

RFC0084 Autorisatie voor verzamelen + delen + abonneren + workflow

1. Samenvatting

<p>Waarom is deze RFC nodig?</p>	<p>Deze RFC is in het algemeen nodig om de gebruiksvriendelijkheid van MedMij te verhogen, door ervoor te zorgen dat Persoon minder vaak hoeft in te loggen en toestemmen/bevestigen. Deze RFC is specifiek ook nodig om ondersteuning van workflow functionaliteit op een gebruiksvriendelijke wijze te kunnen opnemen in MedMij.</p> <p>Doelstelling is dat Persoon in één actie toestemming/bevestiging kan geven voor alle interacties die zij op een bepaald moment met één geselecteerde aanbieder wenst te hebben. Het gaat dan om:</p> <ol style="list-style-type: none"> 1. Verzamelen in de context van één of meerdere gegevensdiensten (kan al in het huidige afsprakenstelsel). 2. Delen in de context van één of meerdere gegevensdiensten. 3. Abonneren op notificaties m.b.t. één of meerdere verzamel-gegevensdiensten, inclusief het daadwerkelijk verzamelen. 4. Abonneren op notificatie m.b.t. één of meerdere workflowtypen, en aanmaken, lezen of wijzigen van taken in de context van één of meerdere workflowtypen. 																													
<p>Oplossingsrichting</p>	<p>Huidige scope</p> <table border="1" data-bbox="383 701 1484 957"> <thead> <tr> <th>Functie</th> <th>Vulling scope</th> <th>Toelichting</th> </tr> </thead> <tbody> <tr> <td>Verzamelen</td> <td>"<aanbieder-1>~<gegevensdienst-1> <aanbieder-1>~<gegevensdienst-2>"</td> <td>Eén of meerdere aanbieder-gegevensdienst-combinaties bij eenzelfde aanbieder. Slechts verzamel-gegevensdiensten toegestaan.</td> </tr> <tr> <td>Delen</td> <td>"<aanbieder-1>~<gegevensdienst-3>"</td> <td>Eén aanbieder-gegevensdienst-combinatie.</td> </tr> <tr> <td>Abonneren</td> <td>"subscribe~<duur>/<aanbieder-1>~<gegevensdienst-1>"</td> <td>Eén aanbieder-gegevensdienst-combinatie.</td> </tr> </tbody> </table> <p>Nieuwe scope</p> <table border="1" data-bbox="383 1024 1484 1919"> <thead> <tr> <th>Functie</th> <th>Vulling scope</th> <th>Toelichting</th> </tr> </thead> <tbody> <tr> <td>Verzamelen + Delen</td> <td>"<aanbieder-1>~<gegevensdienst-1> <aanbieder-1>~<gegevensdienst-2> <aanbieder-1>~<gegevensdienst-3>"</td> <td>Eén of meerdere aanbieder-gegevensdienst-combinaties bij eenzelfde aanbieder. Combinaties van verzamel-gegevensdiensten en delen-gegevensdiensten toegestaan. De DVA weet a.d.h. v. het gegevensdienstnummer of het verzamelen danwel delen betreft.</td> </tr> <tr> <td>Verzamelen + Abonneren</td> <td>"subscribe~<duur>/<aanbieder-1>~<gegevensdienst-1> <aanbieder-1>~<gegevensdienst-2>"</td> <td>Wanneer een abonnement wordt genomen op een aanbieder-gegevensdienst-combinatie, dan wordt direct ook toestemming gegeven voor verzamelen van de betreffende aanbieder-gegevensdienst. In het voorbeeld wordt autorisatie gevraagd voor abonneren én verzamelen van gegevensdienst-1, en voor verzamelen van gegevensdienst-2. Abonneren kan voorsnog niet worden gedaan voor delen-gegevensdiensten.</td> </tr> <tr> <td>Workflow (aankmaken, lezen, wijzigen van taken + abonneren op workflow notificaties)</td> <td>"subscribe~<duur>/<aanbieder-1>~<workflowtype-1> subscribe~<duur>/<aanbieder-1>~<workflowtype-2>"</td> <td>Wanneer een abonnement wordt genomen op een aanbieder-workflowtype-combinatie, dan wordt direct ook toestemming gegeven voor interacties m. b.t. het betreffende aanbieder-workflowtype. In het voorbeeld wordt autorisatie gevraagd voor abonneren én interacties m.b.t. workflowtype-1, en m.b.t. workflowtype-2.</td> </tr> <tr> <td>Alles</td> <td>"subscribe~<duur>/<aanbieder-1>~<gegevensdienst-1> <aanbieder-1>~<gegevensdienst-2> <aanbieder-1>~<gegevensdienst-3> subscribe~<duur>/<aanbieder-1>~<workflowtype-1> subscribe~<duur>/<aanbieder-1>~<workflowtype-2>"</td> <td></td> </tr> </tbody> </table>			Functie	Vulling scope	Toelichting	Verzamelen	"<aanbieder-1>~<gegevensdienst-1> <aanbieder-1>~<gegevensdienst-2>"	Eén of meerdere aanbieder-gegevensdienst-combinaties bij eenzelfde aanbieder. Slechts verzamel-gegevensdiensten toegestaan.	Delen	"<aanbieder-1>~<gegevensdienst-3>"	Eén aanbieder-gegevensdienst-combinatie.	Abonneren	"subscribe~<duur>/<aanbieder-1>~<gegevensdienst-1>"	Eén aanbieder-gegevensdienst-combinatie.	Functie	Vulling scope	Toelichting	Verzamelen + Delen	"<aanbieder-1>~<gegevensdienst-1> <aanbieder-1>~<gegevensdienst-2> <aanbieder-1>~<gegevensdienst-3>"	Eén of meerdere aanbieder-gegevensdienst-combinaties bij eenzelfde aanbieder. Combinaties van verzamel-gegevensdiensten en delen-gegevensdiensten toegestaan. De DVA weet a.d.h. v. het gegevensdienstnummer of het verzamelen danwel delen betreft.	Verzamelen + Abonneren	"subscribe~<duur>/<aanbieder-1>~<gegevensdienst-1> <aanbieder-1>~<gegevensdienst-2>"	Wanneer een abonnement wordt genomen op een aanbieder-gegevensdienst-combinatie, dan wordt direct ook toestemming gegeven voor verzamelen van de betreffende aanbieder-gegevensdienst. In het voorbeeld wordt autorisatie gevraagd voor abonneren én verzamelen van gegevensdienst-1, en voor verzamelen van gegevensdienst-2. Abonneren kan voorsnog niet worden gedaan voor delen-gegevensdiensten.	Workflow (aankmaken, lezen, wijzigen van taken + abonneren op workflow notificaties)	"subscribe~<duur>/<aanbieder-1>~<workflowtype-1> subscribe~<duur>/<aanbieder-1>~<workflowtype-2>"	Wanneer een abonnement wordt genomen op een aanbieder-workflowtype-combinatie, dan wordt direct ook toestemming gegeven voor interacties m. b.t. het betreffende aanbieder-workflowtype. In het voorbeeld wordt autorisatie gevraagd voor abonneren én interacties m.b.t. workflowtype-1, en m.b.t. workflowtype-2.	Alles	"subscribe~<duur>/<aanbieder-1>~<gegevensdienst-1> <aanbieder-1>~<gegevensdienst-2> <aanbieder-1>~<gegevensdienst-3> subscribe~<duur>/<aanbieder-1>~<workflowtype-1> subscribe~<duur>/<aanbieder-1>~<workflowtype-2>"	
Functie	Vulling scope	Toelichting																												
Verzamelen	"<aanbieder-1>~<gegevensdienst-1> <aanbieder-1>~<gegevensdienst-2>"	Eén of meerdere aanbieder-gegevensdienst-combinaties bij eenzelfde aanbieder. Slechts verzamel-gegevensdiensten toegestaan.																												
Delen	"<aanbieder-1>~<gegevensdienst-3>"	Eén aanbieder-gegevensdienst-combinatie.																												
Abonneren	"subscribe~<duur>/<aanbieder-1>~<gegevensdienst-1>"	Eén aanbieder-gegevensdienst-combinatie.																												
Functie	Vulling scope	Toelichting																												
Verzamelen + Delen	"<aanbieder-1>~<gegevensdienst-1> <aanbieder-1>~<gegevensdienst-2> <aanbieder-1>~<gegevensdienst-3>"	Eén of meerdere aanbieder-gegevensdienst-combinaties bij eenzelfde aanbieder. Combinaties van verzamel-gegevensdiensten en delen-gegevensdiensten toegestaan. De DVA weet a.d.h. v. het gegevensdienstnummer of het verzamelen danwel delen betreft.																												
Verzamelen + Abonneren	"subscribe~<duur>/<aanbieder-1>~<gegevensdienst-1> <aanbieder-1>~<gegevensdienst-2>"	Wanneer een abonnement wordt genomen op een aanbieder-gegevensdienst-combinatie, dan wordt direct ook toestemming gegeven voor verzamelen van de betreffende aanbieder-gegevensdienst. In het voorbeeld wordt autorisatie gevraagd voor abonneren én verzamelen van gegevensdienst-1, en voor verzamelen van gegevensdienst-2. Abonneren kan voorsnog niet worden gedaan voor delen-gegevensdiensten.																												
Workflow (aankmaken, lezen, wijzigen van taken + abonneren op workflow notificaties)	"subscribe~<duur>/<aanbieder-1>~<workflowtype-1> subscribe~<duur>/<aanbieder-1>~<workflowtype-2>"	Wanneer een abonnement wordt genomen op een aanbieder-workflowtype-combinatie, dan wordt direct ook toestemming gegeven voor interacties m. b.t. het betreffende aanbieder-workflowtype. In het voorbeeld wordt autorisatie gevraagd voor abonneren én interacties m.b.t. workflowtype-1, en m.b.t. workflowtype-2.																												
Alles	"subscribe~<duur>/<aanbieder-1>~<gegevensdienst-1> <aanbieder-1>~<gegevensdienst-2> <aanbieder-1>~<gegevensdienst-3> subscribe~<duur>/<aanbieder-1>~<workflowtype-1> subscribe~<duur>/<aanbieder-1>~<workflowtype-2>"																													

Verwerking authorization request

Wanneer een authorization server een authorization request ontvangt met een nieuwe scope dan dient ze:

1. te toetsen of alle scope onderdelen geldig zijn (alle onderdelen moeten geldig zijn);
2. te toetsen of alle scope onderdelen worden ondersteund door DVP (alle onderdelen moeten worden ondersteund);
3. te toetsen of alle scope onderdelen, via eenzelfde authorization endpoint en via eenzelfde token endpoint, worden ondersteund door aanbieder (alle onderdelen moeten worden ondersteund);
4. de vereiste ontvankelijkheids- en beschikbaarheidstoetsen uit te voeren (de toetsen hoeven niet per sé positief te zijn voor alle onderdelen);
5. voor alle onderdelen waarvoor het ontvankelijkheids- of beschikbaarheidscriterium is vervuld, de juiste toestemmings- en bevestigingsschermen te tonen (voor alle getoonde onderdelen dient toestemming/bevestiging te worden gegeven, geen selectie door persoon meer mogelijk in het scherm, danwel de schermen);
6. de scope in de token response te vullen met alle scope onderdelen waarvoor het ontvankelijkheids- of beschikbaarheidscriterium werd vervuld.

Huidige toestemmings- en bevestigingsschermen

Toestemmingsverklaring (verzamelen)

Ik wil persoons- en medische gegevens opslaan in mijn persoonlijke gezondheidsomgeving (PGO).

Persoonsgegevens zijn bijvoorbeeld je naam en geboortedatum. Medische gegevens zijn de gegevens die een zorgverlener bijhoudt over jouw behandeling in jouw medisch dossier. Bijvoorbeeld de medicijnen die je slikt en bloeduitslagen.

Hierbij geef ik NaamZorgaanbieder toestemming om de gegevens die ik opvraag aan NaamLeverancierPGO, de aanbieder van mijn PGO, te sturen.

De volgende gegevens wil ik opvragen en in mijn PGO opslaan:

- NaamGegevensdienst
- NaamGegevensdienst

Bevestigingsverklaring (delen)

Ik wil persoons- en medische gegevens delen met NaamZorgaanbieder. Jouw zorgverlener bepaalt daarna of hij deze informatie opneemt in jouw medisch dossier en/of gebruikt voor jouw behandeling.

Persoonsgegevens zijn bijvoorbeeld je naam en geboortedatum. Medische gegevens zijn de gegevens die een zorgverlener bijhoudt over jouw behandeling. Bijvoorbeeld de medicijnen die je slikt en bloeduitslagen.

Hierbij geef ik NaamLeverancierPGO, de aanbieder van mijn PGO, toestemming om de volgende gegevens te delen met NaamZorgaanbieder:

- NaamGegevensdienst
- NaamGegevensdienst

Toestemmingsverklaring (abonneren op notificaties m.b.t. verzamelen)

Hierbij geef ik NaamZorgaanbieder toestemming om NaamLeverancierPGO, de aanbieder van mijn PGO, een melding te sturen als er iets wijzigt in de gegevens die NaamZorgaanbieder over mij bijhoudt.

Het gaat hierbij om meldingen over veranderingen in:

- NaamGegevensdienst

Ik geef deze toestemming voor de komende Duur dagen. Let op, NaamZorgaanbieder mag en kan deze periode korter maken.

Nieuwe toestemmings- en bevestigingsschermen

Toestemmingsverklaring (abonneren + verzamelen)

Ik wil persoons- en medische gegevens opslaan in mijn persoonlijke gezondheidsomgeving (PGO).

Persoonsgegevens zijn bijvoorbeeld je naam en geboortedatum. Medische gegevens zijn de gegevens die een zorgverlener bijhoudt over jouw behandeling in jouw medisch dossier. Bijvoorbeeld de medicijnen die je slikt en bloeduitslagen.

Hierbij geef ik NaamZorgaanbieder toestemming om NaamLeverancierPGO, de aanbieder van mijn PGO, een melding te sturen als er iets wijzigt in de gegevens die NaamZorgaanbieder over mij bijhoudt, en om de gegevens die ik opvraag aan NaamLeverancierPGO te sturen.

Ik geef toestemming voor de volgende gegevens:

- NaamGegevensdienst
- NaamGegevensdienst

Ik geef deze toestemming voor de komende Duur dagen. Let op, NaamZorgaanbieder mag en kan deze periode korter maken.

Toestemmingverklaring (workflow)

Ik wil met NaamZorgaanbieder gegevens uitwisselen over taken die bij mijn behandeling horen. Taken zijn bijvoorbeeld zelfmetingen die ik uit moet voeren en die door NaamZorgaanbieder moeten worden bekeken.

Ook geef ik NaamZorgaanbieder toestemming om NaamLeverancierPGO, de aanbieder van mijn PGO, een melding te sturen als er iets wijzigt in de gegevens over taken die mijn behandeling horen.

Ik wil gegeven uitwisselen en meldingen ontvangen over de volgende soorten taken:

- NaamWorkflow
- NaamWorkflow

In de nieuwe situatie spelen de volgende schermen een rol:

1. Toestemmingverklaring (verzamelen), voor één of meerdere gegevensdiensten
2. Bevestigingsverklaring (delen), voor één of meerdere gegevensdiensten
3. Toestemmingverklaring (abonneren op notificaties m.b.t. verzamelen)
4. Toestemmingverklaring (abonneren + verzamelen)
5. Toestemmingsverklaring (workflow)

Wanneer de scope die moet worden verwerkt bestaat uit onderdelen die betrekking hebben op verschillende schermen, dan worden de betreffende schermen na elkaar getoond. Persoon geeft dan scherm-voor-scherm haar toestemming. Zodra persoon op één van de schermen weigert, dan wordt autorisatie voor de gehele scope afgekeurd.

Beschikbaarheids- en ontvankelijkheidstoets

Toegestane moment van toetsing in de huidige situatie:

- Bij verzamelen en bij abonneren op notificaties m.b.t. verzamelen, mag de beschikbaarheidstoets vroeg of laat worden uitgevoerd.
- Bij delen moet de ontvankelijkheidstoets vroeg worden uitgevoerd.

Een toets moet in één keer worden uitgevoerd voor alle onderdelen in de scope.

Toegestane moment van toetsing in de nieuwe situatie:

- Bij abonneren + verzamelen op notificaties m.b.t. verzamelen mag de beschikbaarheidstoets vroeg of laat worden uitgevoerd.
- Bij workflow een beschikbaarheids/ontvankelijkheidstoets vroeg worden uitgevoerd.

Een toets moet in één keer, en dus ook op hetzelfde moment, worden uitgevoerd voor alle onderdelen in de scope.

Verwerking van resource request, subscription request, workflow request vergezeld van access_token met een meervoudige scope

De volgende regels zijn van toepassing:

	<ul style="list-style-type: none"> • Een resource endpoint mag slechts gegevens verwerken voor één gegevensdienst - is huidige situatie • Een subscription endpoint mag abonnementen verwerken voor meerdere gegevensdiensten of workflowtypen (de gegevensdienst is een attribuut van de subscription, het workflowtype zal worden toegevoegd als een attribuut van de subscription) • Een workflow endpoint mag slechts gegevens verwerken voor één workflow type - de Task zou weliswaar kunnen worden afgeleid van de attributen van een Task, bijv. Task.code of van een ActivityDefinition, maar eenzelfde type Task kan worden gebruikt binnen verschillende workflowtypen.
RACI	<ul style="list-style-type: none"> • Responsible: • Accountable: <ul style="list-style-type: none"> • \$RFC_RACI_Accountable • Consulted <ul style="list-style-type: none"> • Ontwikkelteam (ontwikkeling@medmij.nl) • Security Management (secmgt@medmij.nl) • Acceptatie (acceptatie@medmij.nl) • Stelselregie • Deelnemers (Expertgroepsessie) • Informed <ul style="list-style-type: none"> • Communicatie • Loket (info@medmij.nl) • Leveranciersmanagement
Aanpassing van	TBD
Impact op rollen	TBD
Impact op beheer	TBD
Impact op RnA	TBD
Impact op Acceptatie	TBD
PIA noodzakelijk	TBD
Gerelateerd aan (Andere RFCs, PIM issues)	Epic AF-1210 Workflow
Implementatietermijn	TBD
Motivatie verkorte RFC procedure (patch)	N.v.t.

2. Uitwerking

Volgt.

2.1.1.1. Optioneel: Impact op foutafhandeling (zie <https://confluence.vzvv.nl/display/MMAS/Foutmeldingen+MedMij>)

TBD.

3. Principe's

Principe		Principe	
1 Het MedMij-netwerk is zoveel mogelijk gegevensneutraal	<input type="checkbox"/>	11 Stelselfuncties worden vanaf de start ingevuld	<input type="checkbox"/>
2 Dienstverleners zijn transparant over de gegevensdiensten	<input type="checkbox"/>	12 Het afsprakenstelsel is een groeimodel	<input type="checkbox"/>

3 Dienstverleners concurreren op de functionaliteiten	<input type="checkbox"/>	13 Ontwikkeling geschiedt in een half-open proces met verschillende stakeholders	<input type="checkbox"/>
4 Dienstverleners zijn aanspreekbaar door de gebruiker	<input type="checkbox"/>	14 Uitwisseling is een keuze	<input type="checkbox"/>
5 De persoon wisselt gegevens uit met de zorgaanbieder	<input type="checkbox"/>	15 Het MedMij-netwerk is gebruiksrechten-neutraal	<input type="checkbox"/>
6 MedMij spreekt alleen af wat nodig is	<input type="checkbox"/>	16 De burger regisseert zijn gezondheidsinformatie als uitgever	<input type="checkbox"/>
7 De persoon en de zorgaanbieder kiezen hun eigen dienstverlener	<input type="checkbox"/>	17 Aan de persoonlijke gezondheidsomgeving zelf worden eisen gesteld	<input type="checkbox"/>
9 De dienstverleners zijn deelnemers van het afsprakenstelsel	<input type="checkbox"/>	18 Afspraken worden aantoonbaar nageleefd en gehandhaafd	<input type="checkbox"/>
10 Alleen de dienstverleners oefenen macht uit over persoonsgegevens bij de uitwisseling	<input type="checkbox"/>	19 Het afsprakenstelsel snijdt het gebruik van normen en standaarden op eigen maat	<input type="checkbox"/>
Toelichting			

4. Risico's

Omschrijf de (privacy)risico's die kunnen ontstaan als deze RFC wordt aangenomen. In het onwaarschijnlijke geval dat deze RFC's geen risico's introduceert, geef dat dan wel aan.

Dreiging	Kans	Impact	DreigingsID (intern)	Maatregelen

5. Bijlagen

File

Modified 

No files shared here yet.

6. Goedkeuring

Beoordelaar	Datum	Toelichting	Beoordelaar	Datum	Toelichting
Productmanager Stichting MedMij			Productmanager Beheerorganisatie		
Leadarchitect Stichting MedMij			Leadarchitect Beheerorganisatie		
Ontwerpteam					
Deelnemersraad			Eigenaarsraad		