Eindrapportage PROVES Elektronische Toegangsdiensten

Proof of Concept 2020-2021

Datum: 20 oktober 2021

Versie: 1.0

Martijn Mallie, Ron van Holland & Carlos Villa Baars

Managementsamenvatting – context PoC

*huidige ontwikkelingen van DigiD vallen buiten de scope van de PoC en maken daarmee geen deel uit van het onderzoek
**De middelen die zijn beproefd zijn binnen het MedMij stelsel nog niet toegelaten in afwachting van de Wet Digitale Overheid (WDO)

Inleiding

Authenticatie binnen MedMij kent diverse uitdagingen, waaronder: het proces met DigiD was in 2019 niet erg gebruiksvriendelijk, de koppeling van de identiteit van de zorggebruiker in het persoons- en zorgaanbiedersdomein was niet erg sterk, DigiD op niveau Substantieel was nog niet breed beschikbaar en de zorggebruiker moest zich voor iedere opvraging bij iedere zorgaanbieder authenticeren*. Dit alles bemoeilijkt uitrol van MedMij in de praktijk. Als aanleiding hiervoor werd in 2020 de Proof of Concept (PoC) elektronischte toegangsdiensten (eTD) gestart, waarbij gebruik is gemaakt van eHerkenning. In de rapportage wordt verder gesproken over eTD.

Doelstellingen

Om de huidige uitdagingen te overwinnen, werd in 2020 een PoC gestart voor authenticatie met een dienst binnen het Elektronische Toegangsdienst (eTD)-stelsel. De doelstellingen van de PoC zijn als volgt:

1. Beproeven van de mogelijkheid om niet opnieuw te hoeven authenticeren bij herhaalde opvraging van gegevens bij dezelfde zorgaanbieder.
2. Beproeven van een oplossing die authenticatie op eIDAS-niveau Substantieel mogelijk maakt.
3. Borgen dat de zorggebruiker die inlogt in de PGO dezelfde is als degene die inlogt bij zorgaanbieder.
4. Generiek technisch koppelvlak definiëren tussen dienstverlener persoon (DVP), dienstverlener zorgaanbieder (DVZA) en eHerkenning-partijen.
5. Beproeven van een alternatief authenticatiemiddel naast DigiD.

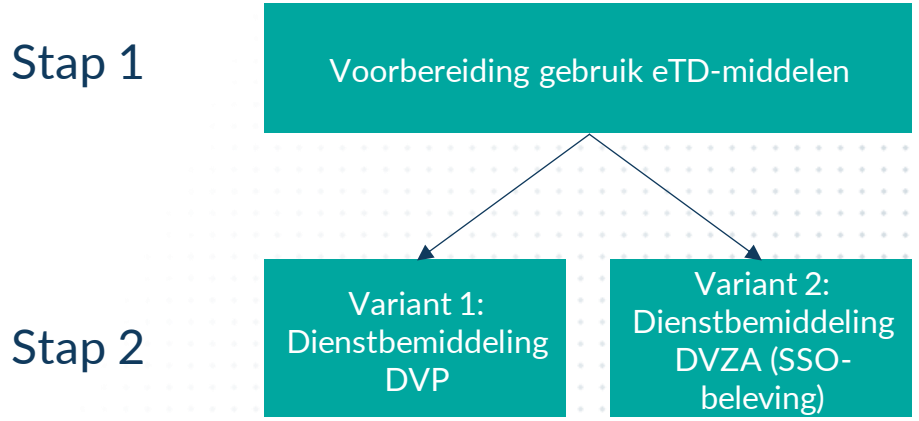
Uitgangspunten

Tijdens de PoC zijn de volgende uitgangspunten gehanteerd:

- De oplossing past binnen het MedMij Afsprakenstelsel en eTD Afsprakenstelsel
- Geen verwerking van BSN in het persoonsdomein

Beproefde oplossing**

Om succesvol het gebruik van eTD-middelen binnen het MedMij Afsprakenstelsel te beproeven zijn twee stappen gedefinieerd (zie figuur 1). Stap 1 is de voorbereiding voor het kunnen gebruiken van eTD-middelen. Hierbij worden eTD-koppelvlakken tussen eTD leveranciers en dienstverleners gerealiseerd. Stap 2 bestaat uit het beproeven van twee varianten. Variant 1 is dienstbemiddeling en variant 2 is SSO-beleving.



Figuur 1. Weergave van gerealiseerde stappen

Managementsamenvatting - resultaten

Succesvolle generieke koppeling (eindtest) tussen het eTD-stelsel en het MedMij-stelsel

Eén van de belangrijkste doelstellingen om dienstbemiddeling en een single sign on beleving mogelijk te maken was het definiëren en technisch realiseren van een generiek koppelvlak tussen eTD-partijen en DVP en DVZA. Tijdens de PoC is het generieke koppelvlak succesvol gerealiseerd en beproefd waardoor de mogelijkheid voor authenticatie en uitwisseling van sleutelmateriaal middels eTD-partijen binnen het MedMij-stelsel bewezen is.

Succesvol beproefd variant 1: dienstbemiddeling DVP

Dienstbemiddeling DVP, waarbij de zorggebruiker in één sessie meerdere gegevensdiensten bij één zorgaanbieder kan verzamelen is succesvol beproefd. Tijdens de theoretische verdieping in dienstbemiddeling tijdens de PoC met alle deelnemers is besproken dat in de toekomst dynamische dienstbemiddeling mogelijk kan zijn. Bij dynamische dienstbemiddeling kan een zorggebruiker tijdens één sessie meerdere gegevensdiensten bij meerdere zorgaanbieders ineens verzamelen.

Succesvol beproefd variant 2: dienstbemiddeling DVZA (SSO beleving)

Dienstbemiddeling DVZA (SSO-beleving), waarbij de gekozen authenticatiedienst wordt onthouden door de herkenningsmakelaar en de authenticatiedienst de inlog van de zorggebruiker onthoudt is succesvol beproefd.

Technische realisatie van eTD-middelen binnen het MedMij-stelsel vereist extra onderzoek*

Ondanks dat de doelstellingen van de PoC zijn behaald vergt het technisch realiseren en uitrollen van eTD-middelen binnen het MedMij-stelsel extra onderzoek op het gebied van onder andere kosten; bijeenkomen van de dienstencatalogi en verbeteringen in de beproefde varianten.

Het gebruik van eTD-middelen binnen het MedMij-stelsel vereist ondersteuning

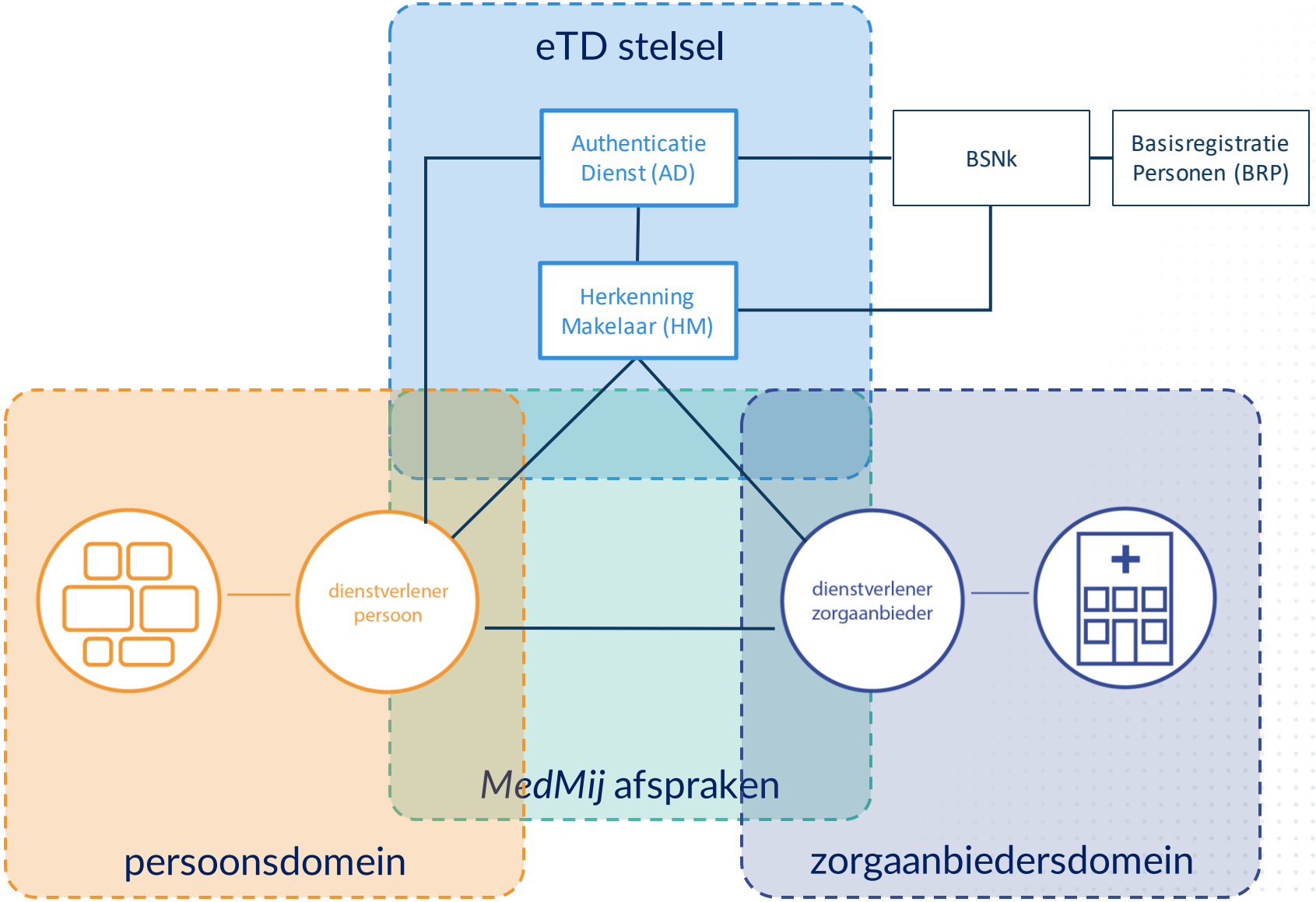
Wanneer het mogelijk is voor de DVP en DVZA om eTD-middelen te gebruiken, wordt een goede ondersteuning geadviseerd. Het gebruik van eTD-middelen is complex (en nieuw) voor de DVP en DVZA op het gebied van onder andere versleutelingen, vereiste certificaten, de docker-container voor ontsleutelen en dienstcatalogus eTD. Ondersteuning in de vorm van een onboardingsproces vanuit de herkenningsmakelaar voor de DVP en DVZA zou de complexiteit enigszins kunnen wegnemen.

Deelnemers kijken terug op een complexe, maar interessante en leerzame Proof of Concept

Het koppelen van twee verschillende stelsels (zie figuur 2 op pagina 4) is enorm complex, maar ook interessant en leerzaam. UnifiedPost (AD), Signicat (HM), Drimpy (DVP), ZWConnect (DVP) en Vecozo (DVZA-rol) zijn deze uitdaging succesvol aangegaan. Klik hier voor het filmpje van de succesvolle eindtest.

*De benodigde juridische borging om eHerkenning in de praktijk te kunnen inzetten in het burgerdomein en binnen het MedMij-stelsel valt buiten scope van deze technische beproeving

Managementsamenvatting – samenkomen stelsels



Figuur 2. Weergave samenkomen stelsel

Inhoudsopgave

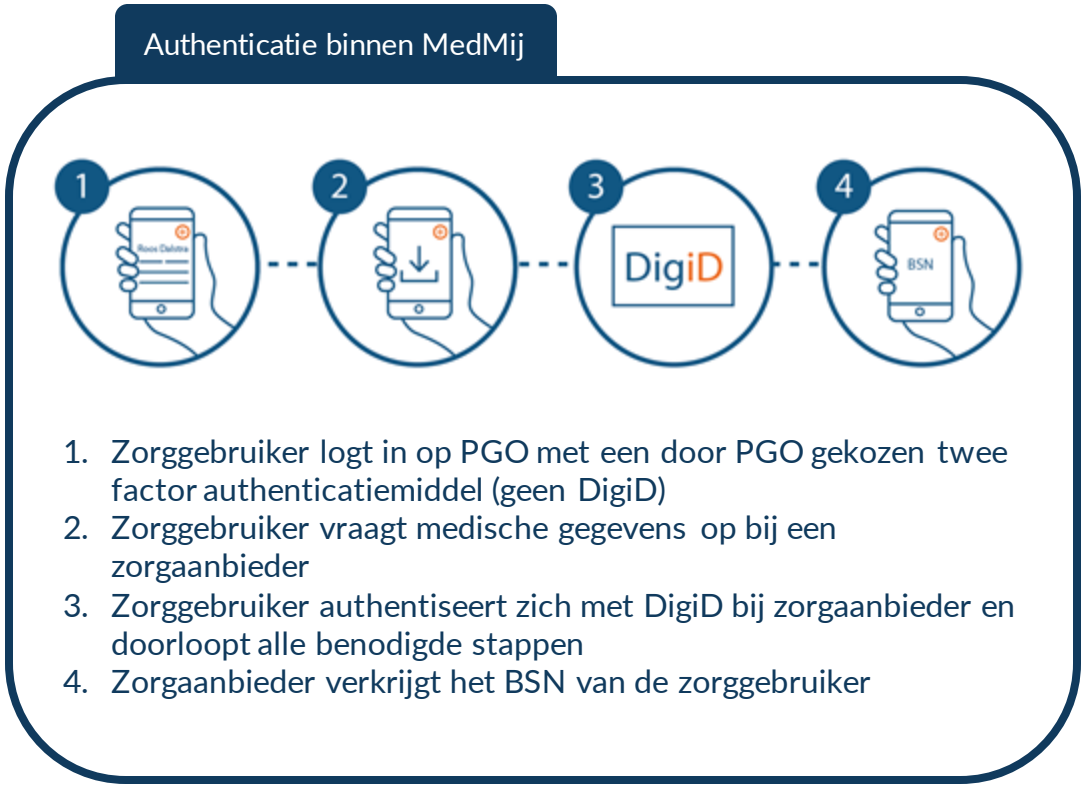
Hoofdstuk 1

Context PoC

Context

Authenticatie binnen MedMij

Momenteel kan binnen MedMij enkel met DigiD geauthentiseerd worden in het zorgaanbiedersdomein. Zie figuur 2 voor een weergave van dit authenticatieproces vanuit het perspectief van de zorggebruiker.



Figuur 3. Huidige flow van authenticatie binnen MedMij

Uitdagingen

De huidige situatie kent de volgende uitdagingen, zoals:

- Authenticatie binnen MedMij is niet erg gebruiksvriendelijk. De twee voornaamste redenen hiervoor zijn:
  - Een zorggebruiker moet zich voor iedere opvraging bij iedere zorgaanbieder authenticeren binnen zijn/haar persoonlijke gezondheidsomgeving (PGO) met DigiD. Ook bij herhaalde opvraging op een later moment, waarbij dezelfde gegevens bij dezelfde zorgaanbieder opgehaald worden, moet de zorggebruiker (opnieuw) authenticeren.
  - De zorggebruiker authentiseert met een ander middel bij zijn PGO (geen DigiD) dan bij de zorgaanbieder (DigiD)
- De koppeling van de identiteit van de zorggebruiker in het persoonsdomein en het zorgaanbiedersdomein is niet erg sterk. In theorie betekent dit dat gegevens van zorggebruiker A in de PGO van zorggebruiker B terecht kunnen komen.
- Bij aanvang van de PoC was DigiD op niveau Substantieel nog niet breed beschikbaar. Het authenticatieniveau moet in de zorg zo snel mogelijk naar minimaal niveau Substantieel worden gebracht.
- Het gebruik van private middelen voor authenticatie wordt momenteel niet toegelaten in het MedMij Afsprakenstelsel in afwachting van de WDO
- In het persoonsdomein mag het BSN niet worden verwerkt.

Proof of Concept Elektronische ToegangsDiensten (ETD)

Doelstellingen

Om de huidige uitdagingen te overwinnen, werd in 2020 een PoC gestart voor authenticatie met een inlogmiddel van het Elektronische Toegangsdienst (eTD) stelsel. De doelstellingen van de PoC waren als volgt:

1. Beproeven van de mogelijkheid om niet opnieuw te hoeven authenticeren bij herhaalde opvraging van gegevens bij dezelfde zorgaanbieder.
2. Beproeven van een oplossing die authenticatie op eIDAS-niveau Substantieel mogelijk maakt.
3. Borgen dat de zorggebruiker die inlogt in de PGO dezelfde is als degene die inlogt bij de zorgaanbieder.
4. Generiek technisch koppelvlak definiëren tussen DVP, DVZA en eTD-leveranciers.
5. Beproeven van een alternatief authenticatiemiddel naast DigiD.

Uitgangspunten

Tijdens de PoC zijn de volgende uitgangspunten gehanteerd:

- De oplossing past binnen het MedMij Afsprakenstelsel
- Geen verwerking van BSN in het persoonsdomein

PROVES

Sinds 2018 voert het programma PROVES technische beproevingen (proof of concepts) en gecontroleerde livegangen uit voor (onder andere) MedMij. Hiermee worden nieuwe gegevensdiensten en functionaliteiten van het afsprakenstelsel beproefd in de praktijk, worden (zorg)innovaties gecontroleerd live gebracht en wordt er bijgedragen aan het door ontwikkelen van het MedMij Afsprakenstelsel.

Tijdens een proof of concept (PoC) wordt gekeken naar de (technische) maakbaarheid, haalbaarheid, informatiestandaarden, gemeenschappelijke voorzieningen en beveiligingsaspecten in testomgevingen. Met een standaard werkwijze per route van PGO-leverancier, DVZA-leverancier en bronsysteem, zijn er diverse technische beproevingen uitgevoerd in de afgelopen jaren met nieuwe gegevensdiensten en functionaliteiten.

In 2019 is PROVES uitgebreid met gecontroleerde livegangen, waarin patiënten een PGO gebruiken en medische gegevens uitwisselen met zorgaanbieders. Middels ondersteuning vanuit PROVES in de vorm van projectleiding en programmamanagement worden alle stakeholders betrokken om in een regio te komen tot een begeleide uitrol van MedMij.

eTD Afsprakenstelsel en rollen

eTD Afsprakenstelsel

Het eTD Afsprakenstelsel is net als DigiD onderdeel van het Elektronische Identiteitsstelsel (eID).[1] Het eID conformeert zich aan de Europese 'electronic IDentification Authentication Tnd trust Services' (eIDAS)[2] -verordening. Het eTD Afsprakenstelsel is een set van technische, functionele, juridische en organisatorische afspraken. Binnen het eTD Afsprakenstelsel wordt eHerkenning geleverd, waarmee ondernemers, bedrijven, organisaties en intermediairs veilig en betrouwbaar online zaken kunnen doen met (overheids)organisaties en bedrijven.

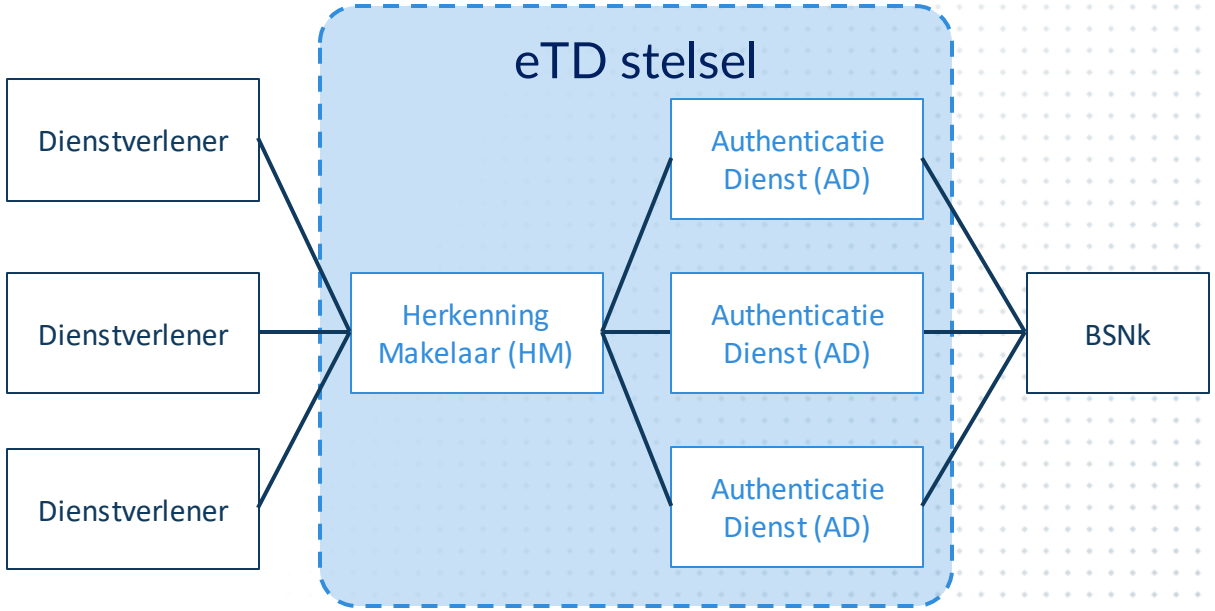
Rollen binnen het eTD Afsprakenstelsel

Het eTD Afsprakenstelsel kent een aantal rollen die belangrijk zijn in de context van deze PoC. Zie ook Figuur 3.

- Authenticatiedienst (AD): stelt een middel beschikbaar waarmee een gebruiker zich kan authenticeren. Binnen deze PoC is gebruik gemaakt van eHerkenning.
- Herkenningsmakelaar (HM): faciliteert berichtenverkeer tussen dienstverleners en authenticatiediensten.

Gebruik BSNk binnen het eTD-stelsel

BSN-koppelregister (BSNk): zorgt voor de koppeling tussen het BSN en het authenticatiemiddel. Meer uitleg over pseudoniemen en identiteiten is te lezen op pagina 10 en 11.



Figuur 4. Omschrijving toevoegen

1. Klik hier voor meer informatie over eID
2. Klik hier voor meer informatie over eIDAS

Versleutelingen binnen het eTD Afsprakenstelsel (in casu PoC)

Authenticatiediensten, herkenningsmakelaren en DVP's mogen het BSN niet verwerken. Daarom wordt het BSN door BSNk getransformeerd. Dit gebeurt op twee manieren (zie Figuur 5 op pagina 11 voor een schematische weergave.):

1. Transformatie naar pseudoniem
2. Transformatie naar identiteit

Transformatie naar pseudoniem

De authenticatiedienst activeert het BSN van de zorggebruiker bij BSNk-activatie en krijgt een Polymorfe Pseudoniem terug. Dit Polymorfe Pseudoniem is cryptografisch van het BSN afgeleid maar is niet cryptografisch terug te herleiden tot het BSN.

Als de zorggebruiker authenticeert ihkv MedMij dan zal de authenticatiedienst deze Polymorfe Pseudoniem transformeren tot Versleutelde Pseudoniem specifiek voor de DVP.

De DVP kan een pseudoniem ontsleutelen uit een Versleuteld Pseudoniem. Indirect is dit pseudoniem dus ook afgeleid van (maar niet herleidbaar tot) het BSN en daardoor gegarandeerd het zelfde (persistent) ongeacht de authenticatiedienst.

Transformatie naar identiteit

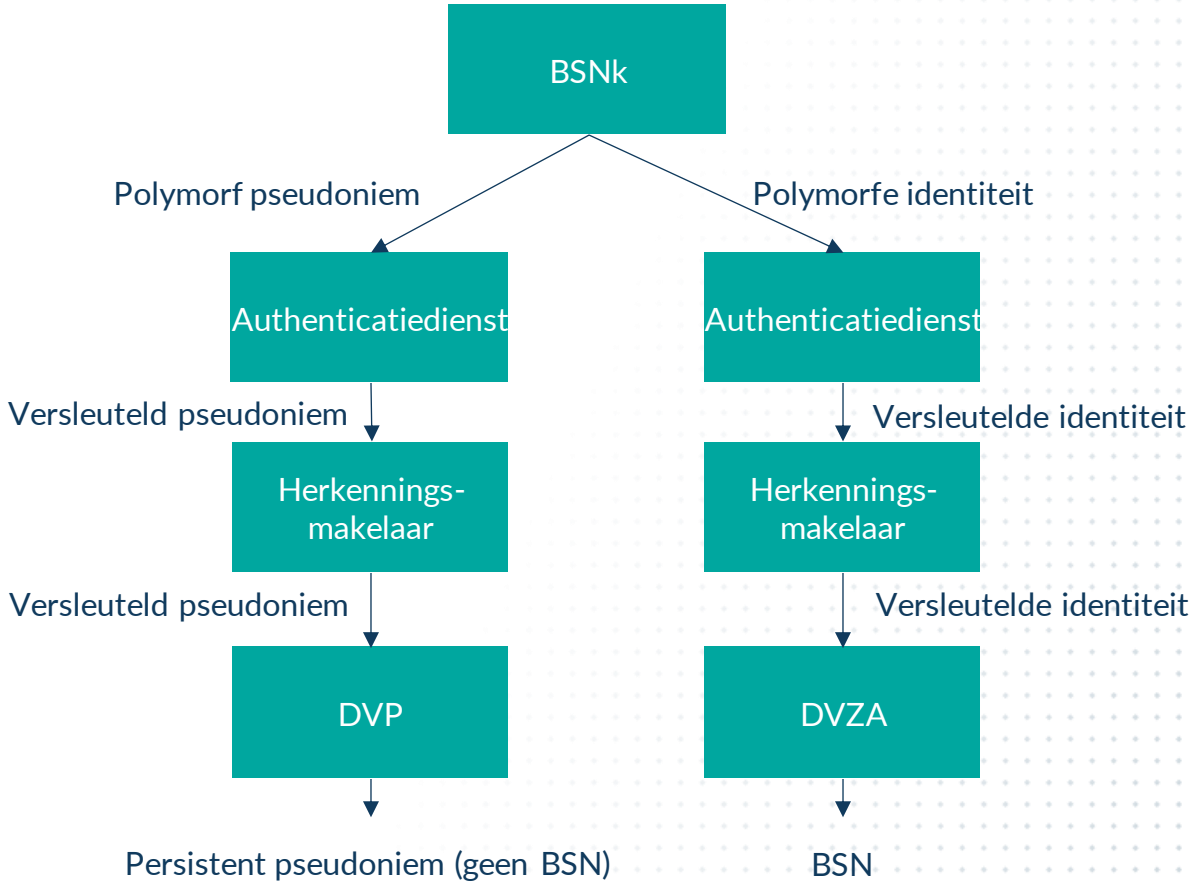
Bij de activatie van het BSN ontvangt de authenticatiedienst ook een Polymorfe Identiteit die ook cryptografisch is afgeleid van het BSN, maar wel cryptografisch herleidbaar is tot het BSN. De Polymorfe Identiteit kan getransformeerd worden naar een Versleutelde Identiteit specifiek voor een BSN-gerechtigde partij zoals een DVZA. Deze DVZA kan tenslotte de BSN ontsleutelen uit deze Versleuteld Identiteit.

Het is niet mogelijk voor een authenticatiedienst, herkenningsmakelaar en dienstverlener persoon om het BSN uit de versleutelde identiteit te herleiden.

Toepassing eTD-stelsel voor MedMij (in casu PoC)

Bij de toepassing van het stelsel binnen de PoC werkt de DVP dus met een (versleuteld) pseudoniem en de DVZA met een (versleuteld) BSN die cryptografisch onderling verbonden zijn en daardoor aantoonbaar van dezelfde persoon zijn. Hierdoor kan de DVP met de DVZA betrouwbaar, veilig en privacy vriendelijk communiceren over een zorggebruiker zonder dat:

- de DVP de BSN en de DVZA de (DVP specifieke) pseudoniem van de zorggebruiker kent
- de DVP en de DVZA ooit eerder contact hebben gehad over deze zorggebruiker
- 'MedMij/PGO-specifieke' onboardingsprocedures van de zorggebruiker bij de (DV)ZA noodzakelijk zijn.



Figuur 5. Versimpelde weergave van uitgifte van pseudoniemen en identiteiten door BSNk.

Hoofdstuk 2

Beproefde oplossing & Resultaten

Toelichting beproefde oplossing in PoC

In de PoC is eHerkenning, als eTD-middel, toegepast binnen MedMij voor authenticatie bij de PGO en de zorgaanbieder. Om dit te realiseren, zijn er drie onderdelen uitgewerkt (zie figuur 5). Deze onderdelen worden toegelicht vanuit gebruikers- en technisch perspectief op de volgende pagina's. Klik hier voor een video van de oplossing.

Stap 1: Voorbereiding gebruik eTD-middel

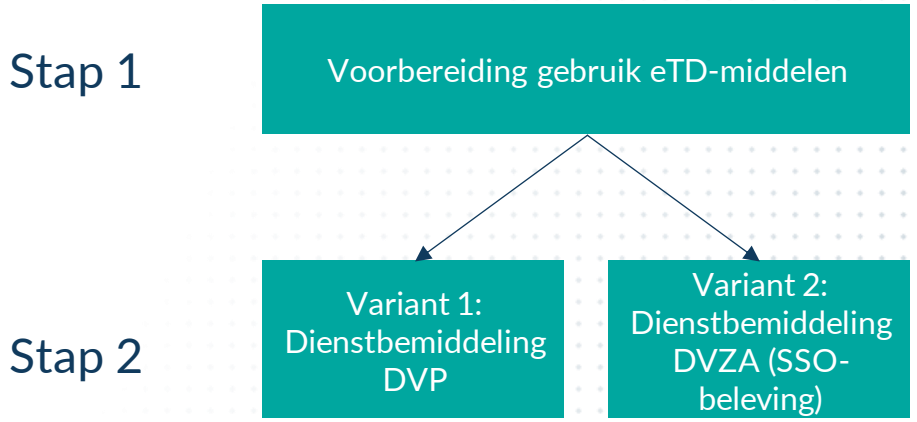
Om gebruik te kunnen maken van eTD-middelen binnen een PGO, dient de zorggebruiker een authenticatiedienst te koppelen aan de PGO. Nadat de authenticatiedienst succesvol is gekoppeld kan de zorggebruiker voortaan inloggen met behulp van een eTD-middel. Zie pagina 14 voor de uitwerking.

Stap 2: Variant 1 – Dienstbemiddeling DVP

Bij variant 1 wordt de DVP automatisch ondersteund door de authenticatiedienst en herkenningsmakelaar, waardoor de gebruiker in één sessie meerdere gegevens-diensten bij één zorgaanbieder kan verzamelen. Kenmerkend voor dienstbemiddeling is dat de zorggebruiker aan het begin van de sessie kiest bij welke gegevensdiensten en zorgaanbieder gegevens verzameld moeten worden. De DVP stuurt deze aanvraag door naar de HM en ontvangt een versleutelde identiteit retour. Dit voegt de DVP toe aan de conform MedMij aanvraag voor verzamelen gegevens bij de DVZA. Alleen de DVZA kan uit de verkregen versleutelde identiteit het BSN transformeren en zo de zorggebruiker identificeren. Vervolgens wordt het verzamelen van de gegevens conform de standaard MedMij flow afgerond. Het in één sessie meerdere gegevens-diensten bij meerdere zorgaanbieders verzamelen, dynamische dienstbemiddeling, is theoretisch beproefd en verwerkt in de bevindingen. Zie pagina 15 voor de uitwerking vanuit gebruikers- en technisch perspectief.

Stap 2: Variant 2 – Dienstbemiddeling DVZA (SSO beleving)

Bij variant 2 wordt de gekozen authenticatiedienst onthouden door de herkenningsmakelaar en onthoudt de authenticatiedienst de inlog van de zorggebruiker. De authenticatiedienst authentiseert tijdens het verzamelen van gegevens de zorggebruiker. Vervolgens vraagt de authenticatiedienst een pseudoniem voor de DVP en een pseudoniem en identiteit voor de DVZA aan. Doordat de DVP zowel vanuit de DVZA en de herkenningsmakelaar een ontvangt kan de DVP de controleren dat er namens de juiste zorggebruiker gegevens verzameld worden. Zie pagina 16 voor de uitwerking vanuit gebruikers- en technisch perspectief.



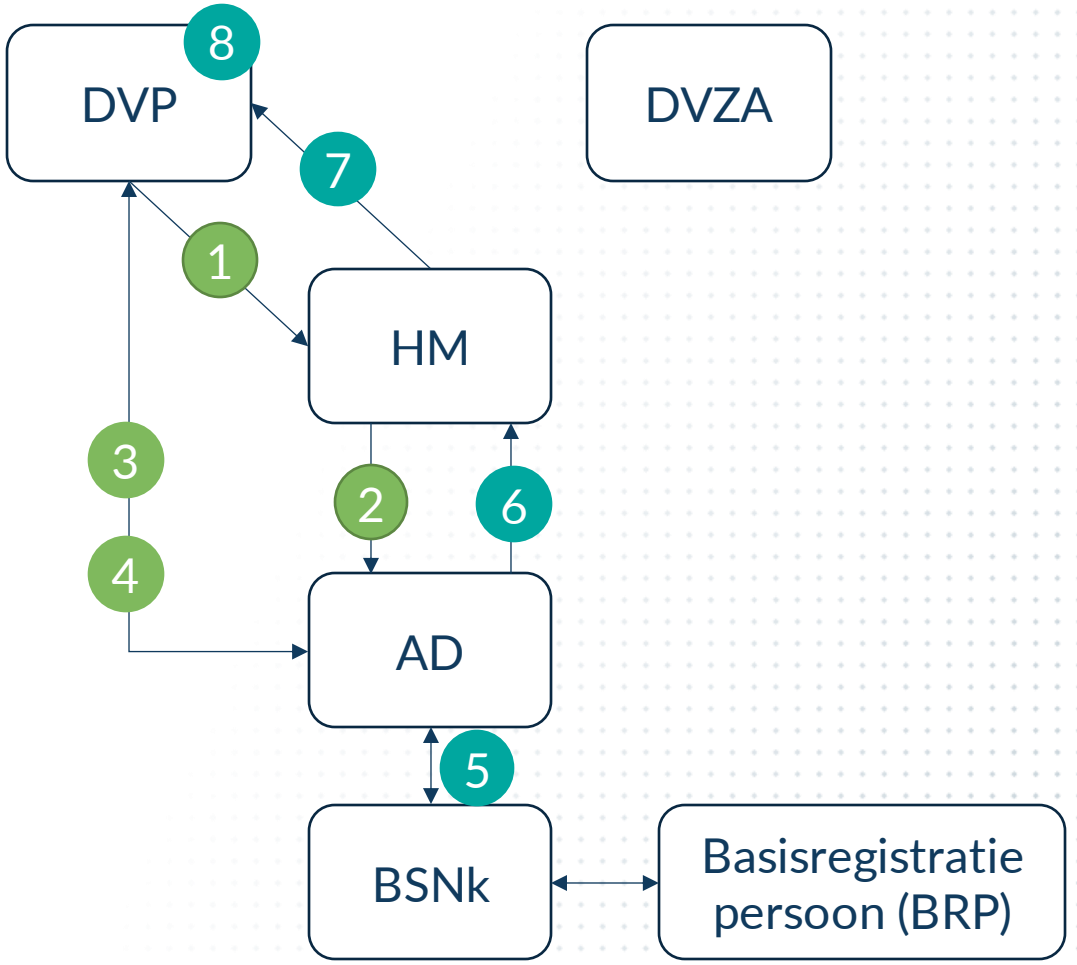
Figuur 6. Weergave van gerealiseerde stappen

Zie bijlage 1 voor de architectuurplaat

Stap 1: Voorbereiding gebruik eTD-middel

Handeling zorggebruiker	Technische stappen (na handeling zorggebruiker)
Zorggebruiker geeft aan een authenticatiedienst te willen koppelen en kiest vervolgens een authenticatiedienst	1. DVP stuurt de aanvraag naar de herkenningsmakelaar 2. Herkenningsmakelaar stuurt de aanvraag door naar de door zorggebruiker gekozen AD 3. Authenticatiedienst authentiseert zorggebruiker 4. Authenticatiedienst vraagt zorggebruiker toestemming om in te loggen bij PGO
Zorggebruiker geeft toestemming aan authenticatiedienst om in te loggen op PGO	5. Authenticatiedienst vraagt BSNk om de benodigde attributen (pseudoniemen en/of identiteiten) 6. Authenticatiedienst stuurt de attributen naar de herkenningsmakelaar 7. Herkenningsmakelaar stuurt de attributen naar de DVP 8. DVP verifieert en ontsleutelt de verkregen attributen en bewaart het ontsleutelde materiaal in deze gebruikerssessie
Zorggebruiker krijgt melding dat koppeling van PGO met AD is geslaagd	nvt

Tabel 1. Voorbereiding vanuit gebruikers- en technisch perspectief

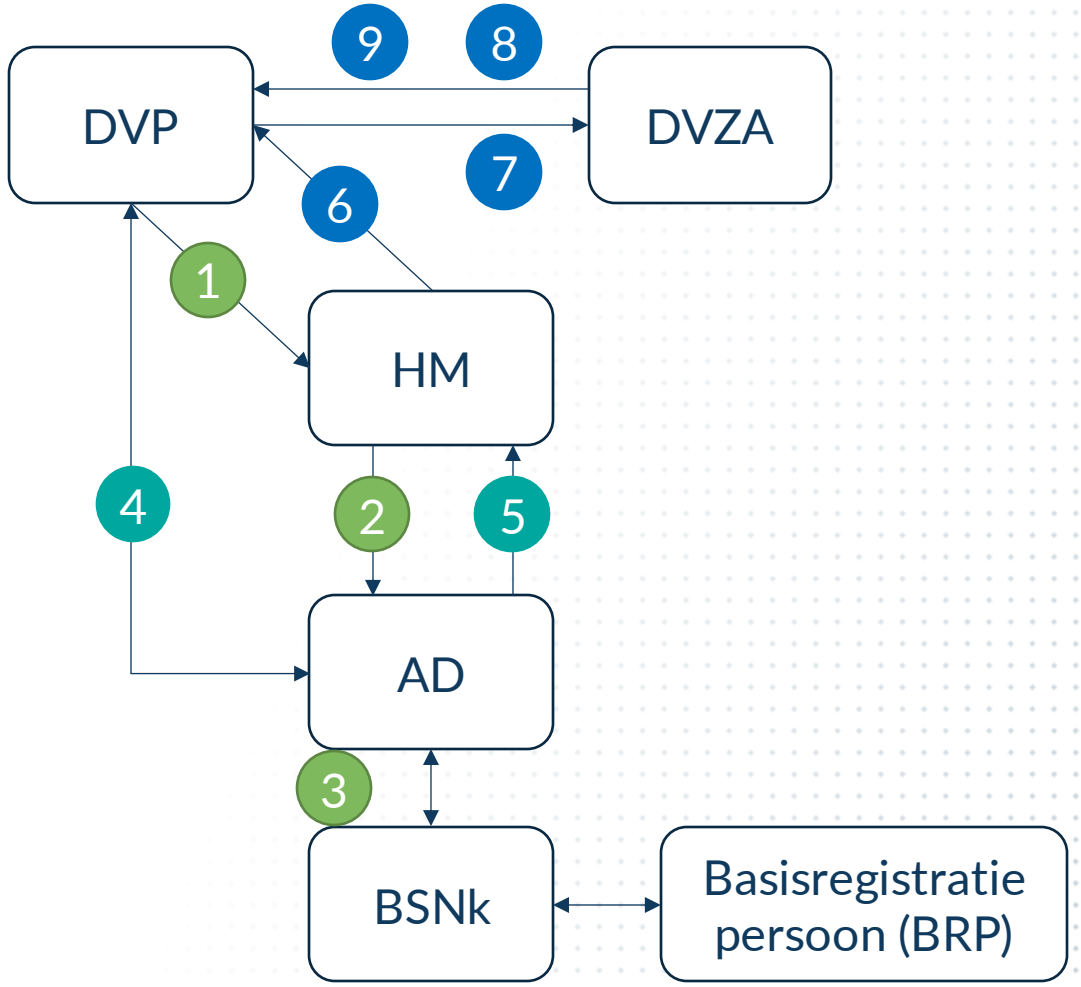


Figuur 7. Schematische weergave voorbereiding gebruik eTD-middel

Stap 2: Variant 1 – dienstbemiddeling DVP

Handeling zorggebruiker	Technische stappen (na handeling zorggebruiker)
Zorggebruiker kiest bij welke zorgaanbieder hij/zij welke gegevens wilt verzamelen	1. DVP stuurt aanvraag en lijst met gekozen zorgaanbieder en gevraagde gegevens naar herkenningsmakelaar 2. Herkenningsmakelaar stuurt de aanvraag en lijst door naar authenticatiedienst 3. Authenticatiedienst authentiseert gebruiker en vraagt benodigde versleutelingen aan bij BSNk 4. Authenticatiedienst vraagt toestemming aan zorggebruiker om de versleutelingen te mogen delen met de DVP
Zorggebruiker geeft toestemming aan authenticatiedienst	5. Authenticatie dienst retourneert de versleutelingen naar de herkenningsmakelaar 6. Herkenningsmakelaar stuurt de versleutelde identiteit voor de DVZA door naar DVP 7. DVP stuurt aanvraag voor autorisatie naar DVZA met daarbij de versleutelde identiteit 8. DVZA ontsleutelt de versleutelde identiteit en vraagt toestemming aan zorggebruiker om gegevens te mogen delen met DVP
Zorggebruiker geeft toestemming aan zorgaanbieder	9. DVZA retourneert een ophaalbewijs (access token)
Zorggebruiker verzamelt gegevens in zijn/haar PGO	Vervolgens conform MedMij het verzamelen van MedMij-gegevens

Tabel 2. Dienstbemiddeling DVP vanuit gebruikers- en technisch perspectief

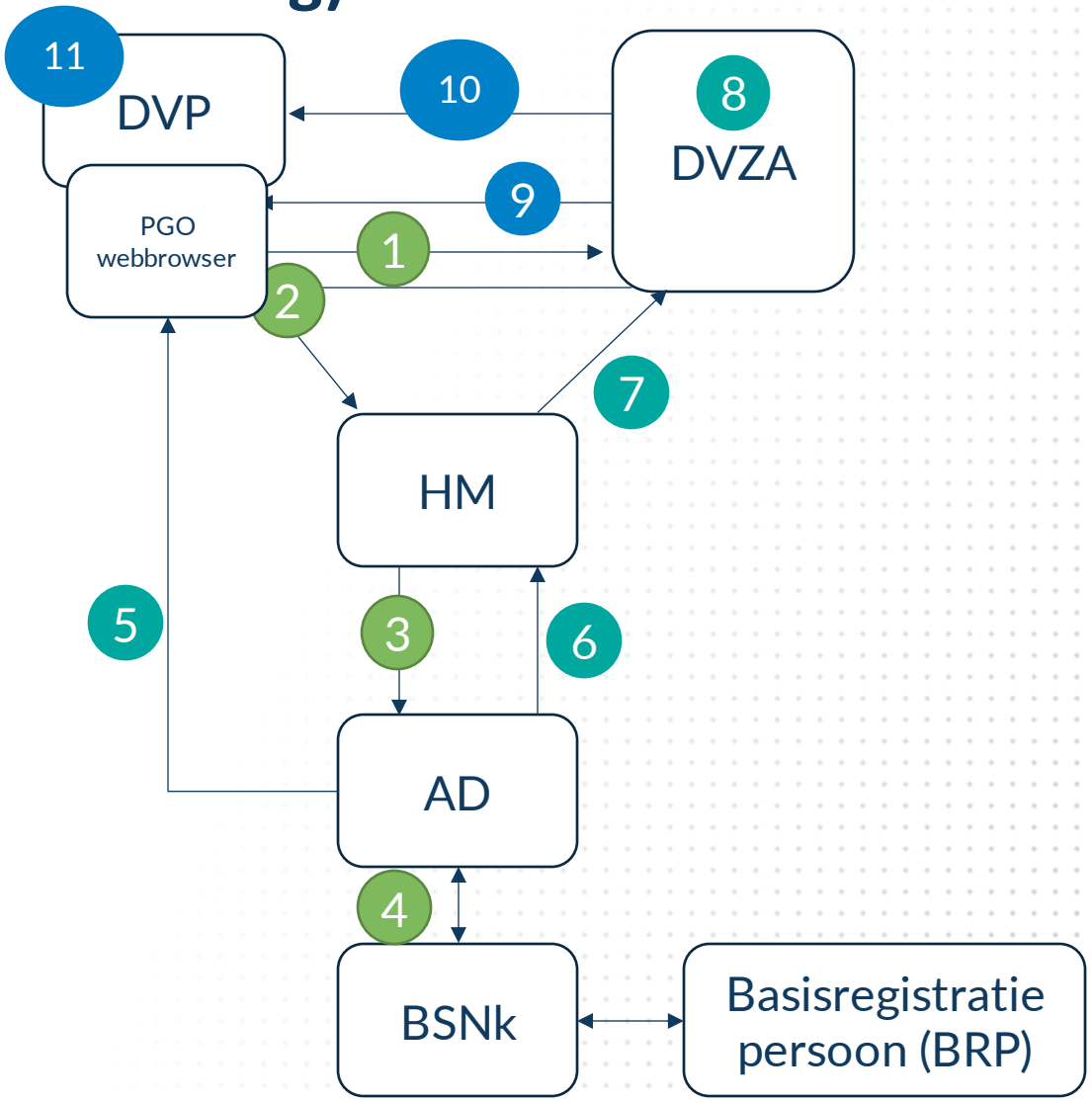


Figuur 8. Schematische weergave dienstbemiddeling DVP

Stap 2: Variant dienstbemiddeling DVZA (SSO-beleving)

Handeling van zorggebruiker	Technische stappen (opvolgend)
Zorggebruiker kiest bij welke zorgaanbieder hij/zij welke gegevens wilt verzamelen	1. DVP stuurt aanvraag voor autorisatie via de PGO webbrowser naar DVZA 2. DVZA laat de PGO webbrowser een authenticatie-aanvraag naar de Herkenningsmakelaar sturen 3. Herkenningsmakelaar stuurt de aanvraag door naar authenticatiedienst 4. Authenticatiedienst authentiseert gebruiker en vraagt benodigde versleutelingen aan bij BSNk 5. Authenticatiedienst vraagt toestemming aan zorggebruiker om de versleutelingen te mogen delen met de DVZA
Zorggebruiker geeft toestemming aan de authenticatiedienst	6. Authenticatiedienst retourneert de versleutelingen naar de herkenningsmakelaar 7. Herkenningsmakelaar stuurt de versleutelde identiteit en versleutelde pseudoniem naar de DVZA 8. DVZA ontsleutelt de identiteit en verifieert zorggebruiker 9. DVZA vraagt toestemming aan zorggebruiker om gegevens te mogen delen met DVP
Zorggebruiker geeft toestemming aan zorgaanbieder om gevraagde gegevens te mogen delen met DVP	10. DVP ontvangt een versleutelde pseudoniem van de DVZA 11. DVP vergelijkt de versleutelde pseudoniem van de DVZA met de versleutelde pseudoniem van de Herkenningsmakelaar
Zorggebruiker verzamelt gegevens in zijn/haar PGO	Vervolgens conform MedMij het verzamelen van MedMij gegevens

Tabel 3. Dienstbemiddeling DVZA (SSO-beleving) vanuit gebruikers- en technisch perspectief



Figuur 9. Schematische weergave dienstbemiddeling DVZA

Aanpak en deelnemers

Stappen van de PoC

In de PoC zijn twee stappen doorlopen om tot een nadere uitwerking en beproeving van de oplossing te komen.

1. **Nadere uitwerking.** In deze fase is de technische basis gelegd om ETD-middelen uit te kunnen wisselen tussen eTD-partijen, DVP en DVZA.
2. **Technische realisatie.** Technische realisatie van de varianten dienstbemiddeling en SSO-beleving.

Aanvullende theoretische verdieping

Gezamenlijke verdieping van dynamische dienstbemiddeling, waarmee in de toekomst de zorggebruiker bij meerdere zorgaanbieders in één keer meerdere gegevensdiensten kan verzamelen zonder opnieuw te hoeven authenticeren. Ten tijde van uitvoering van de PoC is dit niet beschikbaar voor zowel eTD als MedMij en daarmee nog niet ondersteund. Resultaten zijn verwerkt in de bevindingen.

Deelnemers *

Rol	Leverancier
PGO	Drimpy, Zorg & Welzijn Connect
DVZA	VECOZO
Herkenningsmakelaar	Signicat
Authenticatiedienst	UnifiedPost (Z-login)
BSNk	Logius

Tabel 4. Rollen en deelnemende leveranciers

*Leveranciers, behalve Logius (BSNk), hebben voor deelname aan de PoC een vergoeding ontvangen

Resultaten

- ☑ Succesvolle generieke koppeling (eindtest) tussen het eTD-stelsel en het MedMij-stelsel
- ☑ Dienstbemiddeling DVP: vooraf via een lijst kunnen aangeven bij welke zorgaanbieder je welke gegevensdiensten wil verzamelen
- ☑ Dienstbemiddeling DVZA (SSO-beleving): succesvolle beproeving van de mogelijkheid om niet opnieuw te hoeven authenticeren bij herhaaldelijke opvraging van gegevens bij dezelfde zorgaanbieder
- ☑ Dynamische dienstbemiddeling theoretisch uitgewerkt en een eerste voorstel voor specificaties opgezet
- ☑ Vastlegging eindtest (video)
- ☑ Eindrapportage met bevindingen en aanbevelingen

Hoofdstuk 3

Bevindingen & aanbevelingen

Categorisering bevindingen en aanbevelingen

In totaal zijn er ongeveer **45 bevindingen** aangeleverd.
Deze eindrapportage bevat alleen de belangrijkste bevindingen en aanbevelingen.

De bevindingen en aanbevelingen zijn besproken met MedMij en beheerorganisatie eTD

De bevindingen zijn gebaseerd op het beproeven met een klein aantal leveranciers.
Alvorens daadwerkelijk aanpassingen geadviseerd worden, wordt er aanbevolen om te onderzoeken of de opgedane bevindingen breder gedeeld worden door andere partijen.

Noodzakelijk	Ter verbetering	Ter overweging
Bevindingen en aanbevelingen die een ernstige belemmering vormen voor succesvolle implementatie in de praktijk.	Bevindingen en aanbevelingen die wezenlijk bijdragen aan de doorontwikkeling van het afsprakenstelsel en drempelverlagend werken voor de implementatie en landelijke uitrol.	Bevindingen en aanbevelingen die een bijdrage kunnen leveren aan doorontwikkeling van het afsprakenstelsel en succesvol opschalen.
Deze rapportage bevat zes noodzakelijke bevindingen	Deze rapportage bevat acht bevindingen ter verbetering	Deze rapportage bevat één bevinding ter overweging

Bevindingen & Aanbevelingen – Noodzakelijk

		Bevinding	Eigenaar	Aanbeveling
1	MedMij Afspraken-stelsel / eTD-stelsel	**Afstemming metadata eTD- en MedMij stelsel vergt meer onderzoek** In de PoC is het afstemmen van de MedMij-metadata en eTD-dienstcatalogus handmatig gedaan. Dat is niet gewenst en moet in de toekomst geautomatiseerd worden zodat een veilige consistente gebruikerservaring gecreëerd kan worden. Hiervoor zal de gebruiker bij de DVP, DVZA (zelf) en de eTD-authenticatiedienst dezelfde zorgaanbieder-organisatienaam moeten zien. Er mogen ook geen zorgaanbieders ontbreken in de ETD-Dienstcatalogus. Daarnaast moet de DVP in het huidige ontwerp eTD specifieke ServiceUUID's van alle zorgaanbieders kennen. Dat is niet schaalbaar.	Stichting MedMij, eTD	Onderzoek verschillende opties en impact (voor en nadelen) voor afstemming van (synchronisatie van) zorgaanbieder organisatienamen en maak een keuze. Onderzoek mogelijkheden van synchronisatie van de eTD service catalogus en MedMij zorgaanbiederslijst (ZAL)
2	eTD-stelsel	**Kosten voor authenticatiemiddelen zijn nog niet bepaald** Mocht er in de toekomst worden besloten dat eTD-authenticatiemiddelen binnen het MedMij Afsprakenstelsel gebruikt mogen worden, dan moet er tevens worden nagedacht over bij wie de kosten voor het gebruik van eTD-authenticatiemiddelen binnen het burgerdomein landen.	BZK	Onderzoek (voordat leveranciers binnen MedMij met eTD aan de slag gaan) of de verwachte kosten voor gebruik van eTD-middelen binnen het burgerdomein dusdanig zijn dat deze het gebruik binnen MedMij niet in de weg staan.
3	MedMij Afspraken-stelsel / eTD-stelsel	**ETD stopt bij dienstbemiddeling de Versleutelde-Identiteit@zorgaanbieder (DV)ZA in een EncryptedID@zorgaanbieder (DV)ZA, maar die is zo groot de DVP die niet in het MedMij-koppelvlak kan gebruiken.** Als tijdelijke oplossing werd de EncryptedID@zorgaanbieder (DV)ZA niet versleuteld voor de DVZA maar voor de DVP door het DVZA PKI-certificaat in de Dienstcatalogus te vervangen door het DVP-certificaat. Voor beveiliging is dit geen probleem, immers de DVP kan de Versleutelde-Identiteit@zorgaanbieder (DV)ZA die daarin staat niet ontsleutelen. Maar deze oplossing is niet netjes en niet schaalbaar naar meerdere DVP's.	Stichting MedMij, eTD	Onderzoek en implementeer een nette en schaalbare oplossing. Bijvoorbeeld: 1. Onderzoek of EncryptedID@zorgaanbieder (DV)ZA bij dienstbemiddeling standaard versleuteld moeten worden met PKI-certificaat van Dienstbemiddelaar (DVP). 2. Onderzoek of Medmij-koppelvlak meer ruimte moet krijgen voor een EncryptedID@zorgaanbieder (DV)ZA. 3. Onderzoek alternatieve oplossingen

Bevindingen & Aanbevelingen – Noodzakelijk

		Bevinding	Eigenaar	Aanbeveling
4	eTD-stelsel	**De docker-container voor decryptie (van BSNk-beheerorganisatie) viel tijdens de PoC door onbekende oorzaken geregeld uit wanneer hier gebruik van werd gemaakt** Een container is een verpakking (container) waarin codes en afhankelijkheden van een applicatie worden verpakt volgens een standaardformaat. Een docker-container bevat alles wat een applicatie nodig heeft om uit te voeren, zoals codes en systeemtools. De docker-container die wordt gebruikt voor decryptie viel tijdens de PoC geregeld uit. De oorzaak hiervan is onbekend.	eTD	Onderzoek de oorzaak van de uitval en bepaal op basis daarvan de benodigde maatregelen
5	eTD-stelsel	**De SAML vulling van Atlantis (testomgeving) is anders dan bij de authenticatiedienst** Security Assertion Markup Language (SAML) is een standaard dat wordt gebruikt om veilig authenticatie- en autorisatiegegevens van gebruikers tussen verschillende organisaties uit te wisselen. SAML-standaarden worden anders gehanteerd wanneer dat wordt vereist binnen een stelsel. Tijdens de PoC is ondervonden dat binnen het eTD-stelsels de SAML-standaard anders wordt gehanteerd door de testomgeving Atlantis en de authenticatiedienst. Met Atlantis kunnen niet alle dienstverleners (binnen het MedMij-stelsel) direct samenwerken.	eTD	Onderzoek hoe in de eTD-profielen kan worden gegarandeerd dat dienstverleners met alle authenticatiediensten naadloos kunnen samenwerken
6	eTD-stelsel	**Niet alle SAML-libraries kunnen de eTD SAML-standaard aan** De SAML-libraries (bibliotheken) kunnen verschillende elementen bevatten zoals het Advice-element. Het Advice-element maakt het voor organisaties mogelijk om extra informatie naar eigen keuze toe te voegen en kan genegeerd worden door applicaties. Echter, het Advice-element is de oorzaak waardoor sommige dienstverleners een error ontvangen binnen hun SAML-library. SAML wordt in zijn algemeenheid complexer ervaren dan Oauth van MedMij	eTD	Onderzoek of het Advice-element vervangen kan worden

Bevindingen & Aanbevelingen – Ter verbetering

		Bevinding	Eigenaar	Aanbeveling
1	eTD-stelsel	**De implementatie van het SAML-koppelvlak van eTD is voor een PGO zonder juiste (hot) debugging erg complex** Het SAML-koppelvlak van eTD is complex en nieuw, waardoor snel fouten gemaakt kunnen worden. Inzage in logging is niet mogelijk voor DVP's, waardoor fouten minder snel worden gevonden en DVP's afhankelijk zijn van herkenningsmakelaren voor ondersteuning.	eTD	Onderzoek waar MedMij-dienstverleners behoefte aan hebben wat betreft ondersteuning in het technisch realiseren
2	eTD-stelsel	**Er is diepgaande kennis nodig van ETD om te begrijpen waar de verschillende vereiste metadata voor zijn en hoe ze toegepast dienen te worden** Er zijn verschillende metadata bestanden nodig zodat alle partijen elkaars informatie hebben. Denk aan de SAML metadata van de HM en SAML metadata van de DVP/DVZA. Ook de eTD dienstencatalogus. En ook de netwerkmetadata van het BSNk.	eTD	Zorg voor een duidelijke handleiding en ondersteuning in een onboardingsproces van de herkenningsmakelaar
3	eTD-stelsel	**Benodigde certificaten zijn lastig te begrijpen en worden op een ongebruikelijke manier aangeleverd** De herkenningsmakelaar heeft van de DV een PKIo-certificaat nodig voor meerdere doeleinden. Voor de DV's zijn de doeleinden lastig te begrijpen. Bovendien worden de certificaten op een ongebruikelijke manier aangeleverd waardoor er een handleiding nodig is om ze daadwerkelijk te kunnen gebruiken.	eTD	Zorg voor een duidelijke handleiding en ondersteuning in een onboardingsproces van de herkenningsmakelaar

Bevindingen & Aanbevelingen – Ter verbetering

		BEVINDING	EIGENAAR	AANBEVELING
4	eTD-stelsel	**Het is onduidelijk voor dienstverleners (DV's) hoe bepaald kan worden welk EncryptedID een pseudoniem of een identiteit bevat** Het is niet direct duidelijk (of eenvoudig) hoe bepaald kan worden welk EncryptedID een pseudoniem bevat of een identiteit. Een identiteit of pseudoniem vergt voor het ontsleutelen een andere actie, waardoor het belangrijk is dat voorafgaand het ontsleutelen duidelijk is welk variant is gestuurd.	eTD	Onderzoek / denk na, over wijze van onboarding voor DV's
5	MedMij Afspraken-stelsel / eTD-stelsel	**Zorggebruikers moeten via een PGO een authenticatiedienst koppelen** Op dit moment is het niet mogelijk om als zorggebruiker direct gebruik te maken van een authenticatiedienst bij het inloggen op de PGO. Een zorggebruiker moet eerst inloggen en een authenticatiedienst koppelen om vervolgens met behulp van een authenticatiedienst te kunnen inloggen.	Stichting MedMij, eTD	Onderzoek / denk na, over wijze van onboarding voor DV's Maak het mogelijk om ook met eTD-middelen in te kunnen loggen in de PGO, zonder dat de PGO-gebruiker een account met een ander authenticatiemiddel moet aanmaken
6	MedMij Afspraken-stelsel / eTD-stelsel	**Zorggebruiker moet veel keuzes maken voordat er gegevens verzameld kunnen worden** Een zorggebruiker heeft mogelijk ook net een lastige keuze gemaakt welke PGO hij wil gebruiken en moet (potentieel) bij de eerste inlog direct weer een lastige keuze maken. Voor landelijke uitrol is ten eerste transparante communicatie in het netwerk vereist. Dit betekent dat het PGO haar gebruiker voorafgaand aan uitwisseling met Zorgaanbieder X moet kunnen voorbereiden op het inlogmiddel van X.	Stichting MedMij, eTD	Onderzoek / denk na, over wijze van onboarding voor zorggebruikers

Bevindingen & Aanbevelingen – Ter verbetering

		BEVINDING	EIGENAAR	AANBEVELING
7	eTD-stelsel	**Beproefde scenario's dienen verder te worden uitgewerkt om zowel een hoge beveiliging als gebruiksvriendelijkheid te garanderen** Dynamische dienstbemiddeling is wenselijk en deels haalbaars, maar daarnaast zal een SSO-beleving ook een must zijn voor een goede totaaloplossing. Uitdaging hierbij is om wel te blijven voldoen aan de vereiste betrouwbaarheidsniveaus.	eTD	Onderzoek naar hoe dynamische dienstbemiddeling te realiseren op niveau hoog, met daarin elementen van SSO-beleving Ontwerp dynamische dienstbemiddeling in combinatie met een SSO-beleving op een hoog betrouwbaarheidsniveau goed
8	MedMij Afspraken-stelsel / eTD-stelsel	**Docker-container ondersteunt dienstverleners, maar kan nog verbeterd worden** Voordelen: • Platformonafhankelijke manier van decryptie die qua implementatie en gedrag gelijk is voor alle partijen. • Een deel van de complexiteit is hiermee geabstraheerd Verbeterpunten: • De implementatie zou nog meer kunnen abstraheren. Het ontsleutelen van pseudoniemen vereist nu een specifieke call die geen identiteiten kan ontsleutelen. En andersom geeft de call voor het ontsleutelen van een identiteit een foutmelding als een pseudoniem wordt aangeboden. Het zou helpen als er 1 methode is die beide varianten kan ontsleutelen. • Het gebruik van Docker stelt extra eisen aan de infrastructuur om te kunnen hosten • Moet op een intern netwerk gehost worden omdat de container zelf geen beveiliging biedt. Dat is binnen een PoC lastig om in te richten, voor productie geen probleem. • Bij het starten van de container kreeg deze soms een andere TCP-port toegewezen waardoor de authorization server geen verbinding kan maken. • Onduidelijk in hoeverre de DVZA/DVP zelf nog beveiligingsmaatregelen moet treffen voor zaken die zich binnen de container afspelen.	Stichting MedMij, eTD	Onderzoek of het mogelijk is om de docker-container door te ontwikkelen zodat nog meer complexiteit weggenomen kan worden.

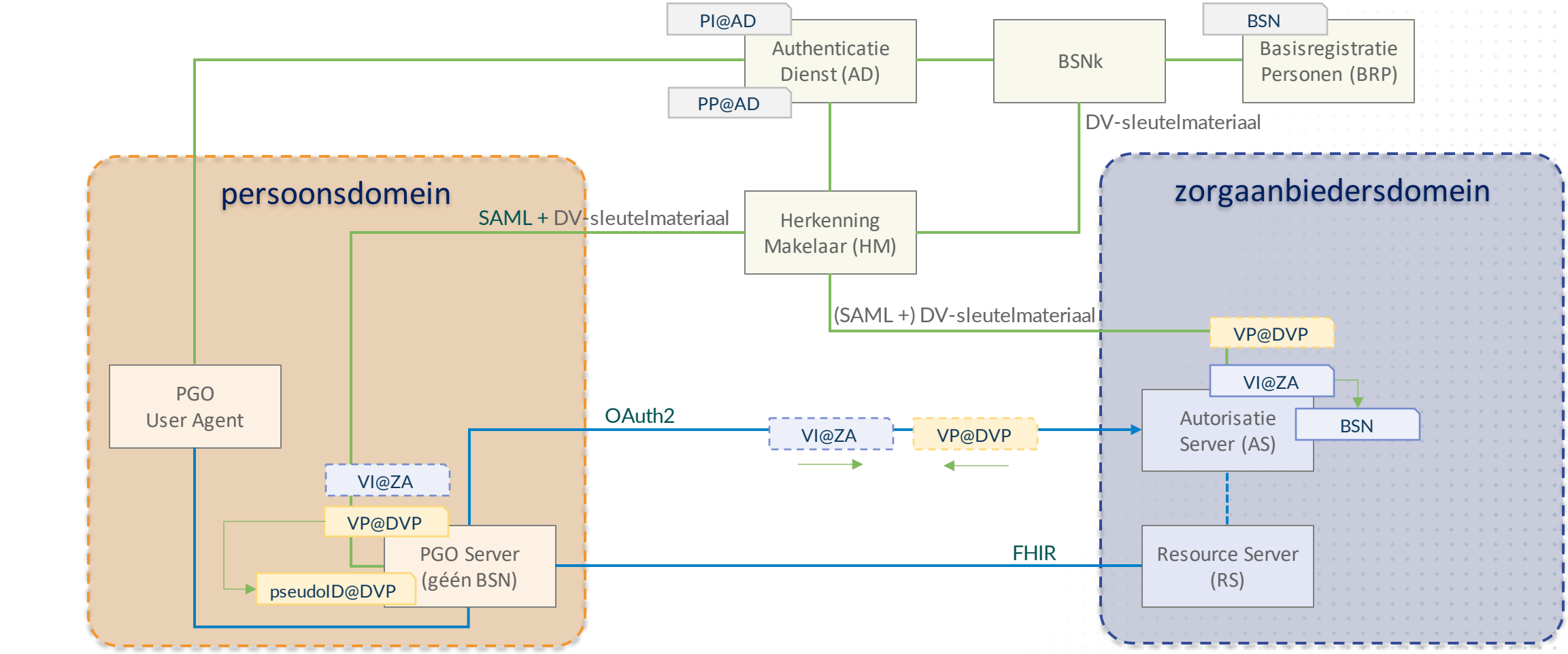
Bevindingen & Aanbevelingen – Ter overweging

		BEVINDING	EIGENAAR	AANBEVELING
1	MedMij Afspraken-stelsel / eTD-stelsel	**Het op de juiste wijze gebruiken van het eTD SAML-koppelvlak middels een no-code platform is complex** Door leveranciers met veel ervaring in hard-coding werd het gebruik en inbouwen van eTD SAML-koppelvlakken als complex ervaren. Dit geldt voor no/low-code platform leveranciers nog meer.	Stichting MedMij, eTD	Onderzoek hoe partijen die een no/low-code platform gebruiken ondersteund kunnen worden bij het gebruiken van een eTD SAML-koppelvlak

Hoofdstuk 4

Bijlagen

Bijlage 1: Architectuurplaat PoC eTD



Bijlage 2: Overzicht PoC's