dat de <i>PGO Server</i> voor deze <i>Gegevensdienst</i> een authorization code heeft ontvangen ( <a href="#">UCI verzamelen stap 10</a> en <a href="#">11</a> , <a href="#">UCI Delen stap 13</a> en <a href="#">14</a> )	het aantal keren dat de <i>Authorization Server</i> voor deze <i>Gegevensdienst</i> een <a href="#">authorization request</a> heeft ontvangen waarop een succesvolle authorization response is uitgegaan
	AuthorizationRequestNumbers. AantalOnsuccesvol	Dit element dient <b>niet</b> te worden aangeleverd.	het aantal keren dat de <i>Authorization Server</i> voor deze <i>Gegevensdienst</i> een <a href="#">authorization request</a> heeft ontvangen waarop geen succesvolle authorization response is uitgegaan
	TokenRequestNumbers.	het aantal keren	het aantal keren



AantalSuccesvol	dat de <i>PGO Server</i> voor deze <i>Gegevensdienst</i> een <b>token request</b> heeft gedaan waarop een succesvolle authorization response is ontvangen	dat de <i>Authorization Server</i> voor deze <i>Gegevensdienst</i> een <b>token request</b> heeft ontvangen waarop een succesvolle authorization response is uitgegaan
TokenRequestNumbers. AantalOnsuccesvol	het aantal keren dat de <i>PGO Server</i> voor deze <i>Gegevensdienst</i> een <b>token request</b> heeft gedaan waarop geen succesvolle token response is ontvangen	het aantal keren dat de <i>Authorization Server</i> voor deze <i>Gegevensdienst</i> een <b>token request</b> heeft ontvangen waarop geen succesvolle token response is uitgegaan
ResourceRequestNumbers. AantalSuccesvol	het aantal keren dat de <i>PGO Server</i> voor deze <i>Gegevensdienst</i> een <b>resource request</b> heeft gedaan waarop een succesvolle resource response is ontvangen	het aantal keren dat de <i>Resource Server</i> voor deze <i>Gegevensdienst</i> een <b>resource request</b> heeft ontvangen waarop een succesvolle resource response is uitgegaan
ResourceRequestNumbers. AantalOnsuccesvol	het aantal keren dat de <i>PGO Server</i> voor deze <i>Gegevensdienst</i> een <b>resource request</b> heeft gedaan waarop geen succesvolle resource response is ontvangen	het aantal keren dat de <i>Resource Server</i> voor deze <i>Gegevensdienst</i> een <b>resource request</b> heeft ontvangen waarop geen succesvolle resource response is uitgegaan
SubscriptionRequestNumbers. AantalSuccesvol	het aantal keren dat de <i>PGO Server</i> voor deze <i>Gegevensdienst</i> een <b>subscription request</b> heeft gedaan waarop een succesvolle subscription	het aantal keren dat de <i>Subscription Server</i> voor deze <i>Gegevensdienst</i> een <b>subscription request</b> heeft ontvangen waarop een succesvolle

	response is ontvangen	subscription response is uitgegaan
SubscriptionRequestNumbers. AantalOnsuccesvol	het aantal keren dat de <i>PGO Server</i> voor deze <i>Gegevensdienst</i> een <a href="#">subscription request</a> heeft gedaan waarop geen succesvolle subscription response is ontvangen	het aantal keren dat de <i>Subscription Server</i> voor deze <i>Gegevensdienst</i> een <a href="#">subscription request</a> heeft ontvangen waarop geen succesvolle subscription response is uitgegaan
SubscriptionNotificationNumbers. AantalSuccesvol	het aantal keren dat bij de <i>Notification Server</i> voor deze <i>Gegevensdienst</i> een <a href="#">subscription notification</a> is binnengekomen waarop een succesvolle subscription notification response kon worden gestuurd	het aantal keren dat de <i>Notification Client</i> voor deze <i>Gegevensdienst</i> een <a href="#">subscription notification</a> heeft gestuurd waarop een succesvolle subscription notification response is ontvangen
SubscriptionNotificationNumbers. AantalOnsuccesvol	het aantal keren dat bij de <i>Notification Server</i> voor deze <i>Gegevensdienst</i> een <a href="#">subscription notification</a> is binnengekomen waarop geen succesvolle subscription notification response kon worden gestuurd	het aantal keren dat bij de <i>Notification Client</i> voor deze <i>Gegevensdienst</i> een <a href="#">subscription notification</a> heeft gestuurd waarop geen succesvolle subscription notification response is ontvangen
ResourceNotificationNumbers. AantalSuccesvol	het aantal keren dat bij de <i>Notification Server</i> voor deze <i>Gegevensdienst</i> een <a href="#">resource notification</a> is binnengekomen waarop een	het aantal keren dat bij de <i>Notification Client</i> voor deze <i>Gegevensdienst</i> een <a href="#">resource notification</a> heeft gestuurd waarop een succesvolle

		succesvolle resource notification response kon worden gestuurd	resource notification response is ontvangen
	ResourceNotificationNumbers. AantalOnsuccesvol	het aantal keren dat bij de <i>Notification Server</i> voor deze <i>Gegevensdienst</i> een <a href="#">resource notification</a> is binnengekomen waarop geen succesvolle subscription notification response kon worden gestuurd	het aantal keren dat bij de <i>Notification Client</i> voor deze <i>Gegevensdienst</i> een <a href="#">resource notification</a> heeft gestuurd waarop geen succesvolle subscription notification response is ontvangen

## Beheerrapporten

Met de algemene informatie over *Personen* in de *Beheerrapporten* verkrijgt de Stichting MedMij informatie over de mate waarin MedMij de doelstelling behaalt om alle Nederlanders in de gelegenheid te stellen met een PGO regie te voeren over hun gezondheid(sgegevens).

Met de informatie per *Gegevensdienst* verkrijgt de Stichting MedMij informatie over het succes van de verschillende *Gegevensdiensten*, zodat zij passend beleid kan voeren op de [Catalogus](#). Voor elke *Gegevensdienst* is deze informatie geordend per [Interface](#). Op deze wijze kunnen *Dienstverleners persoon* en *Dienstverleners zorgaanbieder* de gevraagde informatie verzamelen op een wijze die past bij hun implementatie. Uit de interface-gewijze informatie kunnen door de Stichting MedMij cijfers worden afgeleid over het gebruik van de use cases [UC Verzamelen](#), [UC Delen](#), [UC Abonneren](#) en [UC Notificeren](#).

De Stichting MedMij en de *MedMij Beheerorganisatie* gebruiken deze informatie niet:

- voor doelen die niet voortvloeien uit de specifieke missie van MedMij;
- op wijzen die niet stroken met de [grondslagen](#) van MedMij, of welk deel van het MedMij Afsprakenstelsel dan ook.

De *Gegevensdienst*-specifieke elementen in het *Beheerrapport* van alle *Dienstverleners persoon* samen zouden iedere maand tot hetzelfde totaal moeten leiden als die van alle *Dienstverleners zorgaanbieder* samen. Zij gelden wederzijds als elkaars checksums voor de Stichting MedMij. Voorts geven deze cijfers inzicht in de verdeling van het gebruik van het MedMij-netwerk over de verschillende *Dienstverleners* in beide domein. Daarmee krijgt de Stichting MedMij een indicatie van de mate waarin de [Speelveld-principes](#) goed werken.

## Correcties op deze release

Met deze pagina worden alle correcties, voorziene en doorgevoerde, bijgehouden op deze release van het MedMij Afsprakenstelsel. Bij correcties gaat het om aanpassingen die de inhoudelijke strekking van de tekst van het MedMijAfsprakenstelsel niet raken. Voorbeelden zijn:

- gebroken of foute verwijzingen;
- fouten in terminologie;
- weggevalen passages;
- taalfouten.

Om te voorkomen dat lezers van het MedMij Afsprakenstelsel voortdurend een lijst van errata zouden moeten raadplegen, worden de correcties doorgevoerd in de hoofdtekst. Onderstaande tabel geldt daarbij als vastlegging van de correctiegeschiedenis.

Nr	Pagina('s)	Correctie(s)	Reden	Aangepast op
1.2.0-1	<a href="https://afsprakenstelsel.medmij.nl">https://afsprakenstelsel.medmij.nl</a>	"Actieve" i.p.v. "Geldende"	Terminologie	4 feb 2020
1.2.0-2	<a href="#">Authorization interface</a> , verantwoordelijkheid 6, tweede kolom van de tabel	De respectievelijk uitzonderingen van UC Abonneren toevoegen.	Het authorization interface wordt ook gebruikt door UC Abonneren.	3 feb 2020
1.2.0-3	<a href="#">Token interface</a> , verantwoordelijkheid 6, tweede kolom van de tabel	De respectievelijk uitzonderingen van UC Abonneren toevoegen.	Het token interface wordt ook gebruikt door UC Abonneren.	3 feb 2020
1.2.0-4	<a href="#">Catalogus</a>	De kolom <code>MaximaleDuurAbonnement</code> toevoegen in <i>Catalogus</i> .	Moet conform <a href="#">logisch model</a> <i>Catalogus</i> .	3 feb 2020
1.2.0-5	<a href="#">Normenkader informatiebeveiliging</a>	Foutmelding bij weergave rollen (plaatjes werken niet)		3 feb 2020
1.2.0-6	<a href="#">Coördinatie, regie en uitwisseling</a>	Plaatje is verdwenen. Er staat een foutmelding.		3 feb 2020
1.2.0-7	<a href="#">Normenkader informatiebeveiliging</a>	Meerdere verwijzingen werken niet.		3 feb 2020
1.2.0-8	<a href="#">Subscription interface</a> , verantwoordelijkheid 1c	JSON als verplicht formaat toevoegen	Was weggevalen.	3 feb 2020
1.2.0-9	<a href="#">Processen en informatie</a>	dode link		4 feb 2020

1.2.0-10	<a href="#">GNL-, OCL- en ZAL-interface</a>	Versienummers interfaces aanpassen op 1.2.0	Was nagelaten.	5 feb 2020
1.2.0-11	<a href="#">UCI Notificeren</a>	'ia' gecorrigeerd naar 'is'	Typo	6 feb 2020
1.2.0-12	<a href="#">UCI Notificeren</a>	Dubbele 'resource notification' vervangen door correcte 'subscription notification'	Vertyping hersteld in lijn met diagram	6 feb 2020
1.2.0-13	<a href="#">Subscription notification interface</a>	In de tabel onder punt 3 'Server Server' vervangen door 'Server'.	Typo	6 feb 2020
1.2.0-14	<a href="#">Notificatie van Zorggebruiker</a>	Zin tussen de verplichte teksten verhelderd.	Was voor meerdere interpretaties vatbaar.	11 feb 2020
1.2.0-15	<a href="#">Subscription notification interface</a> en <a href="#">Resource notification interface</a>	Op beide pagina's ontbrak bij uitzondering 1 "invalid_notification_type" in de foutmelding.	Was nagelaten.	11 feb 2020
1.2.0-16	<a href="#">Processen en informatie</a>	Bij verantwoordelijkheid .20 de referentie gecorrigeerd van .20 naar .19.	Typo	18 feb 2020
1.2.0-17	<a href="#">Informatieclassificatiebeleid</a>	Niet werkend linkje naar <a href="#">A. 8.2.1 Classificatie van informatie</a> hersteld.	Typo	30 mrt 2020
1.2.0-18	<a href="#">Nalevingsbeleid, Changelog release 1.1 versie 1.0, Privacy- en informatiebeveiligingsbeleid, Risicoanalyse, Deelnemersovereenkomst Dienstverlener persoon</a>	Niet werkende links naar <a href="#">Normenkader informatiebeveiliging</a> hersteld.	Typo	30 mrt 2020
1.2.0-19	<a href="#">Managementinformatie</a>	MedMijRapport . Beheerrapport . Personen . AantalActiefOnsuccesvol gecorrigeerd naar ..één keer <b>onsuccesvol</b> gebruik ..	Typo	15 apr 2020
1.2.0-20	<a href="#">Managementinformatie</a>	Definities en toelichting succesvol /niet-succesvol aantallen voor DVP toegevoegd.	Toelichting	16 apr 2020
1.2.0-21	<a href="#">Managementinformatie</a>	Beheerrapport schema én voorbeeld vervangen door correcte versies.	Correctie nav vragen	29 apr 2020
1.2.0-	<a href="#">XML-schema's</a>	Ontbrekende slash toegevoegd in	Correctie	29 mei 2020

22		Namespace-paden in Whitelist, Zorgaanbiederslijst en OAuthClientList.		
1.2.0-23	<a href="#">XML-schema's</a>	AuthorizationEndpoint en TokenEndpoint naar 0..1 gewijzigd (van 1..1) nav uitlevering door RnA	Correctie	15 juni 2020
1.2.0-24	<a href="#">XML-schema's</a>	Schema portabiliteitsrapport bijgewerkt	Correctie	22 juni 2020
1.2.0-25	<a href="#">Managementinformatie</a>	Definities voor velden Personen. AantalActiefSuccesvol, Personen. AantalActiefOnsuccesvol, AuthorizationRequest Numbers. AantalSuccesvol en AuthorizationRequest Numbers. AantalOnsuccesvol aangepast	Nav discussie en vragen	23 juni 2020
1.2.0-26	<a href="#">XML-schema's</a>	Beheerrapport voorbeeld toegevoegd (stond link naar schema)	Correctie	25 juni 2020
1.2.0-27	<a href="#">XML-schema's</a>	Portabiliteits voorbeeld vervangen	Correctie	25 juni 2020
1.2.0-28	<a href="#">XML-schema's</a>	Voorbeeld OCL bestand vervangen	Correctie	7 juli 2020
1.2.0-29	<a href="#">XML-schema's</a>	Voorbeeld ZAL bestand vervangen	Correctie	9 juli 2020
1.2.0-30	<a href="#">Aanvullende auditverklaring en onderbouwende rapportage</a>	Verwijzing naar versie 1.1.2 gecorrigeerd naar 1.2.0	Correctie	24 juli 2020
1.2.0-31	<a href="#">XML-schema's</a>	Correctie op schema van portabiliteitsrapport; ontbrekend 'elementFormDefault="qualified" ' toegevoegd.	Correctie	9 september 2020
1.2.0-32	<a href="#">Toestemmingsverklaring</a>	Toestemmingsverklaring verruimd conform RFC0033.	Correctie	22 september 2020
1.2.0-33	<a href="#">Bevestigingsverklaring</a>	Bevestigingsverklaring verruimd conform RFC0033.	Correctie	22 september 2020
1.2.0-34	<a href="#">Toestemmingsverklaring Abonneren</a>	Toestemmingsverklaring verruimd conform RFC0033.	Correctie	22 september 2020
1.2.0-35	<a href="#">Netwerk</a>	Eisen aan PKIoverheid certificaten aangepast	Correctie	8 oktober 2020
1.2.0-36	<a href="#">Zorgaanbiedersnamenbeleid</a>	Eisen aan fragment aangepast conform RFC0035	Correctie	13 oktober 2020
1.2.0-37	<a href="#">XML-schema's</a>	MedMij_Zorgaanbiedersnamenlijst. xsd specificatie van	Correctie	29 oktober

		zorgaanbiedersnaam conform tekst dus lengte tussen 3 - 280 karakters en ruimere karakterset		
1.3.0-4	<a href="#">Netwerk</a>	Ondersteuning G3 certificaten tot 31 december 2020	Correctie	11 november 2020
1.2.0-38	<a href="#">XML-schema's</a>	Verwijzing naar xsd gecorrigeerd in voorbeelden	Correctie	16 november 2020
1.2.0-39	<a href="#">XML-schema's</a>	Voorbeeldbestanden aangepast: tijdstempels voorzien van tijdzones	Correctie	17 december 2020

## Catalogus

De Catalogus is release-onafhankelijk en kan worden gevonden op [MedMij Catalogus](#).



## Deelnemersovereenkomsten

De Deelnemersovereenkomst bevat de basisafspraken tussen Stichting MedMij en een deelnemer aan het afsprakenstelsel. Aangezien er twee typen deelnemers zijn, wordt onderscheid gemaakt tussen een [Deelnemersovereenkomst Dienstverlener persoon](#) en een [Deelnemersovereenkomst Dienstverlener zorgaanbieder](#). Deze overeenkomsten zorgen ervoor dat deelnemers gehouden zijn aan de op hen rustende verantwoordelijkheden en verplichtingen. De overeenkomsten binden deelnemers tevens aan de besturings- en nalevingsafspraken die noodzakelijk zijn voor het borgen van het vertrouwen in MedMij. Deelnemers mogen binnen MedMij in hun rol alleen diensten verrichten indien zij een Deelnemersovereenkomst hebben gesloten met Stichting MedMij.

## Deelnemersovereenkomst Dienstverlener persoon

### Doel

De Deelnemersovereenkomsten bevatten de basisafspraken tussen Stichting MedMij en de Deelnemers van het MedMij Afsprakenstelsel. Er zijn twee typen Deelnemersovereenkomsten, namelijk de [Deelnemersovereenkomst Dienstverlener persoon](#) en de [Deelnemersovereenkomst Dienstverlener zorgaanbieder](#).

### Partijen

De <Stichting MedMij>, te dezen vertegenwoordigd door <naam>, <functie>

Verder te noemen: Stichting MedMij

en

<Naam partij > gevestigd te <adres>, te dezen vertegenwoordigd door <naam>, <functie>

verder te noemen: Deelnemer,

Hierna gezamenlijk te noemen: Partijen

### Overwegende dat

I. het doel van het MedMij Afsprakenstelsel is een veilige, interoperabele en betrouwbare gegevensuitwisseling tussen de Persoon met zijn PGO en de Zorgaanbieder met zijn informatiesystemen te waarborgen;

II. de Stichting MedMij verantwoordelijk is voor het beheer van het MedMij Afsprakenstelsel en de controle van de naleving hiervan door de Deelnemer;

III. de Deelnemer wenst toe te treden tot het MedMij Afsprakenstelsel in de rol van Dienstverlener persoon en in deze hoedanigheid wenst te worden toegelaten tot het Netwerk;

IV. de Deelnemer de Toetredingsprocedure voor de rol Dienstverlener persoon met goed gevolg heeft doorlopen;

V. het de Deelnemer wordt toegestaan Diensten aan te bieden. De Deelnemer committeert zich hiervoor aan de laatst geldende release(s) van het MedMij Afsprakenstelsel zoals vastgesteld door de Stichting MedMij en de daarin opgenomen afspraken voor de rol Dienstverlener persoon;

VI. in het MedMij Afsprakenstelsel de verplichtingen zijn vastgelegd waaraan de Deelnemer dient te voldoen;

VII. de Deelnemer desgevraagd te allen tijde zijn medewerking verleent aan de controle op de naleving van de verplichtingen die in het MedMij Afsprakenstelsel voor de rol van Dienstverlener persoon zijn vastgelegd;

VIII. de Deelnemer een actieve bijdrage levert aan de (door)ontwikkeling van het MedMij Afsprakenstelsel.

## **Verklaren te zijn overeengekomen als volgt**

### **Artikel 1 Definities**

De hierna met een hoofdletter aangeduide begrippen hebben in deze Overeenkomst de volgende betekenis:

1.1 Architectuur en technische specificaties: de beschrijving van de technische eisen voor de uitwisseling van (persoons)gegevens en/of gezondheidsinformatie voor de Deelnemer conform het MedMij Afsprakenstelsel.

1.2 AVG: Algemene Verordening Gegevensbescherming.

1.3 Deelnemer: een organisatie die conform de statuten van de Stichting is toegelaten tot de Stichting, toetreedt tot het MedMij Afsprakenstelsel en overeenkomstig hetgeen daarover in het MedMij Afsprakenstelsel is opgenomen de rol van Dienstverlener persoon of Dienstverlener zorgaanbieder vervult.

1.4 Dienstverlener persoon: dit betreft een rol in het MedMij Afsprakenstelsel. De Dienstverlener persoon levert een PGO, een dienst aan de Persoon voor de regie op zijn gezondheid die minimaal gegevensuitwisseling met de Zorgaanbieder mogelijk maakt via het Netwerk en conform de afspraken van het MedMij Afsprakenstelsel.

1.5 Dienstverlener zorgaanbieder: dit betreft een rol in het MedMij Afsprakenstelsel. De Dienstverlener zorgaanbieder levert Diensten aan Zorgaanbieders gerelateerd aan de gegevensuitwisseling tussen de Persoon en de Zorgaanbieder via het Netwerk en committeert zich hiervoor aan de naleving van de afspraken van het MedMij Afsprakenstelsel.

1.6 Dienst(en): activiteiten, processen en functionaliteit van de Dienstverlener persoon aan de Persoon teneinde de gegevensuitwisseling tussen Gebruikers te realiseren overeenkomstig het bepaalde in het MedMij Afsprakenstelsel.

1.7 Gebruiker: afnemer van de Dienst(en) van de Dienstverlener persoon, zijnde de Persoon, of een afnemer van de Dienst(en) van de Dienstverlener zorgaanbieder, zijnde de Zorgaanbieder.

1.8 Gegevensdienst: een gestandaardiseerde dienst voor gegevensuitwisseling met waarde voor de Gebruiker die door een Dienstverlener persoon of Dienstverlener zorgaanbieder wordt aangeboden over het Netwerk. MedMij definieert welke Gegevensdiensten over het Netwerk aangeboden mogen worden en biedt een faciliteit om het aanbod van de Dienstverlener persoon en Dienstverlener zorgaanbieder inzichtelijk te maken.

1.9 MedMij Afsprakenstelsel: de door de Stichting MedMij vastgestelde laatst geldende release(s) van het MedMij Afsprakenstelsel.

1.10 Merk: (de) woordmerk(en) en/of beeldmerk(en) ten aanzien waarvan Stichting MedMij het merkenrecht uitoefent.

1.11 Netwerk: het MedMij-netwerk zoals gedefinieerd in het MedMij Afsprakenstelsel.

1.12 Overeenkomst: deze Deelnemersovereenkomst.

1.13 Persoon: Persoon die gebruik wenst te maken van een PGO welke gegevens kan uitwisselen met de Zorgaanbieder conform het MedMij Afsprakenstelsel.

1.14 PGO: Een persoonlijke gezondheidsomgeving is een dienst aan de Persoon voor de regie op zijn gezondheid die minimaal gegevensuitwisseling met de Zorgaanbieder mogelijk maakt middels het MedMij Afsprakenstelsel.

1.15 Stichting MedMij: beheerder van het MedMij Afsprakenstelsel.

1.16 Toetredingsprocedure: procedure zoals beschreven in de operationele processen van het MedMij Afsprakenstelsel die een organisatie succesvol moet doorlopen om toe te kunnen treden tot en deel te kunnen nemen aan het MedMij Afsprakenstelsel.

1.17 Zorgaanbieder: een zorgverlener of een verband van zorgverleners die behandelingsovereenkomsten kunnen aangaan met patiënten overeenkomstig artikel 7:446 BW, en die via een Dienstverlener zorgaanbieder gegevens kan uitwisselen met de Persoon conform het MedMij Afsprakenstelsel.

## Artikel 2 Voorwerp van de Deelnemersovereenkomst

2.1 De Deelnemer heeft het recht voor eigen rekening en risico een PGO en Diensten via het Netwerk aan de Persoon aan te bieden.

2.2 De Deelnemer staat in voor de aantoonbare en controleerbare naleving van de Nederlandse wet- en regelgeving die van toepassing is bij het aanbieden van zijn Diensten en de PGO.

2.3 De Deelnemer is gedurende de looptijd van deze Overeenkomst verplicht op elk en op enig moment ten minste één Gegevensdienst aan de Persoon aan te bieden.

2.4 Partijen zijn gehouden onverkort alle verantwoordelijkheden en verplichtingen op grond van deze Overeenkomst en alle overige bindende regelingen die op enig moment in het MedMij Afsprakenstelsel voor hun rol zijn vastgesteld en in werking zijn getreden, na te komen.

2.5 De Deelnemer conformeert en houdt zich aan de [operationele processen](#) en het [beleid](#) van het MedMij Afsprakenstelsel, alsmede de voor de Deelnemer relevante [architectuur en technische specificaties](#), het [normenkader Informatiebeveiliging](#) en de afspraken over [managementinformatie](#) en [communicatie](#).

2.6 Partijen erkennen de [grondslagen](#) en de [juridische context](#) van het MedMij Afsprakenstelsel.

2.7 De Deelnemer levert in samenwerking met Stichting MedMij een actieve bijdrage aan de (door)ontwikkeling van de volgende release van het MedMij Afsprakenstelsel. Partijen houden hiervoor de door de Stichting MedMij vastgestelde strategische releaseplanning aan.

2.8 Het is de Deelnemer niet toegestaan tevens Diensten aan te bieden in de rol van Dienstverlener zorgaanbieder zonder hiervoor de Toetredingsprocedure voor deze rol in het MedMij Afsprakenstelsel te doorlopen.

2.9 De Stichting zorgt ervoor dat de Deelnemer te allen tijde kennis heeft van en/of te allen tijde kennis kan nemen van de operationele processen en samenwerkingsafspraken in relatie tot het beheer, het onderhoud en de (door)ontwikkeling van het MedMij Afsprakenstelsel opdat de Deelnemer (zo nodig) zijn taken en verantwoordelijkheid in of bij de uitvoering van deze operationele processen en samenwerkingsafspraken - dan wel anderszins voor zover van belang voor het vertrouwen in het MedMij Afsprakenstelsel - in zijn rol als Deelnemer kan nemen en/of vervullen.

2.10 Deelnemers brengen elkaar geen onderlinge vergoeding in rekening voor de gegevensuitwisseling tussen Deelnemers ten behoeve van het kunnen leveren van Diensten en Gegevensdiensten via het Netwerk.

## Artikel 3 Duur en beëindiging van de Overeenkomst

3.1 Deze Overeenkomst treedt inwerking vanaf de datum van ondertekening en geldt voor onbepaalde tijd.

3.2. De Deelnemer is te allen tijde gerechtigd de Overeenkomst tussentijds door middel van een aangetekend schrijven te beëindigen met inachtneming van een opzegtermijn van vier weken, onverminderd zijn lopende verplichtingen uit deze Overeenkomst zoals, doch niet beperkt tot geheimhouding, privacy en (informatie)beveiliging, als ook nader bepaald in de artikelen 5 en 10 van de Overeenkomst.

3.3 Na beëindiging van de Overeenkomst, om wat voor reden dan ook, zal de Deelnemer direct alle activiteiten en uitingen in het kader van het vervullen van de desbetreffende rol(len) staken, dan wel zo snel mogelijk staken als praktisch haalbaar is. De Deelnemer zal alle medewerking verlenen aan het proces uittreding, zoals opgenomen in het MedMij Afsprakenstelsel. De Deelnemer verleent tevens alle medewerking om zijn Gebruikers te informeren over de stopzetting van de Diensten evenals de verwijzing naar meer informatie voor de mogelijkheden om via een andere Dienstverlener persoon Diensten in het kader van het MedMij Afsprakenstelsel af te nemen.

#### **Artikel 4 Informatieplicht en communicatie**

4.1 De Deelnemer draagt, overeenkomstig het bepaalde in het MedMij Afsprakenstelsel en alvorens gebruik wordt gemaakt van zijn Diensten, zorg voor adequate informatieverstrekking en communicatie over zijn Diensten en de PGO aan de Persoon. De Deelnemer hanteert hiervoor de afspraken omtrent [communicatie](#). De informatieverstrekking heeft tenminste betrekking op:

1. deze Overeenkomst;
2. de overeenkomst van de Deelnemer met de Persoon;
3. de verantwoordelijkheid van de Persoon;
4. de Gebruikersvoorlichting zoals ter beschikking gesteld in het MedMij Afsprakenstelsel;
5. de werking van de PGO en bijbehorende Dienst(en);
6. de verwerking van persoonsgegevens overeenkomstig de geldende privacywet-en regelgeving en hoe de Persoon zijn rechten in deze bij de Deelnemer kan uitoefenen.

4.2 De Deelnemer legt communicatie, waaronder persberichten, met betrekking tot de Overeenkomst en het MedMij Afsprakenstelsel ter goedkeuring voor aan de Stichting MedMij alvorens deze wordt gepubliceerd.

4.3 De Deelnemer is te allen tijde aanspreekbaar voor de Persoon op het verlenen van zijn Diensten aan de Persoon en draagt zorg voor een adequate afhandeling hiervan.

4.4 De Deelnemer geeft toestemming voor vermelding van zijn organisatie, zijn rol in het MedMij Afsprakenstelsel en zijn Gegevensdiensten op de MedMij-website.

#### **Artikel 5 Privacy en (Informatie)beveiliging**

5.1 Partijen zijn verplicht te voldoen aan de privacy- en beveiligingseisen zoals opgenomen in het [normenkader informatiebeveiliging](#) van het MedMij Afsprakenstelsel.

5.2 De Deelnemer is verplicht jegens de Stichting MedMij aan te tonen dat hij voldoet aan de voor hem geldende eisen op het gebied van [privacy- en informatiebeveiligingsbeleid](#) evenals het [normenkader informatiebeveiliging](#) van het MedMij Afsprakenstelsel.

5.3 Partijen informeren elkaar onverwijld indien sprake is van een storing, aantasting van de betrouwbaarheid van Diensten en/of de PGO of een beveiligingsincident alsmede alle andere aangelegenheden die verband houden met of gevolgen kunnen hebben voor de veiligheid, betrouwbaarheid, beschikbaarheid en continuïteit van de Diensten en/of de PGO overeenkomstig het bepaalde in het MedMij

Afsprakenstelsel. De Deelnemer volgt hiervoor het [incidenten- en calamiteitenproces](#), zoals beschreven in het MedMij Afsprakenstelsel.

5.4 De Deelnemer is verantwoordelijk voor de beveiliging en controle van de eigen netwerkverbindingen en -systemen die worden gebruikt voor de koppeling met de netwerkverbindingen en/of -systemen van de Persoon.

5.5 In het kader van deze Overeenkomst is het doel van de verwerking van de persoonsgegevens de waarborging en realisering van een veilige, interoperabele en betrouwbare gegevensuitwisseling tussen de Persoon en Zorgaanbieder via de Dienstverlener Persoon en de Dienstverlener Zorgaanbieder overeenkomstig het bepaalde in het MedMij Afsprakenstelsel.

5.6 Voor zover de verwerking van persoonsgegevens door de Deelnemer wordt gebaseerd op de rechtmatigheidsgrondslag 'toestemming' in de zin van artikel 6 lid 1 AVG is de verwerking voor een ander doel dan genoemd in artikel 5.5 van deze Overeenkomst toegestaan, mits de beginselen van de AVG op deze verdere verwerking wordt toegepast, de Persoon over deze verdere verwerking wordt geïnformeerd alsmede over de rechten die de Persoon tegen deze verdere verwerking kan uitoefenen. Voor zover de verwerking van de persoonsgegevens wordt gebaseerd op de rechtmatigheidsgrondslag 'noodzakelijk voor de uitvoering van de overeenkomst' in de zin van artikel 6 lid 1 sub c AVG, is verdere verwerking van de persoonsgegevens door de Deelnemer alleen toegestaan indien de evenredigheidstoets van artikel 6 lid 4 AVG succesvol is doorlopen.

5.7 De Deelnemer verstrekt geen persoonsgegevens van de Persoon aan anderen dan degenen waaraan de Deelnemer uit hoofde van de Overeenkomst gegevens mag verstrekken c.q. op grond van een wettelijke verplichting moet verstrekken. Het is de Deelnemer uitdrukkelijk verboden om data betreffende de Persoon te verkopen.

5.8 De Deelnemer en de Stichting hebben aan elkaar kenbaar gemaakt wie binnen de organisatie aanspreekbaar is op het onderwerp privacy en de bepalingen in artikel 5 van de Overeenkomst.

## **Artikel 6 Aansprakelijkheid**

6.1 Partijen aanvaarden door ondertekening van deze Overeenkomst aansprakelijkheid voor het eigen handelen en/of nalaten binnen de rol die zij vervullen. Gebruikers kunnen zich jegens Partijen onmiddellijk en direct op deze aansprakelijkheid beroepen.

6.2 In het kader van aansprakelijkheid gelden de algemene regels van het Nederlands recht ten aanzien van de inhoud en omvang van wettelijke verplichtingen tot schadevergoeding.

6.3 De Deelnemer vrijwaart de Stichting MedMij voor vorderingen van derden, uit welke hoofde dan ook, ten gevolge van het gebruik van Diensten en Gegevensdiensten van de Deelnemer.

## **Artikel 7 Opschorting en ontbinding**

7.1 De Stichting is gerechtigd de Overeenkomst door middel van een aangetekend schrijven met onmiddellijke ingang buiten rechte te ontbinden, indien de Deelnemer ook na schriftelijke ingebrekestelling stellende een redelijke termijn in gebreke blijft enige verplichting(en) uit deze Overeenkomst te voldoen.

7.2 Buiten hetgeen elders in deze Overeenkomst is bepaald, is de Stichting MedMij gerechtigd deze Overeenkomst door middel van een aangetekend schrijven met onmiddellijke ingang buiten rechte zonder dat enige ingebrekestelling is vereist te ontbinden indien:

1. De Deelnemer zijn faillissement aanvraagt of failliet is verklaard.
2. De Deelnemer (voorlopige) surseance van betaling aanvraagt of aan hem surseance van betaling is verleend, of onder een schuldsaneringsregeling valt.
3. De onderneming van Deelnemer wordt geliquideerd.
4. De Deelnemer zijn huidige onderneming staakt dan wel op een aanmerkelijk deel van het vermogen van de Deelnemer beslag wordt gelegd.

7.3 Indien niet-nakoming als bedoeld in artikel 7.1 van de Overeenkomst een gevaar vormt voor de veilige en betrouwbare werking van het Netwerk is de Stichting MedMij gerechtigd passende maatregelen te treffen, waaronder het sommeren van de Deelnemer de levering van Diensten per direct voor een bepaalde tijd op te schorten.

7.4 Indien de Stichting MedMij gebruik maakt van het recht als bedoeld in artikel 7.2 en/of 7.3 van de Overeenkomst meldt hij dit onverwijld aan de Deelnemer.

## **Artikel 8 Verantwoordelijkheid voor derde partij**

8.1 Het is de Deelnemer toegestaan voor zijn Diensten derden in te schakelen.

8.2 Indien de Deelnemer derden inschakelt voor de verwerking van persoonsgegevens, vertaalt de Deelnemer de voor hem geldende afspraken uit het MedMij Afsprakenstelsel in dit kader door naar (sub) verwerkers. De uitvoering van de verwerking van persoonsgegevens door een door de Deelnemer ingeschakelde verwerker wordt geregeld in een (sub)verwerkersovereenkomst.

8.3 De Deelnemer staat er jegens de Stichting MedMij voor in dat de door hem ingeschakelde derde voor zijn Diensten en/of Gegevensdiensten alle verplichtingen uit deze Overeenkomst nakomt en is aansprakelijk voor het handelen op grond van deze Overeenkomst van de door hem ingeschakelde derde.

## **Artikel 9 Controle naleving**

9.1 De Stichting MedMij is bevoegd te (laten) onderzoeken of de Deelnemer de afspraken, eisen en voorwaarden uit het MedMij Afsprakenstelsel en deze Overeenkomst naleeft.

9.2 De Deelnemer verleent zijn medewerking aan een onderzoek tot naleving van het MedMij Afsprakenstelsel en deze Overeenkomst door of namens de Stichting MedMij, dan wel verstrekt de Stichting MedMij in dit kader alle noodzakelijke informatie op eerste verzoek.

## **Artikel 10 Geheimhouding**

10.1 Partijen nemen in relatie tot het MedMij Afsprakenstelsel strikte geheimhouding in acht voor zover het vertrouwelijke informatie betreft of informatie waarvan men het vertrouwelijk karakter redelijkerwijs kan vermoeden, tenzij een wettelijke plicht of een rechterlijke uitspraak openbaarmaking van deze gegevens gebiedt.

## **Artikel 11 Intellectueel eigendom**

11.1 Alle intellectuele eigendom voor alle soorten zaken die worden ontwikkeld door, voor of namens de Stichting MedMij, zoals bijdragen aan Request For Changes (RFC'S) en/of overige documentatie die

bijdragen aan de ontwikkeling van de afspraken binnen het MedMij Afsprakenstelsel en die via het MedMij Afsprakenstelsel openbaar worden gemaakt, komen toe aan Stichting MedMij.

11.2 Alle auteursrechten die door de Deelnemer kunnen worden uitgeoefend voor alle soorten zaken die worden ontwikkeld door, voor of namens de Stichting MedMij, waar en wanneer dan ook, zoals bijdragen aan Request For Changes (RFC'S) en/of overige documentatie die via het MedMij Afsprakenstelsel openbaar worden, berusten bij de Stichting MedMij. Deze intellectuele eigendomsrechten worden op grond van deze Overeenkomst door de Deelnemer om niet aan de Stichting MedMij overgedragen, welke overdracht door Stichting MedMij wordt aanvaard.

11.3 De Deelnemer doet hierbij afstand jegens de Stichting MedMij voor zover van toepassing op bijdragen aan de ontwikkeling van de afspraken binnen het MedMij Afsprakenstelsel zoals bedoeld in artikel 11.1, alsmede van alle eventueel aan hem toekomende persoonlijkheidsrechten als bedoeld in de Auteurswet en voor zover de toepasselijke regelgeving zodanige afstand toelaat. Deelnemer doet dit ook namens eventueel aan zijn zijde betrokken personeelsleden afstand jegens de Stichting MedMij van alle eventueel aan deze personeelsleden toekomende persoonlijkheidsrechten, in de mate waarin de toepasselijke regelgeving zodanige afstand toelaat.

11.4 De Deelnemer heeft het niet-exclusieve en niet-overdraagbare recht om, gedurende de looptijd van deze Overeenkomst, het Merk te gebruiken in verband met het aanbieden van Diensten, in overeenstemming met deze Overeenkomst en de daaruit voortvloeiende voorschriften.

11.5 De Deelnemer zal niets doen dan wel nalaten waardoor de rechten van de Stichting MedMij ten aanzien van het Merk kunnen worden aangetast en/of de ter zake van het Merk opgebouwde goodwill negatief zou kunnen worden beïnvloed en zal op geen enkele wijze, direct dan wel indirect schade toebrengen aan het Merk zoals, maar niet beperkt tot, het niet voldoen aan de privacy- en beveiligingseisen.

## **Artikel 12 Overdraagbaarheid rechten en verplichtingen overeenkomst**

12.1 Partijen zijn niet bevoegd hun rechten en verplichtingen uit de Overeenkomst over te dragen aan een derde, behalve na schriftelijke toestemming van de wederpartij.

12.2 In het geval de Deelnemer zijn rechten en plichten uit de Overeenkomst wil overdragen, dient de overnemende partij eveneens toegelaten te zijn tot het MedMij Afsprakenstelsel in de rol van Dienstverlener p ersoon.

## **Artikel 13 Geschillen en toepasselijk recht**

13.1 Partijen proberen ieder geschil naar aanleiding van deze Overeenkomst eerst in onderling overleg op te lossen. Indien Partijen het geschil ter zake van deze Overeenkomst niet in onderling overleg kunnen beslechten zal het geschil worden voorgelegd aan de ter zake bevoegde rechter te Utrecht, tenzij Partijen zelf alsnog minitrial, bindend advies, arbitrage of andere vormen van alternatieve geschillenbeslechting overeenkomen.

13.2 Op deze Overeenkomst, de uitvoering van deze Overeenkomst en op alle geschillen die daaruit mochten voortvloeien is Nederlands recht van toepassing.

## **Artikel 14 Overig**



14.1 Deze Overeenkomst komt in de plaats van en vervangt alle eerdere overeenkomsten en/of bindende afspraken tussen Partijen in relatie tot het MedMij Afsprakenstelsel.

14.2 De Deelnemer is in de Europese Unie ingeschreven in een door het betreffende lidstaat van vestiging erkend handelsregister.

14.3 In het geval de Deelnemer van juridische status verandert en daarmee mogelijk niet meer aan de toetredingseisen voldoet, dient de Deelnemer deze wijziging schriftelijk te melden aan de Stichting MedMij. Te denken valt aan overname door een onderneming buiten Nederland of de EU, fusie of splitsing en faillissement. In het geval van wijziging van de juridische status behoudt de Stichting MedMij het recht de Overeenkomst te beëindigen en/of de Deelnemer te vragen opnieuw de Toetredingsprocedure te doorlopen.

Aldus overeengekomen in tweevoud,

Namens Stichting MedMij	Namens de Deelnemer
Naam:	Naam:
Functie:	Functie:
Datum:	Datum:
Plaats:	Plaats:
<Handtekening Stichting MedMij>	<Handtekening deelnemer>



## Deelnemersovereenkomst Dienstverlener zorgaanbieder

### Doel

De Deelnemersovereenkomsten bevatten de basisafspraken tussen Stichting MedMij en de deelnemers van het afsprakenstelsel. Er zijn twee type Deelnemersovereenkomsten, namelijk de [Deelnemersovereenkomst Dienstverlener persoon](#) en de [Deelnemersovereenkomst Dienstverlener zorgaanbieder](#).

### Partijen

De <Stichting MedMij>, te dezen vertegenwoordigd door <naam>, <functie>,

Verder te noemen: Stichting MedMij

en

<Naam partij> gevestigd te <adres>, te dezen vertegenwoordigd door <naam>, <functie>,

Verder te noemen: Deelnemer,

Hierna gezamenlijk te noemen: Partijen

### Overwegende dat

I. het doel van het MedMij Afsprakenstelsel is een veilige, interoperabele en betrouwbare gegevensuitwisseling tussen de Persoon met zijn PGO en de Zorgaanbieder met zijn informatiesystemen te waarborgen;

II. de Stichting MedMij verantwoordelijk is voor het beheer van het MedMij Afsprakenstelsel en de controle van de naleving hiervan door de Deelnemer;

III. de Deelnemer wenst toe te treden tot het MedMij Afsprakenstelsel in de rol van Dienstverlener zorgaanbieder en in deze hoedanigheid wenst te worden toegelaten tot het Netwerk;

IV. het de Deelnemer de Toetredingsprocedure voor de rol Dienstverlener zorgaanbieder met goed gevolg heeft doorlopen;

V. de Deelnemer wordt toegestaan Diensten aan te bieden. De Deelnemer committeert zich hiervoor aan de laatst geldende release(s) van het MedMij Afsprakenstelsel zoals vastgesteld door de Stichting MedMij en de daarin opgenomen afspraken voor de rol Dienstverlener zorgaanbieder;

VI. in het MedMij Afsprakenstelsel de verplichtingen zijn opgenomen waaraan de Deelnemer dient te voldoen;

VII. de Deelnemer desgevraagd te allen tijde zijn medewerking verleent aan de controle op de naleving van de verplichtingen die in het MedMij Afsprakenstelsel voor de rol van Dienstverlener zorgaanbieder zijn vastgelegd;

VIII. de Deelnemer een bijdrage wenst te leveren aan de (door)ontwikkeling van het MedMij Afsprakenstelsel.

## **Verklaren te zijn overeengekomen als volgt**

### **Artikel 1 Definities**

De hierna met een hoofdletter aangeduide begrippen hebben in deze Overeenkomst de volgende betekenis:

1.1 Architectuur en technische specificaties: de beschrijving van de technische eisen voor de uitwisseling van (persoons)gegevens en/of gezondheidsinformatie door de Deelnemer conform het MedMij Afsprakenstelsel.

1.2 AVG: Algemene Verordening Gegevensbescherming.

1.3 Deelnemer: een organisatie die conform de statuten van de Stichting is toegelaten tot de Stichting, toetreedt tot het MedMij Afsprakenstelsel en overeenkomstig hetgeen daarover in het MedMij Afsprakenstelsel is opgenomen de rol van Dienstverlener persoon of Dienstverlener zorgaanbieder vervult.

1.4 Dienstverlener persoon: dit betreft een rol in het MedMij Afsprakenstelsel. De Dienstverlener persoon levert een PGO, een dienst aan de Persoon voor de regie op zijn gezondheid die minimaal gegevensuitwisseling met de Zorgaanbieder mogelijk maakt via het Netwerk en conform de afspraken van het MedMij Afsprakenstelsel.

1.5 Dienstverlener zorgaanbieder: dit betreft een rol in het MedMij Afsprakenstelsel. De Dienstverlener zorgaanbieder levert Diensten aan Zorgaanbieders gerelateerd aan de gegevensuitwisseling tussen de Persoon en de Zorgaanbieder via het Netwerk en committeert zich hiervoor aan de naleving van de afspraken van het MedMij

1.6 Dienst(en): activiteiten, processen en functionaliteit van de Dienstverlener zorgaanbieder aan de Zorgaanbieder teneinde de gegevensuitwisseling tussen de Zorgaanbieder en de Persoon van 16 jaar of ouder te realiseren overeenkomstig het bepaalde in het MedMij Afsprakenstelsel.

1.7 Gebruiker: afnemer van de Dienst(en) van de Dienstverlener zorgaanbieder, zijnde de Zorgaanbieder, of een afnemer van de Dienst(en) van de Dienstverlener persoon, zijnde de Persoon.

1.8 Gegevensdienst: een gestandaardiseerde dienst voor gegevensuitwisseling met waarde voor de Gebruiker die door een Dienstverlener persoon of Dienstverlener zorgaanbieder wordt aangeboden over het Netwerk. MedMij definieert welke Gegevensdiensten over het Netwerk aangeboden mogen worden en biedt een faciliteit om het aanbod van de Dienstverlener persoon en Dienstverlener zorgaanbieder inzichtelijk te maken. De Dienstverlener zorgaanbieder levert Gegevensdiensten in opdracht van en volgens schriftelijke instructie van de Zorgaanbieder via het Netwerk en heeft voor de verwerking van persoonsgegevens in relatie tot deze Gegevensdiensten een verwerkersovereenkomst met de Zorgaanbieder afgesloten.

1.9 MedMij Afsprakenstelsel: de door de Stichting MedMij vastgestelde laatst geldende release van het MedMij Afsprakenstelsel.

1.10 Merk: (de) woordmerk(en) en/of beeldmerk(en) ten aanzien waarvan Stichting MedMij het merkenrecht uitoefent.

1.11 Netwerk: het MedMij-netwerk zoals gedefinieerd in het MedMij Afsprakenstelsel.

1.12 Overeenkomst: deze Deelnemersovereenkomst.

1.13 Persoon: Persoon die gebruik wenst te maken van een PGO welke gegevens kan uitwisselen met de Zorgaanbieder conform het MedMij Afsprakenstelsel.

1.14 PGO: Een persoonlijke gezondheidsomgeving is een dienst aan de Persoon voor de regie op zijn gezondheid die minimaal gegevensuitwisseling met de Zorgaanbieder mogelijk maakt middels het MedMij Afsprakenstelsel.

1.15 Stichting MedMij: beheerder van het afsprakenstelsel MedMij.

1.16 Toetredingsprocedure: procedure zoals beschreven in de operationele processen van het MedMij Afsprakenstelsel die een organisatie succesvol moet doorlopen om toe te kunnen treden en deel te kunnen nemen aan het MedMij Afsprakenstelsel.

1.17 Zorgaanbieder: een zorgverlener of een verband van zorgverleners die behandelingsovereenkomsten kunnen aangaan met patiënten overeenkomstig artikel 7:446 BW, en die via een Dienstverlener zorgaanbieder gegevens kan uitwisselen met de Persoon conform het MedMij Afsprakenstelsel.

## Artikel 2 Voorwerp van de Deelnemersovereenkomst

2.1 De Deelnemer heeft het recht voor eigen rekening en risico Diensten via het Netwerk aan te bieden aan de Zorgaanbieder.

2.2 De Deelnemer staat in voor de aantoonbare en controleerbare naleving van de Nederlandse wet- en regelgeving die van toepassing is bij het aanbieden van zijn Diensten en de PGO.

2.3 De Deelnemer is gedurende de looptijd van deze Overeenkomst verplicht op elk en op enig moment ten minste één Gegevensdienst aan zijn Gebruikers aan te bieden.

2.4 Partijen zijn gehouden onverkort alle verantwoordelijkheden en verplichtingen op grond van deze Overeenkomst en alle overige bindende regelingen die op enig moment in het MedMij Afsprakenstelsel voor hun rol zijn vastgesteld en in werking zijn getreden, na te komen.

2.5 De Deelnemer conformeert en houdt zich aan de [operationele processen](#) en het [beleid](#) van het MedMij Afsprakenstelsel, alsmede de voor de Deelnemer relevante [architectuur en technische specificaties](#), het [normenkader Informatiebeveiliging](#) en de afspraken over [managementinformatie](#) en [communicatie](#).

2.6 Partijen erkennen de [grondslagen](#) en de [juridische context](#) van het MedMij Afsprakenstelsel.

2.7 De Deelnemer levert in samenwerking met Stichting MedMij een actieve bijdrage aan de (door)ontwikkeling van de volgende release van het MedMij Afsprakenstelsel. Partijen houden hiervoor de door de Stichting MedMij vastgestelde strategische releaseplanning aan.

2.8 Het is de Deelnemer niet toegestaan tevens Diensten aan te bieden in de rol van Dienstverlener persoon zonder hiervoor de Toetredingsprocedure voor deze rol in het MedMij Afsprakenstelsel te doorlopen.

2.9 De Stichting MedMij zorgt ervoor dat de Deelnemer te allen tijde kennis heeft van en/of te allen tijde kennis kan nemen van de operationele processen en samenwerkingsafspraken in relatie tot het beheer, het onderhoud en de (door)ontwikkeling van het MedMij Afsprakenstelsel opdat de Deelnemer (zo nodig) zijn taken en verantwoordelijkheid in of bij de uitvoering van deze operationele processen en samenwerkingsafspraken - dan wel anderszins voor zover van belang voor het vertrouwen in het MedMij Afsprakenstelsel - in zijn rol als Deelnemer kan nemen en/of vervullen.

2.10 Deelnemers brengen elkaar geen onderlinge vergoeding in rekening voor de gegevensuitwisseling tussen Deelnemers ten behoeve van het kunnen leveren van Diensten en Gegevensdiensten via het Netwerk.

### Artikel 3 Duur en beëindiging van Overeenkomst

3.1 Deze Overeenkomst treedt inwerking vanaf de datum van ondertekening en geldt voor onbepaalde tijd.

3.2. De Deelnemer is te allen tijde gerechtigd de Overeenkomst tussentijds door middel van een aangetekend schrijven te beëindigen met inachtneming van een opzegtermijn van vier weken, onverminderd zijn lopende verplichtingen uit deze Overeenkomst zoals, doch niet beperkt tot geheimhouding, privacy en (informatie)beveiliging, als ook nader bepaald in de artikelen 5 en 10 van de Overeenkomst.

3.3 Na beëindiging van de Overeenkomst, om wat voor reden dan ook, zal de Deelnemer direct alle activiteiten en uitingen in het kader van het vervullen van de desbetreffende rol(len) staken, dan wel zo snel mogelijk staken als praktisch haalbaar is. De Deelnemer zal alle medewerking verlenen aan het proces uittreding, zoals opgenomen in het MedMij Afsprakenstelsel. De Deelnemer verleent tevens alle medewerking om zijn Gebruikers te informeren over de stopzetting van de Diensten evenals de verwijzing naar meer informatie voor de mogelijkheden om via een andere Dienstverlener persoon Diensten in het kader van het MedMij Afsprakenstelsel af te nemen.

### Artikel 4 Informatieplicht en communicatie

4.1 De Deelnemer draagt, overeenkomstig het bepaalde in het MedMij Afsprakenstelsel en alvorens gebruik wordt gemaakt van zijn Diensten, zorg voor adequate informatieverstrekking en communicatie over zijn Diensten richting de Zorgaanbieder. De Deelnemer hanteert hiervoor de afspraken omtrent [communicatie](#). De informatieverstrekking heeft tenminste betrekking op:

1. deze Overeenkomst;
2. de overeenkomst van de Deelnemer met de Zorgaanbieder;
3. de verantwoordelijkheden van de Zorgaanbieder;
4. de Gebruikersvoorlichting zoals ter beschikking gesteld in het MedMij Afsprakenstelsel;
5. de werking van de Dienst;
6. de verwerking van persoonsgegevens overeenkomstig de geldende privacywet-en regelgeving.

4.2 De Deelnemer legt communicatie, waaronder persberichten, met betrekking tot de Overeenkomst en het MedMij Afsprakenstelsel ter goedkeuring voor aan de Stichting MedMij alvorens deze wordt gepubliceerd.

4.3 De Deelnemer is te allen tijde aanspreekbaar voor de Zorgaanbieder op het verlenen van zijn Diensten conform het MedMij Afsprakenstelsel.

4.4 De Deelnemer geeft toestemming voor vermelding van zijn organisatie, zijn rol in het MedMij Afsprakenstelsel en zijn Gegevensdiensten op de MedMij-website.

### Artikel 5 Privacy en (Informatie)beveiliging

5.1 Partijen zijn verplicht te voldoen aan de privacy- en beveiligingseisen zoals opgenomen in het [normenkader informatiebeveiliging](#) van het MedMij Afsprakenstelsel.

5.2 De Deelnemer is verplicht jegens de Stichting MedMij aan te tonen dat hij voldoet aan de voor hem geldende eisen op het gebied van [privacy- en informatiebeveiligingsbeleid](#) evenals het [normenkader informatiebeveiliging](#) van het MedMij Afsprakenstelsel.

5.3 Partijen informeren elkaar onverwijld indien sprake is van een storing, aantasting van de betrouwbaarheid van Diensten en/of de PGO of een beveiligingsincident alsmede alle andere aangelegenheden die verband houden met of gevolgen kunnen hebben voor de veiligheid, betrouwbaarheid, beschikbaarheid en continuïteit van de Diensten en/of de PGO overeenkomstig het bepaalde in het MedMij Afsprakenstelsel. De Deelnemer volgt hiervoor het [incidenten- en calamiteitenproces](#), zoals beschreven in het MedMij Afsprakenstelsel.

5.4 De Deelnemer is verantwoordelijk voor de beveiliging en controle van de eigen netwerkverbindingen en -systemen die worden gebruikt voor de koppeling met de netwerkverbindingen en/of -systemen van de Zorgaanbieder.

5.5 In het kader van deze Overeenkomst is het doel van de verwerking van de persoonsgegevens de waarborging en realisering van een veilige, interoperabele en betrouwbare gegevensuitwisseling tussen de Persoon en Zorgaanbieder via de Dienstverlener Persoon en de Dienstverlener Zorgaanbieder overeenkomstig het bepaalde in het MedMij Afsprakenstelsel. De Deelnemer verwerkt de persoonsgegevens in het kader van deze Overeenkomst in opdracht van en namens de Zorgaanbieder.

5.6 De Deelnemer verstrekt de persoonsgegevens van de Persoon, die hij in opdracht van en namens de Zorgaanbieder verwerkt, niet aan anderen dan degenen waaraan de Deelnemer de gegevens mag verstrekken c.q. op grond van een wettelijke verplichting moet verstrekken. Het is de Deelnemer uitdrukkelijk verboden om data betreffende de Persoon te verkopen.

5.7 Voor de Diensten van de Deelnemer die geschieden in opdracht van de Zorgaanbieder en door Deelnemer in het kader van de uitvoering van deze Overeenkomst plaatsvinden en waarbij persoonsgegevens in de zin van de AVG worden verwerkt, kan voor deze verwerking van persoonsgegevens gebruik worden gemaakt van de [modelverwerkersovereenkomst](#).

5.8 De Deelnemer en de Stichting hebben aan elkaar kenbaar gemaakt wie binnen de organisatie aanspreekbaar is op het onderwerp privacy en de bepalingen in artikel 5 van de Overeenkomst.

## Artikel 6 Aansprakelijkheid

6.1 Partijen aanvaarden door ondertekening van deze Overeenkomst aansprakelijkheid voor het eigen handelen en/of nalaten binnen de rol die zij vervullen. Gebruikers kunnen zich jegens Partijen onmiddellijk en direct op deze aansprakelijkheid beroepen.

6.2 In het kader van aansprakelijkheid gelden de algemene regels van het Nederlands recht ten aanzien van de inhoud en omvang van wettelijke verplichtingen tot schadevergoeding.

6.3 De Deelnemer vrijwaart de Stichting MedMij voor vorderingen van derden, uit welke hoofde dan ook, ten gevolge van het gebruik van Diensten en Gegevensdiensten van de Deelnemer.

## Artikel 7 Opschorting en ontbinding

7.1 De Stichting is gerechtigd de Overeenkomst door middel van een aangetekend schrijven met onmiddellijke ingang buiten rechte te ontbinden, indien de Deelnemer ook na schriftelijke ingebrekestelling stellende een redelijke termijn in gebreke blijft enige verplichting(en) uit deze Overeenkomst te voldoen.

7.2 Buiten hetgeen elders in deze Overeenkomst is bepaald, is de Stichting MedMij gerechtigd deze Overeenkomst door middel van een aangetekend schrijven met onmiddellijke ingang buiten rechte zonder dat enige ingebrekestelling is vereist te ontbinden indien:

1. De Deelnemer zijn faillissement aanvraagt of failliet is verklaard.
2. De Deelnemer (voorlopige) surseance van betaling aanvraagt of aan hem surseance van betaling is verleend, of onder een schuldsaneringsregeling valt.
3. De onderneming van Deelnemer wordt geliquideerd.
4. De Deelnemer zijn huidige onderneming staakt dan wel op een aanmerkelijk deel van het vermogen van de Deelnemer beslag wordt gelegd.

7.3 Indien niet-nakoming als bedoeld in artikel 7.1 van de Overeenkomst een gevaar vormt voor de veilige en betrouwbare werking van het Netwerk is de Stichting MedMij gerechtigd passende maatregelen te treffen, waaronder het sommeren van de Deelnemer de levering van Diensten per direct voor een bepaalde tijd op te schorten.

7.4 Indien de Stichting MedMij gebruik maakt van het recht als bedoeld in artikel 7.2 en/of 7.3 van de Overeenkomst meldt hij dit onverwijld aan de Deelnemer.

## **Artikel 8 Verantwoordelijkheid voor derde partij**

8.1 Het is de Deelnemer toegestaan voor zijn Diensten derden in te schakelen.

8.2 Indien de Deelnemer derden inschakelt voor de verwerking van persoonsgegevens, vertaalt de Deelnemer de voor hem geldende afspraken uit het MedMij Afsprakenstelsel in dit kader door naar (sub) verwerkers. De uitvoering van de verwerking van persoonsgegevens door een door de Deelnemer ingeschakelde verwerker wordt geregeld in een (sub)verwerkersovereenkomst.

8.3 De Deelnemer staat er jegens de Stichting MedMij voor in dat de door hem ingeschakelde derde voor zijn Diensten en/of Gegevensdiensten alle verplichtingen uit deze Overeenkomst nakomt en is aansprakelijk voor het handelen op grond van deze Overeenkomst van de door hem ingeschakelde derde.

## **Artikel 9 Controle naleving**

9.1 De Stichting MedMij is bevoegd te (laten) onderzoeken of de Deelnemer de afspraken, eisen en voorwaarden uit het MedMij Afsprakenstelsel en deze Overeenkomst naleeft.

9.2 De Deelnemer verleent zijn medewerking aan een onderzoek tot naleving van het MedMij Afsprakenstelsel en deze Overeenkomst door of namens de Stichting MedMij, dan wel verstrekt de Stichting MedMij in dit kader alle noodzakelijke informatie op eerste verzoek.

## **Artikel 10 Geheimhouding**

10.1 Partijen nemen in relatie tot het MedMij Afsprakenstelsel strikte geheimhouding in acht voor zover het vertrouwelijke informatie betreft of informatie waarvan men het vertrouwelijk karakter redelijkerwijs kan vermoeden, tenzij een wettelijke plicht of een rechterlijke uitspraak openbaarmaking van deze gegevens gebiedt.

## **Artikel 11 Intellectueel eigendom**



11.1 Alle intellectuele eigendom voor alle soorten zaken die worden ontwikkeld door, voor of namens de Stichting MedMij, zoals bijdragen aan Request For Changes (RFC'S) en/of overige documentatie die bijdragen aan de ontwikkeling van de afspraken binnen het MedMij Afsprakenstelsel en die via het MedMij Afsprakenstelsel openbaar worden gemaakt, komen toe aan Stichting MedMij.

11.2 Alle auteursrechten die door de Deelnemer kunnen worden uitgeoefend voor alle soorten zaken die worden ontwikkeld door, voor of namens de Stichting MedMij, waar en wanneer dan ook, zoals bijdragen aan Request For Changes (RFC'S) en/of overige documentatie die via het MedMij Afsprakenstelsel openbaar worden, berusten bij de Stichting MedMij. Deze intellectuele eigendomsrechten worden op grond van deze Overeenkomst door Deelnemer om niet aan de Stichting MedMij overgedragen, welke overdracht door Stichting MedMij wordt aanvaard.

11.3 De Deelnemer doet hierbij afstand jegens de Stichting MedMij voor zover van toepassing op bijdragen aan de ontwikkeling van de afspraken binnen het MedMij Afsprakenstelsel zoals bedoeld in artikel 11.1, alsmede van alle eventueel aan hem toekomende persoonlijkheidsrechten als bedoeld in de Auteurswet en voor zover de toepasselijke regelgeving zodanige afstand toelaat. Deelnemer doet dit ook namens eventueel aan zijn zijde betrokken personeelsleden afstand jegens de Stichting MedMij van alle eventueel aan deze personeelsleden toekomende persoonlijkheidsrechten, in de mate waarin de toepasselijke regelgeving zodanige afstand toelaat.

11.4 De Deelnemer heeft het niet-exclusieve en niet-overdraagbare recht om, gedurende de looptijd van deze Overeenkomst, het Merk te gebruiken in verband met het aanbieden van Diensten, in overeenstemming met deze Overeenkomst en de daaruit voortvloeiende voorschriften.

11.5 De Deelnemer zal niets doen dan wel nalaten waardoor de rechten van de Stichting MedMij ten aanzien van het Merk kunnen worden aangetast en/of de ter zake van het Merk opgebouwde goodwill negatief zou kunnen worden beïnvloed en zal op geen enkele wijze, direct dan wel indirect schade toebrengen aan het Merk zoals, maar niet beperkt tot, het niet voldoen aan de privacy- en beveiligingseisen.

## **Artikel 12 Overdraagbaarheid rechten en verplichtingen overeenkomst**

12.1 Partijen zijn niet bevoegd hun rechten en verplichtingen uit de Overeenkomst over te dragen aan een derde, behalve na schriftelijke toestemming van de wederpartij.

12.2 In het geval de Deelnemer zijn rechten en plichten uit de Overeenkomst wil overdragen, dient de overnemende partij eveneens toegelaten te zijn tot het MedMij Afsprakenstelsel in de rol van Dienstverlener zorgaanbieder.

## **Artikel 13 Geschillen en toepasselijk recht**

13.1 Partijen proberen ieder geschil naar aanleiding van deze Overeenkomst eerst in onderling overleg op te lossen. Indien Partijen het geschil ter zake van deze Overeenkomst niet in onderling overleg kunnen oplossen, zal het geschil worden voorgelegd aan de ter zake bevoegde rechter te Utrecht, tenzij Partijen zelf alsnog minitrial, bindend advies, arbitrage of andere vormen van alternatieve geschillenbeslechting overeenkomen.

13.2 Op deze Overeenkomst, de uitvoering van deze Overeenkomst en op alle geschillen die daaruit mochten voortvloeien is Nederlands recht van toepassing.

## Artikel 14 Overig

14.1 Deze Overeenkomst komt in de plaats van en vervangt alle eerdere overeenkomsten en/of bindende afspraken tussen Partijen in relatie tot het MedMij Afsprakenstelsel.

14.2 De Deelnemer is in de Europese Unie ingeschreven in een door het betreffende lidstaat van vestiging erkend handelsregister.

14.3 In het geval de Deelnemer van juridische status verandert en daarmee mogelijk niet meer aan de toetredingseisen voldoet, dient de Deelnemer deze wijziging schriftelijk te melden aan de Stichting MedMij. Te denken valt aan overname door een onderneming buiten Nederland of de EU, fusie of splitsing en faillissement. In het geval van wijziging van de juridische status behoudt de Stichting MedMij het recht de Overeenkomst te beëindigen en/of de Deelnemer te vragen opnieuw de Toetredingsprocedure te doorlopen.

Aldus overeengekomen in tweevoud,

Namens MedMij	Namens de Deelnemer
Naam:	Naam:
Functie:	Functie:
Datum:	Datum:
Plaats:	Plaats:
<Handtekening Stichting MedMij	<Handtekening deelnemer>

## Toetreding

Toetreding beschrijft de afspraken rondom toetreding tot het MedMij Afsprakenstelsel. Hierbij beschrijft het [Toetredingsbeleid](#) de belangrijkste kaders en het [Toetredingsproces](#) de processtappen. De [Zelfverklaring integriteit](#) en [Intentieverklaringen](#) zijn documenten die in het toetredingsproces worden gebruikt.

## Toetredingsbeleid

Het toetredingsbeleid beschrijft de belangrijkste kaders waarbinnen de toetreding tot het MedMij Afsprakenstelsel plaatsvindt.

Het bestuur van Stichting MedMij besluit over toetreding van deelnemers. De uitvoeringsorganisatie bereidt, met input van de aanmeldende partij, deze besluitvorming voor conform het [Toetredingsproces](#). De uitvoeringsorganisatie ziet erop toe dat een nieuwe deelnemer, alvorens toe te treden, over juiste en volledige informatie beschikt en dat is vastgesteld of de partij aan de afspraken kan voldoen. Op basis van de verzamelde input formuleert de uitvoeringsorganisatie een advies aan het bestuur. Deelname van een nieuwe partij wordt alleen afgeraden wanneer een partij niet voldoet aan de eisen, dan wel er andere zwaarwegende motivaties zijn om deze partij niet toe te laten treden.

De uitvoeringsorganisatie toetst voorafgaand aan het toetredingsproces op de aanwezigheid van:

- De basale informatie over de potentiële deelnemer, zoals organisatie- en contactgegevens (van wettelijk vertegenwoordiger en contactpersoon voor toetreding);
- Een door de potentiële deelnemer ingevulde en ondertekende [Zelfverklaring integriteit](#);
- Een inschrijving in een handelsregister in de EU;
- Een intentieverklaring Kandidaat-deelnemer voor de betreffende rol waarin de *Deelnemer* toetreedt.

Na een positieve beoordeling van de aangeleverde documentatie is de aanmeldende partij kandidaat-deelnemer. Tijdens het vervolg van het toetredingsproces dient de kandidaat-deelnemer erkend te worden als ontsluiters van minimaal één gegevensdienst (zie [Gegevensdienstenbeleid](#) en [Testbeleid](#)). Toetreding vindt plaats op basis van de dan verplichte release van het MedMij Afsprakenstelsel (zie [Change- en releasebeleid](#)).

Ook dient de kandidaat-deelnemer bewijs van NEN7510-certificering en de aanvullende auditverklaring, conform het [Normenkader informatiebeveiliging](#), aan te leveren. Het toetredingsproces wordt afgerond met de ondertekening van de [Deelnemersovereenkomst](#) door de kandidaat-deelnemer en Stichting MedMij.

In de situatie dat een kandidaat-deelnemer reeds over een geldig NEN 7510-certificaat beschikt, waarbij het MedMij Afsprakenstelsel nog geen onderdeel uitmaakt van de scope, dan kan deze worden gebruikt voor toetreding tot MedMij. Wel dient de vereiste aanvullende auditverklaring met onderbouwende rapportage van een certificerende instelling te worden aangetoond voor het Normenkader MedMij. Op het moment dat hercertificering op NEN 7510 plaatsvindt, moet het MedMij Afsprakenstelsel wel onderdeel uitmaken van de scope.

Na de toetreding levert de *Deelnemer* de informatie aan voor de *Whitelist*, *OAuthClientList* en de *Zorgaanbiederslijst*, conform de registratieprocessen daarvoor (zie [Operationele processen](#)).

De implementatie van de afspraken en het aanleveren van de juiste informatie is de verantwoordelijkheid van de *Deelnemer*. Waar nodig en gepast kan de beheerorganisatie ondersteuning bieden door concrete problemen op te lossen, voorlichting te geven over het MedMij Afsprakenstelsel en ondersteuning te bieden in de vorm van aanvullende workshops, ketentesten en POC's.

Bij toetreding worden met de deelnemer aanvullend ook afspraken gemaakt over de rol in de governance. Zo kan een *Deelnemer* plaatsnemen in de Deelnemersraad en bij overleggen over de doorontwikkeling.

## Toetredingsproces

Het toetredingsbeleid beschrijft het proces van toetreding tot het MedMij Afsprakenstelsel.

- **Doel:** Het toetredingsproces heeft als doel een gecontroleerde toetreding tot het MedMij Afsprakenstelsel mogelijk te maken.
- **Initiatie:** Deelnemer wil toetreden tot het afsprakenstelsel.
- **Afspraken over het proces:**
  - Potentiële deelnemer toont aan te voldoen aan de afspraken uit de [Afsprakenset release 1.2.0](#);
  - Potentiële deelnemer en Stichting MedMij bekrachtigen de toetreding door het ondertekenen van de [Deelnemersovereenkomst](#).
- **Resultaat:** Deelnemer is toegetreden tot het afsprakenstelsel.
- **Uitzonderingen:** Deelnemer is niet toegelaten tot het stelsel, omdat niet aan alle afspraken wordt voldaan.

## Zelfverklaring integriteit

### Doel

Toelating van een partij waarvan de integriteit in het geding is, kan het merk en de geloofwaardigheid hiervan aantasten. Met de zelfverklaring integriteit heeft het bestuur van Stichting MedMij een instrument om bij toetreding in kaart brengen welke issues bij de potentiële deelnemer spelen op het gebied van integriteit. Met de verklaring wordt getracht integriteitskwesties van (bestuurders van) de potentiële deelnemer vroegtijdig aan het licht te krijgen. Denk bijvoorbeeld aan het niet zijn nagekomen van belangrijke wettelijke verplichtingen op het gebied van privacy en informatiebeveiliging. De aanwezigheid van integriteitskwesties kan reden zijn voor het bestuur om een deelnemer uit te sluiten voor deelname. Mocht een deelnemer bij toetreding de verklaring niet naar waarheid hebben ingevuld, dan kan dit aanleiding geven om alsnog de deelnemersovereenkomst te ontbinden.

Zie [Zelfverklaring integriteit MedMij Afsprakenstelsel](#) voor de Word-versie van de zelfverklaring.

### Ondergetekende,

Bedrijf:

Naam rechtsgeldig vertegenwoordiger:

Handelsnaam:

KvK nummer:

### Contactpersoon

Naam contactpersoon:

Functie:

E-mailadres:

Telefoonnummer:

### Verklaart hierbij als potentiële deelnemer voor de rol waarvoor hij wenst toe te treden tot het MedMij Afsprakenstelsel dat:

I. De potentiële deelnemer zelf, of iemand die lid is van het bestuurs-, leidinggevend of toezichthoudend orgaan van de potentiële deelnemer of daarin vertegenwoordigings-, beslissings- of controlebevoegdheid heeft, niet is veroordeeld bij onherroepelijk vonnis, welk vonnis niet langer dan vijf jaar geleden is gewezen voor een veroordeling met betrekking tot:

1. deelneming aan een criminele organisatie in de zin artikel 140 Wetboek van Strafrecht (WvSr);
2. corruptie (328ter WvSr) ;
3. fraude in de zin van diefstal (310 WvSr), verduistering (321WvSr), valsheid in geschriften (225 WvSr), oplichting (326 WvSr) en bedrog bij jaarstukken (336 WvSr).

II. Op de potentiële deelnemer geen van de volgende situaties van toepassing is:

1. hij failliet is, of
2. hij in staat van insolventie of liquidatie verkeert, of
3. hij een regeling met schuldeisers heeft getroffen, of
4. hij in een andere, vergelijkbare toestand ingevolge een soortgelijke procedure uit hoofde van nationale wet- of regelgeving verkeert, bijvoorbeeld doordat de potentiële deelnemer een schuldsaneringsregeling heeft getroffen op basis van de Wet schuldsanering natuurlijke personen, of
5. zijn activa worden beheerd door een curator of door de rechtbank, of f) zijn bedrijfsactiviteiten zijn gestaakt.

III. De potentiële deelnemer zelf, of iemand die lid is van het bestuurs-, leidinggevend of toezichthoudend orgaan van de potentiële deelnemer of daarin vertegenwoordigings-, beslissings- of controlebevoegdheid zich niet schuldig heeft gemaakt aan ernstige beroepsfouten.

IV. Dat de potentiële deelnemer kan bevestigen dat hij aantoonbaar en controleerbaar voldoet aan de beginselen en verplichtingen van de Algemene Verordening Gegevensbescherming (AVG).

V. De potentiële deelnemer kan bevestigen dat:

1. hij zich niet in ernstige mate schuldig heeft gemaakt aan valse verklaringen bij het verstrekken van de informatie aangaande deze zelfverklaring, en
2. hij geen informatie heeft achtergehouden aangaande deze zelfverklaring.

### Nadere toelichting door potentiële deelnemer

Indien de potentiële deelnemer één of meerdere van de bovengenoemde punten niet positief kan bevestigen, graag hieronder per onderwerp een toelichting opnemen met daarbij een duidelijke omschrijving van:

1. wat thans precies de concrete situatie is, en
2. welke acties en/of adequate maatregelen binnen welke tijdsperiode zijn en/of worden opgenomen, en
3. de redenen waarom de potentiële deelnemer desondanks een betrouwbare partij is, en
4. waarom Stichting MedMij wel zou moeten besluiten om potentiële deelnemer als deelnemer toe te laten tot toelating tot het MedMij Afsprakenstelsel.

Onderwerp <sup>1</sup>	Toelichting acties en maatregelen
1. ....	1. .... 2. .... 3. .... 4. ....
2. ....	

Tot slot

Ondergetekende verklaart desgevraagd en onverwijld de eventuele bewijsstukken - in het kader van bewijsvoering van deze zelfverklaring en de besluitvorming over de toetreding als deelnemer tot het MedMij Afsprakenstelsel - op eerste verzoek van de Stichting MedMij te kunnen overleggen.

Datum:

Plaats:

Functie

Naam:

<Handtekening deelnemer><sup>2</sup>

#### **Noot**

- 1. Opnemen onderwerp dat niet positief kan worden bevestigd.*
- 2. Ondertekening dient plaats te vinden door een bevoegd vertegenwoordiger van de rechtspersoon. Dat kan zijn de statutair bestuurder van de rechtspersoon of een gevolmachtigde, in dat geval moet een kopie van een volmacht worden bijgevoegd. Indien dit document afgedrukt meerdere pagina's bestrijkt, graag alle voorliggende pagina's paraferen.*



## Intentieverklaringen

De Intentieverklaringen expliciteert de verwachtingen die de kandidaat-deelnemer en Stichting MedMij van elkaar mogen hebben rondom het toetredingsproces. Er is een [Intentieverklaring Dienstverlener persoon](#) en een [Intentieverklaring Dienstverlener zorgaanbieder](#). De inhoud van de verklaring is voor beide rollen hetzelfde, de terminologie is per verklaring toegespitst op de rol.

## Intentieverklaring Dienstverlener persoon

De Intentieverklaring Dienstverlener persoon expliciteert de verwachtingen die de kandidaat-deelnemer voor de rol van Dienstverlener persoon en Stichting MedMij van elkaar mogen hebben rondom het toetredingsproces. Zie [Voorbeeld intentieverklaring Dienstverlener Persoon](#) voor een pdf-versie van de Intentieverklaring Dienstverlener persoon. Dit document dient als voorbeeld. De intentieverklaring wordt bij een volledige aanmelding tot kandidaat-deelnemer opgemaakt door de uitvoeringsorganisatie.

### Ondergetekenden,

<< Naam Bedrijf >>, gevestigd en kantoorhoudende te << Plaatsnaam, postcode en adres >>, ten deze rechtsgeldig vertegenwoordigd door << naam + functie >>,

Hierna verder te noemen: 'kandidaat-deelnemer'

Stichting MedMij, gevestigd en kantoorhoudend te << Plaatsnaam, postcode en adres >>, ten deze rechtsgeldig vertegenwoordigd door << naam + functie >>,

Hierna verder te noemen 'Stichting MedMij'

Hierna gezamenlijk te noemen: Partijen

### Overwegende dat:

1. Stichting MedMij verantwoordelijk is voor het beheer en de doorontwikkeling van het MedMij Afsprakenstelsel;
2. VZVZ Servicecentrum in opdracht van de Stichting MedMij zorgdraagt voor het beheer, de doorontwikkeling en de toetreding van partijen tot het MedMij Afsprakenstelsel;
3. Nictiz in opdracht van Stichting MedMij zorgdraagt voor de coördinatie van de informatiestandaarden waarnaar bij de gegevensdiensten in het MedMij Afsprakenstelsel wordt verwezen;
4. Stichting MedMij, in gezamenlijkheid met VZVZ Servicecentrum en Nictiz, zich inspannen kandidaat-deelnemer naar beste vermogen te ondersteunen bij het doorlopen van het toetredingsproces voor deelname aan het MedMij Afsprakenstelsel;
5. kandidaat-deelnemer kennis heeft genomen van de meest recente versie van het MedMij Afsprakenstelsel en de informatiestandaarden waarnaar bij de gegevensdiensten in het MedMij Afsprakenstelsel wordt verwezen;
6. kandidaat-deelnemer begrijpt wat deelname aan het MedMij Afsprakenstelsel betekent;
7. kandidaat-deelnemer zelf verantwoordelijk is voor de implementatie van het MedMij Afsprakenstelsel voor de rol waarvoor hij toetreedt;
8. kandidaat-deelnemer begrijpt dat voor de gegevensdiensten die hij via het MedMij-netwerk wenst te leveren, voordat deze in productie mogen worden uitgewisseld - als onderdeel van het toetredingsproces van het MedMij Afsprakenstelsel - eerst met succes een toets moet worden afgelegd op de inhoud van de informatiestandaard (kwalificatie) en op de uitwisseling van de gegevensdienst (acceptatie);
9. kandidaat-deelnemer begrijpt dat het MedMij Afsprakenstelsel op het moment van ondertekening van deze Intentieverklaring nog in ontwikkeling is en dat de kwalificatie op de inhoud en de acceptatie op de uitwisseling zoals genoemd in Overweging VIII. alleen kan worden ontvangen op basis van de formele release van het MedMij Afsprakenstelsel;

10. kandidaat-deelnemer begrijpt dat de release van het MedMij Afsprakenstelsel zoals gepubliceerd op het moment van ondertekening van deze Intentieverklaring niet de formele release van het MedMij Afsprakenstelsel is, maar juist is bedoeld ter voorbereiding op toetreding tot de formele release van het MedMij Afsprakenstelsel.
11. kandidaat-deelnemer alleen wordt toegestaan een rol in het MedMij-netwerk te vervullen indien zij daartoe een Deelnemersovereenkomst met de Stichting MedMij heeft afgesloten;

## **Verklaren als volgt:**

### **Artikel 1 Onderwerp**

- 1.1 Kandidaat-deelnemer wenst toe te treden als Deelnemer van het MedMij Afsprakenstelsel in de rol van Dienstverlener persoon.
- 1.2 Kandidaat-deelnemer gegevensdiensten levert zoals gedefinieerd in het MedMij Afsprakenstelsel.
- 1.3 De in artikel 1.2 bedoelde gegevensdiensten, als onderdeel van het toetredingsproces van het MedMij Afsprakenstelsel, worden gekwalificeerd op de inhoud van de informatiestandaard en worden geaccepteerd op de uitwisseling overeenkomstig het bepaalde in het MedMij Afsprakenstelsel.
- 1.4 Kandidaat-deelnemer een inspanningsverplichting heeft een kwalificatie op de informatiestandaarden zoals opgenomen in het MedMij Afsprakenstelsel via Nictiz te behalen.
- 1.5 Kandidaat-deelnemer een inspanningsverplichting heeft een acceptatie op de uitwisseling overeenkomstig het bepaalde in het MedMij Afsprakenstelsel via VZVZ Servicecentrum te behalen.
- 1.6 Kandidaat-deelnemer in het bezit komt van de benodigde NEN 7510-certificering overeenkomstig het bepaalde in het MedMij Afsprakenstelsel, alsmede van de aanvullende auditverklaringen als bedoeld in het Normenkader informatiebeveiliging van het MedMij Afsprakenstelsel.
- 1.7 Stichting MedMij zorgdraagt voor de volledigheid van de benodigde documentatie en de toegankelijkheid van de laatst geldende versie van het MedMij Afsprakenstelsel opdat kandidaat -deelnemer opvolging kan geven aan de artikelen 1.2, 1.3, 1.4, 1.5 en 1.6 van deze Intentieverklaring.
- 1.8 Stichting MedMij zich inspant om kandidaat-deelnemer waar mogelijk in het toetredingsproces te ondersteunen.
- 1.9 Stichting MedMij zorgdraagt voor duidelijke communicatie over de planning van het toetredingsproces.
- 1.10 Partijen bereid zijn om aan het eind van het succesvol doorlopen van het toetredingsproces de Deelnemersovereenkomst Dienstverlener persoon te sluiten.

### **Artikel 2 Contactpersoon en rapportage**

- 2.1 Partijen wijzen een contactpersoon aan die als primair aanspreekpunt fungeert voor de tenuitvoerlegging van deze Intentieverklaring.
- 2.2 De in artikel 2.1 genoemde contactpersonen hebben tot taak de contacten over de (wijze van) uitvoering van de Intentieverklaring te coördineren en te onderhouden.

2.3 In het geval de voortgang van de werkzaamheden bij één van de Partijen vertraging dreigt te ondervinden, stellen de contactpersonen elkaar hiervan zo spoedig mogelijk op de hoogte, alsmede wat de oorzaak van de vertraging is en wat de consequenties van de vertraging zijn.

### **Artikel 3 Communicatie**

3.1 Partijen zullen persberichten aangaande de toetreding tot het MedMij Afsprakenstelsel met elkaar afstemmen en berichten pas naar buiten brengen nadat beide Partijen met het persbericht hebben ingestemd.

### **Artikel 4 Geheimhouding**

4.1 Partijen zullen zich ervoor inspannen dat informatie welke hen in het kader van deze Intentieverklaring bereikt en waarvan zij weten althans behoren te weten dat deze informatie een vertrouwelijk karakter heeft, niet aan derden bekend wordt, anders dan na schriftelijke toestemming van de wederpartij. Partijen zullen de in dit artikel bedoelde informatie binnen hun organisatie niet in ruimere kring verspreiden dan ten behoeve van deze Intentieverklaring noodzakelijk is en zullen aan eventueel in te schakelen derden een geheimhoudingsverplichting opleggen. Deze bepaling geldt niet voor zover Partijen wettelijk verplicht zijn bedoelde informatie aan een derde ter beschikking te stellen en evenmin voor wat betreft gegevens die aan hen ten tijde van het ter beschikking stellen reeds uit andere hoofde op rechtmatige wijze ter kennis is gekomen.

### **Artikel 5 Inwerkingtreding en duur**

5.1 Deze Intentieverklaring treedt inwerking onmiddellijk na ondertekening en eindigt met de ondertekening van de Deelnemersovereenkomst Dienstverlenerpersoon tussen Partijen.

5.2 De intentieverklaring is niet in rechte afdwingbaar met uitzondering van de in artikel 4 opgenomen geheimhoudingsbepaling.

### **Aldus verklaard in tweevoud**

Namens Stichting MedMij:

Datum:	
Plaats:	
Functie:	
Naam:	
Handtekening:	

---

Namens de kandidaat-deelnemer:

Datum:	
Plaats:	
Functie:	
Naam:	
Handtekening:	

## Intentieverklaring Dienstverlener zorgaanbieder

De Intentieverklaring Dienstverlener zorgaanbieder expliciteert de verwachtingen die de kandidaat-deelnemer voor de rol van Dienstverlener zorgaanbieder en Stichting MedMij van elkaar mogen hebben rondom het toetredingsproces. Zie [Voorbeeld intentieverklaring Dienstverlener zorgaanbieder](#) voor een pdf-versie van de Intentieverklaring Dienstverlener zorgaanbieder. Dit document dient als voorbeeld. De intentieverklaring wordt bij een volledige aanmelding tot kandidaat-deelnemer opgemaakt door de uitvoeringsorganisatie.

### Ondergetekenden,

<< Naam Bedrijf >>, gevestigd en kantoorhoudende te << Plaatsnaam, postcode en adres >>, ten deze rechtsgeldig vertegenwoordigd door << naam + functie >>,

Hierna verder te noemen: 'kandidaat-deelnemer'

Stichting MedMij, gevestigd en kantoorhoudend te << Plaatsnaam, postcode en adres >>, ten deze rechtsgeldig vertegenwoordigd door << naam + functie >>,

Hierna verder te noemen 'Stichting MedMij'

Hierna gezamenlijk te noemen: Partijen

### Overwegende dat:

1. Stichting MedMij verantwoordelijk is voor het beheer en de doorontwikkeling van het MedMij Afsprakenstelsel;
2. VZVZ Servicecentrum in opdracht van de Stichting MedMij zorgdraagt voor het beheer, de doorontwikkeling en de toetreding van partijen tot het MedMij Afsprakenstelsel;
3. Nictiz in opdracht van Stichting MedMij zorgdraagt voor de coördinatie van de informatiestandaarden waarnaar bij de gegevensdiensten in het MedMij Afsprakenstelsel wordt verwezen;
4. Stichting MedMij, in gezamenlijkheid met VZVZ Servicecentrum en Nictiz, zich inspannen kandidaat-deelnemer naar beste vermogen te ondersteunen bij het doorlopen van het toetredingsproces voor deelname aan het MedMij Afsprakenstelsel;
5. kandidaat-deelnemer kennis heeft genomen van de meest recente versie van het MedMij Afsprakenstelsel en de informatiestandaarden waarnaar bij de gegevensdiensten in het MedMij Afsprakenstelsel wordt verwezen;
6. kandidaat-deelnemer begrijpt wat deelname aan het MedMij Afsprakenstelsel betekent;
7. kandidaat-deelnemer zelf verantwoordelijk is voor de implementatie van het MedMij Afsprakenstelsel voor de rol waarvoor hij toetreedt;
8. kandidaat-deelnemer begrijpt dat voor de gegevensdiensten die hij via het MedMij-netwerk wenst te leveren, voordat deze in productie mogen worden uitgewisseld - als onderdeel van het toetredingsproces van het MedMij Afsprakenstelsel - eerst met succes een toets moet worden afgelegd op de inhoud van de informatiestandaard (kwalificatie) en op de uitwisseling van de gegevensdienst (acceptatie);
9. kandidaat-deelnemer begrijpt dat het MedMij Afsprakenstelsel op het moment van ondertekening van deze Intentieverklaring nog in ontwikkeling is en dat de kwalificatie op de inhoud en de acceptatie op de uitwisseling zoals genoemd in Overweging VIII. alleen kan worden ontvangen op basis van de formele release van het MedMij Afsprakenstelsel;

10. kandidaat-deelnemer begrijpt dat de release van het MedMij Afsprakenstelsel zoals gepubliceerd op het moment van ondertekening van deze Intentieverklaring niet de formele release van het MedMij Afsprakenstelsel is, maar juist is bedoeld ter voorbereiding op toetreding tot de formele release van het MedMij Afsprakenstelsel.
11. kandidaat-deelnemer alleen wordt toegestaan een rol in het MedMij-netwerk te vervullen indien zij daartoe een Deelnemersovereenkomst met de Stichting MedMij heeft afgesloten;

## **Verklaren als volgt:**

### **Artikel 1 Onderwerp**

1.1 Kandidaat-deelnemer wenst toe te treden als Deelnemer van het MedMij Afsprakenstelsel in de rol van Dienstverlener zorgaanbieder.

1.2 Kandidaat-deelnemer gegevensdiensten levert zoals gedefinieerd in het MedMij Afsprakenstelsel.

1.3 De in artikel 1.2 bedoelde gegevensdiensten, als onderdeel van het toetredingsproces van het MedMij Afsprakenstelsel, worden gekwalificeerd op de inhoud van de informatiestandaard en worden geaccepteerd op de uitwisseling overeenkomstig het bepaalde in het MedMij Afsprakenstelsel.

1.4 Kandidaat-deelnemer een inspanningsverplichting heeft een kwalificatie op de informatiestandaarden zoals opgenomen in het MedMij Afsprakenstelsel via Nictiz te behalen.

1.5 Kandidaat-deelnemer een inspanningsverplichting heeft een acceptatie op de uitwisseling overeenkomstig het bepaalde in het MedMij Afsprakenstelsel via VZVZ Servicecentrum te behalen.

1.6 Kandidaat-deelnemer in het bezit komt van de benodigde NEN 7510-certificering overeenkomstig het bepaalde in het MedMij Afsprakenstelsel, alsmede van de aanvullende auditverklaringen als bedoeld in het Normenkader informatiebeveiliging van het MedMij Afsprakenstelsel.

1.7 Stichting MedMij zorgdraagt voor de volledigheid van de benodigde documentatie en de toegankelijkheid van de laatst geldende versie van het MedMij Afsprakenstelsel opdat kandidaat -deelnemer opvolging kan geven aan de artikelen 1.2, 1.3, 1.4, 1.5 en 1.6 van deze Intentieverklaring.

1.8 Stichting MedMij zich inspant om kandidaat-deelnemer waar mogelijk in het toetredingsproces te ondersteunen.

1.9 Stichting MedMij zorgdraagt voor duidelijke communicatie over de planning van het toetredingsproces.

1.10 Partijen bereid zijn om aan het eind van het succesvol doorlopen van het toetredingsproces de Deelnemersovereenkomst Dienstverlener zorgaanbieder te sluiten.

### **Artikel 2 Contactpersoon en rapportage**

2.1 Partijen wijzen een contactpersoon aan die als primair aanspreekpunt fungeert voor de tenuitvoerlegging van deze Intentieverklaring.

2.2 De in artikel 2.1 genoemde contactpersonen hebben tot taak de contacten over de (wijze van) uitvoering van de Intentieverklaring te coördineren en te onderhouden.

2.3 In het geval de voortgang van de werkzaamheden bij één van de Partijen vertraging dreigt te ondervinden, stellen de contactpersonen elkaar hiervan zo spoedig mogelijk op de hoogte, alsmede wat de oorzaak van de vertraging is en wat de consequenties van de vertraging zijn.

### **Artikel 3 Communicatie**

3.1 Partijen zullen persberichten aangaande de toetreding tot het MedMij Afsprakenstelsel met elkaar afstemmen en berichten pas naar buiten brengen nadat beide Partijen met het persbericht hebben ingestemd.

### **Artikel 4 Geheimhouding**

4.1 Partijen zullen zich ervoor inspannen dat informatie welke hen in het kader van deze Intentieverklaring bereikt en waarvan zij weten althans behoren te weten dat deze informatie een vertrouwelijk karakter heeft, niet aan derden bekend wordt, anders dan na schriftelijke toestemming van de wederpartij. Partijen zullen de in dit artikel bedoelde informatie binnen hun organisatie niet in ruimere kring verspreiden dan ten behoeve van deze Intentieverklaring noodzakelijk is en zullen aan eventueel in te schakelen derden een geheimhoudingsverplichting opleggen. Deze bepaling geldt niet voor zover Partijen wettelijk verplicht zijn bedoelde informatie aan een derde ter beschikking te stellen en evenmin voor wat betreft gegevens die aan hen ten tijde van het ter beschikking stellen reeds uit andere hoofde op rechtmatige wijze ter kennis is gekomen.

### **Artikel 5 Inwerkingtreding en duur**

5.1 Deze Intentieverklaring treedt inwerking onmiddellijk na ondertekening en eindigt met de ondertekening van de Deelnemersovereenkomst Dienstverlener zorgaanbieder tussen Partijen.

5.2 De intentieverklaring is niet in rechte afdwingbaar met uitzondering van de in artikel 4 opgenomen geheimhoudingsbepaling.

### **Aldus verklaard in tweevoud**

Namens Stichting MedMij:

Datum:	
Plaats:	
Functie:	
Naam:	
Handtekening:	



---

Namens de kandidaat-deelnemer:

Datum:	
Plaats:	
Functie:	
Naam:	
Handtekening:	

## Governance

Het MedMij Afsprakenstelsel is een 'levende' set van afspraken. De zorg en IT zijn en blijven in beweging en de afspraken moeten hierbij blijven aansluiten. Ook zijn de afspraken voor deelnemers aan het stelsel niet vrijblijvend. Er moet daarom toe worden gezien op naleving van de afspraken. Dit vraagt om goed beheer en regie op de afspraken, ofwel de inrichting van governance op het afsprakenstelsel.

Hoewel er vele definities bestaan van governance kan het worden omschreven als (een reeks van) processen (tradities, beleid of regels) die formeel en/of informeel worden toegepast om verantwoordelijkheden tussen actoren van een bepaald systeem te verdelen. Governance gaat daarmee over actoren, relaties en de manier waarop een gezamenlijk doel wordt bereikt. De governance omschrijft op welke wijze de afspraken worden beheerd, welke rollen daarin te onderkennen zijn en door welke partijen die rollen worden vervuld.

Een goede inrichting van de governance draagt bij aan het vertrouwen in het stelsel. Hierbij zijn verschillende aspecten van belang. Een goede governance:

- Ziet toe op en draagt bij aan de realisatie van het hogere maatschappelijk doel, namelijk de persoon meer regie geven over de gezondheid door grip de eigen gezondheidsgegevens;
- Brengt vertegenwoordiging van de betrokken partijen in gesprek met elkaar zodat zij samen sturing kunnen geven aan het afsprakenstelsel;
- Legt taken, bevoegdheden en verantwoordelijkheden duidelijk en transparant vast;
- Legt duidelijk vast wat wel en wat niet onder verantwoordelijkheid van de governance valt;
- Borgt het publiek belang van het stelsel als geheel;
- Is slagvaardig op ieder niveau van besturing door voldoende ruimte voor besluitvorming en initiatief /innovatie;
- Is open en gaat uit van een samenwerkingsmodel. De overlegstructuur is transparant, toekomstvast en schaalbaar en kent een werkbare vorm door afvaardiging met mandaat;
- Is in overeenstemming met de mededingings- en andere wetgeving. Dienstverleners kunnen op grond van objectieve criteria en processen tot het stelsel toetreden;
- Borgt onafhankelijkheid en transparantie bij toetreding, sanctiebeleid en geschillenbeslechting, en heeft controles en toezicht goed en onafhankelijk georganiseerd;
- Is klaar voor het opvangen en oplossen van toekomstige beveiligingsincidenten en andere calamiteiten;
- Zorgt dat afspraken aan blijven sluiten bij de praktijk en nageleefd kunnen worden;
- Zorgt voor duidelijke regie op het stelsel (onder andere bij aansluiting op het stelsel, kwalificaties, toezicht en handhaving, etc.);
- Is begrijpelijk en transparant voor alle stakeholders;
- Regelt waar nodig en waar haalbaar middelen om gemeenschappelijke doelstellingen te behalen.

De keuzes op deze aspecten worden geleid door een viertal criteria:

1. **Vertrouwd.** Het belangrijkste criterium is dat de governance van het Afsprakenstelsel vertrouwen moet opwekken bij alle betrokkenen bij het stelsel. Personen moeten voldoende vertrouwen hebben in de uitwisseling van gegevens om voor elkaar te krijgen dat zij gebruik maken van PGO's, zorgaanbieders moeten hun gegevens beschikbaar durven stellen via MedMij en IT-leveranciers moeten deel willen nemen aan het stelsel.
2. **Doelgericht en doelmatig.** De besturingsstructuur moet helpen het doel van het Afsprakenstelsel MedMij op een zo efficiënt en effectief mogelijke manier te bereiken. Daarvoor moet de governance doelmatig zijn, 'lean and mean' en slagvaardig.
3. **Draagvlak.** De besturingsstructuur moet voldoende draagvlak hebben om legitiem te zijn en zijn taken goed te kunnen uitvoeren. Het is daarom belangrijk dat de governance structuur gedragen wordt door de verschillende stakeholders, en dat de structuur rekening houdt met de verhoudingen zoals ze nu zijn en kan meeveranderen naar behoefte.

4. **Omgevingsbewust.** Er zijn veel aanpalende ontwikkelingen die effect kunnen hebben op het Afsprakenstelsel of waar de verdere ontwikkeling van afhankelijk is. Om deze afhankelijkheden te ondervangen moet in de governance worden stilgestaan bij responsiviteit, de mate waarin kan worden geanticipeerd op ontwikkelingen en innovaties mogelijk kunnen worden gemaakt. Ketenproblemen moeten worden geïdentificeerd en tevens duidelijk en kloppend zijn.

Naast het afsprakenstelsel, levert het programma MedMij ook profielen bij bestaande informatiestandaarden en een financieringsstelsel op. Het beheer van deze producten, plus de activiteiten die ondernomen worden om MedMij van de grond te krijgen, moeten uiteindelijk ook ergens landen. Voor de informatiestandaarden geldt dat het afsprakenstelsel hier alleen naar verwijst en dat het beheer bij andere partijen is belegd (bijvoorbeeld bij Nictiz, Zorginstituut Nederland, etc.). Voor het financieringsstelsel geldt dat zij waarschijnlijk moet landen in de governance van de financierende partij(en). Van de stimulerende activiteiten om MedMij van de grond te krijgen, moet verder nog worden bepaald óf en waar deze moeten worden belegd.

De governance wordt in de documentatie nader uitgewerkt aan de hand van de volgende onderwerpen:

- **Rollen:** welke rollen zijn te onderkennen binnen de governance en welke partijen vullen deze rollen in?
- **Inrichting:** hoe ziet met deze rollen de inrichting van de governance eruit en welke verantwoordelijkheden hebben zij hierbinnen?
- **Statuten Stichting MedMij:** de formele vertaling van de rollen en inrichting in statuten voor de rechtspersoon Stichting MedMij.

## Rollen

Rollen beschrijft de rollen die binnen de governance te onderkennen zijn en welke partijen deze rollen invullen.

Binnen de governance worden zes rollen onderscheiden, namelijk:

- **Deelnemer:** een partij die dienstverlening aanbiedt binnen het MedMij Afsprakenstelsel;
- **Gebruiker:** een partij die gebruik maakt van dienstverlening van deelnemers aan het afsprakenstelsel;
- **Eigenaar:** een partij die eindverantwoordelijk is voor het stelsel en de strategische kaders;
- **Financier:** een partij die het beheer van het stelsel financiert;
- **Beheerder:** een partij verantwoordelijk voor het beheer van het afsprakenstelsel;
- **Toezichthouder:** een partij die toeziet op het handelen binnen wet- en regelgeving;

Een groot aantal partijen hebben belang bij het bestaan van het afsprakenstelsel en kunnen in meer of mindere mate deze rollen invullen:

- Individuele personen, met als specifieke doelgroep patiënten
- Vertegenwoordiging van patiënten
- Zorgaanbieders, waaronder huisartsen, ziekenhuizen, verpleeghuizen en andere partijen die omwille van hun professie gegevens over jouw gezondheid bijhouden;
- Rijksoverheid
- Gemeenten
- PGO-leveranciers
- XIS-leveranciers
- Andere ICT-dienstverleners (integrators, infrastructuurpartijen, etc.)
- Zorgverzekeraars
- Standaardisatie-instituten
- Certificerings- en auditbureaus

Hieronder wordt beargumenteerd welke rol MedMij ziet voor deze partijen binnen de governance van het stelsel.

### Deelnemer

Een deelnemer biedt diensten aan binnen het MedMij Afsprakenstelsel vanuit de rol van Dienstverlener persoon en/of Dienstverlener zorgaanbieder. Zie [Opzet](#) voor meer informatie over de rol van dienstverlener in het stelsel. Partijen die de rol van deelnemer kunnen invullen zijn XIS-, PGO-leveranciers en andere IT-dienstverleners in de zorg. Ook zorgaanbieders, die eigen IT-systemen ontwikkelen en hiermee willen toetreden tot het stelsel, acteren als deelnemer.

#### Deelnemer MedMij Afsprakenstelsel

XIS-, PGO-leveranciers en andere IT-dienstverleners in de zorg.

### Gebruiker

Een gebruiker neemt diensten af van deelnemers aan het MedMij afsprakenstelsel. Onder gebruikers verstaan we patiënten en zorgaanbieders, maar ook PGO- en XIS-leveranciers die bij de ontsluiting van gegevens richting MedMij ontlast worden door deelnemers aan het stelsel. Zie [Opzet](#) voor meer informatie over de rol van gebruiker in het stelsel.

### **Gebruiker MedMij Afsprakenstelsel**

Patiënten, zorgaanbieders, PGO- en XIS-leveranciers.

## **Eigenaar**

Een eigenaar is eindverantwoordelijk voor het stelsel en bepaalt de strategische koers. Het gaat dan om verantwoordelijkheid voor het grotere geheel en niet om verantwoordelijkheid voor individuele dienstverlening (deze ligt bij deelnemers zelf). Kijkend naar de lijst van betrokken actoren is er een bijna onuitputtelijke lijst van mogelijke combinaties van eigenaren te benoemen. Echter een groot deel lijkt al bij voorbaat af te vallen, zeker als we kijken naar het doel van MedMij en hoe partijen participeren. De doelstelling van MedMij maakt het bijna vanzelfsprekend dat in ieder geval patiënten en zorgaanbieders optreden als eigenaar. Immers, zij zijn de voornaamste belanghebbenden en zullen vanuit dat belang stevige invloed willen kunnen uitoefenen op het blijvend functioneren van het afsprakenstelsel.

Achter het belang van patiënten en zorgaanbieders gaat een forse marktpotentie schuil voor de deelnemers aan het stelsel. Vanuit die potentie zouden ook zij wellicht eigenaar willen zijn van het stelsel. Zeker ook omdat zij uiteindelijk moeten voldoen aan de afspraken. Een wezenlijke vraag die speelt is of deelnemers ook tegelijkertijd eigenaar zouden mogen zijn. Kijken we naar bestaande afsprakenstelsels zoals iDEAL, GSM en eHerkenning, dan lijkt dat gebruikelijk. Gelet op de doelstelling van MedMij, het belang om de patiënt centraal te stellen, alsook op termijn het afsprakenstelsel te verbreden naar andere sectoren omdat gezondheid geen monopolie is van zorg, alsmede de belangenverstrengeling die dan kan ontstaan tussen het 'doel' waar de eigenaren zich hard voor maken en de 'middelen' die van de deelnemers komen, is het wenselijk om de rollen waar mogelijk gescheiden te houden. Dit leidt dan tot de afweging dat deelnemers, lees: de ICT-leveranciers in de zorg, geen eigenaarschap inzake MedMij op zich kunnen nemen. Zij krijgen wel, vanwege het grote belang van deze partijen bij de uitvoering, een (andere) rol in de besturing.

De overheid is belanghebbende, maar gelet op haar meer afstandelijke positie met betrekking tot de zorgsector ligt (mede-)eigenaarschap wat minder voor de hand. De zorgverzekeraars hebben wellicht wel een voorkeur om als eigenaar deel te nemen in MedMij, te meer omdat verdergaande digitalisering in de zorg, en dan met name in het primaire zorgproces (eHealth toepassingen) kunnen bijdragen aan de efficiency en kwaliteitsverhoging van de zorg. Burgers en zorgaanbieders zijn echter huiverig voor grote inmenging van overheid en zorgverzekeraars met betrekking tot zorginformatie. We volgen daarom het advies van PBLQ, dat is gegeven na een eerste verkenning van de governance voor het afsprakenstelsel, waarin zij stellen dat deelname van zorgverzekeraars en overheid in de actieve besluitvorming potentieel minder vertrouwenwekkend is voor burgers en politiek.

De andere genoemde instanties zoals standaardisatiebureaus, certificatie- en auditbureaus zijn minder voor de hand liggend als mogelijke eigenaar, al is het wel weer mogelijk dat dergelijke bureaus in opdracht c.q. ten behoeve van MedMij werkzaamheden uitvoeren.

### **Eigenaar MedMij Afsprakenstelsel**

Om het belang van patiënten en zorgaanbieders blijvend te borgen, gericht op vertrouwde uitwisseling van gezondheidsgegevens, en te voorkomen dat die belangen vermengd raken met andere, kunnen alleen zij optreden als eigenaar. Een vertegenwoordiging van deze patiënten en zorgaanbieders geeft georganiseerd sturing aan het beheer van MedMij. De organisatie waarin zij dat doen, treedt formeel op als eigenaar van het stelsel.

## **Financier**

Een financier is verantwoordelijk voor de financiële ondersteuning van het beheer van de afspraken. Een aloude zegswijze 'Wie betaalt, wie bepaalt' kan bij de vraag wie optreedt als financier behulpzaam zijn. Als gekeken wordt naar de meest voor-de-hand-liggende eigenaren, patiënten en zorgaanbieders, dan zien we

dat dit geen vermogende groepen zijn die het Afsprakenstelsel financieel kunnen trekken. Immers, patiënten c.q. burgers zijn relatief slecht georganiseerd. In onze vertegenwoordigde democratie is het daarom doorgaans de overheid die voor het belang van de burgers opkomt. Dit roept daarmee de vraag op of een eigenaar ook financier dan wel de financier ook eigenaar zou moeten zijn? Het antwoord daarop is nee. Op dit moment ondersteunt de overheid de rol van de patiënt bijvoorbeeld door de Patiëntenfederatie Nederland te subsidiëren. Dit laatste zou een wijze van financiering vanuit de overheid kunnen zijn zonder dat de overheid hoeft op te treden als (mede-)eigenaar. Op die manier bepaalt de overheid alleen of en onder welke voorwaarde de financiering wordt verstrekt, maar niet wat er op de agenda komt.

Een andere partij die, in een zelfde constructie als bij de overheid, als financier zou kunnen optreden, en ook een zeker belang heeft bij de ontwikkeling van MedMij, zijn de zorgverzekeraars. Zij hebben baat bij afspraken en een toekomstvisie die in lijn ligt met het verder ontwikkelen van PGO's ten dienste van het verbeteren van de zorg en het verlagen van de kosten.

Een andere optie is om deelnemers te laten betalen voor het beheer van de afspraken. Daarmee worden deelnemers mede-eigenaar van dat Afsprakenstelsel. Deze optie ligt nu minder voor de hand. Het programma MedMij is juist opgestart omdat er vanuit de markt onvoldoende initiatief ontstond om op non-concurrentie basis interoperabiliteitsafspraken te maken. ICT-leveranciers hebben dan ook niet direct profijt van hun investering in het beheer. Indien zij optreden als financier zullen zij daarnaast ook als eigenaar invloed willen uitoefenen, waarmee zij direct invloed krijgen op de set van eisen waar zij zelf aan moeten voldoen. Een risico hierbij is dat een 'race-to-the-bottom' ontstaat doordat de deelnemers zo min mogelijk kwijt willen zijn aan het beheer van de afspraken, waardoor een goede taakuitvoering lastig wordt. Eventueel is het mogelijk om in de toekomst nadat de markt verder is ontwikkeld de deelnemers een rol te laten spelen als financier.

Het voorstel is om overheid en zorgverzekeraars (tijdelijk) het beheer te laten financieren. Omdat de financiers geen eigenaar zijn van het stelsel, moeten zij bereid zijn om de financiering op zich te nemen zonder daarvoor 'zeggenschap' over de afspraken te verlangen. Zorgverzekeraars en overheid hebben via financiering van het beheer wel een rol in het stellen van randvoorwaarden en de besteding van de middelen. Deze financiering vanuit overheid en zorgverzekeraars is eindig, in die zin dat na een zekere periode heroverweging van de financiering aan de orde is.

#### **Financier MedMij Afsprakenstelsel**

De rijksoverheid en/of de zorgverzekeraars nemen voor de eerste jaren de financiering van het afsprakenstelsel MedMij (beheer) voor haar rekening. Dit geeft ruimte aan alle andere financiële vragen die nog voorliggen en benadrukt het belang van de overheid en de zorgverzekeraars om te komen tot een stelsel van afspraken als randvoorwaarde waarbinnen ICT-leveranciers in de zorg invulling kunnen aan de totstandkoming van diensten en producten die nodig zijn om gezondheidsgegevens uit te wisselen.

#### **Beheerder**

Gezien de grote belangen die rond het stelsel gaan spelen, is goed beheer een vereiste. Dit beheer moet uitgevoerd kunnen worden zonder dat hierbij verstremgeling van belangen kan ontstaan. Een toegewijde beheerorganisatie, de MedMij-beheerorganisatie, wordt daarom op- en ingericht om de eindverantwoordelijkheid over het pakket van [Beheerverantwoordelijkheden](#) rondom het beheer van het afsprakenstelsel te beleggen. Waar dit synergievoordelen oplevert, kunnen beheerverantwoordelijkheden door de MedMij-beheerorganisatie worden uitbesteed bij (een) bestaande beheerorganisatie(s). De verantwoordelijkheden krijgen in de dagelijkse praktijk vorm via processen. Niet met alle beheerprocessen hebben deelnemers direct te maken. De beheerprocessen waarin deelnemers zelf een rol spelen en de processen die zijn ingericht als dienstverlening vanuit de beheerorganisatie, staan beschreven bij [Operationele processen](#).

#### **Beheerder MedMij Afsprakenstelsel**

De eindverantwoordelijkheid voor het pakket van verantwoordelijkheden rondom het beheer van het afsprakenstelsel wordt belegd bij een nieuw op te richten MedMij-beheerorganisatie. Waar dit synergievoordelen oplevert, kunnen beheerverantwoordelijkheden door de MedMij-beheerorganisatie worden uitbesteed aan (een) bestaande beheerorganisatie(s).

## Toezichthouder

Toezicht is belangrijk om de integriteit van het stelsel te waarborgen. Het toezicht is voor MedMij tweeledig, namelijk extern en intern. Onder extern toezicht wordt allereerst het toezicht door de wettelijke toezichthouders verstaan. Omdat het afsprakenstelsel geen wettelijke basis heeft, is er geen wettelijk toezicht op het stelsel an sich. Wel is er toezicht op de deelnemers en de beheerder(s) in de uitvoering van wet- en regelgeving door deze partijen. De belangrijkste wet- en regelgeving die hierbij van toepassing is, staat genoemd in het [Juridisch kader](#). Deelnemers en de beheerder(s) zijn door de toezichthouders zelf aanspreekbaar op hun handelen en de bevoegdheden van de wettelijke toezichthouders zijn van kracht ongeacht de afspraken in het stelsel. De MedMij-beheerorganisatie stemt af met de toezichthouders vanuit het belang van het stelsel. Hiermee wordt ervoor gezorgd dat deelnemers en beheerorganisatie bij het hanteren van de afspraken kunnen voldoen aan de geldende wet- en regelgeving.

Een tweede vorm van extern toezicht, is het toezicht door de financiers. Zij hebben een rol in het toezicht op de besteding van de middelen.

Ten slotte is er dan nog het interne toezicht. Het gaat dan om het dagelijkse toezicht op de uitvoering van afspraken in de deelnemersovereenkomst door deelnemers. De eigenaar is verantwoordelijk voor dit interne toezicht. De beheerder voert het toezicht uit.

### **Toezichthouder MedMij Afsprakenstelsel**

Voor MedMij is sprake van wettelijk toezicht door toezichthouders, toezicht op de besteding van de middelen door de financiers en toezicht door de beheerder op het handelen van de deelnemers.

## Inrichting

Inrichting beschrijft voor de [Rollen](#) de positie en verantwoordelijkheden binnen de governance.

Een goede borging, doorontwikkeling en naleving van de afspraken is cruciaal voor het vertrouwen in en de continuïteit van MedMij. Er is op dit moment (april 2018) in de zorg geen bestaande organisatie waar de eindverantwoordelijkheid over het stelsel kan worden belegd, zonder taakvertroebeling te creëren. Een toegewijde rechtspersoon, Stichting MedMij, wordt daarom ingericht om de eindverantwoordelijkheid voor het beheer van het afsprakenstelsel bij te beleggen. Deze rechtspersoon borgt het belang van het afsprakenstelsel, neemt verantwoordelijkheid voor het beheer en is eigenaar van het merk MedMij.

De inrichting van Stichting MedMij betekent niet dat geen hergebruik wordt gemaakt van bestaande beheerexpertise in de zorg en dat alle processen bij Stichting MedMij opnieuw worden ingericht. Een van de belangrijke uitgangspunten van het afsprakenstelsel is om zoveel mogelijk aan te sluiten bij bestaande, geaccepteerde standaarden. Met wat creativiteit kan dit uitgangspunt worden vertaald naar een uitgangspunt om, waar mogelijk en gewenst, zoveel mogelijk gebruik te maken van bestaande beheerexpertise in het veld. Na een verkenning van de mogelijkheden, is daarom gekozen om een deel van de beheertaken uit te besteden aan een gevestigde beheerder, VZVZ Servicecentrum (hierna: uitvoeringsorganisatie). De verantwoordelijkheden die echt bij Stichting MedMij moeten worden ingericht kunnen hierdoor beperkt blijven. Stichting MedMij en de uitvoeringsorganisatie vormen samen het MedMij Beheer.

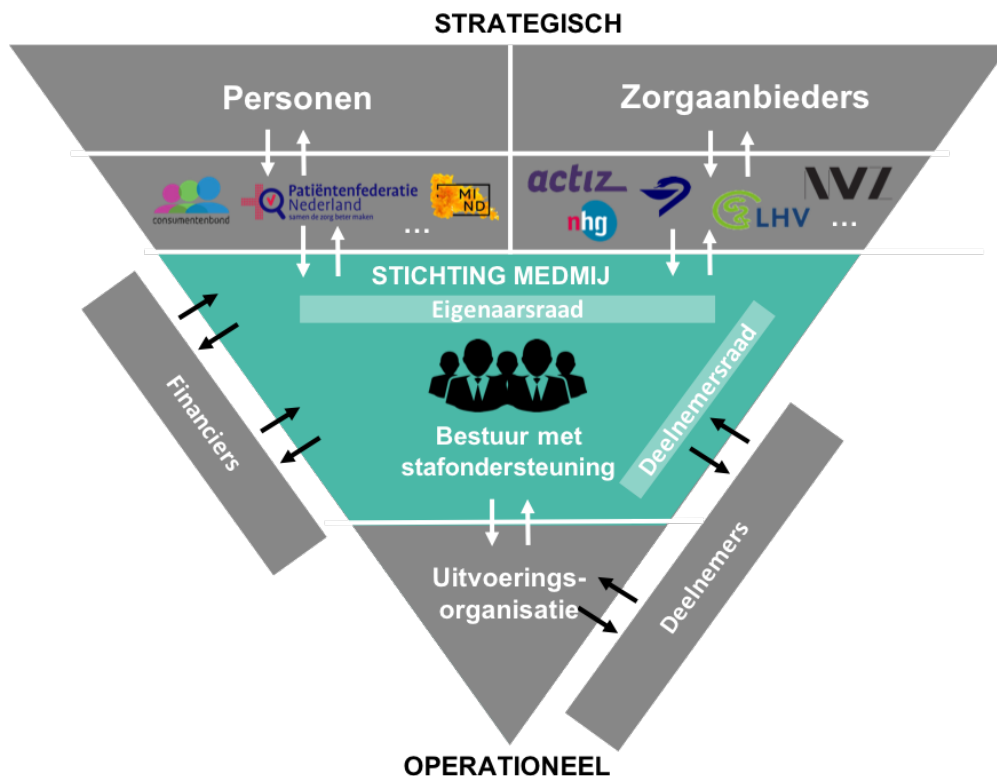
## Invulling rollen

De eerder gedefinieerde rollen moeten een plek krijgen in de governance:

- **Eigenaar/gebruiker:** De eigenaren en tevens gebruikers van het stelsel vormen de eigenaarsraad van Stichting MedMij.
- **Deelnemer:** Deelnemers zijn geen eigenaar van het stelsel, maar krijgen vanwege hun belangrijke rol in de uitvoering een expliciete plek in de governance in de vorm van een deelnemersraad. Deze deelnemersraad heeft een adviserende rol richting het bestuur. De deelnemersraad is onderdeel van Stichting MedMij.
- **Beheerder:** Beheerverantwoordelijkheden zijn er op verschillende niveaus. De meer strategische beheerverantwoordelijkheden gaan over de koers van MedMij en de dagelijkse regie daarop moet daarom belegd zijn bij Stichting MedMij. De meer tactische/operationele verantwoordelijkheden worden zoveel mogelijk belegd bij de uitvoeringsorganisatie.
- **Financier:** Financiers zijn geen eigenaar van het stelsel. Zij stellen wel kaders aan de financiering van het beheer via de financieringsrelatie. Hoe deze financiering eruit komt te zien, wordt nog uitgewerkt.
- **Toezichthouder:** Deelnemers en beheerders hebben zich per definitie te houden aan wet- en regelgeving. Voor het wettelijke toezicht op hun handelen conform deze wet- en regelgeving, zijn er de daartoe ingestelde instanties (zie [Juridisch kader](#) voor een overzicht van de toezichthouders). Daarnaast zijn de privaatrechtelijke afspraken uit het stelsel van kracht. De beheerorganisatie ziet toe op de naleving van de afspraken van deelnemers. De beheerder wint hierbij advies in van anderen, waaronder van een trusted third party voor controle op de toepassing van het normenkader door de deelnemer, van het Handelsregister, van Nictiz voor de kwalificatie op de informatiestandaarden, etc.

Schematisch vertaalt dit zich in het volgende governance-model, dat hieronder nader wordt uitgewerkt:





## Stichting MedMij

### Rechtsvorm

Bij de keuze voor een rechtsvorm is belangrijk wie eindverantwoordelijk is. Bij **Rollen** is beargumenteerd dat een vertegenwoordiging van patiënten en zorgaanbieders eigenaar is van het stelsel. Er moet dan ook een rechtsvorm worden gekozen waarin private partijen een rol kunnen spelen. Binnen publieke rechtsvormen, zoals een afdeling op het Ministerie van Volksgezondheid, Welzijn en Sport of een zelfstandig bestuursorgaan, kan dit eigenaarschap onvoldoende vorm krijgen.

Resteren de private rechtsvormen zonder winstoogmerk, de stichting en de vereniging. Een 'stichting' kenmerkt zich door snelheid en onafhankelijkheid, een vereniging (of als speciale vorm: de coöperatie) door haar legitimiteit vanwege grote inspraak van leden. In een vereniging heeft de algemene ledenvergadering het laatste woord. Hierdoor kan de besluitvorming in een vereniging veel tijd kosten. Ook de afstand van leden tot de materie komt de kwaliteit van besluitvorming vaak niet ten goede. Dat, gecombineerd met de grote fragmentatie in de zorg, maakt de kans groot dat een vereniging door te grote stroperigheid niet slagvaardig genoeg is bij het beheren en doorontwikkelen van het afsprakenstelsel. Een stichting kent dit probleem niet, omdat het bestuur eindverantwoordelijk is. Hoewel het democratisch gehalte van een vereniging groter is en er meer inspraak is van verschillende betrokkenen, kan ook in een stichting een goede relatie met het veld worden vormgegeven om de legitimiteit van de besturing te borgen. Er is daarom gekozen voor de rechtsvorm stichting.

De keuze voor de rechtsvorm stichting sluit tevens goed aan bij de wens om de rol van financier en eigenaar te scheiden. Dit kan via subsidieregelingen worden geregeld.

### Doel en middelen

Stichting MedMij heeft een afgebakend doel dat in grote mate de bewegingsvrijheid van de stichting bepaalt. Stichting MedMij wordt opgericht met als doel personen meer regie te geven over hun eigen

gezondheid door gegevensuitwisseling overeenkomstig het MedMij Afsprakenstelsel mogelijk te maken en te stimuleren. De stichting tracht dit doel te bereiken door het beheren van het MedMij Afsprakenstelsel, het doorontwikkelen van het stelsel en het waarborgen van de optimale vertrouwelijkheid, veiligheid en betrouwbaarheid van de gegevensuitwisseling volgens de afspraken uit het stelsel. Stichting MedMij zet zich daarnaast ook in om het gebruik van het MedMij Afsprakenstelsel door (potentiële) deelnemers en eindgebruikers te stimuleren.

## Bestuur en toezicht: bestuursmodel

Voor de besturing van de stichting kan worden gekozen tussen een bestuurs- en een raad-van-toezichtmodel. Het verschil tussen beide modellen ligt in de scheiding tussen toezicht en uitvoering. Bij een bestuursmodel liggen zowel toezicht als uitvoering in handen van het bestuur en zorgt vooral een evenwichtige invulling van het bestuur voor het onderlinge toezicht. In een raad-van-toezichtmodel zijn de verantwoordelijkheden voor toezicht en uitvoering duidelijk gescheiden.

Het is zeer gebruikelijk om bij de ontwikkeling van een stichting te beginnen met een bestuursmodel. Deze invulling past ook bij het uitgangspunt om de stichting licht te houden, het hanteren van een groeimodel en het feit dat er al min of meer toezichthoudende organen in het model zijn opgenomen in de vorm van een eigenaarsraad en de deelnemersraad. Het bestuursmodel wordt daarom als uitgangspunt genomen.

## Bestuur

Doordat de eigenaren zitting nemen in de eigenaarsraad, hoeft de dagelijkse besturing geen afspiegeling te zijn van personen en zorgaanbieders. Er wordt daarom een onafhankelijk bestuur ingericht dat bestaat uit minimaal drie en maximaal vijf bestuursleden. Dit aantal mag gedurende het eerste jaar na oprichting van de stichting ook lager zijn dan drie om klein op te kunnen starten naast het programma. Het bestuur wordt voorgezeten door een voorzitter, die tevens eerste aanspreekpunt is voor de dagelijkse operatie.

Het bestuur bestaat uit meerdere bestuursleden zodat verschillende perspectieven en expertise kunnen worden ingebracht, waaronder in ieder geval het perspectief van de persoon, het perspectief van de zorgaanbieder en expertise over technische, juridische, privacy- en beveiligingsaspecten van de gegevensuitwisseling. Aanvullend dienen bestuursleden bij voorkeur te beschikken over een relevant bestuurlijk netwerk, affiniteit te hebben met de digitale uitwisseling van gezondheidsgegevens (met patiënten) en affiniteit te hebben met netwerksamenwerking en het ontwikkelen van afspraken met diverse belanghebbenden. Bestuursleden dienen daarnaast gemotiveerd zijn om als ambassadeur bij te dragen aan het succes van MedMij.

Bestuursleden treden aan voor een periode van drie jaar en kunnen eenmalig herbenoemd worden voor eenzelfde periode. Alleen in uitzonderlijke gevallen is het mogelijk hier een derde periode aan vast te plakken. Het bestuur stelt een rooster van aftreden op om ervoor te zorgen dat bestuursleden gecoördineerd aftreden en ervaring zoveel mogelijk behouden blijft. Mocht een bestuurslid niet functioneren, dan kunnen de overige in functie zijnde bestuursleden gezamenlijk besluiten om dit bestuurslid te ontslaan. De eigenaarsraad kan alleen het vertrouwen in het volledige bestuur opzeggen. In dat geval defungeren alle bestuurders en stelt de eigenaarsraad een nieuw bestuur aan.

Nieuwe bestuursleden worden voorgedragen door het bestuur in lijn met de profielschetsen zoals afgestemd tussen bestuur en eigenaarsraad. De eigenaarsraad stemt in met deze voordrachten.

Het bestuur van de stichting vergadert minimaal vier keer per jaar. Deze bestuursvergaderingen zijn niet openbaar om een vrije discussie te kunnen laten plaatsvinden. Wel wordt een verslag opgesteld dat gekuist is voor openbaarmaking. Dit verslag wordt gedeeld met de belanghebbenden. Op die manier kunnen zij de overwegingen en besluiten van het bestuur blijven volgen.

Het bestuur is eindverantwoordelijk voor het functioneren van het stelsel en neemt daarbij, op basis van voorbereidingen van de staf van de stichting, besluiten over de te hanteren strategie (visie en meerjarenkoers), deelname en uittreding van deelnemers, het optreden van de stichting en de

uitvoeringsorganisaties en het accorderen van releases en ketenwijzigingen. Het streven is om dit te doen door middel van consensus. In het geval consensus niet tot stand komt en er behoefte is aan een stemming, dan moet dit ook mogelijk zijn. Besluitvorming vindt in dat geval plaats op basis van meerderheid van stemmen. Voor de onderwerpen waarbij dat statutair is vastgelegd, betreft het bestuur de eigenaarsraad in de besluitvorming.

## Eigenaarsraad

Een eigenaarsraad wordt ingericht om het eigenaarschap van personen en zorgaanbieders in de stichting een plek te geven. De eigenaarsraad is te vergelijken met de ledenraad van een vereniging, maar kent alleen die verantwoordelijkheden die nodig zijn om de rol van eigenaar goed te vervullen en is qua omvang beperkt. Statutair dient de eigenaarsraad goedkeuring te geven op de besluiten van het bestuur omtrent:

- Majeure aanpassingen van het MedMij Afsprakenstelsel;
- De strategische releaseplanning van het MedMij Afsprakenstelsel;
- De vaststelling van het aantal tot de stichting toe te laten eigenaars;
- De toelating van eigenaars;
- De opzegging van het eigenaarschap;
- De vaststelling van het aantal bestuurders;
- De vaststelling van de actuele profielschets voor het bestuur;
- De (her)benoeming van een bestuurder;
- De wijziging van de statuten van de stichting;
- De ontbinding van de stichting.

Personen en zorgaanbieders zijn grote, gedifferentieerde groepen en het is onpraktisch om zelf uit deze groepen leden voor eigenaarsraad te werven. De koepels van personen en zorgaanbieders dienen daarom als vertegenwoordiging van deze groepen. Het begrip koepel wordt ruim opgevat. MedMij gaat over een breed spectrum van de zorg, sociaal domein, preventie en gezondheid en is er zowel voor uitwisseling met zieke als gezonde personen. Een vertegenwoordiging van gezonde personen (bijvoorbeeld via de Consumentenbond en de Ouderenbond), moet ook zitting kunnen nemen in de eigenaarsraad.

De koepels nemen als rechtspersoon deel aan de eigenaarsraad. Voorafgaand aan deelname maken Stichting MedMij en de desbetreffende koepel afspraken over wie de koepel vertegenwoordigd. Vertegenwoordigers beschikken bij voorkeur over deskundigheid op het gebied van de digitale uitwisseling van gezondheidsgegevens (met patiënten) en visie op de ontwikkeling van de zorg en eHealth in de toekomst.

De eigenaarsraad bestaat uit minimaal zes en maximaal twaalf leden. Personen en zorgaanbieders zijn samen eigenaar van het stelsel. Daarom moet altijd sprake zijn van een gelijkwaardige verdeling van zetels.

Het streven is om de besluitvorming in de eigenaarsraad te laten plaatsvinden door middel van consensus. In het geval consensus niet tot stand komt en er behoefte is aan een stemming, dan is dit ook mogelijk. Ieder lid heeft één stem en besluiten worden aangenomen bij volstrekte meerderheid van uitgebrachte stemmen. Bij staking van de stemming is het voorstel verworpen.

De eigenaarsraad vergadert minimaal één keer per jaar en wordt in de regel voorgezeten door de voorzitter van het bestuur. De vergaderingen zijn niet openbaar om een vrije discussie te kunnen laten plaatsvinden. Wel wordt een verslag opgesteld dat gekuist is voor openbaarmaking. Dit verslag wordt gedeeld met de belanghebbenden. Op die manier kunnen zij de overwegingen en besluiten blijven volgen.

## Deelnemersraad

Deelnemers zijn geen eigenaar van het stelsel. Hun input is wel belangrijk om te komen tot gedragen en toekomstbestendige strategische keuzes. Zonder deze input loopt MedMij het risico dat belangrijke perspectieven, zoals economische motieven (bedrijfseconomische haalbaarheid voor aanbieders bij nieuwe functionaliteit) en het uitvoeringsbelang (technische haalbaarheid, implementeerbaarheid binnen een

bepaalde termijn, kwetsbaarheid), onvoldoende worden meegenomen in de keuzes. Binnen Stichting MedMij wordt daarom statutair een deelnemersraad ingericht. Deze deelnemersraad geeft gevraagd advies aan het bestuur op het gebied van de strategische doorontwikkeling van het MedMij Afsprakenstelsel en fungeert bovenal als klankbordgroep van het bestuur. De adviezen van de deelnemersraad zijn niet bindend. Indien het bestuur afwijkt van adviezen van de deelnemersraad, dan heeft zij een motiveringsplicht richting de raad. Een van de bestuursleden van Stichting MedMij is voorzitter van de deelnemersraad en de staf van de stichting voert het secretariaat. Er worden verslagen bijgehouden van de bijeenkomsten.

Elke deelnemer neemt als rechtspersoon deel aan de deelnemersraad. Voorafgaand aan deelname maken Stichting MedMij en de desbetreffende deelnemer afspraken over wie de deelnemer vertegenwoordigd. Vertegenwoordigers beschikken bij voorkeur over deskundigheid op het gebied van de digitale uitwisseling van gezondheidsgegevens (met patiënten) en visie op de ontwikkeling van de zorg en eHealth in de toekomst.

Naast een rol op strategisch niveau, worden deelnemers ook op tactisch/operationeel niveau door de uitvoeringsorganisatie betrokken bij de verdere ontwikkeling van het afsprakenstelsel.

### Dagelijkse operatie

Binnen de kaders van het bestuur geeft de staf van Stichting MedMij op dagelijkse basis invulling aan het strategische beheer. De staf zorgt voor nadere invulling van de grote lijnen, behartigt het belang van het stelsel en waarborgt het vertrouwen van betrokken bij het stelsel. Voor een beschrijving van de beheerverantwoordelijkheden van Stichting MedMij, zie [Beheerverantwoordelijkheden](#).

### Uitvoeringsorganisatie

De uitvoeringsorganisatie geeft in opdracht van Stichting MedMij invulling aan de tactisch /operationele beheertaken. Een belangrijke taak van de uitvoeringsorganisatie is om de dagelijkse gang van zaken in het stelsel te verbinden met de strategische koers van het stelsel. Het gaat dan zowel om het vertalen van strategische besluiten naar de tactisch/operationele toepassing binnen het afsprakenstelsel, als om het ophalen van wensen bij leveranciers en deze vertalen naar adviezen voor besluitvorming. Op dagelijkse basis regelt de uitvoeringsorganisatie het beheer van de afsprakenstelsel, de regie op toe- en uittreding van deelnemers, de regie op het afhandelen van incidenten en calamiteiten en de regie op ketenwijzigingen. De volledige opdracht is uitgewerkt in een programma van eisen. De verantwoordelijkheid voor de doorontwikkeling van de afspraken ligt begin 2018 nog bij het project Afsprakenstelsel, maar moet vanaf halverwege dat jaar ook een plek vinden bij de uitvoeringsorganisatie.

Voor een beschrijving van de beheerverantwoordelijkheden van de uitvoeringsorganisatie, zie [Beheerverantwoordelijkheden](#).

### Relatie met financiers

Om het scenario te voorkomen dat pas aan het eind van een financieringsperiode duidelijk wordt dat verwachtingen van financiers en het bestuur te ver uit elkaar lagen, is het belangrijk om gedurende het jaar (enige) betrokkenheid te organiseren. Deze betrokkenheid is onderdeel van het financieringsarrangement met de desbetreffende financier. Het bestuur heeft de vrijheid om via het financieringsarrangement met de desbetreffende financier afspraken te maken over de voorwaarden aan de financiering. Hierbij dient zij wel te waarborgen dat zij voldoende vrijheid krijgt om haar taak vanuit het belang van personen en zorgaanbieders uit te oefenen.

Mogelijke partijen voor de financiering van het beheer van het stelsel zijn de overheid en Zorgverzekeraars Nederland. VWS heeft aangegeven geen rol te kunnen spelen in de financiering en/of governance van de beoogde stichting en zich afzijdig te houden als het gaat om besluitvorming over de inrichting van de stichting.

## Relatie met het Programma MedMij

Het Programma MedMij heeft in 2018 nog een belangrijke rol bij:

- De doorontwikkeling van het afsprakenstelsel en het verwerken van de resultaten van Proves. De stuurgroep is daarmee nog verantwoordelijk voor de sturing op deze doorontwikkeling totdat de nieuwe versie van het afsprakenstelsel op advies van de stuurgroep wordt vastgesteld door de stichting en in beheer wordt gegeven bij de uitvoeringsorganisatie;
- Het inrichten van de governance en de bijkomende taken, zoals het opstellen van statuten, het werven van bestuursleden, het werven van ondersteunende staf, het regelen van duurzame financiering voor het beheer, etc.;
- Het uitvoeren van de staftaken van de stichting.

## Beheerverantwoordelijkheden

De volgende beheerverantwoordelijkheden worden ingevuld door Stichting MedMij en de uitvoeringsorganisatie:

### Stichting MedMij

- **Eindverantwoordelijkheid functioneren stelsel:** Het gehele beheertakenpakket dat hoort bij het in stand houden van een afsprakenstelsel vereist een vorm van aan- en besturing. Het bestuur van Stichting MedMij heeft deze eindverantwoordelijkheid. Zij dient onder andere over toekomstige afspraken en (criteria voor) toe- of uittreding te besluiten en ervoor te zorgen dat de activiteiten van alle bestuurslagen gericht blijven op het maatschappelijke doel van MedMij.
- **Besluitvorming bestuur:** Bestuursvergaderingen moeten worden voorbereid en bestuurders worden geadviseerd om de besluitvorming soepel te laten verlopen. De besluitvorming zelf moet ook georganiseerd worden.
- **Wijzigingsautoriteit:** Een belangrijk onderwerp voor besluitvorming van het bestuur zijn de nieuwe releases. Deze releases met wijzigingen aan het stelsel moeten worden goedgekeurd.
- **Visie/meerjarenplan:** Het stelsel zal mee moeten en willen ontwikkelen met de behoeften vanuit de twee grote belanghebbende partijen, de patiënten en de zorgaanbieders, en met de steeds verder toenemende mogelijkheden die de ICT ons biedt om gezondheidsgegevens te genereren en uit te wisselen. Ook moeten ontwikkelingen in de zorg, de maatschappij en wet- en regelgeving (bijv. vanuit de EU), in de gaten worden gehouden. Het hebben van een stappenplan waar het afsprakenstelsel zich naartoe ontwikkelt, is van groot belang voor alle betrokkenen, opdat voldoende vroegtijdig daarop geanticipeerd kan worden. Het afsprakenstelsel zal zich blijven ontwikkelen, en daarmee is deze beheertaak essentieel om blijvend richting te kunnen geven aan die verdere ontwikkeling.
- **Omgevingsmanagement:** De koers van het afsprakenstelsel staat niet los van andere ontwikkelingen in het zorgveld. Het succes van het Afsprakenstelsel is afhankelijk van een aantal maatschappijbrede ontwikkelingen, zoals de ontwikkeling van betrouwbare elektronische identificatiemiddelen. Afstemming daarmee is van essentieel belang. Ook zal het afsprakenstelsel een zeker beslag gaan leggen op de capaciteit van bestaande toezichthouders zoals Autoriteit Persoonsgegevens, Inspectie Gezondheidszorg en Jeugd en de Nederlandse Zorgautoriteit. Wat precies de impact van de komst van MedMij is voor deze toezichthouders en hoe die zich ontwikkelt, is nog onbekend. Juist daarom is afstemming met hen van groot belang.
- **Financiering:** Het in stand houden van het beheer van het afsprakenstelsel kost geld. Er zal derhalve een financiële functie moeten zijn ingericht die ervoor zorg draagt dat de te maken kosten gedekt worden.
- **Risicomanagement en uitvoeren privacy- en informatiebeveiligingsbeleid:** Voor het vertrouwen in het stelsel is het noodzakelijk informatiebeveiligingsrisico's te beheersen. Doorlopend risicomanagement is dan ook onontbeerlijk. Duidelijk moet zijn welke risico's het stelsel loopt, wie deze bewaakt en wie verantwoordelijk is voor het nemen van maatregelen.
- **Aansturen uitvoeringsorganisatie:** Het programma geeft, binnen de kaders van het bestuur van Stichting MedMij, sturing aan de uitvoeringsorganisatie. Ook maakt het programma afspraken over de gehanteerde service levels.

## Uitvoeringsorganisatie

- **Beheer van de afsprakenstelsel:** De kern van het afsprakenstelsel zijn de afspraken waar deelnemers zich aan moeten houden. Deze afspraken moeten worden bijgehouden en beheerd. In de afspraken wordt verwezen naar standaarden. De verantwoordelijkheid voor het beheer van deze standaarden is belegd bij andere partijen (veelal standaardisatieorganisaties). Het beheer van de afspraken is dus niet hetzelfde als het beheer van de standaarden. De grote afhankelijkheid van de beheerders van de



standaarden maakt afstemming noodzakelijk. De uitvoeringsorganisatie is hiervoor verantwoordelijk. Naast deze afstemming, moeten de uitvoeringsorganisatie er ook voor zorgen dat de documentatie wordt onderhouden en dat er tekst en uitleg kan worden gegeven bij de afspraken.

- **Regie op doorontwikkeling afspraken:** Het afsprakenstelsel moet meeveranderen met ontwikkelingen in de omgeving, veranderende dienstverlening bij betrokken deelnemers en de wensen van eindgebruikers. Bij deze doorontwikkeling komt veel kijken. Zo moeten afspraken een plek krijgen binnen de bredere architectuur en moeten keuzes worden gemaakt over de ondersteuning van informatie- en andere technische standaarden. Concrete afspraken moeten worden gemaakt met de organisaties die de standaarden beheren. Ook is het van groot belang om in nauw overleg met de deelnemers te onderzoeken wat de impact van keuzes is op de bestaande voorzieningen die al door de deelnemers worden aangeboden. En in vervolg daarop te onderzoeken wat een goede ontwikkelstrategie is om die nieuwe versie ook geïmplementeerd te krijgen in de voorzieningen van de deelnemers. Er moet voldoende voeding uit het veld en de deelnemers worden verzameld om goede beslissingen te kunnen nemen bij de ontwikkeling van afspraken. Deze nieuwe afspraken moeten worden verwerkt in een nieuwe versie van het afsprakenstelsel.
- **Regie op ketenwijzigingen:** Deelnemers zijn voor de uitwisseling via MedMij van elkaar afhankelijk. Bij wijzigingen aan de afspraken is daarom regie nodig op de implementatie.
- **Regie op toe- en uittreding:** De uitvoeringsorganisatie ziet erop toe dat deelnemers die willen participeren in het stelsel ook daadwerkelijk hun zaken op orde hebben. Ook bij een eventuele uittreding ziet de uitvoeringsorganisatie toe op een goede afhandeling van zaken. De eindverantwoordelijkheid voor toe- en uittreding ligt bij Stichting MedMij. De uitvoeringsorganisatie bereidt toe- en uittredingen voor en Stichting MedMij zorgt voor de besluitvorming.
- **Deelnemersmanagement:** Deelnemende partijen moeten goed geïnformeerd zijn en er moet op worden toegezien dat mededinging niet in gevaar komt. Hiervoor moeten relaties worden onderhouden.
- **Implementatieondersteuning:** De uitvoeringsorganisatie ondersteunt deelnemers waar nodig en gepast bij het wegnemen van barrières.
- **Aanspreekpunt, voorlichting en communicatie:** De uitvoeringsorganisatie vormt het eerste aanspreekpunt voor (potentiële) deelnemers inzake (door)ontwikkeling, implementatie en naleving van het afsprakenstelsel, dan wel bij de stagnatie of onduidelijkheid in onderlinge samenwerking tussen de deelnemers. Voor de deelnemers moet duidelijk zijn voor welke vraag, informatie of ondersteuning zij waar moeten zijn. Er moet voor deelnemers één ingang zijn waar vandaan de deelnemer naar het antwoord wordt begeleid. Tevens wordt proactief informatie aan (potentiële) deelnemers verstrekt, onder andere via bijeenkomsten, waardoor betrokkenheid ontstaat bij het afsprakenstelsel.
- **Regie op het afhandelen van incidenten en calamiteiten:** In geval van incidenten en calamiteiten zal er vanuit het stelsel geacteerd moeten worden om de impact van de ernstige verstoring te mitigeren en daarmee het vertrouwen in het stelsel niet te beschadigen.
- **Handhaven deelnemersovereenkomst:** De uitvoeringsorganisatie ziet erop toe dat deelnemers zich houden aan de afspraken uit de deelnemersovereenkomst.
- **Bevorderen samenwerking deelnemers:** De uitvoeringsorganisatie faciliteert samenwerking tussen deelnemers en draagt bij aan een fair playfield. Deelnemers worden betrokken in de afstemming op verschillende onderwerpen en er wordt voorkomen dat bepaalde partijen hierin een te dominante positie verwerven.
- **Regie centrale voorzieningen:** Centrale voorzieningen die de uitwisseling in het netwerk faciliteren, moeten voor zover ze niet door de markt zelf geleverd kunnen worden, centraal worden geregeld /ingekocht. Denk hierbij bijvoorbeeld aan de inrichting van MedMij Registratie.
- **Afhandelen klachten en geschillen:** De uitvoeringsorganisatie is eerste ingang voor het registreren en behandelen van klachten. Zij hanteert hierbij een bemiddelende aanpak. Op het moment dat de klacht niet door de uitvoeringsorganisatie kan worden afgehandeld, dan volgt een doorgeleiding naar Stichting MedMij.
- **Afhandelen algemene vragen en klachten van eindgebruikers:** Deelnemers bedienen met het afsprakenstelsel uiteindelijk de gebruikers. Eindgebruikers moeten een neutrale plek kennen waarbij ze terecht kunnen voor meer informatie over MedMij, met vragen over het gebruik daarvan en/of met eventuele klachten.

## Statuten Stichting MedMij

De [statuten](#) van Stichting MedMij zijn een vertaling van de [Rollen](#) en [Inrichting](#) en formaliseren de positie van actoren binnen de governance.



## Modelverwerkersovereenkomst

### Modelverwerkersovereenkomst Zorgaanbieder - Dienstverlener zorgaanbieder

#### Doel

De zorgaanbieder is als verwerkingsverantwoordelijke verantwoordelijk om verwerkingsovereenkomsten af te sluiten in het geval persoonsgegevens in opdracht van hem door een derde (lees: verwerker) worden verwerkt. Binnen het MedMij Afsprakenstelsel opereert de Dienstverlener zorgaanbieder onder verantwoordelijkheid van de Zorgaanbieder. Daarmee dient er altijd een verwerkingsovereenkomst tussen Zorgaanbieder en Dienstverlener zorgaanbieder getekend te worden.

Deze verwerkersovereenkomst is een modelovereenkomst die door de Zorgaanbieder kan worden gebruikt voor MedMij specifieke onderdelen, zoals het verwerken van BSN ten behoeve van authenticatie, het verkrijgen van toestemming van de Persoon voor gegevensuitwisseling met zijn Dienstverlener persoon en het verwerken van persoonsgegevens ten behoeve van de gegevensuitwisseling zelf zoals logging en de verwerking van de betreffende persoonsgegevens door de Dienstverlener zorgaanbieder overeenkomstig het bepaalde in het MedMij Afsprakenstelsel.

#### De ondergetekenden:

1. << naam Zorgaanbieder >> , gevestigd te << plaatsnaam + adres >>, te dezen rechtsgeldig vertegenwoordigd door << naam + functie >>

hierna te noemen: 'Opdrachtgever',

en

2. << naam Dienstverlener zorgaanbieder >>, (statutair) gevestigd te << plaatsnaam + adres >>, te dezen rechtsgeldig vertegenwoordigd door << functie + naam >>.

hierna te noemen: 'Opdrachtnemer',

hierna gezamenlijk te noemen: 'Partijen';

#### Overwegende dat:

I. Partijen in overeenstemming met de Algemene Verordening gegevensbescherming (AVG) in deze Verwerkersovereenkomst hun afspraken opnemen over het verwerken van persoonsgegevens ten behoeve van de gegevensuitwisseling tussen persoonlijke gezondheidsomgevingen MedMij en de informatiesystemen van de Opdrachtgever.

II. In het kader van de uitvoering van deze Verwerkersovereenkomst de Persoonsgegevens in de zin van artikel 4 sub 1 AVG worden verwerkt binnen de scope van de afspraken zoals opgesteld in het MedMij Afsprakenstelsel.

III. De Opdrachtgever verantwoordelijk is voor het verlenen van toegang tot de persoonsgegevens aan de Persoon en het vaststellen van de identiteit van de Persoon aan de hand van een BSN. De Opdrachtnemer voert dit proces uit, conform de afspraken in het MedMij Afsprakenstelsel, in opdracht van de Opdrachtgever. De wettelijke basis voor de verwerking van het BSN door Opdrachtgever ten behoeve van authenticatie van de Persoon, met als doel de gegevensuitwisseling tussen Persoon en Opdrachtgever, overeenkomstig het bepaalde in het MedMij Afsprakenstelsel, volgt uit artikel 4 en artikel 5 van de Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg.

IV. De Opdrachtgever alleen gegevens en/of gezondheidsinformatie met de Persoon via MedMij uitwisselt met wie hij een (actuele) behandelrelatie in de zin van de Wet op geneeskundige behandelingsovereenkomst heeft.

V. Opdrachtnemer een zogenaamde 'Dienstverlener Zorgaanbieder' binnen het MedMij Afsprakenstelsel is en daarvoor de [Deelnemersovereenkomst Dienstverlener zorgaanbieder](#) met de Stichting MedMij heeft afgesloten.

VI. Krachtens artikel 4 sub 7 AVG de Opdrachtgever "Verwerkingsverantwoordelijke" is voor de Persoonsgegevens en krachtens artikel 4 sub 8 AVG de Opdrachtnemer "Verwerker" is in het kader van de uitvoering van deze Verwerkersovereenkomst.

VII. Deze overeenkomst is aan te merken als een 'Verwerkersovereenkomst' in de zin van artikel 28 lid 3 AVG.

## **Verklaren te zijn overeengekomen als volgt**

### **Artikel 1. Begrippen**

De hierna en hiervoor in deze Verwerkersovereenkomst vermelde, met een hoofdletter

geschreven begrippen, hebben de volgende betekenis:

1.1 Deelnemersovereenkomst: *'Deelnemersovereenkomst Dienstverlener zorgaanbieder'* die is gesloten tussen Stichting *MedMij* en Opdrachtnemer en op basis waarvan Opdrachtnemer is toegetreten tot het MedMij Afsprakenstelsel.

1.2 Bijlage: aanhangsels bij deze Verwerkersovereenkomst of onder deze Verwerkersovereenkomst aangegane nadere overeenkomst die onlosmakelijk zijn verbonden met deze Verwerkersovereenkomst.

1.3 BSN; het nummer, bedoeld in artikel 1, onder b, van de Wet algemene bepalingen Burgerservicenummer.

1.4 Functionaris voor de gegevensbescherming: de door Opdrachtgever benoemde functionaris als bedoeld in artikel 37 AVG.

1.5 Gegevensdienst: een gestandaardiseerde dienst voor gegevensuitwisseling met waarde voor de gebruiker die door een Dienstverlener persoon of Dienstverlener zorgaanbieder wordt aangeboden over het MedMij-netwerk. De Het MedMij Afsprakenstelsel definieert welke Gegevensdiensten over het MedMij-netwerk aangeboden mogen worden en biedt een faciliteit om het aanbod van de Dienstverlener persoon en Dienstverlener zorgaanbieder inzichtelijk te maken. Opdrachtnemer levert Gegevensdiensten in opdracht van en volgens schriftelijke instructie van de Opdrachtgever via het MedMij-netwerk en heeft voor de verwerking van persoonsgegevens in relatie tot deze Gegevensdiensten de Verwerkersovereenkomst met Opdrachtgever afgesloten.

1.6 MedMij Afsprakenstelsel: de door de Stichting MedMij vastgestelde laatst geldende release van het MedMij Afsprakenstelsel.

1.7 Persoon: degene op wie een Persoonsgegevens betrekking heeft, 16 jaar of ouder is, en zich bij Opdrachtnemer authentificeert met een authenticatiemiddel.

1.8 Persoonsgegevens: persoonsgegevens in de zin van artikel 4 sub 1 en sub 15 Algemene Verordening Gegevensbescherming.

1.9 Verwerking: verwerking in de zin van artikel 4 sub 2 Algemene Verordening Gegevensbescherming.

1.10 Verwerkersovereenkomst: deze overeenkomst inclusief Overwegingen en bijbehorende Bijlage(n).

## **Artikel 2. Totstandkoming, duur van de Verwerkersovereenkomst**

2.1 Deze Verwerkersovereenkomst geldt vanaf de datum van ondertekening en wordt aangegaan voor de duur van de Deelnemersovereenkomst.

2.2 De Verwerkersovereenkomst eindigt van rechtswege wanneer de Deelnemersovereenkomst eindigt.

## **Artikel 3. Voorwerp van de Verwerkersovereenkomst**

3.1 Opdrachtnemer verwerkt het BSN ten behoeven van authenticatie en verwerkt Persoonsgegevens voor:

- het verkrijgen van toestemming van de Persoon voor het verstrekken van Persoonsgegevens aan een derde partij namelijk de Dienstverlener persoon;
- de inhoud van de gegevensuitwisseling;
- handelingen ten behoeve van de gegevensuitwisseling;

overeenkomstig het bepaalde in het MedMij Afsprakenstelsel voor Opdrachtgever op basis van de Gegevensdiensten van het MedMij Afsprakenstelsel zoals opgenomen in Bijlage I. De verwerking van Persoonsgegevens vindt uitsluitend plaats in opdracht en volgens schriftelijke instructie van de Opdrachtgever en zoals in Bijlage I aangegeven, behoudens afwijkende wettelijke verplichtingen.

3.2 Indien op verzoek van de Persoon, de Persoon Persoonsgegevens met Opdrachtgever wil delen, vergewist Opdrachtnemer zich ervan, overeenkomstig het bepaalde in het MedMij Afsprakenstelsel, dat Opdrachtgever een (actuele) behandelrelatie in de zin van artikel 7:446 van het Burgerlijk Wetboek met de Persoon heeft.

3.3 Opdrachtnemer zal de Persoonsgegevens aantoonbaar op behoorlijke en zorgvuldige wijze en in overeenstemming met de op hem als Verwerker op grond van de privacy- en andere toepasselijke wet- en regelgeving betreffende de verwerking van Persoonsgegevens verwerken.

3.4 Opdrachtnemer verwerkt de Persoonsgegevens niet voor eigen doeleinden. Voor zover niet anders is bepaald in deze Verwerkersovereenkomst, neemt Opdrachtnemer geen beslissingen over het gebruik van de gegevens, de verstrekking aan derden en de duur van de opslag van gegevens. De zeggenschap over het doel en de middelen voor de Verwerking van de Persoonsgegevens berust nimmer bij Opdrachtnemer.

3.5 Opdrachtnemer schakelt geen derden in zonder voorafgaande specifieke of algemene schriftelijke toestemming van Opdrachtgever. Opdrachtgever kan aan de toestemming om derden in te schakelen voorwaarden verbinden.

3.6 Indien Opdrachtnemer op grond van een wettelijke verplichting gegevens dient te verstrekken, verifieert Opdrachtnemer de grondslag van het verzoek en de identiteit van de verzoeker en informeert hij onmiddellijk, zo mogelijk voorafgaand aan de verstrekking, Opdrachtgever ter zake.

3.7 Opdrachtnemer verleent Opdrachtgever volledige medewerking om binnen de wettelijke termijnen te voldoen aan de verplichtingen op grond van de privacy- en andere toepasselijke wet- en regelgeving betreffende de verwerking van Persoonsgegevens, meer in het bijzonder met betrekking tot de rechten van betrokkenen, zoals, maar niet beperkt tot, een verzoek om inzage, verbetering, aanvulling, verwijdering, afscherming of de overdraagbaarheid van Persoonsgegevens en het uitvoeren van een gehonoreerd aangetekend verzet. Tevens verleent Opdrachtnemer volledige medewerking aan het adequaat informeren van de betrokkenen in het kader van de meldplicht datalekken. De eventuele kosten die voortvloeien uit het niet of niet tijdig voldoen aan de meldplicht met betrekking tot datalekken komen voor rekening van Opdrachtnemer.

3.8 Indien Opdrachtnemer (pogingen tot) onrechtmatige of anderszins ongeautoriseerde verwerkingen of inbreuken op de beveiligingsmaatregelen van de Persoonsgegevens signaleert, zal hij Opdrachtgever hierover onmiddellijk inlichten en op eigen kosten alle redelijkerwijs benodigde maatregelen treffen om een (dreigende) schending van de privacy- en andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens te voorkomen of te beperken; één en ander onverminderd de verplichting van Opdrachtnemer om de eventueel door Opdrachtgever daardoor geleden schade te vergoeden.

3.9 Opdrachtgever en Opdrachtnemer betrekken de Functionaris voor de gegevensbescherming tijdig en naar behoren bij alle aangelegenheden die verband houden met de bescherming van persoonsgegevens.

3.10 Overeenkomstig het bepaalde in Hoofdstuk V van de Algemene Verordening Gegevensbescherming verwerkt Opdrachtnemer geen Persoonsgegevens buiten een land van de Europese Unie/Europese Economische ruimte zonder een passend beschermingsniveau.

#### **Artikel 4. Beveiliging**

4.1 Opdrachtnemer zal overeenkomstig de voor Opdrachtgever geldende wet- en regelgeving voor beveiliging de benodigde maatregelen implementeren die het vertrouwen en de continuïteit van de Verwerking borgen. De maatregelen, die zijn opgenomen in het Normenkader informatiebeveiliging van het MedMij Afsprakenstelsel, dienen met inachtneming van de stand der techniek een passend beschermingsniveau te verzekeren voor de Verwerking in relatie tot het MedMij Afsprakenstelsel, zulks met inachtneming van de risico's die de Verwerking met zich meebrengen.

4.2 Opdrachtnemer rapporteert aan Opdrachtgever over de door hem genomen maatregelen aangaande de getroffen technische en organisatorische beveiligingsmaatregelen en eventuele aandachtspunten daarin. De rapportage dient betrekking te hebben op de in het eerste lid bedoelde beveiligingsmaatregelen. Daarnaast toont Opdrachtnemer aan dat hij voldoet aan de voor hem geldende normen op het gebied van informatiebeveiliging. Opdrachtnemer kan aan de hand van geldige certificering of een gelijkwaardig bewijsmiddel aantonen dat hij hieraan voldoet.

#### **Artikel 5. Geheimhouding**

5.1 Opdrachtnemer is gehouden tot geheimhouding van alle Persoonsgegevens en informatie die zij als uitvloeisel van deze Verwerkersovereenkomst verwerkt, behoudens in zoverre die gegevens of informatie klaarblijkelijk geen geheim of vertrouwelijk karakter hebben, dan wel reeds algemeen bekend zijn.

5.2 Indien en voor zover Opdrachtgever daarom uitdrukkelijk schriftelijk verzoekt, zal Opdrachtnemer ten aanzien van de daarbij aangeduide gegevens of informatie bijzondere maatregelen treffen met het oog op de geheimhouding daarvan, welke maatregelen onder meer kunnen inhouden de vernietiging van betrokken gegevens of informatie zodra de noodzaak voor Opdrachtnemer om daarvan nog langer kennis te nemen, is komen te vervallen.

5.3 Opdrachtnemer zal in haar overeenkomsten met het personeel van Opdrachtnemer bedingen dat door die personen op overeenkomstige wijze als in artikel 5.1 en 5.2 bepaald geheimhouding zal worden betracht ten aanzien van alle gegevens en informatie die zij in het kader van hun werkzaamheden voor Opdrachtnemer verwerken. Opdrachtnemer staat er jegens Opdrachtgever voor in dat de bedoelde bedingen door de betrokken personen zullen worden nageleefd.

## **Artikel 6. Gebruik onderaannemers (subverwerkers)**

6.1 Opdrachtnemer zal aan de door hem ingeschakelde derde dezelfde of strengere verplichtingen opleggen als voor hemzelf gelden op basis van deze Verwerkersovereenkomst en uit de wet- en regelgeving voortvloeien en ziet toe op de naleving daarvan door de derde. De betreffende afspraken met de derde worden schriftelijk vastgelegd. Opdrachtnemer zal Opdrachtgever op eerste verzoek een afschrift verstrekken van deze overeenkomsten(en).

6.2 Niettegenstaande de toestemming van de Opdrachtgever voor het inschakelen van een derde partij blijft Opdrachtnemer volledig aansprakelijk jegens Opdrachtgever voor de gevolgen van het uitbesteden van werkzaamheden aan een derde. De toestemming van Opdrachtgever voor het uitbesteden van werkzaamheden aan een derde partij laat onverlet dat voor de inzet van subverwerkers artikel 3.10 van overeenkomstige toepassing is.

## **Artikel 7. Controle**

7.1 Opdrachtgever kan de Verwerking en de naleving van de overeengekomen technische en organisatorische beveiligingsmaatregelen van Opdrachtnemer, dan wel die van door Opdrachtnemer ingeschakelde derden, op elk door hem gewenst moment controleren of doen controleren. In verband daarmee verstrekt Opdrachtnemer op eerste verzoek van Opdrachtgever een (zelf)verklaring waarin een oordeel wordt gegeven over de genoemde naleving.

7.2 Opdrachtnemer zal alle redelijkerwijs benodigde medewerking verlenen aan de controle en er voor zorg dragen ook de door hem ingeschakelde derden hiertoe de redelijkerwijs benodigde medewerking zullen verlenen.

7.3 Het uitvoeren van een controle zal niet tot een vertraging van de door Opdrachtnemer in het kader van deze Verwerkersovereenkomst te verrichten werkzaamheden mogen leiden. Indien niettemin vertraging optreedt, zullen Partijen in overleg treden teneinde daarvoor zo snel mogelijk een oplossing te vinden.

7.4 De met de controle gemoeide kosten zijn voor rekening van Opdrachtgever, tenzij uit de controle blijkt dat Opdrachtnemer is tekortgeschoten in de nakoming van zijn verplichting(en) uit deze Verwerkersovereenkomst.

7.5 Opdrachtnemer voert de door Opdrachtgever aangegeven aanbevelingen ter verbetering uit binnen de daartoe door Opdrachtgever te bepalen termijn.

## **Artikel 8. Opschorting en beëindiging**

8.1 Partijen kunnen deze Verwerkersovereenkomst tussentijds opzeggen met inachtneming van een opzegtermijn van één kalendermaand.

8.2 Deze Verwerkersovereenkomst kan door Opdrachtgever met onmiddellijke ingang worden beëindigd indien Opdrachtgever heeft vastgesteld dat Opdrachtnemer niet of onvoldoende voldoet aan de in artikel 4 van deze Verwerkersovereenkomst voorgeschreven technische en organisatorische beveiligingseisen dan wel anderszins de in deze Verwerkersovereenkomst opgenomen voorschriften, verplichtingen of procedures niet nakomt of volgt.

8.3 Verplichtingen welke naar hun aard bestemd zijn ook na beëindiging van deze Verwerkersovereenkomst voort te duren, blijven na beëindiging van de Verwerkersovereenkomst gelden. Tot deze bepalingen behorend onder meer de bepalingen betreffende geheimhouding, aansprakelijkheid en toepasselijk recht.

8.4 Partijen zijn gerechtigd, onverminderd hetgeen daartoe bepaalde in de [Deelnemersovereenkomst Dienstverlener zorgaanbieder](#), de uitvoering van de Verwerkersovereenkomst en de daarmee samenhangende Deelnemersovereenkomst op te schorten, dan wel zonder rechterlijke tussenkomst met onmiddellijke ingang te ontbinden, indien:

- a) de ander partij wordt ontbonden of anderszins ophoudt te bestaan;
- b) de andere partij aantoonbaar tekortschiet in de nakoming van de verplichtingen die voortvloeien uit deze Verwerkersovereenkomst en die ernstige toerekenbare tekortkoming niet binnen 30 dagen is hersteld na een daartoe strekkende schriftelijke ingebrekestelling;
- c) een partij in staat van faillissement wordt verklaard of surseance van betaling.

8.5 Opdrachtgever is gerechtigd deze Verwerkersovereenkomst per direct te ontbinden indien de Opdrachtnemer te kennen geeft niet (langer) te kunnen voldoen aan de betrouwbaarheidseisen die op grond van ontwikkelingen in de wet en/of rechtspraak aan de verwerking van persoonsgegevens worden gesteld.

## **Artikel 9. Bewaartermijn, teruggave en vernietiging van Persoonsgegevens**

9.1 Opdrachtnemer bewaart de Persoonsgegevens niet langer dan strikt noodzakelijk voor het doel zoals opgenomen in Bijlage I en conform de bepalingen in het MedMij Afsprakenstelsel.

9.2 Bij beëindiging van de Verwerkersovereenkomst of indien van toepassing aan het einde van de overeengekomen bewaartermijnen, indien blijkt dat overeenkomstig de vergewisplicht van artikel 3.2 van de Verwerkersovereenkomst de Opdrachtgever geen (actuele) behandelrelatie in de zin van artikel 7:446 van het Burgerlijk Wetboek met de Persoon heeft, of op schriftelijke verzoek van Opdrachtgever zal Opdrachtnemer, kosteloos, naar keuze van Opdrachtgever, de Persoonsgegevens vernietigen of teruggeven aan Opdrachtgever. Op eerste verzoek van Opdrachtgever verstrekt Opdrachtnemer bewijs van het feit dat de Persoonsgegevens vernietigd of verwijderd zijn.

## **Artikel 10. Aansprakelijkheid**

10.1 Partijen zijn ieder verantwoordelijk en aansprakelijk voor hun eigen handelen. Gebruikers kunnen zich jegens Partijen onmiddellijk en direct op deze aansprakelijkheid beroepen.

10.2 Partijen zijn jegens elkaar aansprakelijk indien zij de verplichtingen uit de Verwerkersovereenkomst en/of de privacy- en andere toepasselijke wet- en regelgeving betreffende de Verwerking van Persoonsgegevens schenden door deze niet of niet naar behoren na te komen. Indien en voor zover deze schending toerekenbaar is, heeft deze schadeplichtigheid tot gevolg.

10.3 Opdrachtnemer vrijwaart Opdrachtgever en stelt Opdrachtgever schadeloos voor alle claims, acties, aanspraken van derden voor verliezen, schade of kosten, waaronder boetes van de Autoriteit Persoonsgegevens die Opdrachtgever maakt of lijdt en die rechtstreeks of indirect voortvloeien uit of tot stand komen in verband met een tekortkoming door de Opdrachtnemer en/of diens onderaannemers in de nakoming van zijn verplichtingen onder deze Verwerkersovereenkomst.

## Artikel 11. Slotbepalingen

11.1 Afwijkingen van deze Verwerkersovereenkomst zijn slechts bindend voor zover zij uitdrukkelijk tussen Partijen schriftelijk zijn overeengekomen.

11.2 Op deze Verwerkersovereenkomst is Nederlands recht van toepassing

11.3 Geschillen over en die voortvloeien uit deze overeenkomst worden voorgelegd aan de bevoegde rechter in Den Haag.

Aldus op de laatste van de twee hierna genoemde data overeengekomen en in tweevoud ondertekend,

<< naam Zorgaanbieder >>

namens deze,

Naam:

Functie:

Datum

Plaats

<< Naam Dienstverlener Zorgaanbieder >>

namens deze,

Naam:

Functie:

Datum:

Plaats:

## Bijlage 1. Overzicht Persoonsgegevens en Procedure

Het doel van de Verwerking voor MedMij specifieke onderdelen, overeenkomstig het bepaalde in het MedMij Afsprakenstelsel is op verzoek van de Persoon door de Opdrachtnemer het verwerken van het BSN ten behoeven van authenticatie, het verkrijgen van toestemming van de Persoon voor gegevensuitwisseling, het verwerken van persoonsgegevens ten behoeve van de gegevensuitwisseling, zoals logging, de verwerking van de betreffende persoonsgegevens zelf namens de Opdrachtgever van deze Persoon.

Hiervoor worden uitsluitend de volgende Persoonsgegevens door Opdrachtnemer verwerkt:

- BSN;
- Toestemmingsverklaring van de Persoon voor het verstrekken van gegevens aan een derde partij namelijk de Dienstverlener persoon;
- Informatie ten behoeve van het zich vergewissen van het bestaan van een (actuele) behandelrelatie tussen de Persoon en de Opdrachtgever;
- Bevestigingsverklaring van de Persoon voor het delen van gegevens met de Opdrachtgever;
- De Persoonsgegevens uit de gegevensdiensten die door de Opdrachtgever conform de afspraken uit het MedMij Afsprakenstelsel via het MedMij-netwerk worden verstrekt of verkregen;
- De persoonsgegevens ten behoeve van de gegevensuitwisseling (zoals logging).

De categorie betrokkenen van wie bovenstaande persoonsgegevens worden verwerkt zijn: Personen die willen beschikken over hun gezondheidsinformatie in de PGO en 16 jaar of ouder zijn.

Overeenkomstig artikel 3.1 van deze Verwerkersovereenkomst worden de Persoonsgegevens overeenkomstig de beschreven [Processen & Informatie](#) met de bijbehorende use cases door 'Dienstverlener zorgaanbieder' zoals opgenomen in het MedMij Afsprakenstelsel door Opdrachtnemer verwerkt.



## Issues

Loopt u als (potentiële) deelnemer aan tegen problemen bij de implementatie van de afspraken of heeft u suggesties voor doorontwikkeling? Laat dat dan vooral aan MedMij weten door het [issueformulier](#) in te vullen en te sturen naar [productmanagement@medmij.nl](mailto:productmanagement@medmij.nl). Zie verder het [Change- en releasebeleid](#) voor een nadere beschrijving van de afhandeling.

## pdf.images

Deze plaatjes worden gebruikt bij de PDF export.

