EINDRAPPORTAGE PROVES

ATTRIBUUT-GEBASEERDE AUTHENTICATIE

PROOF OF CONCEPT 2019/2020

16 juli 2020
Versie: 1.0
Martijn Mallie, Marcel Settels, Ron van Holland & Quinten van Geest

MANAGEMENTSAMENVATTING

Inleiding

Authenticatie binnen MedMij kent diverse uitdagingen, waaronder: DigiD is niet erg gebruiksvriendelijk, de koppeling van de identiteit van de zorggebruiker in het persoons- en zorgaanbiedersdomein is niet erg sterk, DigiD op niveau Substantieel is nog niet breed beschikbaar en het aansluiten van zorgaanbieders op DigiD gaat gepaard met hoge vaste kosten. Dit alles bemoeilijkt uitrol van MedMij in de praktijk.

In de Proof of Concept (PoC) is een oplossing uitgewerkt en succesvol technisch beproefd om op basis van attributen te authenticeren in de zorgsector. Attributen zijn eigenschappen van personen (bijv. naam en leeftijd) waaruit de identiteit afgeleid kan worden. Attributen worden opgeslagen in een *attributen-wallet*.

Doelstellingen en uitgangspunten

De **doelstellingen** van de PoC zijn als volgt:

1. Bevorderen van de gebruiksvriendelijkheid van authenticatie
2. Mogelijkheid bieden om niet opnieuw te hoeven authenticeren bij herhaalde opvraging van gegevens bij dezelfde zorgaanbieder
3. Realiseren van een sterkere koppeling tussen identiteiten in het persoonsdomein en zorgaanbiedersdomein (t.b.v. veiligheid)
4. Beproeven van een oplossing die authenticatie op eIDAS niveau Substantieel mogelijk maakt
5. Opleveren van 'raamwerk' voor Afsprakenstelsel attribuut-gebaseerde authenticatie*

De volgende **uitgangspunten** zijn gehanteerd:

- De oplossing past binnen het MedMij Afsprakenstelsel
- De oplossing is neutraal en te implementeren met verschillende attributen-wallets
- Geen verwerking van BSN in het persoonsdomein

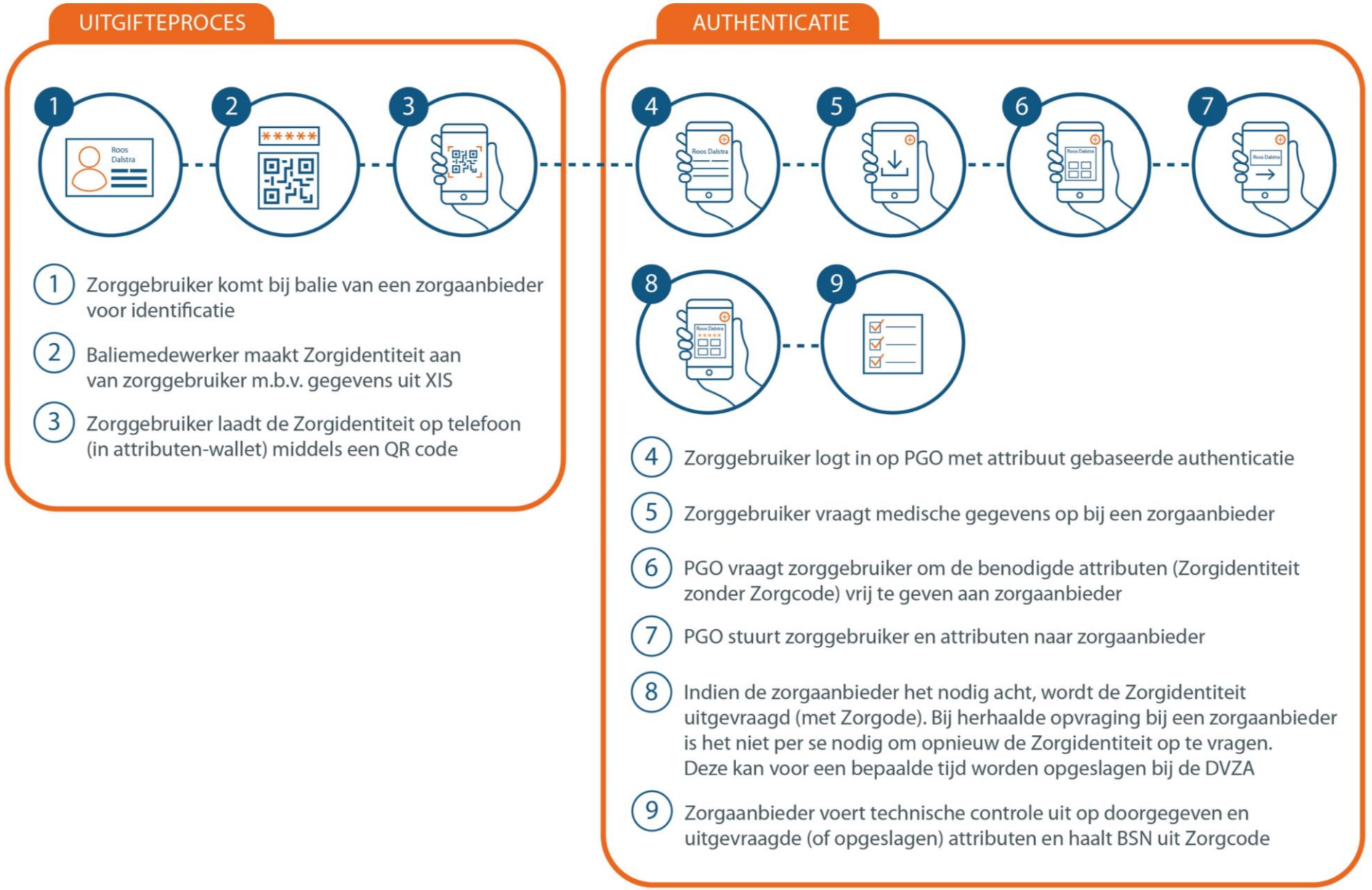
Zorgidentiteit van zorggebruiker

In de PoC is het concept *Zorgidentiteit* geïntroduceerd. Dit is een verzameling van attributen van een zorggebruiker die zijn digitale identiteit in de zorg borgt. Een belangrijk onderdeel van de Zorgidentiteit, naast attributen zoals voorletter(s), voornaam, achternaam etc., is het attribuut *Zorgcode*. De Zorgcode is een versleuteld attribuut uitgegeven door een zorgaanbieder, bestaande uit het BSN, de URA van de zorgaanbieder en een volgnummer. Dit attribuut kan enkel door zorgaanbieders worden ontsleuteld en wordt tussen zorgaanbieders onderling vertrouwd. Dat betekent dat het BSN niet wordt verkregen door niet-rechtmatige partijen.

Oplossing in een notendop

Zie figuur 1 voor een schematische weergave van het proces van authenticatie op basis van attributen vanuit het perspectief van een zorggebruiker. Daarbij wordt onderscheid gemaakt tussen het **uitgifteproces van de Zorgidentiteit** bij de balie van een zorgaanbieder en het **gebruik van attribuut-gebaseerde authenticatie** om gegevens te verzamelen bij een zorgaanbieder via een PGO. Bekijk ook de video.

* Dit afsprakenstelsel bestaat momenteel nog niet, maar wordt mogelijk vormgegeven naar aanleiding van deze PoC



Figuur 1. Functionele uitwerking van oplossing vanuit het perspectief van de zorggebruiker

MANAGEMENTSAMENVATTING

Resultaten

De oplossing is gedurende de PoC nader uitgewerkt met experts van betrokken partijen: AET, ChipSoft, Drimpy, Ivido, MedMij, VECOZO en VZVZ. Experts van IRMA zijn geconsulteerd gedurende de PoC. Tevens hebben de betrokken partijen de oplossing technisch gerealiseerd.

Externe experts hebben een juridische analyse en security quickscan uitgevoerd op de oplossing (interne documenten). Hier is een aantal aanvullende aandachtspunten uit voortgekomen. Alle opgehaalde input vormt een 'raamwerk' voor het Afsprakenstelsel attribuut-gebaseerde authenticatie.

De behaalde resultaten in relatie tot doelstellingen

1. Bevorderen van de gebruiksvriendelijkheid van authenticatie binnen MedMij, door in persoonsdomein en zorgaanbiedersdomein met hetzelfde middel te kunnen authenticeren.
De oplossing maakt het mogelijk om met één authenticatiemiddel in zowel de PGO als bij de zorgaanbieder te authenticeren.

2. Bieden van de mogelijkheid om niet opnieuw te hoeven authenticeren bij herhaalde opvraging van gegevens bij dezelfde zorgaanbieder.
In de oplossing is herauthenticatie bij een zorgaanbieder geïntroduceerd, doordat een getekende set attributen doorgegeven wordt van een PGO naar de DVZA. De DVZA kan besluiten om de Zorgcode voor een bepaalde tijd te bewaren (als dit past binnen de risicoanalyse van de zorgaanbieder). Hierdoor hoeft niet opnieuw geauthenticeerd te worden door de zorggebruiker als deze opnieuw gegevens wilt opvragen bij de desbetreffende zorgaanbieder. Het is aan de DVZA en zorgaanbieder om hier invulling aan te geven.

3. Realiseren van een sterkere koppeling tussen identiteiten in het persoonsdomein en zorgaanbiedersdomein (t.b.v. veiligheid).
De koppeling tussen identiteiten in het persoonsdomein en zorgaanbiedersdomein is versterkt door het doorgeven van een getekende set attributen. Daarmee is het een sterke verbetering ten opzichte van de huidige situatie met DigiD. De koppeling kan verder versterkt worden als de Zorgcode in beide domeinen gebruikt mag worden (en dus toegevoegd wordt aan de getekende set attributen die vanuit PGO naar de DVZA wordt gestuurd). Op basis van de PIA lijkt dit mogelijk, omdat de Zorgcode niet wordt gezien als (pseudo) BSN en er dus geen juridische bezwaren zijn om de Zorgcode te verwerken in het persoonsdomein.

4. Beproeven van een oplossing die authenticatie op eIDAS niveau Substantieel mogelijk maakt.
Er zijn geen bevindingen opgedaan die in de weg staan om de beproefde vorm van authenticatie op eIDAS niveau Substantieel te krijgen. In de security scan zijn enkele aandachtspunten naar voren gekomen die helpen dit te bewerkstelligen.

5. Opleveren van 'raamwerk' voor Afsprakenstelsel attribuut-gebaseerde authenticatie.
Alle opgedane kennis en input is verwerkt in diverse minimale eisen en uitgangspunten voor het Afsprakenstelsel attribuut-gebaseerde authenticatie.

Doordat de oplossing generiek is opgezet, kan deze breder ingezet worden dan enkel voor MedMij. Denk hierbij aan authenticatie van zorgverleners en zorgmedewerkers. Dit dient nader uitgewerkt te worden in een business-case, waarin de verwachte kosten afgewogen worden tegen de baten.

MANAGEMENTSAMENVATTING

Borgen randvoorwaarden

Een aantal bevindingen en aanbeveling is aangemerkt als randvoorwaardelijk. Dat betekent dat deze zaken als eerste opgepakt dienen te worden als vervolgstap. De vragen die in de eerste stap beantwoord dienen te worden zijn als volgt:

1. Welke exacte eisen dienen vastgelegd te worden in het Afsprakenstelsel attribuut-gebaseerde authenticatie omtrent de (her)uitgifte van de Zorgidentiteit op betrouwbaarheidsniveau Substantieel, zoals voorgeschreven door eIDAS?

2. Wat is de exacte set van attributen die gezamenlijk de Zorgidentiteit vormen, waarbij aangesloten wordt bij de set attributen zoals gedefinieerd door eIDAS?

3. Kan meer zekerheid worden verkregen (middels een juridische toets en bij de Autoriteit Persoonsgegevens) dat de Zorgcode (versleuteld BSN) rechtmatig wordt verwerkt door de desbetreffende partijen?

4. Kunnen zorgaanbieders gebruik (blijven) maken van attribuut-gebaseerde oplossingen, die voldoen aan een op te zetten afsprakenstelsel, als de Wet Digitale Overheid in werking is getreden?

Conclusie en vervolgstappen

Een aantal bevindingen op het gebied van veiligheid en juridica dient eerst opgelost te worden en genoemde risico's dienen gemitigeerd (of geaccepteerd) te worden als eerste vervolgstap.

1. **Borgen randvoorwaarden:** de bevindingen die als randvoorwaardelijk zijn aangemerkt nader uitzoeken.

2. **Gebruikerspanel:** een onderzoek naar gebruiksvriendelijkheid van de beproefde oplossing met eindgebruikers, waarbij de oplossing wordt afgezet tegen een andere vorm van authenticatie (DigiD-Substantieel).

3. **Business-case:** inzichtelijk maken op welke vlakken de oplossing ingezet kan worden (naast authenticatie van patiënten binnen MedMij) en wat de investeringen en besparingen zijn op korte en lange termijn.

4. **Plan van aanpak:** na bestuurlijk akkoord een plan van aanpak opstellen om het Afsprakenstselsel attribuut-gebaseerde authenticatie te concretiseren

5. **Uitwerken Afsprakenstelsel:** afsprakenstelsel attribuut-gebaseerde authenticatie uitwerken tot 80% voordat het beproefd wordt in de praktijk.

6. **Pilot:** kleinschalig in de praktijk de oplossing beproeven met een coalitie van zorgverleners, zorggebruikers en leveranciers ter verbetering van de oplossing en het afsprakenstelsel.

7. **Gecontroleerde livegang:** opschaling van gebruik in de praktijk

INHOUDSOPGAVE

HOOFDSTUK 1
PROVES MEDMIJ

ACHTERGROND EN DOELSTELLING

Achtergrond

Sinds 2018 voert het programma PROVES technische beproevingen uit, genaamd *Proof of Concepts* (PoC), op het afsprakenstelsel en gegevensdiensten. In 2019 zijn hier gecontroleerde livegangen bij gekomen, waarin patiënten een Persoonlijke Gezondheids Omgeving (PGO) gebruiken en medische gegevens uitwisselen. Tijdens de PoC wordt onder andere gekeken naar de (technische) maakbaarheid, informatiestandaarden, haalbaarheid, gemeenschappelijke voorzieningen en beveiligingsaspecten.

Met een standaard werkwijze per route van PGO-leverancier, resource server, autorisatie server en zorgaanbieder, zijn er in 2019 diverse technische beproevingen uitgevoerd met nieuwe gegevensdiensten en functionaliteiten van het afsprakenstelsel.

Het uitgangspunt is dat elke functionaliteit of gegevensdienst die binnen MedMij wordt geïntroduceerd, of een significante verandering ondergaat, via een PoC wordt beproefd. De beproevingen leiden tot (noodzakelijke) verbetervoorstellen aan het programma MedMij en Nictiz (indien van toepassing).

In deze eindrapportage worden de bevindingen en aanbevelingen gerapporteerd uit het derde PoC traject van 2019: *attribuut-gebaseerde authenticatie*.

Doelstelling

De scope van deze PoC richt zich op authenticatie van de patiënt in het persoons- en zorgaanbiedersdomein. In de beproefde oplossing wordt gebruik gemaakt van attribuut-gebaseerde authenticatie.

Resultaten

Deze PoC levert informatie op over een nieuwe manier van authenticatie op basis van attributen (naast DigD) voor PGO-leveranciers, DVZA-leveranciers, xIS-leveranciers, uitwisselingsstructuren en zorgaanbieders. In 2020 zijn de volgende resultaten opgeleverd:

- Technische realisatie van oplossing
- Testrapportages van leveranciers
- Privacy Impact Analyse (PIA) van oplossing (intern document)
- Security quickscan van oplossing (intern document)
- Eindrapportage

AANPAK PROVES MEDMIJ

Inhoud werkwijze

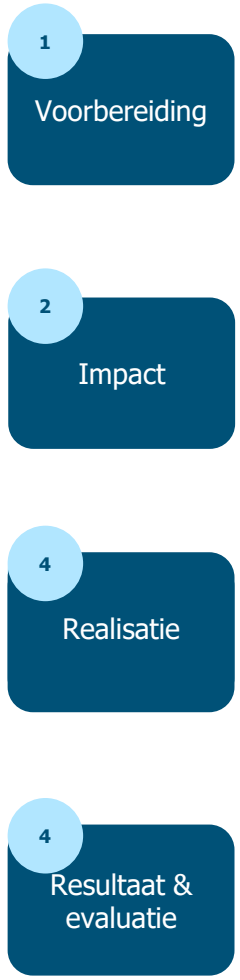
De verschillende stappen van de PoC zijn uitgewerkt aan de rechterkant. Deze uitwerking geeft tevens per processtap zicht op de resultaten.

Vergoeding softwareleveranciers

De softwareleveranciers die deelnemen aan de PoC ontvangen een tegemoetkoming in kosten voor het meewerken aan een eindtest en opleveren van een testrapportage.
Softwareleveranciers worden niet vergoed voor het ontwikkelen van software en/of voorzieningen.

Gebruik afsprakenstelsel

Deze PoC is uitgevoerd op basis van versie 1.1 van het MedMij Afsprakenstelsel. In versie 1.2 van het Afsprakenstelsel wordt niet expliciet voorgeschreven dat DigiD als authenticatiemiddel in het zorgaanbiedersdomein gebruikt dient te worden.



Voorbereiding
Helder gedefinieerde routes
Helderheid over kosten en vergoedingen
Informele toezegging van leveranciers
Kick-off moment gepland

Impactanalyse
Opstellen overeenkomsten leveranciers
Houden van de kick-off
Bepalen benodigde middelen
Opstellen gedragen planning

Realisatie
Realiseren van de benodigde technisch en functionele voorzieningen
(Eind)testen van de uitwisseling

Resultaat & evaluatie
Opleveren van de testrapportages door leveranciers
Opstellen eindrapportage met advies richting programma MedMij en stuurgroep VZVZ

HOOFDSTUK 2
CONTEXT, AANPAK & RESULTATEN

CONTEXT

Authenticatie binnen MedMij

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

Figuur 2. Huidige flow van authenticatie bij zorgaanbieder

Uitdagingen

De huidige situatie kent de volgende uitdagingen, zoals:

- Authenticatie met DigiD is niet gebruiksvriendelijk. Een zorggebruiker moet eerst in zijn/haar PGO authenticeren. Vervolgens moet de zorggebruiker voor iedere opvraging van gegevens bij iedere zorgaanbieder authenticeren. Dat betekent dat ook bij herhaalde opvraging op een later tijdstip, waarbij dezelfde gegevens bij dezelfde zorgaanbieder worden opgevraagd, de zorggebruiker (opnieuw) moet authenticeren.
- De koppeling van de identiteit van de zorggebruiker in het persoons- en zorgaanbiedersdomein is niet erg sterk. Dat betekent theoretisch gezien dat gegevens van zorggebruiker A in de PGO van zorggebruiker B terecht kunnen komen.
- Het authenticatieniveau moet in de zorg zo spoedig mogelijk naar niveau Substantieel worden gebracht. Op dit moment is DigiD op niveau Substantieel nog niet breed beschikbaar.
- Het aansluiten op DigiD gaat voor zorgaanbieders gepaard met hoge vaste kosten (met name de jaarlijkse audit). Dit zorgt voor een grote drempel voor de uitrol van MedMij in de praktijk.
- Het BSN mag niet gebruikt worden in het persoonsdomein

PROOF OF CONCEPT ATTRIBUUT-GEBASEERDE AUTHENTICATIE

Doelstellingen

Om de huidige uitdagingen te overwinnen, is in 2019 een PoC gestart voor attribuut-gebaseerde authenticatie. De doelstellingen van de PoC zijn als volgt:

1. Bevorderen van de gebruiksvriendelijkheid van authenticatie binnen MedMij, door in persoons- en zorgaanbiedersdomein met hetzelfde middel te kunnen authenticeren
2. Bieden van de mogelijkheid om niet opnieuw te hoeven authenticeren bij herhaalde opvraging van gegevens bij dezelfde zorgaanbieder
3. Realiseren van een sterkere koppeling tussen identiteiten in het persoons- en zorgaanbiedersdomein (t.b.v. veiligheid)
4. Beproeven van een oplossing die authenticatie op eIDAS niveau Substantieel mogelijk maakt
5. Opleveren van 'raamwerk' voor Afsprakenstelsel attribuut-gebaseerde authenticatie

Authenticatie met attributen

Attributen zijn eigenschappen van personen (bijv. geslacht en leeftijd) die gebruikt kunnen worden voor authenticatie. Op basis van attributen kan de identiteit van een persoon afgeleid worden. Attributen worden opgeslagen in een *attributen-wallet*.

Kenmerkend voor deze nieuwe vorm van authenticatie is dat de basis uitgifte van het authenticatiemiddel eenvoudig en anoniem kan plaatsvinden. Aan het anonieme middel worden stapsgewijs attributen toegevoegd, ieder met een eigen vertrouwensniveau. Het is aan de ontvanger om de verschillende attributen te 'vertrouwen'. De gebruiker bepaalt zelf welke attributen vrij-gegeven worden bij authenticatie als antwoord op een vraag van een 'verifier' die attributen nodig heeft. Deze nieuwe vorm van authenticatiemiddelen biedt een hoge mate van flexibiliteit, welke in de PGO en zorgaanbiedercontext is toegepast.

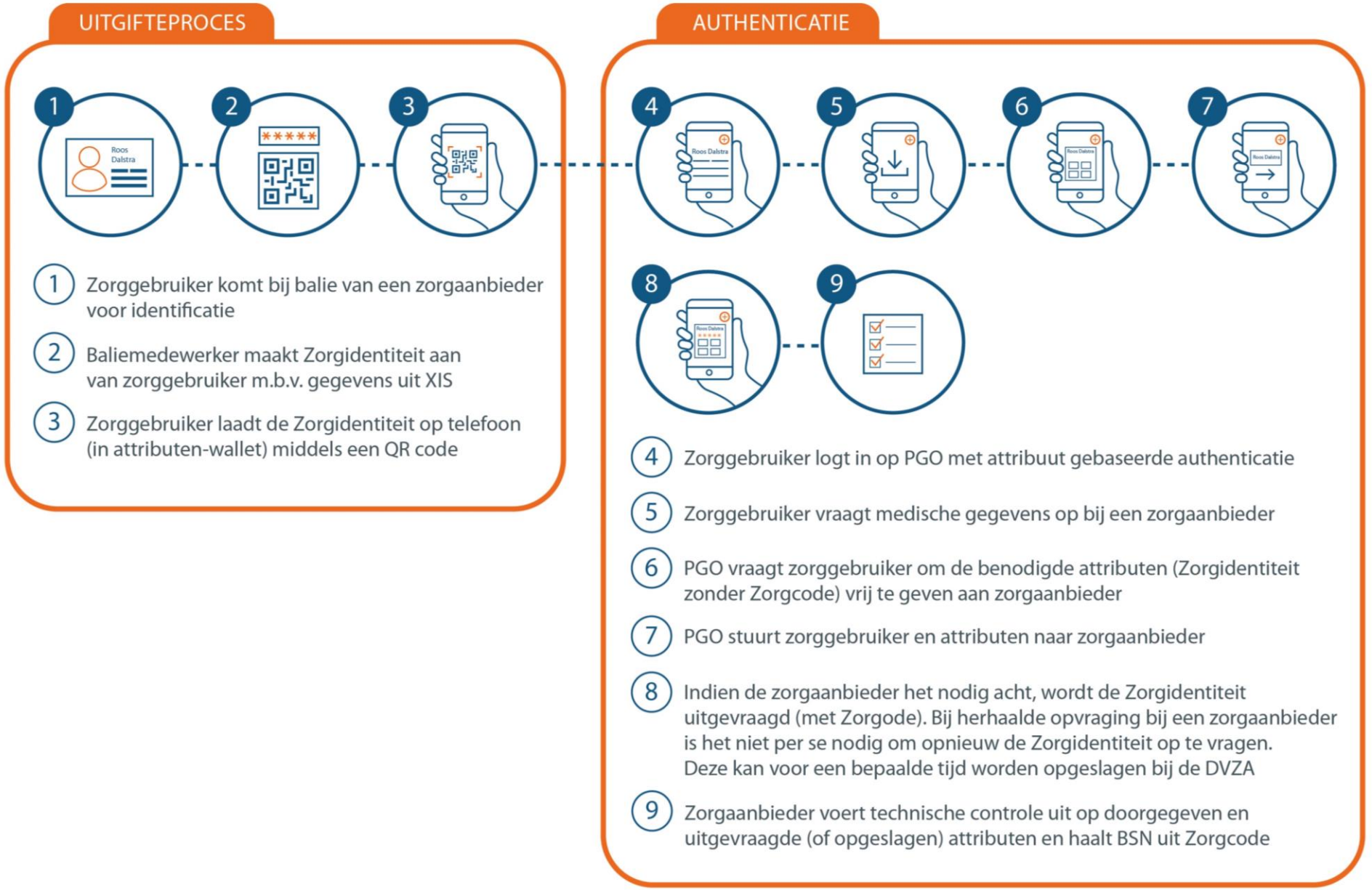
Uitgangspunten

Tijdens de PoC zijn de volgende uitgangspunten gehanteerd:

- De oplossing past binnen het MedMij Afsprakenstelsel
- De oplossing is neutraal en te implementeren met verschillende attributen-wallets
- Geen verwerking van BSN in het persoonsdomein

Oplossing vanuit zorggebruikersperspectief

In figuur 3 (volgende pagina) is de beproefde oplossing schematisch weergegeven vanuit het perspectief van de zorggebruiker. Klik hier voor een video van de oplossing.



Figuur 3. Functionele uitwerking van oplossing zoals technisch is beproefd vanuit perspectief van de zorggebruiker

TOELICHTING BEPROEFDE OPLOSSING IN POC

In de PoC is het concept *Zorgidentiteit* geïntroduceerd. De Zorgidentiteit is een verzameling van attributen van een zorggebruiker die zijn of haar digitale identiteit in de zorg borgt. De Zorgidentiteit wordt uitgegeven door de zorgaanbieder aan de balie (*face-to-face* proces met identificatie).

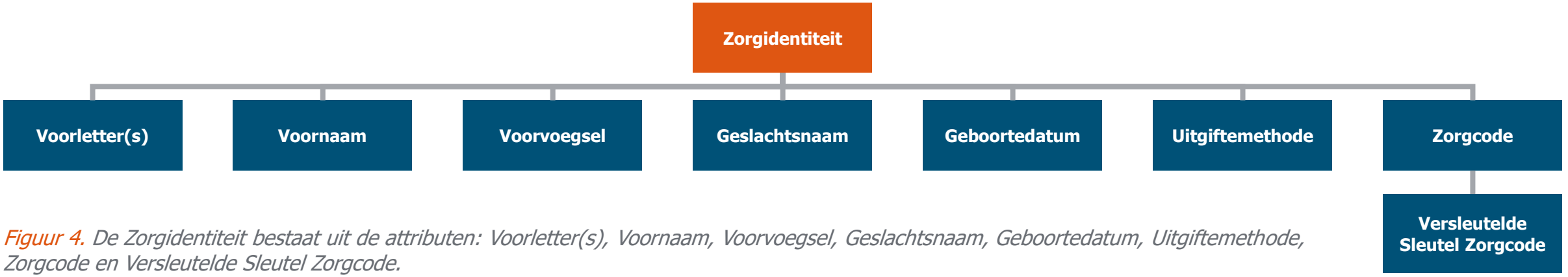
Zorgidentiteit

De Zorgidentiteit bestaat uit de een verzameling van de volgende attributen: Voorletter(s), Voornaam, Voorvoegsel, Geslachtsnaam, Geboortedatum, Uitgiftemethode, Zorgcode en Versleutelde Sleutel van Zorgcode (zie figuur 4).

De *Uitgiftemethode* is de wijze waarop de zorgidentiteit is uitgegeven (in de PoC: aan de balie van een zorgaanbieder).

De *Zorgcode* is een versleuteld attribuut (onleesbare string letters en cijfers) dat wordt uitgegeven door een zorgaanbieder, bestaande uit het BSN van de zorggebruiker, de URA van de uitgevende zorgaanbieder en een volgnummer. Dit attribuut valt enkel door zorgaanbieders te ontsleutelen (en dus te gebruiken).

De *Versleutelde Sleutel Zorgcode* is een sleutel die is versleuteld door een gemeenschappelijke sleuteldienst (*trusted third party*). De zorgaanbieder laat de versleutelde sleutel ontsleutelen door deze sleuteldienst, waarna de zorgaanbieder deze kan gebruiken om decentraal het BSN te extraheren uit de Zorgcode. Hierdoor is het mogelijk dat alle zorgaanbieders het BSN kunnen verkrijgen en wordt voorkomen dan het BSN door een extra (centrale) partij wordt verwerkt. Bekijk de kenmerken van de Zorgidentiteit.



Figuur 4. De Zorgidentiteit bestaat uit de attributen: Voorletter(s), Voornaam, Voorvoegsel, Geslachtsnaam, Geboortedatum, Uitgiftemethode, Zorgcode en Versleutelde Sleutel Zorgcode.

TOELICHTING BEPROEFDE OPLOSSING IN POC

Uitgifte Zorgidentiteit

Een zorggebruiker kan haar Zorgidentiteit ophalen bij haar zorgaanbieder (bijvoorbeeld het ziekenhuis of de huisarts). Het uitgeven van de verzameling attributen behorende bij de Zorgidentiteit gebeurt middels een *face-to-face* balieproces. Dat houdt in dat de zorggebruiker aan de balie van de zorgaanbieder haar identiteitsbewijs moet tonen en dat na controle de attributen aangemaakt worden op basis van gegevens uit het xIS. De attributen worden aan de zorg-gebruiker aangeboden middels een QR-code. Door het scannen van de QR-code via de telefoon wordt de Zorgidentiteit toegevoegd aan de attributen-wallet van de zorggebruiker.

Gebruik Zorgcode

De Zorgcode, als attribuut behorende bij de Zorgidentiteit, kan enkel gebruikt worden in het zorgaanbiedersdomein. In de context van MedMij houdt dat in dat bij het verzamelen/delen van gegevens vanuit een PGO de DVZA de Zorgcode kan uitvragen uit de attributen-wallet van de zorggebruiker. De zorggebruiker kan de Zorgcode vrijgeven, waarna de DVZA het attribuut kan ontsleutelen (door het laten ontsleutelen van de bijbehorende Versleutelde Sleutel Zorgcode). Zorgaanbieders vertrouwen onderling de Zorgcode, wat betekent dat een Zorgcode die is uitgegeven door ziekenhuis A door huisarts B ontsleuteld kan worden.

Fasering van PoC

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

1. **Doorgeven van attribuut van DVP naar DVZA.** In deze fase is de technische basis gelegd om attributen van DVP naar een DVZA door te sturen. Ook is het opvragen van attributen uit de attributen-wallet van de zorggebruiker door de DVZA ontwikkeld.

2. **Doorgeven van verzameling attributen.** Nadat de techniek is gebouwd om attributen door te geven van DVP naar DVZA, is dit uitgebreid met het doorgeven van een *verzameling* attributen (de Zorgidentiteit, zonder de Zorgcode). Dit gebeurt in de vorm van een ondertekend contract, omdat dit extra zekerheden biedt qua beveiliging ten opzichte van het doorsturen van losse attributen.

3. **Versleuteling van Zorgcode (theoretisch).** In de laatste fase is de versleuteling van de Zorgcode theoretisch uitgewerkt. Dit zorgt voor veiligheid en borging dat het BSN niet onnodig wordt verwerkt door (niet-rechtmatige) partijen.

Zie Bijlage 1 t/m 3 voor een nadere (technische) uitwerking van de beproefde oplossing, inclusief ontwikkelde koppelvlakken.

ROLLEN EN BETROKKEN LEVERANCIERS

Rol	Leverancier	Omschrijving
Uitgever Zorgidentiteit	ChipSoft	• Genereren en uitgeven van de Zorgidentiteit aan de gebruiker middels een QR-code
PGO	Drimpy, Ivido	• Inloggen in PGO op basis van attributen • Drimpy vraagt attributen uit via de Attributenmakelaar • Ivido vraagt attributen zelf uit bij attributen-wallet • Geeft ondertekend contract (Zorgidentiteit zonder Zorgcode) mee in authorization request
Attribuut Makelaar en SDK voor uitgifte Zorgidentiteit	AET	• Aanbieden van generiek OpenID Connect (OIDC) koppelvlak op attributen-wallet t.b.v. PGO en uitgifte Zorgidentiteit • Uitvragen attributen bij zorggebruiker
Autorisatieserver en resource server	VECOZO	• Authenticeert gebruiker met behulp van Zorgidentiteit • Geeft resources terug aan PGO

In de PoC is de attributen-wallet IRMA (*I Reveal My Attributes*) toegepast. IRMA is open-source software van Privacy by Design Foundation. Privacy by Design Foundation is op diverse momenten geconsulteerd gedurende de PoC. Tevens is aan Privacy by Design aangeboden om schriftelijk te reageren op de bevindingen uit de security quickscan en privacy impact analyse. Deze reactie is terug te lezen in Bijlage 4.

RESULTATEN

SPECIFICATIE EN REALISATIE VAN TECHNISCHE OPLOSSING

GESLAAGDE EINDTEST

TESTRAPPORTAGES OPGELEVERD

INVENTARISATIE EISEN ATTRIBUUT-GEBASEERDE AUTHENTICATIE*

SECURITY QUICKSCAN EN PRIVACY IMPACT ANALYSE OPGELEVERD

* In Bijlage 5 en 6 staan diverse minimale eisen en uitgangspunten voor het Afsprakenstelsel attribuut-gebaseerde authenticatie geformuleerd die zijn gebaseerd op alle opgedane kennis en inzichten.

HOOFDSTUK 3
AANBEVELINGEN

AANBEVELINGEN

Gedurende de PoC zijn er veel bevindingen opgedaan die direct verwerkt zijn in de beproefde oplossing. Middels evaluatievragen zijn er ongeveer 60 punten naar voren gekomen op basis waarvan de aanbevelingen in deze rapportage geformuleerd zijn.

In deze eindrapportage zijn de belangrijkste aanbevelingen opgenomen in de onderstaande categorieën.
Per aanbeveling is middels een label aangegeven of deze van toepassing is op Afsprakenstelsel MedMij en/of Afsprakenstelsel attribuut-gebaseerde authenticatie (AGA) en hoe belangrijk het is (ter overweging, ter verbetering, noodzakelijk of randvoorwaardelijk). Aanbevelingen die een randvoorwaarde zijn, dienen z.s.m. geborgen te worden. De bevindingen en aanbevelingen zijn teruggekoppeld aan Stichting MedMij en VZVZ.

GEBRUIKSVRIENDELIJKHEID

In hoeverre wordt de oplossing gebruiksvriendelijk geacht door de softwareleverancier vanuit het perspectief van de burger?

VEILIGHEID

In hoeverre is de oplossing veilig om te gebruiken?

TECHNISCH

In hoeverre is de oplossing technisch implementeerbaar?

JURIDISCH

In hoeverre is de oplossing juridisch implementeerbaar?

SCHAALBAARHEID

In hoeverre is de oplossing generiek schaalbaar naar landelijke zorg?

GEBRUIKSVRIENDELIJKHEID

1

De *user experience* van attributen-wallets dient zo hoog mogelijk te zijn. Dit is randvoorwaardelijk voor bredere toepassing dan enkel in de zorgsector en voor het vertrouwd raken van (zorg)gebruikers met een dergelijke applicatie (en oplossing). Dit komt landelijke uitrol ten goede.
Leveranciers hebben opgemerkt dat in het kader van *user experience* er ook aandacht besteed dient te worden aan een duidelijke (scope) naam van attributen en de berichtgeving richting (zorg)gebruiker over het vrijgeven van attributen aan ontvangers (verifiers).
Dit dient opgenomen te worden in het Afsprakenstelsel attribuut-gebaseerde authenticatie.

●●

2

De uitgifte van de Zorgidentiteit moet op een toegankelijke en gebruiksvriendelijke manier plaatsvinden, waarbij betrouwbaarheidsniveau Substantieel het uitgangspunt is.
Softwareleveranciers geven aan dat er in de uitwerking van het uitgifteproces van de Zorgidentiteit rekening moet worden gehouden met diverse factoren zoals: uitgifte bij zoveel mogelijk zorgverleners (die elkaar onderling vertrouwen), zorggebruikers met fysieke beperkingen en beschikbaarheid van internet bij de balie van de zorgaanbieder.

●●●

3

De geldigheidsduur van attributen en een gebruiksvriendelijke methode om deze te vernieuwen moeten nader worden uitgewerkt.
De bevinding is dat de Zorgidentiteit een maximale geldigheidsduur moet hebben en dat het (na verlopen hiervan) op een gebruiksvriendelijke manier verlengd moet kunnen worden (idealiter onafhankelijk van het uitgifteproces). Ook moet worden nagedacht over het opnieuw ophalen van de Zorgidentiteit op het moment dat de zorggebruiker een nieuwe smartphone heeft. Zowel de geldigheidsduur, verlenging en heruitgifte van de Zorgidentiteit dient uitgewerkt te worden in het Afsprakenstelsel attribuut-gebaseerde authenticatie.

●●●

● Ter overweging ●● Ter verbetering ●●● Noodzakelijk ●●●● Randvoorwaarde Voor MedMij Voor AGA

GEBRUIKSVRIENDELIJKHEID

4

Zorggebruikers dienen van goede informatie te worden voorzien, zodat ze bekend worden met de Zorgidentiteit en het gebruik hiervan.
Er is geconstateerd dat leveranciers twijfelen of de oplossing in de praktijk voldoende kenbaar wordt bij zorggebruikers (naast DigiD), wat een risico vormt voor opschaling. Om dit risico te mitigeren, kan er bijvoorbeeld worden nagedacht over het verstrekken van informatiemateriaal bij zorgaanbieders, waarin de werking van de Zorgidentiteit wordt uitgelegd en zorggebruikers voorbereid naar de balie van de zorgaanbieder komen.

VEILIGHEID

1

De eIDAS checklist moet als basis dienen voor de afspraken die vastgelegd dienen te worden over hoe de Zorgidentiteit op betrouwbaarheidsniveau Substantieel uitgegeven kan worden.
Door softwareleveranciers is opgemerkt dat er een eIDAS checklist bestaat voor uitgifte van middelen op betrouwbaarheidsniveau Substantieel. Dit dient meegenomen te worden in het Afsprakenstel attribuut-gebaseerde authenticatie.

●●●●

2

Alle cruciale softwarecomponenten (zoals Attributenmakelaar, gemeenschappelijke sleuteldienst en attributen-wallet) moeten een beveiligingsaudit doorstaan.
Vanuit softwareleveranciers is aangegeven dat het wenselijk is dat alle cruciale softwarecomponenten een beveiligingsaudit ondergaan. Dit kan vastgelegd worden in het Afsprakenstelsel attribuut-gebaseerde authenticatie in de vorm van een proces van kwalificatie en acceptatie.

●●●

3

Onderzocht moet worden of de oplossing verbeterd kan worden door de getekende set attributen te koppelen aan de PGO van de zorggebruiker.
Softwareleveranciers hebben geconstateerd dat de beproefde oplossing veiliger kan als bij het doorgeven van de getekende set attributen een koppeling gemaakt kan worden met de PGO (waar de set is ondertekend). Hiermee kan de DVZA de set attributen controleren opdat het afkomstig is van de PGO die het ook ondertekend heeft. Zo voorkom je dat de getekende set attributen niet op een andere manier misbruikt kan worden.

●●

● Ter overweging ●● Ter verbetering ●●● Noodzakelijk ●●●● Randvoorwaarde Voor MedMij Voor AGA

VEILIGHEID

4

De set van attributen die wordt afgesproken dient gezamenlijk zo uniek mogelijk te zijn en de inhoud moet niet op een andere wijze gespeld en/of ingevoerd kunnen worden.
Er is opgemerkt door softwareleveranciers dat het risico bestaat dat bij gebruik van bijvoorbeeld voornaam en voorletters deze afwijkend kunnen zijn tussen zorgaanbieders. Dit zou opgelost kunnen worden door attributen uit betrouwbare bronnen op te halen, zoals het BRP. Daarbij is het wel essentieel dat een dergelijk attribuut is uitgegeven op betrouwbaarheidsniveau Substantieel.

●●

5

De set attributen dient vastgesteld te worden, waarbij zo goed mogelijk aangesloten wordt bij de set attributen zoals gedefinieerd door eIDAS.
Zie documentatie: eIDAS SAML Attribute Profile. Dit dient opgenomen te worden in het Afsprakenstelsel attribuut-gebaseerde authenticatie en afgestemd te worden met het MedMij Afsprakenstelsel.

●●●●

6

Om te voorkomen dat een PGO het BSN attribuut kan uitlezen, dient er gewerkt te worden met een BSN versleuteling (zoals theoretisch uitgewerkt in deze PoC). Dit is een neutrale oplossing, onafhankelijk van de attributen-wallet.
Door softwareleveranciers is aangegeven dat op een generieke wijze voorkomen moet worden dat een PGO een BSN attribuut kan uitlezen. Er zijn twee mogelijkheden: het BSN versleutelen (zoals theoretisch uitgewerkt in deze PoC) of werken op basis van een verifier-whitelist. In het tweede geval dient whitelisting voor verifiers ondersteund te worden door de attributen-wallet, met als gevolg afhankelijkheden van deze attributen-wallet en dus een niet-neutrale oplossing.

●●●●

● Ter overweging ●● Ter verbetering ●●● Noodzakelijk ●●●● Randvoorwaarde Voor MedMij Voor AGA

VEILIGHEID

7

Voer een risicoanalyse uit op de beschikbaarheid van de gemeenschappelijke sleuteldienst en de bijbehorende certificaten en werk vervolgens uit hoe hiermee om te gaan in de oplossing en de processen.
Wanneer de versleuteldienst niet beschikbaar is of certificaten gecompromitteerd zijn, kunnen de Zorgcodes niet worden ontsleuteld.

●●●

8

Zorg ervoor dat attributen waarmee wordt ingelogd in de PGO op een betrouwbare wijze zijn gekoppeld aan een persoon en zorg ervoor dat ook een relatie kan worden gelegd met attributen uit de Zorgidentiteit (bijv. via naam en geboortedatum).
Om zeker te stellen dat de persoon die zich authenticeert in het zorgaanbiedersdomein dezelfde is als degene die inlogt in een PGO is meer nodig dan enkel vaststellen dat dezelfde IRMA app is gebruikt. Welke identiteit gebonden is aan een IRMA app is geheel afhankelijk van de identiteitscontroles van de attribuut verstrekkers. Bij design zit er geen enkel mechanisme in IRMA om te controleren dat alle attributen bij één persoon horen.

●●●

● Ter overweging ●● Ter verbetering ●●● Noodzakelijk ●●●● Randvoorwaarde Voor MedMij Voor AGA

TECHNISCH

1

Het centraal specificeren van de Attributenmakelaar endpoints moet verder worden uitgewerkt.
Softwareleveranciers hebben aangegeven dat geborgd moet worden dat enkel met de juiste OIDC providers op de juiste manier wordt gecommuniceerd. MedMij zal hierbij moeten vertrouwen op het Afsprakenstelsel attribuut-gebaseerde authenticatie, waarin de endpoints opgenomen dienen te worden. Als meerdere authenticatiemethodes toegevoegd gaan worden binnen MedMij, zal mogelijk een extra lijst met geaccepteerde stelsels gecreëerd moeten worden.

●●

2

De oplossing moet gebaseerd zijn op open standaarden (zoals nu is beproefd) en de koppelvlakken dienen technisch te zijn uitgeschreven.
Softwareleveranciers geven aan dat het belangrijk is dat er zoveel mogelijk uit wordt gegaan van de standaard OIDC en JWT-token specificatie voor het format van attributen. Tevens geeft men aan dat de koppelvlakken volledig technisch uitgeschreven moeten worden ter bevordering van implementatie.

●●●

3

Er dient voorkomen te worden dat de oplossing leidt tot het bouwen van nieuwe services/servers door DVP's.
De authenticatie via een Attributenmakelaar vereist enkel uitbreiding op de programmering van de bestaande MedMij authenticatie en leidt niet tot het bouwen van nieuwe services/servers door DVP's. Het gebruik van een Attributenmakelaar maakt de oplossing makkelijker om te implementeren door DVP's dan dat er niet wordt gewerkt met een Attributenmakelaar.

●

● Ter overweging ●● Ter verbetering ●●● Noodzakelijk ●●●● Randvoorwaarde Voor MedMij Voor AGA

TECHNISCH

4

Het moet mogelijk zijn voor EPD's en DVZA's om zowel op basis van een SDK of een REST service de attributen uit te kunnen geven.
Het toepassen van een SDK of een REST service heeft als voordeel dat het authenticatiemiddel voor uitgifte en uitvraag van attributen kan worden vervangen door, en aangevuld met, andere authenticatiemiddelen. Er mag geen afhankelijkheid gecreëerd worden van één leverancier die het mogelijk maakt om attributen uit te geven door zorgaanbieders. Dit betekent dat een open stelsel van authenticatiemiddelen aanbieders wordt nagestreefd (geen aanbesteding aan één partij).

●

5

In het Afsprakenstelsel MedMij dient opgenomen te worden dat in de authorization request een getekende set attributen meegegeven kan worden.
Leveranciers hebben aangegeven dat het de voorkeur heeft om te werken met gespecificeerde unieke parameternamen en parameterwaarden in de authorization request, omdat dit ook wordt toegepast bij andere OIDC implementaties (bijvoorbeeld de 'resource' en 'connection' parameters).

●●

6

Om neutraal te blijven is het belangrijk een gemeenschappelijke dienst in te richten waarmee de identiteit en aanverwante gegevens opgehaald kunnen worden door partijen.
Deze voorziening kan naast DigiD de verschillende attribuut-toepassingen implementeren, zodat automatisch alle DVP- en DVZA-leveranciers over dezelfde functionaliteit beschikken.

●●

● Ter overweging ●● Ter verbetering ●●● Noodzakelijk ●●●● Randvoorwaarde  Voor MedMij  Voor AGA

TECHNISCH

7

Onderzocht dient te worden of binnen MedMij de ZAL uitgebreid kan worden, zodat een DVP vooraf vast kan stellen of een DVZA in staat is om een getekende set attributen te accepteren.
Door softwareleveranciers is aangegeven dat het voor een DVP waarschijnlijk noodzakelijk is om vooraf vast te kunnen stellen of een DVZA in staat is een getekende set attributen te accepteren, zodat het proces voor de zorggebruiker gebruiksvriendelijk verloopt. Daarbij is het een optie om dit te beleggen in de MedMij ZAL, zodat dergelijke functionaliteiten (op het gebied van authenticatie) van een DVZA geraadpleegd kan worden.

●

8

Nader juridisch onderzocht dient te worden of de DVP de Zorgcode zou mogen verwerken, waardoor de getekende set attributen die wordt doorgegeven van DVP naar DVZA 100% overeenkomt met de attributen die de DVZA uitvraagt.
Omdat de DVP de Zorgidentiteit zonder Zorgcode doorgeeft aan de DVZA, matcht deze set niet 100% met de attributen die de DVZA uitvraagt (Zorgidentiteit met Zorgcode).

●●

● Ter overweging ●● Ter verbetering ●●● Noodzakelijk ●●●● Randvoorwaarde Voor MedMij Voor AGA

JURIDISCH

1

Onderzoek hoe de oplossing zich verhoudt tot de Wet Digitale Overheid (WDO) en stem af met betrokken stakeholders binnen de overheid.
De WDO zou beperkingen kunnen opwerpen voor authenticatiemiddelen die gebruikt mogen worden in de zorg.

●●●

2

Objectief vaststellen (middels juridische toets en bij de Autoriteit Persoonsgegevens) dat de Zorgcode (versleuteld BSN) rechtmatig wordt verwerkt door partijen.
Er zit een aanname in de PIA van de oplossing omtrent verwerking van de Zorgcode (versleuteld BSN). De beproefde situatie is nieuw die geen vergelijking kent in Nederland. Hierdoor is niet uit te sluiten dat de onderbouwing van de rechtmatigheid ergens in de keten door anderen, zoals de Autoriteit Persoonsgegevens, kan worden betwist.

●●●●

● Ter overweging ●● Ter verbetering ●●● Noodzakelijk ●●●● Randvoorwaarde Voor MedMij Voor AGA

SCHAALBAARHEID

1

De beproefde oplossing kan (snel) opgeschaald worden door deze op te nemen binnen de GBZ-eisen voor aansluiting op de AORTA infrastructuur (o.a. voor het LSP).
Softwareleveranciers hebben aangegeven dat uitgifte van attributen aan zorggebruikers enkel mogelijk is indien de zorggebruiker is aangesloten bij een zorgaanbieder die de attribuut uitgifte methode ondersteunt. Dit kan een potentieel risico zijn voor opschaling.

●

2

Om neutraal te blijven voor verschillende attributen-wallets wordt er aanbevolen om de uitvraag te doen via een gemeenschappelijke dienst (zoals een Attributenmakelaar).
Daarbij is het wel belangrijk dat attributen-wallets het ondertekenen van een set attributen ondersteunen.

●●

3

Enkel de strikt noodzakelijke afspraken dienen vastgelegd te worden in het Afsprakenstelsel attribuut-gebaseerde authenticatie, zodat de oplossing goed geadopteerd kan worden in het veld.
Door softwareleveranciers is aangegeven dat er geen zaken vastgelegd dienen te worden in het Afsprakenstelsel attribuut-gebaseerde authenticatie die reeds in andere stelsels zijn opgenomen en dat bijvoorbeeld één volledige afgesproken set van attributen, inclusief uitgevers, opgenomen wordt. Het afsprakenstelsel dient onafhankelijk te zijn van het MedMij Afsprakenstelsel, zodat er geen afhankelijkheden zijn bij doorontwikkeling. Tevens dient nagedacht te worden over hoe het Afsprakenstelsel attribuut-gebaseerde authenticatie zich verhoudt tot de WDO.

●●

● Ter overweging ●● Ter verbetering ●●● Noodzakelijk ●●●● Randvoorwaarde Voor MedMij Voor AGA

SCHAALBAARHEID

4

Onderzoek wat de potentiële kosten zijn per zorgaanbieder voor het realiseren van het uitgifteproces.
Door softwareleveranciers is opgemerkt dat er voor zorgaanbieders kosten in rekening zullen worden gebracht voor het inbouwen van deze vorm van authenticatie. Dit geldt echter ook voor andere vormen van authenticatie, zoals een DigiD-koppeling.

●

5

Om op te kunnen schalen, dient op korte termijn het Afsprakenstelsel attribuut-gebaseerde authenticatie verder uitgewerkt en beproefd te worden in de praktijk.
Door softwareleveranciers is aangegeven dat er rekening gehouden moet worden met de ontwikkelingen rond Toegangsverleningsservice (TVS) en de benodigde inspanningen vanuit de softwareleveranciers. Het risico bestaat dat, ondanks deze inspanningen, nog geen brede beschikbaarheid komt van authenticatiemiddelen op niveau Substantieel of hoger, terwijl dat met het Afsprakenstelsel attribuut-gebaseerde authenticatie wel te realiseren is.

●●

6

Vanuit veiligheidsredenen is gekozen voor het ondertekenen en valideren van een set attributen, wat ondersteund dient te worden door attributen-wallets en ingebouwd dient te worden door de DVP en DVZA.
Softwareleveranciers hebben opgemerkt dat de huidige oplossing deels afhankelijk is van attributen-wallets (in de PoC IRMA) en het inbouwen van de oplossing (met name het ondertekenen en doorgeven van een set attributen) door DVP's en DVZA's.

●

● Ter overweging ●● Ter verbetering ●●● Noodzakelijk ●●●● Randvoorwaarde Voor MedMij Voor AGA

SCHAALBAARHEID

7

Onderzoek wat de impact is op MedMij voor het ondersteunen van meerdere authenticatie oplossingen door DVP's en DVZA's.
Door softwareleveranciers is opgemerkt dat het ondersteunen van meerdere authenticatie oplossingen enerzijds verwarrend kan zijn voor zorggebruikers, omdat niet duidelijk is bij welke partijen je met welk middel kan authenticeren (een Attributenmakelaar biedt hier uitkomst). Anderzijds wordt het voor DVZA-leveranciers complexer, omdat ze alle mogelijke (attribuut-gebaseerde) oplossingen voor authenticatie dienen te implementeren die DVP-leveranciers gebruiken. Daarmee wordt de lat voor deelname aan MedMij hoger gelegd en dat strookt mogelijk niet met de ambitie om snel op te schalen wat betreft gebruik van PGO's. Via een gemeenschappelijke dienst kan de complexiteit (tot op bepaalde hoogte) teruggebracht worden.

●● Ter verbetering

RANDVOORWAARDELIJKE BEVINDINGEN

Op basis van de bevindingen is er nog een aantal openstaande vragen die op de korte termijn beantwoord dienen te worden, omdat deze randvoorwaardelijk zijn. Deze vragen worden opgepakt in de vervolgstappen (zie pagina 45). De vragen luiden als volgt:

1. Welke exacte eisen dienen vastgelegd te worden in het Afsprakenstelsel attribuut-gebaseerde authenticatie omtrent de (her)uitgifte van de Zorgidentiteit op betrouwbaarheidsniveau Substantieel, zoals voorgeschreven door eIDAS?
2. Wat is de exacte set van attributen die gezamenlijk de Zorgidentiteit vormen, waarbij aangesloten wordt bij de set attributen zoals gedefinieerd door eIDAS?
3. Kan meer zekerheid worden verkregen (middels een juridische toets en bij de Autoriteit Persoonsgegevens) dat de Zorgcode (versleuteld BSN) rechtmatig wordt verwerkt door de desbetreffende partijen?
4. Kunnen zorgaanbieders gebruik (blijven) maken van attribuut-gebaseerde oplossingen, die voldoen aan een op te zetten afsprakenstelsel, als de Wet Digitale Overheid in werking is getreden?

HOOFDSTUK 4
UITWERKING VERSLEUTELING ZORGCODE

VERSLEUTELING VAN ZORGCODE

Het versleutelen van de Zorgcode is gedurende de PoC nader theoretisch uitgewerkt met betrokken partijen in de vorm van een consensusoplossing. Daarbij zijn de volgende uitgangspunten gehanteerd:

- Minimalisatie van verwerking van data. Dat betekent dat er in de PoC zo min mogelijk gebruik is gemaakt van 'kale' BSN's.
- Geen (centrale) verwerking van het BSN door niet-rechtmatige partijen. Oftewel: enkel zorgaanbieders mogen het BSN ontsleutelen.
- De Zorgcode wordt vertrouwd door alle zorgaanbieders.
- Veiligheid moet geborgen zijn.

Beoogde oplossing

De Zorgidentiteit bevat naast de Zorgcode een sleutel waarmee de Zorgcode kan worden ontsleuteld. Deze sleutel is zelf ook weer versleuteld (attribuut: Versleutelde Sleutel Zorgcode).

In het XIS wordt middels een versleuteloperatie de Zorgcode aangemaakt. De hiervoor gebruikte sleutel wordt versleuteld door de gemeenschappelijke sleuteldienst, wat resulteert in de Versleutelde Sleutel Zorgcode.

Wanneer een zorgaanbieder het BSN moet verkrijgen uit de Zorgcode, laat de zorgaanbieder de Versleutelde Sleutel Zorgcode ontsleutelen door de gemeenschappelijke sleuteldienst. Vervolgens kan de zorgaanbieder zelf het BSN uit de Zorgcode extraheren. Hierdoor wordt het BSN enkel verwerkt door de zorgaanbieder.

De Versleutelde Sleutel Zorgcode kan enkel door de gemeenschappelijke sleuteldienst worden ontsleuteld. Dit wordt slechts gedaan voor zorgaanbieders.

Zie Bijlage 7 voor de technische uitwerking van de oplossing voor versleuteling van de Zorgcode.

HOOFDSTUK 5
SAMENVATTING SECURITY QUICKSCAN

SAMENVATTING SECURITY QUICKSCAN

In het kader van de PoC is een security quickscan uitgevoerd door een externe security specialist. Deze quickscan richt zich enerzijds op de consensus oplossing voor versleuteling van de Zorgcode* en anderzijds specifiek op de toegepaste attributen-wallet (IRMA). De hoofdbevindingen uit deze quickscan zijn hieronder weergegeven.

Uitgifte en versleuteling Zorgcode

- Identificatie van de gebruiker is betrouwbaar, omdat uitgifte van de Zorgcode plaatsvindt na controle van de identiteit van de gebruiker aan de balie van de zorgaanbieder. De kwaliteit van uitvoering kan verschillen, waardoor de betrouwbaarheid van de oplossing gelijk is aan de zwakste uitvoering van uitgifte.
- Door uitgifte van de Zorgcode in twee stappen uit te voeren**, wordt er geborgd dat enkel de zorgaanbieder verwerker van het BSN is (en niet een gemeenschappelijke sleuteldienst).
- Bij verlies van de centrale sleutel (voor de versleuteling van de sleutels) worden alle daarmee uitgegeven Zorgcodes onbruikbaar (*single point of failure*).

Gemeenschappelijke authenticatiedienst

- De Zorgcode is relatief statisch***, waardoor iedere partij die de Zorgcode in communicatie kan waarnemen, de gebruiker kan observeren en linken aan eerdere bezoeken.
- De gemeenschappelijke versleuteldienst en gemeenschappelijke authenticatiedienst zijn *single points of failure* en de risico's die hiermee gepaard gaan moeten gemitigeerd worden (bijvoorbeeld door dubbele uitvoering van deze gemeenschappelijke diensten).

* Met de betrokken partijen is een oplossing uitgewerkt omtrent het versleutelen van de Zorgcode. Daarbij wordt uitgegaan van een gemeenschappelijke sleuteldienst die versleuteling van de sleutels verzorgt en daarmee geen verwerker van het BSN is

** De zorgaanbieder versleutelt het BSN; de daarvoor gebruikte sleutel wordt centraal versleuteld

*** Iedere uitgifte leidt tot een unieke nieuwe Zorgcode

SAMENVATTING SECURITY QUICKSCAN

Attributen-wallet IRMA

- De attributen-wallet moet onderworpen worden aan certificering door een externe audit op punten van beveiliging. Er is nog geen volledige audit uitgevoerd op de attributen-wallet.
- Er is geconstateerd dat voor beveiligde opslag van attributen wordt vertrouwd op de beveiliging van het onderliggende operating systeem. In de nieuwe versie van de applicatie zijn de attributen versleuteld opgeslagen op de telefoon.
- De attributen kunnen gekloond worden, waarbij het mogelijk is een kopie van gegevens te maken. Dit vereist wel dat eerst het OS gecompromitteerd wordt. Om deze gegevens te kunnen misbruiken (de attributen gebruiken) moet de PIN-code achterhaald worden van de applicatie. De bezit factor valt daarom te ondermijnen; het attribuut is niet sterk (fysiek) aan het desbetreffende toestel gebonden.
- Er zijn geen maatregelen tegen *phishing* genomen. De gebruiker kan verleid worden het attribuut vrij te geven aan een partij buiten het zorgaanbiedersdomein. In de beproefde oplossing is mede hierom gewerkt met een Zorgcode die enkel door zorgaanbieders in het zorgaanbiedersdomein ontsleuteld kan worden.

HOOFDSTUK 6
SAMENVATTING PRIVACY IMPACT ANALYSE

SAMENVATTING PRIVACY IMPACT ANALYSE

In het kader van de PoC is door een externe jurist een PIA opgesteld voor de beproefde oplossing en de gebruikte attributen-wallet IRMA. Dit is een intern document.

Er kan gesteld worden dat een attribuut-gebaseerd authenticatiemiddel, waarbij gebruik wordt gemaakt van de Zorgcode, juridisch haalbaar is. Wel dienen de bevindingen opgepakt te worden. In het Afsprakenstelsel attribuut-gebaseerde authenticatie moet worden opgenomen dat bij attribuut-gebaseerde authenticatie middelen geen sprake mag zijn van BSN-verwerking en/of ongeoorloofde verwerking van persoonsgegevens (met inachtneming van aanbevelingen uit de PIA).

De hoofdbevindingen uit de PIA worden hieronder kort toegelicht.

- Mogelijke privacy-risico's ten aanzien van de betrouwbaarheid van de authenticatie hangen samen met (onder andere) welke attributen worden gebruikt en de definitieve invulling van de oplossing.
- Het verwerken van het BSN is een belangrijk punt in de risicoweging.
  - Er is vastgesteld dat op plaatsen waar het BSN niet mag worden verwerkt dit ook niet als zodanig gebeurt in de PoC (encryptie) en daar waar het BSN wel wordt verwerkt er een grondslag voor bestaat in wetgeving.
  - De beproefde situatie is een nieuwe, die geen vergelijking kent in Nederland. Hierdoor is het niet uit te sluiten dat de onderbouwing van de rechtmatigheid ergens in de keten door anderen (zoals de Autoriteit Persoonsgegevens) kan worden betwist. Dit is een belangrijk punt van bewustzijn, omdat het verwerken van het BSN zonder grondslag een groot privacy-risico is.
- Er kan een privacy-risico volgen uit het gebruik van IRMA:
  - Het borgen van een goed toestemmingsproces is essentieel voor het hebben van een geldige grondslag van gegevensverwerking met IRMA. In IRMA geeft de gebruiker expliciet toestemming.
  - Een passende beveiliging is essentieel voor het succes en de rechtmatigheid van IRMA (zowel qua toegangsbeveiliging als betrouwbaarheidsniveau van authenticatie).
  - Wanneer de Wet digitale overheid van kracht wordt, is het van belang dat IRMA onder de toegelaten middelen valt en wordt genotificeerd om aan de wet te voldoen.

HOOFDSTUK 7
OPLOSSING IN RELATIE TOT MEDMIJ

OPLOSSING IN RELATIE TOT MEDMIJ

Om de oplossing binnen MedMij te passen, wordt geadviseerd ten minste de volgende zaken uit te werken:

- MedMij wordt geadviseerd te specificeren op welke wijze attributen doorgegeven kunnen worden in de Oauth flow (idealiter een getekende set attributen).
- PROVES adviseert om binnen MedMij ruimte te bieden in het zorgaanbiedersdomein om niet opnieuw te hoeven authenticeren bij herhaalde opvraging van gegevens bij dezelfde zorgaanbieder.
- Binnen MedMij wordt aanbevolen om authenticatie op basis van attributen toe te staan, waarbij vertrouwd wordt op een toekomstig Afsprakenstelsel voor attribuut-gebaseerde authenticatie.

HOOFDSTUK 8
OPLOSSING IN BREDER PERSPECTIEF

OPLOSSING IN BREDER PERSPECTIEF

Huidige ontwikkelingen

- Patiëntauthenticatie/patiëntidentificatie is een veel besproken onderwerp, zeker als het over de grens van de zorgaanbieders heen gaat:
  - 'Commerciëlen' moeten niet voorzien kunnen worden van middelen om gegevensverzamelingen ongewild aan elkaar te koppelen. Een 'domein'-specifieke identificatie is hiervoor wenselijk
  - Het 'hergebruiken' van verstrekte waarborgen (*signed attributes*) lijkt internationaal steeds meer ingang te vinden
- De UZI-pas zal op termijn binnen de Wet Digitale Overheid /eHerkenningsstelsel (eID) en de Toegangsverleningsservice (TVS) dienst van BZK/VWS als 'een' authenticatiemiddel worden gezien en niet als 'het' authenticatiemiddel binnen de zorg. De ontwikkeling van signed attributes bij de UZI-pas van het Centraal Informatiepunt Beroepen en Gezondheidszorg (CIBG) is te verwachten maar zeker niet reeds besloten.

De toekomst

- Een authenticatiemiddel voor een persoon met daaraan gekoppelde (leesbare) attributen is het gewenste eindpunt, waarbij eveneens BSN, UZI-NR, UZI-Rolcode, Functie, Werkgever, Personeelsnummer, polymorf synoniem en Clubnummer gekoppeld kunnen worden.
- Uitgifte moet zeer zorgvuldig gaan plaatsvinden, zodat het op eIDAS niveau Hoog uitgegeven kan worden.
- Attributen moeten op de smartphone in een hoogwaardige digitale kluis worden opgeslagen. Er moet een vrije keus voor digitale kluizen ontstaan.
- Uniforme inlogmethodiek voor *single sign-on* op basis van oAuth (OpenID Connect) binnen de zorg met signed contracts.

HOOFDSTUK 9
VERVOLGSTAPPEN

VOORSTEL VERVOLGSTAPPEN

Borgen randvoorwaarden
De bevindingen die als randvoorwaardelijk zijn aangemerkt, dienen nader uitgezocht te worden.

1

Gebruikerspanel
Vergelijken van gebruiksvriendelijkheid tussen beproefde oplossing en DigiD met eindgebruikers. Het doel is om tot een go/no-go besluit te komen o.b.v. bevindingen.

2

Business-case uitwerken
Inzichtelijk maken op welke vlakken de oplossing ingezet kan worden en wat de investeringen en besparingen zijn op korte en lange termijn.

3

Plan van aanpak Afsprakenstelsel attribuut-gebaseerde authenticatie
Na bestuurlijk akkoord dient er een plan van aanpak opgesteld te worden om het Afsprakenstselsel attribuut-gebaseerde authenticatie te concretiseren.

4

Uitwerken Afsprakenstelsel attribuut-gebaseerde authenticatie
Het afsprakenstelsel uitwerken tot 80%, zodat het beproefd kan worden in de praktijk.

5

Pilot
Kleinschalig in praktijk beproeven met coalitie van zorgverleners, zorggebruikers en leveranciers. Input wordt verwerkt in nieuwe release van afsprakenstelsel.

6

Gecontroleerde livegang
Opschalen van gebruik in praktijk

7

Behoefte aan meer informatie?

Neem contact op met het programma PROVES

Martijn Mallie — programmamanager
martijn.mallie@vzvz.nl — 06-13310965

Quinten van Geest — projectleider
quinten.van.geest@vzvz.nl — 06-12636139

HOOFDSTUK 10
BIJLAGEN

OVERZICHT BIJLAGEN

Bijlage 1 Technische flow beproefde oplossing

Bijlage 2 Architectuur beproefde oplossing

Bijlage 3 Specificaties van de Attributenmakelaar results

Bijlage 4 Schriftelijke reactie Privacy by Design

Bijlage 5 Inventarisatie eisen voor Afsprakenstelsel attribuut-gebaseerde authenticatie

Bijlage 6 Uitgangpunten en requirements m.b.t. uitgifte en consumptie van attributen

Bijlage 7 Versleuteling van BSN

BIJLAGE 1: TECHNISCHE FLOW BEPROEFDE OPLOSSING

Zie bijlage 2 voor de bijbehorende architectuurplaat van de beproefde oplossing. In de oplossing is de volgende flow doorlopen:

1. Uitgifte Zorgidentiteit in zorgaanbiedersdomein (middels een *face-to-face* balieproces) en toevoegen van Zorgidentiteit aan attributen-wallet van gebruiker.
2. Gebruiker logt in op haar PGO
   a. Middels OIDC en IRMA via de Attributenmakelaar (AtM) o.b.v. email-attribuut
      - PGO Server stuurt hiervoor gebruiker naar de AtM met een OIDC authorization request (responsetype=code, client_id=<pgo_server>, scope=openid **irma_email**, redirect_uri, state)
      - AtM zet een IRMA sessie op met gebruiker en vraagt daarbij het email-attribuut
      - PGO Server ontvangt vervolgens een access code en haalt hiermee bij de AtM via een OIDC token request een id_token op. Het id_token is een JWT en bevat het gevraagde email attribuut (in de vorm van een ***IRMA_disclosure_result***)
   b. Direct via IRMA: o.b.v. email-attribuut (en eventueel andere eigen attributen van het PGO)
3. Wanneer gebruiker een interactie wil starten met een zorgaanbieder, dan vraagt haar PGO toestemming om attributen uit te mogen wisselen met zorgaanbieders
   a. Middels OIDC en IRMA via de AtM d.m.v. een ***message*** ondertekend met pgo_setA
      - PGO Server stuurt hiervoor gebruiker naar de AtM met een OIDC authorization request (responsetype=code, client_id=<pgo_server>, scope=openid **irma_medmij_contract**, redirect_uri, state)
      - AtM zet een IRMA sessie op met gebruiker en vraagt daarbij om een signature op de *message* o.b.v. **pgo_setA**
      - PGO Server ontvangt vervolgens een access code en haalt hiermee bij de AtM via een OIDC token request een id_token op. Het id_token is een JWT en bevat de gevraagde toestemming (in de vorm van een ***IRMA_signature_result***)

   a) Direct via IRMA: ***message*** ondertekend met pgo_set_A

BIJLAGE 1: TECHNISCHE FLOW BEPROEFDE OPLOSSING

4. PGO Server stuurt gebruiker met een regulier MedMij authorization request naar de autorisatieserver, met daaraan toegevoegd een ***medmij_contract*** parameter. Deze parameter bevat een JWT met het ***IRMA_signature_result***.

5. Autorisatieserver verifieert het ontvangen medmij_contract via een REST call op de AtM (deze retourneert een status)

6. Autorisatieserver authenticeert gebruiker

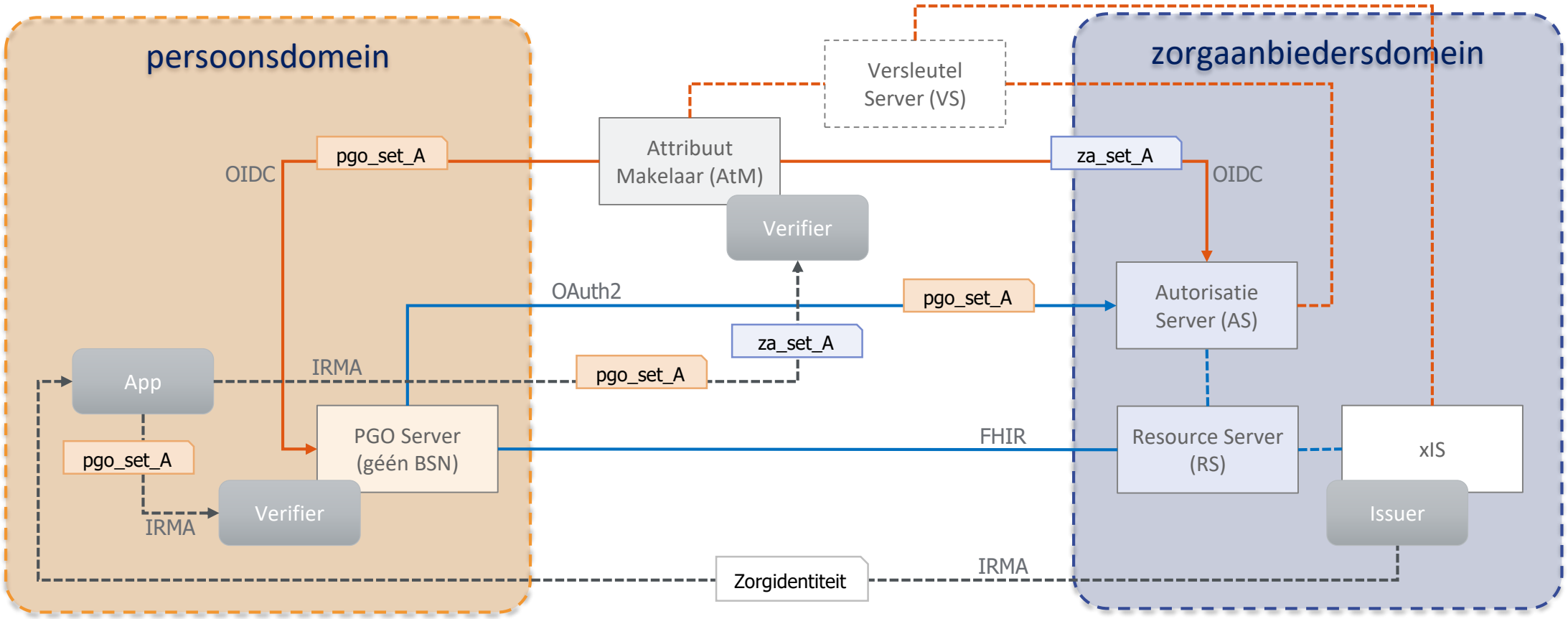
   a. 1e authenticatie: AS redirect gebruiker naar de AtM met een OIDC authorization request (responsetype=code, client_id=<as>, scope=openid **irma_za_setA**, redirect_uri, state)

      - AtM zet een IRMA sessie op met gebruiker en vraagt de beoogde attributen uit
      - AtM ontvangt de attributen en redirect gebruiker via een authorization response met daarin een access code terug naar autorisatieserver
      - Autorisatieserver stuurt een token request naar AtM ontvangt een token response met in het id_token een JWT met de gevraagde attributen (in de vorm van een ***IRMA_disclosure_result***)
      - Autorisatieserver controleert of de attributen die zijn ontvangen via het medmij_contract overeenkomen met de attributen in het IRMA_disclosure_result en slaat de attributen uit het IRMA_disclosure_result (dus inclusief het BSN) op (in haar database)

   b. Herhaalde authenticatie: autorisatieserver zoekt in haar database o.b.v. de attributen in het ontvangen medmij_contract het bijbehorende BSN op

7. Autorisatieserver presenteert de toestemmingsvraag aan gebruiker, waarna de reguliere MedMij flow wordt doorlopen

BIJLAGE 2: ARCHITECTUUR BEPROEFDE OPLOSSING



- Zorgidentiteit: Zorgcode, Versleutelde Sleutel Zorgcode, Voornamen, Voorvoegsel, Geslachtsnaam, Geboortedatum en Wijze van uitgifte
- pgo_set_A: Email, Voornamen, Voorvoegsel, Geslachtsnaam, Geboortedatum en Wijze van uitgifte, eventueel eigen attribuut van PGO. Worden gecommuniceerd als *ondertekende set attributen (contract)*
- za_set_A: Zorgcode + pgo_setA

BIJLAGE 3: SPECIFICATIES VAN DE ATTRIBUTENMAKELAAR RESULTS

- SCOPE: pgo_seta - disclosure:
{"source":"irma","category":"disclosure","type":"za_seta","raw":{"token":"7RXrCCDi8XepDgVkVhDZ","status":"DONE","type":"disclosing","proofStatus":"VALID","disclosed":[[{"rawvalue":"gulikmarc.van@gmail.com","value":{"":"gulikmarc.van@gmail.com","en":"gulikmarc.van@gmail.com","nl":"gulikmarc.van@gmail.com"},"id":"pbdf.pbdf.email.email","status":"PRESENT","issuancetime":1561593600},{"rawvalue":"Jack","value":{"":"Jack","en":"Jack","nl":"Jack"},"id":"irma-demo.vzvz.healthcareidentity.firstnames","status":"PRESENT","issuancetime":1573689600},{"rawvalue":"GY","value":{"":"GY","en":"GY","nl":"GY"},"id":"irma-demo.vzvz.healthcareidentity.prefix","status":"PRESENT","issuancetime":1573689600},{"rawvalue":"thasijd","value":{"":"thasijd","en":"thasijd","nl":"thasijd"},"id":"irma-demo.vzvz.healthcareidentity.familyname","status":"PRESENT","issuancetime":1573689600},{"rawvalue":"02-05-1984","value":{"":"02-05-1984","en":"02-05-1984","nl":"02-05-1984"},"id":"irma-demo.vzvz.healthcareidentity.dateofbirth","status":"PRESENT","issuancetime":1573689600},{"rawvalue":"Balie proces","value":{"":"Balie proces","en":"Balie proces","nl":"Balie proces"},"id":"irma-demo.vzvz.healthcareidentity.issuancemethod","status":"PRESENT","issuancetime":1573689600}]]}}

- SCOPE: za_seta - disclosure:
{"source":"irma","category":"contract","type":"pgo_za_contract","raw":{{"token":"W8zWfXGme442gsKUGrVr","status":"DONE","type":"disclosing","proofStatus":"VALID","disclosed":[[{"rawvalue":"wB8Vuae3ZiGOIi+yJaQC0PI/h0JuK8UqJUO1WiN2KnxCsVrPpiK8zmHG2h0MJFd4cx+GPnrc4QcP907wXOck8ivOjGy1lIU0cnd7qdoCk1nGZvTm2k8sstNFV8f7lFE7nQG99bOHBsXwAhO2R3tzMVSVpV+pDHWAzZTjCJX9jnJYCsViqrRduOQC67/orozfuyCMJ+8czgVC5ddcJZJZpx0rHDSWT+6r5zB/Vp93duHDJwtRqjrNzR0joY131wCxfEyj+0Uu1pVtibzuV6mDfPrmYiOLdO+uqwI4zbmNHTMep5hQCrFRJ65NDzb0w6vXjk2+bmHsyGpaO3imsWQRBQ==","value":{"":"wB8Vuae3ZiGOIi+yJaQC0PI/h0JuK8UqJUO1WiN2KnxCsVrPpiK8zmHG2h0MJFd4cx+GPnrc4QcP907wXOck8ivOjGy1lIU0cnd7qdoCk1nGZvTm2k8sstNFV8f7lFE7nQG99bOHBsXwAhO2R3tzMVSVpV+pDHWAzZTjCJX9jnJYCsViqrRduOQC67/orozfuyCMJ+8czgVC5ddcJZJZpx0rHDSWT+6r5zB/Vp93duHDJwtRqjrNzR0joY131wCxfEyj+0Uu1pVtibzuV6mDfPrmYiOLdO+uqwI4zbmNHTMep5hQCrFRJ65NDzb0w6vXjk2+bmHsyGpaO3imsWQRBQ==","en":"wB8Vuae3ZiGOIi+yJaQC0PI/h0JuK8UqJUO1WiN2KnxCsVrPpiK8zmHG2h0MJFd4cx+GPnrc4QcP907wXOck8ivOjGy1lIU0cnd7qdoCk1nGZvTm2k8sstNFV8f7lFE7nQG99bOHBsXwAhO2R3tzMVSVpV+pDHWAzZTjCJX9jnJYCsViqrRduOQC67/orozfuyCMJ+8czgVC5ddcJZJZpx0rHDSWT+6r5zB/Vp93duHDJwtRqjrNzR0joY131wCxfEyj+0Uu1pVtibzuV6mDfPrmYiOLdO+uqwI4zbmNHTMep5hQCrFRJ65NDzb0w6vXjk2+bmHsyGpaO3imsWQRBQ==","nl":"wB8Vuae3ZiGOIi+yJaQC0PI/h0JuK8UqJUO1WiN2KnxCsVrPpiK8zmHG2h0MJFd4cx+GPnrc4QcP907wXOck8ivOjGy1lIU0cnd7qdoCk1nGZvTm2k8sstNFV8f7lFE7nQG99bOHBsXwAhO2R3tzMVSVpV+pDHWAzZTjCJX9jnJYCsViqrRduOQC67/orozfuyCMJ+8czgVC5ddcJZJZpx0rHDSWT+6r5zB/Vp93duHDJwtRqjrNzR0joY131wCxfEyj+0Uu1pVtibzuV6mDfPrmYiOLdO+uqwI4zbmNHTMep5hQCrFRJ65NDzb0w6vXjk2+bmHsyGpaO3imsWQRBQ==","id":"irma-demo.vzvz.healthcareidentity.healthcarecode","status":"PRESENT","issuancetime":1573689600},{"rawvalue":"Jack","value":{"":"Jack","en":"Jack","nl":"Jack"},"id":"irma-demo.vzvz.healthcareidentity.firstnames","status":"PRESENT","issuancetime":1573689600},{"rawvalue":"GY","value":{"":"GY","en":"GY","nl":"GY"},"id":"irma-demo.vzvz.healthcareidentity.prefix","status":"PRESENT","issuancetime":1573689600},{"rawvalue":"thasijd","value":{"":"thasijd","en":"thasijd","nl":"thasijd"},"id":"irma-demo.vzvz.healthcareidentity.familyname","status":"PRESENT","issuancetime":1573689600},{"rawvalue":"02-05-1984","value":{"":"02-05-1984","en":"02-05-1984","nl":"02-05-1984"},"id":"irma-demo.vzvz.healthcareidentity.dateofbirth","status":"PRESENT","issuancetime":1573689600},{"rawvalue":"Balie proces","value":{"":"Balie proces","en":"Balie proces","nl":"Balie proces"},"id":"irma-demo.vzvz.healthcareidentity.issuancemethod","status":"PRESENT","issuancetime":1573689600},{"rawvalue":"gulikmarc.van@gmail.com","value":{"":"gulikmarc.van@gmail.com","en":"gulikmarc.van@gmail.com","nl":"gulikmarc.van@gmail.com"},"id":"pbdf.pbdf.email.email","status":"PRESENT","issuancetime":1561593600}]]}}}

- SCOPE: pgo_za_contract - contract:
{"source":"irma","category":"disclosure","type":"pgo_seta","raw":{"token":"4ODCTsSQBV93hbhStNKj","status":"DONE","type":"signing","proofStatus":"VALID","disclosed":[[{"rawvalue":"Jack","value":{"":"Jack","en":"Jack","nl":"Jack"},"id":"irma-demo.vzvz.healthcareidentity.firstnames","status":"PRESENT","issuancetime":1573689600},{"rawvalue":"GY","value":{"":"GY","en":"GY","nl":"GY"},"id":"irma-demo.vzvz.healthcareidentity.prefix","status":"PRESENT","issuancetime":1573689600},{"rawvalue":"thasijd","value":{"":"thasijd","en":"thasijd","nl":"thasijd"},"id":"irma-demo.vzvz.healthcareidentity.familyname","status":"PRESENT","issuancetime":1573689600},{"rawvalue":"02-05-1984","value":{"":"02-05-1984","en":"02-05-1984","nl":"02-05-1984"},"id":"irma-demo.vzvz.healthcareidentity.dateofbirth","status":"PRESENT","issuancetime":1573689600},{"rawvalue":"Balie proces","value":{"":"Balie proces","en":"Balie proces","nl":"Balie proces"},"id":"irma-demo.vzvz.healthcareidentity.issuancemethod","status":"PRESENT","issuancetime":1573689600}]],"signature":{"@context":"https://irma.app/ld/signature/v2","signature":[{"c":"6/Z65rtHx5r40aWyDsmpewMl2ckq8p8nrWn6W9wUSzI=","A":"gYG6+1oRWEgpJBI1iaYumHSpqWcjxy/W4CISqG2NwT6ExrbxVvsX/9JMd4TOpaJpvCBnD5YbkrxrztAxtDek49t7621bxXNHc9wTcKoI7MKkzdMmrAvumWBET9VOS4VBLfiQWn4h++QIwg6KFgbk6NBYWneZ7U7By/YIHC6zttU=","e_response":"de3YkCMgxkPffaLGMfHtjnsZXg7AZKJYirPBLBR/WJq39+kO3TLoFoAKWjzUfYZA/RolFt4rORin","v_response":"BOJ5WU+2HycuYdDmlJBtVfQYd1fouOD9Bz6Lv5vgStVZod+KlpFP/pP98ilQqPh+puTLp6+qjGlJtUZm9+duEkaaBBCuZnGXpDQA/5DXIBMW/FXKkZAnsNYb1kKyhG5dNetBOUA6sPjZ8ZldFoZDOJmYCwrLyX+JfQ4jflshzS9fI6mQHEHicjk6PwZbOCB/6LkWpZ3fY6uePvhB4zwPnvKOc4l2SXPIR8yBFRIVsfTK2Sk+fpNPzJFEh+HhCZ7slR9mVBTalfc/9tpjvoKOgBfMK+Mpmd7cfHbLbgloMXlhSREg0rr4OaPC/3SBr8gt18LLaEbdVP5P2GzjDRII","a_responses":{"0":"7tVjc0AKIsJqYhH0FeptSbY8nuxgoEPQli+cEX/APrEsRm7J00qzS0ZcJaNyQbC7mWMgMqSekk5j+Wnzi+c2uWFwzWS0/GwCRhA=","2":"AY9CmEACc3F5edqn1ZenLYr8U3QpzFF5RpUPrMzI4FmMwfe/HtNCLAUlN8W9k35zpO9Oz2lt5ItSxUj8zo/JGcXNEa1ZIz8rBCI=","3":"C6N5nVAXzzVAD50cxe0oBzIw3lf7CYHiWKN8I8KD/WeCAZvlD8K3W9MOAtUIa3bqSOoVH5h9n0Pstho74iAsPjIopwHZwGAOWDk="},"a_disclosed":{"1":"AwAKKgAaAABBNdPzLGpSK3VDw22laeqK","4":"lMLG1w==","5":"jrM=","6":"6NDC5tLUyQ==","7":"YGRaYGpaYnJwaQ==","8":"hMLY0spA4OTexsrn"}}],"indices":[[{"cred":0,"attr":4},{"cred":0,"attr":5},{"cred":0,"attr":6},{"cred":0,"attr":7},{"cred":0,"attr":8}]],"nonce":"1TxeY3sZkFRN+MGa0fDPug==","context":"AQ==","message":"Hierbij bevestig ik dat mijn namen en geboortedatum door mogen worden gegeven aan zorgaanbieders met wie ik medische gegevens uit wil
wisselen.","timestamp":{"Time":1583742156,"ServerUrl":"https://keyshare.privacybydesign.foundation/atumd/","Sig":{"Alg":"ed25519","Data":"oSmss+4UlqntuiMuOc0SBT+v5LxVxfvXAZZD/75MdSo7TMbAwuKAg5SgM+OT/DanW881cDzqDClVcAE15i3pDg==","PublicKey":"MKdXxJxEWPRIwNP7SuvP0J/M/NV51VZvqCyO+7eDwJ8="}}}}}

BIJLAGE 4: SCHRIFTELIJKE REACTIE PRIVACY BY DESIGN FOUNDATION

Privacy by Design (PbD) Foundation heeft schriftelijk gereageerd op de security quickscan en de hoofdbevindingen uit de PIA (hetgeen dat betrekking heeft op IRMA). Hieronder staat de reactie puntsgewijs weergegeven.

Security quickscan

- Onlangs is een interne code audit afgerond, zie het eerste item op: https://privacybydesign.foundation/reviews-en/
  Een uitgebreidere audit kan misschien met een aantal partijen gecoördineerd worden, zoals de gemeente Amsterdam of het Ministerie van Binnenlandse Zaken. Die coördinatie kan het beste gaan via SIDN.
- Het klonen van attributen kan na compromitteren van het operating systeem. Dit is in de praktijk echter niet eenvouding.
- PbD is aan het experimenteren met het toevoegen van een simpele code, zoals DigiD ook doet, zodat phishing kan worden voorkomen. Daarbij wordt opgemerkt dat phishing alleen speelt bij uitgifte van attributen, en enkel bij uitgifte via een aparte computer (met QR-code). Als je op je mobiel werkt (wat heel veel mensen doen) wordt er automatische overgeschakeld naar de IRMA app, zonder dat je een QR-code te zien krijgt.
- Met de nieuwste versie van IRMA kunnen attributen ingetrokken worden.
- In de PoC is niet de laatst versie van IRMA gebruikt. De nieuwste versie van IRMA heeft een geheel vernieuwde interface.
- Er bestaat nog discussie met PbD over de noodzaak en de vorm van versleuteling van het BSN.

PIA

- Borgen van toestemming is inderdaad essentieel. In de IRMA app geeft de gebruiker heel expliciet toestemming.
- SIDN zal de verantwoordelijke partij zijn die IRMA gaat aanmelden voor toelating onder de WDO.

BIJLAGE 5: INVENTARISATIE EISEN VOOR AFSPRAKENSTELSEL ATTRIBUUT-GEBASEERDE AUTHENTICATIE

Gedurende de PoC zijn de volgende eisen geïnventariseerd waar rekening mee moet worden gehouden in het Afsprakenstelsel attribuut-gebaseerde authenticatie:

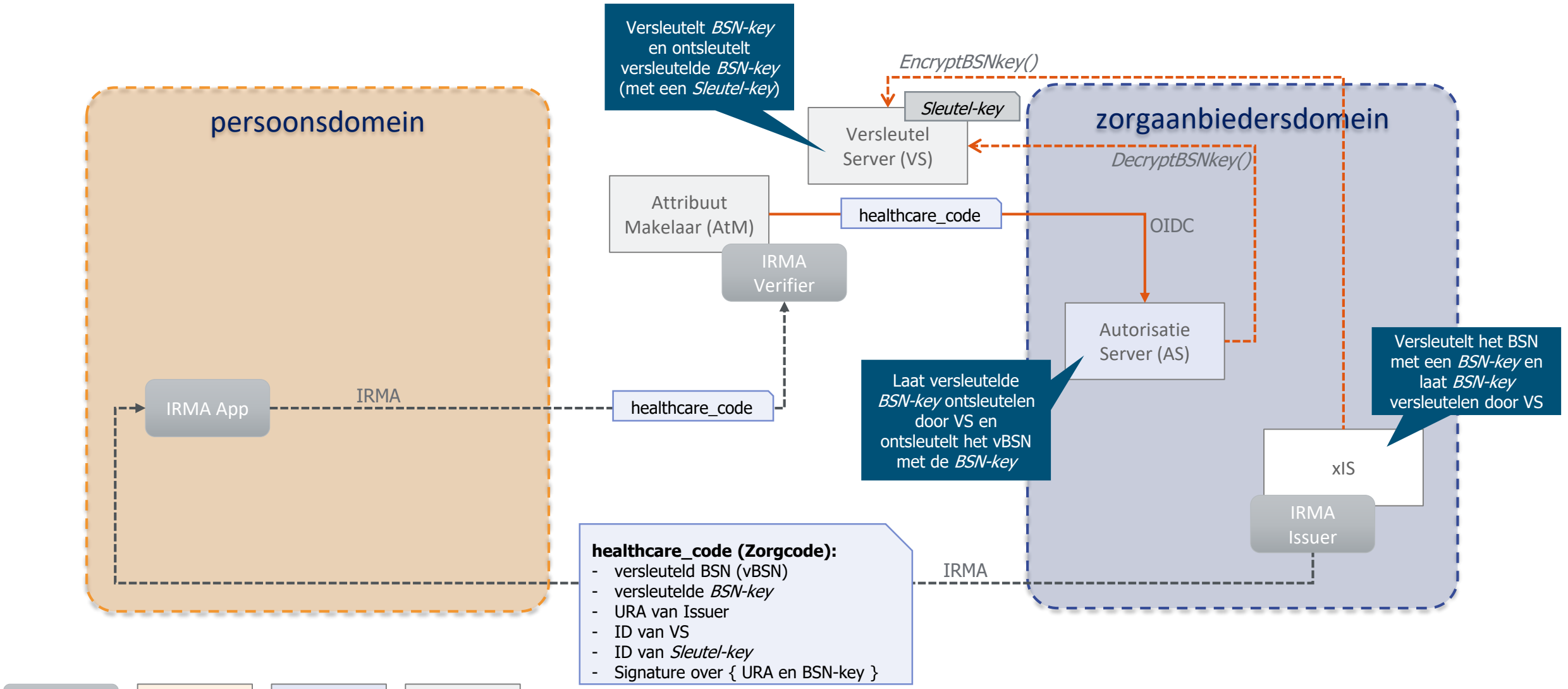
1. Uitgevers (issuers), controleurs (verifiers) en centrale voorzieningen moeten worden gekwalificeerd om deel te kunnen nemen aan het Afsprakenstelsel attribuut-gebaseerde authenticatie. De oplossing dient generiek te zijn voor attribuut-gebaseerde authenticatie bij MedMij, Twiin en AORTA.
2. Uitgifte, opslag en uitwisseling van attributen is beveiligd (conform ETSI aangevuld met Nederlandse specifieke eisen)
3. Attributen kunnen worden voorzien van een betrouwbaarheidsniveau (conform eIDAS te auditen/vast te stellen)
4. De uitgever van een attribuut krijgt geen kennis over het gebruik van het betreffende attribuut
5. Attributen-wallets hanteren eenzelfde technische standaard (bijvoorbeeld SAML2 en/of JWT) voor het uitwisselen van attributen en attribuut-gebaseerde handtekeningen
6. Uitgevraagde attributen kunnen tussen partijen die elkaar (binnen een ander afsprakenstelsel of zorginfrastructuur) vertrouwen worden doorgegeven middels contracten, waarbij ‘herauthenticatie’ binnen een sessie over meerdere partijen mogelijk wordt
7. Attributen en attribuut-gebaseerde handtekeningen kunnen (ook) m.b.v. OIDC standaarden worden uitgevraagd en uitgewisseld
8. Uitvraag of toegang tot de inhoud van attributen kan worden ingeperkt tot partijen met specifieke kwalificaties (bijvoorbeeld “behorende tot het BSN-domein”)

BIJLAGE 6: UITGANGSPUNTEN EN REQUIREMENTS M.B.T UITGIFTE EN CONSUMPTIE VAN ATTRIBUTEN

Gedurende de PoC zijn de volgende uitgangspunten en requirements geïnventariseerd:

- *Must:* Uitgifte en consumptie van attributen zijn geïntegreerd in de zorgapplicaties, desgewenst ondersteund door gemeenschappelijke modules
- *Must:* Open protocollen (API en verwerking/ontwerp) gebruiken voor uitgifte en consumptie van attributen en voor encryptie en decryptie van sleutels borgt interoperabiliteit met de zorgtoepassingen
- *Should:* Issuers en verifiers middels een generiek koppelvlak ondersteunen om attributen makkelijk uit te kunnen geven en consumeren in verschillende attributen-wallets (IRMA, Sovrin, etc.)
- *Could:* Zelf kunnen kiezen waar componenten (verifier, autorisatie server, sleuteldienst) draaien en dus waar verwerking van gegevens (persoonsgegevens en met name het BSN) plaatsvindt en wie verwerkt

BIJLAGE 7: VERSLEUTELING VAN BSN



BIJLAGE 7: VERSLEUTELING VAN BSN

- IRMA attribuut: **irma-demo.vzvz.healthcareidentity.healthcarecode**, dit is een Base64 JSON string, met als inhoud:
  a. Het, met *BSN-key*, door uitgevende zorginstelling, versleutelde BSN
  b. URA van de uitgevende zorginstelling
  c. de (met *Sleutel-key*) versleutelde *BSN-key*
  d. Signature over { URA en *BSN-key* } (door Versleutel Service gedaan – vereist 2-zijdig TLS tussen issuer en versleutel server)
  e. ID van de Versleutel Server
  f. ID van de gebruikte Sleutel-key
- De *Sleutel-key* bestaat is een private key (symmetrisch)
- De signature over { URA en *BSN-key* } wordt geplaats m.b.v. een andere private sleutel dan Sleutel-key (asymmetrisch)
- Een Versleutel Server biedt twee services:
  - Voor Issuers: EncryptBSNkey (<URA uitgevende zorginstelling>, <*BSN-key*>)
    Deze service encrypt de BSN-key m.b.v. de Sleutel-key en retourneert een versleutelde *BSN-key* en de signature over { URA en *BSN-key* }
  - Voor Verifiers: DecryptBSNkey (<URA uitgevende zorginstelling>, <versleutelde *BSN-key*>, signature over { URA en *BSN-key* })
    Deze service decrypt de versleutelde *BSN-key* en retourneert deze
    Een Verifier kan de juiste Versleutel Server vinden o.b.v. het ID die is opgenomen in de **healthcarecode**