MedMij Afsprakenstelsel

Afsprakenset release 1.1

Auteur Project Afsprakenstelsel
Datum 28 september 2018
This deliverable contains original unpublished work or work to which the author holds all rights except where clearly indicated otherwise.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. Afsprakenset release 1.1 4
1.1 Releaseinfo 6
1.1.1 Release- en versiebeschrijving 7
1.1.2 Changelog 9
1.1.2.1 Changelog release 1.1 10
1.1.2.1.1 Changelog release 1.1 versie 1.0 11
1.1.2.1.2 Changelog release 1.1 versie 0.9 12
1.1.2.1.3 Changelog release 1.1 versie 0.8 15
1.1.2.2 Changelog release 1.0 18
1.1.2.2.1 Changelog release 1.0 versie 1.0 19
1.1.2.2.2 Changelog release 1.0 versie 0.991 20
1.1.2.2.3 Changelog release 1.0 versie 0.99 21
1.1.2.2.4 Changelog release 1.0 versie 0.9 22
1.1.2.2.5 Changelog release 1.0 versie 0.8 24
1.1.2.2.6 Changelog release 1.0 versie 0.3 26
1.2 Grondslagen 28
1.2.1 Achtergrond 29
1.2.2 Criteria 35
1.2.3 Principes 39
1.2.4 Opzet 45
1.2.5 Begrippenlijst 47
1.3 Juridische context 49
1.3.1 Juridisch kader 50
1.3.2 Overeenkomsten en rechtsrelaties 63
1.3.3 Toelichting verwerkingsverantwoordelijkheid 67
1.3.4 Toelichting AVG-normen 71
1.4 Architectuur en technische specificaties 105
1.4.1 Juridica 109
1.4.2 Processen en informatie 110
1.4.2.1 UC Verzamelen 118
1.4.2.2 UC Delen 124
1.4.2.3 UC Opvragen ZAL 131
1.4.2.4 UC Opvragen OCL 132
1.4.2.5 UC Opvragen GNL 133
1.4.3 Applicatie 134
1.4.3.1 UCI Verzamelen 149
1.4.3.2 UCI Delen 159
1.4.3.3 UCI Opvragen ZAL 169
1.4.3.4 UCI Opvragen OCL 170
1.4.3.5 UCI Opvragen GNL 171
1.4.3.6 Gegevens en performance in UCI Verzamelen en UCI Delen 172
1.4.3.7 Gegevens en performance inzake opvragen lijsten 177
1.4.3.8 XML-bestanden voor lijsten 178
1.4.4 Netwerk 179
1.4.4.1 UCI Opvragen WHL 187
1.4.5 Informatiemodellen 188
1.4.5.1 Metamodel 189
1.4.5.2 Logische modellen 203
1.4.5.3 XML-schema's 214
1.5 Normenkader informatiebeveiliging 221
1.5.1 A.5.1.1 Beleidsregels voor informatiebeveiliging 225
1.5.2 A.6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging 226
1.5.3 A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging . 227
1.5.4 A.8.2.1 Classificatie van informatie 228
1.5.5 A.9.1.1 Beleid voor toegangsbeveiliging 229
1.5.6 A.9.2.5 Beoordeling van toegangsrechten van gebruikers 230
1.5.7 A.9.4.1 Beperking toegang tot informatie 231
1.5.8 A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen . . 232
1.5.9 A.12.1.2 Wijzigingsbeheer 233
1.5.10 A.12.1.3 Capaciteitsbeheer 234
1.5.11 A.12.3.1 Back-up van informatie 235

1.5.12 A.12.4.1 Gebeurtenissen registreren . . . 236
1.5.13 A.12.4.4 Kloksynchronisatie . . . 237
1.5.14 A.12.5.1 Software installeren op operationele systemen . . . 238
1.5.15 A.12.6.1 Beheer van technische kwetsbaarheden . . . 239
1.5.16 A.14.2.1 Beleid voor beveiligd ontwikkelen . . . 240
1.5.17 A.16.1.1 Verantwoordelijkheden en procedures . . . 241
1.5.18 A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging . . . 242
1.5.19 A.16.1.7 Verzamelen van bewijsmateriaal . . . 243
1.5.20 A.18.2.3 Beoordeling van technische naleving . . . 244
1.6 Beleid . . . 245
1.6.1 Change- en releasebeleid . . . 246
1.6.2 Dienstverleningsoverdrachtsbeleid . . . 248
1.6.3 Gegevensdienstenbeleid . . . 249
1.6.4 Informatieclassificatiebeleid . . . 251
1.6.5 Intellectueel eigendomsbeleid . . . 254
1.6.6 Klachten- en geschillenbeleid . . . 256
1.6.7 Nalevingsbeleid . . . 257
1.6.8 OAuthclient-namenbeleid . . . 259
1.6.9 Performancebeleid . . . 260
1.6.10 Privacy- en informatiebeveiligingsbeleid . . . 261
1.6.10.1 Risicoanalyse . . . 262
1.6.11 Samenwerkings- en escalatiebeleid . . . 264
1.6.12 Testbeleid . . . 265
1.6.13 Zorgaanbiedersnamenbeleid . . . 267
1.7 Operationele processen . . . 268
1.8 Communicatie . . . 272
1.8.1 Merkgebruik . . . 273
1.8.2 Gebruikersvoorlichting . . . 275
1.8.3 Toestemmingsverklaring . . . 276
1.8.4 Bevestigingsverklaring . . . 278
1.9 Managementinformatie . . . 280
2. Toelichtingen afsprakenset release 1.1 . . . 281

Afsprakenset release 1.1

Voor u ligt release 1.1 van de afsprakenset van het MedMij Afsprakenstelsel. De afsprakenset 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 afsprakenset is preconcurrentieel. 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.

Release 1.1 is de eerste productierelease van het stelsel. 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 afsprakenset. 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 afsprakenset is als volgt opgebouwd:

- **Releaseinfo:** Het hoofdstuk biedt meta-informatie over deze release van de afsprakenset.
- **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 afsprakenset te bestuderen, eerst kennis te nemen van de stelselbrede Introductie en Afsprakenstelsel in de praktijk (release-onafhankelijk) en daarna van de context van voorliggende afsprakenset (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 afsprakenset. 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. Wijzigingen die naar verwachting worden doorgevoerd in de eerstvolgende release zijn benoemd onder de voorgenomen wijzigingen.

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	1.1
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	• Potentiële deelnemers (dienstverleners persoon en dienstverleners zorgaanbieder) • Deelnemers • Beheerorganisatie MedMij • Programma MedMij • Geïnteresseerden in de doorontwikkeling van het MedMij Afsprakenstelsel
Totstandkoming	Deze versie is tot stand gekomen onder leiding van het project Afsprakenstelsel binnen het programma MedMij in samenwerking met diverse partijen in de zorg, zoals ICT-leveranciers, het ministerie van VWS, Patiëntenfederatie Nederland en vertegenwoordigers van zorgaanbieders. Bij de nadere uitwerking van het N ormenkader Informatiebeveiliging en de Governance zijn ook NEN, certificeringsbureaus en de uitvoeringsorganisatie betrokken geweest. De nadere uitwerking van de Architectuur en technische specificaties is daarnaast maandelijks voorgelegd aan de Werkgroep Gegevensuitwisseling.
Inwerkingtreding	Nadat de afsprakenset is vastgesteld door het bestuur.
Operationeel toepassingsgebied	• Alle deelnemers aan de eerste productiefase van het MedMij Afsprakenstelsel. • De beheerorganisatie MedMij.
Status (augustus 2018)	Het gebruik van de producten heeft nog geen formele status en er is nog geen sprake van een formeel afsprakenstelsel. Formalisering moet nog plaatsvinden via vaststelling van het afsprakenstelsel door Stichting MedMij. Operationele situaties waarin gebruik wordt gemaakt van het afsprakenstelsel vallen buiten de verantwoordelijkheid van MedMij. Gebruik van de producten is op eigen risico.

Functionele scope	Het afsprakenstelsel ondersteunt in deze release: • Het opvragen van gezondheidsgegevens door een persoon bij een zorgaanbieder, voor bewaring in een persoonlijke gezondheidsomgeving; • Het delen van gezondheidsgegevens door een persoon met een zorgaanbieder, voor gebruik bij de behandeling.
Licentie	Creative Commons: Naamsvermelding-GeenAfgeleideWerken 4.0 Internationaal (CC BY-ND 4.0).

Changelog

De changelog beschrijft de wijzigingen die zijn doorgevoerd bij releases van het afsprakenstelsel.

Changelog release 1.1

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

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:

- Toelichtingen afsprakenset release 1.1: toelichtingenpagina op afsprakenset release 1.1 toegevoegd.
- 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

> **Afsprakenset 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 afspraken*set*. 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 (resulterend 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 bezien 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 afsprakenset 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: Modellering 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 afsprakenset 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 sleutelelementen.
- 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 PKIoverheid-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 bètaversiefase.
- 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 verwijdert 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

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 release 1.1 van het afsprakenstelsel worden nog niet alle functionaliteiten aangeboden. De Release- en versiebeschrijving geeft een overzicht van de inhoud van release 1.1 van het 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 werkbare 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 vertrouwelijkheid 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 verwikkeld 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 afsprakendomein tussen de dienstverleners onderling. Dit zijn veel dynamischer afspraken die vooral gaan over de werkwijzen; dergelijke afspraken zijn dan ook niet technologieneutraal. 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-stempel 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-stempel 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-stempel 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 preconcurrentieel 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
D1	**Creëren van vertrouwen bij personen en zorgaanbieders in gegevensuitwisseling**
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
D2	**Interoperabiliteit van gegevensuitwisseling**
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
D3	**Creëren van een tweezijdige markt met de juiste innovatie- en kwaliteitsprikkels en voldoende keuzemogelijkheden**
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
D4	**Gebruiksvriendelijkheid**

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
D5	**Snelheid van implementatie door dienstverleners**
D6	**Toekomstvastheid van de oplossing**
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
D7	**Compatibiliteit met zoveel mogelijk gewenste kenmerken van een persoonlijke gezondheidsomgeving**
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
D8	**Betaalbaarheid**

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 patient en wat eHealth daaraan kan bijdragen.

Randvoorwaarden

Nr.	Titel	Toelichting
R1	**Voldoen aan actuele wet- en regelgeving**	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.
R2	**Snelle oplevering van een eerste werkende versie van het afsprakenstelsel en het MedMij-netwerk**	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.
R3	**Verbinden van meerdere domeinen**	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. Het verzamelen van relevante gezondheidsgegevens betekent dan ook meer voor een persoonlijke gezondheidsomgeving dan alleen gegevens verzamelen vanuit de professionele curatieve zorg.

		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.
R4	**Transparante en open besluitvorming over (door)ontwikkeling**	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 kerndossier 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 regiemodellen 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

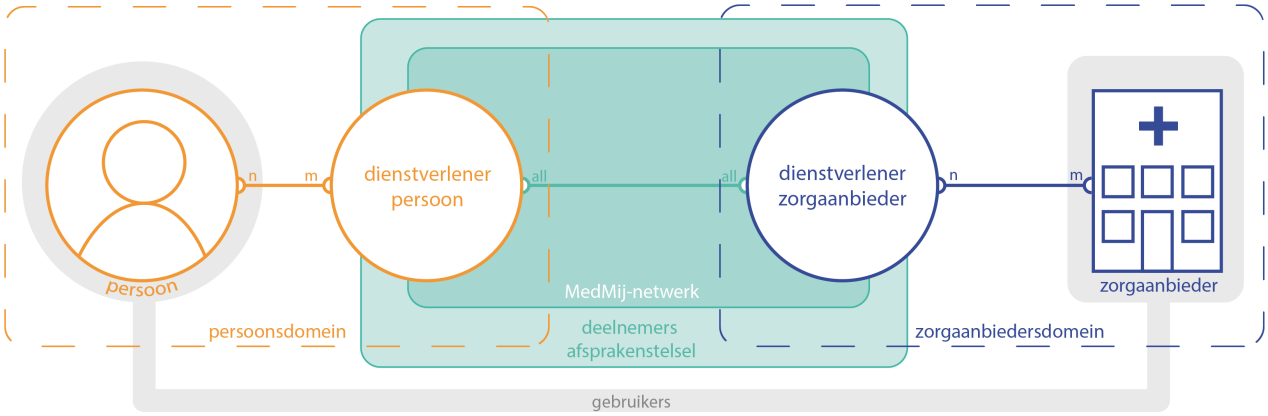
Het afsprakenstelsel wordt (door)ontwikkeld in samenspraak met de belangrijkste stakeholders, waaronder vertegenwoordigers van de deelnemers, de gebruikers en partijen met een belang bij het functioneren van het stelsel. Dit zorgt ervoor dat (door)ontwikkeling en gebruik zoveel mogelijk van elkaar profiteren, 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.	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. De Dienstverlener zorgaanbieder informeert de Zorgaanbieder over de nieuwe gegevens.

Begrippenlijst

Doel

De begrippenlijst geeft een eenduidige definitie van de belangrijkste begrippen die in het afsprakenstelsel worden gebruikt.

Begrip	Definitie	Synoniemen
Afsprakenstelsel	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
Deelnemer	Een partij die dienstverlening aanbiedt binnen het MedMij Afsprakenstelsel. De Dienstverlener persoon en de Dienstverlener zorgaanbieder zijn Deelnemer in het afsprakenstelsel en daarmee gebonden aan de afspraken, bekrachtigd door het tekenen van een deelnemersovereenkomst.	Dienstverlener persoon, Dienstverlener zorgaanbieder
Dienstverlener persoon	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	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	Een partij die gebruik maakt van dienstverlening van deelnemers aan het afsprakenstelsel. De Persoon en de Zorgaanbieder zijn Gebruiker van MedMij.	
Gegevensdienst	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.	
Gezondheidsgegeven	Gegeven betreffende de geestelijke en/of lichamelijke gesteldheid van een persoon.	Persoonlijke gezondheidsinformatie,

		gezondheidsinformatie
MedMij-netwerk	Alle Dienstverleners persoon en alle Dienstverleners zorgaanbieder vormen samen het MedMij-netwerk. Elke Dienstverlener persoon moet elke Dienstverlener zorgaanbieder kunnen bereiken, en vice versa.	Netwerk
Persoon	Degene, 16 jaar of ouder, op wie G ezondheidsgegevens betrekking hebben die via MedMij worden uitgewisseld en tevens de Gebruiker in het Persoonsdomein.	Betrokkene, burger, individu, gebruiker, patiënt, cliënt, zorgconsument, zorggebruiker
Persoonlijke gezondheidsomgeving	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	Alle Personen en alle Dienstverleners personen vormen samen het Persoonsdomein.	
Rol	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.	Functierol
Zorgaanbieder	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	Alle Zorgaanbieders en alle Dienstverleners zorgaanbieder vormen samen het Zorgaanbiedersdomein.	
Zorginformatiesysteem	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
Algemene Verordening Gegevensbescherming (AVG) (gepubliceerd 27-04-2016, geldend vanaf 25-05-2018)	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. 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.	Of een partij die met gebruik making 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: • welke partij(en) in de concrete situatie feitelijk (gezamenlijk) doel en middelen bepaalt (bepalen) van de verwerking van persoonsgegevens; • 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. 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 Overeenkomsten en rechtsrelaties. Ten eerste wordt - voor wat betreft de verantwoordelijkheidsverdeling ten

		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.	aanzien van de naleving van de wet- en 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 WGBO, 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 WGBO, 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 aan de Persoon aanbiedt. 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 wordt daarom gezien als zelfstandig verwerkingsverantwoordelijke binnen het afsprakenstelsel. Alleen in het geval dat Diensten en Gegevensdiensten via het MedMij Afsprakenstelsel worden geleverd, dient er dus een Deelnemersovereenkomst Dienstverlener Persoon of een Deelnemersovereenkomst Dienstverlener Zorgaanbieder 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 Toelichting verwerkingsverantwoordelijkheid. 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 toelichting op de verantwoordelijkheden en normen in de AVG opgenomen. De AP biedt ondersteuning bij de uitvoering van de AVG. 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 praktijkgids 'Patiëntgegevens in de cloud' uitgegeven. De AP heeft deze praktijkgids uitgegeven omdat het gebruik van de cloud risico's met zich meebrengt.
Wet op de geneeskundige behandelingsovereenkomst (WGBO) (geldend vanaf 01-02-2006)	De Wet op de geneeskundige behandelingsovereenkomst (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).	Zorgaanbieders dienen de wettelijke bepalingen te volgen voor 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 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 Gebruikersvoorlichting zijn hiervoor ondersteunende teksten opgenomen.
Wet aanvullende bepalingen verwerking persoonsgegevens in de zorg (geldend vanaf 01-01-2018)	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. De wet introduceert rechten en waarborgen voor cliënten bij elektronische gegevensuitwisseling en het beschikbaar stellen van gegevens via elektronische uitwisselingssystemen. Daarnaast verplicht het zorgaanbieders 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	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

verstrekken van persoonsgegevens met betrekking tot de verlening van, indicatiestelling voor of verzekering van zorg aan andere zorgaanbieders, een indicatieorgaan of aan zorgverzekeraars moet de zorgaanbieder het burgerservicenummer gebruiken.

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 zorgaanbieders, indicatieorganen en 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

vinden in de Handreiking Betrouwbaarheidsniveaus voor digitale dienstverlening en onderzoek patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg, PrivacyCare en PBLQ, 2016.

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 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

		(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 om aan deze verplichtingen te voldoen.	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 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 Architectuur en technische specificaties evenals in het Normenkader informatiebeveiliging. 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 Architectuur en technische specificaties. 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.
Toezicht en controle op de naleving	Binnen het zorgaanbiedersdomein zijn verschillende instanties die wettelijk toezicht houden. Dit toezicht op de uitvoering van geldende wet- en regelgeving blijft onverminderd van kracht. 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	De Stichting MedMij is verantwoordelijk voor controle op de naleving van de verplichtingen van het MedMij Afsprakenstelsel door de deelnemers. 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.

	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 houdt zij toezicht op zorgaanbieders en zorgverzekeraars; • Working Party 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.	
Verordening (EU) 2017/745 van het Europees parlement en de Raad betreffende medische hulpmiddelen (gepubliceerd 05-04-2017, geldend vanaf 26-05-2020)	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.	De Inspectie Gezondheidszorg en Jeugd beschrijft op haar eigen website 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". Vanuit het MedMij Afsprakenstelsel worden geen aanvullende zaken geregeld met betrekking tot medische

	Tegelijkertijd stelt deze verordening hoge kwaliteits- en veiligheidseisen aan medische hulpmiddelen, teneinde tegemoet te komen aan gemeenschappelijke veiligheidsbezwaren ten aanzien van dergelijke producten. Beide doelstellingen worden gelijktijdig nagestreefd en zijn onlosmakelijk met elkaar verbonden waarbij de ene niet ondergeschikt is aan de andere.	hulpmiddelen. Deelnemers dienen zelf een afweging te maken met betrekking tot de toepassing van deze verordening voor hun eigen dienstverlening.
Aanpassingswet richtlijn inzake elektronische handel (geldend vanaf 30-06-2014)	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 de informatiemaatschappij tussen de lidstaten te waarborgen. Dit wordt gerealiseerd door belemmeringen voor de elektronische handel weg te nemen.	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.
Implementatiewet richtlijn consumentenrechten (geldend vanaf 13-06-2014)	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 verkoopruimten (bijvoorbeeld colportage) geregeld. Ook wordt er voor verkoop op afstand en buiten verkoopruimten het herroepingsrecht (bedenktijd voor de consument) geregeld.	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.
Wet gelijke behandeling op grond van handicap en chronische ziekte (wgbh/cz) (geldend vanaf 03-04-2003)	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	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.

	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.	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 ontwerpbepalingen je kunt meenemen. Vaak kom je in die dialoog vanzelf ook tot de evenredige aanpassingen, die je bovendien dan vanaf de start kunt meenemen. Handvatten/concreet stappenplan voor uitvoering: https://www.digitoegankelijk.nl/onderwerpen/stappenplan-toegankelijkheid De verplicht te gebruiken schermen voor de toestemmings- en bevestigingsverklaring binnen het afsprakenstelsel in de usecases voor verzamelen en delen (architectuur en technische specificaties) zijn toegankelijk gemaakt conform de bepalingen in deze wet. Hetzelfde geldt voor de schermen van een door BZK aangewezen authenticatiemiddel.
Aansprakelijkheid	Voor de aansprakelijkheid gelden de algemene regels van het Nederlands recht ten aanzien van de inhoud en omvang van wettelijke verplichtingen tot schadevergoeding. 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. • Bij het 'niet nakomen van een wettelijke verplichting' gaat het bijvoorbeeld om de niet naleving van de voor de deelnemer van toepassing	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. 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.

	zijnde (specifieke) wet- en regelgeving omtrent privacy en informatiebeveiliging. • 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.	

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 Afsprakenstselsel 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 toegetreden 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 Afsrakenstelsel. 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.

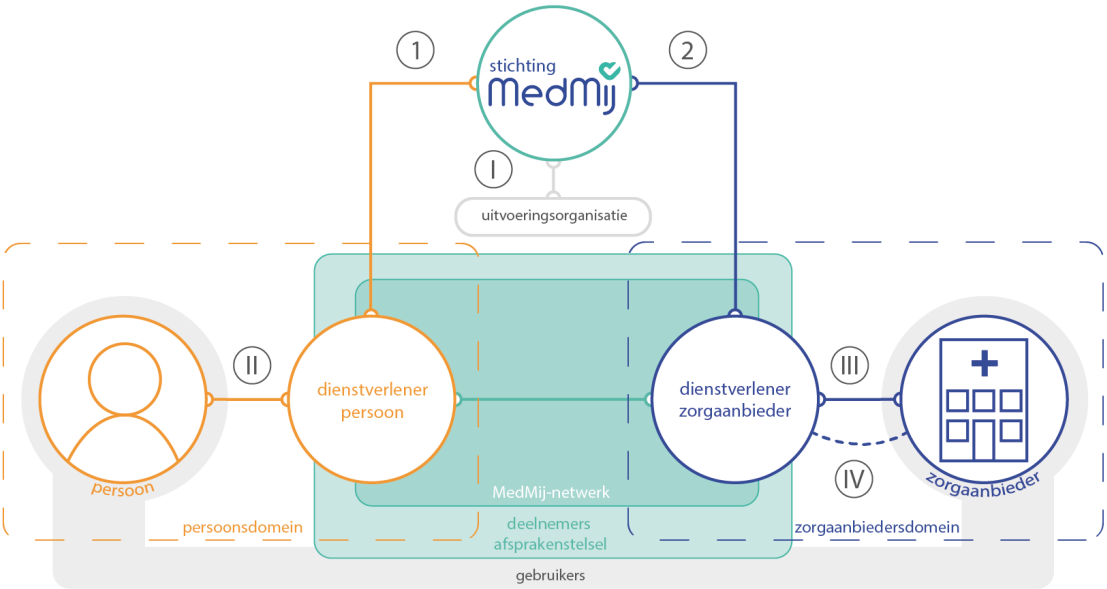
Rechtsrelaties die van belang zijn voor MedMij	Type overeenkomst

I. Stichting MedMij - Beheer /uitvoeringsorganisatie	Opdrachtverlening voor ondersteuning en uitvoering van taken van Stichting MedMij zoals: 1. De instandhouding van de goede technische werking van de gemeenschappelijke voorzieningen in het afsprakenstelsel. 2. Het voeren van de regie over de werking van het Netwerk en het beheer van het MedMij Afsprakenstelsel.
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 Afspakenstelsel - 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.


1
stichting MedMij
2
I
uitvoeringsorganisatie
II
dienstverlener persoon
dienstverlener zorgaanbieder
III
IV
persoon
zorgaanbieder
MedMij-netwerk
deelnemers afsprakenstelsel
persoonsdomein
zorgaanbiedersdomein
gebruikers

Toelichting verwerkingsverantwoordelijkheid

Inleiding

Het MedMij Afsprakenstelsel onderscheidt een tweetal 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.

In de uitvoering van de use case Verzamelen en de use case Delen zijn verschillende partijen 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 zowel de use case Verzamelen als de use case Delen geldt dat in het geval de Persoon gegevens en /of gezondheidsinformatie met zijn Zorgaanbieder wil uitwisselen, de Zorgaanbieder de Persoon altijd eerst moet identificeren en authenticeren. Zoals ook in het Juridisch kader is aangeven 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. Immers de Zorgaanbieder is 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 - de 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 (via de DVZA) en na de authenticatie van de Persoon door de Zorgaanbieder - over de Persoon van de ZA 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 patient hiervoor zijn toestemming heeft gegeven. De Dienstverlener persoon aan wie de ZA (via de DVZA) 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.

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 (via de Dienstverlener persoon persoonsgegevens en/of gegevens over de gezondheid van de Persoon (via 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 (via 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 bevestigt, stuurt de Dienstverlener zorgaanbieder een zogenaamde autorisatiecode aan de Dienstverlener Persoon van de Persoon op basis waarvan de Dienstverlener 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 autorisatiecode 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 wel een autorisatiecode 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.

Release 1.1

De verstrekking van de autorisatiecode door de Dienstverlener zorgaanbieder, onder verantwoordelijkheid van de Zorgaanbieder, aan de Dienstverlener persoon wordt nog nader geanalyseerd in relatie tot de wet- en regelgeving. Deze pagina biedt mogelijk nog geen volledig overzicht van de juridisch relevante aspecten van deze verstrekking.

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 het feit dat het de eigen verantwoordelijkheid van de verwerkingsverantwoordelijke is 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
		Toepassingsgebied AVG	
Artikel 2, 3	De AVG is van toepassing op: • verwerkingen die geheel of gedeeltelijk geautomatiseerd zijn, alsmede; • op de verwerking van persoonsgegevens die in een bestand zijn opgenomen of die bestemd zijn om daarin te worden opgenomen. Waarbij bestand elk gestructureerd geheel van persoonsgegevens inhoudt die volgens bepaalde criteria toegankelijk zijn. Deze verwerking van persoonsgegevens waar de AVG op 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. 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.	Het afsprakenstelsel bepaalt dat de deelnemers aan het afsprakenstelsel 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.	

Algemene bepalingen en definities			
Artikel 4, 9	Het begrip Persoonsgegevens betreft alle informatie over een geïdentificeerde of identificeerbare natuurlijke persoon. De AVG maakt een onderscheid tussen: 1) persoonsgegevens, en 2) bijzondere categorieën van persoonsgegevens. Bijzondere categorieën van persoonsgegevens, hierna bijzondere persoonsgegevens, betreft 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. Persoonsgegevens die via het MedMij netwerk uitgewisseld zullen worden, zullen voornamelijk bijzondere persoonsgegevens betreffen aangezien de verwerking voornamelijk op gegevens betreffende de gezondheid van personen zal zien		
Artikel 4	In de AVG worden twee rollen gedefinieerd:	Gelet op de rolomschrijvingen in het afsprakenstelsel zullen de Zorgaanbieder en de Dienstverlener Persoon	

	1) verwerkingsverantwoordelijke, 2) verwerker. Een **verwerkingsverantwoordelijke** 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. Een **verwerker** 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. Het is de feitelijke situatie waaruit afgeleid wordt welke partij welke rol vervult, dit is contractueel niet af te spreken.	waarschijnlijk de rol van verwerkingsverantwoordelijke vervullen. De Dienstverlener Zorgaanbieder zal, indien gegevens verwerkt worden in opdracht van de Zorgaanbieder, de rol aannemen van verwerker. Dit hangt echter wel altijd af van de feitelijke informatie en omstandigheden. Een toelichting is gegeven op de pagina Toelichting verwerkingsverantwoordelijkheden	
Artikel 4	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.		
Artikel 5	Persoonsgegevens die verwerkt worden dienen juist te zijn en zo nodig geactualiseerd te worden. Redelijke maatregelen moeten worden genomen door		Zorgaanbieders 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.		Dienstverleners Persoon, als aanbieder van een PGO, dienen zich er van 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 Persoon wordt opgenomen.
Artikel 5	In beginsel mogen persoonsgegevens slechts voor: • welbepaalde, • uitdrukkelijk omschreven, en • gerechtvaardigde doeleinden verwerkt worden. 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. Tot slot mogen persoonsgegevens niet langer worden bewaard in een vorm die het mogelijk maakt de betrokkene te identificeren dan noodzakelijk voor de	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 Persoon en Zorgaanbieder via de Dienstverlener Persoon en de Dienstverlener Zorgaanbieder overeenkomstig het bepaalde in het MedMij Afsprakenstelsel is. Deze bepaling is ook opgenomen in artikel 9 van de Modelverwerkersovereenkomst Zorgaanbieder – Dienstverlener zorgaanbieder In het MedMij Afsprakenstelsel zijn bewaartermijnen gegeven voor de vereiste logging van de gegevensuitwisseling en de verwerking.	Aanvullend dienen de dienstverlener persoon en de zorgaanbieder de doeleinden voor (de verdere/ eigen) verwerking van de persoonsgegevens specifiek geformuleerd te worden richting de persoon 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. Doordat het doel duidelijk geformuleerd is, wordt het ook snel duidelijk indien persoonsgegevens verwerkt zullen worden voor secundaire doeleinden. Voordat een Persoon zijn persoonlijke gezondheidsomgeving in gebruik neemt dient de Dienstverlener persoon een specifieke toestemming te verkrijgen van de Persoon voor het verwerken van persoonsgegevens.

	verwezenlijking van de doeleinden waarvoor zij worden verzameld en verder verwerkt.		
Artikel 5	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. **Proportionaliteit** 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. Bij **subsidiariteit** wordt bekeken of de verwerkingsdoeleinden met minder ingrijpende middelen kunnen worden bereikt.	In het MedMij Afsprakenstelsel is onder andere in de architectuur en technische specificaties 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) en vindt onafhankelijke toetsing daarvan plaats.	
Artikel 5, 6	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	
Artikel 6, 7, 9	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 **grondslagen**: 1) Toestemming van de betrokkene; 2) De gegevens zijn noodzakelijk voor de uitvoering van een overeenkomst waarbij de betrokkene een partij is; 3) De gegevens zijn noodzakelijk voor het volgen van een wettelijke verplichting; 4) De gegevensverwerking is noodzakelijk om vitale belangen van de betrokkene of van een ander natuurlijk persoon te beschermen; 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; 6) De gegevensverwerking is noodzakelijk voor de behartiging van het gerechtvaardigde belang van u of van een	**Algemeen:** 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 Persoon en Zorgaanbieder via de Dienstverlener Persoon en de Dienstverlener Zorgaanbieder overeenkomstig het bepaalde in het MedMij Afsprakenstelsel is. 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 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.	**Algemeen:** Let goed op het verschil tussen toestemming en expliciete toestemming. Een grondslag voor de verwerking van bijzondere persoonsgegevens is uitdrukkelijke toestemming. 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.

	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; 5. de verwerking betrekking heeft op persoonsgegevens die kennelijk door	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.	

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 diagnosen, het verstrekken van gezondheidzorg 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. • De toestemming moet zijn gegeven door middel van een duidelijke actieve handeling. • De toestemming moet gevraagd zijn in een begrijpelijk en gemakkelijk toegankelijke vorm. • De toestemming moet vrijelijk gegeven kunnen worden. • De toestemmingsvraag moet in duidelijke en eenvoudige taal gepresenteerd worden. • De toestemming moet ten alle tijden ingetrokken kunnen worden. Indien een verdere verwerking niet verenigbaar is met het oorspronkelijke doel, dan zal de verwerkingsverantwoordelijke een specifieke wettelijke grondslag moeten hebben of toestemming moeten vragen van de betrokkene voor de verdere verwerking. 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.	Voor de rechtmatigheid van de verwerking van het BSN binnen de scope van het MedMij Afsprakenstelsel wordt verwezen naar het Juridisch kader (wet aanvullende bepalingen verwerking persoonsgegevens in de zorg) en de Toelichting verwerkingsverantwoordelijkheid	

Artikel 8	Specifieke voorwaarden worden gesteld in de AVG voor toestemming van kinderen in het geval er sprake is van **diensten van de informatiemaatschappij**. Indien sprake is van een dergelijke situatie, dient de toestemming verleend te worden door de ouder of voogd. Het aanbieden van een PGO door een Dienstverlener Persoon 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.	**Algemeen:** In het afsprakenstelsel is afgesproken dat voorlopig alleen gezondheidsgegevens van personen van 16 jaar en ouder uitgewisseld worden.	**Let op:** Voor het verwerken van persoonsgegevens van kinderen gelden specifieke (strengere) eisen en evenueel de betrokkenheid van ouder of voogd. 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.
Informatievoorziening			
Artikel 12, 13, 14	Een verwerkingsverantwoordelijke is verantwoordelijk om betrokkenen te **informeren**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.	**Algemeen:** De Dienstverlener persoon is aanvullend op de AVG ook op grond van de Deelnemersovereenkomst (artikel 4.1) verplicht verwerking van de persoonsgegevens overeenkomstig de privacy wet- en regelgeving uit te voeren. Specifiek voor de Dienstverlener persoon is nog opgenomen dat Gebruikers worden geïnformeerd over hoe de Persoon zijn rechten in deze bij de Dienstverlener persoon kan uitoefenen.	

	Indien persoonsgegevens rechtstreeks bij de betrokkene worden verzameld, dient de volgende informatie bij de verkrijging van de persoonsgegevens verstrekt te worden door de verwerkingsverantwoordelijke: • De identiteit en contactgegevens van de verwerkingsverantwoordelijke, en indien van toepassing van de vertegenwoordiger 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 maand na de verkrijging van de persoonsgegevens. 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.		
		Rechten van betrokkenen	
Artikel 15, 16, 17, 18, 20, 21, 22, 23	**Betrokkenen** waarvan persoonsgegevens verwerkt worden komen verschillende **rechten**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. **Recht op inzage** Betrokkenen hebben het recht om van de verwerkingsverantwoordelijke uitsluitsel te verkrijgen over het al dan niet verwerken	**Algemeen**: Betrokkenen, Personen in termen van het MedMij Afsprakenstelsel, kunnen hun rechten uitoefenen jegens de Dienstverlener persoon voor de gegevens die verwerkt worden binnen de PGO omgeving. Verzoeken die gebaseerd zijn op een recht dat de betrokkene toekomt dienen daarom rechtstreeks aan de Dienstverlener persoon gericht te worden indien het gaat om persoonsgegevens die verwerkt worden in de PGO. In art. 4.1 van de Deelnemersovereenkomst hebben we opgenomen dan de deelnemers de verwerking van de persoonsgegevens overeenkomstig de privacy wet- en regelgeving uitvoeren. Specifiek voor de Dienstverlener persoon is nog opgenomen dat Gebruikers worden geïnformeerd over hoe de Persoon zijn rechten in deze bij de Dienstverlener persoon kan uitoefenen.	**Algemeen**: Zorg dat betrokkenen, personen, de genoemde rechten kunnen uitoefenen en richt hiervoor processen in. Het is van belang dat de deelnemer kan aantonen dat dit (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.

van hen betreffende persoonsgegevens. Indien dit het geval is, heeft de betrokkene het recht om inzage te verkrijgen van die 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

Algemeen : Betrokkenen, Personen in termen van het MedMij Afsprakenstelsel, kunnen daarnaast hun rechten uitoefenen jegens de zorgaanbieder met betrekking tot de gegevens die verwerkt worden door de zorgaanbieder in de uitoefening van zijn zorgtaken. De relatie Persoon – 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 modelverwerkersovereenkomst tussen de Dienstverlener zorgaanbieder en de Zorgaanbieder opgenomen dat de Dienstverlener zorgaanbieder zijn medewerking verleent.

betreffende persoonsgegevens te verkrijgen. De verwerkingsverantwoordelijke is in de 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 is in afwachting 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 dat hergebruik ondersteunt;
- hun 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
- dat 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 onderwerpen aan een besluit dat tot stand is gekomen door een uitsluitend geautomatiseerde verwerking of profilering. **NB** 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.		
		Verplichtingen verwerkingsverantwoordelijken	
Artikel 5, 24 t /m 28, 30 t/m 36	Op partijen die de rol van **verwerkingsverantwoordelijke** vervullen rusten diverse **verplichtingen**. 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. 2. De verwerkingsverantwoordelijke is verantwoordelijk voor het implementeren van passende **technische en organisatorische maatregelen** om te	**Algemeen**: Het afsprakenstelsel bepaalt dat de deelnemers aan het afsprakenstelsel ingeschreven dienen te zijn in een handelsregister in de EU. In het MedMij Afsprakenstelsel is onder andere in de architectuur en technische specificaties 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) en vindt onafhankelijke toetsing daarvan plaats.	

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 omvatten. Het naleven van goedgekeurde gedragscodes kan een bewijs zijn van naleving.

3. Verwerkingsverantwoordelijke 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 respectieve 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 voor de 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. Bijvoorbeeld het inschakelen van een hostingbedrijf om data van een PGO te hosten.	**6. Verwerkersovereenkomst** . Aanvullend op de verplichtingen in de AVG wordt in het 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.	

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 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

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. Als deelnemer 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.

	• indien van toepassing die van 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. 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**	**9. Passende technische en organisatorische beveiligingsmaatregelen**. In het MedMij afsprakenstelsel is een aanvullend normenkader informatiebeveiliging opgenomen. Op basis van een stelsel risicoanalyse 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.	.

	organisatorische beveiligingsmaatregelen treffen om persoonsgegevens te beschermen tegen onopzettelijke of onrechtmatige vernietiging of verlies, wijziging, ongeautoriseerde openbaarmaking of toegang. Afhankelijk 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 inbeuk 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 dat beoordeeld is dat het niet waarschijnlijk is dat de	**10. Datalek** . Deelnemers aan het afsprakenstelsel zijn zelf verantwoordelijk om eventuele datalekken te signaleren. Zie hiervoor ook de Guidelines on Personal data breach notification van de Europese privacytoezichthouders. https://autoriteitpersoonsgegevens.nl/nl/onderwerpen/beveiliging/meldplicht-datalekken In het MedMij Afsprakenstelsel is in het Normenkader 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.	

inbreuk in verband met persoonsgegevens een risico inhoudt voor de rechten en vrijheden van betrokkenen. De melding moet minimaal de volgende informatie bevatten:

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. 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

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 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; • beoogde maatregelen om de risico's aan te pakken. 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.		
		Verplichtingen verwerker	
Artikel 28 t/m 33, 37	Op partijen die de rol van **verwerker** vervullen rusten diverse **verplichtingen**. 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. 2. Een verwerker moet de beveiliging van de persoonsgegevens die hij verwerkt	In artikel 8 van de Deelnemersovereenkomst zijn, aanvullend op de AVG, verantwoordelijkheden van een deelnemer jegens derden, waaronder verwerkers van persoonsgegevens, opgenomen.	**Algemeen:** Ook voor verwerkers (bijvoorbeeld de dienstverlener zorgaanbieder 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.

garanderen aan de verwerkingsverantwoordelijke.

3. De verwerker moet ervoor zorgen dat alle persoonsgegevens die hij verwerkt vertrouwelijk worden behandeld. De 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 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 die van 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. 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	

	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 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 inbeuk in verband met persoonsgegevens, ook wel **datalek** genoemd, zonder onredelijke vertraging te melden aan de verwerkingsverantwoordelijke. 9. Indien de verwerkingsverantwoordelijke waar de verwerker persoonsgegevens voor	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 afsprakenstelsel, en is aansprakelijk voor het handelen op grond van deze Overeenkomst van de door hem ingeschakelde derde.	**9. Functionaris voor de gegevensbescherming.** We raden aan voor verwerkers om zelf te onderzoeken of zij een functionaris voor de gegevensbescherming aan moeten stellen doordat de verwerkingsverantwoordelijke hiertoe ook verplicht is.

	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 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 zorg- en 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. Op dit abstractieniveau zijn de proceslaag en de informatielaag uit het interoperabiliteitsmodel van Nictiz 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.

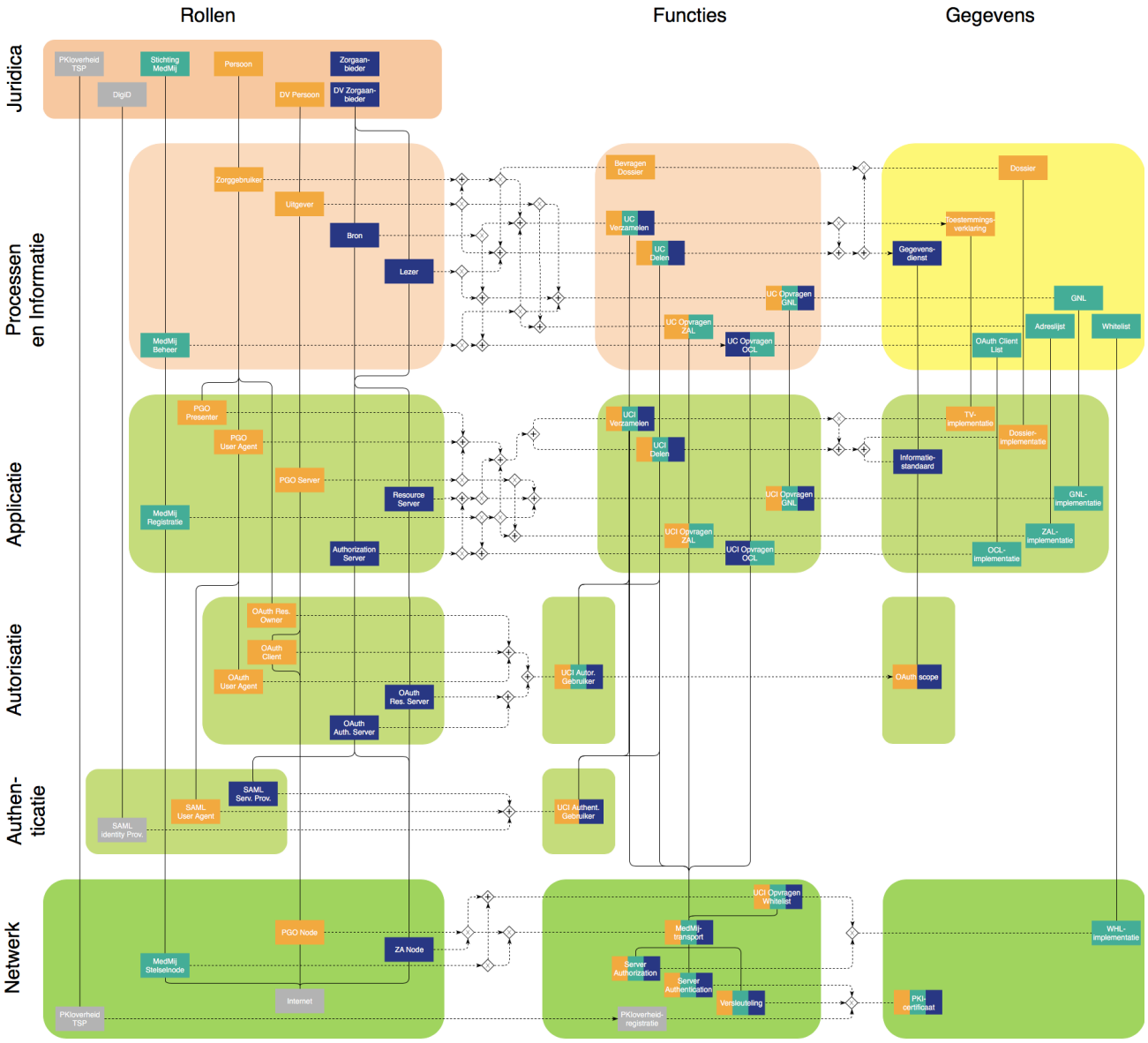
Op het onderste abstractieniveau, de Netwerk-laag, zijn de verantwoordelijkheden opgenomen op het gebied van de netwerkinfrastructuur.

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 specificatie lagen 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 grof 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.

De totale architectuur van het MedMij Afsprakenstelsel is weergegeven in onderstaande figuur.



Toelichting

In de architectuur is ook een driedeling in kolommen aangebracht: rollen, functies en gegevens. 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, niet om die van een oplossing, speelt de rollenkolom een sleutelrol in de samenhang van de gehele architectuur. Rollen zijn bundels van verantwoordelijkheden, geen componenten. Die verantwoordelijkheden zijn gekoppeld aan uit te voeren functies (tweede kolom), die op hun beurt gebruik maken van gegevens (derde kolom).

De applicatielaag is verfijnd door twee deellagen af te zonderen: 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 gerealiseerd.

Bovendien is het op deze manier mogelijk om de afspraken die specifiek voortvloeien uit het ontwerp van die standaard 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 SAML-koppelvlak van DigiD. 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. 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 maalteken 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 zes use cases: *UC Verzamelen*, *UC Delen*, *UC Opvragen ZAL*, *UC Opvragen OCL*, *UC Opvragen WHL* 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.

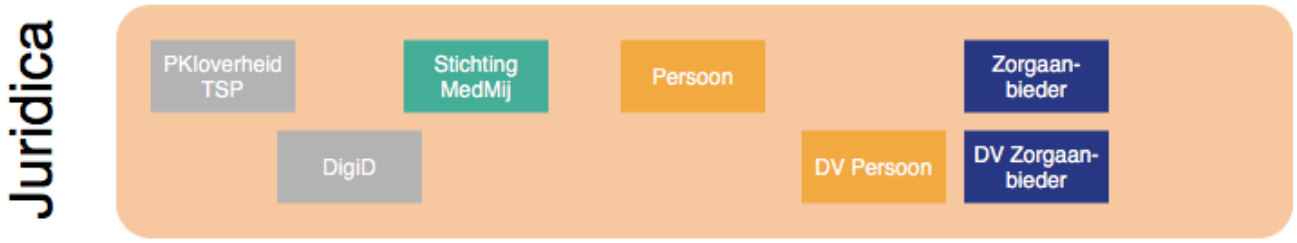
De rollen en verantwoordelijkheden zijn om te beginnen bondig en stellig als regel geformuleerd. Pas in tweede instantie zijn ze voorzien van toelich-ting. De opzet is dus niet die van een verhalende uiteenzetting van het stelsel, maar die van een setje afspraken, artikelsgewijs. Dat maakt de architectuur 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.

Juridica



Toelichting

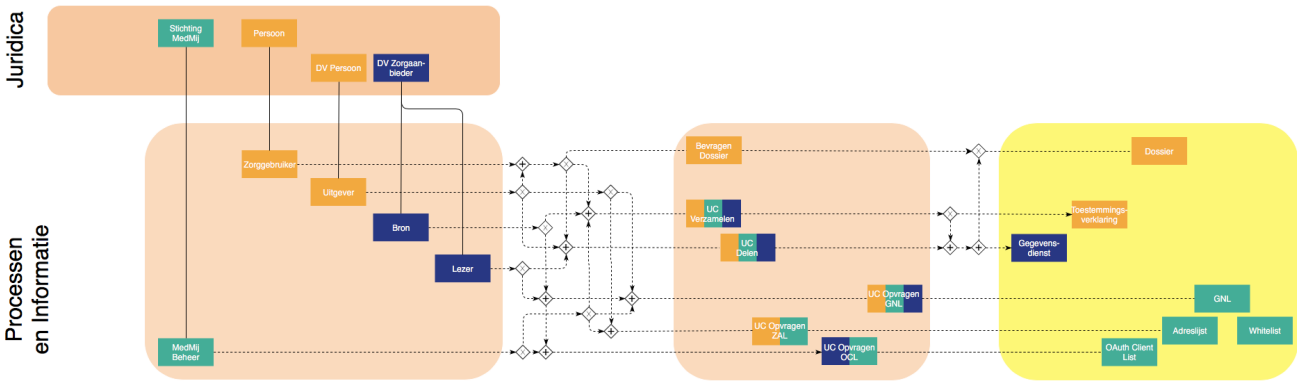
In deze laag staan de juridische rollen, als juridische basis voor de rollen op andere lagen van de architectuur. De enige reden dat deze laag in deze architectuur is opgenomen is dat rollen voor de samenhang tussen de verschillende architectuurlagen zorgen en de architectuur ook geborgd moet zijn in 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 *directe* juridische rollen, die partij zijn in MedMij-deelnemersovereenkomsten: *Dienstverlener persoon*, *Dienstverlener zorgaanbieder* en *Stichting MedMij*.
2. de *indirecte* 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 *DigiD*, *PKIoverheid TSP*, *Persoon* en *Zorgaanbieder*.

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*.

Processen en informatie



Toelichting

Voor een overzicht over alle lagen van de architectuur, en voor een toelichting van de betekenis van de symbolen en lijntjes, zie de overzichtspagina.

In deze figuur zijn de rollen, functies en gegevens-elementen uit de proces- en informatie-architectuur weergegeven, inclusief de binding (verticale lijnen) van deze rollen aan de juridische (zie Juridica). 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.

Rollen

1. *Dienstverlener persoon* neemt de functionele rol van *Uitgever* op zich.
2. *Dienstverlener zorgaanbieder* neemt de functionele rol van *Bron* en/of *Lezer* op zich.
3. *Stichting MedMij* neemt de functionele rol van *MedMij Beheer* op zich.
4. *Persoon* neemt de functionele rol van *Zorggebruiker* op zich.

Toelichting

Met de rollen *Uitgever, Bron* en *Lezer* staat hier de principiële keus die het afsprakenstelsel maakt voor de aard van de regie die zij aan personen wil geven over de gezondheidsinformatie waarvan zijzelf het onderwerp zijn. Er zijn andere regiemodellen mogelijk, zwakkere en sterkere. In dit model is de *Dienstverlener persoon*, namens de *Persoon*, *Uitgever* van zijn/haar gezondheidsinformatie, betrekt die informatie daartoe van *Bronnen* en stelt die informatie beschikbaar aan *Lezers*. Zo krijgt de *Persoon* de regie die MedMij hem wil bieden. In deze release van het MedMij Afsprakenstelsel verzamelt *Uitgever* gezondheidsinformatie bij *Bronnen* en deelt hij gezondheidsinformatie met *Lezers.*

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. Alle complexiteit voor de implementatie van die verantwoordelijkheid ligt bij de *Bron*, respectievelijk *Lezer*. Dat werkt door in de Applicatielaag en de Netwerklaag.

Omdat ook de *Stichting MedMij* operationele verantwoordelijkheden heeft, staat hier de functionele rol van *MedMij Beheer*.

Verantwoordelijkheden

Toelichting

De verantwoordelijkheden op deze laag en die op de Applicatielaag hebben een vergelijkbare opbouw. Ze zijn geordend in hoofdstukken en secties als volgt:

- Dossier
  - Use cases
  - Gegevensdiensten
  - Authenticatie
  - Autorisatie
- Lijsten
  - Zorgaanbiederslijst
  - OAuth Client List
  - Gegevensdienstnamenlijst
  - Whitelist
- Logging

Op meerdere plaatsen komen daarbij use cases (op deze laag) en use case-implementatie (op de applicatielaag) aan de orde. Een use case-implementatie is de implementatie van de use case met dezelfde naam. In deze release van het afsprakenstelsel zijn er zes use cases, waarvan vijf zich afspelen tussen het Persoons- en het Zorgaanbiedersdomein. Van deze vijf maken, om de interoperabiliteit in het MedMij-netwerk te borgen, stroomdiagrammen deel uit van het afsprakenstelsel. De zesde speelt zich helemaal binnen het Persoonsdomein af. Hiervan eist het MedMij Afsprakenstelsel wel dat erin moet worden voorzien, maar niet hoe; dat wordt aan de vrijheid van de MedMij-deelnemers gelaten.

Het gaat om de volgende use cases:

Use case	Stroomdiagram
UC Verzamelen	met
UC Delen	met
Raadplegen dossier	zonder
UC Opvragen ZAL	met
UC Opvragen OCL	met
UC Opvragen GNL	met

Voor registratie van MedMij-deelnemers en van hun vanwege hun deelname belangrijke gegevens zijn vooralsnog geen separate use cases geïdentificeerd, omdat registratie een secundair en vooralsnog niet geautomatiseerd proces is. 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 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 regel 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 Dele*n 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

De nummering van de verantwoordelijkheden is zo gekozen om in dezen achterwaartse compatibiliteit te behouden met release 1.0. 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*.

2. *Uitgever* biedt *Zorggebruiker* de use case *Bevragen dossier* om het persoonlijk gezondheidsdossier te raadplegen.

Toelichting

Zie onder 1. Omdat deze functie zich niet over meerdere functionele rollen uitstrekt, is zij niet nader gespecificeerd in een stroomdiagram. Het is aan de vrijheid van de deelnemer in het afsprakenstelsel om deze naar behoefte van haar klanten in te richten. Maar zij mag niet ontbreken, omdat dan de Zorggebruiker geen regie over het dossier kan voeren.

3. In het kader van de use case *Bevragen 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.

Gegevensdiensten

4. *Uitgever* laat *Zorggebruiker* met een *Gegevensdienst* uit de *Gegevensdienstnamenlijst* gezondheidsinformatie verzamelen door 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 in deze release kunnen worden geboden.

5. Elke *Bron* biedt op elk moment minstens één *Gegevensdienst*. Elke *Lezer* biedt op elk moment minstens één *Gegevensdienst*.

> **Toelichting**
>
> Het bieden 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.

6. *MedMij Beheer* zal alleen in de *Zorgaanbiederslijst* opnemen dat een zekere *Gegevensdienst* voor 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 *Informatiestandaard* ontsluit) om ervoor te zorgen dat de *Dienstverlener zorgaanbieder* zich voor die *Informatiestandaard* moet kwalificeren in het afsprakenstelsel.

7a. Voor elke *Gegevensdienst* waarvan de *Zorgaanbiederslijst* aan-geeft dat een zekere*Zorgaanbieder* deze aanbiedt, zal *Bron*, respectievelijk *Lezer*, ervoor zorgdragen dat daaraan opvol-ging gegeven wordt, zonder daarbij welke *Uitgever* dan ook bij voorbaat uit te sluiten. Dat geldt ook voor de mogelijke andere *Gegevensdienst(en)* die in de *Catalogus* staan genoemd als *Vereist* bij eerstgenoemde *Gegevensdienst*.

> **Toelichting**
>
> Net als regel 6, moet regel 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. Zo ontzorgt de *Dienstverlener zorgaanbieder* zijn tegenspelers in het afsprakenstelsel.

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 naijlende 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, 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* geldt niet buiten deze doorloping van de *UC Verzamelen*.

Toelichting

Het is dus de *Bron* die de *Toestemming* ophaalt bij de *Zorggebruiker*. De tweede zin van deze regel maakt de toestemming functioneel zo eenvoudig mogelijk, omdat in de huidige 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.

Authenticatie

9. *Bron* en *Lezer* dragen ervoor zorg dat de onder 7 bedoelde opvolging, en de onder 8a en 8b bedoelde vraag om *Toestemming*, respectievelijk bevestiging, slechts plaatsvindt wanneer hij de identiteit van de *Zorggebruiker* met passende zekerheid heeft vastgesteld.

Toelichting

Op de applicatielaag wordt beschreven dat de identiteit van de Zorggebruiker wordt met een BSN en die passende zekerheid wordt verkregen door middel van *DigiD*.

Lijsten

Zorgaanbiederslijst

10. *MedMij Beheer* beheert en publiceert een *Zorgaanbiederslijst*, namens de deelnemende *Dienstverleners Zorgaanbieder*. De *Zorgaan-bie-derslijst* beschrijft van elke *Zorgaanbieder* welke *Gegevensdiensten* deze momenteel biedt via welke *Bron* en *Lezer,* en welke technische adressen daarvoor moeten worden aangesproken bij die *Bron* of *Lezer.* De gepubliceerde *Zorgaanbiederslijst* bevat steeds en slechts alle actuele entries.

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*. Zonder deze functie zou het stelsel niet functioneren.

11. De inhoud van de *Zorgaanbiederslijst* voldoet aan het metamodel en het daaruit afgeleide logische model van de *Zorgaanbiederslijst*.

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: *Opvragen Zorgaanbiederslijst*. Betrokken rollen gebruiken hiertoe het betreffende stroomdiagram.

OAuth Client List

14. *MedMij Beheer* beheert en publiceert een actuele *OAuth Client List*, namens de deelnemende *Dienstverleners persoon*. Deze beschrijft wat de gebruikersvriendelijke namen zijn die voor de *Dienstverleners persoon* worden gebruikt in de toestemmingsverklaring*. De inhoud van de OAuth Client List voldoet aan het logische metamodel.*

> **Toelichting**
>
> De *OAuth Client List* bevat dus geen namen voor *Dienstverleners zorgaanbieder*. Dat is niet nodig, omdat deze niet voorkomen in de toestemmingsverklaring.

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 *GegevensdienstIds.* De inhoud van de *Gegevensdienstnamenlijst* voldoet aan het logische metamodel.

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 inhoud van de *Whitelist* voldoet aan het logische metamodel.

> **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

19. *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 persoonsgege-vens 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.

20. De bewaartermijn van de logbestanden is ten minste 12 maanden en niet meer dan 15 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.

21. *MedMij Beheer* onderhoudt een archief van alle ooit ontsloten 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 20.

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. Voor zover laatstgenoemde deelnemer is in het MedMij Afsprakenstelsel, kan deze dus 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. Voor zover laatstgenoemde deelnemer is in het MedMij Afsprakenstelsel, kan deze dus 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 gecomprimeerd en anoniem weergegeven.

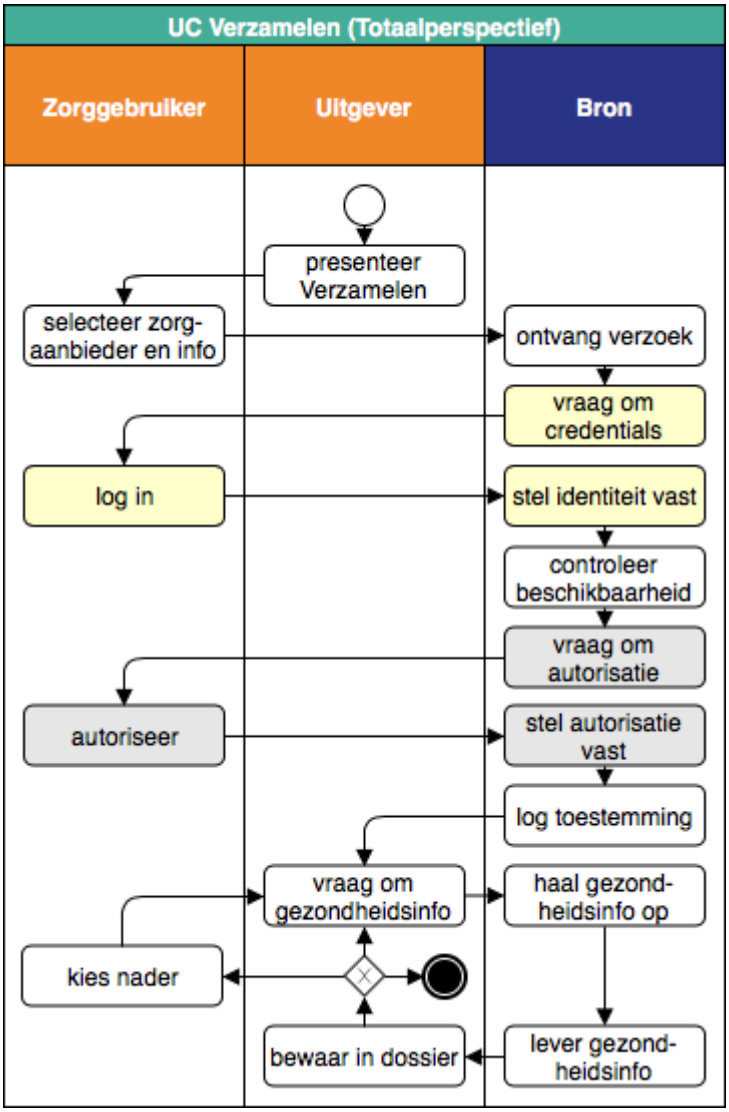
Tot slot bespreken we de uitzonderingen op de happy flow. Daarbij werken we alleen vanuit het totaalperspectief.

Totaalperspectief (happy flow)

Toelichting

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 soort te verzamelen informatie. Daarvoor kunnen desgewenst de *Gegevensdienstnamen* worden gebruikt uit de *Gegevensdienstnamenlijst*. Het verzoek gaat naar de passende *Bron*.
- De *Bron* laat de *Zorggebruiker* zich authenticeren.
- Als dat slaagt, controleert de *Bron* alvast of de *Zorgaanbieder* voor de betreffende *Gegevensdienst* überhaupt gezondheidsinformatie van die *Persoon* beschikbaar heeft.
- Zo ja, dan vraagt de *Bron* aan de *Zorggebruiker* of hij toestemming geeft tot het verstrekken van de gevraagde informatie aan de *Uitgever*.
- De *Bron* logt die toestemming en laat de *Uitgever* weten of de autorisatie geslaagd is.
- Zo ja, dan kan de *Uitgever* de *Bron* vragen om de gezondheidsinformatie.
- Bij ontvangst slaat de *Uitgever* die informatie op in het persoonlijke dossier.
- Mocht de *Gegevensdienst* waartoe de *Zorggebruiker* heeft geautoriseerd uit meerdere *Transacties* bestaan, bevraagt de *Uitgever* de *Bron* daarna mogelijk opnieuw voor de nog resterende *Transacties*, eventueel na nieuwe gebruikersinteractie.
- Bij de informatie wordt ook de meta-informatie opgeslagen die wordt bedoeld in verantwoordelijkheid 20 van de Processen- en Informatielaag.



De vraag die aan de *Zorggebruiker* gesteld moet worden in de stap "autoriseer" staat op de pagina Toestemmingsverklaring. Op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen is omschreven hoe de variabelen in deze verklaring gevuld worden.

Uitzonderingen (Totaalperspectief)

Toelichting

In onderstaande tabel staan de uitzonderingssituaties beschreven. Alle worden door de *Bron* ontdekt. In deze release 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 *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*, in de controle op beschikbaarheid, de gevraagde gezondheidsinformatie ter beschikking 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 beschikbaarheidstoets worden opgevat. Wanneer een toekomstige release van het MedMij afsprakenstelsel wel zulke toestemmingen of machtigingen omvat, zal de leeftijdstoets gescheiden moeten worden van de beschikbaarheidstoets.

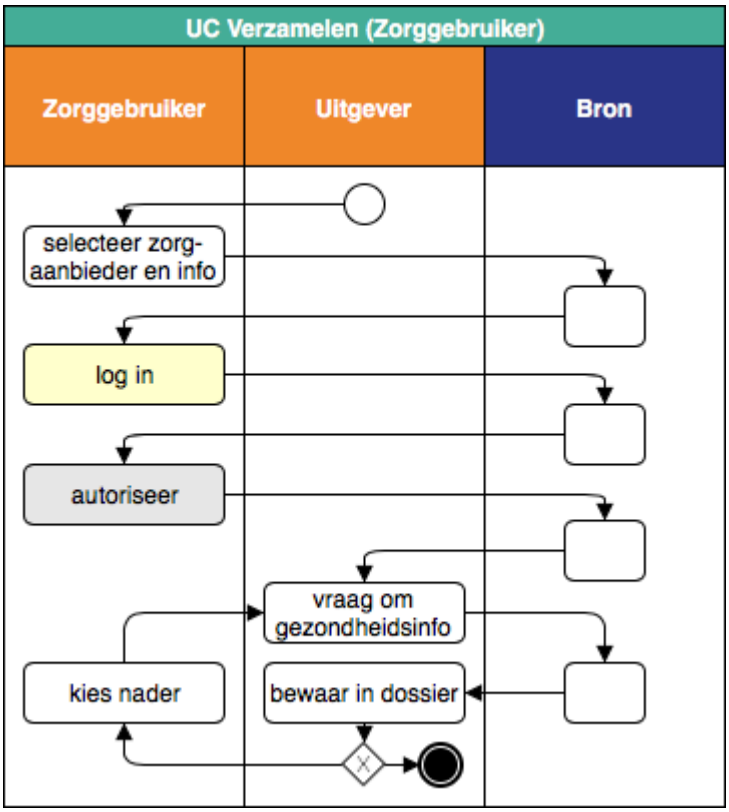
nr.	uitzondering	actie	vervolg
UC Verzamelen 1	*Bron* vindt het ontvangen verzoek ongeldig.	*Bron* informeert *Uitgever* over deze uitzondering. *Uitgever* informeert daarop *Zorggebruiker* hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Verzamelen 2	*Bron* kan de identiteit van de *Zorggebruiker* niet vaststellen.	*Bron* informeert *Uitgever* dat verzamelen niet toegelaten wordt.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Verzamelen 3	*Bron* stelt vast dat van *Persoon* bij *Zorgaanbieder* geen gezondheidsinformatie voor die *Gegevensdienst* beschikbaar is. Hiervan is in elk geval sprake indien hetzij: • er geen behandelrelatie is aan te wijzen als grondslag voor het verzamelen; • *Zorggebruiker* nog geen zestien jaar oud is.		
UC Verzamelen 4	De autorisatievraag wordt ontkennend beantwoord.		
UC Verzamelen 5	*Bron* kan het antwoord op de autorisatievraag niet vaststellen.	*Bron* informeert *Uitgever* over deze uitzondering. *Uitgever* informeert daarop *Zorggebruiker* hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.

UC Verzamelen 6	*Bron* kan, zelfs na autorisatie, de gezondheidsinformatie alsnog niet ter beschikking stellen aan de *Uitgever*.	*Bron* informeert *Uitgever* over deze uitzondering. *Uitgever* informeert daarop *Zorggebruiker* hierover, met opgave van oorzaak.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.

Perspectief van de Zorggebruiker (happy flow)

Toelichting

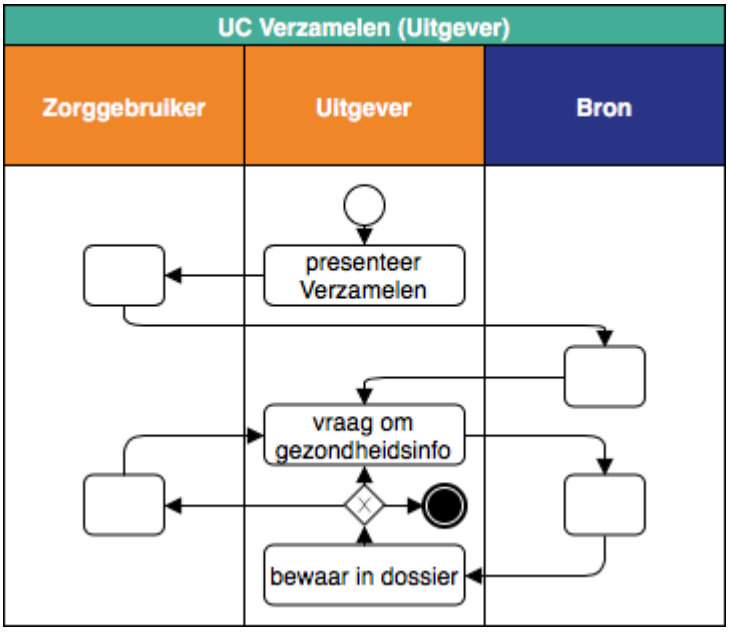
De *Zorggebruiker* moet drie stappen doorlopen: selectie van zorgaanbieder en soort informatie, inloggen en autoriseren. Als alles slaagt, slaat de Uitgever voor hem zowel de toestemming als de verkregen gezondheidsinformatie op.



Perspectief van de Uitgever (happy flow)

Toelichting

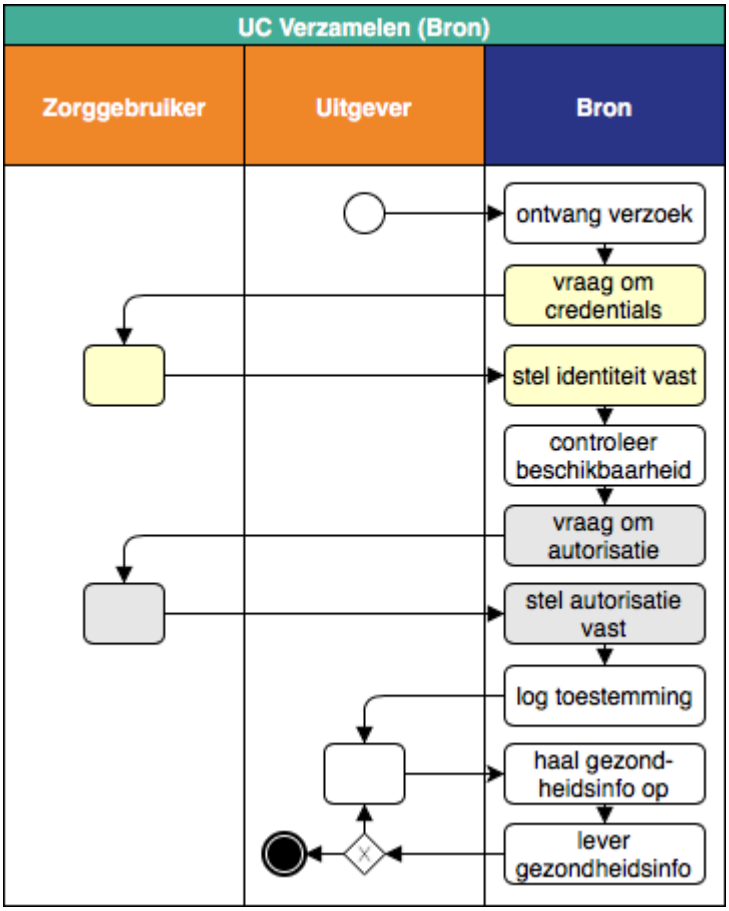
De *Uitgever* start de use case door aan de *Zorggebruiker* de mogelijkheid tot verzamelen te presenteren. Van de *Bron* krijgt hij na enige tijd het bericht dat de toestemming daarvoor is verleend, waarna hij die toestemming logt en de gezondheidsinformatie ophaalt bij de *Bron*, en opslaat.



Perspectief van de Bron (happy flow)

Toelichting

De *Bron* regisseert, na ontvangst van het verzoek tot Verzamelen, de authenticatie en de autorisatie. 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 Verzamelen (Bron)
Zorggebruiker
Uitgever
Bron
ontvang verzoek
vraag om credentials
stel identiteit vast
controleer beschikbaarheid
vraag om autorisatie
stel autorisatie vast
log toestemming
haal gezond-heidsinfo op
lever gezondheidsinfo

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 met de rolomdraaiing ook 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 betrekt, 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*. Wanneer de *Zorggebruiker* deze vraag wordt gepresenteerd, kan hij daaruit de conclusie trekken dat de de betreffende *Zorgaanbieder* ontvankelijk is voor betreffende informatie. Mocht hij dat niet zijn, dan verschijnt een andere melding. Zo blijft de *Zorggebruiker* niet, te lang, in het ongewisse over de voortgang van de use case.
- 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. Voor zover laatstgenoemde deelnemer is in het MedMij Afsprakenstelsel, kan deze dus 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. Voor zover laatstgenoemde deelnemer is in het MedMij Afsprakenstelsel, kan deze dus 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.

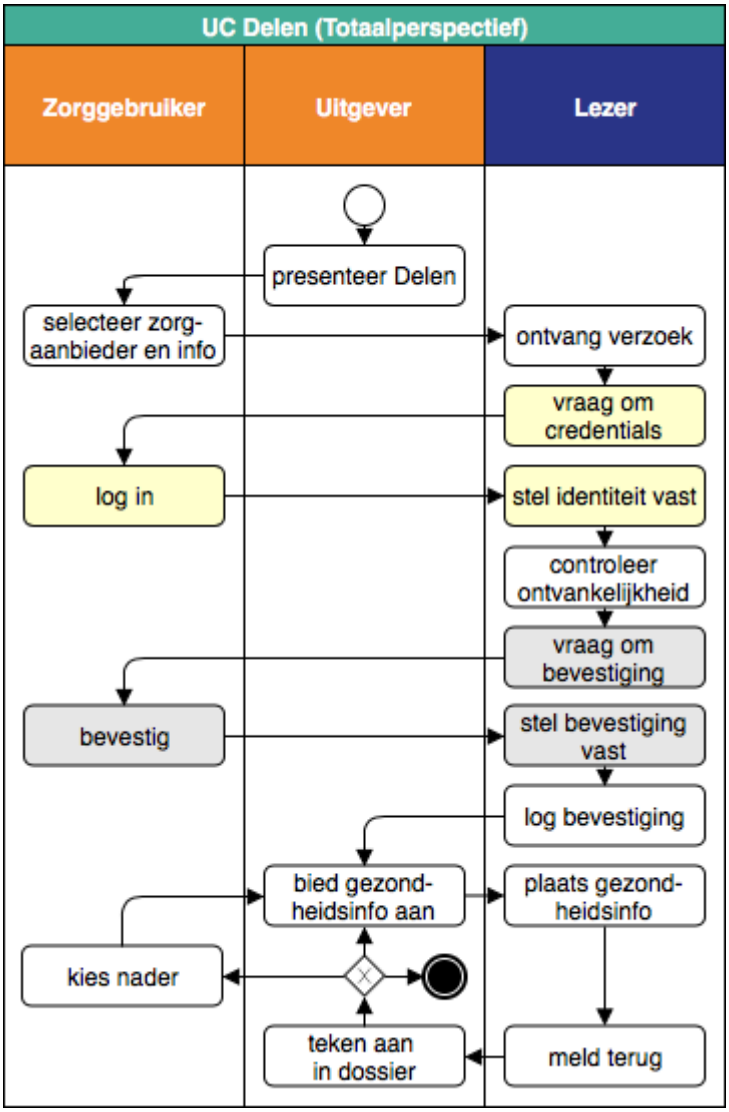
Tot slot bespreken we de uitzonderingen op de happy flow. Daarbij werken we alleen vanuit het totaalperspectief.

Totaalperspectief (happy flow)

Toelichting

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 expliciet de zorgaanbieder waarmee hij de informatie wenst te delen en de te delen informatie. Daarvoor kunnen desgewenst de *Gegevensdienstnamen* worden gebruikt uit de *Gegevensdienstnamenlijst*. Het verzoek gaat naar de passende *Lezer*.
- De *Lezer* laat de *Zorggebruiker* zich authenticeren.
- Als dat slaagt, controleert de *Lezer* alvast of de *Zorgaanbieder* voor de betreffende *Gegevensdienst* überhaupt gezondheidsinformatie van die *Persoon* wenst te ontvangen. Daarvoor is het in elk geval nodig dat de *Zorgaanbieder* een behandelrelatie heeft met de *Persoon*.
- Zo ja, dan vraagt de *Lezer* aan de *Zorggebruiker* of hij de wens bevestigt de informatie te laten verstrekken aan de *Zorgaanbieder*.
- De *Lezer* logt die bevestiging en laat de *Uitgever* weten of die geslaagd is.
- Zo ja, dan kan de *Uitgever* de gezondheidsinformatie plaatsen bij de *Lezer*.
- Mocht de *Gegevensdienst* waartoe de *Zorggebruiker* heeft geautoriseerd uit meerdere *Transacties* bestaan, plaatst de *Uitgever* daarna mogelijk opnieuw bij de *Lezer* voor de nog resterende *Transacties*, eventueel na nieuwe gebruikersinteractie.
- De Uitgever tekent bij de informatie ook de meta-informatie aan die wordt bedoeld in verantwoordelijkheid 20 van de Processen- en Informatielaag.



De vraag die aan de *Zorggebruiker* gesteld moet worden in de stap "bevestig" staat op de pagina Bevestigingsverklaring. Op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen is omschreven hoe de variabelen in deze verklaring gevuld worden.

Uitzonderingen (Totaalperspectief)

Toelichting

In onderstaande tabel staan de uitzonderingssituaties beschreven. Alle worden door de *Lezer* ontdekt. In deze release 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 *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 verklaard 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 ontvankelijkheidstoets worden opgevat. Wanneer een toekomstige release van het MedMij Afsprakenstelsel wel zulke toestemmingen of machtigingen omvat, zal de leeftijdstoets gescheiden moeten worden van de ontvankelijkheidstoets.

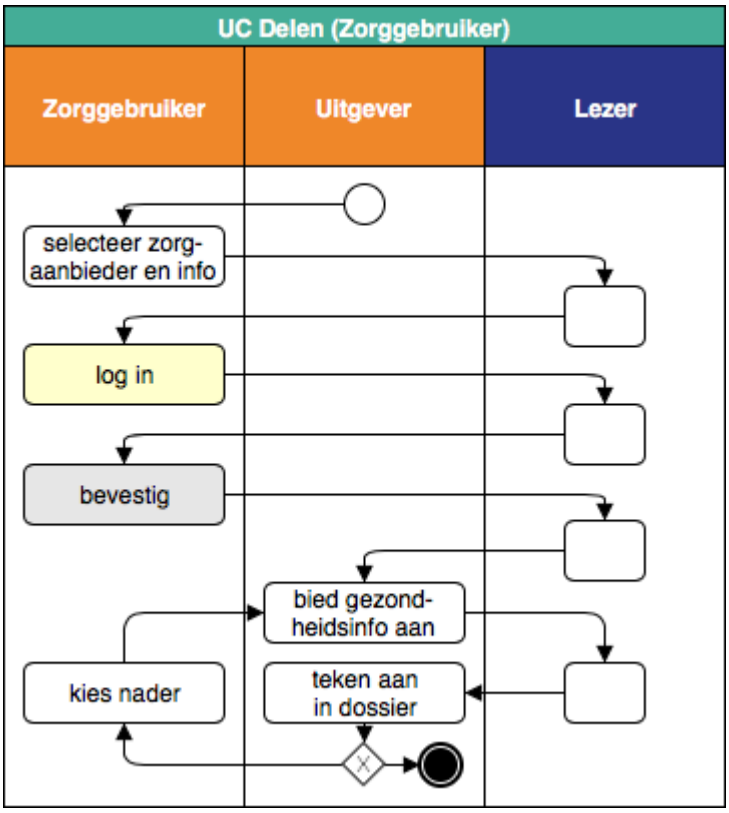
nr.	uitzondering	actie	vervolg
UC Delen 1	*Lezer* vindt het ontvangen verzoek ongeldig.	*Lezer* informeert *Uitgever* over deze uitzondering. *Uitgever* informeert daarop *Zorggebruiker* hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Delen 2	*Lezer* kan de identiteit van de *Zorggebruiker* niet vaststellen.	*Lezer* informeert *Uitgever* dat delen niet toegelaten wordt.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Delen 3	*Lezer* stelt vast dat betreffende informatie van *Persoon* bij *Zorgaanbieder* niet welkom is. Hiervan is in elk geval sprake indien hetzij: • er geen behandelrelatie is aan te wijzen als grondslag voor het delen; • *Zorggebruiker* nog geen zestien jaar oud is.		
UC Delen 4	De bevestigingsvraag wordt ontkennend beantwoord.		
UC Delen 5	*Lezer* kan het antwoord op de bevestigingsvraag niet vaststellen.	*Lezer* informeert *Uitgever* over deze uitzondering. *Uitgever* informeert daarop *Zorggebruiker* hierover.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UC Delen 6	*Uitgever* kan, zelfs na bevestiging, de gezondheidsinformatie alsnog niet plaatsen bij *Lezer*.	*Uitgever* informeert daarop *Zorggebruiker* hierover, met opgave van oorzaak.	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn

			over de uitzondering.

Perspectief van de *Zorggebruiker* (happy flow)

Toelichting

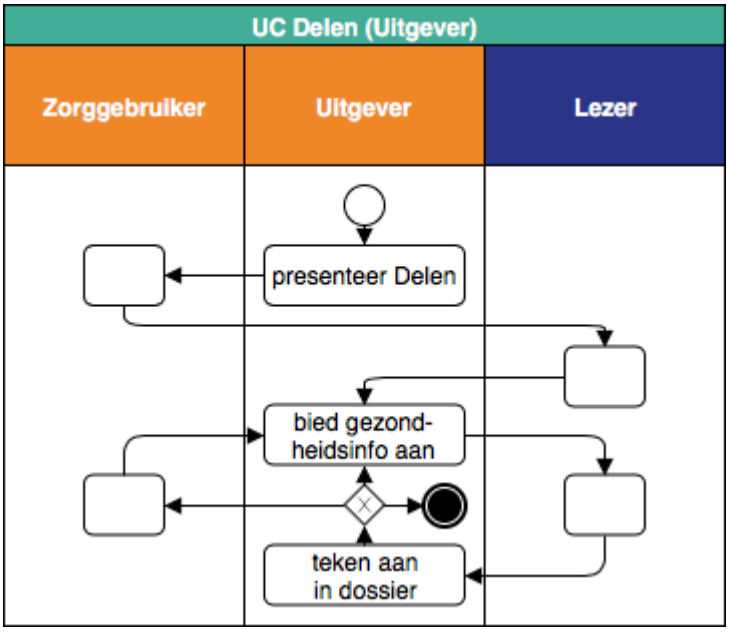
De *Zorggebruiker* moet om te beginnen drie stappen doorlopen: selectie van zorgaanbieder en informatie, inloggen en bevestigen. Eventueel kiest hij daarna voor nadere informatie om te laten plaatsen.



Perspectief van de *Uitgever* (happy flow)

Toelichting

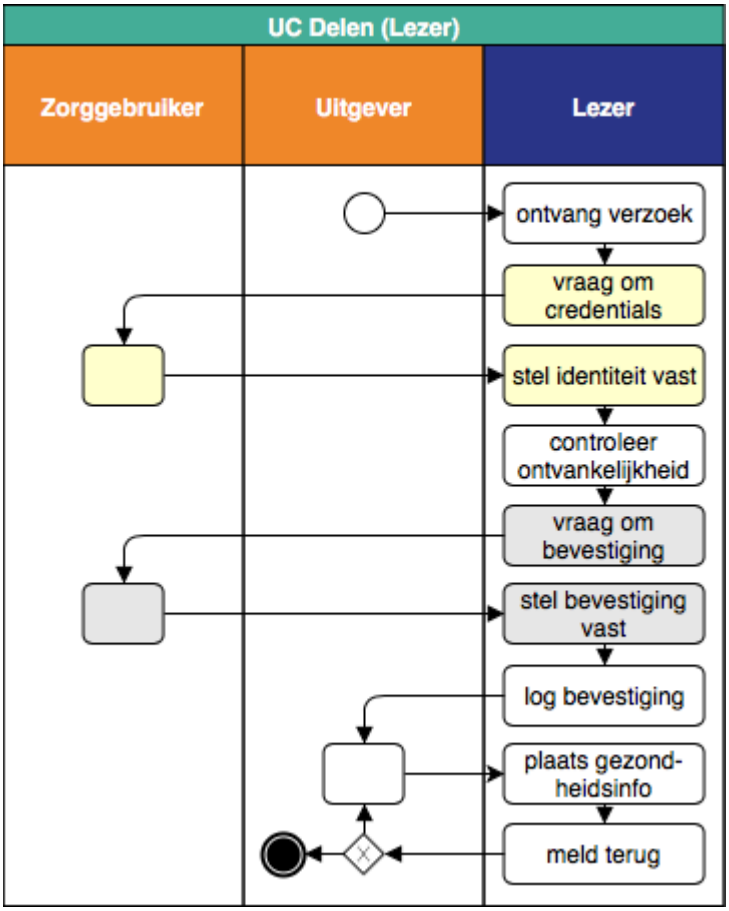
De *Uitgever* start de use case door aan de *Zorggebruiker* de mogelijkheid tot delen te presenteren. Van de *Lezer* krijgt hij na enige tijd het bericht dat de wens daartoe door Zorggebruiker is bevestigd, waarna hij de gezondheidsinformatie aanbiedt aan de *Lezer*. De reactie daarop tekent hij aan in het *Dossier*.



Perspectief van de *Lezer* (happy flow)

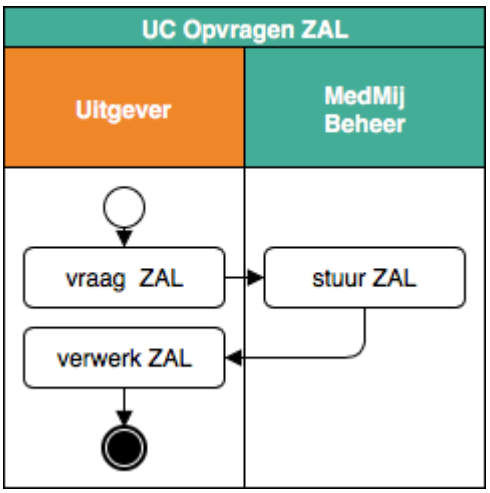
Toelichting

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 Delen (Lezer)
Zorggebruiker
Uitgever
Lezer
ontvang verzoek
vraag om credentials
stel identiteit vast
controleer ontvankelijkheid
vraag om bevestiging
stel bevestiging vast
log bevestiging
plaats gezond-heidsinfo
meld terug

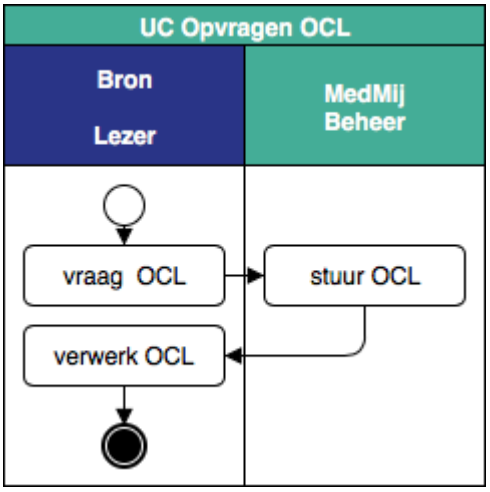
UC Opvragen ZAL

Stroomdiagram



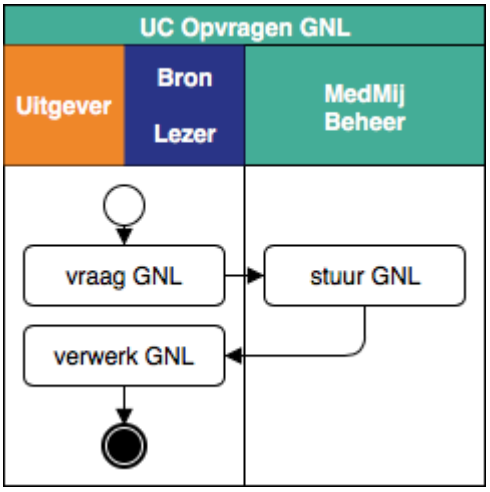
UC Opvragen OCL

Stroomdiagram

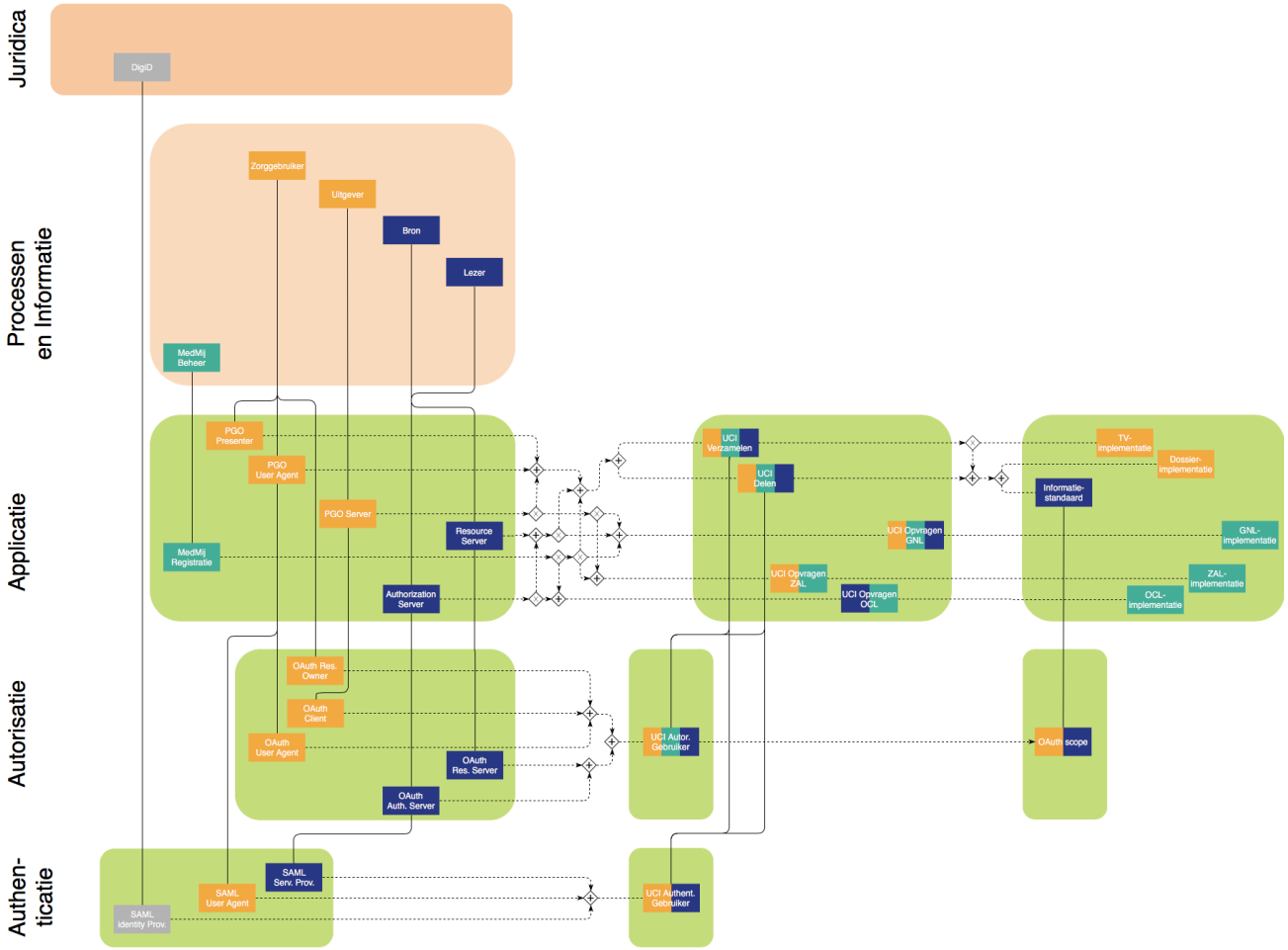


UC Opvragen GNL

Stroomdiagram



Applicatie



Toelichting

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:

- *TV* staat voor *Toestemmingsverklaring;*
- *ZAL* staat voor *Zorgaanbiederslijst;*
- *OCL* staat voor *OAuth Client List*;
- *GNL* staat voor *Gegevensdienstnamenlijst*.

Rollen

1. *Uitgever* biedt aan *Zorggebruiker,* in het kader van de toepasselijke *Dienstverleningsovereenkomst*, een geautomatiseerd systeem ter gebruik, hier genoemd: *PGO Server*.

2. *Bron* biedt, en *Lezer* biedt, een geautomatiseerde dienst, voor het namens zorgaanbieders uitwisselen van gezondheidsinformatie met *PGO Server*, bestaande uit: *Authorization Server* en *Resource Server*.
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 deze release van het MedMij Afsprakenstelsel) gebruikmaken van *DigiD* als *SAML Identity provider*, volgens het SAML 2.0 koppelvlak van DigiD, waarbij:
    1. de SAML-rol van *User Agent* wordt verzorgd door de *PGO User Agent*;
    2. de SAML-rol van *Service Provider* wordt verzorgd door de *Authorization Server*;
    3. de SAML-rol van *Identity Provider* dus wordt verzorgd door *DigiD*.
6. Ten behoeve van het autoriseren van *PGO Server* voor toegang tot *Resource Server*, in het kader van de functies *UC Verzamelen* en *UC Delen*, zullen de betrokken *PGO User Agent*, *PGO Server, Authorization Server* en *Resource Server* gebruik maken van OAuth 2.0, waarbij als grant type gebruik wordt gemaakt van Authorization Code en waarbij:
    1. de rol van *OAuth User Agent* wordt verzorgd door de *PGO User Agent*;
    2. de rol van *OAuth Client* wordt verzorgd door de *PGO Server*;
    3. de rol van *OAuth Resource Server* wordt verzorgd door de *Resource Server*;
    4. 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*,
    - ten tweede *PGO User Agent*,
    - ten derde *Authorization Server* of *Resource Server* en
    - ten vierde *MedMij Registratie*,

    met dien verstande dat:
    - in deze rollen telkens begrepen zijn de door hen eventueel verzorgde respectievelijke *OAuth*-rollen,
    - van deze rollen telkens uitgesloten zijn de door hen eventueel verzorgde respectievelijke *SAML*-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 functionele rollen vertaald naar rollen op applicatieniveau. 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 authenticatierollen 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 *SAML*-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 identificeren en 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 *SAML User Agent*. De *PGO User Agent* spreekt uiteindelijk dus ook *DigiD* aan, de *SAML Identity Provider*.

De rollen *Authorization Server* en *Resource Server* werken in het huidige MedMij-afsprakenstelsel samen in eenzelfde synchrone 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* te laten samenwerken met meerdere *Resource Servers* en om één *Resource Server* zaken te laten doen met meerdere *Authorization 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* uitstrekt, moet er in geval van gescheiden implementatie van *Authorization Server* en *Resource Server* een interface worden gerealiseerd waarin die sessiecoördinatie in stand blijft. Bovendien moet, als de relatie tussen *Authorization Server* en *Resource 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* en *Gegevensdienst* (en, respectievelijk, *Systeemrol*) maar één authorization endpoint en één token endpoint (en, respectievelijk, één resource endpoint) kan zijn. Bovendien voorkomen beperkingen op de informatie-inhoud van authorization codes en access tokens ervoor dat het interface tussen *Authorization Server* en *Resource 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 (voorziene) acceptant van de authorization code of het access token de *Authorization 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*. Dat betekent dat de interoperabiliteit tussen *Authorization Server* en *Resource Server* moet vallen onder de overeenkomst die de betreffende *Dienstverlener Zorgaanbieder* aangaat met eventuele onderaannemers, bijvoorbeeld als de *Dienstverlener Zorgaanbieder* zelf de *Resource 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*-functionaliteit..

Het is denkbaar dat een community van dienstverleners in het Zorgaanbiedersdomein tot een afsprakenstelsel komt, aanpalend aan en voldoend 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.

De standaarden OAuth 2.0 en SAML 2.0 hebben 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 dienstverlener (bij OAuth de *Authorization Provider* en bij SAML de *Service Provider*) niet onmiddellijk de gewenste informatie (bij OAuth het access token en bij SAML de gebruikersidentiteit, bij DigiD het BSN), 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.

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*. SAML-verkeer is uitgesloten, omdat het MedMij Afsprakenstelsel geen eisen kan opleggen aan DigiD. Deze afbakening is bovendien de opmaat voor artikel 8. Het daarin gemaakte onderscheid tussen frontchannel- en backchannelverkeer is nodig voor het formuleren van verantwoordelijkheden over adressering (zie Gegevens en performance in UCI Verzamelen en UCI Delen) en beveiliging (zie Netwerk). In artikel 7 moet ermee rekening gehouden worden dat er ook een use case-implementatie is op de Netwerk-laag: *UCI Opvragen WHL*.

Verantwoordelijkheden

Toelichting

De verantwoordelijkheden op deze laag en die op de processen- en informatielaag hebben een vergelijkbare opbouw. Ze zijn geordend in hoofdstukjes en secties als volgt:

- Dossier en toestemmingen
  - Use cases
  - Gegevensdiensten
  - Authenticatie
  - Autorisatie
- Lijsten
  - Zorgaanbiederslijst
  - OAuth Client List
  - Gegevensdienstnamenlijst
- Beveiliging

Van vijf van de zes use cases (zie de laag Processen en Informatie) wordt op deze (Applicatie)laag een use case-implementatie (UCI) voorgeschreven. Implementatie van de use case *Raadplegen dossier* valt buiten de scope van het MedMij Afsprakenstelsel. Het gaat om de volgende vijf:

use case-implementatie	Stroomdiagram
UCI Verzamelen	met
UCI Delen	met
UCI Opvragen ZAL	met
UCI Opvragen OCL	met
UCI Opvragen GNL	met

Dossier en toestemmingen

Use cases

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 synchroon 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 synchroon uitgevoerd.

Toelichting

In deze release van het MedMij Afsprakenstelsel zijn de use cases *UC Verzamelen* (eenmalige verzameling) en *UC Delen* (eenmalig delen) de enige waarin gezondheidsinformatie wordt gedeeld. Omdat de verzameling en deling eenmalig zijn, kunnen autorisatie en authenticatie nog verweven zijn in de betreffende flows. De gebruikersbeleving wordt het best bediend door de gehele procesgang synchroon te houden.

Gegevensdiensten

2. Als een *Uitgever* een zekere *Gegevensdienst* aanbiedt aan zijn *Zorggebruikers* en daartoe afneemt bij 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.

Authenticatie

3. Tijdens de use case-implementaties *UCI Verzamelen* en *UCI Delen* laat de *Authorization Server,* ten behoeve van zijn rol in deze use case-implementaties, en in zijn SAML-rol als *Service Provider*, onmiddellijk na de start van de OAuth-flow en voordat hij de *Zorggebruiker* om OAuth-autorisatie vraagt, de *Zorggebruiker* authenticeren door DigiD, volgens het SAML 2.0 koppelvlak van DigiD.

Toelichting

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. Uit het Juridisch kader volgt vooralsnog gebruik van DigiD voor dit doel.

Autorisatie

4. Tijdens de use case-implementaties *UCI Verzamelen* en *UCI Delen* zet de *Authorization Server*, onmiddellijk na de authenticatie van de *Zorggebruiker* zoals bedoeld onder 3, de OAuth-autorisatie voort, volgens de standaard OAuth 2.0.

Toelichting

Conform wettelijke verplichting geeft *Zorggebruiker*, in de *UC Verzamelen*, 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.

5. 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.

6. 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.

7. De *OAuth Client* en *OAuth Resource Server* zullen slechts tokens van het type Bearer Token uitwisselen, conform RFC6750. De OAuth Client gebruikt voor het sturen van het acces token de methode `Authorization Request Header Field`, zoals beschreven in sectie 2.1 van 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 verantwoordelijkheden 26, 27 en 28.

Het MedMij Afsprakenstelsel kiest voor de methode `Authorization Request Header Field` omdat die de beste beveiliging biedt.

8. 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 bepaald is door de op te vragen *Gegevensdienst*.

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 opvraging.

9. 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 (zie onder verantwoordelijkheid 26). Bovendien wordt de hele flow van *Verzamelen* synchroon 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.

10a. 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.

10b. 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 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 naam van het token-formaat;
- een digitale handtekening.

10c. Geen andere informatie dan de in verantwoordelijkheid 10b genoemde mag voorkomen in de authorization code of het acces 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.

10d. Met betrekking tot zowel authorization codes als access tokens, draagt de *OAuth Authorization Server* ervoor zorg dat nooit twee dezelfde geldige door haar uitgebrachte daarvan in omloop zijn.

Toelichting

Dit is een maatregel tegen beveiligingsrisico 4.4.1.3 uit RFC 6819 (zie onder verantwoordelijkheid 26). 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 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 corrumpering, in het *Persoonsdomein*, van de authorization code of het access token waarbij het verloopmoment verlaat zou worden, toch niet kan leiden 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 corrumpering kan het verloopmoment ook vervroegen, maar richt dan weinig schade aan. Overigens kan in de huidige 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.

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*, *Zorgaanbieder*, *Gegevensdienst* of *Systeemrol* en
- 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 acces token, via de *OAuth Client*.

11. 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 4.4.1 uit RFC 6819 (zie onder verantwoordelijkheid 26). 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.

12. De *OAuth Authorization Server* draagt alleen een access token over aan een *OAuth Client* als de daartoe aangeboden authorization code aan diezelfde *OAuth Client* is afgegeven.

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 onder verantwoordelijkheid 26). Hiervoor moet de *Authorization Server* dus bijhouden aan welke *Clients* hij de authorization codes uitdeelt. Dit betekent dat het access token alleen mag worden uitgereikt via een redirect URI waarbij de hostname gelijk is aan de hostname van de *OAuth Client* voor wie de bijbehorende authorization code bedoeld was.

13. De *OAuth Client* en *OAuth Authorization Server* gebruiken voor al hun onderlinge verkeer PKIoverheid-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 (zie onder verantwoordelijkheid 26). 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.

14. De *OAuth Client* biedt, al dan niet via de *OAuth User Agent*, aan de *OAuth Authorization Servers* slechts redirect URI's aan die volledig (full) zijn én verwijzen naar een `https`-beschermd endpoint. *OAuth Authorization Servers* redirecten niet naar een URI die niet aan deze eisen voldoet.

Toelichting

Dit is een maatregel tegen beveiligingsrisico's 4.1.5, 4.2.4, 4.4.1.1, 4.4.1.5 en 4.4.1.6 in RFC 6819 (zie onder verantwoordelijkheid 26). Zie bovendien de toelichting onder verantwoordelijkheid 12.

15. 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, blijven nog steeds mogelijk, maar daarvan zal worden gevraagd dat zij al het verkeer van OAuth client credentials in de achtergrond op een server zullen afhandelen, niet op het user device.

Lijsten

Zorgaanbiederslijst

16. *MedMij Registratie* en elke *PGO Server* implementeren de use case *UC Opvragen ZAL* met de use case-implementatie *UCI Opvragen ZAL*. Zij gebruiken hiertoe het betreffende stroomdiagram.

17. *PGO Server* betrekt minstens elke vijftien minuten (900 seconden) de meest recente *ZAL-implementatie* van *MedMij Registratie*.

18. *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.

OAuth Client List

19. *MedMij Registratie* en *Authorization Server* implementeren de use case *UC Opvragen OCL* met de use case-implementatie *UCI Opvragen OCL*. Zij gebruiken hiervoor het betreffende stroomdiagram.

20. *Authorization Server* betrekt minstens elke vijftien minuten (900 seconden) de meest recente *OCL-implementatie* van *MedMij Registratie*.

21. *Authorization Server* valideert elke nieuwe verkregen *OCL-implementatie* tegen het XML-schema van de *OAuth Client List*. Dit XML-schema is een technische implementatie van het MedMij-metamodel.

Gegevensdienstnamenlijst

22. *MedMij Registratie*, *PGO Server en Authorization Server* implementeren de use case *UC Opvragen GNL* met de use case-implementatie *UCI Opvragen GNL*. Zij gebruiken hiervoor het betreffende stroomdiagram.

23. *PGO Server* betrekt minstens elke vijftien minuten (900 seconden) de meest recente *GNL-implementatie* van *MedMij Registratie*.

24. *PGO Server* valideert elke nieuwe verkregen *GNL-implementatie* tegen het XML-schema van de GNL. Dit XML-schema is een technische implementatie van het MedMij-metamodel.

Beveiliging

25. In het gegevensverkeer dat zich voltrekt in het kader van *UCI Verzamelen*, *UCI Delen*, *UCI Opvragen ZAL*, *UCI Opvragen OCL* en *UCI Opvragen GNL*, maken deze gebruik van de functies *Versleuteling*, *Server Authentication* en *Server Authorization*, volgens het bepaalde op de Netwerk-laag.

26. 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 the redirect URI used to deliver the access token.	5.3.5	4.4.1.8
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

27. De *PGO Server* realiseert de volgende beveiligingsmaatregelen, conform RFC6819:

beveiligingsmaatregel	paragraaf in RFC6819	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

28. De *OAuth Authorization Server* realiseert de volgende beveiligingsmaatregelen, conform RFC6819:

beveiligingsmaatregel	paragraaf in RFC6819	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 26,27 en 28 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 7 op deze laag.

In hoofdstuk 4 van RFC 6819 staat een uitgebreide lijst van beveiligingsrisico's. Niet van toepassing zijn, voor de huidige release van het afsprakenstelsel:

- bedreiging 4.1.1: Obtaining Client Secrets, omdat authenticatie van OAuth Clients in MedMij werkt op basis van PKI-servercertificaten, niet op basis van client secrets;
- 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 4.4.1.1: 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. Deze betreffen bijvoorbeeld het gebruik van TLS (Netwerk-laag) en Digid (Applicatie-laag) en het beperken van de scope en de geldigheidsduur van authorization codes en access tokens (Applicatie-laag);
- 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*.

Met bovenstaande verantwoordelijkheden 26, 27 en 28 is die laatste groep van maatregelen ook onderdeel van het MedMij Afsprakenstelsel.

29. *OAuth Clients*, *Authorization Server* en *OAuth Resource Server* implementeren de op deze respectievelijke rollen toepasselijke beveiligingsmaatregelen, volgens paragaaf 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.

UCI Verzamelen

Toelichting

In de platen hieronder staat het stroomdiagram van de use case-implementatie *Verzamelen*, in vier perspectieven:

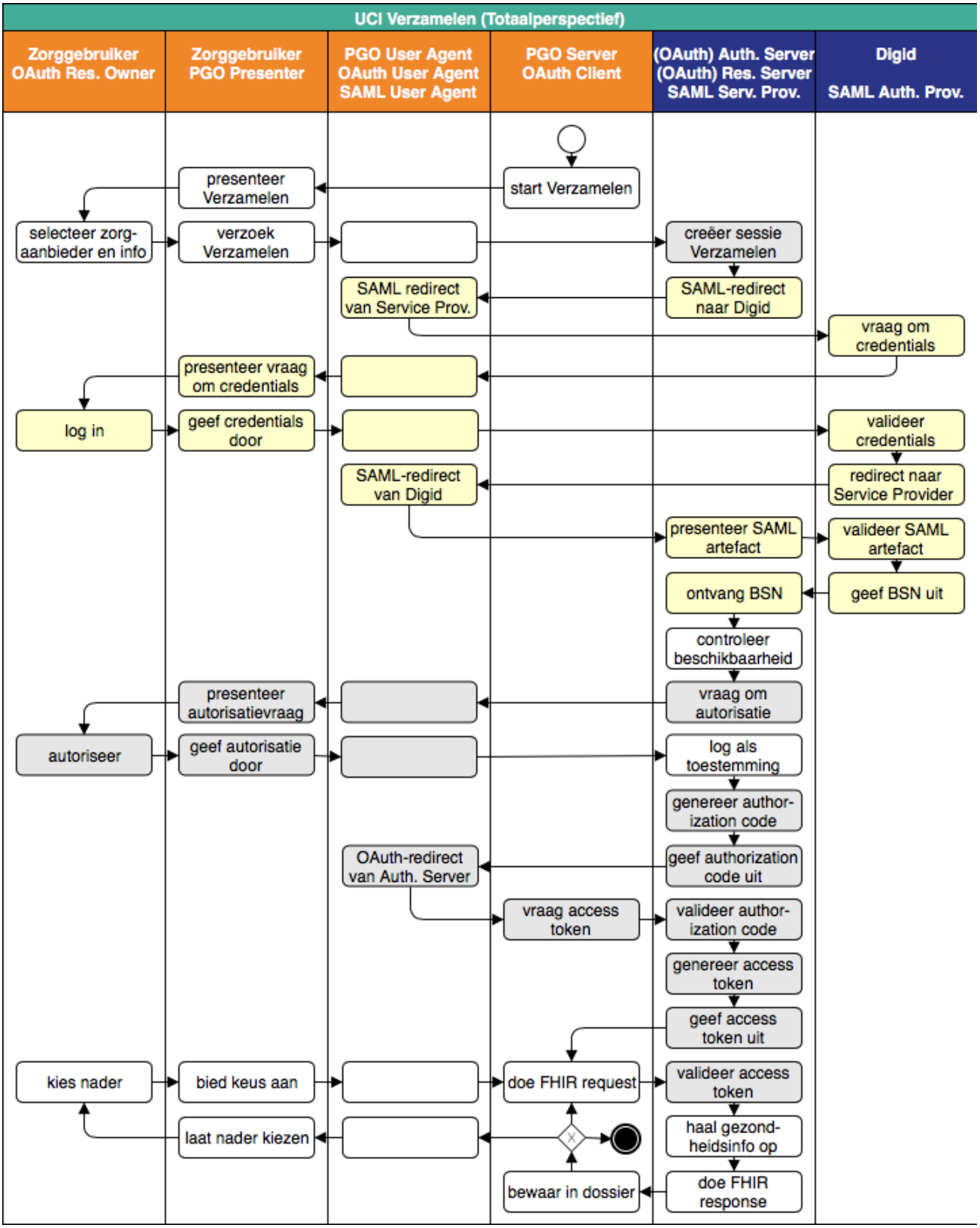
- het totaalperspectief, met zowel de happy flow als de uitzonderingen;
- het perspectief van de *PGO Server* (= *OAuth Client*), die onder de hoede van de *Dienstverlener Persoon* valt. Voor zover laatstgenoemde deelnemer is in het MedMij Afsprakenstelsel, kan deze dus deze plaat lezen als zijn verplichte aandeel in de use case-implementatie *Verzamelen;*
- het perspectief van de (*OAuth) Authorization Server/*(*OAuth) Resource Server/ SAML Service Provider*, die onder de hoede van de *Dienstverlener Zorgaanbieder* valt. Voor zover laatstgenoemde deelnemer is in het MedMij Afsprakenstelsel, kan deze dus 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 volgens DigiD/SAML. 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 de gegevens die omgaan in deze use case-implementatie zijn, samen met die van UCI Delen, opgenomen in een aparte pagina.

Totaalperspectief

Happy flow


UCI Verzamelen (Totaalperspectief)
Zorggebruiker OAuth Res. Owner
Zorggebruiker PGO Presenter
PGO User Agent OAuth User Agent SAML User Agent
PGO Server OAuth Client
(OAuth) Auth. Server (OAuth) Res. Server SAML Serv. Prov.
Digid SAML Auth. Prov.
start Verzamelen
presenteer Verzamelen
selecteer zorg-aanbieder en info
verzoek Verzamelen
creëer sessie Verzamelen
SAML-redirect naar Digid
SAML redirect van Service Prov.
vraag om credentials
presenteer vraag om credentials
log in
geef credentials door
valideer credentials
redirect naar Service Provider
SAML-redirect van Digid
presenteer SAML artefact
valideer SAML artefact
geef BSN uit
ontvang BSN
controleer beschikbaarheid
presenteer autorisatievraag
vraag om autorisatie
autoriseer
geef autorisatie door
log als toestemming
genereer author-ization code
OAuth-redirect van Auth. Server
geef authorization code uit
vraag access token
valideer author-ization code
genereer access token
geef access token uit
kies nader
bied keus aan
doe FHIR request
valideer access token
laat nader kiezen
haal gezond-heidsinfo op
bewaar in dossier
doe FHIR response

Toelichting

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* voor een *Zorgaanbieder* beschikbaar zijn. Desgewenst worden de *Gegevensdienstnamen* uit de *Gegevensdienstnamenlijst* gebruikt.
2. De *Zorggebruiker* maakt expliciet zijn selectie en laat de *OAuth User Agent* een verzamel-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 *SAML Service Provider*) de SAML-flow door de browser naar *DigiD* te redirecten, onder meegeven van een redirect URI, die aangeeft waarnaartoe *DigiD* straks de *OAuth User Agent* moet terugsturen, na het inloggen van de *Zorggebruiker*.
5. DigiD vraagt van de *Zorggebruiker* via zijn *PGO Presenter* om inloggegevens.
6. Wanneer deze juist zijn, redirect *DigiD* de *OAuth User Agent* terug naar de *Authorization Server*, onder meegeven van een ophaalbewijs: het SAML-artefact.
7. Met dit ophaalbewijs haalt de *Authorization Server* rechtstreeks bij *DigiD* het BSN op.
8. De *Authorization Server* controleert alvast of de *Zorgaanbieder* voor de betreffende *Gegevensdienst* überhaupt gezondheidsinformatie van die *Persoon* beschikbaar heeft. 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 autorisatievraag.
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. 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 en verstuurt ze in een FHIR-response naar de *PGO Server*.
16. Deze bewaart de ontvangen gezondheidsinformatie in het persoonlijke dossier. Mocht de *Gegevensdienst* waartoe de *Zorggebruiker* heeft geautoriseerd uit meerdere *Transacties* bestaan, bevraagt de *PGO Server* de *Resource Server* daarna mogelijk opnieuw voor de nog resterende *Transacties* , eventueel na nieuwe gebruikersinteractie. Zolang het access token geldig is, kan dat.

Bij de implementatie van de toets 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 beschikbaarheidstoets 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.

Uitzonderingen

Toelichting

In onderstaande tabel staan de uitzonderingssituaties beschreven. Zij kunnen gezien worden als de implementatie-tegenhangers van de uitzonderingen van de use case Verzamelen. Alle uitzonderingen worden door de *Authorization Server* of de *Resource 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.

Nummer	Implementeert uitzondering	Uitzondering	Actie	Melding	Vervolg
UCI Verzamelen 1	UC Verzamelen 1	*Authorization Server* vindt het ontvangen verzoek ongeldig.	*Authorization Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert *Zorggebruiker* daarover.	conform OAuth 2.0-specificatie, par. 4.1.2.1, error code `invalid_request`, met in de error description de oorzaak	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UCI Verzamelen 2	UC Verzamelen 2	*Authorization Server* kan de identiteit van de *Zorggebruiker* niet vaststellen.	*Authorization Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert *Zorggebruiker* dat diens verzoek geen voortgang kan vinden, maar laat de oorzaak daarvan helemaal in het midden.	conform OAuth 2.0-specificatie, par. 4.1.2.1, error code `access denied`, met in de error description "`Access denied.`"	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UCI Verzamelen 3	UC Verzamelen 3	*Authorization Server* stelt vast dat van *Persoon* bij *Zorgaanbieder* geen gezondheidsinformatie voor die *Gegevensdienst* beschikbaar is.			
UCI Verzamelen 4	UC Verzamelen 4	De autorisatievraag wordt ontkennend beantwoord.			
UCI Verzamelen 5	UC Verzamelen 5	*Authorization Server* kan de autorisatie niet vaststellen.	*Authorization Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert daarop *Zorggebruiker* hierover.	conform OAuth 2.0-specificatie, par. 4.1.2.1, error code `access denied`, met in de error description "`Authorization failed.`"	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.

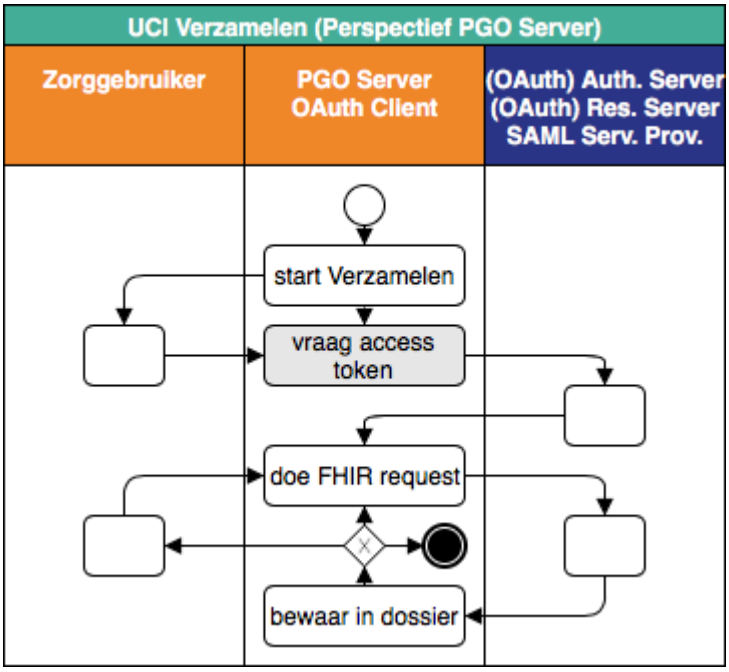
UCI Verzamelen 6	UC Verzamelen 6	De validatie van de authorization code door *Authorization Server* faalt.	*Authorization Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert daarop *Zorggebruiker* hierover.	conform OAuth 2.0-specificatie, par. 5.2, error code `invalid_grant`	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UCI Verzamelen 7	UC Verzamelen 6	De validatie van het access token door *Resource Server* faalt.	*Resource Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert daarop *Zorggebruiker* hierover.	conform FHIR-specificatie, in de FHIR-response, issue type security/suppressed	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UCI Verzamelen 8	UC Verzamelen 5	*Resource Server* kan de gevraagde informatie niet of niet tijdig ophalen bij achterliggende systemen.	*Resource Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert daarop *Zorggebruiker* hierover.	conform FHIR-specificatie, in de FHIR-response, issue type processing/incomplete	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.

Specifieke perspectieven

Perspectief PGO Server (happy flow)

Toelichting

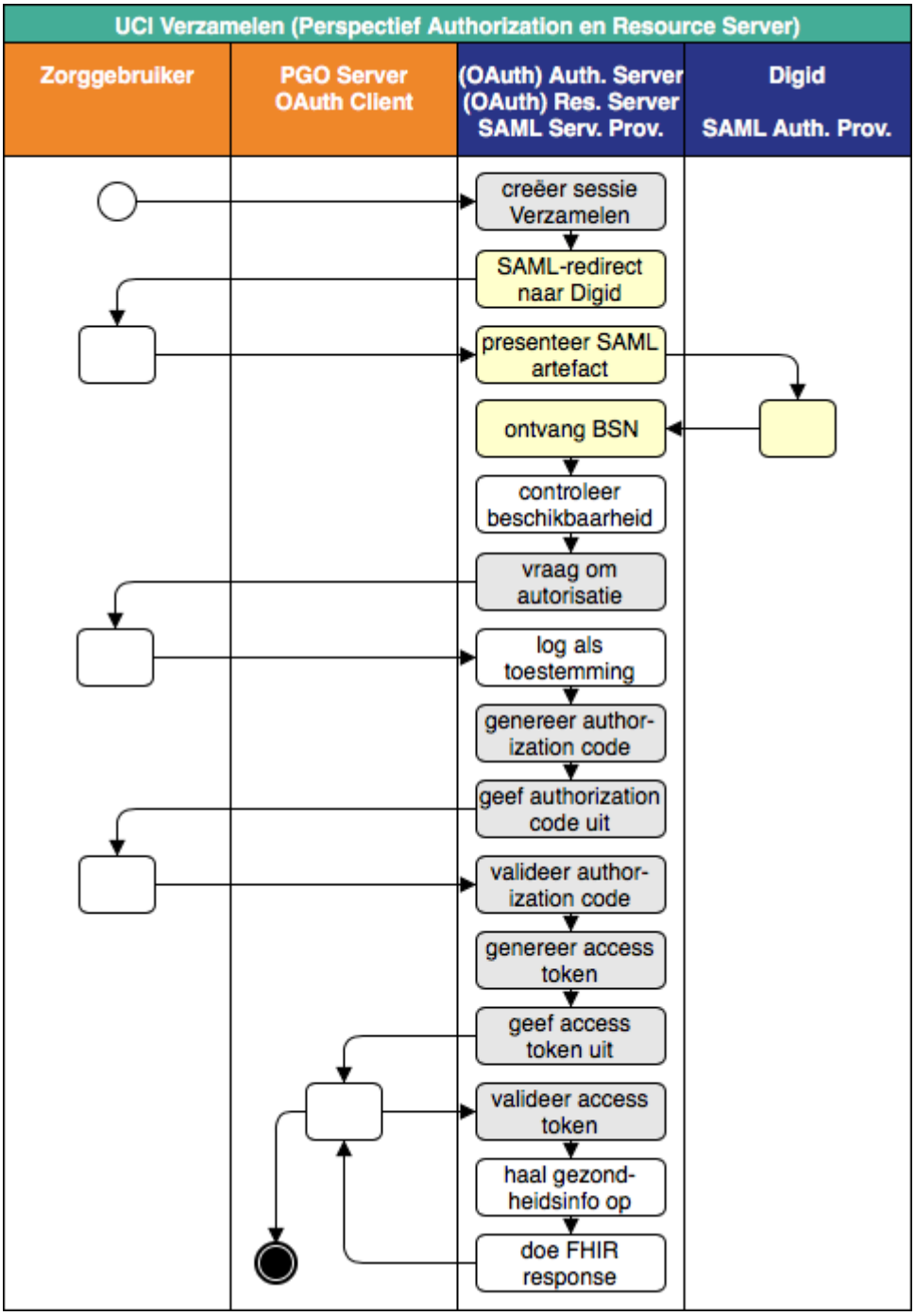
Hieronder staat hetzelfde stroomdiagram, maar vanuit het perspectief van de *PGO Server*. Dat wil zeggen dat alle tussenliggende stappen die niet zichtbaar zijn voor de *PGO Server*, kortgesloten zijn. *Zorggebruiker* is "verborgen achter de browser" en *DigiD* "achter de *Authorization Server*".



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".

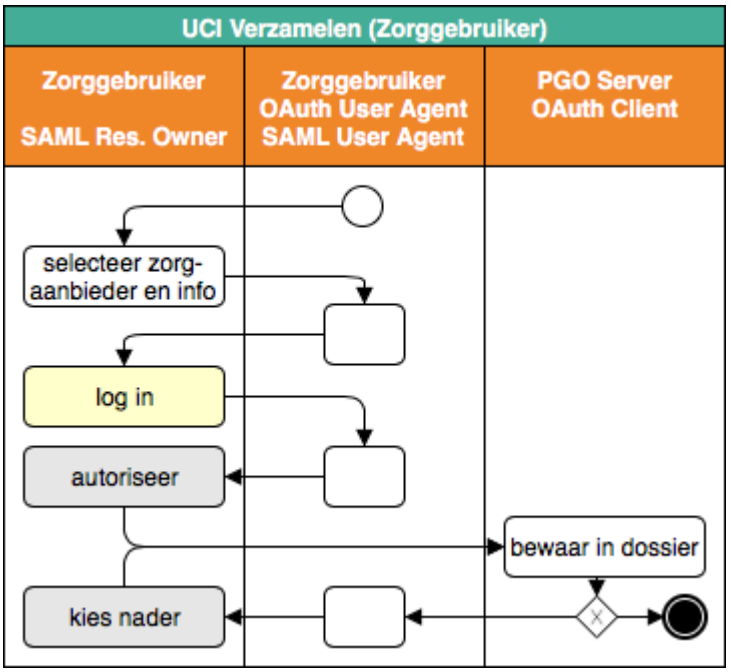


Perspectief Zorggebruiker (happy flow)

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*

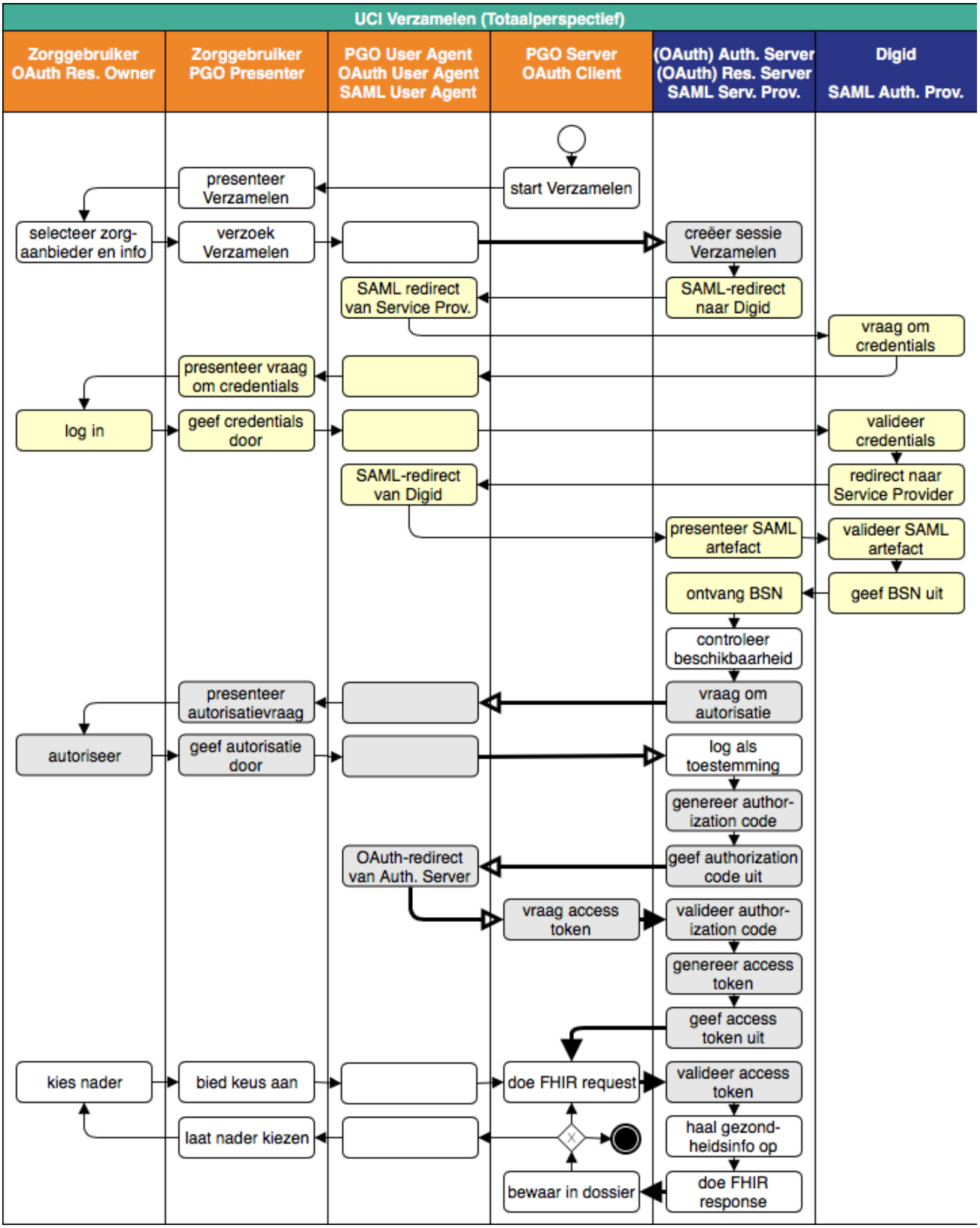
Server zichtbaar gehouden, omdat het bewaren van de verzamelde gezondheidsinformatie betekenis heeft voor de *Zorggebruiker*. Waarschijnlijk zal de *PGO Server* de *Zorggebruiker* laten weten dat het verzamelen geslaagd is, maar dat is niet verplicht.



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 Verzamelen (Totaalperspectief)
Zorggebruiker OAuth Res. Owner
Zorggebruiker PGO Presenter
PGO User Agent OAuth User Agent SAML User Agent
PGO Server OAuth Client
(OAuth) Auth. Server (OAuth) Res. Server SAML Serv. Prov.
Digid SAML Auth. Prov.
start Verzamelen
presenteer Verzamelen
selecteer zorg-aanbieder en info
verzoek Verzamelen
creëer sessie Verzamelen
SAML redirect van Service Prov.
SAML-redirect naar Digid
vraag om credentials
presenteer vraag om credentials
log in
geef credentials door
valideer credentials
SAML-redirect van Digid
redirect naar Service Provider
presenteer SAML artefact
valideer SAML artefact
ontvang BSN
geef BSN uit
controleer beschikbaarheid
presenteer autorisatievraag
vraag om autorisatie
autoriseer
geef autorisatie door
log als toestemming
genereer author-ization code
OAuth-redirect van Auth. Server
geef authorization code uit
vraag access token
valideer author-ization code
genereer access token
geef access token uit
kies nader
bied keus aan
doe FHIR request
valideer access token
laat nader kiezen
haal gezond-heidsinfo op
bewaar in dossier
doe FHIR response

UCI Delen

Toelichting

In de platen hieronder staat het stroomdiagram van de use case-implementatie *Delen*, in vier perspectieven:

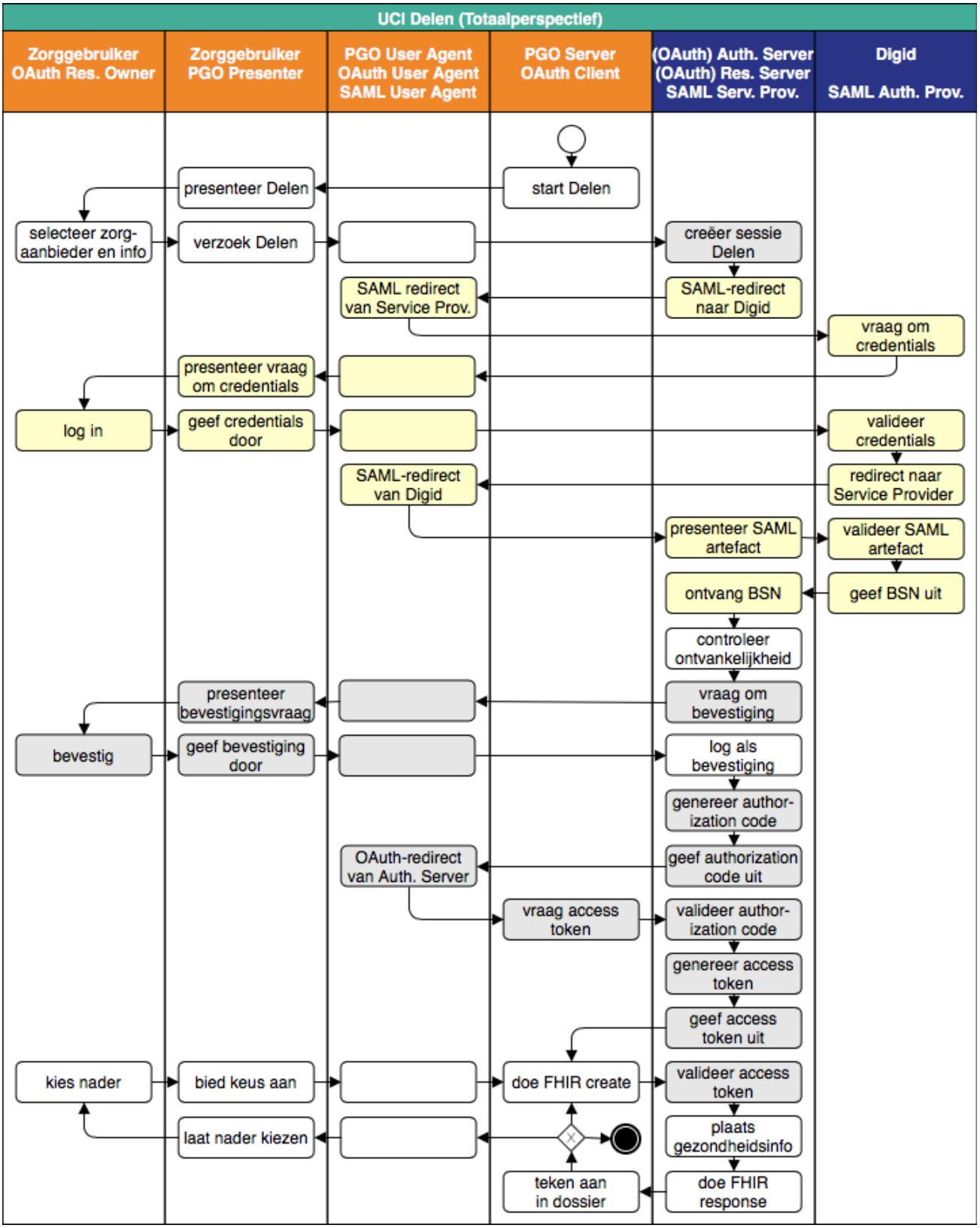
- het totaalperspectief, met zowel de happy flow als de uitzonderingen;
- het perspectief van de *PGO Server* (= *OAuth Client*), die onder de hoede van de *Dienstverlener Persoon* valt. Voor zover laatstgenoemde deelnemer is in het MedMij Afsprakenstelsel, kan deze dus deze plaat lezen als zijn verplichte aandeel in de use case-implementatie *Delen;*
- het perspectief van de (*OAuth) Authorization Server/*(*OAuth) Resource Server/ SAML Service Provider*, die onder de hoede van de *Dienstverlener Zorgaanbieder* valt. Voor zover laatstgenoemde deelnemer is in het MedMij Afsprakenstelsel, kan deze dus 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 volgens DigiD/SAML. 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 de gegevens die omgaan in deze use case-implementatie zijn, samen met die van UCI Verzamelen , opgenomen in een aparte pagina .

Totaalperspectief

Happy flow



Toelichting

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* met een *Zorgaanbieder* beschikbaar zijn. 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 *SAML Service Provider*) de SAML-flow door de *OAuth User Agent* naar *DigiD* te redirecten, onder meegeven van een redirect URI, die aangeeft waarnaartoe *DigiD* straks de *OAuth User Agent* moet terugsturen, na het inloggen van de *Zorggebruiker*.
5. DigiD vraagt van de *Zorggebruiker* via zijn *PGO Presenter* om inloggegevens.
6. Wanneer deze juist zijn, redirect *DigiD* de *OAuth User Agent* terug naar de *Authorization Server*, onder meegeven van een ophaalbewijs: het SAML-artefact.
7. Met dit ophaalbewijs haalt de *Authorization Server* rechtstreeks bij *DigiD* het BSN op.
8. De *Authorization Server* controleert alvast of de *Zorgaanbieder* voor de betreffende *Gegevensdienst* überhaupt ontvankelijk is voor gezondheidsinformatie van die *Persoon* . 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 en stuurt deze naar de *PGO Server*.
14. Nu is de *PGO Server* gereed om de gezondheidsinformatie aan de *Resource Server* aan te bieden. 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, plaatst de *PGO Server* daarna mogelijk opnieuw bij de *Resource Server* voor de nog resterende *Transacties* , eventueel na nieuwe gebruikersinteractie. Zolang het access token geldig is, kan dat.

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.

Uitzonderingen

Toelichting

In onderstaande tabel staan de uitzonderingssituaties beschreven. Zij kunnen gezien worden als de implementatie-tegenhangers van de uitzonderingen van de use case Delen. Alle uitzonderingen worden door de *Authorization Server* of de *Resource 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.

Nummer	Implementeert uitzondering	Uitzondering	Actie	Melding	Vervolg
UCI Delen 1	UC Delen 1	*Authorization Server* vindt het ontvangen verzoek ongeldig.	*Authorization Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert *Zorggebruiker* daarover.	conform OAuth 2.0-specificatie, par. 4.1.2.1, error code `invalid_request`, met in de error description de oorzaak	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UCI Delen 2	UC Delen 2	*Authorization Server* kan de identiteit van de *Zorggebruiker* niet vaststellen.	*Authorization Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert daarop *Zorggebruiker* hierover.	conform OAuth 2.0-specificatie, par. 4.1.2.1, error code `access denied`, met in de error description "`Access denied.`"	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UCI Delen 3	UC Delen 3	*Authorization Server* stelt vast dat *Zorgaanbieder* inzake deze *Gegevensdienst* niet ontvankelijk is voor gezondheidsinformatie van *Persoon*.			
UCI Delen 4	UC Delen 4	De bevestigingvraag wordt ontkennend beantwoord.			
UCI Delen 5	UC Delen 5	*Authorization Server* kan de autorisatie niet vaststellen.	*Authorization Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert daarop *Zorggebruiker* hierover.	conform OAuth 2.0-specificatie, par. 4.1.2.1, error code `access denied`, met in de error description "`Authorization failed.`"	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UCI Delen 6	UC Delen 6	De validatie van de authorization code door *Authorization Server* faalt.	*Authorization Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert daarop *Zorggebruiker* hierover.	conform OAuth 2.0-specificatie, par. 5.2, error code `invalid_grant`	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.

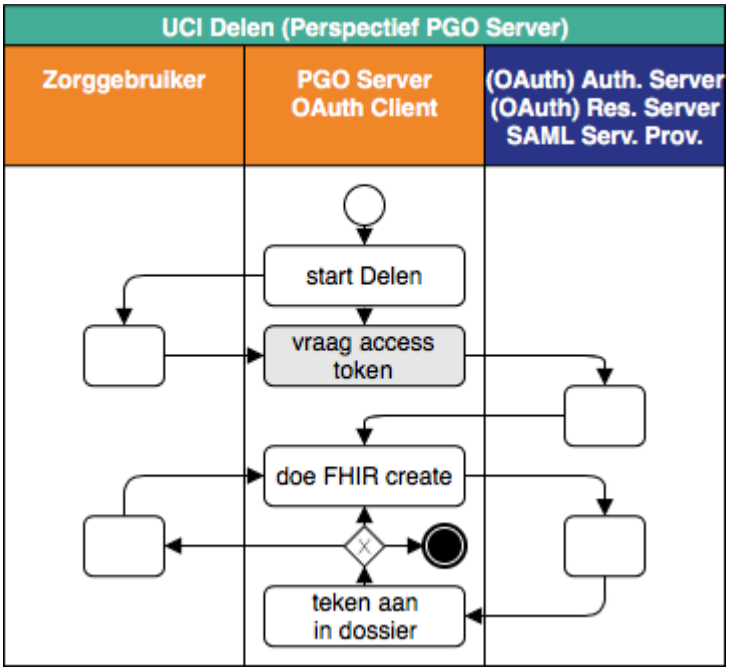
UCI Delen 7	UC Delen 6	De validatie van het access token door *Resource Server* faalt.	*Resource Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert daarop *Zorggebruiker* hierover.	conform FHIR-specificatie, in de FHIR-response, issue type security/suppressed	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.
UCI Delen 8	UC Delen 5	*Resource Server* kan de gevraagde informatie niet of niet tijdig plaatsen bij achterliggende systemen.	*Resource Server* informeert *PGO Server* over deze uitzondering. *PGO Server* informeert daarop *Zorggebruiker* hierover.	conform FHIR-specificatie, in de FHIR-response, issue type processing/incomplete	Allen stoppen de flow onmiddellijk na geïnformeerd te zijn over de uitzondering.

Specifieke perspectieven

Perspectief PGO Server (happy flow)

Toelichting

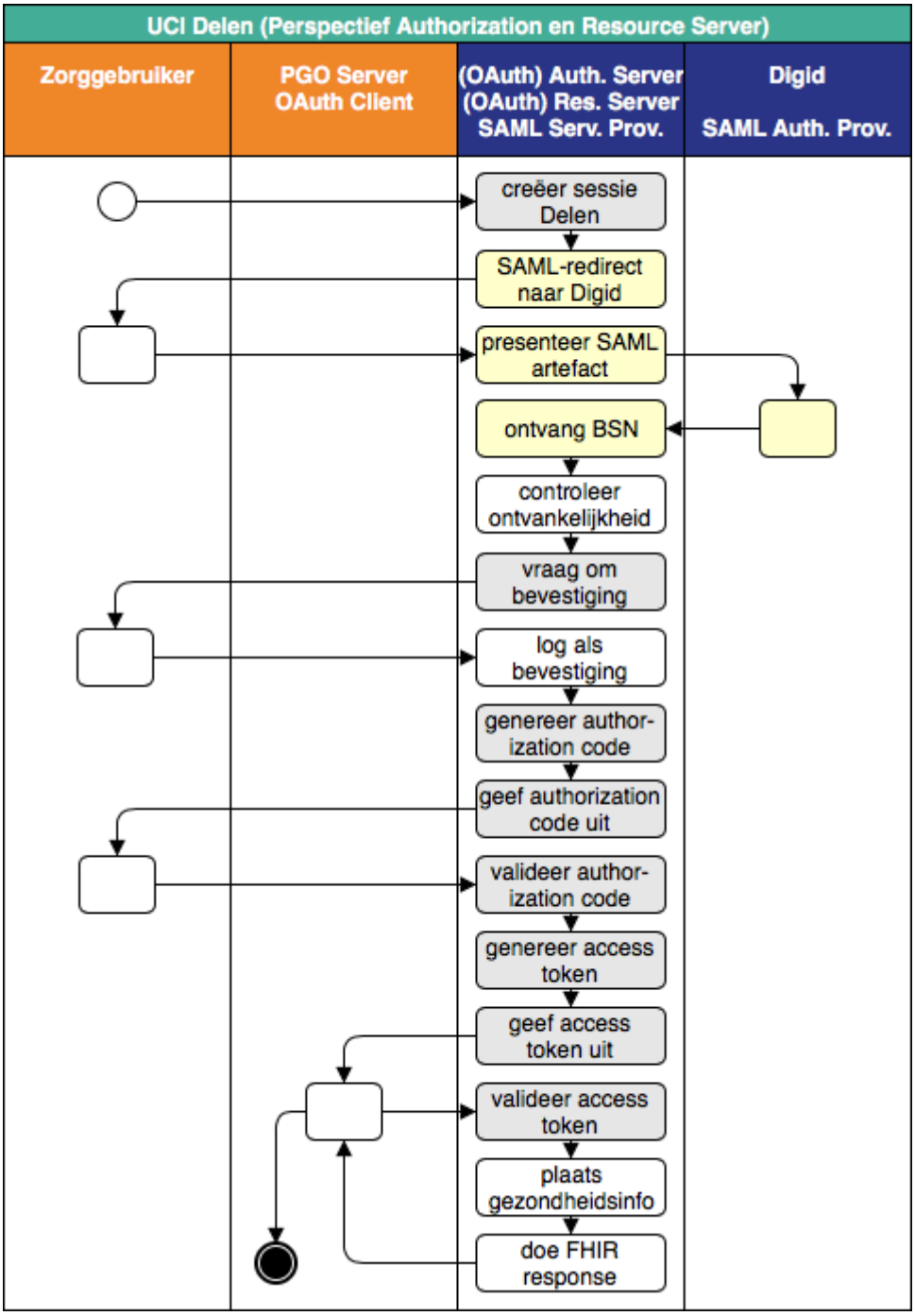
Hieronder staat hetzelfde stroomdiagram, maar vanuit het perspectief van de *PGO Server*. Dat wil zeggen dat alle tussenliggende stappen die niet zichtbaar zijn voor de *PGO Server*, kortgesloten zijn. *Zorggebruiker* is "verborgen achter de browser" en *DigiD* "achter de *Authorization Server*".



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".

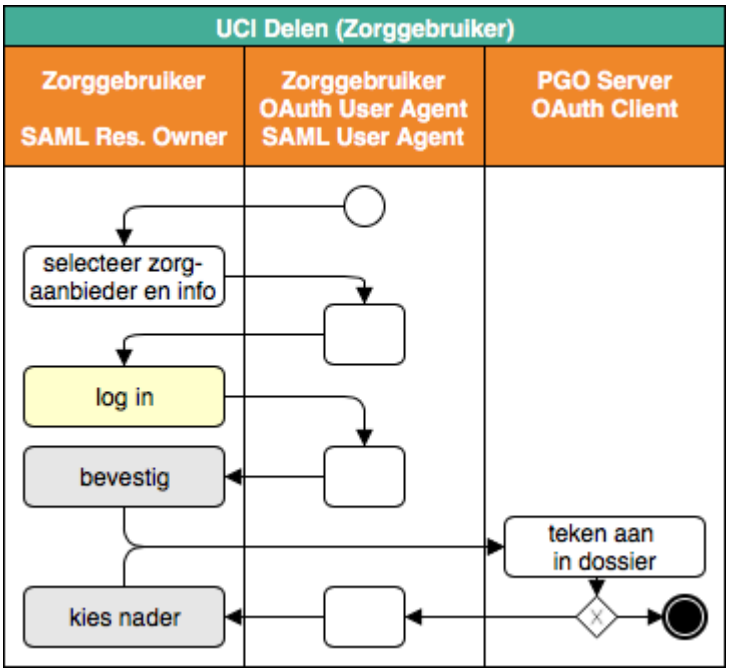


Perspectief Zorggebruiker (happy flow)

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*

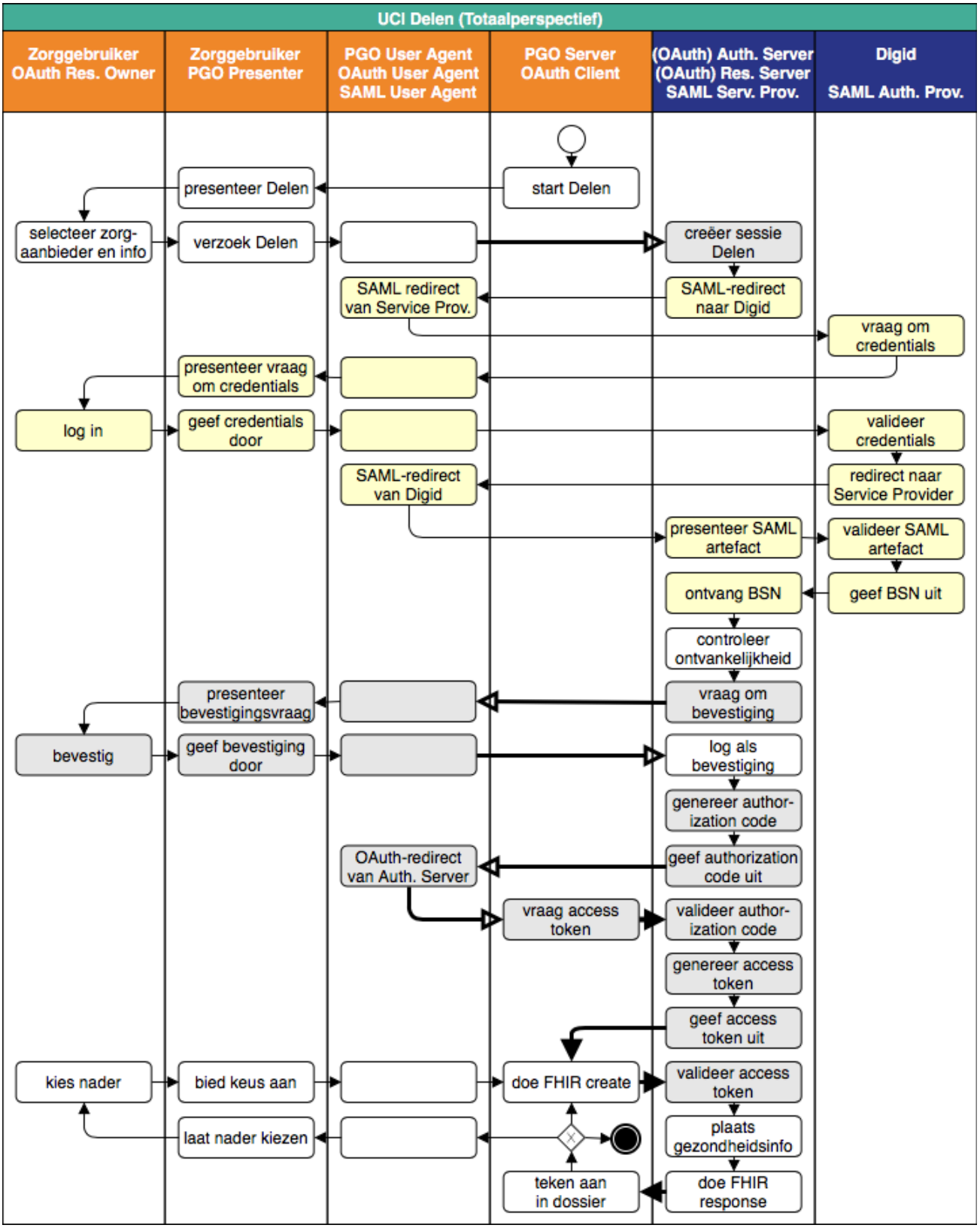
Server zichtbaar gehouden, omdat het markeren van de gedeelde gezondheidsinformatie betekenis heeft voor de *Zorggebruiker*. Waarschijnlijk zal de *PGO Server* de *Zorggebruiker* laten weten dat het delen geslaagd is, maar dat is niet verplicht.



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.

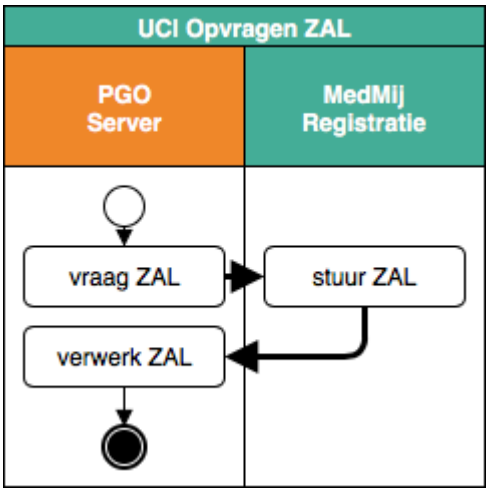

UCI Delen (Totaalperspectief)
Zorggebruiker OAuth Res. Owner
Zorggebruiker PGO Presenter
PGO User Agent OAuth User Agent SAML User Agent
PGO Server OAuth Client
(OAuth) Auth. Server (OAuth) Res. Server SAML Serv. Prov.
Digid SAML Auth. Prov.
start Delen
presenteer Delen
selecteer zorg-aanbieder en info
verzoek Delen
creëer sessie Delen
SAML redirect van Service Prov.
SAML-redirect naar Digid
vraag om credentials
presenteer vraag om credentials
log in
geef credentials door
valideer credentials
SAML-redirect van Digid
redirect naar Service Provider
presenteer SAML artefact
valideer SAML artefact
ontvang BSN
geef BSN uit
controleer ontvankelijkheid
presenteer bevestigingsvraag
vraag om bevestiging
bevestig
geef bevestiging door
log als bevestiging
genereer author-ization code
OAuth-redirect van Auth. Server
geef authorization code uit
vraag access token
valideer author-ization code
genereer access token
geef access token uit
kies nader
bied keus aan
doe FHIR create
valideer access token
laat nader kiezen
plaats gezondheidsinfo
teken aan in dossier
doe FHIR response

UCI Opvragen ZAL

Stroomdiagram

Toelichting

Beide interacties met *MedMij Registratie* zijn backchannel-verkeer.

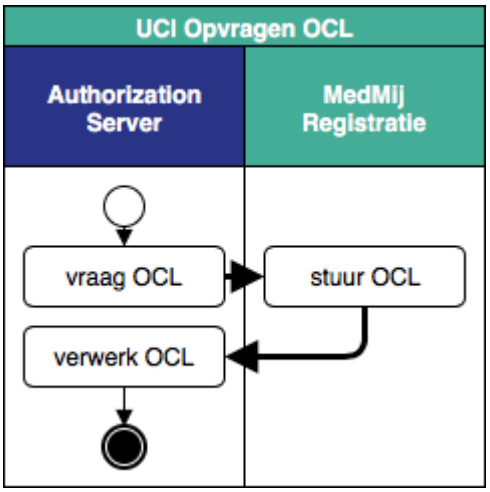


UCI Opvragen OCL

Stroomdiagram

Toelichting

Beide interacties met *MedMij Registratie* zijn backchannel-verkeer.

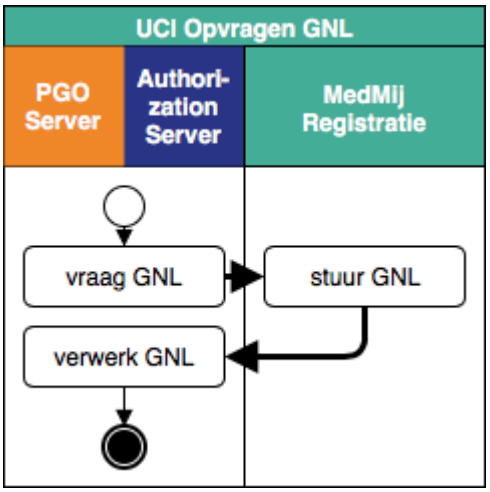


UCI Opvragen GNL

Stroomdiagram

Toelichting

Beide interacties met *MedMij Registratie* zijn backchannel-verkeer.



Gegevens en performance in UCI Verzamelen en UCI Delen

Toelichting

De UCI Verzamelen en UCI Delen zijn analoog van opzet. Voor de gegevens die omgaan in beide use case-implementaties betekent dat, dat zij grotendeels identiek zijn. Anticiperend op een even analoge evolutie in toekomstige releases van het MedMij afsprakenstelsel, zijn de verantwoordelijkheden over de gegevens en performance in beide use case-implementaties daarom in deze pagina bij elkaar geplaatst.

Toestemmingsverklaring en bevestigingsverklaring

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 *Gegevensdienstnaam* 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 *Gegevensdienstnaam* 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.

Adressering en parameters

Toelichting

Op vier momenten in de flow van UCI Verzamelen, en die van UCI Delen, adresseren OAuth-rollen elkaar, op basis van een URI. Onderstaande tabel geeft een overzicht van die vier momenten. De adresbepaler is de OAuth-rol die de URI bepaalt (hier altijd de *OAuth Client*), de gebruiker de OAuth-rol die het bepaalde adres toepast. Wanneer de adresgebruiker de *OAuth User Agent* is, is de gebruiker dus niet de bepaler en verloopt het betreffende verkeer via de zogenoemde front-channel. In de andere twee gevallen is de *OAuth Client* bepaler en gebruiker en verloopt het verkeer via de zogenoemde back-channel.

gebruiksmoment	adresbepaler	adresgebruiker	geadresseerde	parameters
authorization request (stap 1)	*OAuth Client* (stap 1)	*OAuth User Agent*	*Authorization Endpoint* van de *OAuth Authorization Server*	• `response_type` • `client_id` • `redirect_uri` • `scope` • `state`
OAuth redirect (stap 10)	*OAuth Client* (stap 1)	*OAuth User Agent*	*OAuth Client*	
access token request (stap 12)	*OAuth Client* (stap 12)	*OAuth Client*	*Token Endpoint* van de *OAuth Authorization Server*	• `grant_type` • `code` • **geen** client_id • `redirect_uri`
FHIR request (stap 14)	*OAuth Client* (stap 14)	*OAuth Client*	*Resource Endpoint* van de *OAuth Resource Server*	

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, maar inzake poortnummers maken de verantwoordelijkheden een onderscheid tussen front- en back-channel.

2. De *OAuth Client* stelt conform RFC 3986 de URI samen waarmee hij zichzelf, de *OAuth Authorization Server* of de *OAuth Resource Server* adresseert. De URI heeft een hostname die een fully-qualified domain name is, conform RFC3696, sectie 2, en heeft het patroon `scheme://host[:port] 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.

3a. Ingeval de adresgebruiker *OAuth User Agent* is,

- is het gebruik van het voor `https` bedoelde poortnummer verplicht dat is opgenomen in de Service Name and Transport Protocol Port Number Registry van IANA;
- en, ingeval de geadresseerde het *Authorization Endpoint* van de *OAuth Authorization Server* is, betrekt de *OAuth Client* (als adres-bepaler) de URI, inclusief `host` en `path`, uit de *Zorgaanbiederslijst* , op basis van de van toepassing zijnde *Zorgaanbieder* en *Gegevensdienst.*

3b. Ingeval de adresgebruiker de *OAuth Client* is, betrekt de *OAuth Client* (als adres-bepaler) de eerste onderdelen van de URI, namelijk `host`, `path` en eventueel `port`, uit de *Zorgaanbiederslijst*, op basis van de van toepassing zijnde *Zorgaanbieder* en hetzij *Gegevensdienst* (wanneer geadresseerde *OAuth Authorization Server* is) of *Systeemrol* (wanneer geadresseerde *OAuth Resource Server* is). Andere elementen van de algemene URI-syntax, zoals `user`, `password`, `query` en `fragment`, zijn afwezig in de adressen.

> **Toelichting**
>
> Met de eis dat `host` noch `path` op een `/` mag eindigen, wordt mogelijk gemaakt dat de URI, vooral in het vierde van de genoemde momenten, wordt aangevuld met informatiestandaard-specifieke URL-eindstukken, zonder dat de grens met het generieke MedMij-beginstuk onherkenbaar wordt.
>
> ---
>
> De *Zorgaanbiederslijst* wordt dus gebruikt door de *OAuth Client* om het endpoint te kennen dat past bij de van toepassing zijnde *Zorgaanbieder, Gegevensdienst* en, voor het resource endpoint, *Systeemrol*. 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.

4. Voor één *OAuth Authorization Server* zijn de hostnames in de adressen voor zijn *Authorization Endpoint* en zijn *Token Endpoint* identiek.

> **Toelichting**
>
> Deze verantwoordelijkheid is opgenomen met het oog op de afbeelding, op de Netwerk-laag, van één *Authorization Server* op één *ZA Node*. Het *Resource Endpoint* mag wel met een andere hostname geadresseerd worden, omdat de *Resource Server* een andere rol is. Let wel, deze verantwoordelijkheid gaat enkel om de hostnames, niet om de gehele endpointadressen. Op andere elementen dan de hostname mogen de adressen van *Authorization Endpoint* en *Token* Endpoint wel verschillen.

5. De parameters in de authorization request worden als volgt gevuld:

parameter	vulling	toelichting
`response_type`	letterlijke waarde `code`	Dit is het gevolg van verantwoordelijkheid 6 op de Applicatielaag.
`client_id`	dezelfde hostname van de *OAuth Client* die ook in de *OAuth Clientlist* is opgenomen	
`redirect_uri`	zodanig dat de erin opgenomen hostname gelijk is aan de `client_id` en er geen poortnummer is opgenomen	Zie verantwoordelijkheid 3 hierboven.
`scope`	verplicht, met: • de betreffende (één) *Zorgaanbiedernaam*, ontdaan van de suffix `@medmij`, gevolgd door • een tilde (~), gevolgd door • het *GegevensdienstId* van de betreffende (één) *Gegevensdienst* uit de *Gegevensdienstnamen.*	De scope bestaat dus uit twee onderdelen, in een specifieke volgorde, gescheiden door een tilde. Er mag in de huidige versie van het MedMij Afsprakenstelsel slechts sprake zijn van één van elk. Bij interpretatie van de *Zorgaanbiedernaam* door de ontvanger zal deze de suffix `@medmij` weer moeten toevoegen.
`state`	conform sectie 4.1.1. van RFC 6749	Hiermee geeft de *OAuth Client* informatie mee aan de *OAuth Authorization Server*, waaraan eerstgenoemde later, bij de redirect, kan afleiden bij welk verzoek de authorization code hoort. Deze informatie is verder betekenisloos voor de *OAuth Authorization Server.*

6. 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.

7. 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 6 op de Applicatielaag.
`code`	conform verantwoordelijkheid 11 op de Applicatielaag	Zie de toelichting bij verantwoordelijkheid 11 op de Applicatielaag.
`client_id`	**niet gebruikt**	Deze is niet nodig, want door verantwoordelijkheid 13 op de Applicatielaag wordt geborgd dat het access token alleen wordt verstrekt aan de *OAuth Client* aan wie de *OAuth Resource Owner* toestemming heeft verleend.
`redirect_uri`	dezelfde waarde als in de voorafgaande authorization request	

8. In de resource request is de custom HTTP header `medmijscope:` opgenomen, met als waarde dezelfde scope als in de authorization request (zie verantwoordelijkheid 5).

> **Toelichting**
>
> Zo beschikt ook de *Resource Server* over de scope. Dit zorgt ervoor dat resource endpoint-adressen hergebruikt kunnen worden voor meerdere zorgaanbieders en geeft *Resource Servers* de mogelijkheid de toepasselijke *Authorization Server* te vinden ingeval *Authorization Servers* en *Resource Server* gescheiden geïmplementeerd zijn en één *Resource Server* met meerdere *Authorization Servers* van doen heeft.

Performance

9. Na ontvangst van een access token request, in *UCI Verzamelen* of *UCI Delen*, zal de *Authorization Server* , indien in antwoord daarop een access token dient te worden uitgegeven, na maximaal tien (10) seconden dit acces token ter beschikking stellen aan de *PGO Server*. Dit gedrag van de *Authorization Server* is gedurende minimaal 99,5% van de tijd beschikbaar.

10. Na ontvangst van een FHIR request, in *UCI Verzamelen* of *UCI Delen*, zal de *Resource Server*, indien in antwoord daarop een FHIR response dient te worden gedaan, na maximaal zestig (60) seconden dit FHIR response ter beschikking stellen aan de *PGO Server*. Dit gedrag van de *Resource Server* is gedurende minimaal 98,5% van de tijd beschikbaar.

Gegevens en performance inzake opvragen lijsten

Toelichting

Op enkele punten zijn er overeenkomsten tussen de verantwoordelijkheden inzake *UCI Opvragen ZAL*, *UCI Opvragen OCL* en *UCI Opvragen GNL* (Applicatie-laag) en *UCI Opvragen WHL* (Netwerk-laag). Deze verantwoordelijkheden zijn in deze pagina ondergebracht.

1. *MedMij Registratie* (in *UCI Opvragen ZAL*, *UCI Opvragen OCL* en *UCI Opvragen GNL*) en *MedMij Stelselnode* (in *UCI Opvragen WHL*) worden geadresseerd met de hostname `stelselnode.medmij.nl`. De URI van de:

- *Zorgaanbiederslijst* is `https://stelselnode.medmij.nl/MedMij_Zorgaanbiederslijst.xml`
- *OAuthclientlist* is `https://stelselnode.medmij.nl/MedMij_OAuthclientlist.xml`
- *Gegevensdienstnamenlijst* is `https://stelselnode.medmij.nl/MedMij_Gegevensdienstnamenlijst.xml`
- *Whitelist* is `https://stelselnode.medmij.nl/MedMij_Whitelist.xml`

2. Het aandeel van *MedMij Registratie* in elk van de use case-implementaties *UCI Opvragen ZAL*, *UCI Opvragen OCL* en *UCI Opvragen GNL* en 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 Registratie* (in *UCI Opvragen ZAL*, *UCI Opvragen OCL* en *UCI Opvragen GNL*) of *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.

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.

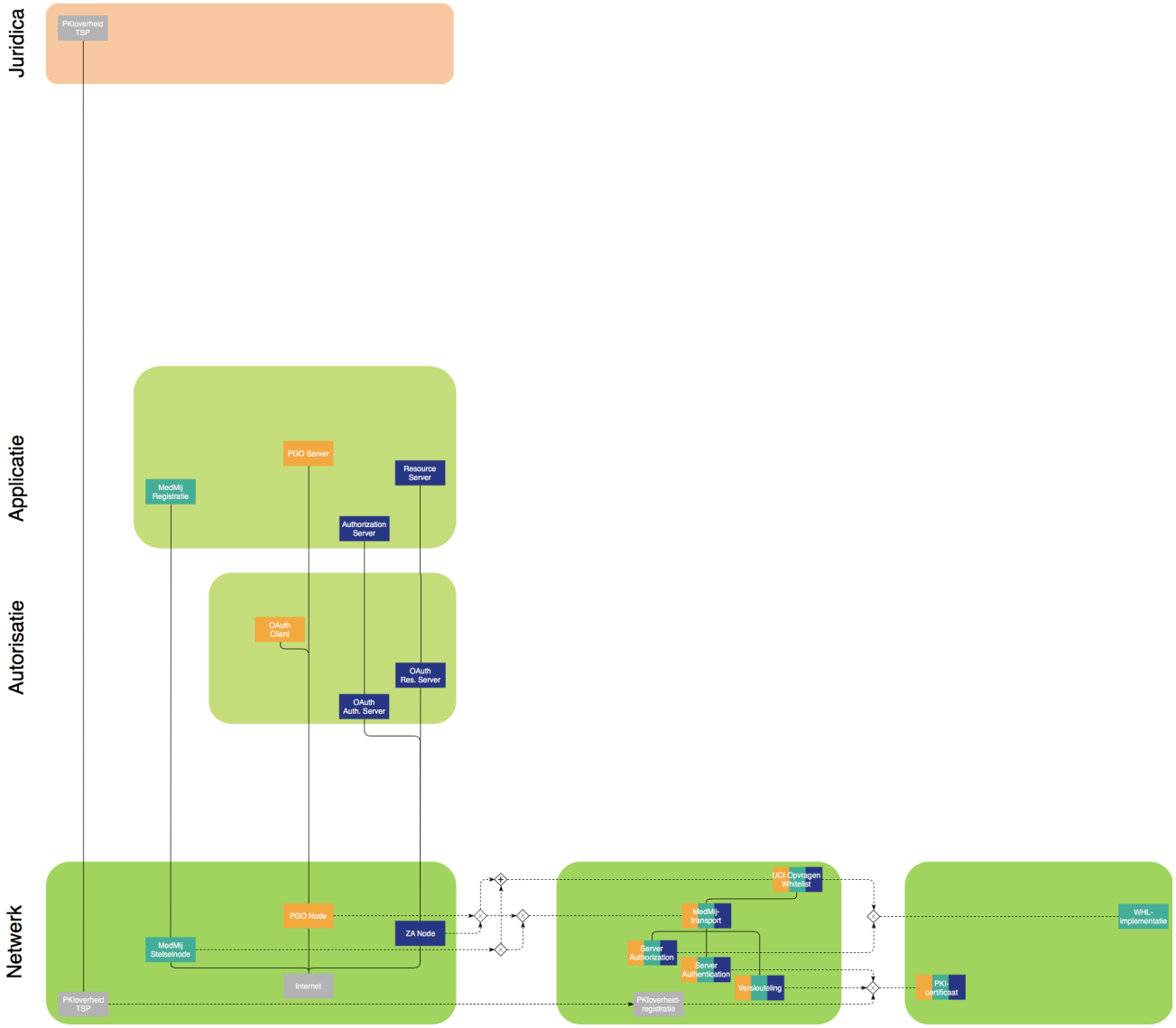
4. De in verantwoordelijkheid 1 bedoelde XML-bestanden:

- 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.

Netwerk



Toelichting

Op deze laag worden de 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 Nodes 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 whitelist-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`-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 PKIoverheid, jegens alle betrokken Certificate Authorities (CA's). PKIoverheid kent echter die mogelijkheid niet.
- De MedMij-beheerorganisatie geeft een **domeinverklaring** af, zodat deelnemers zelf een subdomein onder .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.
- Analoog 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 wegvalt, 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 PKIOverheid). 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 PKIoverheid-certificaat	altijd		
identificatie op basis van ...	`redirect_uri` of *Zorgaanbiederslijst*		PKIoverheid-certificaat
authenticatie, op basis van PKIoverheid-certificaat, van ...	alleen de TLS-server	TLS-client én TLS-server	
autorisatie op basis van controle tegen de *Whitelist*	niet	voorafgaand aan de TLS-handshake	tijdens de TLS-handshake

Rollen

Het MedMij-projectteam heeft vastgesteld dat tweede en derde bullet onder verantwoordelijkheid 1 iets vrijer geformuleerd kan worden. Er kunnen ook meerdere *ZA Nodes* gebruikt worden voor een enkele *Authorization Server* of *Resource Server*. Door deze verruiming kan de eerste alinea uit de daarop volgende toelichting genegeerd worden. Implementaties die voldoen aan de huidige beschrijving van de verantwoordelijkheden zullen ook na deze verruiming blijven voldoen. Bij een volgende release wordt de tekst tekst formeel aangepast.

1. In het *MedMij-netwerk* functioneert:

- elke *PGO Server*, met inbegrip van zijn *OAuth*-rol, op één of meerdere *PGO Nodes*. Voor frontchannel-verkeer gebruikt elke *PGO Server* één *PGO Node*, en wel met een hostname die voor die *PGO Server* voorkomt op de *OAuth Clientlist*.
- elke *Authorization Server*, met inbegrip van zijn *OAuth*-rol, op één *ZA Node*;
- elke *Resource Server*, met inbegrip van zijn *OAuth*-rol, op één *ZA Node*;
- precies één *MedMij Stelselnode*, waarop *MedMij Registratie* functioneert.

2. Op één:

- *PGO Node* functioneert één *PGO Server*;
- *ZA Node* functioneert één *Authorization Server* en/of één *Resource Server.*

3. Een of meerdere *PKIoverheid TSP*'s treden op als *PKIoverheid TSP*.

Toelichting

De getalsverhouding tussen Servers en Nodes is gespiegeld tussen het persoonsdomein (één-op-meer) en het zorgaanbiedersdomein (meer-op-één). Dat komt doordat er twee lijsten aan de orde zijn die in in tegengestelde richting een vertaling maken: de OAuth Clientlist vertaalt van hostnames, de Zorgaanbiederslijst juist naar hostnames. Om deze vertalingen te kunnen laten slagen moet er bij elke PGO Node één PGO Server horen, en (andersom) bij één Authorization Server of één Resource Server dus één ZA Node.

Het is dus mogelijk voor een *PGO Server* om verschillende certificaten te hanteren voor frontchannel- en backchannel-verkeer, zolang op de *OAuth Clientlist* maar de hostname in het certificaat voor frontchannelverkeer voorkomt die tevens voorkomt in de redirect URI inzake OAuth. Want laatstgenoemde wordt gebruikt door de Authorization Server ten behoeve van de toestemmingsvraag (in UCI Verzamelen) en de bevestigingsvraag (in UCI Delen).

Beide eisen onder punt 2 zorgen er bovendien voor dat aan de *Node*, en dus aan de *Hostname* daarvan, de Dienstverlener ter zake herkend kan worden, onder andere voor loggingsdoeleinden. Met betrekking tot het Zorgaanbiedersdomein zou dat de indruk kunnen wekken dat het onmogelijk wordt om als *Dienstverlener Zorgaanbieder* gebruik te maken van meerdere onderaannemers, bijvoorbeeld voor *Authorization Servers*, vanuit de gedachte dat die hun eigen *Nodes* in het MedMij-netwerk zullen gaan onderbrengen. Dat laatste is echter niet de bedoeling: de netwerkcomponenten van die eventuele onderaannemers zijn niet zichtbaar op het MedMij-netwerk, maar worden daarvan afgeschermd door *Nodes* van de *Dienstverlener Zorgaanbieder*. Op zulke *Nodes* kan dan bovendien de routering worden verzorgd over de verschillende onderaannemers, volgens een routeringsbeleid dat geheel aan de *Dienstverlener Zorgaanbieder* is.

Zie tevens verantwoordelijkheid 4 op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen.

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 xIS'en niet over het *MedMij-netwerk* communiceren met de *ZA Node*. Dat verkeer is verborgen achter de *ZA Node*. Alle daarvoor benodigde routering wordt afgehandeld door de server-implementaties en speelt zich buiten het zicht van het MedMij Afsprakenstelsel af.

Verantwoordelijkheden

TLS en certificaten

1. Al het verkeer over het *MedMij-netwerk* is beveiligd met Transport Layer Security (TLS). 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 1.0, van 3 november 2014 van het NCSC.

2. Om zich te kunnen authenticeren en autoriseren op het *MedMij-netwerk*, waar en zoals het MedMij Afsprakenstelsel dat vereist, kunnen elke *PGO Node*, elke *ZA Node* en de *MedMij Stelselnode*, in het kader van het TLS-verkeer zoals bedoeld in verantwoordelijkheid 1, een PKIoverheid-certificaat overleggen, en wel een server-certificaat van een *PKIoverheid TSP*.

3. Alle certificaathouders verbinden zich aan de op hen toepasselijke eisen van het PKIoverheid-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 ontlenen, 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: PKIoverheid 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 PKIoverheid-stelsel, op het door dat stelsel vastgestelde programma van eisen voor de in dat stelsel betrokken TSP's en op de certificatiehiërarchie van PKIoverheid. Deelnemers in het MedMij Afsprakenstelsel zullen dus service-certificaten moeten betrekken bij een bij PKIoverheid 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.

6. *ZA Node, PGO Node en MedMij Stelselnode* valideren tijdens de TLS-handshake aan het begin van een TLS-sessie of het een PKIoverheid-certificaat is en controleren, bij de *Certification Authority,* op basis van OCSP, of het ontvangen certificaat geldig is. In geval van het falen van één van deze controles, of het uitblijven van een controleresultaat, wordt het certificaat niet geaccepteerd en de TLS-sessie niet gestart.

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* maakt deze 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.

14. 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* uit tijdens de TLS-handshake, en wel onmiddellijk voorafgaand aan de voorziene verzending van de `Finished message`. Indien die controle niet kan worden uitgevoerd, of een negatief resultaat oplevert, wordt in plaats van de `Finished message` de uitzondering `access_denied` verzonden. In dit geval slaagt de controle tegen de *Whitelist* 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`.

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 de TLS-handshake, aan de hand van het certificaat dat hij, conform verantwoordelijkheid 1b, 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.

Wanneer de *Whitelist* wordt geraadpleegd gedurende de TLS-handshake, vraagt dat in de implementatie van de TLS-handshake mogelijk een extra stap ten opzichte van sommige standaard-implementaties. Daarom zijn alternatieven overwogen voor de *Whitelist*-controle in geval van inkomend verkeer. Eén alternatief is om de *Whitelist*-controle te laten plaatsvinden na afloop van een (succesvolle) TLS-handshake, maar dat introduceert een beveiligingsrisico, omdat na een succesvolle TLS-handshake ook al inhoudelijk gegevensverkeer kan plaatsvinden, mogelijk dus on-geautoriseerd. Bovendien zou deze variant een MedMij-specifiek autorisatieprotocol introduceren, terwijl de internationale en open TLS-standaard, door middel van de foutmelding `access_denied`, deze functionaliteit al biedt. Een andere overweging zou nog zijn de *Whitelist*-controle te verplaatsen naar de Applicatie-laag, maar dat zou weinig mogelijkheden bieden tot hergebruik en tot extra complexiteit leiden in zowel implementatie als onderhoud van het MedMij Afsprakenstelsel.

De foutmelding `access_denied` wordt besproken in sectie 7.2.2 van de TLS-specificatie.

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 wordt deze uitzondering behandeld als ware het de eerstvolgende inhoudelijke uitzondering conform de tabellen met uitzonderingen op UCI Verzamelen, respectievelijk UCI Delen, met dien verstande dat de betrokken Applicatie-rollen elkaar hiervan niet op de hoogte stellen.

Toelichting

Zo krijgt een uitzondering op Netwerk-niveau ook betekenis op Applicatie-niveau. 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. Elke *Dienstverlener Persoon*, elke *Dienstverlener Zorgaanbieder* en *MedMij Beheer* dragen ervoor zorg, in zijn rol als DNS Server, of cliënt daarvan, in het publieke Domain Name System, inzake de hostnames van de *MedMij Nodes*, respectievelijk *MedMij Stelselnode*, waarvoor hij verantwoordelijk is, dat de name records behorende bij die hostname 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

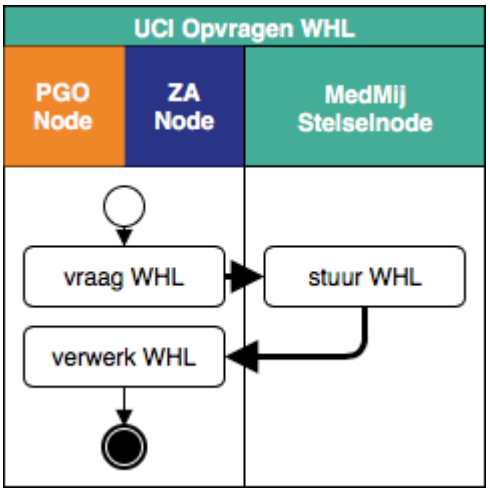
Het gebruik van DNSSEC (RFC 4033, RFC 4034, RFC 4035) vermindert de kwetsbaarheid van het Domain Name System voor bijvoorbeeld DNS spoofing.

UCI Opvragen WHL

Stroomdiagram

Toelichting

Beide interacties met de *MedMij Stelselnode* zijn backchannel-verkeer.



Informatiemodellen

Toelichting

Op de pagina's onder deze pagina zijn, op drie abstractieniveaus, modellen opgenomen van delen van de informatie die een rol speelt in de architectuur van het MedMij Afsprakenstelsel. De 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 huidige 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;
- en een voor de *MedMijStelselNode*, die in het afsprakenstelsel zelf gepubliceerd wordt, op deze pagina.

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. 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 onder andere worden gebruikt in een aantal registers, catalogi en lijsten. Vier daarvan worden door *MedMij Beheer* gepubliceerd voor operationeel gebruik door Dienstverleners:

- de *Zorgaanbiederslijst*, waaraan de *OAuth Client* kan zien welke *Zorgaanbieders* momenteel welke *Gegevensdiensten* aanbieden en waarmee hij 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 *OAuthc lient list*, waarmee de de *OAuth Authorization Server* een gebruikersvriendelijke naam van de *OAuth Client* kan vinden om te gebruiken in de toestemmingsverklaring danwel de bevestigingsverklaring;
- 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, de *Catalogus*, wordt door MedMij gepubliceerd als annex van het MedMij Afsprakenstelsel, op deze pagina. Voor alle vijf 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:

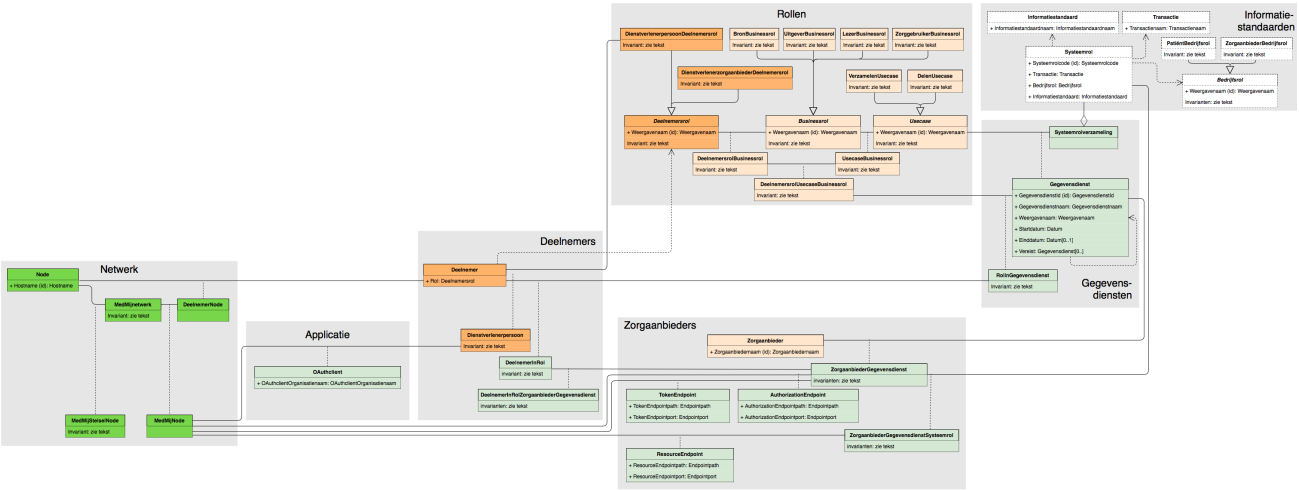
- de uses-relatie, vooral in het *Informatiestandaarden*-domein, omdat dat domein niet onder beheer van MedMij valt;
- de aggregatie-relatie, idem;
- de objectgeoriënteerde specialisatie, namelijk waar we een opsommende definitie geven van *Deelnemersrol*, *Businessrol*, *Usecase* en *Bedrijfsrol*;
- 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 een aantal modeldomeinen: *Rollen*, *Deelnemers*, *Zorgaanbieders*, *Gegevensdiensten*, *Informatiestandaarden* en *Netwerk*.

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 eigennaam wordt gebruikt die anderszins eist. Het metamodel

noteert dus *OAuthclient*, omdat de naam *OAuth* een eigennaam 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 *MedMijnetwerk*. Sterker, zonder de *MedMijStelselNode* kan het *MedMijnetwerk* 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 (*Organisatienaam*), om gebruikt te worden in de toestemmingsverklaring en de bevestigingsverklaring . Ook de *OAuthclientlist* is een implementatiecomponent en verschijnt pas in de logische modellen.

In het *Rollen*-modeldomein verschijnen de *Deelnemerrollen*, *Businessrollen* en *Usecases* die in deze release van het MedMij Afsprakenstelsel bestaan, en hun toegestane combinaties. In het *Deelnemers* -modeldomein 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 RolInGegevensdienst 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 modeldomein *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 *Systeemrol verzameling* 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 modeldomein is de basis voor het logische model van de *Zorgaanbiederslijst*. Wanneer een *Zorgaanbieder* een zekere *Gegevensdienst* aanbiedt, hoort daarbij een *Zorgaanbieder Gegevensdienst*. Deze klasse kan worden gebruikt om *Zorggebruikers* te informeren over wie van de *Zorgaanbieders* welke *Gegevensdiensten* aanbieden. Binnen een *Gegevensdienst* zijn bovendien één of meerdere *Systeemrollen* aan de orde. Deze relatie is vervat in de klasse *ZorgaanbiederGegevensdienstSysteemrol*.

Bij een *ZorgaanbiederGegevensdienst* hoort één *AuthorizationEndpoint* en één *TokenEndpoint*, en bij een *ZorgaanbiederGegevensdienstSysteemrol* één *ResourceEndpoint*. Bij alle drie soorten endpoints noemt het metamodel onderdelen van het technische adres (URI) waarmee zij geadresseerd worden, namelijk:

- het *Endpointpath*, dat wil zeggen, een eerste stuk van het path in de URI;
- de *Endpointport*, dat wil zeggen, het (optionele) poortnummer dat gebruikt wordt in het verkeer via de back-channel. Dit is niet aan de orde bij het *AuthorizationEndpoint*, omdat deze via het front-channel wordt aangesproken en daarvoor dus de standaard IANA-poort voor `https` verplicht is.

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 pagina Gegevens en performance in UCI Verzamelen en UCI Delen.

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.

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.

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
Bedrijfsrol	Elke *Bedrijfsrol* is hetzij *PatiëntBedrijfsrol* of *ZorgaanbiedersBedrijfsrol.*	*Informatiestandaarden*	Dit is een uitsluitende opsomming.
Bedrijfsrol	Voor elke *Bedrijfsrol b* geldt: ALS(*b : PatiëntBedrijfsrol* DAN *b.Weergavenaam* = "Patiënt"; *b : ZorgaanbiedersBedrijfsrol* DAN *b. Weergavenaam* = "Zorgaanbieder"; ANDERS FOUT)	*Informatiestandaarden*	Dit koppelt de namen van de subklassen de weergavenamen.
BronBusinessrol	Er is precies één instantie hiervan.	*Deelnemers*	Dit is een eenling in het model.
Businessrol	Voor elke *Businessrol b* geldt: ALS(*b : BronBusinessrol* DAN *b.Weergavenaam* = "Bron"; *b : LezerBusinessrol* DAN *b.Weergavenaam* = "Lezer"; *b : UitgeverBusinessrol* DAN *b.Weergavenaam*	*Rollen*	Dit koppelt de namen van de subklassen de weergavenamen.

	= "Uitgever"; ANDERS FOUT)		
DeelnemerInRol	Voor elke *DeelnemerInRol d* geldt: *d.Deelnemer.Deelnemersrol* en *d. RollnGegevensdienst. DeelnemersrolUsecaseBusinessrol. Deelnemersrol* zijn identiek.	*Deelnemers*	De betreffende *Deelnemer* kan zich allee aanmelden voor rollen die hem door de *Catalogus* geboden worden.
DeelnemerInRolZorgaanbiederGegevensdienst	Voor elke *DeelnemerInRolZorgaanbiederGegevensdienst d* geldt: *d. ZorgaanbiederGegevensdienst. Gegevensdienst = d.DeelnemerInRol. RollnGegevensdienst.Gegevensdienst*	*Zorgaanbieders*	Een *Deelnemer* kan alleen gezag doen g over de opname, in de *Zorgaanbiederslij* van een *Gegevensdienst* bij een *Zorgaanbieder*, als die *Deelnemer* ook v die *Gegevensdienst* is toegelaten in Med
Dienstverlenerpersoon	Er bestaat hooguit één instantie hiervan bij één *Deelnemer*, en precies één als de *Deelnemersrol* van laatstgenoemde van het type *DienstverlenerpersoonDeelnemersrol* is.	*Deelnemers*	Een Deelnemer heet een *Dienstverlenerpersoon* dan en slechts da hij de toepasselijke rol speelt.
Deelnemersrol	Voor elke *Deelnemersrol d* geldt: ALS(*d : DienstverlenerpersoonDeelnemersrol* DAN *d.Weergavenaam* = "Dienstverlener persoon"; *d : DienstverlenerzorgaanbiederDeelnemersrol DAN d.Weergavenaam* = "Dienstverlener zorgaanbieder" *;* ANDERS FOUT)	*Rollen*	Dit koppelt de namen van de subklassen de weergavenamen.
DeelnemersrolBusinessrol	Er bestaan precies drie instanties hiervan, namelijk:	*Rollen*	Hier worden de twee juridische rollen *Dienstverlener zorgaanbieder* en *Dienstverlener persoon* verbonden aan d Businessrollen *Uitgever*, *Bron* en *Lezer*.

	• één zodanig dat *DeelnemersrolBusinessrol*. *Deelnemersrol* : *DienstverlenerpersoonDeelnemersrol* en *DeelnemersrolBusiness.Businessrol* : *UitgeverBusinessrol*; • één zodanig dat *DeelnemersrolBusinessrol*. *Deelnemersrol* : *DienstverlenerzorgaanbiederDeelnemersrol* en *DeelnemersrolBusiness.Businessrol* : *BronBusinessrol*; en • één zodanig dat *DeelnemersrolBusinessrol* . *Deelnemersrol* : *DienstverlenerzorgaanbiederDeelnemersrol* en *DeelnemersrolBusiness* . *Businessrol* : *LezerBusinessrol* ;		
DeelnemersrolUsecaseBusinessRol	Deze klasse bestaat uit precies één instantie voor elke combinatie van een instantie *d* van *DeelnemersrolBusinessrol* en een instantie *u* van *UsecaseBusinessrol* waarvoor geldt: *d. BusinessRol = u.BusinessRol.*	*Rollen*	Hier worden alle (namelijk vier) passende combinaties gemaakt van *DeelnemersrolBusinessrol* en *UsecaseBusinessrol*. Het gaat om: DienstverlenerPersoon/Uitgever/Verzam DienstverlenerPersoon/Uitgever/Delen, DienstverlenerZorgaanbieder/Bron /Verzamelen en DienstverlenerZorgaanb /Lezer/Delen.
DelenUsecase	Er is precies één instantie hiervan.	*Rollen*	Dit is een eenling in het model.
DienstverlenerpersoonDeelnemersrol	Er is precies één instantie hiervan.	*Rollen*	Dit is een eenling in het model.
DienstverlenerzorgaanbiederDeelnemersrol	Er is precies één instantie hiervan.	*Rollen*	Dit is een eenling in het model.
Gegevensdienst	Er zijn nul of meer *Gegevensdiensten*.	*Gegevensdiensten*	Er kunnen op enig moment nul *Gegevensdiensten* zijn.

Gegevensdienst	Voor elke *Gegevensdienst g* geldt: *g.Startdatum* ligt niet na *g.Einddatum*.	*Gegevensdiensten*	Anders heeft de geldigheidsperiode geer
Gegevensdienst	Voor elke *Gegevensdienst g1* en *g2* geldt: ALS g*2* voorkomt in g *1* . *Vereist DAN* (g*2* staat als *Gegevensdienst* in *Catalogus* EN *g2.Startdatum* ligt niet voor g*1.Startdatum* EN *g2.Einddatum* ligt niet na g*1.Einddatum*)	*Gegevensdiensten*	Een geldige *Gegevensdienst* kan geen onbestaande of ongeldige *Gegevensdie* vereisen. Een ontbrekende Einddatum (v die is optioneel) betekent "voor onbepaal tijd" en ligt na elke "bepaalde tijd".
Gegevensdienst	Voor elke Gegevensdienst g geldt: g.Gegevensdienstnaam is een concatenatie van g.Usecase.Weergavenaam, g. Weergavenaam en Systeemrol.Versie met een spatie als scheidingsteken.		
LezerBusinessrol	Er is precies één instantie hiervan.	*Rollen*	Dit is een eenling in het model.
MedMijnetwerk	Er is precies één instantie hiervan.	*Netwerk*	Dit is een eenling in het model.
MedMijStelselNode	Er is precies één instantie hiervan.	*Netwerk*	Zonder *MedMijStelselNode* geen *MedMijNetwerk* en geen *Whitelist*.
Node	De hostname van een Node bevat een domeinnaam die een fully-qualified domain name is, conform RFC3696, sectie 2 .	*Netwerk*	Dit is een maatregel tegen risico 4.4.1.4 RFC 6819.
OAuthclient	Voor elke *OAuthclient o*: *o.OAuthclientOrganisatienaam* voldoet aan het OAuthclient-namenbeleid.	*Applicatie*	Zie het OAuthclient-namenbeleid.
PatiëntBedrijfsrol	Er is precies één instantie hiervan.	*Informatiestandaarden*	Dit is een eenling in het model.
RollnGegevensdienst	Deze klasse bestaat uit precies één instantie *r* voor elke combinatie van een instantie *d* van *r*. *DeelnemersrolUsecaseBusinessrol* en een	*Deelnemers*	Zo wordt ervoor gezorgd dat de *Usecase* bij de betreffende *Gegevensdienst* hoort overeenkomt met de Usecase die bij de

	instantie *g* van *r.Gegevensdienst* waarvoor geldt: *g.Usecase* = *d.UsecaseBusinessrol*. *Usecase*		*DeelnemersrolUsecaseBusinessrol* hoort Voor elke keer dat dat zo is, heeft deze k een instantie.
Systeemrol	Voor elke *Systeemrol s* geldt: ALS *s.Bedrijfsrol : PatiëntBedrijfsrol* DAN geldt voor alle *RollnGegevensdienst r*. (ALS *s* in *r* . *Gegevensdienst* . *TransactieVerzameling* DAN *r* . *DeelnemersrolUsecaseBusinessrol* . *Deelnemersrol* : *DienstverlenerpersoonDeelnemersrol*)	*Deelnemers*	Dit koppelt de MedMij-rol *Dienstverlener Persoon* aan de Nictiz-rol *Patiënt*.
Systeemrol	Voor elke *Systeemrol s* geldt: ALS *s.Bedrijfsrol : ZorgaanbiederBedrijfsrol* DAN geldt voor alle *RollnGegevensdienst r* : (ALS *s* in *r* . *Gegevensdienst* . *TransactieVerzameling* DAN *r* . *DeelnemersrolUsecaseBusinessrol* . *Deelnemersrol* : *DienstverlenerzorgaanbiederDeelnemersrol*)	*Deelnemers*	Dit koppelt de MedMij-rol *Dienstverlener Zorgaanbieder* aan de Nictiz-rol *Zorgaan* .
UitgeverBusinessrol	Er is precies één instantie hiervan.	*Rollen*	Dit is een eenling in het model.
Usecase	Voor elke *Usecase u* geldt: ALS(*u : VerzamelenUsecase* DAN *u.Weergavenaam* = "Verzamelen"; *u : DelenUsecase DAN u.Weergavenaam =* "Delen"*;* ANDERS FOUT)	*Rollen*	Dit koppelt de namen van de subklassen de weergavenamen.
Usecase Businessrol	Er zijn precies vier instanties hiervan, namelijk:	*Rollen*	Hier wordt bepaald welke *Businessrollen* participeren in welke *Usecases*.

	• één zodanig dat *UseCaseBusinessrol. Businessrol : UitgeverBusinessrol* en *UseCaseBusinessrol . Usecase : VerzamelenUsecase* ; • één zodanig dat *UseCaseBusinessrol. Businessrol : UitgeverBusinessrol* en *UseCaseBusinessrol.Usecase : DelenUsecase* ; en • één zodanig dat *UseCaseBusinessrol. Businessrol : BronBusinessrol* en *UseCaseBusinessrol.Usecase : VerzamelenUsecase* ; en • één zodanig dat *UseCaseBusinessrol. Businessrol : LezerBusinessrol* en *UseCaseBusinessrol.Usecase : DelenUsecase.*		
VerzamelenUsecase	Er is precies één instantie hiervan.	*Rollen*	Dit is een eenling in het model.
ZorgaanbiedersBedrijfsrol	Er is precies één instantie hiervan.	*Informatiestandaarden*	Dit is een eenling in het model.
Zorgaanbieder	Elke *Zorgaanbieder* heeft minstens één *ZorgaanbiederGegevensdienst*	*Zorgaanbieders*	Anders is de opname van de *Zorgaanbie* de *Zorgaanbiederslijst* nutteloos.
Zorgaanbieder	Elke *Zorgaanbieder* heeft bij elke *Gegevensdienst* ten hoogste één *ZorgaanbiederGegevensdienst*.	*Zorgaanbieders*	Zo kan de *OAuth Client* bij de combinatie een *Zorgaanbieder* en een *Gegevensdie* het *AuthorizationEndpoint* en *TokenEndp* vinden, in de *Zorgaanbiederslijst*.
ZorgaanbiederGegevensdienst	Voor elke *ZorgaanbiederGegevensdienst. Gegevensdienst. TransactieVerzameling. Transactie.Systeemrol s* waarvoor geldt dat *s.Bedrijfsrol* = *ZorgaanbiederBedrijfsrol*,	*Zorgaanbieders*	Als in de Catalogus een *Systeemrol* voor *Zorgaanbieders* hoort bij een namens ee zekere *Zorgaanbieder* aangeboden

	geldt dat er een *ZorgaanbiederGegevensdienstSysteemrol z* is zodat *z.Systeemrol* = s.		*Gegevensdienst*, dan moet namens deze *Zorgaanbieder* ook deze *Systeemrol* wor aangeboden.
ZorgaanbiederGegevensdienst	Elke *ZorgaanbiederGegevensdienst* heeft precies één *AuthorizationEndpoint*.	*Zorgaanbieders*	Zo kan de *OAuth Client* bij de combinatie een *Zorgaanbieder* en een *Gegevensdie* het *AuthorizationEndpoint* vinden, in de *Zorgaanbiederslijst*.
ZorgaanbiederGegevensdienst	Elke *ZorgaanbiederGegevensdienst* heeft precies één *TokenEndpoint*.	*Zorgaanbieders*	Zo kan de *OAuth Client* bij de combinatie een *Zorgaanbieder* en een *Gegevensdie* het *TokenEndpoint* vinden, in de *Zorgaanbiederslijst*.
ZorgaanbiederGegevensdienst	Elke *ZorgaanbiederGegevensdienst* heeft precies één *DeelnemerInRolZorgaanbiederGegevensdienst d*, en wel zo dat *d.DeelnemerInRol.Deelnemer.Rol* = *DienstverlenerzorgaanbiederDeelnemersrol*.	*Zorgaanbieders*	Zo is duidelijk welke *DeelnemerInRol* zor voor een *ZorgaanbiederGegevensdienst* dat dat een *Dienstverlener zorgaanbiede* betreft.
ZorgaanbiederGegevensdienst	Voor elke *ZorgaanbiederGegevensdienst z*, voor elk *AuthorizationEndpoint a* van *z* en voor elke *DeelnemerinRolZorgaanbiederGegevensdienst d* van *z* geldt: er is een *MedMijNode m* zodanig dat: *a.AuthorizationEndpointuri* bevat *m.DeelnemerNode.Node.Hostname* en *d.DeelnemerinRol.Deelnemer* = *m.DeelnemerNode.Deelnemer*	*Zorgaanbieders*	Deze ingewikkelde invariant regelt dat de van elk authorization endpoint de hostna bevat van een *MedMijNode* die van deze *Deelnemer* is die ook de betreffende *ZorgaanbiederGegevensdienst* aanbiedt. Hoewel de invariant spreekt van "elk *AuthorizationEndpoint t* van *z*" en van "el *DeelnemerinRolZorgaanbiederGegevens d* van *z*" zijn er van beide maar één voor *ZorgaanbiederGegevensdienst*. Dat wor geregeld door andere invarianten, maar daarvan wil deze invariant niet afhankelij
ZorgaanbiederGegevensdienst	Voor elke *ZorgaanbiederGegevensdienst z* ,	*Zorgaanbieders*	Deze ingewikkelde invariant regelt dat de

	voor elk *TokenEndpoint t* van *z* en voor elke *DeelnemerinRolZorgaanbiederGegevensdienst d* van *z* geldt: er is een *MedMijNode m* zodanig dat: *t.TokenEndpointuri* bevat *m.DeelnemerNode* . *Node* . *Hostname* en *d.DeelnemerinRol.Deelnemer* = *m*. *DeelnemerNode.Deelnemer*		van elk token endpoint de hostname bev van een *MedMijNode* die van dezelfde *Deelnemer* is die ook de betreffende *ZorgaanbiederGegevensdienst* aanbiedt. Hoewel de invariant spreekt van " elk *ResourceEndpoint r* van *z* " en van " elke *DeelnemerinRolZorgaanbiederGegevens d* van *z* " zijn er van beide maar één voor *ZorgaanbiederGegevensdienst* . Dat wor geregeld door andere invarianten, maar daarvan wil deze invariant niet afhankelij
ZorgaanbiederGegevensdienst	Voor elke *ZorgaanbiederGegevensdienst z* , voor elke *ZorgaanbiederGegevensdienstSysteemrol zs* van *z*, voor elk *ResourceEndpoint r* van *zs* en voor elke *DeelnemerinRolZorgaanbiederGegevensdienst d* van *z* geldt: er is een *MedMijNode m* zodanig dat: *r.ResourceEndpointuri* bevat *m*. *DeelnemerNode* . *Node* . *Hostname* en *d.DeelnemerinRol.Deelnemer* = *m*. *DeelnemerNode.Deelnemer*	*Zorgaanbieders*	Deze ingewikkelde invariant regelt dat de van elk resource endpoint de hostname l van een MedMijNode die van dezelfde *Deelnemer* is die ook de betreffende *ZorgaanbiederGegevensdienst* aanbiedt. Hoewel de invariant spreekt van " elk *TokenEndpoint a* van *z* " en van " elke *DeelnemerinRolZorgaanbiederGegevens d* van *z* " zijn er van beide maar één voor *ZorgaanbiederGegevensdienst* . Dat wor geregeld door andere invarianten, maar daarvan wil deze invariant niet afhankelij
ZorgaanbiederGegevensdienstSysteemrol	Elke combinatie van een *Zorgaanbieder Gegevensdienst* en een *Systeemrol* heeft ten hoogste één *ZorgaanbiederGegevensdienstSysteemrol*.	*Zorgaanbieders*	Zo kan de *OAuth Client* bij de combinatie een *Zorgaanbieder,* een *Gegevensdiens* een Systeemrol het *ResourceEndpoint* vinden, in de *Zorgaanbiederslijst*.
ZorgaanbiederGegevensdienst Systeemrol	*ZorgaanbiederGegevensdienstSysteemrol. Systeemrol.Bedrijfsrol* = *ZorgaanbiederBedrijfsrol*	*Zorgaanbieders*	*Zorgaanbieders* kunnen alleen *Systeemr* aanbieden die voor *Zorgaanbieders* bedo zijn.

ZorgaanbiederGegevensdienstSysteemrol	Elke *ZorgaanbiederGegevensdienstSysteemrol* heeft precies één *ResourceEndpoint*.	*Zorgaanbieders*	Zo kan de *OAuth Client* bij de combinatie een *Zorgaanbieder,* een *Gegevensdiens* een Systeemrol het *ResourceEndpoint* vinden, in de *Zorgaanbiederslijst*.
ZorggebruikerBusinessrol	Er is precies één instantie hiervan.	*Rollen*	Dit is een eenling in het model.

Basisklassen

Basisklasse	Definitie
Datum	Conform het type `xs:date`, zoals gespecificeerd in XML Schema 1.0.
Endpointport	Zie adresseringsverantwoordelijkheden op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen .
Endpointpath	Zie adresseringsverantwoordelijkheden op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen .
GegevensdienstId	String van minimaal één en maximaal 30 tekens.
Gegevensdienstnaam	String van minimaal drie en maximaal 50 tekens.
Hostname	Zie adresseringsverantwoordelijkheden op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen.
Informatiestandaardnaam	String van minimaal drie en maximaal 50 tekens.
OAuthclientOrganisatienaam	Conform toepasselijk Oauthclient-namenbeleid.
Systeemrolcode	String van minimaal één en maximaal 30 tekens.
Transactienaam	String van minimaal drie en maximaal 50 tekens.
Weergavenaam	String van minimaal drie en maximaal 50 tekens.
Zorgaanbiedernaam	Conform toepasselijk Zorgaanbiedersnamenbeleid.

MedMij
Grip op je eigen gezondheidsgegevens

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. De huidige 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 vier lijsten staan gecombineerd in één logisch model, onder de klasse *MedMijBeheerlijst*, omdat zij twee kenmerken delen: een tijdstempel en een volgnummer.

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 logisch 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 verervingen: 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 verervingsinvariant staat opgeschreven met een . Vóór dat pijltje staat het ervende attribuut van de *logische* klasse, erachter staat het pad *in het metamodel* naar de verervende 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.

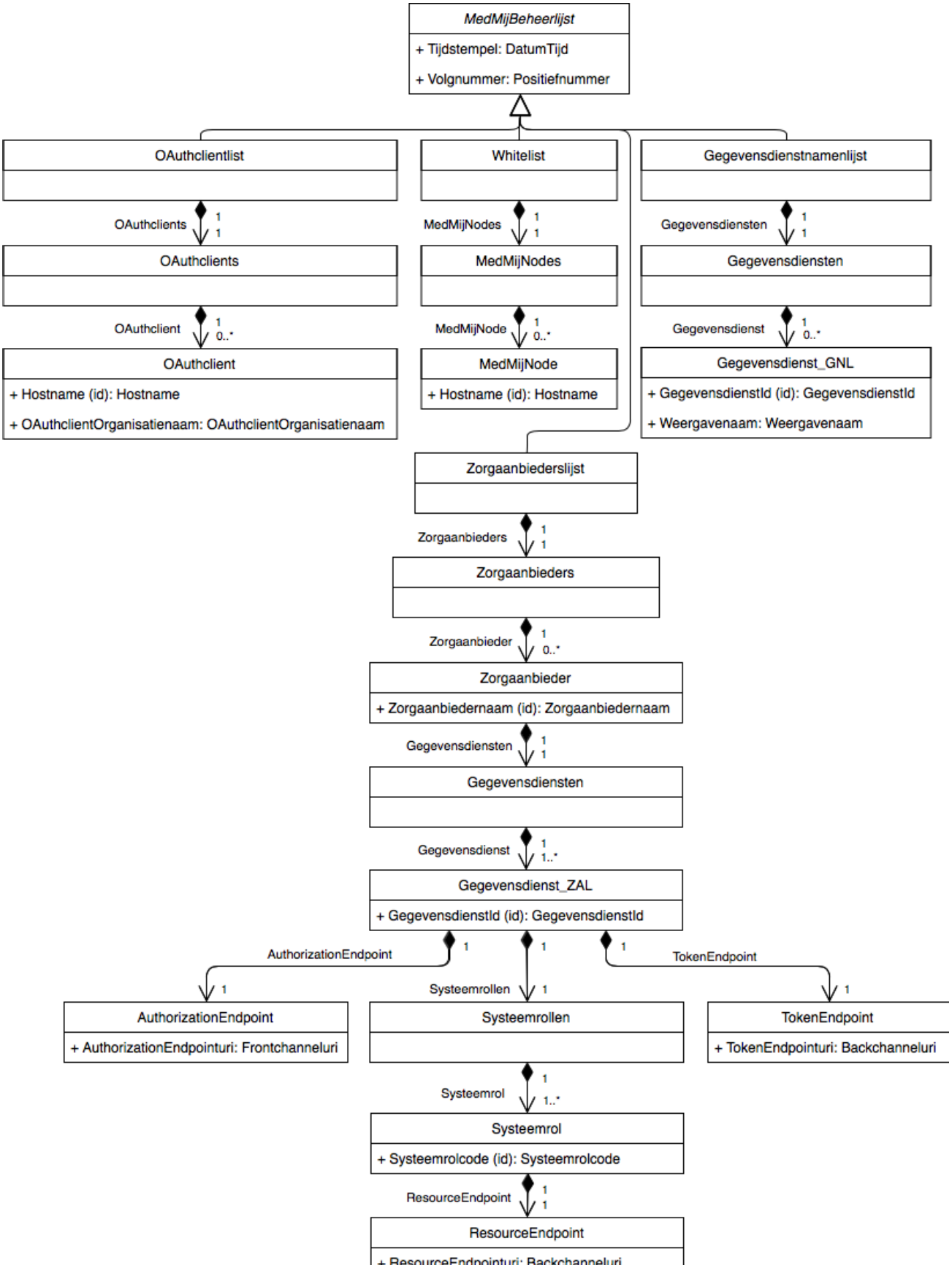
Bij de vertaling van de associativiteit van het metamodel naar de hiërarchie van de logische modellen is een aantal vuistregels gebruikt.

- 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 (namelijk *Gegevensdienst* in het logische model van de lijsten). In dat geval worden de namen uitgebreid zodat hun hiërarchische context zichtbaar wordt (namelijk tot *Gegevensdienst_GNL* en *Gegevensdienst_ZAL*).

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


MedMijBeheerlijst
+ Tijdstempel: DatumTijd
+ Volgnummer: Positiefnummer
OAuthclientlist
Whitelist
Gegevensdienstnamenlijst
OAuthclients
1
1
MedMijNodes
1
1
Gegevensdiensten
1
1
OAuthclients
MedMijNodes
Gegevensdiensten
OAuthclient
1
0..*
MedMijNode
1
0..*
Gegevensdienst
1
0..*
OAuthclient
+ Hostname (id): Hostname
+ OAuthclientOrganisatienaam: OAuthclientOrganisatienaam
MedMijNode
+ Hostname (id): Hostname
Gegevensdienst_GNL
+ GegevensdienstId (id): GegevensdienstId
+ Weergavenaam: Weergavenaam
Zorgaanbiederslijst
Zorgaanbieders
1
1
Zorgaanbieders
Zorgaanbieder
1
0..*
Zorgaanbieder
+ Zorgaanbiedernaam (id): Zorgaanbiedernaam
Gegevensdiensten
1
1
Gegevensdiensten
Gegevensdienst
1
1..*
Gegevensdienst_ZAL
+ GegevensdienstId (id): GegevensdienstId
AuthorizationEndpoint
1
1
1
TokenEndpoint
1
Systeemrollen
1
1
AuthorizationEndpoint
+ AuthorizationEndpointuri: Frontchanneluri
Systeemrollen
TokenEndpoint
+ TokenEndpointuri: Backchanneluri
Systeemrol
1
1..*
Systeemrol
+ Systeemrolcode (id): Systeemrolcode
ResourceEndpoint
1
1
ResourceEndpoint

+ ResourceEndpointum: Backchannelen

Logische invarianten

Betreft instanties van logische klasse ...	Invariant	Component	Toelichting	Aard	Herkomst
AuthorizationEndpoint	Voor elke *AuthorizationEndpoint a* geldt: *a* . *AuthorizationEndpoint uri* combinatie van *a* . *MedMijNode* . *DeelnemerNode* . *Node* . *Hostname* en *a. AuthorizationEndpointpath*, conform de adresseringsverantwoordelijkheden op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen	*Zorgaanbiederslijst*	Zie de pagina Gegevens en performance in UCI Verzamelen en UCI Delen.	vererving	logisch model
Gegevensdienst_ZAL	Voor elke *Gegevensdienst_ZAL g* met haar corresponderende *ZorgaanbiederGegevensdienst z* geldt: *g.GegevensdienstId z.Gegevensdienst. GegevensdienstId*	*Zorgaanbiederslijst*	Zo erft de *Zorgaanbiederslijst* de *GegevensdienstId* 's van de *Catalogus*.	vererving	logisch model
Gegevensdienstnamenlijst	Er is precies één instantie hiervan.	*Gegevensdienstnamenlijst*	Dit is een eenling in het model.	getalsverhouding	logisch model
MedMijNode	Voor elke *MedMijNode m* geldt: *m.Hostname = m.DeelnemerNode.Node. Hostname*	*Whitelist*	Zo erft de *MedMijNode* de *Hostname* van de *Node* die het is.	vererving	logisch model
MedMijNode	De hostname van een *MedMijNode* bevat een domeinnaam die een fully-qualified domain name is, conform RFC3696, sectie 2.	*Whitelist*	Dit is een maatregel tegen risico 4.4.1.4 uit RFC 6819.	lokale afhankelijkheid	metamodel (bij *Node*)
OAuthclient	Voor elke *OAuthclient o*: *o.OAuthclientOrganisatienaam* voldoet	*Applicatie*	Zie het OAuthclient-namenbeleid.	lokale afhankelijkheid	metamodel (bij

	aan het OAuthclient-namenbeleid.				*OAuthclient*)
OAuthclient	*Voor elke OAuthclient o geldt: o.Hostname o.MedMijNode .Hostname*.	*OAuthclientlist*	Zo erft de *OAuthclientlist* de *Hostnames* van de *Nodes*.	vererving	logisch model
OAuthclientlist	Er is precies één instantie hiervan.	*OAuthclientlist*	Dit is een eenling in het model.	getalsverhouding	logisch model
ResourceEndpoint	Voor elk *ResourceEndpoint r* geldt: *r. ResourceEndpointuri* combinatie van *r.MedMijNode. DeelnemerNode.Node.Hostname*, *r. ResourceEndpointport en r. ResourceEndpointpath*, conform de adresseringsverantwoordelijkheden op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen .	*Zorgaanbiederslijst*	Zie de pagina Gegevens en performance in UCI Verzamelen en UCI Delen.	vererving	logisch model
Systeemrol	Voor elke *Systeemrol s* met haar corresponderende *ZorgaanbiederGegevensdienstSysteemrol z* geldt: *s.Systeemrolcode z.Systeemrol. Systeemrolcode*	*Zorgaanbiederslijst*	Zo erft de *Zorgaanbiederslijst* de *Systeemrolcodes* van het *Register van Informatiestandaarden* .	vererving	logisch model
TokenEndpoint	Voor elk *TokenEndpoint t* geldt: *t. TokenEndpointuri* combinatie van *t.MedMijNode. DeelnemerNode.Node.Hostname*, *t. TokenEndpointport* en *t. TokenEndpointpath*, conform de adresseringsverantwoordelijkheden op de	*Zorgaanbiederslijst*	Zie de pagina Gegevens en performance in UCI Verzamelen en UCI Delen.	lokale afhankelijkheid	logisch model

	pagina Gegevens en performance in UCI Verzamelen en UCI Delen.				
Whitelist	Er is precies één instantie hiervan.	*Whitelist*	Dit is een eenling in het model.	getalsverhouding	logisch model
Zorgaanbiederslijst	Er is precies één instantie hiervan.	*Zorgaanbiederslijst*	Dit is een eenling in het model.	getalsverhouding	logisch model

Logische basisklassen

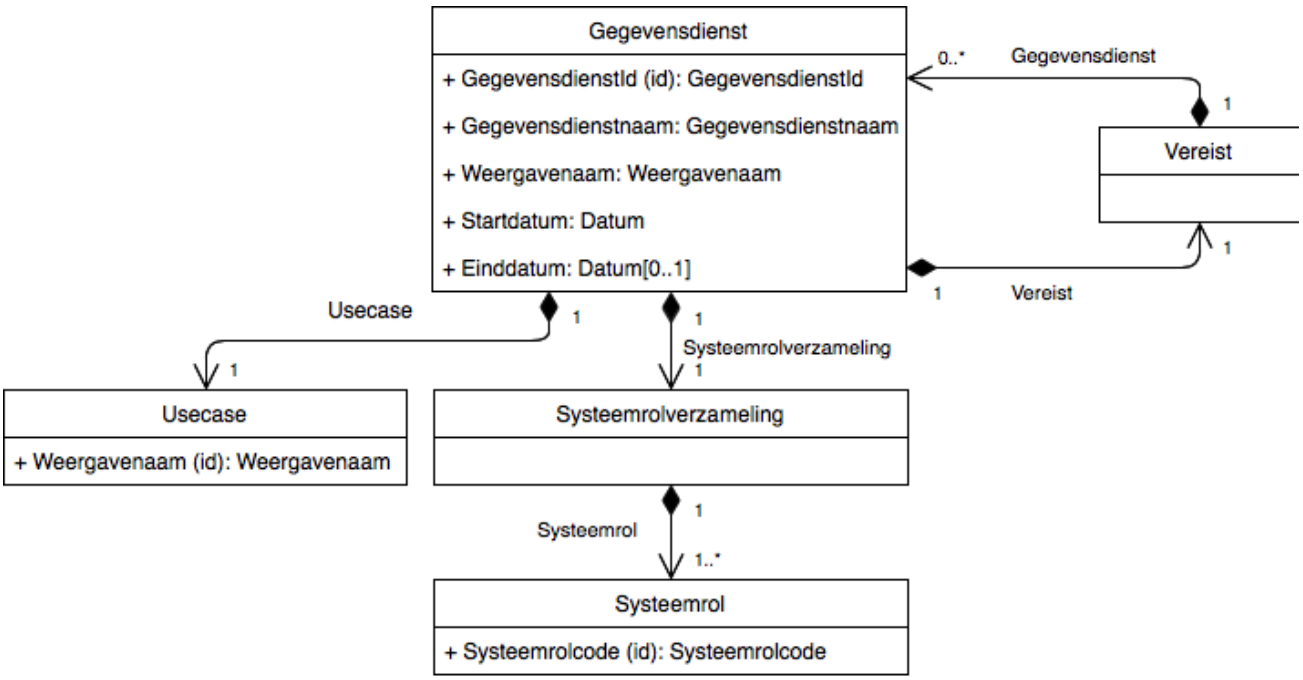
Basisklasse	Definitie	Herkomst
Backchanneluri	Zie adresseringsverantwoordelijkheden op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen. De domeinnaam is een fully-qualified domain name, conform RFC3696, sectie 2.	logisch model
DatumTijd	Conform het type `xs:dateTime` , zoals gespecificeerd in XML Schema 1.0 en inclusief een tijdzone-indicatie.	logisch model
Frontchanneluri	Zie adresseringsverantwoordelijkheden op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen. De domeinnaam is een fully-qualified domain name, conform RFC3696, sectie 2 .	logisch model
GegevensdienstId	String van minimaal één teken en maximaal 30 tekens.	metamodel
Hostname	Zie adresseringsverantwoordelijkheden op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen.	metamodel
OAuthclientOrganisatienaam	Conform toepasselijk Oauthclient-namenbeleid.	metamodel
Positiefnummer	Een geheel getal ongelijk 0.	logisch model
Systeemrolcode	String van minimaal één teken en maximaal 30 tekens.	metamodel
Weergavenaam	String van minimaal drie en maximaal 50 tekens.	metamodel
Zorgaanbiedernaam	Conform toepasselijk Zorgaanbiedersnamenbeleid.	metamodel

Verband met metamodel

Klasse in logisch model	Herkomstklasse in metamodel
AuthorizationEndpoint	*AuthorizationEndpoint*
Gegevensdienst_GNL	*Gegevensdienst*
Gegevensdienst_ZAL	*ZorgaanbiederGegevensdienst*
MedMijNode	*MedMijNode*
OAuthclient	*OAuthclient*
ResourceEndpoint	*ResourceEndpoint*
Systeemrol	*ZorgaanbiederGegevensdienstSysteemrol*
TokenEndpoint	*TokenEndpoint*
Zorgaanbieder	*Zorgaanbieder*

Catalogus

Logisch model



Logische invarianten

Betreft instanties van klasse ...	Invariant	Component	Toelichting	Aard	Herkomst
Usecase	Voor elke *Usecase u* geldt: *u.Weergavenaam* = "Verzamelen" OF *u.Weergavenaam* = "Delen"	*Catalogus*	Dit koppelt de namen van de subklassen aan de weergavenamen.	lokale afhankelijkheid	metamodel (bij *Usecase*)

Logische basisklassen

Basisklasse	Definitie	Herkomst
Datum	Conform het type `xs:date`, zoals gespecificeerd in XML Schema 1.0.	metamodel
GegevensdienstId	String van minimaal één teken en maximaal 30 tekens.	metamodel
Gegevensdienstnaam	String van minimaal drie en maximaal 50 tekens.	metamodel
Systeemrolcode	String van minimaal één teken en maximaal 30 tekens.	metamodel
Weergavenaam	String van minimaal drie en maximaal 50 tekens.	metamodel

Verband met metamodel

Klasse/waarde in logisch model	Herkomstklasse in metamodel
Gegevensdienst	*Gegevensdienst*
Usecase	*Usecase* , *VerzamelenUsecase* en *DelenUsecase*

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 geïnteressseerd 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
MedMijStelselNode	Voor de *MedMijStelselNode m* geldt: *m.Hostname m. Node.Hostname*	*MedMijStelselNode*	Zo erft de *MedMijStelselNode*, van de *Node* die het is, de *Hostname*.	vererving

Logische basisklassen

Basisklasse	Definitie	Herkomst
Hostname	Zie adresseringsverantwoordelijkheden op de pagina Gegevens en performance in UCI Verzamelen en UCI Delen.	metamodel

Verband met metamodel

Klasse in logisch model	Herkomstklasse in metamodel
MedMijStelselNode	*MedMijStelselNode*

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 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, zijn in het XML-schema van de betreffende lijst 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 horen vier technische componenten. De hoogste klasse van elke component wordt het rootelement van het betreffende XML-schema. De attributen van de abstracte klasse erboven (*MedMijBeheerlijst*) worden over de technische modellen van deze vier verspreid. Er is dus voor elke lijst een apart XML-schema. Daardoor is de homonymie van `Gegevensdienst` geen probleem meer en kunnen in de namen de achtervoegsels `_ZAL` en `_GNL` 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 behoeft 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	Bestandsnaam	Release	Versie bestand
Zorgaanbiederslijst	MedMij_Zorgaanbiederslijst.xsd	2	5
Whitelist	MedMij_Whitelist.xsd	2	9
OAuthclientlist	MedMij_OAuthclientlist.xsd	2	5
Gegevensdienstnamenlijst	MedMij_Gegevensdienstnamenlijst.xsd	1	7

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
Zorgaanbiederslijst	MedMij_Zorgaanbiederslijst_example.xml	2	2
Whitelist	MedMij_Whitelist_example.xml	5	2
OAuthclientlist	MedMij_OAuthclientlist_example.xml	2	2
Gegevensdienstnamenlijst	MedMij_Gegevensdienstnamenlijst_example.xml	2	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 tijdselement 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 foutherstel. 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 productieversies; 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]/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 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 component (lijst) welke prefix wordt gebruikt.

Component	Prefix
Gegevensdienstnamenlijst	`gnl`
OAuthclientlist	`ocl`
Whitelist	`whl`
Zorgaanbiederslijst	`zal`

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-attribuut `standalone`, omdat er gebruik gemaakt wordt van XML-schema's in plaats van DTD's.

Omwille 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

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.

Basisklasse	Basis (XML-datatype)	minLength	maxLength	pattern

Backchanneluri	xs:string			https://(([a-z0-9])([a-z0-9-])*(\.))+([a-z0-9])([a-z0-9-])*([a-z0-9])(:(\d){1,5})?(/[^?#/]+)*
DatumTijd	xs:dateTime			.{20,}
Frontchanneluri	xs:string			https://(([a-z0-9])([a-z0-9-])*(\.))+([a-z0-9])([a-z0-9-])*([a-z0-9])?(/[^?#/]+)*
GegevensdienstId	xs:string	1	30	
Hostname	xs:string			(([a-z0-9])([a-z0-9-])*(\.))+([a-z0-9])([a-z0-9-])*([a-z0-9])
OAuthclientOrganisatienaam	xs:string	3	50	
Positiefnummer	xs:positiveInteger			
Systeemrolcode	xs:string	1	30	
Weergavenaam	xs:string	3	50	
Zorgaanbiedernaam	xs:string	10	57	([a-z])+@medmij

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 certificatiedoeleinden 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 7510:2017 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);
- Het MedMij Afsprakenstelsel moet onder, dan wel binnen, de scope van het NEN 7510-certificaat vallen;
- 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 met een onderbouwende rapportage** 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.

Naam	Bestand
Rapportageformat	Rapportage format aanvullende auditverklaring MedMij Afsprakenset release 1.1.docx
Beoordelingskader	Beoordelingskader aanvullende auditverklaring MedMij Afsprakenset release 1.1.docx

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. 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.

Normenkader

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

Vereiste beheersmaatregel inclusief referentie corresponderende NEN norm (NEN 7510: 2017)	DVP	DVZA	BO	Implementatie
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 ENCRYPT-CSA aanbevelingen, zie hieronder. *Een overzicht van publicaties is te vinden op https://www.keylength.com/ Er kan gebruik gemaakt worden van de ENCRYPT-CSA aanbevelingen en/of die van het BSI*
A.12.1.2 Wijzigingsbeheer	✓	✓	✓	Er is overkoepelend Change- en releasebeleid gedefinieerd om wijzigingen aan functionele-, operationele- en beveiligingseigenschappen te ontwerpen, testen, communiceren en te implementeren. Deelnemers en de beheerorganisatie dienen aan te sluiten op dit proces en wijzigingen de mogelijk impact hebben op het functioneren van het stelsel conform dit proces af te handelen.
A.12.1.3 Capaciteitsbeheer	✓	✓	✓	• Beschikbaarheid voor **deelnemers** zijn vastgelegd in Gegevens en performance in UCI Verzamelen en UCI Delen. • Beschikbaarheid voor de **beheerorganisatie** zijn vastgelegd in Gegevens en performance inzake opvragen lijsten.
A.12.3.1 Back-up van informatie	✓	✓		De dienstverlener persoon dient een backupschema in plaats te hebben met bijbehorende (minimaal jaarlijks geteste) recovery procedures die ervoor zorgen dat de gegevens van de persoon binnen een dag (24u) terug kunnen worden geplaatst in geval van een incident.
A.12.4.1 Gebeurtenissen registreren	✓	✓	✓	1. Logging moet plaatsvinden zoals gespecificeerd in het afsprakenstelsel (zie Processen en informatie onder Logging) 2. Verzoeken en toestemmingsverklaring van gebruikers ten aanzien van het opvragen van informatie bij zorgaanbieders dienen onweerlegbaar en controleerbaar te worden vastgelegd.
A.12.4.4 Kloksynchronisatie	✓	✓	✓	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met **pool.ntp.org**. Het is toegestaan te synchroniseren met een lokale NTP-server, zolang deze ten minste één keer per 24 uur synchroniseert met bovengenoemde NTP-server.
A.12.5.1 Software installeren op operationele systemen	✓	✓	✓	Het uitvoeren van handelingen op systemen en gegevens die direct impact (kunnen) hebben op de beschikbaarheid, integriteit of vertrouwelijkheid van de keten, dienen op basis van het vier-ogen-principe te worden uitgevoerd.
A.12.6.1 Beheer van technische kwetsbaarheden	✓	✓	✓	Deelnemers dienen aan te sluiten bij het proces van beheren van technische kwetsbaarheden in het afsprakenstelsel (Operationele processen).
A.14.2.1 Beleid voor beveiligd ontwikkelen	✓	✓	✓	Er moeten door de deelnemers beveiligingsstandaarden worden toegepast in de ontwikkelde internet facing applicaties. Minimale beveiligingsstandaarden waaraan alle ontwikkelde applicaties van deelnemers moeten voldoen:

				1. Voor webapplicaties worden de ICT- Beveiligingsrichtlijnen voor webapplicaties van het NCSC gehanteerd. In het bijzonder zijn dan de maatregelen uit het "Uitvoeringsdomein" van belang, https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html. 2. Voor mobiele applicaties kan worden gesteund op richtlijnen van het NCSC hiervoor: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-mobiele-apps.html.
A.16.1.1 Verantwoordelijkheden en procedures	✓	✓	✓	Deelnemers moeten aansluiten bij het proces voor incidenten en calamiteiten zoals dit is gedefinieerd in het afsprakenstelsel (Operationele processen).
A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging	✓	✓	✓	Er is een meldplicht voor alle deelnemers en de beheerorganisatie om incidenten die betrekking hebben op persoonlijke gezondheidsgegevens of het functioneren van het MedMij stelsel onmiddellijk te melden bij centrale incident management team. Zie Deelnemersovereenkomsten.
A.16.1.7 Verzamelen van bewijsmateriaal	✓	✓	✓	Deelnemers en de beheerorganisatie dienen medewerking te verlenen aan (forensische) onderzoeken, door het aanleveren van gevraagde bewijsmaterialen, zulks op verzoek van de beheerorganisatie of bevoegde instanties.
A.18.2.3 Beoordeling van technische naleving	✓	✓	✓	1. Tenminste jaarlijks laten de deelnemers en de beheerorganisatie **whitebox** applicatiepenetratietesten en code reviews uitvoeren op de externe koppelvlakken. Bij toetreding hebben deze minimaal al een keer plaatsgevonden. *Non-conformiteiten* worden gemeld bij de beheerorganisatie. 2. Tenminste jaarlijks laat de beheerorganisatie **blackbox** infrastructuur penetratietesten uitvoeren op de externe koppelvlakken van de deelnemers ten behoeve van het MedMij stelsel.
A.5.1.1 Beleidsregels voor informatiebeveiliging	✓	✓	✓	De beleidsdocumenten van deelnemers dienen de beleidsmaatregelen die van toepassing zijn op MedMij (onder andere gespecificeerd in Privacy- en informatiebeveiligingsbeleid) specifiek te benoemen.
A.6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging	✓	✓	✓	Elke deelnemer en de beheerorganisatie dient een deskundige verantwoordelijke, met mandaat om besluiten te nemen ten aanzien van MedMij, aan te wijzen als contactpersoon voor alle zaken met betrekking tot informatiebeveiliging. De organisatie dient tijdens kantooruren binnen een uur beschikbaar te zijn en buiten kantooruren binnen drie uur op dit onderwerp. (Conform de betreffende Deelnemersovereenkomsten)
A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging	✓	✓	✓	Elke medewerker van de deelnemers en de beheerorganisatie die werkzaamheden verricht gerelateerd aan MedMij dient onderwezen te worden over de algemene werking van het stelsel en op de voor hem/haar van toepassing zijnde beveiligingsmaatregelen. Deze training wordt door de beheerorganisatie beheert en gefaciliteerd. Deelname aan deze training is verplicht.

A.8.2.1 Classificatie van informatie	✓	✓	✓	Classificatie van gegevens die binnen het stelsel worden uitgewisseld (gezondheidsgegevens, metagegevens, operationele gegevens) worden door MedMij geclassificeerd conform het Informatieclassificatiebeleid.
A.9.1.1 Beleid voor toegangsbeveiliging	✓	✓	✓	Het inzien van persoonlijke gezondheidsgegevens door (medewerkers van) deelnemers en door de beheerorganisatie is niet toegestaan. Er dienen passende technische maatregelen te worden genomen om dit te voorkomen en te kunnen controleren. Indien dit (tijdelijk) wel noodzakelijk is (geweest) dient dit gelogd en verantwoord te worden, zodat dit gemeld kan worden aan de persoon en de beheerorganisatie (indien van toepassing).
A.9.2.5 Beoordeling van toegangsrechten van gebruikers	✓	✓	✓	De (medewerkers van) deelnemers en de beheerorganisatie kunnen enkel toegang krijgen tot systemen die persoonlijke gezondheidsgegevens opslaan of verwerken na authenticatie op basis van twee factoren. *Let op: Het betreft toegang tot systemen, geen toegang tot de persoonlijke gezondheidsgegevens zelf.* Toegangsrechten en het gebruik daarvan op systemen waar persoonlijke gezondheidsgegevens worden opgeslagen of worden verwerkt dienen maandelijks gecontroleerd te worden door een functionaris die onafhankelijk is van de personen die rechten toekennen.
A.9.4.1 Beperking toegang tot informatie	✓	✓		Gebruikers kunnen enkel toegang krijgen tot persoonlijke gezondheidsgegevens na authenticatie op basis van twee factoren.

A.5.1.1 Beleidsregels voor informatiebeveiliging

Norm

Rationale	Deze maatregel borgt dat beleidsdocumenten van alle partijen in lijn zijn met het Afsprakenstelsel.
Implementatie	De beleidsdocumenten van deelnemers dienen de beleidsmaatregelen die van toepassing zijn op MedMij (onder andere gespecificeerd in Privacy- en informatiebeveiligingsbeleid) specifiek te benoemen.
Toetsing	Door middel van interviews en het tonen van evidence (beleidsdocumenten).
NEN 7510: 2017	A.5.1.1 Beleidsregels voor informatiebeveiliging
NEN 7510: 2011	A.5.1.1 Beleidsdocument voor informatiebeveiliging

Rollen

DVP	✔
DVZA	✔
BO	✔

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

A.6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging

Norm

Rationale	Deze maatregel borgt dat bij (dreiging van) calamiteiten door alle partijen daadkrachtig kan worden gereageerd. Zie ook A.12.4.1 Gebeurtenissen registreren en A.16.1.1 Verantwoordelijkheden en procedures.
Implementatie	Elke deelnemer en de beheerorganisatie dient een deskundige verantwoordelijke, met mandaat om besluiten te nemen ten aanzien van MedMij, aan te wijzen als contactpersoon voor alle zaken met betrekking tot informatiebeveiliging. De organisatie dient tijdens kantooruren binnen een uur beschikbaar te zijn en buiten kantooruren binnen drie uur op dit onderwerp. (Conform de betreffende Deelnemersovereenkomsten)
Toetsing	Stel vast dat er overeenkomstige rollen zijn ingevuld en dat de vereiste bereikbaarheid geborgd is.
NEN 7510: 2017	A.6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging
NEN 7510: 2011	A.6.1.3 Toewijzing van verantwoordelijkheden voor informatiebeveiliging A.8.1.1 Rollen en verantwoordelijkheden

Rollen

DVP	✔
DVZA	✔
BO	✔

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

A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

e

Norm

Rationale	Deze maatregel borgt dat medewerkers zich bewust zijn van de werking van MedMij en de ketenverantwoordelijkheden.
Implementatie	Elke medewerker van de deelnemers en de beheerorganisatie die werkzaamheden verricht gerelateerd aan MedMij dient onderwezen te worden over de algemene werking van het stelsel en op de voor hem/haar van toepassing zijnde beveiligingsmaatregelen. Deze training wordt door de beheerorganisatie beheert en gefaciliteerd. Deelname aan deze training is verplicht.
Toetsing	Stel vast dat de partij deel heeft genomen aan de training van MedMij en dat relevante medewerkers over de noodzakelijke kennis beschikken.
NEN 7510: 2017	A.7.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging
NEN 7510: 2011	A.8.2.2 Bewustzijn, opleiding en training ten aanzien van informatiebeveiliging

Rollen

DVP	✔
DVZA	✔
BO	✔

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

A.8.2.1 Classificatie van informatie

Norm

Rationale	Deze maatregel borgt dat informatie die binnen het stelsel wordt gebruikt, door deelnemers met dezelfde voorzichtigheid wordt behandeld. Het gaat hier met name om (zeer) vertrouwelijke informatie, zoals risicoanalyses, pentestrapporten en de whitelist.
Implementatie	Classificatie van gegevens die binnen het stelsel worden uitgewisseld (gezondheidsgegevens, metagegevens, operationele gegevens) worden door MedMij geclassificeerd conform het Informatieclassificatiebeleid.
Toetsing	Door middel van interviews en/of het tonen van evidence (zoals het informatieclassificatieschema of -beleid van de partij).
NEN 7510: 2017	A.8.2.1 Classificatie van informatie
NEN 7510: 2011	A.7.2.1 Richtlijnen voor classificatie

Rollen

DVP	✔
DVZA	✔
BO	✔

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

A.9.1.1 Beleid voor toegangsbeveiliging

Norm

Rationale	Deze maatregel borgt dat persoonlijke gezondheidsgegevens alleen toegankelijk zijn voor de zorgaanbieder en de zorggebruiker (zie ook A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen).
Implementatie	Het inzien van persoonlijke gezondheidsgegevens door (medewerkers van) deelnemers en door de beheerorganisatie is niet toegestaan. Er dienen passende technische maatregelen te worden genomen om dit te voorkomen en te kunnen controleren. Indien dit (tijdelijk) wel noodzakelijk is (geweest) dient dit gelogd en verantwoord te worden, zodat dit gemeld kan worden aan de persoon en de beheerorganisatie (indien van toepassing).
Toetsing	Stel vast dat het technisch onmogelijk is gemaakt dat (medewerkers van) partijen zich zonder notificatie inzage kunnen verschaffen in persoonlijke gezondheidsgegevens en dat er een proces bestaat om afwijkingen te loggen, verantwoorden en te melden.
NEN 7510: 2017	A.9.1.1 Beleid voor toegangsbeveiliging
NEN 7510: 2011	A.11.1.1 Toegangsbeleid

Rollen

DVP	✔
DVZA	✔
BO	✔

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

A.9.2.5 Beoordeling van toegangsrechten van gebruikers

Norm

Rationale	Deze maatregel borgt dat partijen regelmatig controleren of alleen gerechtigde gebruikers toegang hebben tot systemen.
Implementatie	De (medewerkers van) deelnemers en de beheerorganisatie kunnen enkel toegang krijgen tot systemen die persoonlijke gezondheidsgegevens opslaan of verwerken na authenticatie op basis van twee factoren. *Let op: Het betreft toegang tot systemen, geen toegang tot de persoonlijke gezondheidsgegevens zelf.* Toegangsrechten en het gebruik daarvan op systemen waar persoonlijke gezondheidsgegevens worden opgeslagen of worden verwerkt dienen maandelijks gecontroleerd te worden door een functionaris die onafhankelijk is van de personen die rechten toekennen.
Toetsing	Stel vast dat de partij toegangsrechten (en het gebruik daarvan) op systemen waar persoonlijke gezondheidsgegevens worden opgeslagen of verwerkt, periodiek controleert.
NEN 7510: 2017	A.9.2.5 Beoordeling van toegangsrechten van gebruikers
NEN 7510: 2011	A.11.2.4 Beoordeling van toegangsrechten van gebruikers

Rollen

DVP	✔
DVZA	✔
BO	✔

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

A.9.4.1 Beperking toegang tot informatie

Norm

Rationale	Deze maatregel borgt dat gebruikers alleen toegang kunnen krijgen tot persoonlijke gegevens na een betrouwbare authenticatie, alleen een gebruikersnaam en wachtwoord is niet veilig genoeg.
Implementatie	Gebruikers kunnen enkel toegang krijgen tot persoonlijke gezondheidsgegevens na authenticatie op basis van twee factoren.
Toetsing	Stel door middel van technische documentatie en de werking vast dat twee factor authenticatie wordt toegepast.
NEN 7510: 2017	A.9.4.1 Beperking toegang tot informatie
NEN 7510: 2011	A.11.5.2 Gebruikersindentificatie en -authenticatie

Rollen

DVP	✔
DVZA	✔
BO	

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

A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen

Norm

Rationale	Deze maatregel borgt dat bij het versleutelen van persoonlijke gezondheidsgegevens gebruik wordt gemaakt van als veilig aangemerkte algoritmen.
Implementatie	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 ENCRYPT-CSA aanbevelingen, zie hieronder. *Een overzicht van publicaties is te vinden op https://www.keylength.com/ Er kan gebruik gemaakt worden van de ENCRYPT-CSA aanbevelingen en/of die van het BSI*
Toetsing	Dit kan worden aangetoond door het tonen van architectuurdiagrammen, waar de auditor door middel van steekproeven moet laten aantonen dat op die punten is voldaan aan de gestelde eisen. Aantonen kan plaatsvinden door middel van uitleg of door het tonen van evidence.
NEN 7510: 2017	A.10.1.1 Beleid inzake het gebruik van cryptografische beheersmaatregelen
NEN 7510: 2011	A.12.3.1 Beleid voor het gebruik van cryptografische beheersmaatregelen

Rollen

DVP	✔
DVZA	✔
BO	

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

A.12.1.2 Wijzigingsbeheer

Norm

Rationale	Deze maatregel borgt dat wijzigingen binnen de keten beheerst verlopen. Zie ook A. 12.5.1 Software installeren op operationele systemen.
Implementatie	Er is overkoepelend Change- en releasebeleid gedefinieerd om wijzigingen aan functionele-, operationele- en beveiligingseigenschappen te ontwerpen, testen, communiceren en te implementeren. Deelnemers en de beheerorganisatie dienen aan te sluiten op dit proces en wijzigingen de mogelijk impact hebben op het functioneren van het stelsel conform dit proces af te handelen.
Toetsing	Dit kan worden aangetoond door het volgen van een recente change/release, of door het aantonen van de raakvlakken van de eigen processen voor wijzigingsbeheer met die van het afsprakenstelsel.
NEN 7510: 2017	A.12.1.2 Wijzigingsbeheer
NEN 7510: 2011	A.10.1.2 Wijzigingsbeheer

Rollen

DVP	✔
DVZA	✔
BO	✔

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

A.12.1.3 Capaciteitsbeheer

Norm

Rationale	Deze maatregel borgt dat alle systemen in de keten voldoen aan de afgesproken eisen omtrent beschikbaarheid.
Implementatie	• Beschikbaarheid voor **deelnemers** zijn vastgelegd in Gegevens en performance in UCI Verzamelen en UCI Delen. • Beschikbaarheid voor de **beheerorganisatie** zijn vastgelegd in Gegevens en performance inzake opvragen lijsten.
Toetsing	Partijen kunnen dit aantonen door middel van eigen rapportages/metingen.
NEN 7510: 2017	A.12.1.3 Capaciteitsbeheer
NEN 7510: 2011	A.10.3.1 Capaciteitsbeheer

Rollen

DVP	✔
DVZA	✔
BO	✔

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

A.12.3.1 Back-up van informatie

Norm

Rationale	Deze maatregel borgt dat deelnemers beschikken over een bruikbare back-up.
Implementatie	De dienstverlener persoon dient een backupschema in plaats te hebben met bijbehorende (minimaal jaarlijks geteste) recovery procedures die ervoor zorgen dat de gegevens van de persoon binnen een dag (24u) terug kunnen worden geplaatst in geval van een incident.
Toetsing	Dit kan worden aangetoond door het aantonen van de raakvlakken van de eigen backup-policy met die van het afsprakenstelsel.
NEN 7510: 2017	A.12.3.1 Back-up van informatie
NEN 7510: 2011	A.10.5.1 Reservekopieën (back-ups)

Rollen

DVP	✔
DVZA	✔
BO	

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

A.12.4.1 Gebeurtenissen registreren

Norm

Rationale	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.
Implementatie	1. Logging moet plaatsvinden zoals gespecificeerd in het afsprakenstelsel (zie Processen en informatie onder Logging) 2. Verzoeken en toestemmingsverklaring van gebruikers ten aanzien van het opvragen van informatie bij zorgaanbieders dienen onweerlegbaar en controleerbaar te worden vastgelegd.
Toetsing	1. Dit kan worden aangetoond door het tonen van logbestanden van alle systemen waar gezondheidsgegevens zijn opgeslagen of worden verwerkt, waarbij specifiek moet worden gelet op de zaken die in het afsprakenstelsel worden gespecificeerd. 2. Dit kan worden aangetoond door het tonen van een registratie van dergelijke verzoeken.
NEN 7510: 2017	A.12.4.1 Gebeurtenissen registreren
NEN 7510: 2011	A.10.10.1 Aanmaken audit-logbestanden A.10.10.2 Controle van systeemgebruik

Rollen

DVP	✔
DVZA	✔
BO	✔

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

A.12.4.4 Kloksynchronisatie

Norm

Rationale	Deze maatregel borgt dat tijdsvermeldingen in logbestanden gelijklopen, wanneer deze worden gebruikt om misbruik in de keten op te sporen. Zie ook A.16.1.7 Verzamelen van bewijsmateriaal.
Implementatie	De klokken van alle relevante informatieverwerkende systemen binnen een organisatie of beveiligingsdomein moeten worden gesynchroniseerd met **pool.ntp.org**. Het is toegestaan te synchroniseren met een lokale NTP-server, zolang deze ten minste één keer per 24 uur synchroniseert met bovengenoemde NTP-server.
Toetsing	Dit kan worden aangetoond door configuratie of logging van synchronisatie met de genoemde NTP-server.
NEN 7510: 2017	A.12.4.4 Kloksynchronisatie
NEN 7510: 2011	A.10.10.6 Synchronisatie van systeemklokken

Rollen

DVP	✔
DVZA	✔
BO	✔

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

A.12.5.1 Software installeren op operationele systemen

Norm

Rationale	Deze maatregel borgt dat er altijd twee medewerkers betrokken zijn bij werkzaamheden aan systemen (configuratiewijzigingen, onderhoud, installatie van updates) en vermindert het risico op onbeschikbaarheid van de keten.
Implementatie	Het uitvoeren van handelingen op systemen en gegevens die direct impact (kunnen) hebben op de beschikbaarheid, integriteit of vertrouwelijkheid van de keten, dienen op basis van het vier-ogen-principe te worden uitgevoerd.
Toetsing	Dit kan worden aangetoond door het tonen van procedures en door interviews met verantwoordelijke medewerkers.
NEN 7510: 2017	A.12.5.1 Software installeren op operationele systemen
NEN 7510: 2011	A.12.4.1 Beheersing van operationele programmatuur

Rollen

DVP	✔
DVZA	✔
BO	✔

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

A.12.6.1 Beheer van technische kwetsbaarheden

Norm

Rationale	Deze maatregel borgt dat deelnemers in staat zijn tijdig te reageren op meldingen van (vermeende) kwetsbaarheden in het MedMij stelsel. Reageren kan bestaan uit: 1. Het onderzoeken of een (vermeende) kwetsbaarheid relevant is voor de eigen systemen 2. Hierover terugkoppelen 3. Het patchen van systemen (zie A.12.5.1 Software installeren op operationele systemen) Zie ook A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging.
Implementatie	Deelnemers dienen aan te sluiten bij het proces van beheren van technische kwetsbaarheden in het afsprakenstelsel (Operationele processen).
Toetsing	Dit kan worden aangetoond door middel van interviews en door het tonen van processen.
NEN 7510: 2017	A.12.6.1 Beheer van technische kwetsbaarheden
NEN 7510: 2011	A.12.6.1 Beheersing van technische kwetsbaarheden

Rollen

DVP	✔
DVZA	✔
BO	✔

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

A.14.2.1 Beleid voor beveiligd ontwikkelen

Norm

Rationale	Deze maatregel borgt dat deelnemers en beheerorganisatie beveiligingsstandaarden toepassen bij het ontwikkelen van software en systemen die aan het internet gekoppeld worden, om te voorkomen dat bekende programmeerfouten worden gemaakt.
Implementatie	Er moeten door de deelnemers beveiligingsstandaarden worden toegepast in de ontwikkelde internet facing applicaties. Minimale beveiligingsstandaarden waaraan alle ontwikkelde applicaties van deelnemers moeten voldoen: 1. Voor webapplicaties worden de ICT- Beveiligingsrichtlijnen voor webapplicaties van het NCSC gehanteerd. In het bijzonder zijn dan de maatregelen uit het "Uitvoeringsdomein" van belang, https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html. 2. Voor mobiele applicaties kan worden gesteund op richtlijnen van het NCSC hiervoor: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-mobiele-apps.html.
Toetsing	Door middel van interviews en het tonen van evidence kan worden vastgesteld of het beleid voor beveiligd ontwikkelen van de partij voldoet aan de eisen die het afsprakenstelsel stelt.
NEN 7510: 2011	Deze maatregel bestond nog niet in NEN 7510:2011

Rollen

DVP	✔
DVZA	✔
BO	✔

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

A.16.1.1 Verantwoordelijkheden en procedures

Norm

Rationale	Deze maatregel borgt dat deelnemers en beheerorganisatie volgens hetzelfde proces handelen in geval van incidenten en calamiteiten. Zie ook A.6.1.1 Rollen en verantwoordelijkheden bij informatiebeveiliging.
Implementatie	Deelnemers moeten aansluiten bij het proces voor incidenten en calamiteiten zoals dit is gedefinieerd in het afsprakenstelsel (Operationele processen).
Toetsing	Door middel van interviews en het tonen van evidence, zoals het incidentenproces van de deelnemer.
NEN 7510: 2017	A.16.1.1 Verantwoordelijkheden en procedures
NEN 7510: 2011	A.13.2.1 Verantwoordelijkheden en procedures

Rollen

DVP	✔
DVZA	✔
BO	✔

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

A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging

Norm

Rationale	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.12.6.1 Beheer van technische kwetsbaarheden.
Implementatie	Er is een meldplicht voor alle deelnemers en de beheerorganisatie om incidenten die betrekking hebben op persoonlijke gezondheidsgegevens of het functioneren van het MedMij stelsel onmiddellijk te melden bij centrale incident management team. Zie Deelnemersovereenkomsten.
Toetsing	Stel vast dat medewerkers op de hoogte zijn van deze eis door middel van interviews of het tonen van beleidsdocument en/of processen.
NEN 7510: 2017	A.16.1.3 Rapportage van zwakke plekken in de informatiebeveiliging
NEN 7510: 2011	A.13.1.2 Rapportage van zwakke plekken in de beveiliging

Rollen

DVP	✔
DVZA	✔
BO	✔

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

A.16.1.7 Verzamelen van bewijsmateriaal

Norm

Rationale	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.12.4.1 Gebeurtenissen registreren).
Implementatie	Deelnemers en de beheerorganisatie dienen medewerking te verlenen aan (forensische) onderzoeken, door het aanleveren van gevraagde bewijsmaterialen, zulks op verzoek van de beheerorganisatie of bevoegde instanties.
Toetsing	Door middel van interviews en het tonen van evidence, zoals processen of beleidsdocumenten.
NEN 7510: 2017	A.16.1.7 Verzamelen van bewijsmateriaal
NEN 7510: 2011	A.13.2.3 Verzamelen van bewijsmateriaal

Rollen

DVP	✔
DVZA	✔
BO	✔

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

A.18.2.3 Beoordeling van technische naleving

Norm

Rationale	Deze maatregel borgt dat deelnemers en de beheerorganisatie met regelmaat (en gebruikmakend van verschillende partijen) hun software en systemen laten toetsen op bekende kwetsbaarheden.
Implementatie	1. Tenminste jaarlijks laten de deelnemers en de beheerorganisatie **whitebox** applicatiepenetratietesten en code reviews uitvoeren op de externe koppelvlakken. Bij toetreding hebben deze minimaal al een keer plaatsgevonden. *Non-conformiteiten* worden gemeld bij de beheerorganisatie. 2. Tenminste jaarlijks laat de beheerorganisatie **blackbox** infrastructuur penetratietesten uitvoeren op de externe koppelvlakken van de deelnemers ten behoeve van het MedMij stelsel.
Toetsing	Door middel van interviews en het tonen van evidence (auditrapporten).
NEN 7510: 2017	A.18.2.3 Beoordeling van technische naleving
NEN 7510: 2011	A.15.2.2 Controle op technische naleving

Rollen

DVP	✔
DVZA	✔
BO	✔

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

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. Indien de situatie daarom vraagt, mag de beheerorganisatie na belangenafweging afwijken van het beleid.

Change- en releasebeleid

Het MedMij Afsprakenstelsel is dynamisch van aard. 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. De uitvoeringsorganisatie 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 de uitvoeringsorganisatie samen met de verschillende belanghebbenden een releaseplanning. 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 van Stichting MedMij. Het bestuur van Stichting MedMij stelt de releaseplanning vast.

Totstandkoming releases

Alle belanghebbenden, waaronder in ieder geval de deelnemers, gebruikers en de beheerorganisatie, 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. De uitvoeringsorganisatie doet een eerste beoordeling van ingediende RFC's door deze te toetsen aan de vigerende wet- en regelgeving, architectuur en grondslagen, strategische koers van MedMij, 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. De uitvoeringsorganisatie 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 controleren 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 dient de uitvoeringsorganisatie erop toe te zien dat Stichting MedMij 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 gereleaset. Deze releases bestaan uit een samenhangende set van RFC's en kunnen daarnaast verbeteringen van niet-inhoudelijke aard bevatten. Per release wordt een implementatieparagraaf toegevoegd die uiteenzet op welke manier een release moet worden geïmplementeerd.

Verschillende typen releases

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:
    1. Wijzigingen die nodig zijn om een onmiddellijke dreiging voor de continuïteit van of het vertrouwen in het MedMij Afsprakenstelsel/-netwerk af te wenden;
    2. 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).

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, moet de release worden ingevoerd. Nieuwe releases worden op gestructureerde wijze in het MedMij-netwerk geïmplementeerd. Per release wordt in overleg met de deelnemers en eigenaren bepaald welke aanpak de minste impact/verstoringen veroorzaakt. Ook wordt de afweging gemaakt of releases in productie naast elkaar kunnen bestaan en of deelnemers op enig moment meerdere releases moeten ondersteunen. De gekozen aanpak wordt gepland en volgens deze planning uitgevoerd. 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.

De uitvoeringsorganisatie 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 de uitvoeringsorganisatie 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 aanbieden van een Gegevensdienst namens die Zorgaanbieder van een andere Dienstverlener zorgaanbieder overnemen. Deze overnemende Dienstverlener zorgaanbieder moet in dat geval erkend zijn als aanbieder voor die gegevensdienst en bij de uitvoeringsorganisatie 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 bieden via MedMij gestandaardiseerde diensten voor gegevensuitwisseling aan, de zogeheten gegevensdiensten. Deze gegevensdiensten worden uitgewisseld via bijbehorende use cases uit de architectuur van het 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 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. De uitvoeringsorganisatie 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 aanbieder van een gegevensdienst

Deelnemers bieden gegevensdiensten aan 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 is in de catalogus aangegeven 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. De uitvoeringsorganisatie ziet erop toe dat aan alle voorwaarden wordt voldaan, alvorens erkenningen wordt afgegeven.

Mutaties van gegevensdiensten

De volgende mutaties zijn toegestaan binnen bestaande gegevensdiensten:

- Wijzigingen in de gegevensdienstnaam of weergavenaam;
- Wijzigingen in de verzameling andere gegevensdiensten die door de gegevensdienst vereist worden;
- Wijzigingen door het instellen van een einddatum of het wijzigen van een geldigheidsperiode.

Aanvullende informatie over doorgevoerde mutaties wordt bij publicatie van een nieuwe versie van de Catalogus opgenomen.

Wijzigingen aan de systeemrolverzameling of de specificaties van een systeemrol van een gegevensdienst, kunnen alleen worden doorgevoerd door een nieuwe gegevensdienst te creëren en te bepalen of en wanneer de oude gegevensdienst wordt uitgefaseerd. Wijzigingen aan een informatiestandaard geven aanleiding tot dit soort wijzigingen en lopen via een mutatie van het Register van Informatiestandaarden. Besluiten over mutaties van het Register van Informatiestandaarden lopen via het bestuur van Stichting MedMij.

Uitfaseren van gegevensdiensten

De volgende triggers kunnen leiden tot het uitfaseren 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, de uitvoeringsorganisatie 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 behoeft 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.

		Classificatie van zekerheidsaspecten		
MedMij-classificatie	**Type informatie**	**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 afsprakenset.	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 afsprakenset, 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 Processen en informatie	Gezondheid
Alle gegevens verkregen of verstrekt in het kader van een van de interacties in het kader van de use cases uit de Architectuur en technische specificaties	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 Normenkader informatiebeveiliging, 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	Architectuur en technische specificaties: beschrijft de maatregelen om de uitwisseling van gezondheidsgegevens veilig en betrouwbaar te laten plaatsvinden. Normenkader informatiebeveiliging: 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. Deelnemersovereenkomsten: beschrijft de juridische bepalingen tussen Stichting MedMij en de deelnemers gericht op de privacy en (informatie)beveiliging van gezondheidsgegevens (artikel 5).
Operationele kern	Architectuur en technische specificaties: beschrijft de maatregelen om op veilige en betrouwbare wijze om te gaan met de operationele uitwisselgegevens. Normenkader informatiebeveiliging: 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.
Samenwerking en ontwikkeling	Change- en releasebeleid: beschrijft hoe met ontwikkelinformatie moet worden omgegaan bij de doorontwikkeling van het MedMij Afsprakenstelsel. Samenwerkings- en escalatiebeleid: beschrijft de onderlinge samenwerking en communicatie van partijen rondom het afsprakenstelsel.
Kwetsbaarheid	Privacy- en informatiebeveiligingsbeleid: beschrijft welke maatregelen zijn ingericht om de privacy- en informatiebeveiliging van het stelsel te borgen. Operationele processen: beschrijft met het Proces beheren technische kwetsbaarheden hoe met kwetsbaarheden wordt omgegaan.

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 preconcurrentiële 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 of de uitvoeringsorganisatie over de dienstverlening van een deelnemer, de uitvoeringsorganisatie of de stichting. 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 deelnemer(s) en de uitvoeringsorganisatie;
3. 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 de uitvoeringsorganisatie (zie Samenwerkings- en escalatiebeleid). De klachten en geschillen moeten gerelateerd zijn aan het niet-nakomen van de afspraken/deelnemersovereenkomst door een deelnemer, de uitvoeringsorganisatie 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. P artijen 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. De uitvoeringsorganisatie 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 de uitvoeringsorganisatie.

Nalevingsbeleid

Een goede naleving van het afsprakenstelsel is onontbeerlijk voor het vertrouwen in het stelsel. Zowel deelnemers, Stichting MedMij, de uitvoeringsorganisatie 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 partijen aan de afspraken blijven voldoen.

Signalen over het niet naleven van de afspraken door deelnemers komen via meerdere routes bij de beheerorganisatie binnen, waaronder bij:

- Een bemiddeling door de uitvoeringsorganisatie 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 aanbieder 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.** De uitvoeringsorganisatie beschrijft zo concreet mogelijk welke verplichting van het MedMij Afsprakenstelsel het betreft, alsmede wat de concrete omstandigheden van het geval zijn;
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 de uitvoeringsorganisatie 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 de uitvoeringsorganisatie en/of 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 de uitvoeringsorganisatie onder verantwoordelijkheid van Stichting MedMij. Besluiten over opschorting of uitsluiting van deelname lopen via Stichting MedMij.

Stichting MedMij en de uitvoeringsorganisatie gaan 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 de Stichting 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 de stichting 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 de uitvoeringsorganisatie. De uitvoeringsorganisatie stelt de naam vast in opdracht van Stichting MedMij.

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 in het verleden niet door een andere Dienstverlener persoon gebruikt zijn;
5. 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 (Gegevens en performance in UCI Verzamelen en UCI Delen). 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 (Gegevens en performance inzake opvragen lijsten).

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. De beheerorganisatie kan hierbij faciliteren en mediëren (zie ook Samenwerkings- en escalatiebeleid). Deelnemers gebruiken alle aanwezige logging, tevens naar redelijkheid, om een probleem te helpen oplossen.

Release 1.1

Om fouten in de eerste productieversie van het stelsel tijdig op te sporen, organiseert de uitvoeringsorganisatie 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. De uitvoeringsorganisatie en elke afzonderlijke deelnemer hebben een verantwoordelijke voor privacy en informatiebeveiliging in dienst (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 de uitvoeringsorganisatie 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, Stichting MedMij en de uitvoeringsorganisatie. 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 autorisatieprocollen);
2. Maatregelen voor risico's die kunnen leiden tot stelselrisico's (een gebeurtenis bij een deelnemer die schade toebrengt aan andere deelnemers, Stichting MedMij of de uitvoeringsorganisatie). 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 wijzingen 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 de uitvoeringsorganisatie (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, de beheerorganisatie of zorgaanbieders terecht komen, dienen deelnemers ook de volgende rol in te vullen:

- Een servicedesk bestaande uit minimaal één persoon als dagelijks aanspreekpunt voor gebruikers.

Deelnemers maken bij de uitvoeringsorganisatie kenbaar hoe de servicedesks en de servicemanager te bereiken zijn. Deze contactgegevens worden, voor de eerste maal tijdens het toetredingsproces, geregistreerd en gepubliceerd in een online samenwerkingsplatform voor deelnemers en uitvoeringsorganisatie.

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 servicedesksmedewerkers 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 de uitvoeringsorganisatie het escalatiekanaal. Namens en samen met de escalerende partijen zal de uitvoeringsorganisatie 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 aanbieden op de juiste manier te ondersteunen. De deelnemer doorloopt hiervoor bij toetreding en op zekere momenten tijdens deelname testen. Bij deze testen wordt niet de volledige implementatie van de deelnemer getoetst en het betreft niet primair een toets op de applicatie van de deelnemer. De testen zijn erop gericht om te bepalen of de deelnemer voldoende geëquipeerd is om de verantwoordelijkheden uit de architectuur en technische specificaties waar te maken en de gegevensdiensten op de juiste manier weet te hanteren. De tests vinden risico-gebaseerd plaats en focussen zich primair op de interoperabiliteit tussen deelnemers en de cruciale maatregelen voor het vertrouwen in MedMij.

Wanneer moet er getest worden? We onderscheiden de volgende situaties:

1. De deelnemer wil erkend worden als aanbieder van een gegevensdienst;
2. Wijzigingen aan de Architectuur en technische specificaties (verplichte hertest volgt in dat geval uit de implementatieparagraaf, zie Change- en releasebeleid);
3. Twijfel over de naleving van de afspraken;
4. Hertoetreding als bedoeld in artikel 14.3 van de Deelnemersovereenkomst.

Situatie 1: De deelnemer wil erkend worden als aanbieder 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:

	Scope van de test (relevante use cases)	
Usecase behorende bij de Gegevensdienst	**DVP**	**DVZA**
Verzamelen	UCI Verzamelen UCI Opvragen ZAL UCI Opvragen GNL	UCI Verzamelen UCI Opvragen OCL UCI Opvragen GNL
Delen	UCI Delen UCI Opvragen ZAL UCI Opvragen GNL	UCI Delen UCI Opvragen OCL UCI Opvragen GNL

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.

Tijdelijke verwijzing (Register van Informatiestandaarden is nog niet gepubliceerd)

Op de volgende pagina heeft Nictiz voor haar standaarden beschreven om welke aanvullende inspanningen het gaat.

De deelnemer kan zich voorbereiden op testen (A) en (B) in een testomgeving aangeboden door de beheerorganisatie. 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 aanbieder voor een nieuwe gegevensdienst.

Situaties 2 t/m 4

Voor situaties 2 t/m 4 geldt dat er per situatie wordt 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.

Wie kiest de zorgaanbiedersnaam?

De zorgaanbieder bepaalt de gekozen naam en de Dienstverlener zorgaanbieder geeft deze naam door aan de uitvoeringsorganisatie. De uitvoeringsorganisatie stelt de naam in opdracht van Stichting MedMij vast. Het is de verantwoordelijkheid van de Dienstverlener zorgaanbieder om de Zorgaanbieder te informeren over de context en het doel van de naam binnen MedMij.

Waar moet de zorgaanbiedersnaam aan voldoen?

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 50 karakters lang (exclusief `@medmij`);
7. De naam wordt geregistreerd in kleine letters;
8. De naam mag alleen bestaan uit karakters die voorkomen in het Nederlandse alfabet (bestaande uit zesentwintig letters). Diakrieten, speciale tekens (zoals spatie, koppelteken en punt) zijn dus niet toegestaan;
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.

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 voor (potentiële) deelnemers beschikbaar bij de uitvoeringsorganisatie.

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 uitvoeringsorganisatie constateert een incident/calamiteit.
- **Afspraken over het proces:**
  - In de nadere uitwerking van het proces bij de uitvoeringsorganisatie wordt gedefinieerd wat een incident en calamiteit is in het kader van MedMij. De procesafspraken hebben hier betrekking op.
  - Deelnemers en uitvoeringsorganisatie 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 uitvoeringsorganisatie dienen zo spoedig mogelijk de benodigde acties uit te zetten om een incident of calamiteit op te lossen.
  - Uitvoeringsorganisatie 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 de uitvoeringsorganisatie hebben alle één persoon binnen de eigen organisatie aangewezen als eindverantwoordelijke en centraal contactpersoon voor informatiebeveiligingsincidenten en -calamiteiten (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 de uitvoeringsorganisatie (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 uitvoeringsorganisatie constateert een kwetsbaarheid.
- **Afspraken over het proces:**
  - Deelnemers en uitvoeringsorganisatie zijn verplicht elkaar te informeren over voor MedMij relevante kwetsbaarheden.
  - Uitvoeringsorganisatie 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 stelsel (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 aanbieder van gegevensdienst

- **Doel:** Het proces erkenning van deelnemer als aanbieder van gegevensdienst heeft als doel te toetsen of de deelnemer een gegevensdienst op de juiste wijze ondersteunt.
- **Initiatie:** Deelnemer wil een gegevensdienst aanbieden.
- **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).
  - Uitvoeringsorganisatie 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 bij de uitvoeringsorganisatie te laten zien (zie Testbeleid).
  - Uitvoeringsorganisatie bepaalt of deelnemer eerst erkend moet worden als aanbieder van andere gegevensdiensten, omdat de gegevensdienst dit vereist (zie Gegevensdienstenbeleid). Indien het geval, dan dient eerst de erkenning als aanbieder van de vereiste gegevensdienst behaald te worden.
- **Resultaat:** Deelnemer is erkend als aanbieder van een gegevensdienst. Uitvoeringsorganisatie initieert het Registratieproces aanbod gegevensdiensten door deelnemer.
- **Uitzonderingen:** Deelnemer voldoet niet aan de vereisten voor de gegevensdienst en wordt niet erkend als aanbieder.

Registratieproces aanbod gegevensdiensten door deelnemer

- **Doel:** Het registratieproces aanbod gegevensdiensten door deelnemer heeft als doel de juiste informatie vast te leggen over het aanbod van gegevensdiensten door de deelnemer.
- **Initiatie:**
  - Deelnemer is erkend voor een gegevensdienst en mag deze aanbieden.
  - Deelnemer wil een gegevensdienst niet meer aanbieden.
  - Deelnemer mag een gegevensdienst niet meer aanbieden op grond van falende herkwalificatie of -acceptatie.
- **Afspraken over het proces:**
  - Uitvoeringsorganisatie 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:** De uitvoeringsorganisatie 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 de uitvoeringsorganisatie 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:
      - Deelnemer wil in het MedMij-netwerk kenbaar maken een gegevensdienst voor een zorgaanbieder aan te bieden.

        - Deelnemer wil in het MedMij-netwerk kenbaar maken een gegevensdienst voor een zorgaanbieder niet meer aan te bieden.
        - Deelnemer 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 OAuthclients toevoegen.
        - Dienstverlener persoon wil een OAuthclient verwijderen.
        - Dienstverlener persoon wil een gebruiksvriendelijke naam opgeven bij een eigen OAuthclient.
        - Dienstverlener persoon wil de gebruiksvriendelijke naam aanpassen bij een eigen OAuthclient.
- **Afspraken over het proces:**
    - Deelnemer is verantwoordelijk voor het aanleveren van mutaties voor de Zorgaanbiederslijst, WhiteList en OAuthclientlist.
    - Mutaties zijn gebonden aan de verantwoordelijkheden en regels zoals gespecificeerd in de Architectuur en technische specificaties, het Zorgaanbiedersnamenbeleid en OAuthclient-namenbeleid.
    - Uitvoeringsorganisatie neemt het verzoek in behandeling en is verantwoordelijk voor een check op integriteit.
    - Valide mutaties worden in 95 procent van de gevallen door de uitvoeringsorganisatie binnen 2 werkdagen verwerkt. Urgente mutaties krijgen daarbij voorrang. De mutatietijd voor urgente mutaties wordt in overleg met de uitvoeringsorganisatie bepaald. Bij verwachte overschrijding van de (overeengekomen) verwerkingstijd, informeert de uitvoeringsorganisatie de deelnemer hierover.
- **Resultaat:** De uitvoeringsorganisatie 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. Uitvoeringsorganisatie vraagt de deelnemer om het verzoek aan te passen.

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.
    - Uitvoeringsorganisatie 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. De uitvoeringsorganisatie 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).
  - Uitvoeringsorganisatie voert de benodigde mutaties door in het deelnemersregister en de relevante lijsten.
- **Resultaat:** Deelnemer is uitgetreden uit het afsprakenstelsel.
- **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 afsprakenset houdt rekening met deze diversiteit en maakt het mogelijk om met een relatief beperkte afsprakenset uitwisseling tussen deze systemen vorm te geven. MedMij heeft niet als doel om met de afsprakenset 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. Profilering 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 aanbieden).

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: Profilering 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 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 dit scherm en de variabelen hierin volgens de instructies bij Gegevens en performance in UCI Verzamelen en UCI Delen te implementeren. De HTML- en CSS-bestanden om het scherm te kunnen gebruiken, zijn als bijlage toegevoegd aan deze pagina (MedMij toestemmings- en bevestigingsscherm.zip).

MedMij
veilig online uitwisselen van gezondheidsgegevens

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

MedMij
veilig online uitwisselen van gezondheidsgegevens

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.

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 dit scherm en de variabelen hierin volgens de instructies bij Gegevens en performance in UCI Verzamelen en UCI Delen te implementeren. De HTML- en CSS-bestanden om het scherm te kunnen gebruiken, zijn als bijlage toegevoegd aan deze pagina (MedMij toestemmings- en bevestigingsscherm.zip).

MedMij
veilig online uitwisselen van gezondheidsgegevens
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

MedMij
veilig online uitwisselen van gezondheidsgegevens
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
zondheidsomgeving via MedMij aan uw zorgaanbieder wordt toegezonden. Het is aan NaamZorgaanbieder om te beoordelen of hij de

Managementinformatie

Om het gebruik van MedMij inzichtelijk te maken, leveren de Dienstverleners persoon maandelijks managementinformatie aan bij de uitvoeringsorganisatie. Deze informatie wordt geaggregeerd tot een managementrapportage voor de stichting en de deelnemers. Concurrentiegevoelige informatie wordt hierbij zoveel mogelijk weggehaald. Het betreft de volgende informatie:

- Aantal aangesloten personen;
- Aantal actieve gebruikers: minimaal één keer al dan niet succesvol gegevens hebben opgevraagd;
- Aantal actieve gebruikers: minimaal één keer al dan niet succesvol gegevens hebben gedeeld;
- Per gegevensdienst (indien van toepassing: een gegevensdienst is in de praktijk verbonden aan hetzij UC Verzamelen, hetzij UC Delen):
    - Aantal keer succesvol verzameld (succesvol afgeronde UC Verzamelen);
    - Aantal keer onsuccesvol verzameld (niet afgeronde UC Verzamelen);
    - Aantal keer succesvol gedeeld (succesvol afgeronde UC Delen);
    - Aantal keer onsuccesvol gedeeld (niet afgeronde UC Delen).

Aan de managementrapportage voegt de uitvoeringsorganisatie informatie toe over het gebruik door zorgaanbieders. Deze informatie wordt betrokken uit MedMij Registratie.

Toelichtingen afsprakenset release 1.1

Toelichting

De toelichtingen bij release 1.1 maken geen onderdeel uit van de formele afspraken, maar verduidelijken bestaande afspraken en dragen daarmee bij aan een eensluidende implementatie. Bij de eerstvolgende major release worden de toelichtingen geïntegreerd in de afsprakenset.

Applicatierollen 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;

- elk endpoint hetzij een *Authorization Endpoint*, hetzij een *Token Endpoint*, hetzij een *Resource Endpoint* 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 Serve*r 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. 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* aanbiedt. Zo blijft die integrale eindverantwoordelijk-heid ook op net-werk-niveau toetsbaar. Zie de drie (ingewikkelde) invarianten bij *Zorgaanbie-derGegevensdienst* 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 Zorgaanbie-der* voor de *Authorization Server* gebruik maken van eenzelfde onderaannemer. De host-names in de adressen van de *Authorization Endpoints* | *Token Endpoints* zullen dan evengoed ver-schillen tussen die twee eindverantwoordelijke *Dienstverleners Zorgaanbieders* , zelfs al zou er het zelfde *Authorization Server* -systeem achter zitten. Voor de *Zorgaanbiedergegevensdiensten* waar-voor *Dienstverlener Zorgaanbieder* A verant-woordelijk is, moet dat de hostname van een *Node* van A zijn; voor de *Zorgaanbieder-Gege-vensdiensten* waarvoor *Dienstverlener Zorgaan-bieder* 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.

Bedoeling van de beschikbaarheids- en de ontvankelijkheidstoets

De bedoeling van de beschikbaarheids- en de ontvankelijkheidstoets — onmiddellijk na de gebruikersauthenticatie in *UC(I) Verzamelen*, respectievelijk *UC(I) Delen* — is tweeledig.

1. De toetsen willen veilig stellen dat er zo snel mogelijk na de authenticatie van de persoon uitgegaan mag worden van het vervuld zijn van twee voorwaarden voor het ver-zamelen of delen van de betreffende informatie: het bestaan van een (eventueel voorbije) behan-del-relatie als grond-slag daarvoor en van een leeftijd van de persoon van minimaal zes-tien jaar. Het is de juri-dische eindverantwoordelijkheid van de zorgaanbieder deze voorwaar-den te (laten) verifiëren. Zie voor het aspect leeftijd verder het Juridisch kader.
2. Het geeft de zorgaanbieder de kans naar eigen bevinden extra beperkingen, structu-reel of incidenteel, op te leggen aan het laten verzamelen of delen van informatie, bijvoorbeeld om technische redenen of vanwege bijzondere situaties, bijzondere patiënten of aangrij-pende inhoud.

Een succesvol resultaat van de toets betekent dus dat de zorgaanbieder ervoor instaat dat de behandelrelatie aanwezig is en dat de leeftijd voldoende is. Hoe de zorgaanbieder dat geborgd heeft is vrij, zolang het eindresultaat maar is dat de zorgaanbieder ervoor kan in-staan. Aan die borging kunnen bijvoorbeeld bijdragen:

- juridische middelen, zoals bepalingen in de dienstverleningsovereenkomst tussen Zorg-aanbieder en Dienstverlener Zorgaanbieder;
- organisatorische maatregelen in de wijze waarop *Zorgaanbieders* het dossier beheren, zodat aan de dossierinfo, aan de ordening ervan, of zelfs aan de loutere aanwezigheid er-van, gezien kan worden of er een behandelrela-tie 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 speci-ficeert daarom geen logica voor de toetsen; het bepaalt slechts twee noodzakelijke onderdelen van hun post-conditie: een toereikende leeftijd van de *Persoon* en het (hebben) bestaan van een toepasselijke behandelrelatie.

Een negatief resultaat van de toets 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.

Er zijn twee hoofdredenen om de toets zo snel mogelijk uit te voeren, dat wil zeggen, onmid-dellijk na de authenticatie van de *Persoon* , nog voor de autorisatievraag (de vroege variant) en niet pas wan-neer de flow bij de *Resource Server* is aangekomen, mogelijk geïntegreerd met de uiteindelij-ke uit-vraag/plaatsing (de late variant). Die redenen zijn dataminimali-satie en gebrui-ksvriendelijkheid. Beide aspecten moeten vanuit het perspectief van de gehele use case en alle betrokken rollen beschouwd worden: de keuze tussen de vroege en de late variant heeft effecten op meerdere plaatsen. De afweging onderscheidt vier situaties, afhankelijk van twee vragen:

- Acht de *Zorgaanbieder* (zich voor) de informatie (uitein-delijk) beschikbaar/ontvankelijk?
- Geeft de *Persoon* (uiteinde-lijk) toestemming?

De twee varianten laten zich als volgt vergelijken inzake dataminimalisatie.

	(uiteindelijk) wel beschikbaar /ontvankelijk	**(uiteindelijk) niet beschikbaar/ontvankelijk**
(uiteindelijk) wel toestemming	• Voor zover er aparte geautoma-ti-seerde mid-de-len worden ge-bruikt voor de toets vraagt de vroege variant ex-tra ver-keer ten opzichte van de late variant, namelijk tussen *Autho-ri-zation Ser-ver* en de com-ponent-(en) die zij voor het uitvoe-ren van die toets aan-spreekt. Dat ver-keer speelt zich wel geheel binnen de verantwoordelijkheid van een enkele verwerkingsverantwoordelijke af; er vindt geen verstrekking plaats. • De *Authorization Server* komt alleen in de vroege variant extra te weten dat behandel-relatie en	• In de late variant vindt, in tegenstelling tot in de vroege, al het verkeer na de au-thenti-catie (de toe-stem-mingsvraag, het uit-de-len van authoriza-tion code en ac-cess to-ken en het aan-spreken van de *Resour-ce Ser-ver*) onnodig plaats. Dit verkeer strekt zich uit over verantwoordelijkheidsgrenzen. • In toevoeging op het vorige punt vindt er in het geval van de *UC(I) Delen* een overbodige uitwisseling en verwerking van medische informatie plaats. De *PGO Server* zal immers medische informatie aanbieden aan de *Resource Server* voordat deze alsnog te weten komt dat de *Zorgaanbieder* zich er niet ontvankelijk voor acht. • In de late variant krijgt de *PGO Server*, onnodig, meer over de beschikbaarheid/ontvankelijkheid,

	leef-tijd in orde zijn. In de late variant komt alleen de *Resource Server* dat te weten. Dat laat onverlet dat beide onder dezelfde eindverantwoordelijke *Dienstverlener Zorgaanbieder* vallen.	en dus over de *Persoon,* te weten van de *Resource Server* dan in de vroege variant van de *Authorization Server*. In de vroege variant kan de betreffende uitzondering immers, vanuit de *PGO Server* bezien, ook door falende authenticatie of weigering van toestemming veroorzaakt zijn. In de late variant komt de *PGO Server* echter wel te weten, door het ontvangen van de onnodige authorization code, dat er sprake is van zowel een behandelrelatie als een toereikende leeftijd.
(uiteinde-lijk) geen toestemming		In de late variant vindt, in tegenstelling tot in de vroege, een overbodige toe-stemmingsvraag 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	In de vroege variant is de persoon onmiddellijk op de hoogte, zodat deze: • geen onnodige en verwarrende handeling (holle toestemming) met rechtsgevolgen hoeft uit te voeren, zoals in de late variant; • 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 *Persoon* voor opheldering op ondersteuningsvragen aangewezen zou zijn, die wellicht zelfs aan de *Zorgaanbieder* gericht worden. In de vroege variant zijn Uitzonderingen 2, 3 en 4 in zowel *UC (I) Verzamelen* als *UC(I) Delen* weliswaar samengenomen in één melding naar de *PGO Server*, zodat deze het onderscheid tussen falende authenticatie, falende autorisatie en falende beschikbaarheid /ontvankelijkheid niet kan maken. De *Persoon* zelf echter kent vanwege zijn/haar voorafgaande rechtstreekse interactie met de *Authorization Server* het resultaat van de authenticatie en de autorisatie en kan dus alsnog uit deze gecombineerde melding, buiten medeweten van de *PGO Server*, afleiden of er sprake was van falende beschikbaarheid/toegankelijkheid.
(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/ontvan-kelijk 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.

De nadelen van de late variant wegen naar verhouding zwaar, omdat het extra verkeer zich voor een belangrijk deel over verantwoordelijkheidsgrenzen uitstrekt en omdat de *Persoon* onno-dige han-delingen (holle toestemming) met rechtsgevolgen moet plegen.

Daarom kiest het MedMij Afsprakenstelsel voor de vroege variant. Het zal afhangen van de specifieke inrichtingskeuzes van *Dienstverlener(s) Zorgaanbieder* welke mix van juridi-sche middelen, organisa-torische maatregelen en geautomatiseerde logica een afdoende en effi-ciënte vervulling van de postconditie van de toetsen oplevert.

Eisen van DigiD inzake uitloggen

Het MedMij Afsprakenstelsel brengt het gebruik van DigiD onder in de OAuth-flow, onder verant-woordelijkheid van de *Authorization Server*. Dat is in zoverre bijzonder dat de te authenti-ce-ren *Persoon* uiteindelijk niet de directe gebruiker is van de aanroeper van DigiD, zoals in veel gevallen van DigiD-gebruik, maar een indirecte gebruiker, namelijk door tussenkomst van de *PGO Server*. De directe interactie van de *Persoon* met de *Authorization Server* is bedoeld om de PGO Server daartoe te autoriseren. Deze indirectie kan vragen oproepen bij de interpretatie van enkele aansluiteisen van DigiD.

Ten eerste eist DigiD dat de eindgebruiker “gedurende de gebruikersessie” de ge-le-gen-heid houdt uit te loggen. Voor de *UC(I) Verzamelen* en *UC(I) Delen* strekt deze gebrui-kerssessie zich niet verder uit dan de *Authorization Server*. Daarna is immers de *Persoon* geen gebruiker meer van de *Authorization Server*, maar van de *PGO Server*, die op zijn beurt de gebruiker van de *Resource Server* is geworden, daartoe eerder door *Persoon* geautoriseerd. Tijdens de gebruikerssessie bij de *Authorization Server* is er boven-dien slechts één eindgebruikersinteractie, namelijk bij het voorleggen van de toestemmings-vraag. Het afwijzen van die toestemming door de *Per-soon* mag worden opgevat als uitlog-gen. Er zijn geen verdere uitlogvoorzieningen nodig.

Ten tweede stelt DigiD eisen aan de “DigiD-sessiegegevens” en de daarvan afgeleide gege-vens. Dat roept de vraag op om welke gegevens dat gaat en of de authorization code en het access token moeten wor-den opgevat als afgeleide gegevens. De reden voor deze eis is dat de bedoelde gegevens nodig zijn om weer uit te loggen, vooral in het geval van single sign-on. In de *UC(I) Verzamelen* en *UC(I) Delen* zijn deze gegevens echter niet nodig voor uitlog-gen. Überhaupt worden authoriza-tion code en access token niet als afgeleide gegevens opgevat.

Ten derde eist DigiD dat na de authenticatie wordt geredirect naar hetzelfde domein van waaruit DigiD is aangeroepen. Daaraan is eenvoudig voldaan in het MedMij Afsprakenstelsel, zij het dat deze DigiD-aanroep en -redirect zijn ingebed in een vergelijkbare Oauth-aanroep en -redirect. De situatie is dus genest: de *PGO Server* roept de *Authorization Server* aan, die DigiD aanroept, die redirect naar de *Authorization Server* , die de OAuth-flow vervolgt, waarin onder meer een redirect naar de *PGO Server* plaatsvindt.

Whitelist -controle tijdens de TLS-handshake

In het MedMij Afsprakenstelsel wordt gewerkt met een *Whitelist* voor het autoriseren van servers voor deelname in MedMij-verkeer. In het geval van inkomend backchannel-verkeer vindt de controle tegen de *Whitelist* plaats gedurende de TLS-handshake. De implementatie daarvan kan enige complexiteit opleveren. Het MedMij Afsprakenstelsel kiest niettemin voor deze optie om de volgende redenen.

Allereerst is een reeks van alternatieven voor de *Whitelist* overwogen, vooral op basis van certificaten. Deze overwegingen zijn te vinden in het eerste toelichtingsblok op de Netwerk-pagina. Gegeven het gebruik van een *Whitelist* kan vervolgens, in het geval van inkomend back-chan-nel-verkeer, gedacht worden aan de volgende plaatsen om de controle tegen de *Whitelist* uit te voeren:

- op TLS-niveau, voorafgaand aan de TLS-handshake;
- op TLS-niveau, tijdens de TLS-handshake;
- op TLS-niveau, na de TLS-handshake;
- boven TLS-niveau, in een apart autorisatieprotocol.

De eerste optie kan niet, want de identiteit van de tegenpartij wordt pas tijdens de TLS-handshake bekend, uit het aangeboden certificaat. De derde optie is ongewenst omdat deze leidt tot het starten van onveilige TLS-sessies, waarin ongeautoriseerd verkeer kan plaatsvin-den. De andere twee opties kennen allebei een extra implementatie-complexi-teit. Die van de vierde optie is echter ruim groter dan van de tweede, omdat de vierde optie om een MedMij-eigen autorisatieprotocol zou vragen. De tweede optie is preferent.

G2- en G3-certificaten van PKIoverheid

Certificate Authorities in PKIoverheid geven certificaten uit onder twee verschillende rootcertificaten: een oude (G2) en een nieuwe (G3). De geldigheid van G2-certificaten zal uiterlijk eindigen op 22 maart 2020. Hoewel er dus geen G2-certificaten meer kunnen worden uitgegeven met een geldigheid van drie jaar, moet het vooralsnog mogelijk zijn oudere G2-certificaten te gebruiken voor MedMij-doeleinden. Waar PKIoverheid-certificaten moet worden geaccepteerd, moeten die dus G2- of G3-certificaten kunnen zijn. Het MedMij Afsprakenstelsel heeft geen redenen extra beperkingen op te leggen ten opzichte van hoe PKIoverheid de transitie van G2 naar G3 maakt.