Anna van Buerenplein 1
2595 DA Den Haag
Postbus 96800
2509 JE Den Haag

www.tno.nl

T +31 88 866 00 00

TNO-rapport

TNO 2022 R10707 | Eindrapport

Een nieuw perspectief voor vertrouwensmodellen in de zorg

Datum 14 april 2022

Auteur(s) Maaike van Leuken, Rieks Joosten

Aantal pagina's 29 (incl. bijlagen)
Opdrachtgever Zorginstituut Nederland
Projectnaam SSI voor ZIN
Projectnummer 060.51829

Managementuittreksel

Titel :	Een nieuw perspectief voor vertrouwensmodellen in de zorg
Auteur(s) :	Maaike van Leuken, Rieks Joosten
Datum :	14 april 2022
Rapportnr. :	TNO 2022 R10707

Net zoals in andere domeinen zorgt de digitalisering in de zorg ervoor dat steeds meer gegevens digitaal worden uitgewisseld, te denken aan medische gegevens over patiënten, maar ook gegevens over zorginstellingen. Dit heeft zijn weerslag op de efficiëntie en effectiviteit van zorgprocessen. Het digitaal uitwisselen van gegevens kan allerlei voordelen bieden, mits erop vertrouwd kan worden dat gegevens juist en geldig zijn, privacy gewaarborgd is, er aan de toepasselijke wet- en regelgeving is voldaan, enzovoorts. Onder een **vertrouwensmodel** verstaan we zaken als standaarden, raamwerken en afsprakenstelsels die zulk vertrouwen beogen te borgen. Voorbeelden zijn Twiin en NEN 7512, maar ook de eID, UZI-pas e.d. Bestaande vertrouwensmodellen lijken aan te nemen dat 'vertrouwen' voor iedereen hetzelfde betekent. Die aanname maakt het makkelijker om voor iedereen dezelfde (soort) vertrouwensmaatregelen te specificeren. Echter, een academisch onderzoek heeft behoefte aan een ander soorten vertrouwen dan een zorgverlener die patiënten moet overplaatsen, waarschijnlijk de oorzaak van de veelheid aan zulke vertrouwensmodellen. Kortom, meerdere factoren, waaronder het doel waarvoor de gegevens nodig zijn, hebben invloed op wat voor vertrouwen er nodig is in een gegevensuitwisseling.

In dit rapport kijken wij door een nieuwe bril naar vertrouwensmodellen: we zetten de individuele partij en diens subjectieve vertrouwen centraal. We nemen niet langer aan dat vertrouwen voor iedereen hetzelfde betekent, maar dat dit gekoppeld wordt aan specifieke soorten van interacties (transacties) die individuele partijen met anderen aangaan. Daarmee leggen we een basis voor zulke partijen om zelf regie te gaan voeren op wat ze wel en niet vertrouwen. Dit stelt hun in staat om beter maatwerk te leveren en zelf bepalen welke handelingen relevant zijn om hun beoogde resultaat te behalen. Het stelt ze echter tegelijk voor de opdracht om daar verantwoordelijkheid voor te nemen.

Ons vertrouwensmodel is gebaseerd op **Qualified Data Exhange** (**QDX**). Dat is een manier om na te denken over gegevensuitwisseling en wat daar verder bij komt kijken. Dat gaat niet alleen over syntax en semantiek maar ook over andere kenmerken van data die ze (on)geschikt maken om gebruikt te moeten of mogen worden in individuele transacties tussen twee individuele zorginstellingen of professionals. QDX gaat ook over governance en management processen waarin vraag en aanbod wordt geformuleerd, en op elkaar kan worden afgestemd.

De feitelijke gegevensuitwisseling kan (nog steeds) via verschillende modaliteiten plaatsvinden. Gegevens kunnen rechtstreeks bij de bron worden gevraagd, of middels een PGO-achtige app waarin de gebruiker deze gegevens over zichzelf al heeft verzameld.

We beschrijven een drietal technologische ontwikkelingen die wij denken dat hiervoor relevant zullen zijn. Eén daarvan zijn de ontwikkelingen die op dit moment haastig door de EU en lidstaten in gang worden gezet om een zogenaamde 'EUID wallet' beschikbaar te maken voor burgers, en grote(re) bedrijven te verplichten om burgers die van daaruit gegevens willen aanleveren hierin tegemoet te komen.[1] In combinatie met de nieuwe Europese verordening 'The European Health Data Space' met als doel de individuele partij meer controle te geven over hun eigen medische gegevens, zou dit als zo'n 'PGO-achtige app' kunnen kwalificeren. Hoe dat precies gaat passen binnen de zorg (en binnen het vertrouwensmodel) is op dit moment nog niet duidelijk.

We hebben middels twee use-cases (de verpleegkundige overdracht, en door het te vergelijken met KIK-V), op hoofdlijnen laten zien hoe dit model werkt. Wellicht kan dit rapport eraan bijdragen dat deze onderliggende visie breder gebruikt gaat worden en nog verder gaat worden uitgewerkt.

[1] In 2023 worden hier wallets voor aangewezen, die grote bedrijven dan in 2024 verplicht moeten kunnen accepteren. Wat er onder 'grote bedrijven' verstaan zal worden is nog niet gespecificeerd.

Inhoudsopgave

1 Achtergrond

In de zorg worden steeds meer gegevens digitaal uitgewisseld. Het gaat niet alleen om gegevens over de gezondheid of medische situaties van patiënten, maar bijvoorbeeld ook om gegevens van zorginstellingen (wie heeft waar nog een plekje voor een patiënt), of over de efficiency en effectiviteit van zorgprocessen. Het digitaal uitwisselen van gegevens mag dan allerlei voordelen (kunnen) bieden, maar je moet er wel op kunnen vertrouwen dat ze juist/geldig zijn, dat privacy is gewaarborgd, dat aan toepasselijke wet- en regelgeving is voldaan, enzovoorts. In dit rapport staat dat vertrouwen centraal.
Het Zorginstituut zet in op het ontwikkelen van een duurzame informatie-infrastructuur voor de zorg en het stimuleren van digitalisering en moderniseringen in de informatievoorziening. Dat betekent concreet dat als een zorgverlenende instantie een resultaat produceert ten behoeve van een zeker doel, dan moet die instantie kunnen garanderen dat dit resultaat *valide* is voor dat doel. Als voor het produceren van dat resultaat gegevens nodig zijn c.q. verwerkt moeten worden, dan moet de organisatie er ook van op aan kunnen dat die gegevens *valide* zijn. Dat blijkt niet alleen uit de juiste syntax en semantiek, maar ook doordat de gegevens aan ander validiteitscriteria voldoen, *die specifiek zijn voor de context waarin de gegevens worden gebruikt*. In de context waarbij gekeken wordt of een patiënt naar een andere zorginstelling verplaatst kan worden moeten gegevens bijvoorbeeld op een betrouwbare manier (en door een betrouwbare partij) tot stand gekomen zijn, ze moeten van toepassing zijn op de te verplaatsen persoon, de diagnostische gegevens moeten nog steeds op de patiënt van toepassing zijn, enzovoorts.
Binnen de zorg wordt regelmatig gesproken over vertrouwensmodellen[2] en eigenschappen die ze zouden hebben. De meest concrete lijken Twiin, en de combinatie van de NEN 7510, NEN 7512 en NEN 7513 standaarden te zijn, maar stelsels rondom eID, UZI-pas e.d. worden daar ook wel onder verstaan. Wat opvalt aan deze vertrouwensmodellen is de aanname dat 'vertrouwen' voor iedereen hetzelfde betekent, en dat de contextafhankelijkheid niet of nauwelijks wordt genoemd. Bijgevolg wordt als 'holy grail' dat ene vertrouwensmodel gezocht dat iedereen kan gebruiken: een 'one size fits all'. Dat dit in de praktijk gemakkelijk leidt tot 'maatwerk' en/of het opzoeken van de grenzen van wat nog mag, laat zien dat zulke aannames niet (goed) werken. We zien dan ook dat de voornoemde vertrouwensmodellen nog ruimte laten zodat zorginstellingen dit naar hun eigen contexten kunnen doorvertalen. Dat brengt het risico met zich mee dat ze zich wellicht meer bezighouden met het 'compliant zijn' dan met de kernvraag, d.w.z. met de (context afhankelijke) condities die vervuld moeten zijn om gegevens-uitwisselingen *valide* te doen zijn.
Het Zorginstituut (ZIN) heeft TNO gevraagd een toekomstbestendig vertrouwens-model te schetsen die aansluit bij huidige ontwikkelingen, met daarbij een overzicht van de benodigde onderdelen en criteria voor een robuust vertrouwensmodel. Het model is toegepast in twee scenario's voor validatie en het illustreren van de werking. Het eerste scenario is de verpleegkundige overdracht, waarin zichtbaar wordt hoe het model invulling kan krijgen. Het tweede scenario is KIK-V, waarbij het

[2] Twiin definieert 'vertrouwensmodel' als: het geheel van technische, organisatorische en juridische waarborgen voor het vertrouwen in de landelijke elektronische uitwisseling van medische gegevens.

ontwikkelde model wordt vergeleken met het huidige KIK-V model. Verder zijn er aanbevelingen gedaan over middelen die gebruikt kunnen worden om het model te realiseren en over het volgen van technologische ontwikkelingen. Hieronder is een overzicht te vinden van deze stappen in de vorm van onderzoeksvragen.
Onderzoeksvragen:

- Wat zijn de criteria voor het waarborgen van vertrouwen in het vertrouwensmodel?
- Wat zijn de onderdelen van een vertrouwensmodel dat aan deze criteria invulling geeft?
- Hoe werken deze onderdelen samen in een aantal scenario's voor gegevensuitwisseling in de zorg?
- Hoe worden de vertrouwensmodellen toegepast in deze scenario's? Welke afspraken en governance is hierbij noodzakelijk?
- Wat zijn middelen waarmee een vertrouwensmodel gerealiseerd kan worden, wat is er? Wat moet ontwikkeld worden?
- Wat zijn interessante technologische ontwikkelingen en welke daarvan worden aanbevolen om daarvan in de gaten houden?

2 Doel

Het doel van het onderzoek is om een aanzet[3] te vinden voor handvatten die individuele zorginstellingen c.q. zorgverleners in willekeurige situaties[4] kunnen gebruiken om te borgen dat het (elektronisch) uitwisselen van medische en niet-medische gegevens gebeurt op een efficiënte en doelmatige manier, binnen de vigerende wetten, regels en standaarden, en die passend is voor de betrokkenen en de situatie waarin ze verkeren. Het idee is dat het operationaliseren van zulke handvatten door individuele partijen gaat leiden tot een collectief ervaren appreciatie van de kwaliteit van de gegevensuitwisseling.

[3] Het omvang van het project is te klein om veel meer dan een aanzet te geven.
[4] Vaak zijn vertrouwensmodellen gericht op bepaalde klassen van situaties, bijv. binnen de curatieve zorg. Daarmee is zo'n model mogelijk niet of minder bruikbaar in andere contexten, zoals onderzoek.

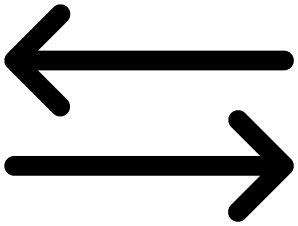
3 Aannames bekeken door een andere bril

Zoals eerder genoemd zijn er al verschillende vertrouwensmodellen binnen de zorg. Het gaat hier doorgaans om regels (afsprakenstelsels) die het vertrouwen borgen zolang alle betrokkenen zich er tenminste aan houden. Dat gaat op hoofdlijnen wel goed, maar het venijn zit steeds weer in de details. Zo werkt het voorschrift om het BSN te gebruiken voor patiëntidentificatie doorgaans heel goed, maar pasgeborenen of buitenlanders hebben niet altijd (al) zo'n BSN (zie Twiin). Voor alle situaties – en dat zijn er heel veel – waarin een regel of voorschrift niet werkt is maatwerk nodig. Dit heeft ertoe geleid dat er een heleboel verschillende vertrouwensmodellen zijn voor verschillende toepassingen, waardoor de zorgverlener, die in meerdere van deze toepassingsdomeinen werkzaam is, bij verschillende gegevensuitwisselingen op zoek moet gaan naar verschillende vertrouwensmodellen.
Wij stellen daarom voor om door een andere bril naar hetzelfde probleem te kijken ('omdenken'). In plaats van 'top-down' te kijken wat er doorgaans nodig is (bijvoorbeeld het voldoen aan wet- en regelgeving), gaan we na wat individuele partijen (mensen, organisaties) nodig hebben om gegevens die in een interactie van belang zijn, te kunnen vertrouwen. Stel je voor dat je de verpleegkundige bent in verpleeghuis 'Zonneschijn' die moet besluiten of meneer Pieterse komende maandag opgenomen kan worden. Om te beginnen moet je dan weten wat meneer Pieterse aan zorg nodig heeft (en of die dan geleverd kan worden). Maar je moet ook weten wat er nodig is om zulke gegevens te vertrouwen. Als de melding telefonisch doorkomt en je herkent de persoon aan de andere kant van de lijn als een eerste klas verpleegkundige, dan is dat vaak voldoende. Maar ken je de persoon niet, dan is het theoretisch mogelijk dat je te maken hebt met de partner van meneer Pieterse die probeert hem geplaatst te krijgen terwijl hij daar (nog) geen recht op heeft.
Zulke uitwisselingen vinden steeds plaats binnen de context van wat we een **transactie** noemen. Doorgaans betekent dit "(een combinatie van) producten, diensten, of geld", maar het laat zich gemakkelijk uitbreiden met (bijvoorbeeld) gegevens (en patiënten). Elke transactie kent drie fases[5]:

1. een onderhandelingsfase waarin partijen de 'transactie-overeenkomst' tot stand brengen (die hoeft niet altijd op papier te staan), EN besluiten zich daaraan te verbinden (of er mee op te houden);
2. de uitvoeringsfase, waarin elke deelnemer aan de slag gaat om zijn deel van de transactie na te komen en de verwachtte resultaten op te leveren, en

[5] Dit model is ontleend aan DEMO (Design & Engineering Methodology for Organizations). Dit is een methode om bedrijfsprocessen te beschrijven, waarbij het handelen van mensen centraal staat.

3. de afrondingsfase, waarin elke deelnemer checkt of hij heeft gekregen wat hij verwachtte, (eventueel nog correcties aan kan laten brengen) EN besluit de resultaten te accepteren (dan wel te escaleren).



Transactie

1. Onderhandelingsfase → transactie-overeenkomst
2. Uitvoeren zodat eigen deel contract wordt nageleefd → resultaten delen
3. Evaluatie à besluit om resultaten te accepteren of te bediscussiëren

We zien dat in fases 1 en 3 besluiten worden genomen. Om een besluit te kunnen nemen zijn gegevens nodig, en die moeten uiteraard vertrouwd kunnen worden door de partij die dat besluit neemt. In fase 2 kan het nodig zijn dat gegevens worden gebruikt om een resultaat te produceren, en ook die moeten vertrouwd kunnen worden door de partij die het resultaat produceert. We concluderen dan ook dat:

De kern van vertrouwen is gelegen in het vermogen om gegevens te valideren, d.w.z. om zelf vast te kunnen stellen of een (verzameling) gegeven(s) geschikt is om voor een specifiek, zelf gesteld doel (besluit, resultaat) te worden gebruikt.

We merken op dat transacties niet alleen tussen verschillende partijen plaatsvinden, maar ook binnen de context van individuele partijen, bijvoorbeeld als het transactie-onderwerp tussen afdelingen wordt verplaatst, of tussen een medewerk(st)er en een IT-systeem.
Wie zich er rekenschap van geeft dat al dit soort transacties van elkaar verschillen, heeft een gerede kans om de moed in de schoenen te voelen zakken: het lijkt zo onbehapbaar, zo kansloos, zo'n onbegonnen werk. Daarom is het belangrijk om een begin te maken met het ontwerpen van een vertrouwensmodel dat in individuele interacties kan worden gebruikt. En we zullen zien hoe we dankbaar gebruik maken van het werk dat is verzet bij het maken van bestaande (of nog in ontwikkeling zijnde) modellen en afsprakenstelsels.

3.1 Een nieuwe bril

Om een goed begin te kunnen maken is het nodig dat we eerst wat terminologie[6] te introduceren op een manier waarvan we verwachten dat verschillende lezers daar hetzelfde onder verstaan – dat spreekt niet vanzelf[7]. Geïnteresseerden kunnen de achterliggende ideeën en samenhangen nalezen in het Parties, Actors and Actions (PAA) denkmodel[8].
Een **entiteit** (d.w.z.: iets dat bestaat) noemen we een **partij** als die eigen doelen stelt, een eigen kennis onderhoudt, die kennis gebruikt om die doelen te behalen, op dat alles op een autonome (een soevereine) manier. Dat zijn typisch mensen en

[6] De dikgedrukte woorden in dit rapport zijn termen die we expliciet hier definiëren, of ze zijn gedefinieerd in de eSSIF-Lab glossary, of beiden.
[7] Joosten, 2021: "On Terminology, and the Resolution of Related Issues". TNO. Report R11793.
[8] Zie het eSSIF-Lab Parties, Actors and Actors model voor een uitgebreide en complete beschrijving van dit model.

organisaties. Een entiteit noemen we een **actor** als die handelingen kan uitvoeren. Typische voorbeelden zijn mensen en machines (computers). Een **handeling** is elke eenheid van werk die binnen een zekere context door één actor, namens één partij wordt uitgevoerd als een enkelvoudige (ondeelbare) operatie[9]. Een voorbeeld is het ondertekenen van een brief.
Organisaties kwalificeren niet als actor omdat ze geen handelingen kunnen uitvoeren. TNO bijvoorbeeld heeft nog nooit een contract getekend of een medewerker aangenomen – daar is een actor voor nodig die dit soort handelingen namens TNO verricht, zoals een persoon die lid is van de RvB, of de rol van HR-medewerk(st)er vervult. We kunnen overigens best het gangbare taalgebruik blijven hanteren waarin organisaties gewoon handelingen verrichten (als in: "TNO heeft vandaag 5 medewerkers aangenomen"). We moeten ons dan wel realiseren dat de *eigenlijke* betekenis hiervan is dat er een actor bestaat die deze handeling namens de organisatie verricht.
Mensen kwalificeren niet alleen als actor (ze kunnen immers handelingen uitvoeren) maar ook als partij (ze hebben immers eigen doelstellingen, onderhouden een eigen kennis, enzovoorts). Als een persoon een handeling uitvoert, kan hij/zij dat doen namens zichzelf, maar ook namens een andere partij, bijvoorbeeld diens werkgever.
Omdat elke handeling wordt uitgevoerd namens één partij, bepaalt die partij ook de regels (werkinstructies, beleidsregels, andere richtlijnen – dat is onderdeel van diens kennis) volgens welke een actor die handeling moet uitvoeren. Die regels gaan bijvoorbeeld over hoe een zeker besluit genomen moet worden, welke gegevens daarvoor nodig zijn, wanneer iets 'waar' is, onder welke voorwaarden die gegevens **valide** zijn, d.w.z. tot een geldig/juist besluit leiden, enzovoorts. Actoren worden geacht die regels te volgen. Bij het opstellen van die regels wordt aangenomen dat de uitvoerende actoren al over zekere kennis (en kunde) beschikken, die daarom niet alsnog gespecificeerd hoeft te worden. Een werkinstructie over het toedienen van medicatie gaat dan ook niet over hoe een pil, druppels, een spuit e.d. moeten worden toegediend, maar meer over de plaats, tijd en omstandigheden waarin dat moet gebeuren. Er is van uit gegaan dat de mensen (actoren) die dat doen zelf wel weten hoe ze pillen, druppels, of een spuit moeten worden toegediend. Ook een robot of computer (actor) beschikt zelf over kennis (zijn programmacode), en die wordt ingezet volgens de regels ('policies') van de persoon of organisatie (partij) die ze gebruikt.
Volgens deze denkwijze zijn partijen volstrekt autonoom (soeverein) als het gaat om hun kennis (doelen, werkvoorschriften, enz.). Dat gaat zelfs zó ver dat een partij zich niet (meer) achter wet- en regelgeving kan verschuilen. Een partij kiest (bewust of onbewust) zelf of, c.q. in hoeverre hij zich aan welke regels houdt. Dat dit ook werkelijk zo is zal iedereen beamen die wel eens te hard, of door rood licht gereden heeft, of die zich krantenartikelen herinnert waarin organisaties (weer) 'de fout in zijn gegaan'.
Wij nemen deze autonomie als uitgangspunt. Het betekent dat elke zorginstelling, zorgverlener en andere partij zelf bepaalt wat zijn missie en andere doelen zijn, wat en hoe dingen worden gedaan, en welke regels al dan niet worden nageleefd. Maar ook met welke andere partijen ze interacties doen, wat (en hoe) zij daarin doen, en welke gegevens ze met elkaar uitwisselen. En, ons beperkend tot deze gegevens, zal elke partij dan ook voor zichzelf – op technisch, organisatorisch en juridisch vlak – moeten waarborgen dat de gegevens die ze krijgt door haar vertrouwd kunnen

[9] Zie: "Praktijkboek voor Procesarchitecten", van Gorcum, 2002. Handelingen zijn de basisblokken waaruit processen en procedures worden samengesteld.

worden, en gegevens die ze beschikbaar maakt voor anderen de eigenschappen hebben die ze voor die ander voldoende betrouwbaar maken.

4 Qualified Data Exchange (QDX)

Bij een goede gegevensuitwisseling komt heel wat kijken. Uiteraard moeten gegevens, zoals de naam of het adres van een persoon, de juiste syntax en semantiek hebben ('semantische interoperabiliteit'). Maar dat is niet voldoende. In sommige gevallen is het ook nodig om te weten wie deze gegevens heeft vastgesteld (bijv. de overheid, een bank, een ziekenhuis), of met welke methode (bijv. voor een bloedgroepbepaling).
We introduceren de term **Qualified Data Exchange** (**QDX**) voor een gegevens-uitwisseling waarbij niet alleen naar gegevens wordt gevraagd die een bepaalde syntax en semantiek hebben, maar ook zodanige eigenschappen hebben dat ze zich kwalificeren als 'valide' om te worden gebruikt voor het doel waarvoor ze werden gevraagd. Daar valt dan ook het aanbieden van gegevens onder die (naast de goed gedefinieerde syntax en semantiek) eigenschappen hebben op basis waarvan een gegevensvrager kan nagaan of ze zich kwalificeren als 'valide' om voor een of meer van zijn doeleinden te kunnen worden gebruikt. Laten we dit eens bekijken vanuit de twee bijbehorende perspectieven, namelijk die van de gegevensvrager (gegevensconsument) en de gegevensaanbieder (gegevensleverancier):

4.1 Perspectief van de Gegevensvrager

De gegevensvrager heeft gegevens nodig omdat hij er iets specifieks mee wil doen, zoals het nemen van een besluit. Een zorginstelling die gevraagd wordt een patiënt op te nemen, moet bijvoorbeeld besluiten of dat wel kan (en mag). Om dat besluit te nemen heeft de instelling gegevens nodig (bijvoorbeeld de diagnose), en die gegevens moeten **valide** zijn om dat besluit mee te nemen, zodat het besluit zelf ook geldig is. In het voorbeeld is dus ook zekerheid nodig dat de diagnose die patiënt betreft (en geen andere), dat die is gesteld door een persoon die daartoe bekwaam en bevoegd is, dat de diagnose nog steeds geldig is, e.d.
De gegevensvrager is dus op zoek naar **qualified data**, d.w.z. een gegeven dat zich kwalificeert als valide om te worden gebruikt voor het doel dat de gegevensvrager nastreeft. Over zo'n gegeven bestaat dan zekerheid over een of meer eigenschappen, zoals de herkomst en de integriteit van het gegeven, de wijze waarop het tot stand gekomen is, e.d.
Kortom, het perspectief van de gegevensvrager is erg subjectief en doel- en context-afhankelijk.

4.2 Perspectief van de Gegevensaanbieder

De gegevensaanbieder beschikt over gegevens die het voor anderen beschikbaar wil maken (bijvoorbeeld diagnoses), maar weet vaak niet waartoe die anderen de gegevens willen gaan gebruiken, laat staan welke validiteitscriteria ze daarbij hanteren.[10] De gegevensaanbieder zal op een of andere manier moeten zorgen dat de gegevensvrager er achter kan komen over welke kwalificaties zijn gegevens beschikken, zodat hij kan besluiten of ze bruikbaar zijn voor zijn doeleinden.

[10] Oorzaak hiervan is bijvoorbeeld dat de gegevens meervoudig gebruikt moeten kunnen worden (een van de doelstellingen van het Informatieberaad Zorg). Een arts kan vanuit zijn professionaliteit misschien nog wel weten wat een andere arts (ongeveer) nodig heeft, maar weet dat niet voor bijvoorbeeld een onderzoeker, beleidsmedewerker etc.

Dat is niet zo abstract als het lijkt: in winkels zie je ook hoeveel en hoelang je garantie krijgt op een product, wat de producteigenschappen zijn en andere gegevens die klanten zoal gebruiken om te besluiten of ze het product kopen (i.e.: gaan gebruiken). En hoewel de keuze van de soorten gegevens die aan de klant worden getoond aan de aanbieder is (en dus subjectief), zijn de gegevens zelf dat (voor een eerlijke aanbieder) niet: ze zijn (idealiter) objectief vastgesteld (en te verifiëren).

4.3 QDX Governance

Een medewerk(st)er of IT systeem van een zorgorganisatie die (run-time[11]) gegevens nodig heeft om (bijvoorbeeld) een besluit te nemen, moet dus weten welke gegevens dat zijn, en welke validiteitscriteria daar bij horen. Zulke criteria moeten dan al eerder (design-time[12]) zijn vastgesteld en op een adequate manier voor deze 'actoren' beschikbaar zijn gemaakt. Tijdens design-time worden er dus keuzes gemaakt die het run-time uitwisselen van (valide) gegevens mogelijk (of onmogelijk) maken.
Onder **QDX governance** verstaan we het design-time proces dat *een partij in de rol van gegevensvrager* uitvoert, en waarin deze vaststelt wat de validiteitscriteria zijn voor de gegevens die moeten worden uitgevraagd bij een zeker type transactie. Daarbij zal de gegevensvrager de risico's van de transactie in ogenschouw nemen die het gevolg kunnen zijn van gegevens die onjuist zijn, niet over het juiste 'subject' betrekking hebben, te gedateerd zijn, onbetrouwbaar zijn (volgens het oordeel van de gegevensvrager uiteraard), enz. En om zulke risico's te mitigeren zullen (validiteits)eisen aan de gegevens worden gesteld, zoals welke de betrouwbare gegevensleveranciers zijn, of het nodig is te weten welke persoon de gegevens heeft vastgesteld en wat diens kwalificaties zijn, gegevens over de identiteit van het 'subject', e.d.
Pas nadat de validiteitscriteria zijn vastgesteld, kan per type transactie (interactie-handeling) de gegevensbehoefte als concrete vraag worden geformuleerd in termen van (a) welk soort gegevens zijn nodig, (b) van welke partijen mogen die komen, en (c) en met welke eigenschappen deze gegevens moeten komen zodat ze als 'valide' kwalificeren.[13]
De persoon die deze criteria opstelt moet dan uiteraard wel kunnen weten welke partijen welk soort gegevens kunnen en willen leveren (syntax, semantiek), uit welke eigenschappen van gegevens blijkt dat ze aan (onderdelen van) de validiteitscriteria voldoen, en ook: waar en hoe die gegevens dan te krijgen zijn en onder welke condities ze worden geleverd.

---

[11] Dat is: in het operationele werk, als er dus in één specifieke situatie door één specifieke actor één (echt) besluit wordt genomen.
[12] Dat is: in het voorbereidende werk. Dat is onderdeel van activiteiten horend bij (het risico-management onderdeel van) procesontwerp en/of informatie-modellering.
[13] De W3C Recommentation voor Verifiable Credentials heeft hier de properties 'credentialSubject', 'proof' en 'evidence' voor.

Gegevensvrager

QDX governance
Stelt vast (a) welk soort gegevens hij wilt ontvangen, (b) aan welke validiteitscriteria deze gegevens zouden moeten voldoen, (c) van welke partijen mogen die komen en (d) voor welk doel de gegevens gebruikt gaan worden.

4.4 QDX Management

Onder **QDX management** verstaan we het design-time proces dat *een partij in de rol van gegevensleverancier* uitvoert, en waarin deze vaststelt (a) welk (soort) gegevens hij wil en zal gaan uitgeven, (b) met welke 'zekerheden' deze gegevens zullen worden geleverd, en (c) waar en hoe ze geleverd gaan worden, en onder welke condities.
Dit kan vervolgens worden vastgelegd in een **advertentie** die terug te vinden is in een (of meerdere) credential catalogue(s). Een **credential catalogue** is een verzameling van advertenties van gegevensaanbieders, waar de gegevensaanbieder doorheen kan kijken om een potentiële match te vinden[14]. De Data Catalog Vocabulary (DCAT), een W3C aanbeveling voor standaardisatie, is een goed startpunt voor het maken van advertenties. Data catalogues kunnen gebruik maken van deze standaard, zodat gegevens vindbaar zijn (volgens het FAIR vindbaarheidsprincipe) en er generieke structuur in zit, zoals wie welke gegevens aanbiedt onder welke toegangsrechten. Wij zien een credential catalogue als een uitbreiding op een data catalogue, namelijk een credential catalogue is een data catalogue met de zekerheden die bij de gegevens geleverd zullen worden[15].

Vervolgens moet natuurlijk ook de feitelijke uitgifte van gegevens worden ingericht. Dat gaat dan om het opstellen en onderhouden van uitgifteprocessen en (bij handmatige processen) de bijbehorende werkinstructies, en/of (bij elektronische uitgifte) de bijbehorende IT-systemen/componenten.

Gegevensaanbieder

QDX management
Stelt vast (a) welk soort gegevens hij wil en zal gaan uitgeven, (b) met welke zekerheden deze gegevens zullen worden geleverd, en (c) waar en hoe ze geleverd gaan worden, en onder welke condities.

[14] We gaan er hier vanuit dat een credential catalogue alleen *advertenties* bevat. Een credential catalogue zou ook *uitnodigingen* kunnen bevatten, namelijk de vraag van de gegevensvrager.
[15] Misschien is het al mogelijk om in de huidige data catalogues al zekerheden te verwerken. Dit zou nader onderzocht kunnen worden.

4.5 QDX Matching

Onder **QDX matching** verstaan we de activiteiten die partijen in hun rollen als gegevensvrager en leverancier ontplooien tijdens design-time om vraag en aanbod van gegevens op elkaar af te stemmen. Dat lijkt wel op 'semantische interoperabiliteit', waar syntax en semantiek van gegevens wordt afgestemd, hetgeen dan leidt tot een gestandaardiseerd aanbod waar de gegevensvragers zich dan vervolgens (run-time) aan conformeren. Maar hier gaat het nadrukkelijk óók om af te stemmen wat de bijbehorende zekerheden zijn die meegeleverd kunnen of moeten worden, en hoe een gegevensvrager die kan verifiëren om de 'gewone' gegevens mee te valideren.
Het afstemmen van vraag en aanbod van gegevens is conceptueel hetzelfde als het afstemmen van vraag en aanbod van willekeurige andere producten (of diensten). Er zijn dan ook verschillende manieren om dat gestalte te geven. Het kan bijvoorbeeld 'op afstand', waarbij een gegevensleverancier zijn gegevens ('producten') adverteert en afwacht wie ze gaat afnemen, en de gegevensvrager op een of andere manier die advertenties langs ziet komen (als 'spam', of omdat hij er naar heeft gezocht) en dan kijkt wat hij kan gebruiken. Een credential catalogue kan hierbij een nuttige rol vervullen.
In de zorg ligt het voor de hand om dit binnen (bestaande) samenwerkingsvormen (communities) in te richten, omdat naarmate je al meer samenwerkt de wederzijdse behoefte om tot een werkbare afstemming te komen veel groter is. We kunnen voor elk bestaand samenwerkingsverband een **QDX community** introduceren, die zich tot doel stelt om het idee van QDX voor de deelnemende organisaties te gaan faciliteren. Het kan dan bijvoorbeeld gaan om het beschikbaar maken van een credential catalogue (waarin de gegevensaanbieder zijn advertentie zet en waardoor de gegevensvrager kan gaan bladeren), het bijdragen aan of het faciliteren van (QDX-enabled) berichten, het ondersteunen van partijen bij het aanpassen van hun bestaande IT, enzovoorts. Hoe dit het best vorm kan krijgen moet echter wel verder worden onderzocht.

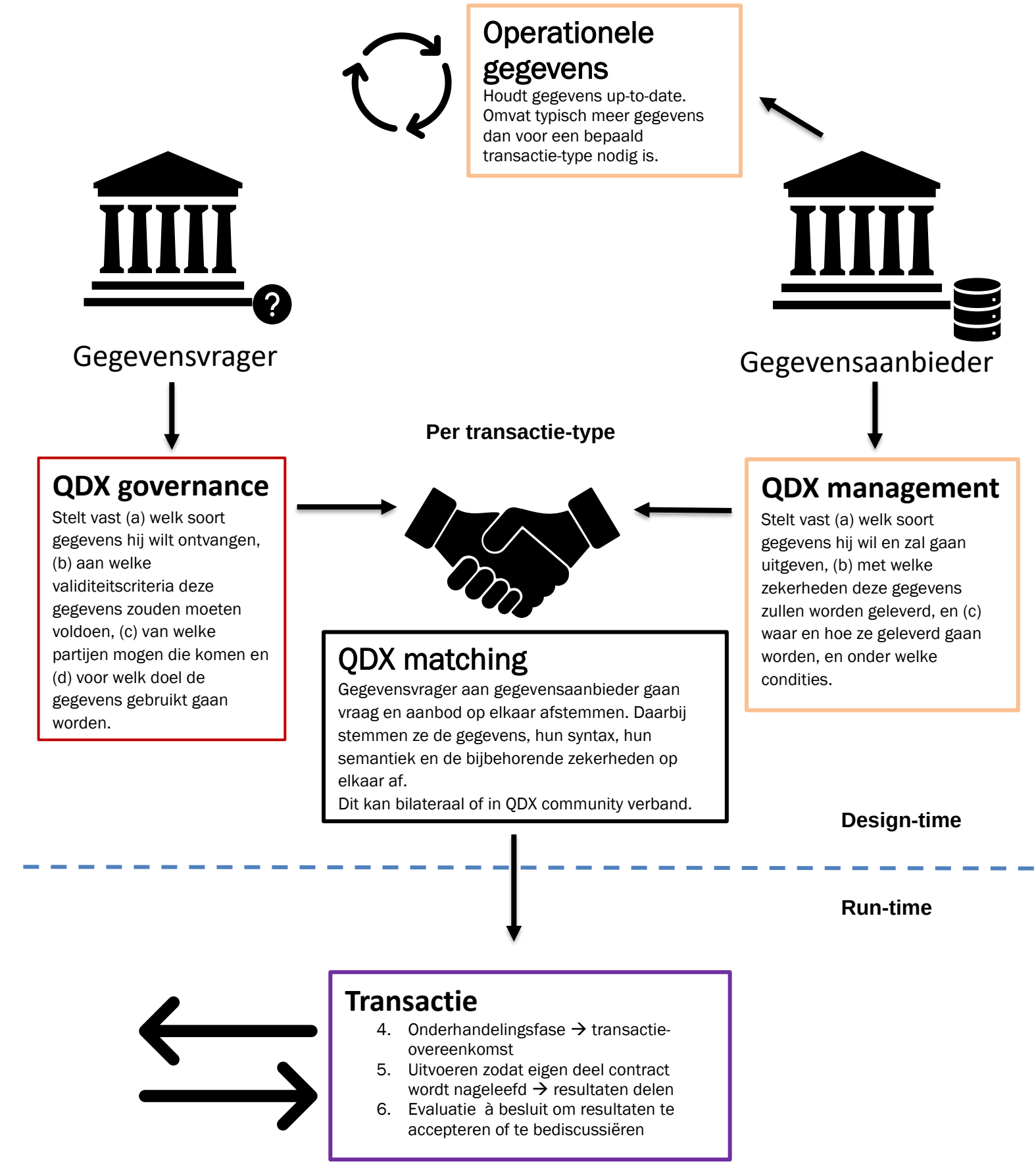
QDX matching

Gegevensvrager aan gegevensaanbieder gaan vraag en aanbod op elkaar afstemmen. Daarbij stemmen ze de gegevens, hun syntax, hun semantiek en de bijbehorende zekerheden op elkaar af. Dit kan bilateraal of in QDX community verband.

4.6 Gegevensuitwisseling

Na de design-time processen (QDX governance, QDX management en QDX matching) hebben we alles wat er nodig is om run-time gegevens uit te wisselen die het doel dienen van de gegevensvrager. Er kan een transactie plaatsvinden.

Dit vertrouwensmodel is op de volgende pagina grafische weergegeven.


Operationele gegevens
Houdt gegevens up-to-date. Omvat typisch meer gegevens dan voor een bepaald transactie-type nodig is.
Gegevensvrager
Gegevensaanbieder
Per transactie-type
QDX governance
Stelt vast (a) welk soort gegevens hij wilt ontvangen, (b) aan welke validiteitscriteria deze gegevens zouden moeten voldoen, (c) van welke partijen mogen die komen en (d) voor welk doel de gegevens gebruikt gaan worden.
QDX management
Stelt vast (a) welk soort gegevens hij wil en zal gaan uitgeven, (b) met welke zekerheden deze gegevens zullen worden geleverd, en (c) waar en hoe ze geleverd gaan worden, en onder welke condities.
QDX matching
Gegevensvrager aan gegevensaanbieder gaan vraag en aanbod op elkaar afstemmen. Daarbij stemmen ze de gegevens, hun syntax, hun semantiek en de bijbehorende zekerheden op elkaar af.
Dit kan bilateraal of in QDX community verband.
Design-time
Run-time
Transactie
4. Onderhandelingsfase → transactie-overeenkomst
5. Uitvoeren zodat eigen deel contract wordt nageleefd → resultaten delen
6. Evaluatie à besluit om resultaten te accepteren of te bediscussiëren

5 Een model voor Vertrouwen

Eerder zeiden we al dat de kern van vertrouwen (voor gegevensuitwisselingen) is gelegen in het eigen vermogen om gegevens te valideren, d.w.z. om zelf vast te kunnen stellen of een (verzameling) gegeven(s) geschikt is om voor een specifiek, zelf-gesteld doel (besluit, resultaat) te worden gebruikt. Daarmee zeggen we ook dat vertrouwen iets is van individuele partijen: elke partij besluit zelf wie/wat te vertrouwen is. En dat hangt af van allerlei factoren, zoals de context, gerelateerde risico's e.d. En die veranderen continu.
Het is niet praktisch als elke partij bij elke gegevensuitwisseling daarbij stil moet staan, omdat dit de bedrijfsprocessen stremt. Maar het is ook niet handig als een partij in elke situatie steeds dezelfde criteria hanteert, of slechts een heel beperkt aantal variaties. Dan komt het maatwerk dat vaak nodig is in het gedrang. We zoeken dus naar een manier waarop iedere partij zijn eigen 'middenweg' kan vinden. Feitelijk zijn we dus op zoek naar manieren waarop individuele partijen hun QDX governance, management en matching kunnen doen.
We memoreerden al dat bestaande vertrouwensmodellen c.q. afsprakenstelsels niet dé oplossing zijn. Maar dat maakt ze nog niet onbruikbaar. Vooral waar ze concreet worden (zoals een aantal van de beheersmaatregelen van NEN 7512) bieden ze aanknopingspunten waar binnen een van de QDX-processen gebruik van gemaakt kan worden. Wat een partij wel of niet bruikbaar vindt, zal afhangen van de soorten transacties waar hij bij betrokken is. Ook op dit punt zouden QDX-communities een ondersteunende rol kunnen spelen omdat de kans best wel groot lijkt, dat per community dezelfde onderdelen van wat er reeds bestaat aan stelsels en modellen bruikbaar zullen zijn.
De zekerheden waarmee gegevens worden geleverd kunnen op verschillende manieren gestalte krijgen. Zo kan bijvoorbeeld de zekerheid dat een gegeven van een zekere andere partij komt, worden afgeleid uit het communicatiekanaal, als het eindpunt van dat kanaal tenminste als liggend bij die partij kan worden geauthentiseerd. Bij elektronische communicatiekanalen kan dat bijvoorbeeld middels PKI-certificaten (SSL/HTTPS verbindingen). Als je het gegeven in een vestiging van die partij ophaalt, weet je het ook. Maar een dergelijk gegeven kan ook op een drager met echtheidskenmerken worden verstuurd en/of met stempels en handtekeningen. Of als een 'verifiable credential' (een digitaal bericht dat een onvervalsbaar bewijs heeft van integriteit (het bericht is niet veranderd sinds het werd gemaakt) en herkomst (de uitgever/afzender van het bericht kan worden vastgesteld)).
Een andere vorm van zekerheid kan zijn dat gegevens binnen een VPN-achtig netwerk worden gecommuniceerd, en waar partijen alleen berichten in mogen stoppen en af mogen halen als ze zich verplicht hebben aan de regels die daarvoor gelden. Dat zou dan geen 'one-size-fits-all-netwerk' moeten zijn, maar eentje dat bijvoorbeeld weer door zo'n QDX community wordt gerund, omdat je dan het meest efficiënt en effectief de zekerheden kunt organiseren die binnen de community nodig zijn (en vaak ook al worden gebruikt).

6 Hoe ziet dat eruit?

We gaan het vertrouwensmodel hierboven toetsen op twee manieren, namelijk (1) het invullen van het model aan de hand van een concrete use case: de verpleegkundige overdracht en (2) het vergelijken van het QDX model met KIK-V.

6.1 Verpleegkundige Overdracht

Om patiënten te kunnen overdragen van een zorginstantie naar een andere wordt eOverdracht gebruikt. Dit probeert door middel van afspraken over de verpleegkundige overdracht de continuïteit en veiligheid van zorg te kunnen waarborgen. De **versturende** (of 'latende') **partij**, d.w.z. de partij die de zorgpatiënt wilt overdragen naar de **ontvangende partij**, stuurt een aanmeldingsbericht naar de ontvangende partij waarmee die het besluit zou moeten kunnen nemen of ze ruimte heeft om de patiënt te kunnen ontvangen. Hier is dus de versturende partij de gegevensaanbieder en de ontvangende partij de gegevensvrager.
Eerder hadden we het voorbeeld over de verpleegkundige werkende bij verpleeghuis 'Zonneschijn'. Meneer Pieterse woont momenteel nog thuis in Delden en dagelijks komt de wijkverpleging uit Hengelo bij hem langs om hem zowel verpleging als verzorging te geven. Zijn situatie is echter achteruitgegaan waardoor hij intensiever verpleging en verzorging nodig heeft dan de wijkverpleging kan bieden. Verpleeghuis Zonneschijn heeft gegevens nodig van de wijkverpleging, zodat (de verpleegkundige van) het verpleeghuis kan besluiten of meneer Pieterse komende maandag geplaatst kan worden. Hier is (de verpleegkundige van)[16] het verpleeghuis Zonneschijn de gegevensvrager en de (verpleegkundige van de)[17] wijkverpleging de gegevensaanbieder. In nog andere termen: verpleeghuis Zonneschijn ontvangt de patiënt en is daarmee de ontvangende partij, terwijl de wijkverpleging de versturende partij noemen.

6.1.1 QDX Governance door het Verpleeghuis Zonneschijn

Om vast te stellen of een patiënt overgedragen kan worden, zijn er verschillende gegevens met zekerheden nodig die tijdens QDX governance worden vastgesteld, zoals de persoonsgegevens[18] van de patiënt (BSN, geslacht, leeftijd), de ontvangstdatum en zijn/haar zorgbehoefte (medische context, medische geschiedenis, verpleegkundige interventie). Dit zijn (onder andere) typische gegevens die nodig zijn om een patiënt over te dragen[19], dus deze gegevens zijn vaak nodig voor het transactie-type 'verpleegkundige overdracht'. Verder moet de ontvangende partij nog validiteitscriteria opstellen voor dit transactie-type. De persoonsgegevens van de patiënt zijn valide als ermee kan worden vastgesteld om welke patiënt het gaat, vandaar dat het verpleeghuis eist dat het BSN van de

---

[16] Hoewel de verpleegkundige het feitelijke werk doet, doet ze dat namens het verpleeghuis. Het verpleeghuis bepaalt dan ook welke gegevens nodig zijn voor het plaatsingsbesluit, en ook welke criteria gebruikt moeten worden om de validiteit daarvan te kunnen vaststellen. De verpleegkundige zal dienovereenkomstig de gegevens verzamelen en valideren.
[17] We nemen hier aan dat de wijkverpleging verantwoordelijk is voor de (thuis)zorg, en de verpleegkundige dus namens de wijkverpleging werkt. De wijkverpleging bepaalt dan ook welke gegevens worden bijgehouden over patiënten en aan welke kwalificaties die dan moeten voldoen. De verpleegkundige zal dat dan dienovereenkomstig doen.
[18] De syntax en semantiek zijn te vinden in zogenaamde zorginformatiebouwstenen, kortom 'zibs'. De zib voor de persoonsgegevens van de patiënt zijn hier te vinden.
[19] Zie de Nictiz opbouw eOverdracht specificatie.

patiënt afkomstig is van een staat-erkend identificatiemiddel, zoals een rijbewijs, ID kaart of paspoort. De ontvangstdatum moet in de (nabije) toekomst liggen. De patiënts zorgbehoefte is opgebouwd uit verschillende componenten, onder andere uit de verpleegkundige interventie. De verpleegkundige interventie is gedefinieerd[20] als *"een behandeling die een verpleegkundige uitvoert op basis van een deskundig oordeel en klinische kennis ten behoeve van een zorgvrager"*. Om te kunnen besluiten wat voor verpleging de patiënt nodig gaat hebben bij de ontvangende partij moet de ontvangende partij beslissen wat in hun ogen een 'deskundig oordeel' is, bijvoorbeeld een oordeel gemaakt door de patiënts verpleegkundige / verzorgende (en niet door een andere verpleegkundige / verzorgende die zelf geen behandelrelatie heeft met de patiënt) . Het verpleeghuis vraagt daarom om een zorgbehoefte die is opgesteld door de patiënt verpleegkundige en wilt daarbij weten wanneer deze zorgbehoefte is opgesteld.

QDX governance van verpleeghuis Zonneschijn

Gegevens met validiteitscriteria:
- Persoonsgegevens
  - BSN (afkomst van een identificatiemiddel)
  - Geslacht
  - Leeftijd
- Overdrachtsdatum (moet in de toekomst liggen)
- Zorgbehoefte (vastgesteld door de behandelende verzorgende, datum van vaststellen)

Voorwaarden:
Gegevens moeten komen van partij die behandelrelatie heeft met patiënt.
Doel:
Gegevens zullen gebruikt worden om te bepalen of de patiënt op de voorgestelde overdrachtsdatum geplaatst kan worden, of op een ander moment.

6.1.2 QDX Management door de Wijkverpleging

De versturende partij heeft bepaalde gegevens over zijn patiënten. We nemen hier aan dat de wijkverpleging verantwoordelijk is voor de zorg aan huis van zijn patiënten. De (verpleegkundige en/of verzorgende) van de wijkverpleging bepaalt welke gegevens worden bijgehouden over patiënten en aan welke kwalificaties die gegevens moeten voldoen. Voor ieder transactie type, dus ook voor de overdracht van patiënten, stelt de wijkverpleging dan ook vast welke soorten gegevens zij willen uitgeven, met welke zekerheden deze gegevens worden geleverd en hoe ze geleverd gaan worden onder welke condities. Voor het transactie-type 'verpleegkundige overdracht' wilt de wijkverpleging de volgende gegevens met bijbehorende zekerheden delen:

- Persoonsgegevens van de patiënt
  - BSN (deze is rechtstreeks afkomstig van het paspoort van de patiënt)
  - Geslacht (deze is rechtstreeks afkomstig van het paspoort van de patiënt)
  - Geboortedatum (deze is rechtstreeks afkomstig van het paspoort van de patiënt)

[20] Zie verpleegkundige interventie zib.

– Overdrachtsdatum (deze is vastgesteld door de wijkverpleging in overleg met naasten en/of patiënt, indien mogelijk)
– Zorgbehoefte van de patiënt (deze is opgesteld door de behandelende verzorgende, gecheckt door BIG-geregistreerde verpleegkundige)

De wijkverpleging wilt deze gegevens leveren aan zorginstellingen in de buurt (minder dan 30 kilometer afstand van Hengelo), die kunnen voorzien in de zorgbehoefte van de patiënt. De gegevens zullen via een XIS[21]-gecertificeerd informatiesysteem geleverd worden. Ook wil de wijkverpleging vaststellen voor de gegevensoverdracht dat de ontvangende partij kan voorzien in de zorgbehoefte van de patiënt.

QDX management door de wijkverpleging

Gegevens met zekerheden:
- Persoonsgegevens
  - BSN (afkomstig van paspoort)
  - Geslacht (afkomstig van paspoort)
  - Geboortedatum (afkomstig van paspoort)
- Overdrachtsdatum (vastgesteld door wijkverpleging in overleg met naasten en/of patiënt)
- Zorgbehoefte (maximaal een maand geleden opgesteld door de behandelende verzorgende, gecheckt door BIG-geregistreerde verpleegkundige)

Levering:
Wilt deze gegevens leveren via XIS aan zorginstellingen in de buurt (<30 km) die kunnen voorzien in de zorgbehoefte van

6.1.3 QDX Matching

De wijkverpleging in Hengelo krijgt vaak te maken met dezelfde partijen, omdat ze vaak patiënten overdragen aan verpleeghuizen en ziekenhuizen in de buurt. Je kunt dit zien als een QDX community. Voor het type transactie ‘verpleegkundige overdracht’, gaan zij, in overleg met andere zorgpartijen in hun community, afstemmen wat er aan gegevens en zekerheden gedeeld moet worden om een patiënt succesvol en efficiënt over te kunnen dragen. Een van deze partijen is verpleeghuis Zonneschijn. Verpleeghuis Zonneschijn wilt net iets andere gegevens of zekerheden over die gegevens ontvangen dan de wijkverpleging aanbiedt. Een voorbeeld daarvan is dat Zonneschijn de leeftijd van de patiënt wilt ontvangen, maar de wijkverpleging levert de geboortedatum. Zonneschijn vindt dit ook prima, aangezien ze dan zelf wel de leeftijd van de patiënt berekenen.

Het verpleeghuis vindt het voldoende zekerheid bieden dat de zorgbehoefte is vastgesteld door de behandelende verpleegkundige / verzorgende, maar wilt daar wel ook nog het moment van vaststellen bij krijgen. De versturende partij geeft aan dat ze niet precies weten wanneer het is vastgesteld, maar dat de zorgbehoefte van patiënten maandelijks wordt bijgehouden. De ontvangende partij vindt dit zekerheid genoeg bieden en zo ontstaat er een overeenkomst over de gegevens en hun zekerheden tussen deze zorginstellingen. Hieronder zie je het resultaat van deze onderhandelingen. Deze overeenkomst zou opgenomen kunnen worden in een credential catalogue.

[21] XIS is een standaard voor informatiesystemen binnen de zorg.

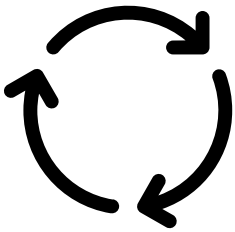
QDX matching

Gegevens met zekerheden:

- Persoonsgegevens
  - BSN (afkomstig van paspoort)
  - Geslacht (afkomstig van paspoort)
  - Geboortedatum (afkomstig van paspoort)
- Overdrachtsdatum (vastgesteld door wijkverpleging in overleg met naasten en/of patiënt)
- Zorgbehoefte (maximaal een maand geleden opgesteld door de behandelende verzorgende, gecheckt door BIG-geregistreerde verpleegkundige)

6.1.4 Operationele Wijkverpleging

De wijkverpleging heeft een zorgdossier met waarin de gegevens over meneer Pieterse zijn gedocumenteerd. Deze gegevens zijn relevant voor het leveren van de zorg, de overdracht, maar ook voor andere doeleinden, zoals kwaliteitsregistraties. De wijkverpleging houdt de gegevens up-to-date. Dat is in hun eigen voordeel, maar het zorgt er ook voor dat ze run-time gegevens kunnen leveren voor bijvoorbeeld een verpleegkundige overdracht. Hieronder zie je de gegevens die de wijkverpleging heeft over meneer Pieterse.



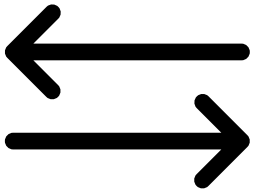
Operationele Wijkverpleging

- Persoonsgegevens:
  - Naam: Jacobus Pieterse
  - BSN: 123456789
  - Geslacht: M
  - Geboortedatum: 11-11-1936
  - Adres: Molenweg 16, Delden
- Contactpersoon: Marietje van Dalen
- Overdrachtsdatum: 01-05-2022
- Medische context
  - Diagnose: dementie
  - Allergie: noten
- Verpleegkundige interventie:
  - Interventie probleemgedrag, zoals onrustig zijn of geagiteerd zijn. Gebruik de GRIP interventie.

6.1.5 Operationele Verpleegkundige Overdracht

Wijkverzorgende Wijnand de Wijk merkt dat meneer Pieterse achteruit is gegaan en is met de naasten en meneer Pieterse zelf in gesprek gegaan over het verhuizen van meneer Pieterse naar een verpleeghuis. Wijnand heeft daaruit opgemaakt dat meneer Pieterse het liefste naar verpleeghuis Zonneschijn zou gaan, dus Wijnand stuurt een aanmeldbericht naar het verpleeghuis. Bij verpleeghuis Zonneschijn kijkt verpleegkundige Zoranna Zonjee welke soort gegevens zij nodig hebben (namelijk het resultaat van QDX governance) om te kunnen besluiten of meneer Pieterse geplaatst kan worden en vraagt Wijnand om deze gegevens met bijbehorende zekerheden te leveren. Wijnand verzamelt de benodigde gegevens met zekerheden over meneer Pieterse uit het IT systeem van de wijkverpleging en stelt op basis van daarvan een bericht samen en stuurt deze naar Zoranna (c.q. een IT-systeem van

verpleeghuis Zonneschijn, waar Zoranna toegang tot heeft). Het IT-systeem valideert zoveel mogelijk van de gegevens, de rest wordt gevalideerd door Zoranna en kan op basis van de gevalideerde gegevens het besluit maken of meneer Pieterse geplaatst kan worden op 1 mei aanstaande of niet.



Operationele verpleegkundige overdracht

Gegevens met zekerheden:

- **Persoonsgegevens**
  - **BSN**: 123456789 (afkomstig van paspoort)
  - **Geslacht**: M (afkomstig van paspoort)
  - **Geboortedatum**: 11-11-1936 (afkomstig van paspoort)
- **Overdrachtsdatum**: 01-05-2022 (vastgesteld door wijkverpleging in overleg met naasten en/of patiënt)
- **Zorgbehoefte** (maximaal een maand geleden vastgesteld door wijkverzorgende Wijnand de Wijk, gecheckt door Verena Verpleeg, BIG:01234001234)
  - **Medische context**
    - **Diagnose**: dementie
    - **Allergie**: noten
  - **Verpleegkundige interventie**: Interventie probleemgedrag, zoals onrustig zijn of geagiteerd zijn. Gebruik de GRIP interventie.

6.2 Vergelijking met KIK-V

Het programma KIK-V (Keteninformatie Kwaliteit Verpleeghuiszorg) is in 2018 van start gegaan om ketenpartijen in de verpleeghuiszorg bij een efficiënte en effectieve gegevensuitwisseling te ondersteunen. De bronhouders en afnemers maken hierin onderling afspraken die worden opgenomen in de afsprakenset KIK-V[22], die bijdragen aan het onderlinge vertrouwen en interoperabiliteit.

In de memo 'Functionele processen KIK-V' staan verschillende processen in de gegevensuitwisseling uitgelegd. In het eerste proces maakt de afnemer een informatiebehoefte kenbaar bij de beheersorganisatie. Voor zo'n gegevensbehoefte wordt een uitwisselingsprofiel opgesteld, die de uitwisseling tussen een afnemer en de bronhouders beschrijft. Als dit uitwisselingsprofiel is goedgekeurd door de belanghebbende partijen, dan is dit uitwisselingsprofiel gevalideerd. Voor elk benodigde gegeven in het uitwisselingsprofiel geeft de beheersorganisatie een gevalideerde vraag als credential uit aan de afnemer en slaat deze op in een credential registry. Vervolgens kan de afnemer deze credential laten zien aan (een selectie van) zelf gekozen bronhouder(s). De bronhouder kan dan de geldigheid en herkomst van de vragen verifiëren. De bronhouder verwerkt de gevalideerde vragen tot een antwoord en stuurt dit antwoord naar de afnemer. De afnemer neemt de antwoorden op in haar software voor kwaliteitscontroles.

[22] Zie afsprakenset KIK-V.

Wat er aan deze processen opvalt is dat ze grotendeels overeenkomen met ons vertrouwensmodel gebaseerd op QDX. De informatiebehoefte van de afnemer correspondeert met het resultaat van het QDX governance proces. Het matchingsproces tussen afnemer en bronhouders komt overeen met QDX matching, en het resultaat ervan, het gevalideerde uitwisselingsprofiel, is te vergelijken met de overeenkomst die resulteert uit QDX matching. Ook dat deze resultaten opgenomen (kunnen) worden in een credential catalogue is overeenkomstig.

Ondanks KIK-V en ons QDX vertrouwensmodel veel overlap vertonen, is er een groot verschil: het perspectief. KIK-V wordt beschreven vanuit het oogpunt van de beheersorganisatie waar het QDX vertrouwensmodel het perspectief van de individuele partij aanhoudt. We beschrijven in QDX governance en QDX management wat de gegevensvrager en gegevensaanbieder respectievelijk moeten doen om vast te stellen wat partijen in deze rollen willen ontvangen aan gegevens (met welke validiteitscriteria voor welk doel en van wie deze gegevens mogen komen) en welke gegevens ze willen uitgeven (met welke zekerheden onder welke condities). Deze processen lijken (nog) niet beschreven te zijn in KIK-V.

Nader onderzoek is nog nodig om te bepalen welke zekerheden worden vastgesteld tijdens het formuleren van de informatiebehoefte van de afnemers binnen het KIK-V proces. Daarnaast, wat individuele partijen moeten doen op transactie-niveau, oftewel run-time, als hun informatiebehoefte niet precies aansluit op het uitwisselingsprofiel en dus de gevalideerde vragen.

6.3 Wat heb je nodig?

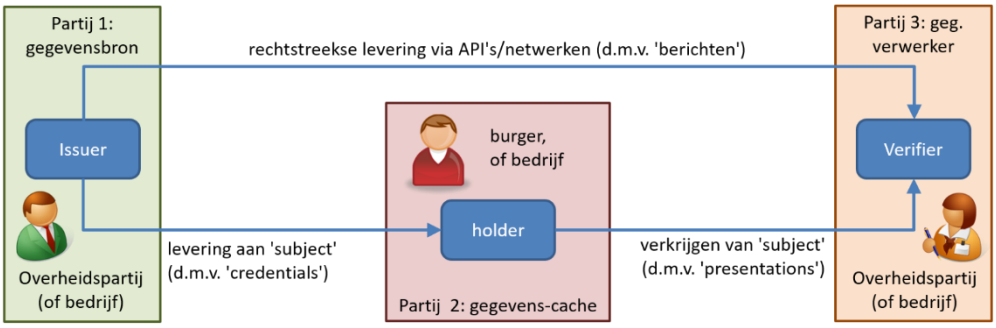
Op hoofdlijnen heb je voor gegevensuitwisseling het volgende nodig:

1. manieren voor partijen om te besluiten welke gegevensleveringen ze willen uitvoeren (onder welke condities, en met welke zekerheden) (QDX management)
2. manieren voor partijen om te besluiten voor welk soort transactie (in welke contexten) ze welk soort gegevens ze nodig hebben, zodanig dat ze op basis van die gegevens tot *valide* verwerkingen ervan komen. (QDX governance)
3. hulpmiddelen om gegevensleveringen te publiceren, en te matchen met gegevensbehoeften (QDX matching).
4. manieren/technieken om de feitelijke leveringen en feitelijke gegevensvragen te kunnen doen (zowel 'handmatig' als elektronisch).

Punten 1 en 2 zijn heel specifiek en subjectief voor de partijen die zich met QDX management en governance bezighouden. Voor de uitvoerders van die design-time processen is het vooral van belang dat ze zich realiseren waartoe de gegevens waar ze mee bezig zijn moeten dienen: wie gaat ze gebruiken, en wat moeten ze er dan mee kunnen doen. Zo doende kunnen ze zorgen dat ze daartoe ook geschikt zijn. Voor zover wij kunnen nagaan is dat op dit moment vooral een 'craft' (een 'kunst') die het een en ander aan ervaring vereist om het efficiënt te kunnen doen. Met betrekking tot punt 3 hebben we de credential catalogue al genoemd. Dat kunnen we nog aanvullen met een 'gouden gids'-achtige service[23], die het gebruikers mogelijk maakt om op klassen van gegevens of gegevensleveringen te kunnen zoeken, en naar de feitelijke gegevenslevering in een zekere catalogue

[23] Gegevens moeten vindbaar zijn volgens de FAIR-principes. Een datacatalogus (gebaseerd op DCAT2) volgt dit principe.

verwijst. We denken dat het mogelijk is om hiervoor generieke IT-systemen te ontwerpen, waarvan de feitelijke instanties op verschillende plekken en voor verschillende communities volgens hun eigen wensen kunnen worden ingericht. Dat is vergelijkbaar met bijvoorbeeld WordPress, wat een generiek ontwerp is voor een webshops en die door individuele partijen naar eigen smaak kan worden ingericht en geoperationaliseerd.
Voor alle punten kan het uit om na te denken over hoe bestaande communities binnen de zorg hierop gefaciliteerd zouden kunnen worden. Zo is het denkbaar dat bepaalde type transacties binnen een community generiek gespecificeerd kunnen worden, wat standaardisatie van uit te wisselen berichten tot gevolg kan hebben.
De feitelijke uitwisseling van gegevens (punt 4) werken we hieronder in wat meer detail uit omdat dit de aansluiting met de technologische middelen helpt te verduidelijken.
Om gegevens uit te wisselen kun je twee vertrekpunten kiezen: die van de gegevensvrager (die gegevens nodig heeft en ze verwerkt), en die van de gegevensaanbieder (die gegevens beschikbaar maakt). Merk op dat dit *rollen* zijn die door alle partijen afwisselend worden vervuld.
De gegevens kunnen via verschillende modaliteiten gedeeld worden[24]. Een gangbare manier is om data bij de bron op te halen. Dit hieronder is grafische weergegeven door middel van het bovenste pijltje. De gegevensverwerker ontvangt direct van de gegevens bron gegevens over het subject (de patiënt).

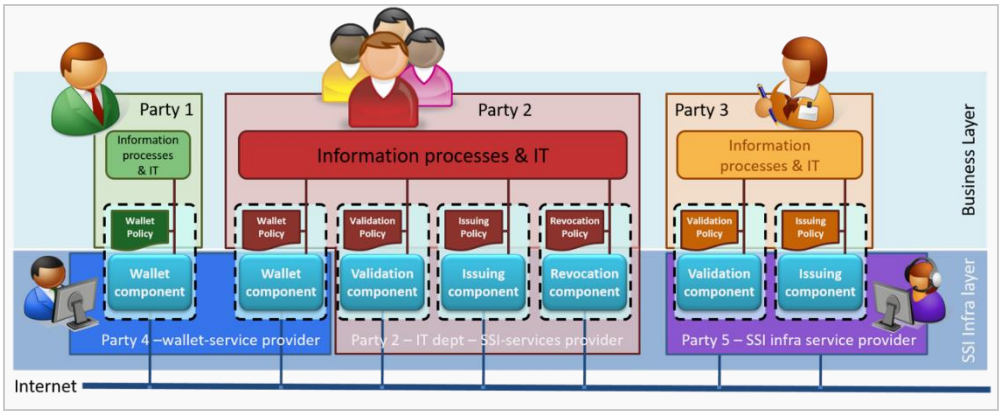


De laatste jaren doet een ontwikkeling opgang waarbij individuele personen (de holders) centraal staan, die zelf gegevens (over henzelf) in een Self-Sovereign Identity (SSI) wallet beheren, en die kunnen delen met wie ze willen. In de figuur is dat het onderste gedeelte. We zien daar de **issuer** (Partij 1), **holder** (Partij 2) en **validator**[25] (Partij 3) van de gegevens. De holder heeft typisch een wallet, een digitale actor die credentials (gekregen van de issuer) omzet in presentations (die wordt aangeboden aan de verifier). Credentials zijn pakketjes die zijn opgebouwd uit claims (de stukjes informatie die gedeeld worden, bijvoorbeeld ‘leeftijd = 30’), metadata (wanneer is deze credential gemaakt en door wie) en bewijzen (dat deze gegevens over het subject gaan en dat ze inderdaad gemaakt zijn door de issuer). Er zijn verschillende manieren om zo’n credential vorm te geven, van hoe je de

[24] Naast Self-Sovereign Identities (SSI) zijn er nog andere modaliteiten denkbaar. We noemen hier alleen Multi-Party Computation (MPC), omdat die voor academisch/statistisch onderzoek binnen de zorg relevant kan zijn, waarbij gegevens van verschillende ziekenhuizen en zorgverzekeraars gecombineerd worden om de effectiviteit van digitale zorg te analyseren, zonder dat deze gegevens daadwerkelijk worden gedeeld. Zie blog "Veilig data delen in de zorg met behoud van privacy".
[25] Wij noemen deze rol **validator** in plaats van **verifier**. Een verifier verifieert de structuur van de gegevens en de cryptografische handtekeningen over de gegevens, terwijl een validator bepaalt of de (geverifieerde) gegevens valide zijn om gebruikt te worden voor een bepaald doel.

gegevens structureert (JSON, JSON-LD, lijstjes, …) tot welke cryptografisch algoritme je gebruikt om de gegevens te versleutelen of een digitale handtekening te zetten. Daarnaast zijn er verschillende ideeën over hoe de user interface eruit zou moeten zien om bruikbaar te zijn voor (verschillende soorten) holders. Al deze variaties leiden er toe dat er ook veel verschillende wallets zijn. Het is natuurlijk mooi dat de gebruiker een ruim assortiment heeft om uit te kiezen, maar voor issuers en verifiers is het lastig om al deze verschillende wallets te accepteren. Dit probleem wordt concreter en urgenter dankzij de nieuwe eIDAS 2 verordening, waar we verderop op terug komen.

Waar bovenstaande figuur een bekende manier is om gegevensuitwisseling inzichtelijk mee te maken, geeft hij niet goed weer wat er voor een individuele partij nodig is. Individuele partijen – en dat geldt zowel voor personen als organisaties – vervullen allemaal (op verschillende tijdstippen) de rollen van issuer, holder en verifier. Immers, in de onderhandelingsfase van een transactie moeten beide partijen gegevens vragen om te besluiten of ze de volgende (uitvoerings)fase ingaan, of dat ze afhaken, en daarin vervullen beiden de rol van verifier. Ook zullen beiden de gegevensvraag van de ander beantwoorden (d.m.v. presentations – zie bovenstaande figuur), en doen dat in de rol van holder. En in de afrondingsfase kan één van de resultaten een credential zijn die ze aan de ander uitgeven in de rol van issuer.



Om zo'n rol te vervullen, moet de partij dus over een IT systeem beschikken die het mogelijk maakt om die rol te vervullen. Dat is wat bovenstaand figuur laat zien. In de bovenste laag, de 'business layer', hebben we verschillende partijen. Partij 1 is bijvoorbeeld een burger (hij kan alleen de rol van holder spelen en de IT daarvoor is in beheer van een externe partij), terwijl partij 2 een groot bedrijf is, aangezien deze partij zowel de rol van issuer, als holder, als validator vervult en daartoe zijn eigen IT systemen heeft ingericht. Om deze componenten het juiste doel te laten dienen, moet de partij een policy hebben die regels biedt aan het component. Een voorbeeld daarvan hebben we gezien in Operationele Verpleegkundige Overdracht, waarbij de IT-systemen van het verpleeghuis Zonneschijn de binnenkomende gegevens valideert op basis van de validatiecriteria die het verpleeghuis heeft opgesteld tijd QDX governance.

De termen gegevensvrager en gegevensaanbieder zijn per transactie te mappen naar de termen issuer, verifier en holder. Als een patiënt zijn bloedgroep laat bepalen door een laboratorium en deze geeft een credential uit voor bloedtype 'A-' aan de patiënt, die de credential is zijn wallet op slaat, dan is het laboratorium de

issuer en de patiënt de holder. Als de patiënt vervolgens in een ambulance ligt en een bloedtransfusie nodig heeft, heeft de ambulance gegevens nodig om te zorgen dat de patiënt bloed kan ontvangen van het juiste type. De patiënt kan dan de credential over zijn bloedgroep aan de ambulancebroeders geven. Hier in is dus de patiënt de gegevensaanbieder en de ambulancebroeders de gegevensvrager, maar ook de verifier.
Maar het zou ook kunnen dat de patiënt zelf weet welke bloedgroep die heeft, aangezien allebei zijn ouders bloedgroep ‘A-’ hebben. De patiënt geeft dan zelf dit credential uit, zodat de patiënt nog steeds de gegevensaanbieder is, maar ook de issuer en de holder is.

De interoperabiliteit is een bekend probleem binnen SSI. Er zijn verschillende initiatieven om dit probleem op te lossen, zoals standaardisatie (W3C VCC, eSSIF-lab) of één gateway te bouwen die meerdere wallets accepteert, op een gelijksoortige wijze als Mollie[26] dat doet voor betalingen. TNO heeft zo’n gateway gebouwd, genaamd EASSI. Deze gateway kan door partijen gekoppeld worden, waardoor ze makkelijk credentials voor verschillende wallets kunnen uitgeven en verifiëren.

[26] Zie Mollie.

7 Technologische ontwikkelingen

Dit hoofdstuk noemt een aantal ontwikkelingen die technische impact (kunnen) gaan hebben op het elektronisch uitwisselen van gegevens. Het is het topje van een grote ijsberg. De onderwerpen voor dit hoofdstuk zijn gekozen, bijvoorbeeld omdat iedereen er toch mee te maken gaat krijgen (eIDAS 2), de mogelijke potentie voor de zorg als het gaat om gebruik van bestaande (technische) systemen (IDS), of de potentie die het (op proces- en informatieniveau) kan hebben (SSI). Een andere ontwikkeling die impact kan gaan hebben op het zorgdomein is dat er een voorstel ligt voor een 'European Health Data Space'. Deze recent voorgestelde verordening richt zich op regie over eigen zorggegevens en veilige uitwisseling van die gegevens. Helaas hebben we dit niet meer uitgebreider kunnen meenemen in het onderzoek.

7.1 eIDAS 2[27]

Na evaluatie van de ontstane praktijk heeft de Europese Commissie in juni 2021 een aantal wijzigingen voorgesteld. Eén daarvan is om lidstaten te gaan verplichten om hun ingezetenen (voor zover die dat tenminste willen) te voorzien van (tenminste) één elektronisch middel – de Europese portemonnee voor digitale identiteit - waarin ze hun eigen 'eID' (een verzameling attributen zoals naam, adres, geboortedatum, geslacht, burgerlijke staat, e.d.) kunnen opslaan. Maar ook: onderwijskwalificaties, beroepskwalificaties, vergunningen, licenties, financiële gegevens e.d. Het is denkbaar dat hier ook gezondheids-gegevens in opgeslagen kunnen worden.

Een persoon kan een dergelijke wallet dan gebruiken voor allerlei elektronische transacties, in elke denkbare rol (zoals klant, werknemer, patiënt, student, rechthebbende, enz.). De persoon kan allerlei attributen uit allerlei contexten daarin opslaan – mits die dan wel als zodanig worden aangeboden. Zulke attributen kunnen dan in principe overal, in verschillende contexten, elektronisch worden gevraagd en dus uitgewisseld, waarbij het idee is dat de persoon daar dan wel eerst toestemming voor geeft. Zulke wallets moeten wel voldoen aan (nog nader te bepalen) security eisen.

In een Recommendation heeft de Europese Commissie lidstaten gevraagd om een ‘toolbox’ te ontwikkelen voor een European Digital Identity framework. Deze toolbox moet leiden tot een technisch referentie framework inclusief ‘best practices’ en richtlijnen voor implementatie. Dit om te waarborgen dat er een geharmoniseerde benadering komt binnen Europa die aansluit bij verwachtingen van burgers en bedrijven. Het is de bedoeling dat deze toolbox in september 2022 gereed is, dat in 2023 wallets worden aangewezen en in 2024 grote bedrijven deze verplicht moeten

[27] De eIDAS-verordening (Verordening (EU) 910/2014) gaat over elektronische identificatie (inlogmiddelen) en vertrouwensdiensten (bijv. voor het zetten van digitale handtekeningen, tijdstempels e.d.) ten behoeve van elektronische transacties binnen de EU. Het idee is dat ingezetenen van de ene lidstaat zijn (genotificeerde) inlogmiddelen ook in andere lidstaten kan gebruiken, en dat digitale handtekeningen en andere artefacten overal in de EU even rechtsgeldig zijn.

kunnen accepteren.[28] In Nederland is deze verantwoordelijkheid belegd bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK).

7.2 IDS

Zekerheid dat gegevens uit een specifieke bron komen wordt onder meer geregeld via public-key infrastructuren (PKI): servers (IT componenten) die zijn voorzien van een PKI certificaat kunnen door andere IT componenten worden geauthenticeerd, en afhankelijk van het afsprakenstelsel waaronder het certificaat werd uitgegeven levert dit meer of minder zekerheid over de partij onder wiens verantwoordelijkheid de betreffende server valt. PKI gaat dus over het authenticeren (en verder beveiligen) van verbindingen (te zien als een 'groen slotje' in browsers). Het zegt niets over de juistheid, courantheid en andere kwalificaties van de gegevens die daarover worden uitgewisseld.
Dat laatste zit wel binnen de scope van wat 'International Data Spaces' (IDS) heet. Het idee is dat een aantal organisaties die (al) met elkaar (willen) samenwerken in wat ze een 'ecosysteem' noemen:

1. een afsprakenstelsel ontwikkelen (met bijbehorende governance), waarin de rechten en plichten van deelnemers zijn gespecificeerd, en waaraan deelnemers zich committeren;
2. technische specificaties ontwikkelen, waaraan IT-componenten moeten voldoen die door deelnemers kunnen worden ingezet om met soortgelijke IT-componenten van andere deelnemers te communiceren;
3. semantische specificaties ontwikkelen voor de berichten die deze IT-componenten met elkaar kunnen uitwisselen, die relevant en bruikbaar zijn voor de doelen waartoe de samenwerking feitelijk bestaat;
4. een stel registratie-services (laten) inrichten, waar deelnemende deelnemers c.q. IT-componenten gegevens in kunnen plaatsen c.q. opzoeken over/met andere deelnemers.

Een concrete, operationele uitvoering van zo'n ecosysteem is het 'Smart Connected Supplier Network', waar leveranciers hun eigen IT systemen (over resource planning) via een dergelijk netwerk kunnen laten communiceren met andere IT systemen, van andere leveranciers.
Het is denkbaar dat de onderliggende IDS concepten ook bruikbaar zijn om verschillende 'ecosystemen' mee in te richten binnen de zorg.[29]

7.3 Self-Sovereign Identity

Hoewel er is (nog steeds) geen echte consensus over wat Self-Sovereign Identity (SSI) is, heeft wel iedereen het steeds over 'wallets', 'de gebruiker centraal c.q. in control' e.d. De eIDAS 2 portemonnee lijkt uit dit soort ideeën te zijn ontsproten. Maar binnen SSI contexten zien we wel veel meer dan alleen een portemonnee met attributen.
De (nog steeds) actuele ideeën waarmee het begonnen is staan in het boek 'Self-Sovereign Identity' (Preukschat, Reed, 2021). Het effect dat burgers, bedrijven en overheden hiervan vooral zien is dat SSI het mogelijk om elektronische/online

[28] Ons lijken deze tijdslijnen wel heel erg, zo niet (veel) te ambitieus.
[29] De IDS architectuur en andere specificaties hebben nog meer leuke ideeën die voor hier echter te ver gaan. De hier beschreven concepten worden overigens ook door andere initiatieven in zekere mate gebruikt (bijv. iShare). Het is de vraag of de technische details van belang zijn zolang nog niet duidelijk is hoe daar vanuit de zorg gebruik van gemaakt zou moeten gaan worden.

formulieren in te laten vullen met gegevens die bij verschillende andere partijen elektronisch beschikbaar zijn, en dat het invullen fundamenteel sneller gaat en het controleren ervan stukken goedkoper – formulieren moeten echter wel zijn ontworpen zoals bij QDX governance beschreven, en de gegevens moeten wel beschikbaar zijn zoals bij QDX management gezegd.
Het idee is dat de gebruiker een wallet/app heeft, waarmee hij bij die andere partijen 'credentials' kan ophalen die gegevens over hem/haarzelf bevatten, en door de uitgevende partij digitaal zijn ondertekend zodat morrelen aan de gegevens wordt gedetecteerd, en duidelijk is wie die uitgevende partij is - een mooi begin voor vertrouwde gegevensuitwisseling. Vervolgens kan de gebruiker die een online formulier wil invullen zijn app een QR-code op dat formulier laten scannen, waardoor die app kan nagaan welk soort gegevens nodig zijn, en van welke partij die gegevens moeten komen. De app kijkt dan of die gegevens in de credentials zitten, en kan die dan (na toestemming van de gebruiker) deze opsturen waarna ze 'automatisch' worden ingevuld.
De ontvangende partij hoeft alleen nog wat elektronische controles te doen, bijvoorbeeld of digitale handtekeningen kloppen. Ook kan hij – mits de uitgevende partij dat heeft gefaciliteerd – controleren of de (gegevens uit) credentials intussen niet zijn ingetrokken.
Dit soort use-cases wordt mogelijk gemaakt door een veelheid aan technologieën, die vaak ook onafhankelijk van deze use-case nut kunnen hebben. Het gaat daarbij om een veelheid aan cryptografische technieken, gedecentraliseerde key-management technieken (bijv. KERI), een nieuw soort identifier (de Decentralized Identifiers (DIDs)), verschillende soorten 'Verifiable Credentials', en meer.
De set technieken die benodigd zijn voor SSI is nog volop in ontwikkeling. Desondanks zijn er al wel werkende oplossingen gestoeld op dit gedachtegoed. Het Nederlandse IRMA bijvoorbeeld kwalificeert zich in onze ogen als een SSI technologie, maar gebruikt helemaal geen DIDs (en ook geen blockchain/DLT, dat door veel mensen en initiatieven, zoals het Europese EBSI, toch ook wel als basis-bouwblok wordt gezien).
In de SSI context wordt veel gesproken over 'centraal' en 'decentraal', en wordt vaak aangenomen dat 'centraal = fout' en 'decentraal = goed'. Wat echter nu precies als 'centraal' of 'decentraal' kwalificeert is doorgaans onduidelijk. Wij hebben uit verschillende discussies de conclusie getrokken dat argument zinvol te begrijpen zijn als we 'centraal' interpreteren als een hiërarchische structuur waarin er een partij is die probeert regels, implementaties of andere dingen op te leggen/verplicht te maken aan een stel anderen zonder daarbij rekening te houden met de individuele belangen van die anderen en 'decentraal' als een gemeenschap, waarin (autonome) partijen samenwerking opzoeken en *elkaar* van dienst willen zijn[30].
In Oktober 2021 heeft de Rijksoverheid het Eindrapport Nederlandse Self-Sovereign Identity ecosysteem (SSI) gepubliceerd, met daarin een verkenning van het Nederlandse SSI speelveld, toekomstige ontwikkelrichtingen, impact op publieke waarden en de rol van de Nederlandse overheid.

[30] Het principe van federatieve samenwerking in de zorg wordt beschreven in de referentiearchitectuur voor de zorg DIZRA.