TxN 2026

Gezamenlijk groeipad Twiin & Nuts

versie 0.98
17-08-2022

Auteurs:
Wouter Tesink
Jorrit Spee

Geconsulteerde experts:
Jan Feenstra
Pascal Looijé
Marc Sandberg
Marcel Settels
Wout Slakhorst
Ben van der Stigchel
Steven van der Vegt

Wijzigingshistorie

Versie	Toelichting
0.94	In ‘bredere’ kring dan Twiin/Nuts gedeeld voor feedback
0.98	● Transformation Map aangevuld met VIPP-regelingen, data verschoven richting 2026, o.a. omdat er al vertraging is opgelopen in de NEN-normeringstrajecten.De titel van het stuk is daarom ook veranderd. ● VIPP-regelingen en EHDS opgenomen in omgevingsanalyse ● Voorgestelde aanpak per aandachtsgebied gestructureerd volgens Nictiz 5-lagen interoperabiliteitsmodel ● Grofmazige verschillenanalyse toegevoegd van bestaande ontwikkelingen / uitwisselingsinfrastructuren t.o.v. van de beoogde visie. ● Stelselbeheer aangevuld met mogelijkheden voor de implementatie voor generieke functies. ● Tabellen aandachtsgebied "Autorisatie Zorgaanbieders" herzien ● Advies voor concreet vervolg (planningshorizon 2022-2023) toegevoegd aan hoofdstuk Conclusie ● Bij aanname 2 aangaande Verifiable Credentials is de kans gewijzigd van 'onbekend' naar 'midden' door release 1.0-versie van standaard door W3C en adoptie door Microsoft.

Inhoud

Managementsamenvatting

De werkgroep eOverdracht van Twiin heeft in samenwerking met Nuts dit document opgesteld. Dit is gedaan naar aanleiding van de fit/gap analyse tussen het Twiin Afsprakenstelsel versie 1.0 bèta enerzijds en de Technische Afspraak eOverdracht van Taskforce Samen Vooruit (TSV) welke is gebaseerd op de Nuts Bolt eOverdracht anderzijds. Uit deze analyse bleek dat de afspraken op basis van Nuts nog niet in het Twiin Afsprakenstelsel konden worden opgenomen.

Architecten en andere experts van Twiin en Nuts hebben nauw samengewerkt om te beschrijven op welke punten en hoe Twiin en Nuts op de langere termijn naar elkaar toe kunnen groeien. Hiertoe zijn elf aandachtsgebieden bekeken, die ook in de fit/gap analyse zijn behandeld. Het betreft de volgende aandachtsgebieden:

1. Identificatie en authenticatie zorgverlener - Uitgifte van attributen: de uitgifte van verklaringen over zorgverleners
2. Identificatie en authenticatie zorgverlener - Authenticatiemiddelen: middelen waarmee een zorgverlener zich kan authenticeren
3. Autorisatie zorgverlener: het autoriseren van toegang tot gegevens op basis van zorgverlener-specifieke kenmerken
4. Identificatie en authenticatie zorgaanbieder: de uitgifte van verklaringen over zorgaanbieders en middelen waarmee een zorgaanbieder zich kan authenticeren
5. Autorisatie zorgaanbieder: het autoriseren van toegang tot gegevens op basis van zorgaanbieder-specifieke kenmerken
6. Grondslagen - Vastleggen en toetsen: het vastleggen van en toetsen op grondslagen voor de verwerking van gezondheidsgegevens zoals expliciete toestemming
7. Datalokalisatie: het lokaliseren van data over een specifieke cliënt
8. Adressering: het verkrijgen van technische adressen van een zorgaanbiedersysteem
9. Communicatiebeveiliging: de technische en organisatorische beveiliging van de communicatie
10. Stelselbeheer: het beheer van het Twiin afsprakenstelsel en het Nuts afsprakenstelsel
11. Vervolgproces visie/transformatie: het vervolgtraject voor het uitvoeren van het groeipad

Per aandachtsgebied is een visie voor 2026 geformuleerd, inclusief een aantal mogelijke stappen om daar te komen.

De belangrijkste conclusie is dat Twiin en Nuts beide op inhoudelijk niveau voldoende mogelijkheden zien om naar elkaar toe te groeien. Om te convergeren hebben niet alleen Twiin en Nuts veel werk te doen. Ook leveranciers van applicaties/voorzieningen die generieke functies willen invullen, dienen veel werk te verzetten. Een belangrijke oplossingsrichting, die in meerdere aandachtsgebieden terugkomt, is het gestandaardiseerd beschikbaar maken van onweerlegbare, digitaal ondertekende verklaringen over zowel data als metadata. Een aanzienlijk deel van het uit te voeren werk is gerelateerd aan het implementeren van het concept self-sovereign identity (SSI) en de hieraan gerelateerde internationale standaard voor digitaal ondertekende verklaringen Verifiable Credentials.

Daarmee is de reikwijdte van deze oplossingsrichting breder dan alleen de zorgtoepassing eOverdracht: het gestandaardiseerd beschikbaar maken van onweerlegbare, digitaal ondertekende verklaringen heeft naar verwachting ook meerwaarde binnen andere zorgtoepassingen. De impact van deze oplossingsrichting is aanzienlijk: de standaard dient door dienstverleners van zorgaanbieders en uitgevers/registers te worden geïmplementeerd en het Twiin afsprakenstelsel dient op punten te worden aangevuld of aangepast. Deze investeringen kunnen slechts beperkt worden gerechtvaardigd wanneer deze oplossingsrichting louter voor de zorgtoepassing eOverdracht wordt ingezet.

Hetgeen beschreven is een basis voor gezamenlijke visievorming binnen het duurzaam informatiestelsel zorg. Advies is om het document op die manier te positioneren.

Het is dus wenselijk om het gebruik van deze oplossingsrichting voor meerdere zorgtoepassingen te overwegen. Hiervoor moet in gezamenlijk overleg met het veld worden bepaald in hoeverre de voorgestelde oplossingsrichtingen echt noodzakelijk zijn, draagvlak hebben en haalbaar zijn. Twiin en Nuts beogen met dit document een kickstart te geven aan dit vervolgtraject voor het vormen die gezamenlijke landelijke visie.

1. Inleiding

Achtergrond

Een groep leveranciers die de zorgtoepassing eOverdracht wil gaan ondersteunen heeft onder begeleiding van de Taskforce Samen Vooruit (TSV) een Technische Afspraak (TA) opgesteld. Deze TA is een technische implementatie-afspraak om de zorgtoepassing eOverdracht te gaan implementeren met behulp van Nuts-standaarden. In 2021 is gestart met het integreren van de zorgtoepassing eOverdracht in het Twiin-afsprakenstelsel. Het idee daarachter is dat meerdere uitwisselingsinfrastructuren de zorgtoepassing eOverdracht kunnen implementeren en dat op basis van het Twiin-afsprakenstelsel de verschillende uitwisselingsinfrastructuren met elkaar worden verbonden. Dit zou dan tevens de basis zijn om in de toekomst ook andere zorgtoepassingen via Twiin te implementeren. Om verschillende redenen is in 2021 besloten de TA voorlopig nog niet in het Twiin-afsprakenstelsel op te nemen. Een van de belangrijkste redenen is dat de verschillen tussen het Twiin-afsprakenstelsel enerzijds en de op Nuts-standaarden gebaseerde TA eOverdracht anderzijds te groot zijn om op korte termijn te overbruggen. Op langere termijn ziet een vertegenwoordiging van architecten van Twiin en Nuts voldoende mogelijkheden om het Twiin-afsprakenstelsel en de TA eOverdracht (op hoofdlijnen) bij elkaar te brengen. Op verschillende onderdelen kunnen Twiin en Nuts elkaar zelfs versterken, vandaar het vermenigvuldigingsteken tussen Twiin en Nuts in de naam van dit document.

Omgeving

Niet alleen Twiin en Nuts houden zich bezig met de totstandkoming van een duurzaam informatiestelsel in de zorg. Voor de omgevingsanalyse van dit document zijn de partijen die zich richten op gegevensuitwisseling tussen zorgaanbieders in het algemeen of de zorgtoepassing eOverdracht in het bijzonder het meest relevant. Dit betreft de zorgverleners en zorgaanbieders zelf, vertegenwoordigd binnen de verschillende brancheverenigingen en koepels (bijv. NFU en NVZ), maar ook de bijbehorende leveranciers en landelijke programma's zoals VIPP, Twiin en OTV en ondersteunende organisaties als VZVZ, CIBG en Nictiz. De besluitvorming en het bijbehorende mandaat van dit groeipad zal daarom niet alleen door de bij eOverdracht betrokken partijen kunnen worden opgepakt.

VIPP-regelingen en andere afsprakenstelsels

Dit document is opgesteld naar aanleiding van de zorgtoepassing eOverdracht. Daarin werd eerder geconcludeerd dat Twiin versie 1.0 Beta en Nuts i.c.m. de afspraken met Taskforce Samen Vooruit nog te ver uit elkaar liggen om de toepassing en technieken in het Twiin afspraken stelsel te kunnen opnemen. Ook werd geconcludeerd dat er op hoofdlijnen dezelfde visie voor een duurzaam informatiestelsel in de zorg is.
Er zijn verschillende VIPP regelingen, waar een aantal gaan over de communicatie tussen zorgaanbieder en de patiënt/cliënt. De inhoud van dit document heeft hier geen directe relatie mee, omdat het alleen communicatie tussen zorgaanbieders betreft. Wel relevant zijn:

- VIPP5 module 3
- VIPP geboortezorg: Babyconnect
- VIPP care: InZicht

- VIPP farmacie en Programma Medicatieoverdracht

Voor deze regelingen zijn de volgende afsprakenstelsels/ uitwisselingsinfrastructuren relevant:

- AORTA (LSP)
- Nuts
- Op IHE XDS gebaseerde (regionale) afsprakenstelsels

Verschillende leveranciers hebben (in het kader van eOverdracht/VIPP InZicht) aangegeven geen andere dingen meer te doen dan nu al gepland, omdat anders de deadline niet gehaald wordt. Dit geldt vermoedelijk ook in trajecten voor andere VIPP-regelingen waarvan de deadline in 2022 of 2023 is. Dit betekent dat er relatief weinig ruimte is om ontwikkelingen volgens of meer in de richting van deze visie te sturen.

Het gaat voor dit document te ver om in detail de implementaties in de verschillende afsprakenstelsels waaraan gewerkt wordt om aan de VIPP-regelingen te voldoen te gaan analyseren, maar op hoofdlijnen is er een vergelijking gemaakt tussen de visie die in dit document staat beschreven en de betreffende implementatie. Deze vergelijking is opgenomen in bijlage 3.

Andere zorgtoepassingen

De in dit document voorgestelde oplossingsrichtingen voor authenticatie, autorisatie, identificatie, lokalisatie en toestemming zijn primair opgesteld vanuit het perspectief van de zorgtoepassing eOverdracht maar zullen pas echt meerwaarde bieden als ze breed worden omarmd door meer en uiteindelijke alle gegevensuitwisselingen in de zorg.

Wegiz en NEN-trajecten

De normalisatietrajecten voor generieke functies (identificatie en authenticatie, toestemming, lokalisatie) zijn van start gegaan. Deze visie zal als input gebruikt worden voor het opstellen van deze normen. Wanneer een norm de visie (nog) niet omarmd zal dit consequenties hebben op de wijze waarop eOverdracht en andere op Nuts gebaseerde zorgtoepassingen in het Twiin afsprakenstelsel opgenomen moeten worden.

De visie en het groeipad uit dit document zouden ingebracht moeten worden bij beleidsmakers als het Informatieberaad Zorg en in de verschillende werkgroepen voor de NEN-normen binnen het Wegiz-traject.

European Health Data Space (EHDS)

Parallel aan het schrijven van deze visie is de conceptverordening voor EHDS gepresenteerd. Wat het concrete effect wordt van deze regelgeving op dit visiestuk is nog moeilijk te bepalen. Wat wel duidelijk is het volgende (o.b.v. de analyse van Geranne Lautenbach)[1]:

[1]https://www.linkedin.com/pulse/nieuwe-eu-concept-verordening-wijkt-op-meerdere-af-van-lautenbach/?trackingId=lazDcoeTTIiqtsf3o4JWSw%3D%3D

- De Europese Unie omarmt het principe van Self Sovereign Identities, en werkt aan een eIDAS-compatibel European Self-Sovereign Identity Framework (ESSIF). Daarmee lijkt het erop dat de standaarden Verifiable Credentials en Decentralized Identifiers, die ook prominent in dit document voorkomen, ook op Europees niveau omarmd zullen worden.
- De EHDS stelt dat patiënten het recht hebben op kosteloze, directe digitale toegang tot de logging en het recht om te bepalen welke zorgverleners toegang krijgen tot hun gegevens. Dit zal betekenen dat er eenduidige standaarden moeten komen om de logging (naar de patiënt) te ontsluiten en om toestemmingen te verwerken. Dit recht kan op verschillende manieren ingevuld worden. Een oplossingsrichting zou het gebruik van Mitz kunnen zijn waarmee toestemmingen verwerkt kunnen worden. Voor inzage van de logging zijn er verschillende opties mogelijk.
- Zorgaanbieders moeten toegang kunnen krijgen tot de patiëntgegevens als dat nodig is om de vitale belangen van natuurlijke personen te beschermen. Ook als de toegang door de patiënt is beperkt (art 4). Dat stelt eisen aan de technische inrichting van systemen voor de uitwisseling van medische gegevens. Dit zal o.a. betekenen dat de gegevens op een eenduidige manier gelokaliseerd moeten kunnen worden. Toegang tot medische gegevens in het geval van spoed kan grofweg op twee manieren: via een breaking-the-glass procedure, waarin de betreffende zorgverlener moet aangeven dat het spoed is, waarna eventuele beperkingen op autorisaties worden weggenomen, of op basis van rollen (denk aan eerste hulp, ambulance, meldkamer, spoedarts, etc). Hierover zullen afspraken gemaakt moeten worden onder het onderwerp autorisatie.
- (De Europese versie van) Beelduitwisseling, medicatie, labuitslagen en ontslagbrieven en de BgZ zijn in de conceptverordening opgenomen (art5), eOverdracht dus niet. Wanneer we in Nederland deze visie willen gaan concretiseren lijken deze toepassingen daarvoor dan al eerst in aanmerking te komen (al dan niet op basis van de te maken eOverdracht implementatie).
- De Europese Commissie zal op basis van deze conceptverordening bepalen wat de technische specificaties zijn voor het uitwisselen van de geprioriteerde gegevensuitwisselingen. Het gaat onder andere om de datasets, codestelsels, technische specificaties en standaarden die gebruikt worden (art 6). De vraag is nog wat de scope van deze eisen gaat zijn. Gelden deze alleen voor het koppelvlak tussen Nederland en Europa, of gelden deze specificaties ook voor de uitwisseling binnen Nederland? In het laatste geval kan dit een enorme impact hebben op deze voorgestelde visie (en de in ontwikkeling zijnde NEN-normen).

Wanneer EHDS in werking zal treden is nog onduidelijk. Het ministerie van VWS geeft schattingen van 1,5 jaar tot 4 jaar. En dan zullen de verschillende Europese standaarden die verplicht ondersteund moeten gaan worden vermoedelijk ook nog ontwikkeld moeten worden. Het idee van het ministerie is dat door via de NEN al verschillende standaarden/normen te ontwerpen hiermee een voorzet gegeven wordt voor de Europese standaardisatie welke dan hopelijk niet veel zal afwijken van wat er in Nederland bedacht is.

De EHDS is niet opgenomen in de transformation map, omdat het nog zo onzeker is wanneer we hier de effecten van gaan merken. EHDS zal zeker impact gaan hebben, maar de verwachting is dat

1. de Nederlandse NEN-normen voor generieke functies als voorbeeld zullen dienen voor de Europese en als we daarom deze NEN-normen volgen er hopelijk weinig impact zal zijn.

2. dat het nog enige tijd duurt voordat EHDS in werking treedt, daarna de deze Europese normen/eisen/specificaties opgesteld moeten worden dat dit verder in de toekomst ligt dan 2026.

Doel

Dit document beschrijft een *voorstel* voor een visie van Twiin en Nuts waarmee beide afsprakenstelsels tot elkaar kunnen komen. Grof gezegd komt dit neer op het gebruik van de technieken die Nuts heeft geadopteerd gecombineerd met het vertrouwensmodel en vertrouwde uitgevers van het Twiin afsprakenstelsel.

Dit voorstel betreft ontwikkelingen vanaf twee richtingen. Van de ene kant betekent dit het komen tot een gedeelde architectuurvisie waar in dit document al een aanzet toe is gedaan. De architectuurvisie geeft een globaal beeld van wat we willen verwezenlijken in de toekomst, maar is geen glazen bol. De architectuurvisie geeft richting, stelt principes en wordt daarmee een sturingsinstrument voor de ontwikkelingen die vanuit de andere kant komen: het maken van implementatiespecificaties en het bouwen van producten en diensten die de architectuurvisie helpen verwezenlijken.

Op het bouwen van producten en diensten is geen of moeilijk grip te krijgen. Welke diensten, wanneer en door wie worden ontwikkelt wordt (deels) door de marktomstandigheden bepaald. De genoemde ontwikkelingen zijn dan ook niet alleen maar zaken die Twiin en/of Nuts zullen uitvoeren. Vaak is er een afhankelijkheid met voorzieningen voor generieke functies die door andere partijen (moeten) worden geleverd. Gezamenlijk met het veld zal er per aspect gekeken moeten worden naar de noodzaak, het draagvlak en haalbaarheid van de voorgestelde oplossing om op basis daarvan een prioritering vast te stellen.

Dit document heeft meerdere doelen:

- Inzicht verschaffen in de zaken waarover concrete gedeelde afspraken moeten worden gemaakt voordat de TA eOverdracht in Twiin kan worden opgenomen. Op basis hiervan zal ook bepaald moeten worden in hoeverre de voorgestelde oplossingen noodzakelijk en haalbaar zijn.
- Communiceren van een gezamenlijke visie op een toekomstige IT-infrastructuur voor de zorg. Niet alleen Twiin en Nuts dienen zich achter deze visie te scharen. Dat zal ook moeten gelden voor andere partijen die zich bezighouden met uitwisselingsinfrastructuren in de zorg.
- Inzicht verschaffen in de acties en bijbehorende eigenaren die nodig zijn om die gedeelde visie te verwezenlijken. Wanneer de visie door meerdere partijen wordt gedeeld, ondersteunt dit het komen tot heldere en concrete(re) opdrachten aan derde partijen om bepaalde zaken te gaan ontwikkelen.
- Input geven aan de trajecten van de NEN voor de normeringen van generieke functies.

Krachtenveldanalyse

Ten aanzien van het groeipad dat in dit document wordt beschreven, is een groot aantal belanghebbenden te identificeren. Deze kunnen worden geordend op basis van de rol die ze binnen deze context vervullen:

- Beslisser: De belanghebbende heeft een besluitvormende macht bij het accorderen van het groeipad, bijvoorbeeld 'Architectuurraad Twiin'.
- Beïnvloeder: De belanghebbende heeft invloed op de inhoud van het groeipad.
- Uitvoerder: De belanghebbende heeft een rol in de uitvoering/uitrol van het groeipad (exclusief leveranciers), bijvoorbeeld 'Kernteam eOverdracht Twiin'.
- Leverancier: de belanghebbende is leverancier van een technologische oplossing die een rol speelt in het groeipad, bijvoorbeeld 'VZVZ'.
- Gebruiker: de belanghebbende gebruikt het groeipad als input voor eigen afspraken, bijvoorbeeld 'NEN-werkgroep Generieke functies'.

Naam	**Beslis-ser**	**Bein-vloe-der**	**Uit-voer-der**	**Leve-ran-cier**	**Ge-brui-ker**
Actiz	N	J	N	N	J
Architectuurboard	N	J	N	N	J
Architectuurraad Twiin	J	J	J	N	N
Redactie Twiin Afsprakenstelsel	N	J	J	N	J
Bureau InZicht	N	J?	N	N	J
Kernteam eOverdracht Twiin	N	J	J	N	N
Leveranciers applicaties t.b.v. generieke functies	N?	J	J	J	N
Leveranciers XIS	N	J	J	J	N
Ministerie van VWS	N?	J	N	N	J
NEN-werkgroep Generieke functies	J (periode >= 2023)	J	J	N	J
Nictiz	N	J	N	N	N
Nuts Community	N	J	J	J	J
Programmaraad Twiin	J	N?	J	N	J
Stichting Nuts	J	N	N	N	N
Taskforce Samen Vooruit	J	J	J	N	J
VGN	N	J	N	N	J
VZVZ - Architectuur	N	J	J	N	J
VZVZ - Dienstverlener van ZORG-AB/ Mitz/ LSP	N	J	N	J	N

Naam	Beslis-ser	Bein-vloe-der	Uit-voer-der	Leve-ran-cier	Ge-brui-ker
Zorginstituut Nederland	N	J	J	N	N

Scope - zorgtoepassingen

Dit document is in nauwe samenwerking tussen Twiin en Nuts opgesteld onder verantwoordelijkheid van het kernteam eOverdracht van Twiin. Het toewerken naar de opname van de zorgtoepassing eOverdracht in het Twiin afsprakenstelsel vormt de concrete aanleiding voor de totstandkoming van dit document en vormt daarmee de primaire scope.

Alhoewel is gestart vanuit het perspectief van de zorgtoepassing eOverdracht beperkt het document zich niet tot alleen deze zorgtoepassing. De elf aandachtsgebieden die worden beschreven zijn generiek voor alle gegevensuitwisselingen in de zorg en kunnen gelden in principe voor alle zorgtoepassingen. Voor de verschillende aandachtsgebieden worden in dit document een aantal oplossingsrichtingen voorgesteld, zoals de implementatie van de standaard Verifiable Credentials. Deze beschreven oplossingsrichtingen zijn generiek van aard en geschikt voor toepassing binnen alle zorgtoepassingen. De mate van geschiktheid en toepasbaarheid van de beschreven oplossingsrichtingen zal echter wel verschillen per zorgtoepassing. Deze hangt met name af van de inhoud van reeds gemaakte keuzes binnen een bepaalde zorgtoepassing.

De zorgtoepassing Beeldbeschikbaarheid en de uitwisseling van documenten binnen de zorgtoepassing Basisgegevensset Zorg zijn bijvoorbeeld al vergaand uitgewerkt met behulp van XDS-transacties. Dit maakt dat het opnemen van de in dit document voorgestelde oplossingsrichtingen in de zorgtoepassing Beeldbeschikbaarheid en de uitwisseling van documenten binnen de zorgtoepassing Basisgegevensset Zorg technisch een grote impact zou hebben.

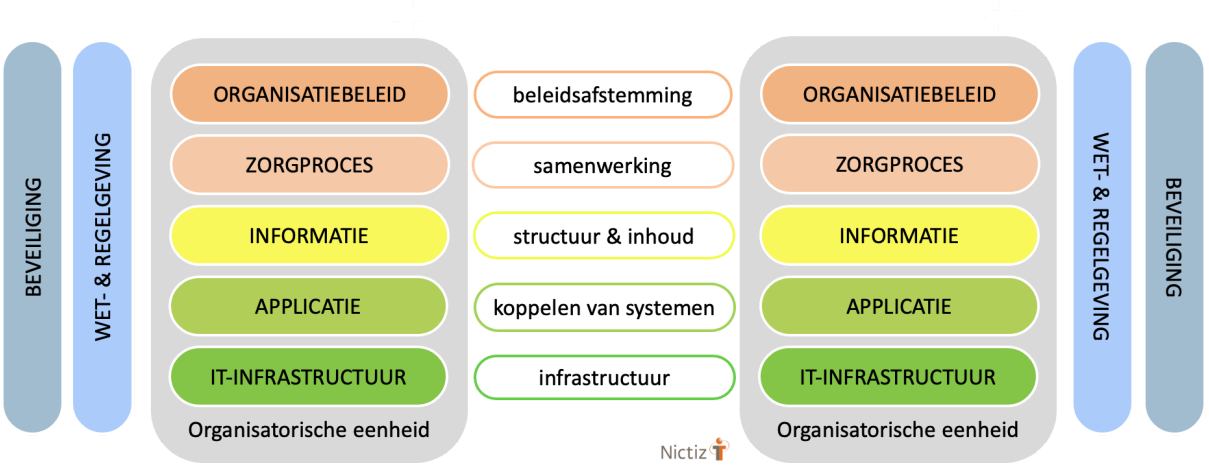
Het is daarom niet de ambitie om de in dit document voorgestelde oplossingsrichtingen op korte termijn in alle zorgtoepassingen toe te passen. De in dit document beschreven oplossingsrichtingen zijn op korte termijn met name geschikt voor zorgtoepassingen die gebruik maken van de uitwisselconcepten 'pull - gerichte bevraging', 'pull - geïndexeerde bevraging' en 'notified pull - versturen notificatie en gerichte bevraging' in combinatie met FHIR-transacties.

Voorbeelden hiervan zijn de zorgtoepassingen eOverdracht, Geboortezorg en de uitwisseling van FHIR-resources binnen de zorgtoepassingen Basisgegevensset Zorg en Actueel medicatieoverzicht. Op langere termijn is de ambitie om de binnen alle verschillende zorgtoepassingen gebruikte technieken en standaarden zo veel mogelijk te harmoniseren. De in dit document voorgestelde oplossingsrichtingen zijn hier op langere termijn geschikt voor.

De impact van de in dit document beschreven oplossingsrichtingen is aanzienlijk: geschikte standaarden dienen door dienstverleners van zorgaanbieders en uitgevers/registers te worden geïmplementeerd en het Twiin afsprakenstelsel dient op punten te worden aangevuld of aangepast. Deze investeringen kunnen slechts beperkt worden gerechtvaardigd wanneer deze oplossingsrichting louter voor de zorgtoepassing eOverdracht wordt ingezet. Het is daarom wenselijk om het gebruik van de in dit document beschreven oplossingsrichtingen voor meerdere zorgtoepassingen te overwegen.

Scope - interoperabiliteitsmodel

Het Nictiz-interoperabiliteitsmodel onderscheidt verschillende aandachtsgebieden op het gebied van interoperabiliteit.



Dit document richt zich op de gemeenschappelijke zaken die over zorgtoepassingen en zorgprocessen heen geregeld moeten worden. Dit betekent dat zorgtoepassing specifieke afspraken m.n. op de lagen organisatiebeleid en zorgproces niet behandeld worden. In de diverse zorg-informatiestandaarden wordt hier wel aandacht aan besteed.

Laag/kolom	**Scope groeipad Twiin X Nuts**
Organisatiebeleid	- Afspraken over gebruik van gemeenschappelijke en/of centrale voorzieningen en vertrouwde partijen. - Afspraken over het volgen en implementeren van normen en standaarden, direct of via een afgestemd groeipad
Zorgproces	- Afspraken maken over eenduidige en gestandaardiseerde zorgtoepassingsonafhankelijke/generieke processen

Informatie	- Structuur en inhoud van attributen
	  - benodigd voor de authenticatie van zorgverleners en zorgaanbieders
	  - benodigd voor technische adressering

Applicatie	- Koppelingen tussen systemen van zorgaanbieders onderling - Koppelingen tussen systemen van zorgaanbieders enerzijds en systemen die invulling geven aan generieke functies anderzijds

Laag/kolom	Scope groeipad Twiin X Nuts
	- Koppelingen tussen systemen van zorgaanbieders enerzijds en authenticatiemiddelen voor zorgverleners anderzijds - Afspraken over het uitgeven, beheren en controleren van verklaringen - Afspraken over het creëren, beheren en controleren van digitale identiteiten
IT-Infrastructuur	- Communicatie Beveiliging - Authenticatie met behulp van certificaten
Beveiliging	- Communicatie Beveiliging
Wet- en regelgeving	- NEN 7510, NEN 7512 en NEN 7513 - De voorgestelde oplossingsrichtingen zijn op basis van de expertise van de auteurs en de geconsulteerde experts getoetst op wet- en regelgeving. Een uitgebreide toets op wet- en regelgeving door een juridisch expert is niet uitgevoerd.

Aannames

Bij de totstandkoming van dit document is een aantal aannames gehanteerd. Deze worden in dit hoofdstuk nader beschreven.

Aanname	Kans	Impact
1. Self-sovereign identity (SSI) wordt het leidende principe voor het aanmaken en beheren van digitale identiteiten.	Onbekend	Hoog
2. De W3C-standaard Verifiable Credentials wordt de de facto internationale standaard voor het aan, beheren en controleren van verklaringen.	Midden	Hoog
3. De W3C-standaard Decentralized Identifiers (DIDs) wordt uiterlijk 2026 de de facto internationale standaard voor het en publiceren beheren van identiteiten.	Onbekend	Hoog
4. Groeipad Twiin-Nuts kan worden afgerond in het jaar 2025.	Hoog (laag voor bestaande implementaties document/beeld)	Hoog
5. Inhoud groeipad Twiin-Nuts sluit goed aan bij toekomstige NEN-normen generieke functies	Hoog	Hoog
6. Draagvlak, capaciteit, financiering en mandaat voor uitvoeren van activiteiten groeipad is binnen Twiin en Nuts aanwezig of kan tijdig worden gecreëerd.	Onbekend	Hoog
7. Draagvlak, capaciteit, financiering en mandaat voor	Midden	Hoog

Aanname	Kans	Impact
uitvoeren van activiteiten groeipad door beoogde uitgevers van verklaringen (zoals VZVZ en CIBG) is aanwezig of kan tijdig worden gecreëerd.		
8. Draagvlak, capaciteit, financiering en mandaat voor uitvoeren van activiteiten groeipad door XIS- en knooppunt-leveranciers is aanwezig of kan tijdig worden gecreëerd.	Midden	Hoog
9. Stelselbeheer wordt ondergebracht bij een staande organisatie. Een staande organisatie neemt de taken van het Twiin-programma over.	Hoog	Midden
10. De in dit rapport voorgestelde oplossingsrichtingen zijn compatibel met de bestaande situatie.	Hoog (laag voor bestaande implementaties document/beeld)	Midden

Aanname 1: Self-sovereign identity (SSI) wordt het leidende principe voor het aanmaken en beheren van digitale identiteiten.

Kans: Onbekend	
Factoren die kans vergroten	- De Europese Unie omarmt het principe en werkt aan een eIDAS compatibel European Self-Sovereign Identity Framework (ESSIF). Self-Sovereign Identity (SSI) is een relatief nieuwe ontwikkeling waarin Twiin en Nuts potentie zien voor een duurzaam, open gegevensuitwisseling o.b.v. internationale standaarden - De Rijksdienst voor Identiteitsgegevens verkent SSI - De principes van SSI zijn onderdeel van DIZRA (zie bijv. de systeemactor Gegevensregisseur)
Factoren die kans verkleinen	- ESSIF nog niet gereed - Initiatieven nog in onderzoeksfase - SSI is een relatief nieuwe ontwikkeling waarvan de impact en adoptie in Nederland zijn echter nog niet echt goed onderzocht zijn.
Impact: Hoog	
Impact wanneer aanname realiteit wordt	- Voldoen aan (concept van) ESSIF - Omarmen Decentralized Identifiers (DID)
Impact wanneer aanname geen realiteit wordt	- Onbekend
Acties	

Acties ter vergroting kans	- Uitdragen principe - Opnemen in Twiin Afsprakenstelsel
Acties om impact te beheren	- In kaart brengen impact op bestaande infrastructuren in Nederland (zie ook aanname 10) - Starten onderzoek in samenwerking met partijen als Informatieberaad, Architectuurboard Zorg, IHE Nederland, HL7 Nederland, leveranciers (OiZ, TSV), Ministerie van VWS, Nictiz, de koepels en VZVZ.

Aanname 2: De W3C-standaard Verifiable Credentials wordt uiterlijk 2026 de de facto internationale standaard voor het uitgeven, houden en controleren van verklaringen.

Kans: Midden	

Factoren die kans vergroten	- De 1.0-versie van de standaard Verifiable Credentials is in juli 2022 vastgesteld door W3C
	- Het gebruik ervan is ook beschreven in de DIZRA (als 'verklaringen')
	- Wordt door W3C en in wetenschappelijke artikelen (o.a. https://ieeexplore.ieee.org/document/9031548) voorgesteld als de standaard voor het uitgeven, houden en controleren van verklaringen.
	- Verifiable Credentials bieden meer flexibiliteit dan PKI (zie Bijlage 2: PKI en SSI)
	- Verifiable Credentials sluit goed aan bij ideeën van Europese Unie over SSI en attribuut-gebaseerd authenticeren (ESSIF)
	- Verifiable Credentials wordt nationaal en internationaal door steeds meer partijen omarmd:
	  - HL7 SMART Healthcards
	  - Apple Verificable Health Records
	  - Microsoft biedt via Azure gestandaardiseerde services aan voor het gebruik van Verifiable Credentials
	  - Zorginstituut Nederland KIK-V
	  - Zorginstituut Nederland iWlz
	  - Zorgaanbieders die in het kader van VIPP InZicht eOverdracht implementeren
	  - Zorgaanbieders die in het kader van VIPP Babyconnect gegevensuitwisseling implementeren
	- Het UZI-register wil de registratie van identiteiten loskoppelen van authenticatiemiddelen en voert hiervoor pilots met de standaard Verifiable Credentials (VC) uit.
	- Nuts stelt gratis open source software beschikbaar om de standaard Verifiable Credentials te implementeren.
	- VC is een relatief nieuwe ontwikkeling en open. internationale standaard.

Factoren die kans verkleinen	- IRMA heeft de standaard Verifiable Credentials nog niet omarmd. - Er is nog geen standaard voor wallets. Hierdoor is er sprake

	van een risico dat voor verschillende verklaringen verschillende apps nodig gaan zijn. Een voorbeeld hiervan is het elektronisch rijbewijs. - ESSIF-traject duurt lang/ trager dan 2026 - Beperkte ervaring met Verifiable Credentials in Nederland - Standaard Verifiable Credentials wordt momenteel nog niet breed omarmd door Zorg-IT leveranciers en VZVZ - VC is een relatief nieuwe ontwikkeling waarvan de impact en adoptie in Nederland zijn echter nog niet echt goed onderzocht is..
Impact: Hoog	
Impact wanneer aanname realiteit wordt	- Acties uitvoeren conform groeipad - Uitdragen standaard
Impact wanneer aanname geen realiteit wordt	- Er kan worden teruggevallen op Nederland-specifieke implementatie van PKI zoals UZI en Nederland-specifieke implementatie van SSI zoals IRMA. - Groeipad Twiin-Nuts is nu gebaseerd op VC. Dient te worden aangepast.
Acties	
Acties ter vergroting kans	- Met behulp van NEN-normeringen bijdragen aan standaardisering - Uitdragen standaard - Opnemen in Twiin Afsprakenstelsel
Acties om impact te beheren	- In kaart brengen impact op bestaande infrastructuren in Nederland (zie ook aanname 10) - Starten onderzoek in samenwerking met partijen als Informatieberaad, Architectuurboard Zorg, IHE Nederland, HL7 Nederland, leveranciers (OiZ, TSV), Ministerie van VWS, Nictiz, de koepels en VZVZ.

Aanname 3: De W3C-standaard Decentralized Identifiers (DIDs) wordt uiterlijk 2026 de de facto internationale standaard voor het publiceren en beheren van identiteiten.

Kans: Onbekend	

Factoren die kans vergroten	- Wordt door W3C en in wetenschappelijke artikelen (o.a. https://ieeexplore.ieee.org/document/9031548) voorgesteld als de standaard voor het publiceren en beheren van identiteiten.
	- DID is een open internationale standaard.
	- DID is meer flexibel dan PKI (zie bijlage 2)
	- DID sluit goed aan bij ideeën van Europese Unie over SSI en attribuut-gebaseerd authenticeren
	- DID wordt nationaal door steeds meer partijen omarmd:
	  - Zorginstituut Nederland KIK-V
	  - Zorginstituut Nederland iWlz
	  - Zorgaanbieders die in het kader van VIPP InZicht

	eOverdracht implementeren - Zorgaanbieders die in het kader van VIPP Babyconnect gegevensuitwisseling implementeren - Wanneer het UZI-register de registratie van identiteiten los wil trekken van de authenticatiemiddelen is dit type technologie nodig - DID is in juli 2022 tot formele standaard benoemd.
Factoren die kans verkleinen	- DID methodes om DIDs te publiceren en in te trekken zijn er nog niet. Dit is ook een kritiek van partijen als Google en Mozilla. - DID is bewust niet gebruikt in het Europese project voor digitale covid-vaccinatiecertificaten - eIDAS-traject duurt lang/ trager dan 2025 - Beperkte ervaring met DID in NL - Niet breed omarmd door Zorg-IT leveranciers en VZVZ - DID is een relatief nieuwe ontwikkeling waarvan.de impact en adoptie in Nederland zijn echter nog niet echt goed onderzocht is.
Impact: Hoog	
Impact wanneer aanname realiteit wordt	- Acties uitvoeren conform groeipad - Uitdragen standaard
Impact wanneer aanname geen realiteit wordt	- Er kan worden teruggevallen op Nederland-specifieke implementatie van PKI zoals UZI en Nederland-specifieke implementatie van SSI zoals IRMA. - Groeipad Twiin-Nuts is nu gebaseerd op VC. Dient te worden aangepast.
Acties	
Acties ter vergroting kans	- Met behulp van NEN-normeringen bijdragen aan standaardisering - Uitdragen standaard - Opnemen in Twiin Afsprakenstelsel
Acties om impact te beheren	- In kaart brengen impact op bestaande infrastructuren in Nederland (zie ook aanname 10) - Starten onderzoek in samenwerking met partijen als Informatieberaad, Architectuurboard Zorg, IHE Nederland, HL7 Nederland, leveranciers (OiZ, TSV), Ministerie van VWS, Nictiz, de koepels en VZVZ.

Aanname 4: Groeipad Twiin-Nuts kan worden afgerond in het jaar 2026.

Kans: Hoog (laag voor bestaande implementaties document/beeld))	
Factoren die kans vergroten	- NEN-normen zorgen voor duidelijkheid en versnelling - Onderschrijving van belang en urgentie door zorgsector - Aantal partijen dat ten behoeve van groeipad ontwikkelingen

	moet uitvoeren is beperkt in omvang - Adoptie door informatieberaad - Opname in doelarchitectuur zorg - Breder draagvlak en participatie van partijen buiten Nuts en Twiin - In veel zorgsectoren en voor veel zorgtoepassingen is sprake van een 'green field' inzake uitwisselingsinfrastructuur. Hierdoor zijn er weinig obstakels voor de implementatie van de in dit rapport voorgestelde oplossingsrichtingen. - Lopende ontwikkelingen aangaande ZORG-ID, ZORG-AB en UZI-register sluiten aan bij in dit document voorgestelde oplossingsrichtingen. - Twiin en Nuts zien potentie in de in dit document beschreven oplossingsrichtingen voor een duurzaam, open gegevensuitwisseling o.b.v. internationale standaarden
Factoren die kans verkleinen	- De impact en adoptie van de genoemde nieuwe standaarden in Nederland is echter nog niet goed onderzocht. - Te veel partijen betrekken waardoor besluitvorming te traag wordt - Het is momenteel nog niet bekend of de XIS-leveranciers van verschillende zorgaanbieders de beschreven oplossingsrichtingen zullen omarmen.
Impact: Hoog	
Impact wanneer aanname realiteit wordt	- Acties uitvoeren conform groeipad
Impact wanneer aanname geen realiteit wordt	- Acties verdelen over grotere tijdsduur
Acties	
Acties ter vergroting kans	- Betere onderbouwing benodigde ontwikkelinspanning per partij - Tijdig betrekken partijen met een verwachte ontwikkelinspanning - De benodigde ontwikkelinspanning modulair beschrijven zodat de gewenste functionaliteit desgewenst door een combinatie van leveranciers kan worden geïmplementeerd en de afhankelijkheid van XIS-leveranciers afneemt.
Acties om impact te beheren	- Volgordelijkheid acties goed in kaart brengen, feitelijke planning kan hiervan worden afgeleid

Aanname 5: Inhoud groeipad Twiin-Nuts sluit goed aan bij toekomstige NEN-normen generieke functies

Kans: Hoog	
Factoren die kans vergroten	- Bemensing NEN-werkgroep Generieke Functies en werkgroep Twiin-Nuts overlapt - NEN-normen en groeipad baseren zich op dezelfde referentiearchitectuur DIZRA - Technologische ontwikkelingen maken het mogelijk/noodzakelijk om scherper te normeren op het gebied van onderling vertrouwen (zie ook aanname 1 over SSI en aanname 2 over Verifiable Credentials) - NEN-normen zijn functioneel van aard en doen geen uitspraken over te hanteren standaarden
Factoren die kans verkleinen	- NEN normen beschrijven geen technische implementatie
Impact: Hoog	
Impact wanneer aanname realiteit wordt	- Acties en oplossingsrichtingen uitvoeren zoals opgenomen in Transformation Map
Impact wanneer aanname geen realiteit wordt	- Aanpassen fases 2024-2025 en 2026 in groeipad
Acties	
Acties ter vergroting kans	- Indienen van dit rapport bij NEN werkgroep Generieke functies door NEN-werkgroepleden die Twiin en Nuts vertegenwoordigen.
Acties om impact te beheren	- Acties groeipad plannen en begroten tot 2023 Q2 en dan herijken op basis van prepublicatie NEN normen (zie ring "NEN-normen" in transformation map) - Conceptversies van normen tijdig bestuderen en waar nodig verwerken in groeipad

Aanname 6: Draagvlak, capaciteit, financiering en mandaat voor uitvoeren van activiteiten groeipad is binnen Twiin en Nuts aanwezig of kan tijdig worden gecreëerd.

Kans: Hoog	
Factoren die kans vergroten	- Experts Twiin en Nuts zijn betrokken bij beschrijving groeipad - Vroegtijdige transparantie over proces en inhoud beschrijving en uitvoering groeipad - Actief betrekken achterbannen Twiin en Nuts - Actief betrekken bestuurders Twiin en Nuts - Actief betrekken DIZRA en Architectuurboard

Factoren die kans verkleinen	- Het groeipad is gedefinieerd door een beperkte vertegenwoordiging van Twiin en Nuts. Achterbannen Twiin en Nuts zijn nog niet uitvoerig geïnformeerd.
Impact: Hoog	
Impact wanneer aanname realiteit wordt	- Acties en oplossingsrichtingen uitvoeren zoals opgenomen in Transformation Map
Impact wanneer aanname geen realiteit wordt	- Geen gezamenlijke uitvoering groeipad - Partijen overhalen om met behulp van 'cherry picking' wel onderdelen van groeipad uit te voeren'
Acties	
Acties ter vergroting kans	- Uitdragen groeipad
Acties om impact te beheren	- Oplossingsrichtingen onafhankelijk van groeipad uitdragen

Aanname 7: Draagvlak, capaciteit, financiering en mandaat voor uitvoeren van activiteiten groeipad door beoogde uitgevers van verklaringen (zoals VZVZ en CIBG) is aanwezig of kan tijdig worden gecreëerd.

Kans: Midden	
Factoren die kans vergroten	- Inzetten op standaarden - Experts VZVZ en CIBG worden vroegtijdig betrokken
Factoren die kans verkleinen	- Experts registers VZVZ en CIBG zijn niet betrokken bij beschrijving groeipad
Impact: Hoog	
Impact wanneer aanname realiteit wordt	- Acties en oplossingsrichtingen uitvoeren zoals opgenomen in Transformation Map
Impact wanneer aanname geen realiteit wordt	- Zoeken naar mogelijke andere manieren om oplossingsrichtingen van groeipad te implementeren
Acties	
Acties ter vergroting kans	- Actief betrekken registers VZVZ en CIBG
Acties om impact te beheren	- Focus op standaarden

Aanname 8: Draagvlak, capaciteit, financiering en mandaat voor uitvoeren van activiteiten groeipad door XIS- en knooppunt-leveranciers is aanwezig of kan tijdig worden gecreëerd.

Kans: Midden	
Factoren die kans vergroten	- Groeipad wordt getoetst door leveranciers via Taskforce Samen Vooruit - Inhoud groeipad wordt opgenomen in Twiin afsprakenstelsel en heeft daarmee al draagvlak bij een deel van de belanghebbenden.
Factoren die kans verkleinen	- Leveranciers zijn niet betrokken bij beschrijving groeipad
Impact: Hoog	
Impact wanneer aanname realiteit wordt	- Acties en oplossingsrichtingen uitvoeren zoals opgenomen in Transformation Map
Impact wanneer aanname geen realiteit wordt	- Dan zal toch weer teruggevallen moeten worden op het maken van procedurele en organisatorische afspraken. De vraag is dan nog of (eOverdracht via) Nuts in het Twiin afsprakenstelsel moet worden opgenomen, omdat er een lage mate van samenhang met andere (Twiin) zorgtoepassingen is.
Acties	
Acties ter vergroting kans	- Uitdragen groeipad - Actief betrekken leveranciers
Acties om impact te beheren	- Meenemen oplossingsrichtingen in ontwerp Twiin-certificering

Aanname 9: Stelselbeheer wordt ondergebracht bij een staande organisatie. Een bestaande organisatie neemt de taken van het Twiin-programma over.

Kans: Hoog	
Factoren die kans vergroten	- Brede toepassing van Twiin afsprakenstelsel - Opname groot aantal zorgtoepassingen in Twiin afsprakenstelsel - Duidelijkheid over beheer
Factoren die kans verkleinen	-
Impact: Middel	
Impact wanneer aanname realiteit	- Acties en oplossingsrichtingen uitvoeren zoals opgenomen in Transformation Map

wordt	
Impact wanneer aanname geen realiteit wordt	- Acties en oplossingsrichtingen uitvoeren zoals opgenomen in Transformation Map. Mogelijk andere invulling zoeken voor rollen zoals Verzekeraar Betrouwbaarheid en Ledenadministratie
Acties	
Acties ter vergroting kans	- Beschrijven rollen en invulling stelselbeheer o.b.v. NEN 7522.
Acties om impact te beheren	- Wanneer rollen zijn beschreven, kunnen verschillende alternatieven voor invulling ervan worden onderzocht

Aanname 10: De in dit rapport voorgestelde oplossingsrichtingen zijn compatibel met de bestaande situatie.

Kans: Hoog (laag voor bestaande implementaties document/beeld)	
Factoren die kans vergroten	- Oplossingsrichtingen sluiten aan op internationale open standaarden - Wanneer bestaande applicaties technisch (nog) niet compatibel kunnen worden gemaakt met de voorgestelde oplossingsrichtingen, kan worden teruggevallen op aanvullende organisatorische afspraken en/of het gebruik van dienstverleners. - Leveranciers worden tijdig betrokken via TSV - In veel zorgsectoren en voor veel zorgtoepassingen is sprake van een 'green field' inzake uitwisselingsinfrastructuur. Hierdoor zijn er weinig obstakels voor de implementatie van de in dit rapport voorgestelde oplossingsrichtingen. - VZVZ's authenticatie-oplossing ZORG-ID sluit goed aan bij de in dit rapport voorgestelde oplossingsrichtingen. ZORG-ID wordt ontwikkeld voor brede toepassing binnen en buiten de context van AORTA/LSP. - Lopende ontwikkelingen aangaande ZORG-AB en UZI-register sluiten aan bij in dit document voorgestelde oplossingsrichtingen
Factoren die kans verkleinen	- Voor de uitwisseling van beelden en documenten wordt (met name binnen de medisch-specialistische zorg) gebruik gemaakt van door IHE gestandaardiseerde XDS-infrastructuren. Er is bekeken hoe bestaande IHE-infrastructuren de Nuts-standaarden, DID, VC en SSI zouden kunnen implementeren. De IHE-standaarden bevatten kansrijke aanknopingspunten (o.a. IUA) die ook door de in Nederland actieve XDS-leveranciers worden aangeboden. Bestaande XDS-implementaties bieden hiervoor echter nog geen ondersteuning wat de compatibiliteit met de in dit rapport voorgestelde

	oplossingsrichtingen drastisch verlaagd.
Impact: Midden	
Impact wanneer aanname realiteit wordt	- Acties en oplossingsrichtingen uitvoeren zoals opgenomen in Transformation Map
Impact wanneer aanname geen realiteit wordt	- Een betrekkelijk eenvoudige oplossing zou kunnen zijn om een 'knip' te maken tussen document-gebaseerde en zib/fhir-gebaseerde zorgtoepassingen. De in dit rapport voorgestelde oplossingsrichtingen kunnen dan in eerste instantie alleen voor zib/fhir-gebaseerde zorgtoepassingen worden overwogen.
Acties	
Acties ter vergroting kans	- Uitdragen groeipad - Actief betrekken leveranciers - Per zorgtoepassing bepalen impact van groeipad - Maken keuzes over welke zorgtoepassingen wel en niet onderdeel zijn van groeipad (bijv. onderscheid tussen document-gebaseerde en zib/fhir-gebaseerde zorgtoepassingen)
Acties om impact te beheren	- Stimuleren totstandkoming keuzemogelijkheden Dienstverleners

Vertrouwen

Bij gegevensuitwisseling in de zorg worden gegevens in de basis uitgewisseld tussen een bronhoudende en een afnemende partij. Het realiseren van de juiste mate van vertrouwen tussen de bronhoudende en de afnemende partij is daarbij essentieel. Alleen wanneer sprake is van de juiste mate van vertrouwen, kunnen gegevens op een veilige en verantwoorde manier en conform wet- en regelgeving worden uitgewisseld. Ter illustratie: Vanuit de bronhoudende partij bekeken zijn o.a. de volgende vragen relevant om te kunnen bepalen of sprake is van de juiste mate van vertrouwen:

- Treedt het afnemende systeem op als verwerker van de beoogde afnemende zorgaanbieder?
- Wat is de identiteit van de zorgverlener die gegevens wil afnemen?
- Vertegenwoordigt de zorgverlener die gegevens wil afnemen de beoogde afnemende zorgaanbieder?

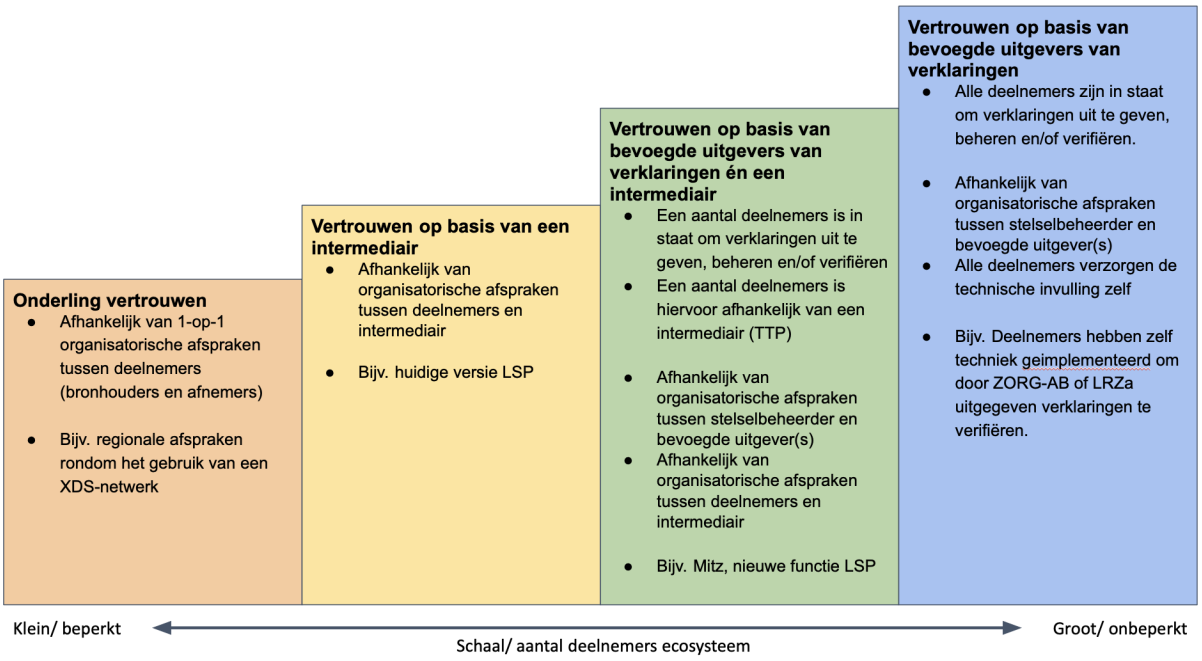
Om de juiste mate van vertrouwen tussen de bronhoudende en de afnemende partij te realiseren zijn op dit soort vragen antwoorden met een voldoende mate van zekerheid nodig. Binnen het Nederlandse zorglandschap is veel ervaring opgedaan met het op verschillende manieren realiseren van vertrouwen. Bij de totstandkoming van XDS-netwerken bijvoorbeeld, maken de deelnemende partijen vooraf organisatorische afspraken met elkaar om de juiste mate van onderling vertrouwen te realiseren. Een voorbeeld hiervan is een afspraak om elkaars authenticatieprocessen te vertrouwen. Dit soort vertrouwen is praktisch beperkt schaalbaar.

Wanneer er op grotere schaal uitgewisseld moet worden is er meer nodig. De duizenden zorgaanbieders die onderling met elkaar uitwisselen via het LSP kunnen praktisch gezien niet met elke andere partij onderling afspraken maken. Daarom is daar gekozen om gebruik te maken van het UZI-register als bevoegde uitgever van identiteiten en (PKI-) middelen voor de authenticatie van zorgaanbieders en zorgverleners. De uitwisseling zelf loopt via het LSP/VZVZ, een partij die door alle andere partijen vertrouwd en gecontroleerd kan worden.

Het realiseren van vertrouwen vindt in de huidige situatie al op verschillende manieren plaats, er is dus geen sprake van een greenfield. De gemene deler is dat vertrouwen wordt gerealiseerd met een combinatie van *technologie* en *organisatorische afspraken*. De balans tussen deze twee kan per gegevensuitwisseling verschillen. Hiermee samenhangend verschilt per gegevensuitwisseling de keuze voor een vertrouwensmodel: *onderling vertrouwen*, *vertrouwen op basis van een intermediair*, of *vertrouwen op basis van een vertrouwde derde partij*.

Om de gewenste situatie te kunnen bepalen is het verstandig om grootheden als schaalbaarheid, betaalbaarheid, technologische innovatie, beveiliging en privacy mee te nemen. Omwille van schaalbaarheid, betaalbaarheid en technologische innovatie is het prettig als vertrouwen voor het leeuwendeel kan worden gerealiseerd op basis van *technologie* en zo min mogelijk afhankelijk is van *organisatorische afspraken*. Daarnaast zijn *vertrouwen op basis van een intermediair* en *vertrouwen op basis van een vertrouwde derde partij* een stuk beter schaalbaar dan *onderling vertrouwen*. Omwille van beveiliging, privacy, technologische innovatie, betaalbaarheid en schaalbaarheid verdient *vertrouwen op basis van een vertrouwde derde partij* de voorkeur boven *vertrouwen op basis van een intermediair*.

Nu de huidige en gewenste situatie zijn verkend, is het mogelijk een globaal groeimodel voor het realiseren van vertrouwen op te stellen:

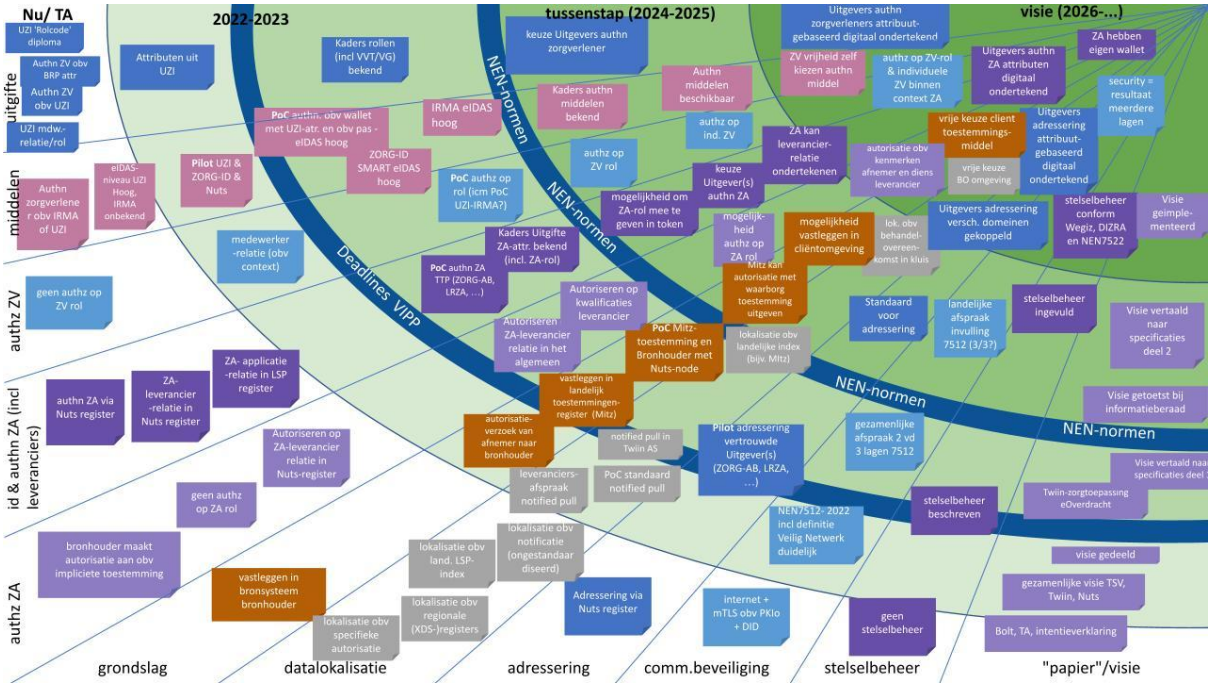


Het groeimodel kan houvast bieden in het bepalen van de juiste volgorde van stappen.

In dit stuk wordt vaak gewezen op de implementatie van de technieken Decentralized Identifiers (DID) en Verifiable Credentials (VC). Dit zijn nieuwe technologieën die deels vervangend en aanvullend zijn op de PKI-technologie die momenteel veel wordt ingezet. In bijlage 2 wordt beschreven hoe deze technologieën zich tot elkaar verhouden.

2. Transformation map

Om een gezamenlijke groeipad van Twiin en Nuts te ontwerpen is gebruik gemaakt van een zogenaamde transformation map.



Figuur 1: Transformation map

Een grotere versie van de transformation map is opgenomen in bijlage 1.

In de transformation map zijn allerlei stappen geplot om te komen tot het verwezenlijken van de gemeenschappelijke visie. Het diagram bevat drie verschillende entiteiten:

1. fases
2. aandachtsgebieden
3. resultaten

Deze entiteiten worden hieronder nader toegelicht.

Fases

Het diagram kent 5 opeenvolgende ontwikkelfases die als ‘ringen’ zijn weergegeven:

- Nu (TA):
    - Deze fase omvat de huidige situatie voor de zorgtoepassing eOverdracht (op basis van de Technische Afspraak eOverdracht en de Nuts Bolt eOverdracht)
    - Resultaten die in deze fase zijn geplot, zijn al beschikbaar.
- 2022-2023 (korte termijn):
    - Resultaten die in deze fase zijn geplot, vormen de eerste voorbereidende stappen die dit jaar kunnen worden gezet.
- Deadline VIPP-regelingen
    - De deadlines van de verschillende VIPP-regelingen zijn op verschillende data, maar voor relevante toepassingen als geboortezorg, eOverdracht en de BgZ vallen ze in 2023 of 2024. De verwachting is dat er over het algemeen

weinig ruimte is om plannen die gemaakt zijn om deze deadlines te halen nog aan te passen zodat de ontwikkelingen meer in de richting van de visie worden gedaan.
    - VIPP InZicht
        - Module eOverdracht behelst de uitwisseling van gegevens ten behoeve van de verpleegkundige overdracht tussen zorgaanbieders in care en cure.
        - Deadline is december 2022
        - Lopende implementaties van de module eOverdracht voldoen op de lagen applicatie en infrastructuur al grotendeels aan inhoud van het groeipad.
        - In het geval van lopende implementaties zal er tot december 2022 weinig tot geen ruimte zijn om acties te ondernemen die bijdragen aan het meer voldoen aan het Twiin x Nuts groeipad.
    - VIPP 5:
        - Module 3 behelst de uitwisseling van de BgZ tussen zorgaanbieders.
        - Deadline voor deze module is juni 2023.
        - Lopende implementaties van module 3 op basis van CDA en XDS voldoen op de lagen applicatie en infrastructuur grotendeels niet aan inhoud van het groeipad.
        - Implementaties van module 3 op basis van FHIR zij nog niet uitgekristalliseerd. Dit is mogelijk een kans om invulling te geven aan het groeipad
        - In het geval van lopende CDA-XDS-implementaties zal er tot juni 2023 weinig tot geen ruimte zijn om acties te ondernemen die bijdragen aan het meer voldoen aan het Twiin x Nuts groeipad
    - VIPP Babyconnect:
        - behelst onder andere de uitwisseling van geboortezorggegevens tussen zorgaanbieders.
        - Deadline is juni 2024
        - Lopende implementaties via Nuts voldoen op de lagen applicatie en infrastructuur al voor een deel aan inhoud van het groeipad.
    - VIPP Farmacie en programma medicatieoverdracht:
        - behelst de uitwisseling van medicatiegegevens tussen zorgaanbieders.
        - De subsidieregeling van de kickstart Medicatieoverdracht loopt tot 2024
        - Einddatum VIPP farmacie is nog niet bekend
    - VIPP OPEN:
        - uitwisseling tussen zorgaanbieders niet in scope
    - VIPP GGZ:
        - uitwisseling tussen zorgaanbieders niet in scope
    - VIPP GGZ Vrijgevestigden:
        - uitwisseling tussen zorgaanbieders niet in scope
- NEN:
    - De werkgroepen voor de generieke functies identificatie & authenticatie, toestemming en lokalisatie zijn onlangs gestart. De verwachting is dat medio 2023 de (ontwerp)normen worden opgeleverd. Deze normen gaan over

dezelfde onderwerpen als in dit stuk behandeld worden en zullen de kaders scheppen waarbinnen technische specificaties gemaakt moeten worden. Wanneer de normeringstrajecten voor de andere gedefinieerde generieke functies gaan starten is niet bekend.

- 2024-2025 (middellange termijn):
    - Deze fase omvat grofweg de kalenderjaren 2024 en 2025 en start na de oplevering van de normen voor de generieke functies.
    - Resultaten die in deze fase zijn geplot, moeten in lijn zijn met de NEN-(ontwerp)normen voor generieke functies.
- 2026 (doel):
    - Deze fase omvat de gewenste situatie in het kalenderjaar 2026.
    - Resultaten die in deze fase zijn geplot, geven de gezamenlijke (kwalitatieve) doelstellingen van Twiin en Nuts weer.

De fase 2026 (einddoel) is rechtsboven in het diagram weergegeven.

Aandachtsgebieden

De ringen in de transformation map worden doorkruist door 11 stralen. Iedere straal staat voor een aandachtsgebied. De volgende aandachtsgebieden zijn opgenomen:

1. Authenticatie Zorgverlener – Uitgifte
2. Authenticatie Zorgverlener – Middelen
3. Autorisatie Zorgverlener
4. Authenticatie Zorgaanbieder
5. Autorisatie Zorgaanbieder
6. Expliciete toestemming
7. Datalokalisatie
8. Adressering
9. Communicatiebeveiliging
10. Stelselbeheer
11. “Papier”/ visie

Een nadere omschrijving per aandachtsgebied is opgenomen in de volgende hoofdstukken nader toegelicht.

Resultaten

Verdeeld over de ringen en stralen is in het diagram een groot aantal rechthoeken geplaatst. Iedere rechthoek staat voor een resultaat. De resultaten van één aandachtsgebied zijn weergegeven in dezelfde kleur. Er is naar gestreefd ieder resultaat logisch te ordenen ten opzichte van de andere resultaten. Dit geldt voor resultaten binnen hetzelfde aandachtsgebied en voor resultaten die zijn verdeeld over verschillende aandachtsgebieden. De resultaten in de ring "2026 (doel)” geven per aandachtsgebied de gezamenlijke (kwalitatieve) doelstelling van Twiin en Nuts weer.

In de hoofdstukken hieronder wordt van ieder aandachtsgebied de inhoud, de visie en de concretisering van het groeipad beschreven. Hierbij wordt het vijf-lagen interoperabiliteitsmodel van Nictiz gebruikt.

3. Aandachtsgebied 1: Identificatie en authenticatie zorgverlener - Uitgifte van attributen

Het vaststellen en controleren van de identiteit en andere eigenschappen van zorgverleners is een onmisbaar onderdeel bij het realiseren van veilige gegevensuitwisseling in de zorg. Dit wordt gerealiseerd door middel van de generieke functie 'identificatie en authenticatie'. In dit document wordt deze generieke functie is twee onderdelen gesplitst:

- Uitgifte van attributen
- Authenticatiemiddelen

Dit hoofdstuk beschrijft de uitgifte van attributen.

Inleiding

Om veilig en verantwoord gegevens uit te kunnen wisselen, is inzage in verschillende kenmerken van de betrokken zorgverlener(s) nodig. Bij gegevensuitwisseling zijn onder andere de volgende vragen relevant:

- Wie is de zorgverlener die informatie wil afnemen of aanbieden?
- Wat zijn de bevoegdheden van de zorgverlener?
- Vanuit welke (zorgaanbieder-specifieke) rol opereert de zorgverlener?

Dit soort kenmerken wordt attributen genoemd. Verschillende attributen kunnen verschillende bronregisters hebben.

Gezamenlijke visie

Doel voor 2026

Voor de authenticatie van zorgverleners wordt gebruikt gemaakt van digitaal ondertekende attributen die door een beperkt aantal vertrouwde instanties worden uitgegeven.

Waarom

Voor veilige gegevensuitwisseling tussen twee verschillende zorgaanbieders is een gezamenlijk beeld van de identiteit en andere voor gegevensuitwisseling relevante kenmerken van de betrokken zorgverleners nodig. Dit noemen we zorgaanbieder-overstijgende authenticatie. In Nederland zijn ongeveer 140.000 verschillende zorgaanbieders actief. Door het grote aantal zorgaanbieders is een vertrouwensmodel gebaseerd op 1-op-1 organisatorische afspraken tussen individuele zorgaanbieders (peer-to-peer trust) slecht schaalbaar. Organisatorische en procedurele oplossingen zijn er wel, zoals Twiin en AORTA, waar een derde partij instaat voor (een deel van) de benodigde waarborgen. Dit model heeft zich bewezen, maar hier is ook kritiek op (om deze modellen als structurele oplossing te gebruiken). Een deel van de zorg zou namelijk ook *zonder* deze partij(en), direct als zorgaanbieders onderling willen uitwisselen.

Consequenties

Er zijn gezamenlijke standaarden nodig voor de syntax en semantiek van attributen en de digitale ondertekening daarvan. Deze standaarden dienen te worden geïmplementeerd door

de eigenaren van de benodigde bronregisters die daarmee de rol van uitgever krijgen. Deze standaarden dienen ook te worden geïmplementeerd door zorgaanbieders die data willen aanbieden of afnemen.

Concretisering

Organisatiebeleid

Landelijk en zorgbreed dienen afspraken te worden gemaakt over de welke partij(en) vertrouwd worden om als uitgever van verklaringen over zorgverleners op mag treden. Een *Bevoegde uitgever van verklaringen* (DIZRA-definitie, vanaf hier: uitgever) geeft verklaringen over kenmerken van zorgverleners uit in de vorm van attributen (zie informatielaag). Om de attributen te kunnen gebruiken dienen deze ontsloten te kunnen worden door de betrokkenen met behulp van een authenticatiemiddel. Het niveau van betrouwbaarheid van het uitgifteproces i.c.m. de betrouwbaarheid van het authenticatiemiddel bepaalt de betrouwbaarheid van het attribuut.

Zorgproces

Zorgaanbieders dienen processen in te richten waarmee attributen beheerd, uitgegeven en gecontroleerd kunnen worden. Nu al er vaak een personeelsregistratie zijn waarin attributen worden aangemaakt en beheerd, maar de mogelijkheid om deze uit te geven, te kunnen koppelen aan een authenticatiemiddel én daarmee voor derde partijen controleerbaar wordt, zal nog ontbreken.

Zorgverleners zelf hebben mogelijk ook de wens om hun eigen attributen te beheren. Hiervoor zullen zij een zogenaamde wallet moeten hebben waar de attributen andere partijen, zoals de werkgever of de opleidingsinstantie in beheerd kunnen worden.

Informatie

De volgende gegevens over zorgverleners dienen door de uitgever(s) als attribuut uitgegeven te worden, zoals:

- Identiteit, een uniek identificatienummer voor een zorgverlener (en zorgmedewerker) die zorgaanbieder overstijgend en levenslang is gekoppeld aan de persoon. Hiermee kunnen personen over instellingen heen uniek geïdentificeerd worden. In een eerder stadium is in het informatieberaad al besloten over het gebruik van het UZI-nummer, uitgegeven door het UZI-register. Momenteel is het niet duidelijk of alle kwalificaties (diploma's) in de zorg een UZI-rolcode kunnen krijgen en/of er (binnen een zorgtoepassing) nog specifieke rollen/functies zijn waarop geautoriseerd kan/moet worden.
- Kwalificatie, een weerspiegeling van de diploma('s) die een zorgverlener heeft. De kwalificatie vormt vaak de basis voor autorisatieregels: welke rol mag de persoon uitvoeren en tot welke gegevens is er toegang? Het UZI-register geeft nu aan een grote groep zorgverleners een UZI-rolcode uit, voornamelijk o.b.v. het BIG-register. Er is in het veld ook behoefte aan codes voor niet-BIG-geregistreerde zorgverleners.
- De werkgeversrelatie en functie. Hiermee kan de communicerende partij bepalen of de persoon daadwerkelijk werkt voor de betreffende zorgorganisatie en in welke rol.

Dat iemand een kwalificatie heeft om een functie te mogen uitvoeren betekent niet automatisch dát de functie ook uitgevoerd wordt. Op basis van de functie kan mede bepaald worden of de persoon bevoegd is om bepaalde medische gegevens te verwerken.

Applicatie

Deze attributen dienen digitaal ondertekend te zijn zodat de herkomst en juistheid eenvoudig kunnen worden gecontroleerd. Omdat verschillende attributen vermoedelijk verschillende bronregisters kunnen hebben en data zo veel mogelijk bij de bron dienen te blijven, is er niet sprake van één maar van meerdere uitgevers.

Applicaties van bevoegde uitgevers zullen zo ingericht moeten worden dat deze op basis van de afgesproken standaarden en technieken de attributen kunnen uitgeven. Voor een zorgaanbieder geldt bijvoorbeeld dat nu al wel een personeelsregistratie is waarin attributen worden aangemaakt en beheerd. De mogelijkheid om deze uit te geven, te kunnen koppelen aan een authenticatiemiddel én daarmee voor derde partijen controleerbaar wordt, zal nog ontbreken.

Voor applicaties die personen moeten authenticeren zal gelden dat deze ingericht moeten worden dat dit gedaan kan worden op basis van de afgesproken standaarden en technieken en koppelingen kunnen maken met de vertrouwde uitgever(s).

De benodigde functionaliteit zal vermoedelijk gebaseerd zijn op de standaarden Decentralized Identitifiers (DID) en Verifiable Credentials. De attributen dienen in de vorm van Verifiable Credentials (VC), cryptografisch te controleren beweringen, uitgegeven te worden en te worden gekoppeld aan een digitale identiteit gemaakt op basis van DID. VC (link) en DID (link) zijn een internationale W3C-standaarden waarmee door een uitwisselingsketen heen onweerlegbaar kan worden vastgesteld om welke persoon/kwalificatie/rol het gaat.

IT-infrastructuur

Er zal een gedeelde IT-infrastructuur moeten zijn waarmee partijen identiteiten, daaraan gekoppelde attributen en af te leiden claims kunnen controleren. Deze infrastructuur zal een (zeer) hoge mate van beschikbaarheid moeten kennen.

Deliverables 2022-2026 en afhankelijkheden

Fase	**Deliverable**	**(Nog niet ingevulde) Afhankelijkheden**	**Betrokkenen**
Nu	UZI-pas 'Rolcode' diploma, UZI-pas mdw.- relatie/rol, Authn ZV obv UZI	(Breed) gebruik van UZI-pas	VZVZ, V&VN, Actiz, ...
2022		Opname gebruik UZI-authenticatie in TA	TSV, leveranciers, Nuts, Twiin

Nu	Authn ZV obv BRP attr	(Breed) gebruik van IRMA	stichting Privacy by Design, V&VN, Actiz, ...
2022	PoC Attributen uit UZI	Uitbreiding functionaliteit UZI-register	CIBG
		Koppeling met attribuutgebaseerd authenticatiemiddel (IRMA)	stichting Privacy by Design, CIBG
		Koppeling met DigiD Hoog	CIBG, BZK
2022 /23	Kaders rollen (incl VVT/VG) bekend	Consensus over (uitbreiding) codelijst rollen	V&VN, Actiz, VGN, CIBG, Nictiz
2022 /23		Rollen opgenomen in informatiestandaard	Nictiz, V&VN, Actiz
2023	**(concept) NEN-normen generieke functies**	**-**	**NEN-werkgroep Generieke Functies**
2024	keuze Uitgevers authn zorgverlener	Eisen aan uitgevers van attributen (onafhankelijk van middelen) zijn bekend (eIDAS-hoog, VC, …)	Ministerie Binnenlandse Zaken, Logius, NEN, Twiin, Nuts
		Geschikte uitgevers die voldoen aan eisen	CIBG, evt. brancheregisters (bijv. KCKZ)
2025 /26	Uitgevers authn zorgverleners attribuut-gebaseerd digitaal ondertekend	geen, resultaat van bovenstaande	geen

Deliverables 2022/23 en acties

Goal	**Strategies**	**Acties**	**Wie**
Attributen uit UZI	Uitbreiding functionaliteit UZI-register & Koppeling met attribuutgebaseerd authenticatiemiddel (IRMA en/of ander middel)	Contouren traject communiceren met CIBG	Twiin/Nuts
		Contouren traject communiceren met Privacy by Design	Twiin/Nuts
		Bepalen gewenste set attributen	Twiin/Nuts
		Bepalen overige eisen	Twiin/Nuts

		Samen met CIBG en Privacy by Design oplossingsrichting vaststellen	Twiin/Nuts & CIBG & PbD
		Formeel verzoek neerleggen bij CIBG	Twiin/Nuts
		Formeel verzoek neerleggen bij PbD	Twiin/Nuts
		Bouwen en opleveren Proof of Concept functionaliteit UZI-register en authn-middel	CIBG en PbD
		Bouwen en opleveren functionaliteit UZI-register en authn-middel	CIBG en PbD
Kaders rollen (incl VVT/VG) bekend	Consensus over (uitbreiding) codelijst rollen	Verschillenanalyse rollen zorgstandaard en rollen UZI-register	V&VN (penhouder) Actiz, VGN, CIBG, Nictiz
		Schrijven memo rollen langdurige zorg UZI-register	V&VN (penhouder) Actiz, VGN, CIBG, Nictiz
		Rollen opgenomen in informatiestandaard	Actiz, Nictiz

4. Aandachtsgebied 2: Identificatie en authenticatie zorgverlener - Authenticatiemiddelen

Inleiding

Om veilig en verantwoord gegevens uit te kunnen wisselen, is inzage in verschillende kenmerken van de betrokken zorgverlener(s) nodig. Verklaringen over deze kenmerken worden in de vorm van attributen uitgegeven (zie ook hoofdstuk 'Identificatie en authenticatie zorgverlener: Uitgifte van attributen). Het uitgeven van attributen alleen is echter niet voldoende. Attributen dienen op een betrouwbare manier aan een voldoende beveiligd authenticatiemiddel gekoppeld te worden om vervolgens gebruikt te kunnen worden.

Gezamenlijke visie

Doel voor 2026

Voor de authenticatie van zorgverleners wordt gebruikt gemaakt van authenticatiemiddelen die door de zorgverlener zelf kunnen worden gekozen, mits deze aan bepaalde eisen voldoen.

Waarom

Attributen dienen op een betrouwbare manier aan een voldoende beveiligd authenticatiemiddel gekoppeld te worden zodat deze niet door derden gebruikt/misbruikt kunnen worden. Men noemt dit Self Sovereign Identities (SSI). Hierbij kan een persoon een door een uitgever uitgegeven attribuut op een betrouwbare manier koppelen aan een zogenaamde ‘wallet’ zodat de persoon houder van het attribuut wordt. Hiermee geef je personen controle over hun eigen digitale identiteit. In Nederland zijn meer dan een miljoen zorgverleners in allerlei verschillende vormen van zorg actief. Verschillende use cases kunnen verschillende gebruikerseisen aan deze middelen stellen. Het best passende authenticatiemiddel verschilt per zorgverlener en per use case. Soms is dat een app op een smartphone, soms is dat een hardwarematige oplossing zoals een pas of druppel. Om die reden is het belangrijk dat zorgverleners zelf een authenticatiemiddel kunnen kiezen.

Consequenties

Er zijn gezamenlijke standaarden nodig voor de syntax en semantiek van attributen en de uitgifte, presentatie en controle daarvan. Deze standaarden dienen te worden geïmplementeerd door de leveranciers van authenticatiemiddelen. Daarnaast dienen authenticatiemiddelen die worden gebruikt bij het verwerken van medische gegevens te voldoen aan eIDAS-betrouwbaarheidsniveau hoog (bron 1, bron 2, NEN7512). Omdat zorgverleners zelf een authenticatiemiddel moeten kunnen kiezen is er een noodzaak om het uitgeven van attributen los te koppelen van het te gebruiken authenticatiemiddel.

Concretisering

Organisatiebeleid

Zorgaanbieders zullen voor het personeel dat elektronisch gegevens moet gaan uitwisselen authenticatiemiddelen moeten regelen die voldoen aan de eIDAS hoog richtlijn. De Nederlandse eisen voor het stelsel moeten nog door de overheid gepubliceerd worden.

Zorgproces

Voor het zorgproces betekent dit dat zorgaanbieders hun medewerkers moeten voorzien van een eIDAS-hoog authenticatiemiddel waaraan en waarmee de uit te geven (/uitgegeven) attributen gekoppeld en gebruikt kunnen worden. Deze middelen moeten toepasbaar zijn in het zorgproces (wat nu een veelgehoorde probleem met de UZI-pas is). Het idee is dat door de uitgifte van het attribuut en het authenticatiemiddel los te trekken er beter in het zorgproces passende middelen gebruikt kunnen worden. Maar het aanbod van eIDAS hoog gekwalificeerde middelen zal vermoedelijk beperkt zijn en er niet altijd een perfect passend beschikbaar is. Mogelijk moet men daarom ook rekening houden met het anders inrichten van werkprocessen om het gebruiksgemak te optimaliseren.

Informatie

Informatie die mogelijk relevant is is het niveau van het authenticatiemiddel en waarop de attributen zijn uitgegeven. eIDAS kent drie niveaus: laag, midden en hoog.

Applicatie

Applicaties zullen zo ingericht moeten worden dat deze de (verschillende) authenticatiemiddelen kunnen ondersteunen. Hopelijk komt het eIDAS stelsel met een standaard applicatie-koppelvlak zodat ieder middel op dezelfde manier door de applicatie aangeroepen wordt.

IT-infrastructuur

Verschillende authenticatiemiddelen kunnen verschillende eisen hebben aan de benodigde hardware. Denk bijvoorbeeld aan contactloze passen of paslezers. Het aantal authenticatiemiddelen dat voldoet aan eIDAS-betrouwbaarheidsniveau is nog beperkt: Op het moment voldoet alleen de UZI-pas hieraan. De hoop en verwachting is dat in 2022 meer authenticatiemiddelen (zoals IRMA en ZORG-ID SMART) eIDAS-betrouwbaarheidsniveau Hoog gaan ondersteunen. Naast het ondersteunen van eIDAS-betrouwbaarheidsniveau Hoog zullen de verschillende authenticatiemiddelen de standaard voor digitaal ondertekende attributen Verifiable Credentials (VC) moeten implementeren.

Twiin en Nuts stellen voor om in 2022 samen met VZVZ en AET een pilot uit te voeren waarin authenticatie met de UZI-pas wordt ingezet binnen een eOverdracht op basis van Nuts-standaarden. Daarnaast willen Twiin en Nuts samen met VZVZ, CIBG, Actiz en Privacy-by-Design een Proof-of-Concept uitvoeren waarin met behulp van IRMA en Zorg-ID Smart op eIDAS-betrouwbaarheidsniveau Hoog wordt geauthenticeerd.

Deliverables 2022-2026 en afhankelijkheden

Fase	Deliverable	(Nog niet ingevulde) Afhankelijkheden	Betrokkenen
Nu	Authn zorgverlener obv IRMA of UZI	IRMA: Zorgverleners moeten beschikken over smartphone of tablet (ook van toepassing op ZORG-ID SMART)	Actiz, V&VN
		UZI: Zorgverleners moeten momenteel beschikken over UZI-pas, UZI-kaartlezer en apparaat met USB en voor SaaS-XISsen is ook ZORG-ID nodig	Actiz, V&VN, CIBG, VZVZ (bij gebruik van ZORG-ID), ...
2022/23	Pilot/ eerste implementatie UZI & ZORG-ID & Nuts	Duidelijke afspraken ZORG-ID API voor XIS-leveranciers	Nuts, VZVZ, AET (leverancier software ZORG-ID)
2023	Uitspraak dat IRMA voldoet aan eIDAS-hoog	Uitspraak nodig over eIDAS-niveau van IRMA	Privacy by Design, Innovalor, …
2023	Uitspraak dat ZORG-ID SMART voldoet aan eIDAS-hoog	Uitspraak nodig over eIDAS-niveau van ZORG-ID SMART	VZVZ, CIBG
2023	PoC authn. obv wallet (IRMA en ZORG-ID SMART) en obv pas (UZI) - eIDAS hoog	IRMA: Uitgifte van attributen uit UZI-register (zie slide 'uitgifte van attributen')	CIBG, Privacy by Design
2023		ZORG-ID SMART: Uitgifte van attributen vanuit zorgaanbieder (bijv. medewerkersrelatie)	Actiz, VZVZ
2023	**(concept) NEN-normen generieke functies**	**-**	**NEN-werkgroep Generieke Functies**
2023	Kaders authn middelen bekend	NEN-normen bekend	NEN
2024	Authn middelen die voldoen aan gestelde kader zijn beschikbaar	Tijdige oplevering middelen door leveranciers	Leveranciers authenticatiemiddelen
2025	ZV vrijheid zelf kiezen authn middel	internationale standaard voor communicatie tussen wallet en service is bekend	EU

Deliverables 2022/23 en acties

Goal	Strategies	Acties	Wie
Pilot/ eerste implementatie UZI & ZORG-ID & Nuts	Verkrijgen helderheid afspraken ZORG-ID API voor XIS-leveranciers	Huidige situatie ZORG-ID API beschrijven	VZVZ, AET
		Gewenste situatie ZORG-ID API beschrijven	VZVZ, AET, Nuts
		Stappenplan ZORG-ID API beschrijven	VZVZ, AET, Twiin, Nuts
	Invullen randvoorwaarden pilot	Keuze zorgaanbieder(s)/ leverancier(s), regio('s)	?
		Verkrijgen financiering	?
Uitspraak dat IRMA voldoet aan eIDAS-hoog	Beoordelingstraject eIDAS-niveau van IRMA	Uitvoeren beoordeling	Innovalor
		Ondersteunen traject	PbD
		periodiek informeren naar status bij PbD	Twiin, Nuts
Uitspraak dat ZORG-ID SMART voldoet aan eIDAS-hoog	Beoordelingstraject eIDAS-niveau van ZORG-ID SMART	Uitvoeren beoordeling	?
		Ondersteunen traject	VZVZ, AET
		periodiek informeren naar status bij PbD	Twiin, Nuts
PoC authn. obv wallet (IRMA en ZORG-ID SMART) en obv pas (UZI) - eIDAS hoog	IRMA: Uitgifte van attributen uit UZI-register (zie slide 'uitgifte van attributen')	zie vorige slide	
	ZORG-ID SMART: Uitgifte van attributen vanuit zorgaanbieder (bijv. medewerkerrelatie)	Proof of Concept van ZORG-ID SMART opleveren	VZVZ, AET
	Invullen randvoorwaarden PoC	Keuze zorgaanbieder(s)/ leverancier(s), regio('s)	
		Verkrijgen financiering	

5. Aandachtsgebied 3: Autorisatie zorgverlener

Inleiding

Identificatie en authenticatie zorgen ervoor dat de identiteit en andere relevante eigenschappen van zorgverleners in de context van een gegevensuitwisseling kunnen worden vastgesteld. 'Autorisatie zorgverlener' behelst de stap om de beschikbare informatie over een zorgverlener toe te passen bij het bepalen van de juiste mate van toegang tot gegevens. In dit hoofdstuk wordt de autorisatie van de verantwoordelijke/gebruiker besproken. Op andere vlakken kan/moet er ook geautoriseerd worden, zie hoofdstukken Autorisatie Zorgaanbieder en Grondslag.

Gezamenlijke visie

Doel voor 2026

Voor de autorisatie van zorgverleners kan gebruik worden gemaakt van de rol van de zorgverlener. Daarnaast is het een wens van de Patiëntenfederatie om individuele zorgverleners te kunnen autoriseren.

Waarom

Niet alle zorgverleners hebben behoefte aan dezelfde gegevens. Met het oog op dataminimalisatie is het de bedoeling om alléén relevante informatie uit te wisselen. Op basis van verschillende attributen kan bepaald worden of en welke informatie uitgewisseld mag worden. Deze autorisatie-afspraken zouden onderdeel van een zorgtoepassing of informatiestandaard moeten zijn.

Consequenties

Er zijn gezamenlijke standaarden nodig voor de syntax en semantiek van attributen en de presentatie en controle daarvan. De W3C-standaard Verifiable Credentials (VC) biedt hiervoor een goede basis (zie hoofdstukken aangaande identificatie en authenticatie zorgverlener). Daarnaast dienen gezamenlijke afspraak voor de autorisatie per rol (bijv. Medisch Autorisatieprotocol) compleet en machineleesbaar te worden gemaakt.

Om individuele zorgverleners te kunnen autoriseren is een unieke identiteit van de zorgverlener nodig. Daarnaast dienen autorisaties van individuele zorgverleners te worden ondersteund voor de verschillende bronsystemen en/of gespecialiseerde toestemmingsvoorzieningen.

Concretisering

Organisatiebeleid

Als onderdeel van een zorgtoepassing of zorginformatiestandaard zullen er afspraken gemaakt moeten worden over de autorisatie: wie mag wat doen (en in welke situatie). Dit

zouden landelijke afspraken moeten zijn, maar op regionaal niveau zullen er wensen zijn om hiervan af te wijken. Indien niet anders afgesproken zijn het de bronhouders van de informatie die verantwoordelijk zijn voor de autorisatie.

Zorgproces

Het doel is dat de bronhouder bij een gegevensverzoek de (externe) zorgverlener kan autoriseren op basis in de uitwisseling meegeven attributen. Dit zal met name nodig zijn in processen waar een hoger risiconiveau geldt, zoals bij het beschikbaar stellen van informatie voor later, nog onbekend gebruik en bijvoorbeeld in bij het uitwisselen van medicatievoorschriften waar het nodig is om de voorschrijver te kunnen controleren op zijn/haar bevoegdheid.

Informatie

De attributen dienen digitaal ondertekend te zijn. Attributen die benodigd zijn voor autorisatie, zijn (o.a.)

- de kwalificatie van de persoon
- de medewerkersrelatie van de persoon met de zorgaanbieder van waaruit het gegevensverzoek wordt verzonden
- de rol van de persoon bij de zorgaanbieder van waaruit het gegevensverzoek wordt verzonden.Correcte informatie over de rol van een zorgverlener geeft informatie over welke gegevens relevant kunnen zijn. Om die reden is de rol van de zorgverlener een gewenste parameter voor autorisatie.

De rol van de zorgverlener kent twee varianten:

1. De algemene rol, ook wel de kwalificaties, van de zorgverlener. De algemene rol van de zorgverlener is afhankelijk van de kennis en kunde van de zorgverlener, welke bijvoorbeeld kan worden afgeleid uit bepaalde diploma's en andere certificeringen. Registers zoals het UZI-register en het BIG-register kunnen hiervoor als bron dienen.
2. De zorgaanbieder-specifieke rol van de zorgverlener. De zorgaanbieder-specifieke rol van de zorgverlener is de rol die een zorgverlener bij een bepaalde zorgaanbieder uitvoert. Om te kunnen autoriseren op deze rol dient een bronhouder naast de zorgaanbieder-specifieke rol ook een betrouwbare verklaring over de relatie tussen de zorgverlener en de afnemende zorgaanbieder te ontvangen.

In verschillende gevallen kan het wenselijk zijn dat individuele zorgverleners kunnen worden geautoriseerd. Dit geldt bijvoorbeeld voor negatieve autorisaties: Bijvoorbeeld wanneer een cliënt een negatieve ervaring heeft gehad met een specifieke zorgverlener wil de cliënt wellicht de toegang tot haar/zijn dossier voor deze zorgverlener blokkeren. Ook wanneer sprake is van een sociale relatie tussen cliënt en zorgverlener kan het gewenst zijn inzage in het dossier te beperken.

Applicatie

Zorgaanbieders die data willen afnemen zullen deze attributen bij het versturen van gegevensverzoeken conform de standaard Verifiable Credentials (VC) moeten meegeven zodat deze cryptografisch kunnen worden geverifieerd. Deze standaard zal moeten worden ingebouwd in afnemende systemen (bijv. viewers en XIS’en) en controlerende systemen.

Zorgaanbieders die data aanbieden zullen bij het ontvangen van elektronische verzoeken in veel gevallen willen autoriseren op basis van de meegestuurde attributen. De standaard Verifiable Credentials (VC) zal moeten worden ingebouwd in de systemen van bronhouders (bijv. autorisatieserver).

IT-infrastructuur

Autorisatie kan op verschillende wijzen ingericht worden. In principe zijn de bronhouders van informatie verantwoordelijk voor het autoriseren van gebruikers die toegang tot de gegevens willen. Maar men zou ook (voor bepaalde situaties) kunnen kiezen om een centrale autorisatiefunctie af te nemen.

Deliverables 2022-2026 en afhankelijkheden

Fase	Deliverable	(Nog niet ingevulde) Afhankelijkheden	Betrokkenen
Nu	geen autorisatie op ZV rol	geen	geen
2022	autorisatie op medewerker-relatie (obv context)	Medewerkersrelatie tussen zorgverlener en zorgaanbieder is correct ingericht in XIS	Actiz
2022	autorisatie op medewerker-relatie (obv context)	Manier nodig om correctheid medewerkersrelatie bij afnemer te vertrouwen: NEN 7510-certificering	Actiz
		Manier nodig om correctheid medewerkersrelatie bij afnemer te vertrouwen: ZORG-ID SMART	Actiz, VZVZ
2022	PoC autorisatie op rol (icm PoC UZI-IRMA-ZORG ID SMART)	Use case rollen kunnen worden uitgegeven door zorgaanbieder (m.b.v. ZORG-ID SMART)	VZVZ, Actiz
2023	**(concept) NEN-normen generieke functies**	**-**	**NEN-werkgroep Generieke Functies**
2023	autorisatie op ZV rol	NEN-normen beschikbaar	
		Standaarden voor invulling van NEN-normen beschikbaar	Twiin, Nuts, TSV

2023	autorisatie op ind. ZV	Identiteit zorgverlener beschikbaar op moment van geven toestemming (register).	CIBG, Actiz, V&VN
2025	autorisatie op ZV-rol & individuele ZV binnen context ZA	geen, resultaat van bovenstaande	geen

Deliverables 2022/23 en acties

Goal	Strategies	Acties	Wie
autorisatie op medewerker-relatie (obv context)	Medewerkerrelatie tussen zorgverlener en zorgaanbieder is correct ingericht in XIS	Voorlichten zorgaanbieders over belang goede inrichting medewerkerrelatie. Beschikbaar in XIS.	Actiz
		Beschrijven en implementeren processen rondom mutatie medewerkers (bijv. in en uit dienst)	Actiz
		Betrekken EPD-leveranciers	TSV
	Manier nodig om correctheid medewerkerrelatie bij afnemer te vertrouwen: NEN7510-certificering	Aanspreken zorgaanbieders op verplichting voldoen aan NEN7510	Actiz
		NEN7510 certificering per zorgaanbieder uitvoeren (inclusief medewerkerrelatie)	Actiz
	Manier nodig om correctheid medewerkerrelatie bij afnemer te vertrouwen: ZORG-ID SMART (en/of IRMA)	Analyse geschiktheid ZORG-ID SMART en/of IRMA	Twiin, Nuts, TSV?
PoC autorisatie op rol (icm PoC UZI-IRMA-ZORG ID SMART)	Use case rollen kunnen worden uitgegeven door zorgaanbieder (bijv.	PoC uitvoeren (zie Identificatie en authenticatie zorgverlener)	VZVZ, Twiin, Nuts

	m.b.v. ZORG-ID SMART)		

6. Aandachtsgebied 4: Identificatie en authenticatie zorgaanbieder (en leverancier)

Inleiding

Om veilig en verantwoord gegevens uit te kunnen wisselen, is inzage in verschillende kenmerken van de betrokken zorgaanbieder(s) nodig. Bij gegevensuitwisseling zijn onder andere de volgende vragen relevant:

- Welke zorgaanbieder wil informatie afnemen of aanbieden?
- Welke rol(len) heeft de zorgaanbieder die informatie wil afnemen of aanbieden?
- Welke leveranciers treden als verwerker op voor de zorgaanbieder die informatie wil afnemen?

Dit soort kenmerken wordt attributen genoemd. Verschillende attributen kunnen verschillende bronregisters hebben.

Gezamenlijke visie

Doel voor 2026

Voor de authenticatie van zorgaanbieders wordt gebruikt gemaakt van digitaal ondertekende attributen die door een beperkt aantal vertrouwde instanties worden uitgegeven. Zorgaanbieders hebben de beschikking over een eigen wallet waarmee ze attributen kunnen ophalen, beheren en presenteren.

Waarom

Voor veilige gegevensuitwisseling tussen twee zorgaanbieders is een gezamenlijk beeld van de identiteit en andere voor gegevensuitwisseling relevante kenmerken van de betrokken zorgaanbieders nodig. Dit noemen we zorgaanbieder-overstijgende authenticatie. In Nederland zijn ongeveer 140.000 verschillende zorgaanbieders actief. Door het grote aantal zorgaanbieders is een vertrouwensmodel gebaseerd op 1-op-1 organisatorische afspraken tussen individuele zorgaanbieders (peer-to-peer trust) slecht schaalbaar.

Consequenties

Er zijn gezamenlijke standaarden nodig voor de syntax en semantiek van attributen en de uitgifte, presentatie en controle daarvan. Deze standaarden dienen te worden geïmplementeerd door de eigenaren van de benodigde bronregisters die daarmee de rol van uitgever krijgen. Deze standaarden dienen ook te worden geïmplementeerd door zorgaanbieders die data willen aanbieden of afnemen.

Concretisering

Organisatiebeleid

Technologie helpt om op een betrouwbare, onweerlegbare afspraken af te dwingen en te faciliteren. Om die reden is een uitgever van verklaringen over zorgaanbieders nodig die door alle zorgaanbieders wordt vertrouwd: een *Bevoegde uitgever van verklaringen* (DIZRA-definitie). Een *Bevoegde uitgever van verklaringen* (vanaf hier: uitgever) geeft verklaringen over kenmerken van zorgaanbieders uit in de vorm van attributen. Landelijke en zorgbreed moet afgesproken worden dat zorgaanbieders zich authenticeren met middelen en daaraan gekoppelde attributen uitgegeven door de bevoegde uitgevers. Het niveau van betrouwbaarheid van het uitgifteproces i.c.m. de betrouwbaarheid van het authenticatiemiddel bepaalt de betrouwbaarheid van het attribuut.

Zorgproces

Zorgaanbieders dienen processen in te richten waarmee attributen beheerd, uitgegeven en gecontroleerd kunnen worden. Nu zijn attributen hard gekoppeld aan het authenticatiemiddel, zoals een UZI- of PKI-servercertificaat. In de voorgestelde situatie wordt dit losgekoppeld en kunnen attributen van meerdere uitgevers (zoals KvK, UZI-register, LRZA, Vecozo) aan de identiteit van de zorgaanbieder gekoppeld worden. Deze attributen dienen in een zogenaamde wallet beheerd te worden.

Voor IT-leveranciers zal dit ook gaan gelden. Bij een gegevensuitwisseling wil een bronhoudende zorgaanbieder van een afnemende partij kunnen vaststellen dat deze opereert als gegevensverwerker van de beoogde afnemende zorgaanbieder. Daarnaast willen zorgaanbieders van leveranciers kunnen vaststellen dat deze gegevens op een juiste technische manier verwerken. Een partij als Nictiz geeft kwalificaties af waarmee kan worden aangetoond dat een stuk software een informatiestandaard correct heeft geïmplementeerd. Vanuit de Wegiz zal worden geëist dat applicaties aan bepaalde normeringen voldoen. Als laatste zou de beheerder van een uitwisselingsinfrastructuur of een afsprakenstelsel ook willen controleren of de deelnemende applicaties correct opereren. De leveranciers en de applicaties die zij aan zorgaanbieders leveren, dienen daarom herkenbaar te zijn. Aan leveranciers kan een ‘deelnemer’ attribuut uitgereikt worden en aan applicaties kunnen verschillende kwalificatie-attributen worden gekoppeld.

Informatie

Attributen ter identificatie van zorgaanbieders dienen uitgegeven te worden door vertrouwde instanties. Het gaat om de volgende attributen:

- een unieke identificatie van een zorgaanbieder (bijv. URA-nummer zoals door het IB is vastgesteld)
- een waarborg dat de organisatie een zorgaanbieder is / mag zijn
- een unieke identificatie van de leverancier / de gebruikte (gecertificeerde) software
- een waarborg dat de zorgaanbieder een contract heeft met de betreffende softwareleverancier

Daarnaast kan een attribuut dat de typering(en) van de zorginstelling aangeeft nuttig zijn voor m.n. autorisatiedoeleinden. In Mitz en ZORG-AB bijvoorbeeld wordt de typering van

Zorgkaart Nederland gebruikt. De vraag is of dit voldoende is. Als laatste zou een zorgaanbieder nog een attribuut kunnen krijgen waaruit blijkt dat deze deelneemt aan de uitwisselingsinfrastructuur en/of voldoet aan het gebruikte afsprakenstelsel.

Applicatie

Deze attributen dienen digitaal ondertekend te zijn zodat de herkomst en juistheid eenvoudig kunnen worden gecontroleerd. Omdat verschillende attributen verschillende bronregisters hebben en data zo veel mogelijk bij de bron dienen te blijven, is er niet sprake van één maar van meerdere uitgevers.

Applicaties van bevoegde uitgevers zullen zo ingericht moeten worden dat deze op basis van de afgesproken standaarden en technieken de attributen kunnen uitgeven. Vervolgens zullen deze gekoppeld moeten worden aan een digitale identiteit en ‘wallet’.

Voor applicaties die personen moeten authenticeren zal gelden dat deze ingericht moeten worden dat dit gedaan kan worden op basis van de afgesproken standaarden en technieken en koppelingen kunnen maken met de vertrouwde uitgever(s).

De attributen dienen in de vorm van Verifiable Credentials (VC) uitgegeven te worden. In 2022 willen Twin en Nuts een Proof-of-Concept van attribuutgebaseerde autorisatie van zorgaanbieders realiseren met bronregisters LRZa en ZORG-AB als uitgevers. Het uitgifteproces zal waarschijnlijk moeten voldoen aan bestaande eisen uit het eIDAS-stelsel.

IT-infrastructuur

Er zal een gedeelde IT-infrastructuur moeten zijn waarmee partijen identiteiten, daaraan gekoppelde attributen en af te leiden claims kunnen controleren. Deze infrastructuur zal een (zeer) hoge mate van beschikbaarheid moeten kennen.

Deliverables 2022-2026 en afhankelijkheden

Fase	**Deliverable**	**(Nog niet ingevulde) Afhankelijkheden**	**Betrokkenen**
Nu	authn ZA via Nuts register	Aanmelding in Nuts-register	TSV
2022	PoC authn ZA via TTP (ZORG-AB, LRZA, …)	Uitgifte van ZA-attributen door TTP	VZVZ, CIBG, TSV
2022	Kaders uitgifte ZA-attr. bekend (incl. ZA-rol)	Inzage welke attributen gewenst zijn	Actiz, VZVZ, Nuts, Twiin
		Uitgifteproces (b2b) bekend	VZVZ, CIBG, TSV
2023	**(concept) NEN-normen generieke functies**	**-**	**NEN-werkgroep Generieke Functies**

2023	keuze Uitgever(s) authn ZA	volgt uit bovenstaande	
2024	Uitgever authn ZA attributen digitaal ondertekend		TSV, XIS-leveranciers
2025	ZA hebben eigen wallet		TSV, XIS-leveranciers

Deliverables 2022/23 en acties

Goal	**Strategies**	**Acties**	**Wie**
authn ZA via Nuts register	Verkennen mogelijkheden gebruik identifiers		
PoC authn ZA via TTP (ZORG-AB, LRZA, …)	Uitgifte van ZA-attributen door TTP	Wens kenbaar maken aan VZVZ en CIBG	Twiin, Nuts
		Implementatie VC's door VZVZ en CIBG	VZVZ, CIBG
	Invullen randvoorwaarden PoC	Keuze zorgaanbieder(s)/ leverancier(s), regio('s)	Twiin, Nuts
		Verkrijgen financiering	Twiin, Nuts
		Uitvoeren PoC	Twiin, Nuts
		Rapportage PoC	Twiin, Nuts
Kaders uitgifte ZA-attr. bekend (incl. ZA-rol)	Inzage welke attributen gewenst zijn	Voorstel schrijven	Twiin, Nuts
		Voorstel ter review aanbieden aan VZVZ, CIBG	Twiin, Nuts,
	Uitgifteproces (b2b) bekend	Voorstel schrijven	Twiin, Nuts
		Bespreken voorstel met uitgevers	Twiin, Nuts
		Voorbereiden officiële opdracht aan uitgevers	Twiin, Nuts

7. Aandachtsgebied 5: Autorisatie zorgaanbieder

Inleiding

Autorisatie bepaalt of een afnemende partij informatie mag verwerken op basis van zijn rol in het zorgproces. Hierbij moet de te verwerken informatie proportioneel zijn. Dat betekent dat de inhoud en omvang van de informatie moet passen bij het doel waarvoor en de context waarin de afnemende partij de informatie wil gebruiken. Ook dienen er voldoende waarborgen geïmplementeerd te zijn om de gegevens veilig te kunnen verwerken. 'Autorisatie zorgaanbieder' behelst de stap om de beschikbare informatie over een zorgaanbieder toe te passen bij het bepalen van de juiste mate van toegang tot gegevens.

Gezamenlijke visie

Doel voor 2026

De autorisatie van zorgaanbieders wordt gedaan op basis van digitaal ondertekende attributen en digitaal ondertekende autorisaties.

Waarom

Zorgaanbieders dienen met grote zekerheid vast te kunnen stellen of het veilig en/of toegestaan is om met bepaalde andere partijen te communiceren. Verschillende niveaus van autorisatie kunnen worden toegepast:

- is de afnemende partij een zorgaanbieder en mag deze dus medische gegevens verwerken?
- zijn de aanbiedende en afnemende partijen een deelnemer aan het afsprakenstelsel en kan er vanuit worden gegaan dat deze voldoen aan de gezamenlijk afgesproken eisen en richtlijnen?
- opereert de afnemende leverancier/software namens de beoogde afnemende zorgaanbieder?
- voldoet de gebruikte software aan de kwaliteitsrichtlijnen die gelden voor de betreffende uitwisseling?
- is er een geldige grondslag op basis waarvan de bronhoudende zorgaanbieder gegevens aan de afnemende zorgaanbieder beschikbaar mag stellen?

Consequenties

Afnemende zorgaanbieders moeten de benodigde attributen en autorisaties kunnen overleggen aan bronhoudende zorgaanbieders. Op hun beurt kunnen die dan controleren of en waarover het toegestaan is te communiceren.

Concretisering

Organisatiebeleid

Partijen die kwalificaties uit gaan geven, zoals Nictiz, mogelijk de NEN en beheerders van afsprakenstelsels zullen dit niet alleen meer administratief moeten doen, maar ook in de vorm van digitaal ondertekende attributen die door andere partijen in het netwerk kunnen worden gepresenteerd en gecontroleerd. De attributen en autorisaties dienen conform de W3C-standaard Verifiable Credentials (VC) te worden uitgegeven, gepresenteerd en gecontroleerd. Het uitgeven, presenteren en controleren van kwalificaties moet eenvoudiger en sneller te regelen zijn waarbij de administratieve lasten afnemen. Hiervoor dienen bovenstaande partijen en eventuele andere stakeholders hierover duidelijke afspraken te maken.

Daarnaast kunnen attributen van een organisatie, zoals het type, gebruikt worden in autorisaties. Dit wordt nu al gedaan in toestemmingsprofielen van Mitz, maar dit zou bijvoorbeeld ook in autorisatieregels voor zorgtoepassingen gedaan worden.

Zorgproces

Het doel is dat de bronhouder bij een gegevensverzoek de andere zorgaanbieder kan autoriseren op basis van in de uitwisseling meegegeven attributen. Deze attributen zouden door verschillende partijen uitgegeven moeten worden en worden beheerd in de ‘wallet’ van zorgaanbieder en/of IT-leverancier/software.

Informatie

Op verschillende punten zou een zorgaanbieder geautoriseerd kunnen worden:

1. Autorisatie op basis van het zijn van een deelnemer aan de uitwisselingsinfrastructuur en/of het gebruikte afsprakenstelsel. De beheerder hiervan een ‘toegangsbewijs’ als attribuut aan de zorgaanbieder afgeven waarmee men op het netwerk toe kan treden.
2. Autorisatie op typering. In Mitz kan expliciete toestemming worden gegeven op type zorgaanbieder.
    a. Typering van bronhoudende zorgaanbieders. Er kan bijvoorbeeld een toestemming worden gegeven waarmee alle apotheken (die een geneeskundige behandelingsovereenkomst (gehad) hebben) medicatiegegevens beschikbaar mogen stellen aan bepaalde afnemers.
    b. Typering van afnemende zorgaanbieders. Het valt voor te stellen dat bepaalde gegevens alleen met bepaalde type zorgaanbieders gedeeld mogen worden. Omdat dat is afgesproken in de informatiestandaard of omdat de patiënt/cliënt dat zo wil. Er kan bijvoorbeeld een toestemming worden gegeven waarmee een bepaalde bronhouder medicatiegegevens beschikbaar mag stellen aan alle apotheken (die een geneeskundige behandelingsovereenkomst (gehad) hebben).
3. Autorisatie op basis van de gebruikte XIS-software (kwalificatie). Niet alle software zal alle medische gegevens (op een correcte manier) kunnen verwerken, maar vaak slechts een beperkt aantal zorgtoepassingen ondersteunen. Welke zorgtoepassingen dit zijn wordt bijvoorbeeld bepaald door de type-kwalificatie die Nictiz afgeeft. Ook loopt er een wetgevend traject om bepaalde zorgtoepassingen te gaan normeren.

Er zijn gezamenlijke standaarden nodig voor de syntax en semantiek van attributen en de uitgifte, presentatie en controle daarvan.

Applicatie

Deze standaarden dienen te worden geïmplementeerd door de eigenaren van de benodigde bronregisters en de zorgaanbieders die data willen aanbieden of afnemen.

IT-infrastructuur

Er zal een gedeelde IT-infrastructuur moeten zijn waarmee partijen identiteiten, daaraan gekoppelde attributen en af te leiden claims kunnen controleren. Claims en/of attributen kunnen namelijk ook weer ingetrokken worden.Deze infrastructuur zal een (zeer) hoge mate van beschikbaarheid moeten kennen.

Deliverables 2022-2026 en afhankelijkheden

Fase	**Deliverable**	**(Nog niet ingevulde) Afhankelijkheden**	**Betrokkenen**
Nu	bronhouder maakt autorisatie aan obv impliciete toestemming	koppeling met nuts-node	TSV
Nu	geen authz op ZA rol	geen	
Nu	Autoriseren op ZA-leverancier relatie in Nuts-register	geen	
2023	Autoriseren op ZA-leverancier relatie in het algemeen	Bevoegde uitgever van ZA-leverancier relaties	
2023	Autoriseren op kwalificaties leverancier	Bevoegde uitgever van kwalificaties	
eind 2023	**(concept) NEN-normen generieke functies**	**-**	**NEN-werkgroep Generieke Functies**
2024-2025	mogelijkheid authz op ZA-rol	Bevoegde uitgever van ZA-rol	
2026	autorisatie obv kenmerken afnemer en diens leverancier		

Deliverables 2022/23 en acties

Goal	Strategies	Acties	Wie
Autoriseren op ZA-leverancier relatie in het algemeen	Bepalen bevoegde uitgever ZA-leverancier relatie	Bepalen of zorgaanbieder zelf deze rol kan vervullen	Twiin, Nuts
		Andere mogelijkheden onderzoeken	Twiin, Nuts
	Uitgever, bronhouder en afnemer implementeren standaard Verifiable Credentials	Schrijven opdracht (use cases, business case, programma van eisen, functioneel ontwerp) aan leveranciers	Twiin, Nuts, VZVZ
		Uitgevers en Zorgaanbieder geven leveranciers opdracht	Zorgaanbieder, uitgevers
Autoriseren op kwalificaties leverancier	Bepalen bevoegde uitgever leverancier-kwalificaties	Bepalen wie (Nictiz, VZVZ, …) deze rol kan vervullen	Twiin, Nuts, Nictiz, NEN, VZVZ
	Uitgever, bronhouder en afnemer implementeren standaard Verifiable Credentials	Schrijven opdracht (use cases, business case, programma van eisen, functioneel ontwerp) aan leveranciers	Twiin, Nuts, VZVZ
		Uitgevers en Zorgaanbieder geven leveranciers opdracht	Zorgaanbieder, uitgevers

8. Aandachtsgebied 6: Grondslagen - vastleggen en toetsen

Inleiding

Grondslagen beschrijven de juridische basis en de voorwaarden waaraan moet worden voldaan om op basis van deze grondslag(en) binnen een bepaalde (medische) context gegevens uit te kunnen wisselen. Allereerst gaat het om de vraag of er een uitzondering of een doorbrekingsgrond is voor het beroepsgeheim. Vervolgens is de vraag of er een AVG grondslag is.

Gegevens uit het dossier mogen gedeeld worden met anderen die betrokken zijn bij de uitvoering van dezelfde geneeskundige behandelingsovereenkomst. Hiervoor geldt een uitzondering op het beroepsgeheim. Het gaat bijvoorbeeld om waarnemers, vervangers en ook om collegiale raadpleging. Gegevens mogen echter alleen gedeeld worden voor zover dat noodzakelijk is in het kader van die behandelrelatie. In andere gevallen is nodig dat het beroepsgeheim doorbroken mag worden. In beginsel mag dat alleen op basis van uitdrukkelijke toestemming. In het kader van een verwijzing en een terugkoppeling, is er ook ruimte voor veronderstelde toestemming mits de patiënt geïnformeerd is en bezwaar heeft kunnen maken.

Daarnaast is ook nodig dat er een AVG grondslag is voor de verwerking van gevoelige gegevens, namelijk gegevens over gezondheid. AVG onderscheid zes grondslagen voor de verwerking van persoonsgegevens. De grondslagen 'toestemming' en 'uitvoeren overeenkomst' worden binnen de gezondheidszorg het meest toegepast.

Gezamenlijke visie

Doel voor 2026

Zorgaanbieders ondersteunen alle relevante grondslagen voor gegevensverwerking in de zorg op een cryptografisch verifieerbare manier. Voor het beheren en raadplegen van toestemmingen wordt o.a. gebruikt gemaakt van toestemmingsvoorzieningen die door de burger zelf kunnen worden gekozen, mits deze aan bepaalde eisen voldoen.

Waarom

Zorgaanbieders moeten allereerst vast kunnen stellen welke grondslagen van toepassing zijn op de uitwisseling. Afhankelijk van het type uitwisseling zou het kunnen dat er andere grondslagen gelden en daarom andere controles moeten worden uitgevoerd waaruit blijkt of de afnemende partij geautoriseerd is om gegevens van de betreffende burger te verwerken.

Grondslagen kunnen op verschillende manieren worden geregistreerd zodat deze door de communicatiepartners cryptografisch verifieerbaar zijn. Burgers willen op een gemakkelijke manier toestemmingen kunnen geven en beheren.

Het is relevant om helder te kunnen toetsen of systemen onder de grondslag 'toestemming' kunnen (moeten) werken en wat daarvoor de randvoorwaarden zijn. Daarnaast is relevant om helder te kunnen toetsen of en hoe een uitwisseling van gegevens onder een andere grondslag kan verlopen en wat daarvoor de eisen zijn.

Daarnaast moeten burgers ook zelf een toestemmingsmiddel kunnen kiezen, dat bijvoorbeeld aansluit bij de persoonlijke gezondheidsomgeving. Daarnaast zullen burgers in bepaalde gevallen iemand anders willen machtigen voor het vastleggen en beheren van toestemmingen.

Consequenties

Er dient daarom zo veel mogelijk gebruik te worden gemaakt van gezamenlijke standaarden die het mogelijk maken dat grondslagen verifieerbaar zijn en los staan van de uit te wisselen gegevens. Omdat de grondslagen in verschillende systemen vastgelegd, beheerd en gecontroleerd kunnen worden is het van belang dat de grondslagen digitaal ondertekend en verifieerbaar zijn. Een bronhouder die een gegevensverzoek vergezeld van een grondslag ontvangt kan dan bijvoorbeeld zeker weten dat de cliënt/patiënt degene is die de toestemming (of andere grondslag) heeft geregistreerd.

Concretisering

Er zijn gezamenlijke standaarden nodig voor de syntax en semantiek van grondslagen en de uitgifte, presentatie en controle daarvan. Grondslagen dienen conform de W3C-standaard Verifiable Credentials (VC) te worden uitgegeven, gepresenteerd en gecontroleerd. Toestemmingsvoorzieningen zoals Mitz zullen de standaard Verifiable Credentials moeten implementeren en toestemmingen conform deze standaard beschikbaar moeten kunnen stellen. Daarnaast dient deze standaard te worden geïmplementeerd in de systemen van bronhoudende en afnemende zorgaanbieders.

Organisatiebeleid

De burger kan ervoor kiezen om een centrale toestemmingsvoorziening als Mitz te gebruiken. Er zullen ook zorgaanbieders zijn die toestemmingen lokaal willen beheren. Verschillen in keuzes maken het voor de burger lastig om een overzicht te krijgen van alle toestemmingen en het leidt er mogelijk ook toe dat zorgaanbieders van op meerdere toestemmingsregistraties zouden moeten aansluiten.

Wanneer er niet voor één systeem, zoals Mitz, wordt gekozen dient er een stelsel te komen waarmee burgers op een plek naar keuze al hun toestemmingen kunnen beheren en het voor brondossierhouders duidelijk is waar dat is.

Zorgproces

Informatie

De volgende grondslagen zijn geïdentificeerd:

- Uitzondering beroepsgeheim o.b.v. behandelrelatie (WGBO)
    - Deze grondslag sluit aan bij de AVG-grondslag 'uitvoeren overeenkomst' omdat de gegevensdeling plaatsvindt in het kader van een behandelovereenkomst
- Veronderstelde toestemming (Wgbo)
    - Deze grondslag geldt o.a. bij overdracht en verwijzing.
    - Deze grondslag sluit aan bij de AVG-grondslag ‘toestemming’
- Expliciete specifieke toestemming (Wgbo)
    - Deze grondslag is van toepassing wanneer de betrokken cliënt/patiënt een expliciete toestemming heeft gegeven voor gegevensdeling tussen een specifieke bronhoudende zorgaanbieder en een specifieke afnemende zorgaanbieder. Van belang hierbij is dat de brondossierhouder de partij die verplicht is om te borgen dat deze toestemming is gegeven. Daarvoor is ook nodig dat deze kan nagaan of de patiënt weet om welke gegevens het gaat en voor welk doel. De vraag is dan ook of het zal voorkomen dat deze toestemming gedeeld moet worden tussen zorgaanbieders.
    - Deze grondslag sluit voor de zorgaanbieder die gegevens deelt vanuit zijn brondossier aan bij de AVG-grondslag 'toestemming' omdat de gegevensdeling plaatsvindt nadat de cliënt expliciet toestemming heeft gegeven voor een specifieke verwerking van gegevens met een specifiek doel.
- Uitdrukkelijke toestemming (Wabvpz)
    - Deze grondslag is van toepassing wanneer de betrokken cliënt/patiënt uitdrukkelijke toestemming heeft gegeven voor het vooraf beschikbaar stellen van gegevens voor nog onbekend later gebruik.
    - Deze grondslag sluit aan bij de AVG-grondslag 'uitdrukkelijke toestemming', waarbij een knelpunt is of de toestemming voldoende specifiek is uitgevraagd.
    - De raadpleging vindt niet plaats op basis van deze uitdrukkelijke toestemming. Daarvoor is vereist dat sprake is van een behandelovereenkomst tussen de raadplegende zorgaanbieder en de cliënt/patiënt. Op deze manier sluit deze werkwijze aan bij de AVG-grondslag 'uitvoeren overeenkomst'.

Applicatie

Verschillende typen grondslagen kunnen verschillende uitgevers, houders en controleurs hebben waarvoor de grondslag betrouwbaar moet zijn. Zo zal een uitdrukkelijke toestemming voor opvragen door een burger uitgegeven worden, is een impliciete toestemming (zoals bij een verwijzing) een claim van een zorgaanbieder zelf.

De houder van een grondslag kan ook per situatie verschillen. Toestemmingen worden nu (bij wet) door de brondossierhouder beheerd (lokaal, of in een toestemmingsvoorziening als Mitz), maar er gaan ook stemmen op om toestemmingen in een PGO te gaan beheren. Betrouwbaarheid van de claim wordt dan nog belangrijker.

Applicaties moeten de verschillende grondslagen cryptografisch kunnen controleren. Applicaties van uitgevers moeten de grondslagen cryptografisch verifieerbaar kunnen vastleggen.

IT-infrastructuur

Er zal een gedeelde IT-infrastructuur moeten zijn waarmee partijen de grondslagen kunnen controleren. Deze kunnen namelijk ook weer ingetrokken of anderzijds ongeldig worden. Deze infrastructuur zal een (zeer) hoge mate van beschikbaarheid moeten kennen.

Deliverables 2022-2026 en afhankelijkheden

Fase	Deliverable	(Nog niet ingevulde) Afhankelijkheden	Betrokkenen
Nu	vastleggen in bronsysteem bronhouder	feitelijk geen, wel verstandig om hierover afspraken te maken	Actiz, Twiin, Nuts, TSV
2022-2023	vastleggen in landelijk toestemmingen- register (Mitz)	Aanpassen Wabvpz (MinVWS)	MinVWS
		Inproductiename	VZVZ
	toestemming versturen van beoogd afnemer en/of zorgcoördinator naar bronhouder (autorisatieverzoek)	Schrijven en beproeven standaard autorisatieverzoek	Nuts
2023	PoC Mitz-toestemming en Bronhouder met Nuts-node	Authn: Mitz kan autorisatie met waarborg toestemming uitgeven	VZVZ, Twiin, Nuts
		Uitbreiden functionaliteit Nuts-node voor acceptatie 'externe' autorisaties	Nuts, Twiin
eind 2023	**(concept) NEN-normen generieke functies**	**-**	**NEN-werkgroep Generieke Functies**
2024-2035	mogelijkheid vastleggen in cliëntomgeving	Oplossing voor identificatie burgers zonder gebruik bsn	Twiin, Nuts, MedMij
2026	vrije keuze client toestemmings- middel	volgt uit bovenstaande	

Deliverables 2022/23 en acties

Goal	Strategies	Acties	Wie
vastleggen in landelijk toestemmingen- register (Mitz)	Aanpassen Wabvpz (MinVWS)	Aanpassen Wabvpz	MinVWS
	Inproductiename	Technisch live	VZVZ
		In gebruik	VZVZ
PoC Mitz-toestemming en Bronhouder met Nuts-node in 2023	Functioneel Ontwerp	Gezamenlijke proces-workshop	VZVZ, Twiin, Nuts
	Technisch Ontwerp (2023)		VZVZ, Twiin, Nuts

9. Aandachtsgebied 7: Datalokalisatie

Inleiding

Datalokalisatie betreft het lokaliseren van informatie over een specifieke cliënt/patiënt. De bekendste manier om dit te doen is door het publiceren van metadata die informatie bevat over waar informatie van een patiënt is. Het betreft geen inhoudelijke zorginformatie of informatie over of deze patiënteninformatie ingezien mag worden door de zorgaanbieder of patiënt, maar enkel over de plek waar de informatie van een patiënt staat. Correcte datalokalisatie voorkomt overbevraging. Immers, indien niet bekend is waar informatie van een patiënt zich bevindt, zouden een patiënt of een zorgaanbieder (en de gebruikte applicaties) in theorie alle bronhoudende zorgaanbieders langs moeten gaan om te vragen of van de patiënt in kwestie (relevante) informatie aanwezig is. Overbevraging is vanuit een technisch en juridisch perspectief (AVG-uitgangspunt 'minimale gegevensverwerking') onwenselijk omdat een groot aantal vragen wordt gesteld/verspreid waarbij slechts een kleine fractie een positief antwoord oplevert. Daarnaast wordt door het stellen van deze vraag ongewenst informatie gedeeld dat een persoon bij een bepaalde zorgaanbieder in zorg is.

Datalokalisatie vindt nu plaats op verschillende manieren:

- Binnen het LSP kan verschillende soorten informatie via de verwijsindex (integratie van lokalisatie en toestemming) worden gelokaliseerd.
- Binnen XDS-netwerken kan informatie via XDS-registers worden gelokaliseerd en tussen verschillende XDS-netwerken kunnen ook lokalisatievragen worden uitgewisseld.
- In het geval van een overdracht of verwijzing kan informatie worden gelokaliseerd doordat de bronhoudende zorgaanbieder een afnemende zorgaanbieder expliciet informeert.
- Binnen netwerken die gebruik maken van Nuts-standaarden kan informatie worden gelokaliseerd op basis van autorisaties die aanwezig zijn in de systemen van de afnemende zorgaanbieder.

Gezamenlijke visie

Doel voor 2026

Zorgaanbieders kunnen omgaan met verschillende gestandaardiseerde manieren voor datalokalisatie.

Waarom

Wanneer er (veel) verschillende indexen zijn leidt dit mogelijk tot zoektochten naar informatie en daarmee toch weer overbevraging. Het niet hebben van relevante informatie kan leiden tot het opnieuw uitvoeren van medisch onderzoek. Dit is een extra belasting voor de patiënt en zorgverlener en levert uiteraard dubbele kosten op. Datalokalisatie is dus essentieel. Er

worden in de huidige situatie al verschillende manieren van datalokalisatie gebruikt die bewezen goed werken.

Consequenties

De huidige verschillende manieren van datalokalisatie dienen te worden gestandaardiseerd.

Om te voorkomen dat een zorgaanbieder verschillende online indices allemaal moet bijhouden/raadplegen, zien we grofweg twee oplossingsrichtingen:

- Eén register waarin behandelingsovereenkomsten worden bijgehouden. Zorgaanbieders die informatie zoeken over een bepaalde patiënt kunnen dan hierin vinden waar deze patiënt eerder behandeld is en vervolgens deze bronnen bevragen (bijv. Mitz). Dit register is alleen te bevragen na toestemming patiënt.
- Een afsprakenstelsel dat een gezamenlijke standaard beschrijft voor alle verschillende indices. De internetstandaard om adressen te achterhalen (DNS) heeft ook een dergelijk model.

Concretisering

Gegevensuitwisselingen tussen een vooraf bekende bronhouder en afnemer (bijv. in het kader van overdracht, verwijzing of expliciete specifieke toestemming) worden op korte termijn gezamenlijke methodes en technieken afgesproken: specifieke autorisatie i.c.m. een ‘notified pull’.

Wanneer er sprake is van een gewenste gegevensuitwisseling op basis van een categorale toestemming (1..n bronhouders, n afnemers) of waarbij nog geen toestemming is gegeven (bijv. in het geval van spoed) is allereerst een identifier van de cliënt/ patiënt en vervolgens een index nodig. Koppeling met een landelijke index is een logische volgende stap die kan worden genomen om deze use cases te ondersteunen. Mitz biedt dergelijke index-functionaliteit in combinatie met een toestemmingsregister. Voor de zorgtoepassing eOverdracht is dit niet relevant maar wel voor andere zorgtoepassingen zoals medicatieproces of geboortezorg.

Organisatiebeleid

Met het veld moet er een keuze worden gemaakt om de verschillende types indices voor datalokalisatie landelijk vindbaar en toegankelijk te maken. Of iedereen kiest voor één gezamenlijke index (bijv Mitz) of er moet een standaard en een stelsel worden ontwikkeld waarmee verschillende indices ontsloten kunnen worden, waardoor iedereen een vrije keuze heeft in een index.

Zorgproces

Afhankelijk van de beleidskeuze dienen de zorgprocessen zo ingericht te worden dat deze de gebruikte index bijhouden met registratie van waar welke gegevens van welke patiënt/cliënt beschikbaar zijn. Dit is met name van belang in use cases waarin het niet direct duidelijk is waar relevante gegevens (nog meer) beschikbaar zijn.

Informatie

De volgende types van indices worden onderscheiden (globaal gesorteerd van klein naar groot):

1. notificatie van bronhouder aan afnemer (bijv. een notificatie bij een verwijzing of overdracht)
2. notificatie van cliënt/patiënt aan afnemer (bijv. mondeling of door middel van een fysieke drager). Als de patiënt gedwongen wordt om het zelf te onthouden dan zullen er bronnen vergeten gaan worden. Middelen als de GGZ-crisiskaart bieden wel enigszins een oplossing waarmee een patiënt kan aangeven waar hij in zorg is.
3. omgeving van burger: informatie over toestemming of behandelovereenkomst (bijv. zorgnetwerk-informatie in persoonlijke gezondheidsomgeving)
4. systeem afnemer: informatie over behandelovereenkomst of grondslag (bijv. Nuts-autorisatieregister van de afnemende zorgaanbieder)
5. landelijke index: informatie over toestemming of behandelovereenkomst (bijv. Mitz-notificatieregister)

Applicatie

De applicatie(s) waarin de index wordt bijgehouden moeten aangepast worden op de landelijke standaard die hiervoor afgesproken is. De NEN-commissie voor lokalisatie zal hier een standaard voor opstellen/aanwijzen.

Het geven van toegang tot deze indices kan online door middel van een digitale waarborg, een bewijs van grondslag voor het verkrijgen van toegang tot 1 of meerdere indices. (Raadplegende) applicaties moeten dit ondersteunen.

IT-infrastructuur

Het geven van toegang tot deze indices zou ook ‘offline’ kunnen. Door middel van een fysiek waarborg/ hardware-token, bijv. een ggz-crisiskaart. De waarborg is dan dat de afnemer en cliënt/ patiënt hebben behandelrelatie/overeenkomst hebben, want deze zijn fysiek bij elkaar.

Deliverables 2022-2026 en afhankelijkheden

Fase	**Deliverable**	**(Nog niet ingevulde) Afhankelijkheden**	**Betrokkenen**
Nu	datalokalisatie obv specifieke autorisatie	Afnemer ondersteunt Nuts-standaarden	Nuts, Twiin, TSV, Actiz
Nu	lokalisatie obv regionale (XDS-)registers		
Nu	lokalisatie obv land. LSP-index		
Nu	lokalisatie obv notificatie (ongestandaardiseerd)		

2022	leveranciers-afspraak notificatie notified pull	Bronhouder en Afnemer ondersteunen Nuts-standaarden	TSV, Twiin, Nuts
2022	PoC standaard notified pull	(concept) leveranciers-afspraak notified pull gereed	TSV, Nuts, Twiin
2022-2023	Opname afspraak notificatie notified pull in Twiin AS	Overeenstemming tussen leveranciersafspraak eOverdracht en Twiin-ideeën notified pull	Twiin, Nuts, TSV
eind 2023	**(concept) NEN-normen generieke functies**	**-**	**NEN-werkgroep Generieke Functies**
2023-2024	Datalokalisatie o.b.v. landelijke index (bijv. Mitz)	Mitz in productie	VZVZ
		Goed gevuld Mitz-notificatieregister én directe toegang tot Mitz-notificatieregister óf Goed gevuld Mitz-toestemmingsregister	MinVWS, VZVZ, alle koepels
2024-2025	Datalokalisatie ook obv behandelovereenkomst in kluis van burger	Oplossing voor identificatie burgers zonder gebruik bsn	MedMij, Twiin, Nuts, …
2026	vrije keuze Behandel Overeenkomst omgeving voor cliënt en zorgverlener	volgt uit bovenstaande	

Deliverables 2022/23 en acties

Goal	**Strategies**	**Acties**	**Wie**
leveranciers-af spraak notificatie notified pull	TSV werkgroep	Schrijven TA	TSV, Twiin, Nuts
PoC notified pull	Uitvoeren PoC aangaande BgZ in FHIR-formaat	Polsen animo, schrijven specificaties, uitvoeren PoC	TSV
Opname afspraak	Overnemen TA	Vertalen naar uitwisselingsconcept	Twiin

notified pull in Twiin AS			

10. Aandachtsgebied 8: Adressering

Inleiding

Voor succesvolle gegevensuitwisseling is het essentieel dat applicaties van verschillende zorgaanbieders elkaar kunnen vinden middels een technisch adres (bijv. een url). Dit noemen we adressering. Binnen de verschillende actieve uitwisselingsinfrastructuur in Nederland is dit adequaat geregeld. Het adresseren van applicaties over verschillende uitwisselingsinfrastructuren heen is een uitdaging. Vaak heeft iedere uitwisselingsinfrastructuur een eigen manier op applicaties te adresseren. Het ontbreekt aan landelijke afspraken rondom elektronische adresgegevens en adresseringsmechanismen.

Gezamenlijke visie

Doel voor 2026

Technische adressen van verschillende uitgevers/beheerders worden op een gestandaardiseerde manier opgezocht en uitgewisseld.

Waarom

Adresseringsmechanismen vormen vaak de kern van een uitwisselingsinfrastructuur, deze zijn daarom niet gemakkelijk te veranderen. Het doel is om te komen tot een manier om de uitgevers/beheerders van de adressen uit verschillende domeinen wel landelijk te kunnen koppelen. Technische adressen kunnen afkomstig zijn uit verschillende domeinen. Digitaal ondertekende adres-attributen moeten op een gestandaardiseerde manier opgezocht en uitgewisseld kunnen worden. Zonder eenduidige afspraken over adressering kunnen verschillende uitwisselingsinfrastructuren alleen maar met elkaar koppelen door voor iedere koppeling aparte afspraken te maken en implementaties te doen. Daarnaast zullen beheerders dan vaak in verschillende systemen de digitale adressen moeten beheren om breed bereikbaar te zijn/blijven.

Consequenties

Alle adresseringsfunctionaliteit zal ter zijner tijd ontsloten moeten kunnen worden via de landelijke afspraken voor adressering.

Concretisering

Het NEN-normeringstraject voor adressering is nog niet gestart. Pas wanneer deze is afgerond zijn er geen de jure kaders om te komen tot een landelijke standaard voor adressering. Tot die tijd zou de markt natuurlijk tot een de facto standaard kunnen komen.

Organisatiebeleid

Voor eOverdracht loopt de adressering nu via het Nuts-register. Voor andere zorgtoepassingen dan wel communicatie met partijen die geen Nuts gebruiken is het idee

om een PoC te starten waarin technische adresgegevens ook uit register(s) van vertrouwde uitgevers opgehaald kunnen worden. Opties hiervoor zijn Zorg-AB van VZVZ of het Landelijk Register Zorgaanbieders van CIBG.

Zorgproces

Informatie

Het aan te bevelen dat verklaringen over technische adresgegevens (mede) door de zorgaanbieder in kwestie digitaal zijn ondertekend. Wanneer dit het geval is, maakt het feitelijk niet meer uit door welke uitgever een verklaring over technische adresgegevens wordt uitgegeven.

Applicatie

De verschillende applicaties zullen moeten koppelen met een of meerdere uitgevers van technische adresseringsgegevens.

Wanneer er een stelsel is ontwikkeld kunnen verschillende uitgevers van technische adresgegevens daar aan kunnen koppelen en hebben zorgaanbieders in theorie nog slechts één koppeling nodig.

IT-infrastructuur

Omdat adresseringsgegevens niet dagelijks wijzigen en veel uitwisseling plaatsvinden met partijen waarin alreeds in een eerder stadium het adres is opgehaald, lijkt een zeer hoge beschikbaarheid van de infrastructuur hier minder relevant.

Deliverables 2022-2026 en afhankelijkheden

Fase	**Deliverable**	**(Nog niet ingevulde) Afhankelijkheden**	**Betrokkenen**
Nu	Adressering via Nuts register	Bronhouder en Afnemer ondersteunen Nuts-standaarden	TSV, Nuts, Actiz
2022	PoC adressering vertrouwde Uitgever(s) (ZORG-AB, LRZA, …)	ZORG-AB kan adres-attributen uitgeven	VZVZ
		LRZa kan adres-attributen uitgeven	CIBG
		Uitbreiden functionaliteit Nuts-node voor acceptatie 'externe' uitgevers adres-attributen	Nuts, Twiin
		Aantal gemotiveerde leveranciers	TSV

	(concept) NEN-normen generieke functies niet gepland	-	NEN-werkgroep Generieke Functies
2023	Standaard voor adressering	Ontwerp norm generieke functie adressering	Twiin, Nuts, VZVZ
2024	Uitgevers adressering versch. domeinen gekoppeld	Uitgevers ondersteunen gemeenschappelijke standaard	VZVZ, CIBG, evt. andere uitgevers
2025	Uitgevers adressering attribuut- gebaseerd digitaal ondertekend	volgt uit bovenstaande	

Deliverables 2022/23 en acties

Goal	Strategies	Acties	Wie
Pilot adressering vertrouwde Uitgever(s) (ZORG-AB, LRZA, …)	ZORG-AB kan adres-attributen uitgeven	Gezamenlijk gesprek Verifiable Credentials icm ZORG-AB	VZVZ, Twiin, Nuts
		Schets functioneel ontwerp	VZVZ
		Voorbereiding Pilot	VZVZ, Twiin, Nuts
	LRZa kan adres-attributen uitgeven	Gezamenlijk gesprek Verifiable Credentials icm CIBG	CIBG, Twiin, Nuts
		Schets functioneel ontwerp	CIBG
		Voorbereiding Pilot	CIBG, Twiin, Nuts
	Uitbreiden functionaliteit Nuts-node voor acceptatie 'externe' uitgevers adres-attributen	Ontwerp/ uitbreiding Verifiable Data Registry	Nuts, Twiin
		Ontwikkeling	Nuts
		Voorbereiding Pilot	Nuts, Twiin

11. Aandachtsgebied 9: Communicatiebeveiliging

Inleiding

Er moeten ook afspraken komen voor netwerken die gebruikt gaan worden. De conceptversie van de nieuwe versie van de NEN7512 stelt hier strengere eisen aan. De norm onderscheid drie lagen van beveiliging, waarvan afhankelijk van het risiconiveau er één tot drie toegepast moeten worden:

- veilig netwerk
- versleuteld bericht en/of
- versleuteld kanaal

Binnen een domein is een keuze redelijk goed te maken. Complex wordt het als twee domeinen willen koppelen die verschillende keuzes hebben gemaakt. Bij overgang van het bericht naar het andere domein zou de keuze in beveiliging omgezet moeten worden.

Gezamenlijke visie

Doel voor 2026

Om verschillende domeinen te koppelen dienen er afspraken gemaakt te zijn over gestandaardiseerde invulling van de beveiligingslagen.

Waarom

Met landelijke afspraken kan verkeer dat domeinoverstijgend is makkelijker gefaciliteerd worden en zijn er waarborgen dat door eventuele inwisseling van de ene maatregel door een andere het totale beveiligingsniveau niet wijzigt.

Consequenties

Alle domeinen moeten een passende invulling geven aan de nieuwe versie van de NEN 7512 en wanneer met een ander domein gekoppeld moet worden afspraken maken over hoe de NEN 7512 wordt ingevuld.

Concretisering

De nieuwe versie NEN 7512 is onlangs gepubliceerd. Om verschillen in invulling van de norm bij domeinoverstijgend verkeer te minimaliseren ligt het voor de hand om in de koppeling tussen domeinen (Twiin afsprakenstelsel) een eenduidige aanpak te kiezen.

Voor de langere termijn dienen er afspraken gemaakt te worden over hoe verschillende invullingen van de beveiligingslagen uit de NEN 7512 op elkaar gemapt kunnen worden.

Organisatiebeleid

Zorgorganisaties dienen in hun gegevensuitwisselingen aan de NEN 7512 te gaan voldoen. Vaak is dit nu nog niet het geval, waar de wettelijke verplichting hiertoe als sinds 2017

bestaat. Omdat de norm op veel punten keuzevrijheid biedt, kunnen er veel verschillende implementaties van de eisen uit de norm gaan ontstaan. Juist omdat veel partijen nog niet voldoen lijkt dit een uitgelezen moment om, voordat partijen individueel aan de slag gaan, hier één lijn in te kiezen.Dat zou het Twiin afsprakenstelsel kunnen zijn.

Zorgproces

Naast dat zorgaanbieders individueel niveau aan de NEN 7510 moeten voldoen, met daarin allerlei verplichtingen om bepaalde processen in te richten, moeten er aanvullende zaken ingevuld worden wanneer de zorgaanbieder gaat communiceren met andere zorgaanbieders volgens de NEN 7512. Het lijkt zinvol om deze processen en eisen zoveel mogelijk eenduidig in te gaan richten.

Informatie

Er dienen afspraken gemaakt te worden over de onderwerpen die in voorgaande hoofdstukken besproken zijn en aanvullend over zaken zoals (o.a.)

- logging, audit trails en de uitwisseling daarvan met communicatiepartners
- beveiligingsniveaus (kanaalversleuteling, berichtversleuteling en/of veilige netwerken)

Applicatie

Een aantal van de eisen die de NEN 7512 stelt, dienen door applicaties ondersteund te worden. Om niet iedere leverancier zelf uit te laten vinden welke en hoe deze eisen geïmplementeerd moeten worden lijkt het zinvol dat hier een landelijk kader voor komt (in het Twiin afsprakenstelsel).

IT-infrastructuur

Voor veel uitwisselingen zullen 2 of 3 beveiligingsmaatregelen genomen moeten worden. Dat betekent als snel dat men gebruik van veilige netwerken moet gaan maken. Een ‘veilig netwerk een beheerd netwerk

- Waar de beheerder moet voldoen aan de NEN7510
- Toegang tot het netwerk uitsluitend is toegestaan voor partijen waarvan de identiteit is vastgesteld middels authenticatie waarvan de betrouwbaarheid overeenkomt met het eIDAS-betrouwbaarheidsniveau ‘hoog’
- Maatregelen zijn getroffen waarmee met grote zekerheid wordt voorkomen dat communicatie binnen het netwerk buiten de Europese Economische Ruimte kan komen.

Dit betekent dat uitwisselingen die lopen via standaard publiek internet niet (meteen) voldoen aan de NEN 7512.

Deliverables 2022-2026 en afhankelijkheden

Fase	**Deliverable**	**(Nog niet ingevulde) Afhankelijkheden**	**Betrokkenen**
Nu	internet + mTLS obv PKIo +	Bronhouder en afnemer	TSV, Nuts, Actiz

	DID	ondersteunen Nuts-standaarden	
2022	NEN 7512- 2022 duidelijk	Publicatie norm	NEN
2022	gezamenlijke afspraak 2 vd 3 lagen 7512	NEN 7512 duidelijk	Twiin, Nuts, TSV
2022	definitie beheerd netwerk verder ingevuld	PvE	Twiin, Nuts, TSV, VZVZ, Nictiz
2023	**(concept) NEN-normen generieke functies**	**-**	**NEN-werkgroep Generieke Functies**
2023	landelijke afspraak invulling 7512 (3/3?)	NEN-norm	Twiin, Nuts, TSV
2025	security = resultaat meerdere lagen	volgt uit bovenstaande	

Deliverables 2022/23 en acties

Goal	Strategies	Acties	Wie
NEN7512- 2022 incl definitie Veilig Netwerk duidelijk	Publicatie norm	nvt	
gezamenlijke afspraak 2 vd 3 lagen 7512	NEN 7512 duidelijk	Bestuderen norm	Twiin, Nuts
		Gezamenlijke afspraak kanaalversleuteling	Twiin, Nuts, TSV
		Bestuderen en input leveren voor actualiseren GZN-eisen en/of ZSP-eisen	Twiin, Nuts
		Beschrijven impact voor zorgaanbieders	Twiin, Nuts, Actiz

12. Aandachtsgebied 10: Stelselbeheer

Inleiding

Iedere gegevensuitwisseling in de zorg wordt uitgevoerd op basis van een standaard. Hierdoor is er een gelijk speelveld voor alle softwareleveranciers en

voorzieningenleveranciers. De softwareproducten, die deze standaarden hebben geïmplementeerd, vormen samen het ecosysteem voor gegevensuitwisseling in de zorg. Standaarden die voor het informatiestelsel zijn ontwikkeld noemt men stelselstandaarden. Deze besturing hiervan is vastgelegd in NEN 7522:2021, de Nederlandse norm voor het ontwikkelen en beheren van standaarden en stelsels van standaarden.

Gezamenlijke visie

Doel voor 2026

In 2026 dient het Twiin afsprakenstelsel bestuurd te worden volgens de NEN 7522.

Waarom

Om een onderdeel te zijn van het duurzame informatiestelsel in de zorg dient de DIZRA gevolgd te worden. Deze schrijft de NEN 7522 voor.

Consequenties

Om aan de NEN 7522 invulling te geven dienen er bepaalde rollen ingericht en toegekend te worden. Daarnaast dienen er bepaalde governance processen ingericht en gevolgd te worden.

Concretisering

Organisatiebeleid

Nuts kent nog geen formeel stelselbeheer. Voor Twiin is er een eerste aanzet gemaakt. Beide afsprakenstelsels dienen het komend jaar het stelselbeheer in te gaan vullen. Waar mogelijk elkaar versterkend.

Daarna (2023-2024) dient dit stelselbeheer ook ingevuld en geïmplementeerd te zijn, zodat in 2026 alles aantoonbaar aan wet (Wegiz) en regelgeving (DIZRA, NEN 7522) voldoet. De status van Twiin als beheerder van het afsprakenstelsel is ook nog wat onduidelijk. Twiin is nog maar een programma. Voor het beheer van een afsprakenstelsel is een bepaalde governance nodig. Twiin en Nuts gaan stelselbeheer beschrijven maar het is nog niet vooraf bekend welke partij of partijen het stelselbeheer daadwerkelijk gaan uitvoeren.

(Zorg)proces

Voor het beheer van een afsprakenstelsel dient de NEN 7522 gevolgd te worden. In deze norm zijn richtlijnen gegeven voor governance en bepaalde processen.

Informatie

Zie NEN 7522

Applicatie

De functionaliteit die voor de verschillende generieke functies gemaakt moet worden kan op verschillende manieren worden ontwikkeld. De volgende modellen worden onderkend:

- Centrale applicatie. In dit model wordt er een applicatie ontwikkeld die door alle partijen gebruikt, al dan niet verplicht, gebruikt wordt. Met de applicatie worden interface specificaties meegeleverd waarmee andere partijen de software kunnen bouwen die met de centrale applicatie communiceert. Redenen om voor dit model te kiezen zijn o.a. kostenefficiëntie (niet iedere partij hoeft de functie zelf te bouwen, slechts de interface) en/of de noodzaak voor centraal beheer (de inhoud/functie wordt door één partij beheerd). Een voorbeeld is de SBV-Z.
- Open source software. In dit model wordt er door meerdere partijen aan een applicatie gebouwd. De programmacode is vrij beschikbaar en kan door de IT-leveranciers in hun software worden ingebouwd. Voordelen van dit model zijn dat de kosten voor ontwikkeling gedeeld worden en niet ieder voor zich de functionaliteit hoeft te bouwen. Voorbeelden van dit model zijn te vinden in Koppeltaal en Nuts-nodes.
- Closed source software. In dit model wordt er door één partij een applicatie ontwikkeld die vervolgens door de andere IT-leveranciers in hun eigen software wordt ingebouwd. Een reden om voor dit model te kiezen (t.o.v. het open source model) is dat hiermee de kwaliteit van de software gegarandeerd kan worden. Een voorbeeld is de software om de UZI-pas aan te roepen.

IT-infrastructuur

n.v.t.

Deliverables 2022-2026 en afhankelijkheden

Fase	Deliverable	(Nog niet ingevulde) Afhankelijkheden	Betrokkenen
Nu	geen stelselbeheer	geen, tijdelijke afspraak over beheer standaard nodig	Twiin, Nuts, Actiz
2022	stelselbeheer beschreven	Expertise NEN 7522 aanwezig (leren van MedMij en Koppeltaal)	Twiin, Nuts
		Vertegenwoordigers rollen NEN7522 betrokken	Twiin, Nuts, Actiz, TSV
2023	**(concept) NEN-normen generieke functies**	**-**	**NEN-werkgroep Generieke Functies**
2023	stelselbeheer ingevuld	Uitvoering rollen geborgd	Twiin, Nuts, Actiz, TSV

2025	stelselbeheer conform Wegiz, DIZRA en NEN 7522	volgt uit bovenstaande	

Deliverables 2022/23 en acties

Goal	**Strategies**	**Acties**	**Wie**	**Wanneer**	**Vragen/ issues**
Stelselbeheer beschreven	Expertise NEN 7522 aanwezig (leren van MedMij en Koppeltaal)	Bestuderen NEN7522, inclusief uitvraag bij MedMij en Koppeltaal	Twiin, Nuts		
		Inrichten processen	Twiin, Nuts		
	Vertegenwoordigers rollen NEN 7522 betrokken	Toewijzen rollen	Twiin, Nuts		

13. Aandachtsgebied 11: Vervolgproces visie/transformatie

De oplettende lezer heeft al opgemerkt dat op veel aspecten de gezamenlijke visie op ongeveer hetzelfde neerkomt:

A. Er moeten landelijke keuzes gemaakt worden in allerlei attributen die in de uitwisseling gebruikt worden om vertrouwen en beveiliging te waarborgen.
B. De attributen moeten uitgegeven worden door de daarvoor vertrouwde instanties. Voor sommige attributen is dat een zorgorganisatie, voor andere is dat de stelselbeheerder (zoals bijvoorbeeld Nuts, Twiin of VZVZ) en voor weer anderen zijn dat vertrouwde organisaties (zoals bijvoorbeeld LRZA, UZI-register, Mitz, Zorg-AB)
C. Om de echtheid en correctheid van deze attributen door de keten heen te borgen moeten deze digitaal ondertekend worden in de vorm van een verifiable credential (VC).

Het vervolgproces van de ontwikkeling van deze visie bestaat uit de volgende stappen:

1. Delen met de Twiin Architectuurraad. Wanneer zij zich ook achter deze visie scharen kan dit breder gedeeld worden.
2. Het delen van de visie met de Taskforce Samen Vooruit. Doel is om de leveranciers daarin de visie te laten onderschrijven, waarna concrete vervolgstappen in de eOverdracht implementatie gepland kunnen worden.
3. Het Twiin breed delen van de visie met de Twiin deelnemers (VZVZ, RSO's, leveranciers. Doel is om deze partijen de visie ook te laten onderschrijven.

In deze stappen kan de visie natuurlijk verder aangescherpt worden. Stap 2 en 3 kunnen desgewenst parallel worden uitgevoerd.

4. Bij voldoende draagvlak kan er dan aan het programma Twiin de opdracht worden gegeven om (gezamenlijk) onderdelen van de visie verder uit te gaan werken en in stappen bepaalde resultaten te behalen. Voor 2022 zijn er in dit document al een aantal te behalen resultaten gedefinieerd. Acties zijn dan o.a.
    a. het schrijven van architectuurontwerpen en specificaties
    b. verzoeken sturen naar de partijen die gemeenschappelijke diensten leveren om functionaliteit te gaan leveren: LRZA,UZI-register, Zorg-AB, Mitz, Nictiz
5. Deze specificaties zijn dan de basis zijn om een nieuwe/aangepaste versie van de Nuts Bolt eOverdracht in het Twiin afsprakenstelsel op te nemen.
6. Tegelijkertijd kan een breed gedragen visie als input dienen voor de NEN-werkgroepen van generieke voorzieningen die komend jaar aan de slag gaan. Dit kan o.a. via een aantal mensen van Twiin en Nuts die deelnemer zijn van dit NEN-traject.

Na het NEN-traject moet er meer duidelijkheid zijn over de kaders waaraan de gemeenschappelijke voorzieningen moeten voldoen. Dit moet voldoende input geven om waar nodig verdere implementatiespecificaties, standaarden en afsprakenstelsels te schrijven en vast te stellen.

7. Om deze op te stellen is een brede samenwerking nodig tussen de Twiin deelnemers en voorzieningenleveranciers om gezamenlijk hiertoe te komen. Commitment en inzet van deze partijen is nodig om de visie in 2026 te kunnen implementeren.

14. Conclusie

De conclusie bestaat uit een aantal deelconclusies. Deze worden afzonderlijk behandeld en van geadviseerde vervolgstappen voorzien.

Een gezamenlijk groeipad
Dit document toont allereerst aan dat Twiin en Nuts beide op inhoudelijk niveau voldoende mogelijkheden zien om naar elkaar toe te groeien: Voor alle 11 aandachtsgebieden zijn een visie en mogelijke tussenliggende stappen geformuleerd waar beide partijen inhoudelijk achter staan. Twiin zet daar wel uitdrukkelijk de kanttekening bij dat voor het daadwerkelijk omarmen van de beschreven oplossingsrichtingen meer onderzoek naar de impact en adoptie ervan nodig is. Het advies is om op korte termijn in samenwerking met de diverse stakeholders de impact en adoptie in kaart te brengen.

Aanzienlijke hoeveelheid werk
Voor het realiseren van de in dit document beschreven oplossingsrichtingen hebben niet alleen Twiin en Nuts veel werk te doen, zoals het op punten aanvullen of aanpassen van het Twiin afsprakenstelsel en de Nuts-standaarden. Ondanks dat de exacte impact nog niet is bepaald, is al duidelijk dat de hoeveelheid werk voor leveranciers van applicaties die generieke functies willen invullen of daarmee willen koppelen aanzienlijk zal zijn. Naast het in kaart brengen van de impact, dienen Twiin en Nuts in samenwerking met de verschillende stakeholders de beschreven oplossingsrichtingen waar mogelijk in kleinere delen te splitsen en te prioriteren.

Self-Sovereign Identity en Verifiable Credentials
Een belangrijke oplossingsrichting, die in meerdere aandachtsgebieden terugkomt, is het gestandaardiseerd beschikbaar maken van onweerlegbare, digitaal ondertekende verklaringen over zowel data als metadata. Een aanzienlijk deel van het uit te voeren werk is gerelateerd aan het implementeren van het concept self-sovereign identity (SSI) en de hieraan gerelateerde internationale standaard voor digitaal ondertekende verklaringen Verifiable Credentials. Internationaal wordt het concept Self-Sovereign Identity en de standaard Verifiable Credentials (en in mindere mate) Decentralized Identifiers steeds breder omarmd en ook Twiin en Nuts zien de potentie ervan. Tegelijkertijd zijn de impact en adoptie in Nederland nog onbekend. Het advies is om op korte termijn in samenwerking met de diverse stakeholders de (noodzaak van de) impact en adoptie van het concept Self-Sovereign Identity en de standaarden Verifiable Credentials en Decentralized Identifiers in kaart te brengen.

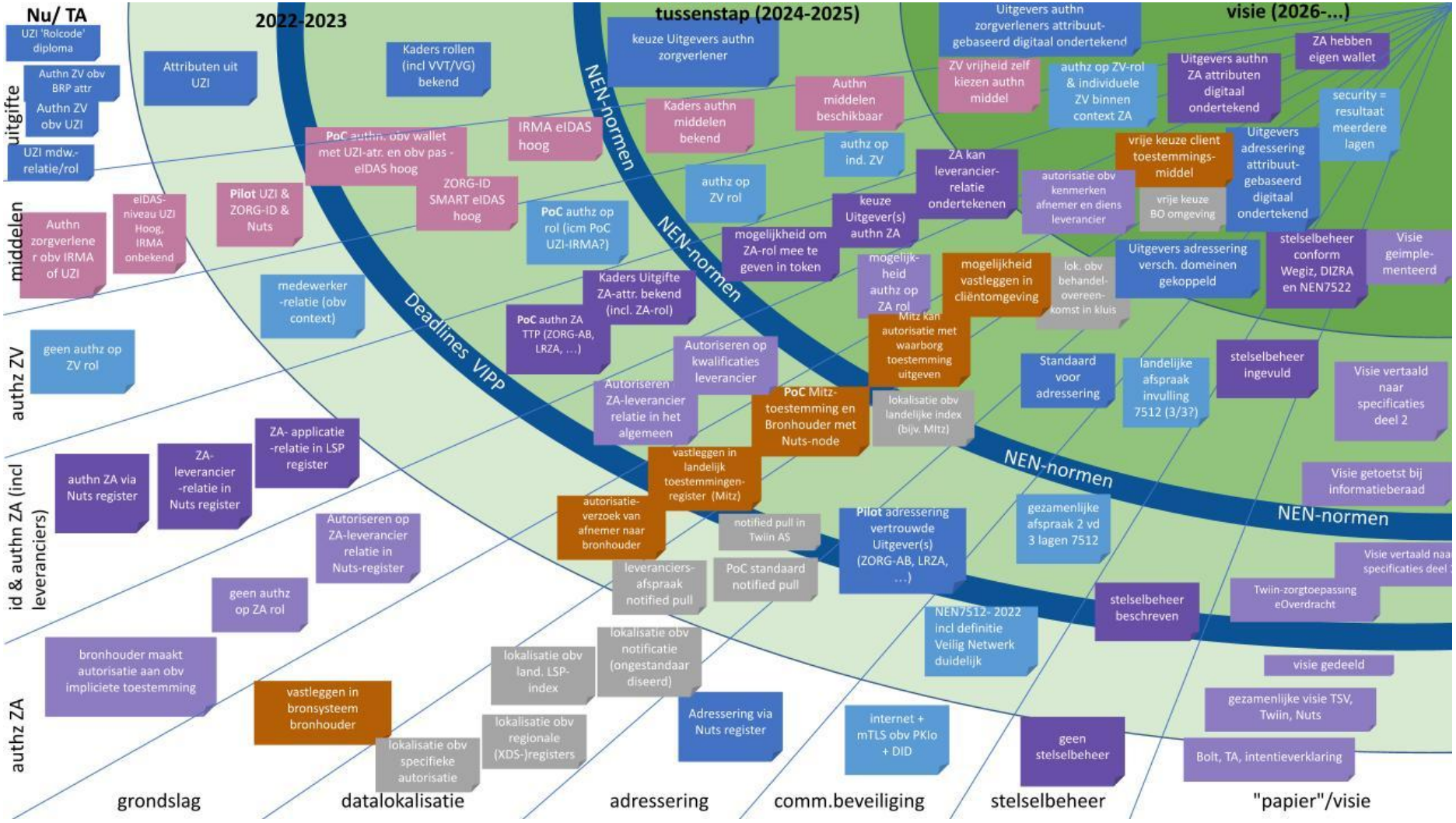
Verbreding naar andere zorgtoepassingen
Dit document is opgesteld naar aanleiding van een fit/gap-analyse aangaande de zorgtoepassing eOverdracht. De reikwijdte van de in dit document beschreven oplossingsrichtingen is echter breder dan alleen de zorgtoepassing eOverdracht: de

beschreven oplossingsrichtingen heeft naar verwachting ook meerwaarde binnen andere zorgtoepassingen. Niet alleen vanuit het oogpunt van meerwaarde is verbreding naar andere zorgtoepassingen opportuun. De verwachte hoeveelheid werk, die met de oplossingsrichtingen gepaard gaat, vergt hierbij aansluitende investeringen. Deze investeringen kunnen slechts beperkt worden gerechtvaardigd wanneer ze louter voor de zorgtoepassing eOverdracht worden ingezet. Het is daarom wenselijk om het gebruik van de beschreven oplossingsrichtingen voor meerdere zorgtoepassingen te overwegen. Hierbij dient te worden opgemerkt dat dit document uitdrukkelijk niet bepleit om bestaande, goed functionerende zorgtoepassingen aan te passen wanneer dat geen functionele meerwaarde heeft. Een afweging over het gebruik van de in dit document beschreven oplossingsrichtingen kan per zorgtoepassing worden gemaakt. Een verschillende afweging en daarmee een verschillende stack aan standaarden per zorgtoepassing hoeft geen probleem te zijn mits het Twiin afsprakenstelsel hierover de juiste afspraken definieert. Omwille van efficiëntie is het echter aantrekkelijker om clusters van zorgtoepassingen te identificeren en de afweging op clusterniveau uit te voeren. Een clustering die goed aansluit bij het vergaarde beeld van de huidige situatie aangaande gegevensuitwisseling in de Nederlandse zorg is het onderscheid tussen document-gebaseerde zorgtoepassingen enerzijds en zib/fhir-gebaseerde zorgtoepassingen anderzijds. Hierbij lijken de mogelijkheden voor het implementeren van de beschreven oplossingsrichtingen het meest kansrijk bij de zib/fhir-gebaseerde zorgtoepassingen.

Verbreden naar meer stakeholders

Dit document is opgesteld door vertegenwoordiger van Twiin en Nuts. De beschreven oplossingsrichtingen raken echter ook een groot aantal andere stakeholders. In gezamenlijk overleg met het veld moet worden bepaald in hoeverre de voorgestelde oplossingsrichtingen noodzakelijk zijn, draagvlak hebben en haalbaar zijn. Het advies is om op korte termijn een gestructureerde inhoudelijke en bestuurlijke samenwerking met de relevante stakeholders aan te gaan om tot een 'nationaal gedragen' groeipad te komen. Twiin en Nuts beogen met dit gezamenlijke document een kickstart te geven aan dit traject.

Bijlage 1: Transformation map



Bijlage 2: PKI en SSI

Bij de uitwisseling van privacygevoelige gegevens, zoals medische gegevens moeten er maatregelen genomen worden die borgen dat de gegevens niet door andere partijen onderschept of gewijzigd kunnen worden. Hiertoe moeten de partijen ondere andere met grote zekerheid elkaars identiteit kunnen vaststellen. Dit betreft niet alleen de identiteiten van de zorgorganisaties, maar ook die van de gebruiker en/of de zorgverlener die verantwoordelijkheid neemt voor de gegevensuitwisseling. Daarnaast zijn er nog andere zaken waar je zekerheid over wil hebben, zoals grondslagen van de verwerking (denk bijvoorbeeld aan impliciete of uitdrukkelijke toestemming), de kwalificaties en/of rollen van de gebruikers (in verband met het toepassen van autorisatieregels) en de IT-dienstverleners (is deze daadwerkelijk een verwerker van de zorgorganisatie en voldoet de software aan de gestelde kwaliteitseisen).

PKI

Een veel gebruikte technologie om deze waarborgen te bieden in Public Key Infrastructure (PKI). In PKI worden digitale certificaten gebruikt. Dit zijn een soort digitale paspoorten voor organisaties en individuen. Deze certificaten worden in de gegevensuitwisseling gebruikt om de partijen te identificeren, de gegevensuitwisseling te versleutelen en gegevens digitaal te ondertekenen.

Hoe werkt PKI

Een vertrouwde partij, zoals de overheid (we noemen het dan PKIoverheid, PKIo) kan de digitale certificaten uitgeven. Om deze te bemachtigen geldt een grondige procedure om de identiteit van de houder ervan vast te stellen, vergelijkbaar met de uitgifte van een paspoort of rijbewijs. Kenmerkend aan PKI is dat het een hiërarchisch vertrouwensmodel kent. Een vertrouwde partij (*certificate authority, CA)* kan een andere partij aanwijzen die certificaten uitgeeft. Maar op haar beurt ook weer taken delegeren. Zo ontstaat er een boom of keten van vertrouwen waarin het startpunt de *root CA* wordt genoemd.

De communicerende partijen kunnen elkaars digitale certificaat controleren. Op het certificaat staat, net als op een identiteitsbewijs, de identiteit van de houder ervan. Daarnaast kunnen er ook andere gegevens op een certificaat gezet worden, bijvoorbeeld een uniek identificatienummer (zoals UZI of URA-nummer), de kwalificatie van de zorgverlener (UZI-rolcode), of het digitale (internet-)adres waarop het certificaat gebruikt wordt. De communicatie partij kan controleren van wie het certificaat is, wie het certificaat heeft uitgegeven (en vertrouwt men deze partij), of het certificaat nog geldig is en of het hoort bij de website die bezocht wordt.

Additionele functies

Naast de authenticatie worden de certificaten ook gebruikt om gegevens te versleutelen of te ondertekenen. Met zogenaamde TLS-kanaalversleuteling kunnen twee partijen borgen dat de gegevensuitwisseling niet wordt afgeluisterd. Men kan ook de eigen gegevens

versleutelen zodat niemand deze kan inzien, of juist de gegevens versleutelen zodat alleen de ontvanger deze kan ontsleutelen.

Daarnaast kan men met een digitale ondertekening kan je borgen dat de gegevens naderhand niet aangepast worden. Als dit wel gebeurt dan past de digitale handtekening niet meer bij de gegevens. Wanneer PKI-middelen op een betrouwbare manier zijn uitgegeven is een digitale handtekening net zo rechtsgeldig als een natte handtekening.

Nadelen van PKI

Flexibiliteit

PKI wordt al decennia met succes toegepast, maar is afhankelijk voor een beperkt aantal centrale vertrouwde partijen die de certificaten mogen uitgegeven. Dit maakt het model vrij star. In de inleiding zijn meerdere zaken genoemd die je bij een uitwisseling van medische gegevens zou willen controleren, een deel daarvan wordt maar door het UZI-register op de digitale certificaten gezet. Aanvullende ‘attributen’ kunnen niet zomaar aan een bestaand certificaat worden toegevoegd. Voor deze andere attributen zou je dan andere certificaten moeten gaan uitgeven. Certificaten van verschillende uitgevers moeilijk te relateren zijn aan één subject omdat daar doorgaans ook andere private keys onder water gebruikt worden. Het combineren van meerdere attributen wordt daardoor erg lastig.

Koppeling identiteiten/certificaten aan het authenticatiemiddel

Bij PKI is het zo dat de identiteit en de daarmee samenhangende attributen hard aan een middel worden gekoppeld. Het is daarmee niet mogelijk om voor de houder, de gebruiker, een andere manier van authenticatie te gebruiken. Dit is nu ook het probleem met de UZI-pas dat men wil oplossen.

Privacy

Een ander nadeel van PKI is dat een controlerende partij direct alle gegevens van het certificaat te weten komt. In de fysieke wereld geldt dit ook. Wanneer je bijvoorbeeld je leeftijd aan moet tonen bij een slijterij en daarvoor je paspoort gebruikt, weet de slijter niet alleen je leeftijd, maar ook je geboortedatum, je naam en je BSN. Dat zijn zaken die je niet wilde delen. In de zorg is dit nadeel vermoedelijk wat minder relevant, maar toch is er een voorbeeld te noemen waarin meer gegevens gedeeld worden in de uitwisseling dan gewenst: wanneer een apothekersassistent gegevens raadpleegt namens een apotheker, is het voor de communicatiepartij niet relevant wie die assistent precies is. Wat wel gecontroleerd dient te worden is of de assistent daadwerkelijk bij de apotheek werkt, namens de apotheker de gegevens opvraagt en wie die apotheker dan precies is.

Self Sovereign Identities (SSI)

Fysieke identiteiten zijn bijvoorbeeld kaarten die zijn uitgegeven door de overheid, werkgever, universiteit, sportschool of een winkel om te verifiëren dat de kaarthouder een burger, werknemer, student, lid of klant van de organisatie is. Iedere uitgever van een identiteit koppelt dit aan een fysiek middel, waardoor een houder ervan met vele verschillende middelen rondloopt.

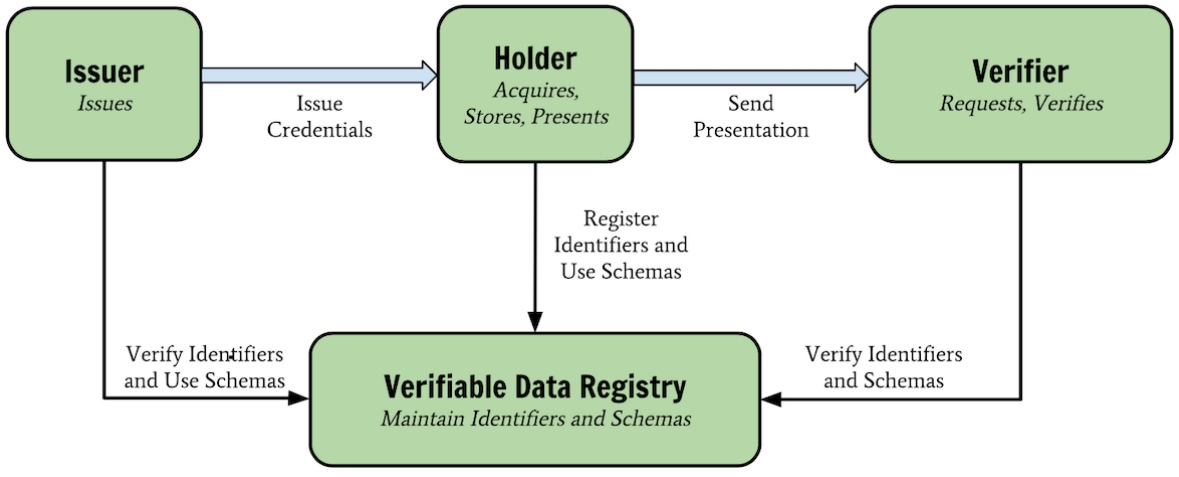
Digitale ID's zijn toegankelijk door te registreren voor een dienst met een e-mailadres of gebruikersnaam en een wachtwoord. Met digitale ID's kunnen gebruikers ook gebruikmaken van inlog-services van derden, zoals Inloggen met Facebook of Inloggen met Google. Gebruikers hebben matig tot geen controle over het delen van hun gegevens. De privacy loopt vaak gevaar met inlog-diensten van derden met financiële prikkels voor het verzamelen en opslaan van gegevens.

Deze (en andere) problemen probeert men op te lossen met een nieuw model Self Sovereign Identities (SSI). De vertaling is zelf-soevereine identiteit, een identiteit die in jouw bezit is en waarin je niet of minder afhankelijk bent van centrale organisaties. Alleen jij houdt het vast, in je eigen persoonlijke digitale identiteitsportefeuille (wallet), en alleen jij bepaalt wie het mag "zien" en wat ze ervan mogen "zien".

Hoe werkt SSI

In de basis is de bedrijfsarchitectuur van SSI niet echt anders dan die van PKI. Uitgevers (*issuer*) van identiteiten en/of attributen kunnen deze koppelen aan jouw identiteit. BIG-register kan bijvoorbeeld een kwalificatie als zorgverlener digitaal uitgeven. De houder (*holder*) ervan koppelt deze kwalificatie in zijn/haar wallet en kan zich daarmee digitaal identificeren als zorgverlener. Een partij die dat wil controleren (*verifier*), zoals een zorginstelling die wil weten welke diploma's iemand heeft kan zien dat de identiteit is uitgeven door het BIG-register en daarmee vertrouwd kan worden. Tevens kan deze controleren of de gegevens nog geldig zijn bij een *verifiable data registry.*

Het grote verschil met PKI is, is dat er geen hiërarchie van vertrouwen is. Iedereen kan onafhankelijk van andere partijen haar eigen identiteit controleren.



werking SSI (bron)

Techniek onder SSI

Wat wel verschilt aan PKI is de technologie waarop het SSI-model gebouwd moet worden. Deze bestaat uit drie pijlers:

- Decentralized Identifiers (DID)
- Verifiable Credentials (VC)
- Distributie-mechanisme

Decentralized Identifiers (DID)

Decentralized Identifiers, of wel gedecentraliseerde identifiers (DID's) zijn een nieuw type identifier dat verifieerbare, gedecentraliseerde digitale identiteit mogelijk maakt. Een DID verwijst naar elk onderwerp (bijvoorbeeld een persoon, organisatie, ding, datamodel, abstracte entiteit, enz.) zoals bepaald door de beheerder van de DID. In tegenstelling tot typische, gefedereerde identifiers, zijn DID's zo ontworpen dat ze kunnen worden losgekoppeld van gecentraliseerde registers, identiteitsproviders en certificeringsinstanties. Het ontwerp stelt de beheerder van een DID in staat om de controle/het eigenaarschap over de DID te bewijzen zonder toestemming/goedkeuring van een andere partij. De identiteiten worden gestandaardiseerd in de vorm van DID’s en gekoppeld aan een zogenaamd DID-document. Aan het DID wordt ook een sleutelpaar (private en publieke sleutels) gekoppeld waarmee gegevens ondertekend kunnen worden.

Verifiable Credentials (VC)

VC is de technologie om bepaalde gegevens, attributen van een identiteit, gestandaardiseerd elektronisch verifieerbaar te maken. Deze moeten dan gekoppeld worden aan de DID van de houder van het attribuut. Andere partijen kunnen hiermee controleren of een attribuut hoort bij de houder ervan en wie het attribuut heeft uitgegeven.

Distributie-mechanisme

SSI vereist een distributie-mechanisme om DID’s en VC mee te publiceren/distribueren. Hiermee kunnen dan VC’s ook weer ingetrokken worden, bijvoorbeeld omdat het attribuut niet meer aan een DID is gekoppeld of anderzijds niet meer geldig is. Het distributie-mechanisme vult daarmee de *verifiable data registry* in. Blockchain is één van de mogelijkheden om invulling te geven aan het distributie mechanisme.

Voorbeeld

Een zorgaanbieder kan haar eigen identiteit maken. Hiervoor creëert deze een DID en bijbehorende DID document. Uitgevers van attributen, zoals de Kamer van Koophandel,het UZI-register, of AGB-register kunnen vervolgens een VC maken van het KvK-nummer, het URA of AGB-code en deze koppelen aan de digitale identiteit van de zorgaanbieder. Andere partijen kunnen dan aan de VC zien dat deze hoort bij de zorgaanbieder en is uitgegeven door de genoemde partijen.

De genoemde technologie maakt het mogelijk dat partijen zelf hun identiteiten beheren, dat attributen gekoppeld kunnen worden die uitgegeven zijn door verschillende organisaties, zonder dat daar steeds een nieuw middel voor uitgegeven hoeft te worden. De belangrijkste innovatie van SSI t.o.v. PKI is de mogelijkheid voor elke entiteit om eenvoudig een privé/openbaar sleutelpaar te genereren en een DID en bijbehorend DID-document te publiceren dat het kan gebruiken om zichzelf aan de wereld te beschrijven. Verifiable Credentials worden gebruikt om informatie tussen entiteiten verifieerbaar uit te wisselen.

Nadelen van SSI

Hoewel SSI en de onderliggende technologie veelbelovend zijn en een aantal problemen oplost die PKI heeft, kent het ook wel wat nadelen.

- SSI, VC en DID m.n. de protocollen en methodes worden nog steeds ontwikkeld. Ondanks dat VC en DID formele standaarden zijn worden deze nog niet breed geaccepteerd en ondersteund. Google, Apple en Mozilla hebben vorig jaar formeel bezwaar gemaakt tegen de goedkeuring van W3C van de Decentralized Identifiers (DIDs) 1.0 specificatie (maar er zitten vermoedelijk ook commerciële belangen achter de weerstand van deze partijen):
    - DID's zijn dan wel gestandaardiseerd, maar de benodigde methodes nog niet. Het standaardiseren van DID-methodes is nu de volgende stap.
    - Het gebruik van blockchain ziet men niet als duurzaam. De DID specificatie verplicht het gebruik van blockchain-technologie niet. Ook evolueert de blockchain technologie zich ook om meer en meer duurzaam te zijn.
- Het is nog onduidelijk hoe men op een betrouwbare manier (eIDAS hoog) attributen aan identiteiten koppelt. De Europese Unie is hier wel mee bezig.

Conclusie

SSI en de onderliggende technieken bieden geen volledige vervanging van PKI-stelsels. PKI is een bewezen en breed gebruikte technologie die (voorlopig) ook nodig is om naast SSI het benodigde vertrouwen te bieden in digitale uitwisseling. SSI biedt wel meer flexibiliteit dan PKI en is nodig om als noodzakelijk bestempelde initiatieven zoals het loskoppelen van UZI-middelen en UZI-attributen mogelijk te maken.

Het aantal huidige en toekomstige zorgtoepassingen is groot en hierbij zijn veel verschillende entiteiten (o.a. zorgverlener, zorgaanbieder, leveranciers, burger) en daarmee veel verschillende kenmerken/attributen per entiteit betrokken. Een schaalbare, toekomstbestendige implementatie van deze zorgtoepassingen stelt hoge eisen aan de flexibiliteit. SSI biedt op dit gebied meer mogelijkheden dan PKI.

Bijlage 3: Uitwisselingsinfrastructuren in relatie tot TxN visie

Om antwoord te geven in hoeverre de meest relevante bestaande uitwisselingsinfrastructuren 'voldoen aan de TxN visie' worden deze in de paragrafen hieronder met de TxN-visie vergeleken. De vergelijking is gedaan door de implementatie van de generieke functies per laag van het Nictiz interoperabiliteitsmodel te vergelijken met de visie :

- Organisatie; de afspraken rondom het gebruik van vertrouwde partijen
- Proces: de afspraken rondom het gebruik van standaard-procedures
- Informatie: het gebruik van gestandaardiseerde identificatoren, codestelsels en metadata
- Applicatie: het gebruik van technologiestandaarden, in het bijzonder Verifiable Credentials
- Infrastructuur: het gebruik van infrastructuur

XDS en andere IHE-ITI profielen

Deze uitwisselingsinfrastructuren worden gebruikt bij o.a. de uitwisseling van de BgZ, bij beeldbeschikbaarheid en verschillende soorten documenten. Onderstaande vergelijking omvat de bestaande XDS-infrastructuren in Nederland.

Laag	**Aansluiting bij groeipad**	**Toelichting**
Organisatie-beleid	Midden	- Er wordt uitgegaan van onderling vertrouwen tussen uitwisselende zorgaanbieders. Dit leidt tot een beperkte schaalbaarheid van deze oplossing. - Niet overal wordt er al gebruik gemaakt van het UZI-register voor identificatie van zorgaanbieder en zorgverlener. eIDAS hoog middelen worden niet gebruikt.
Proces	Midden	- Niet overal wordt informatie over de gebruiker/verantwoordelijke meegegeven in de uitwisseling. Als er gebruik gemaakt wordt van gebruikersrollen, zijn dit geen landelijk afgestemde rollen. - Autorisatie Richtlijnen ontbreken vaak. In het Twiin afsprakenstelsel is een voorstel opgenomen voor een tijdelijke afspraak / groeipad. - Alle type zorgprocessen worden ondersteund
Informatie	Midden	- De uitgewisselde medische informatie kan voldoen aan de informatiestandaard, maar dit wordt niet afgedwongen. - Voor metadata en andere benodigde gegevens is er in het Twiin afsprakenstelsel een voorstel gemaakt, hier zitten nog wel enkele vrijheden in.

Applicatie	Laag	Er zijn nog niet voldoende IHE-profielen die aansluiten bij groeipad. Bestaande XDS-infrastructuren zullen daarom niet-IHE manieren/standaarden moeten implementeren die wel hierbij aansluiten.
Infrastructuur	Laag	Er zijn nog niet voldoende IHE-profielen die aansluiten bij groeipad. Bestaande XDS-infrastructuren zullen daarom niet-IHE manieren/standaarden moeten implementeren die wel hierbij aansluiten. GZN wordt niet overal gebruikt.

FHIR Notified pull

Hier wordt het traject bedoeld om infrastructuur- en zorgtoepassingsonafhankelijk dezelfde implementatie van het notified pull patroon te maken. Dit patroon kan in principe ingezet worden voor alle zorgtoepassingen, maar is beperkt tot een 1:1 uitwisseling tussen zorgaanbieders

Laag	**Aansluiting bij groeipad**	**Toelichting**
Organisatie-beleid	Midden	- Er wordt uitgegaan van onderling vertrouwen tussen uitwisselende zorgaanbieders. Dit leidt tot een beperkte schaalbaarheid van deze oplossing. - Niet overal wordt er al gebruik gemaakt van het UZI-register voor identificatie van zorgaanbieder en zorgverlener. eIDAS hoog middelen worden niet gebruikt.
Proces	Hoog	- Informatie over raadplegende gebruiker wordt meegegeven - Autorisatie Richtlijnen ontbreken vaak. In notified pull oplossingen wordt meestal uitgegaan van autorisatie op het niveau van de zorgaanbieder en lokale autorisatie. - Het ondersteunde zorgprocessen met notified pull betreft alleen de 1:1 uitwisseling tussen zorgaanbieders
Informatie	Midden	- De uitgewisselde medische informatie kan voldoen aan de informatiestandaard, maar dit wordt niet afgedwongen. - Voor metadata en andere benodigde gegevens wordt er in het Twiin afsprakenstelsel een voorstel gemaakt, hier zitten nog wel enkele vrijheden in..
Applicatie	Laag	Geen gebruik van standaard Verifiable Credentials voor verhogen zekerheid verklaringen die nodig zijn voor veilige gegevensuitwisseling.
Infrastructuur	Hoog	Afspraken zijn onafhankelijk van uitwisselingsinfrastructuur

AORTA/ LSP

Deze uitwisselingsinfrastructuur wordt toegepast bij o.a. de uitwisseling van medicatie, bij huisartswaarneming, ketenzorg, in de JGZ, acute zorg en de BgZ.

Laag	**Aansluiting bij groeipad**	**Toelichting**
Organisatie-beleid	Hoog	- Onderling vertrouwen tussen uitwisselende zorgaanbieders niet nodig. De aangesloten zorgaanbieders vertrouwen allen dezelfde intermediair (LSP). Dit leidt tot een betere schaalbaarheid van deze oplossing dan in het geval van onderling vertrouwen. - Overal wordt er al gebruik gemaakt van het UZI-register voor identificatie van zorgaanbieder en zorgverlener. eIDAS hoog middelen worden gebruikt.
Proces	Hoog	- Informatie over raadplegende gebruiker wordt meegegeven - Alle type zorgprocessen worden ondersteund
Informatie	Hoog	- LSP controleert op validiteit uitgewisselde medische informatie in relatie tot de informatiestandaard. - Voor metadata en andere benodigde gegevens volgt AORTA de vertrouwde uitgevers en heeft deels AORTA-specifieke metadata.
Applicatie	Laag	Geen gebruik van standaard Verifiable Credentials voor verhogen zekerheid verklaringen die nodig zijn voor veilige gegevensuitwisseling.
Infrastructuur	Hoog	Geen infrastructurele belemmeringen voor start implementatie Verifiable Credentials.

Nuts

Deze uitwisselingsinfrastructuur wordt momenteel toegepast bij de uitwisseling in het kader van eOverdracht en de geboortezorg.

Laag	**Aansluiting bij groeipad**	**Toelichting**
Organisatie-beleid	Midden	- Onderling vertrouwen tussen uitwisselende zorgaanbieders niet nodig. vertrouwen tussen zorgaanbieders wordt gerealiseerd door middel van cryptografie. - Wel onderling vertrouwen tussen de leveranciers van de aangesloten zorgaanbieders nodig. Dit leidt tot een betere schaalbaarheid van deze oplossing dan in het geval van onderling vertrouwen tussen zorgaanbieders - Mogelijkheid om gebruik te maken van het UZI-register

		voor identificatie van zorgaanbieder en zorgverlener maar dit wordt (nog) niet gebruikt - In de praktijk wordt gebruik gemaakt van authenticatie o.b.v. IRMA & BRP, wat (nog) niet is beoordeeld als eIDAS-hoog.
Proces	Hoog	- Informatie over raadplegende gebruiker wordt meegegeven - Gebruikersrollen worden nog niet ondersteund en autorisatierichtlijnen zijn niet afgestemd. - De ondersteunde zorgprocessen zijn alleen de 1:1 uitwisselingen tussen zorgaanbieders
Informatie	Midden	- Nuts controleert niet op validiteit uitgewisselde medische informatie in relatie tot de informatiestandaard. - Het voldoen aan informatiestandaarden wordt geborgd middels afspraken (zgn. Bolts) - Voor metadata en andere benodigde gegevens biedt Nuts ondersteuning voor vertrouwde uitgevers. Daarnaast heeft Nuts deels Nuts-specifieke metadata (o.a. did:nuts).
Applicatie	Hoog	Gebruik van standaard Verifiable Credentials voor verhogen zekerheid verklaringen die nodig zijn voor veilige gegevensuitwisseling.
Infrastructuur	Hoog	Infrastructuur wordt al ingezet voor gebruik Verifiable Credentials.

Conclusie

De conclusies die getrokken kunnen worden:

- De uitwisselingsinfrastructuur AORTA/LSP is op 4 van de 5 lagen redelijk in lijn met de TxN-visie. Met name op de laag Applicatie is doorontwikkeling (van laag naar hoog) benodigd om aan de TxN-visie te kunnen voldoen.
- De uitwisselingsinfrastructuur Nuts is op de lagen Infrastructuur en Applicatie volledig in lijn met de TxN-visie. Ook op de laag Proces is Nuts redelijk in lijn met de TxN-visie. Op de lagen Organisatiebeleid en Informatie is doorontwikkeling (van midden naar hoog) benodigd om aan de TxN-visie te kunnen voldoen.
- Uitwisseling op basis van FHIR notified pull is op de lagen Proces en Infrastructuur redelijk in lijn met de TxN-visie. Op de lagen Organisatiebeleid is Informatie door ontwikkeling van midden naar hoog benodigd en op de laag Applicatie is doorontwikkeling van laag naar hoog benodigd om aan de TxN-visie te kunnen voldoen.
- Bestaande Nederlandse IHE-XDS uitwisselingsinfrastructuren zijn op geen van de 5 lagen in lijn met de TxN-visie. Op alle 5 lagen is doorontwikkeling benodigd om aan de TxN-visie te kunnen voldoen.

Bijlage 4: Kwartaalplanning 2022-2023