Visiedocument

Dutch Self-Sovereign Identity Framework (DSSIF)

Dutch Blockchain Coalition

connect and create

www.dutchblockchaincoalition.org

Auteur:
Tim Speelman

Eerste Reviewers:
Arno Laeven, Jacob Boersma en Peter Verkoulen

Review Board:
Chantal van der Wijst (Belastingdienst), Simon Sanders (CMS DSB Advocaten), Rein Schaafsma en Wouter Welling (Ministerie van Binnenlandse Zaken en Koninkrijksrelaties), Sandra van Heukelom-Verhage (Pels Rijcken), Tina van der Linden (Vrije Universiteit Amsterdam), Tom Demeyer (Waag)

Illustraties:
Rosa Jager en Tim Speelman

Dutch Blockchain Coalition
connect and create

Inhoudsopgave

1 Introductie 2
2 Een gedeeld vertrekpunt 6
2.1 Van 'Identiteit' naar Administratieve Beeldvorming 6
2.2 Een waardengevoelig ontwerp 7
2.3 De toepassingsruimte: eilanden ondersteunen en verbinden 8
2.4 Een model van de toepassingsruimte 8
2.5 De informatieverzameling: van vraag naar antwoord 9
2.6 Link tussen realiteit en administraties 9
2.6.1 Administratie 10
2.6.2 Identifierbeheer 11
2.6.3 Sleutelbeheer 11
2.6.4 Authenticatie 11
2.7 Verklaringenoverdracht 12
2.7.1 Logistiek 13
2.7.2 Autorisatie van de uitgever 13
2.7.3 Autorisatie van de controleur 14
2.8 Op naar een digitale identiteitsinfrastructuur 15
3 Gedeelde waarden 16
3.1 Nut: een nuttig antwoord 16
3.2 Informationele Privacy: een minimaal antwoord 16
3.3 Representativiteit: een nauwkeurig antwoord 17
3.4 Controle op het antwoord én de verzameling 17
3.5 Betrouwbaarheid: een betrouwbaar antwoord 18
3.6 Beschikbaarheid: altijd een antwoord 19
3.7 (Communicatie)privacy: geen lekkage van (meta)data 19
3.8 Frictie: moeiteloos een antwoord 20
3.9 Fragmentatie: informatie zoveel mogelijk gescheiden 20
4 Een gedeeld mechanisme 21
5 Hoe dan? Een gedeeld bouwplan 23
5.1 Voorwaarde: exclusief bezit van apparaten 24
5.1.1 Inclusie 25
5.1.2 Verlies en diefstal 25
5.1.3 Recentralisatie 26
5.2 Authenticatie met Agents 26
5.2.1 Volledig controle over identifiers 26
5.2.2 Authenticatie met derden 27
5.2.3 (Door)ontwikkeling van mechanische identificatie en authenticatie 28
5.3 Verklaringenoverdracht met Agents 28
5.3.1 Dataminimalisatie 29
5.3.2 Regie op Gegevens: een goed idee? 29
5.3.3 Actualiteit 30
6 En nu? 31
7 Begrippenlijst 32

1 Introductie

Dienstverleners – zoals in de zorg, het bankwezen of bij de overheid – moeten over het algemeen iets over hun afnemers weten om hun diensten te kunnen verlenen. Zoals wie hun afnemers zijn, wat ze kunnen of wat ze mogen. De daarvoor benodigde administratie en de uitwisseling van informatie zijn in toenemende mate problematisch te noemen, voor zowel de dienstverlener als de afnemer. Een voorbeeld hiervan is te vinden in de woningmarkt: potentiële huurders moeten een heel dossier aan documenten verzamelen en aanleveren, alleen maar om te bewijzen dat ze de huur kunnen betalen. Verhuurders moeten al die documenten handmatig op echtheid controleren en vervolgens handmatig beoordelen. Deze werkwijze is niet alleen moeizaam, tijdrovend en duur, maar kan ook ernstige impact hebben op de privacy en (daarmee) veiligheid van de huurder. Er wordt immers veel meer informatie gedeeld dan nodig en het is onduidelijk wat er daarna met al die informatie gebeurt.

Hoewel digitalisering een efficiëntieslag teweeg heeft gebracht in dergelijke processen, heeft het ook geleid tot grotere risico's voor de privacy en (cyber)veiligheid. Mensen en bedrijven zijn in toenemende mate slachtoffer van datalekken, waarna gelekte persoonsgegevens kunnen worden gebruikt voor bijvoorbeeld phishing en andere vormen van identiteitsfraude. In veel domeinen spelen soortgelijke problemen. Desondanks ontbreekt in de meeste gevallen een gezamenlijke aanpak. Het gevolg is een wildgroei van losse identiteitssystemen en ketens, waarbij privacy, betrouwbaarheid en andere waarden telkens opnieuw moeten worden afgewogen en geborgd. Dat vergroot de kans op fouten en maakt het lastig voor gebruikers en toezichthouders om die systemen en ketens te doorgronden en te controleren en dus te weten of privacy en andere waarden voldoende beschermd zijn. De fragmentatie van identiteitssystemen en ketens zorgt tevens voor een gebrek aan interoperabiliteit: culturele, organisatorische, politieke, juridische en economische grenzen belemmeren het delen van data en de identificatie van mensen en organisaties. Dat is niet in de laatste plaats vervelend voor de mens die door al die verschillende situaties moet navigeren.

Dit moet beter en kán beter!

Middels technische standaarden en regelgeving zoals de eIDAS verordening[1] kan interoperabiliteit worden gestimuleerd, maar dan blijft de noodzaak bestaan voor technische en organisatorische invulling hiervan. Die technologie en organisatie zijn nodig om de feitelijke uitwisseling van informatie en de nodige controles te faciliteren. Ook de mens – als klant, student, patiënt of in een andere rol – heeft baat bij een gezamenlijke aanpak: één manier van authenticeren en (persoonlijke) informatie uitwisselen, waarbij ook direct de wederpartij is geauthenticeerd. Idealiter bestaat een gezamenlijke aanpak dan ook uit gedeelde technologie die bruikbaar is in een breed scala aan toepassingen: een digitale identiteitsinfrastructuur. Net als andere kritieke infrastructuren – water, elektra, transport – kan een dergelijke infrastructuur een enorme maatschappelijke en economische waarde toevoegen. De vraag is hoe zo'n digitale identiteitsinfrastructuur het beste ingericht kan worden om aan alle belangen in al die vormen van dienstverlening te voldoen. Een proactieve inzet is nodig van veel meer disciplines dan alleen techniek, zoals wetgeving, beleid, sociologie en ethiek, om deze ontwikkelingen in goede banen te leiden. Wellicht de meest fundamentele ontwerpvraag is wie verantwoordelijk gaat zijn voor

[1] https://www.digitaleoverheid.nl/dossiers/eidas/

Terug naar inhoudsopgave

de ontwikkeling en het beheer van zo'n kritieke infrastructuur. Bij welke partijen kunnen die kritieke taken verantwoord worden belegd? Bij welke partijen zijn gegevens, metadata en gedragsinformatie van allerlei mensen en organisaties veilig? Bij de overheid? Big tech? Big finance? Big telco? Is het überhaupt moreel verantwoord om zoveel macht en kennis bij één of enkele partijen te beleggen?

Self-Sovereign Identity

In de zoektocht naar een antwoord op die vraag, valt steeds vaker de term Self-Sovereign Identity (SSI). De filosofie achter Self-Sovereign Identity is dat de kennis van en macht over gegevens enkel bij het data-subject (mens, organisatie of zelfs machine) zélf mag liggen. Dit kan worden gerealiseerd door ieder mens en iedere organisatie te voorzien van een nieuw stuk gereedschap: een digitale assistent, in SSI ook wel een agent of wallet genoemd. Die digitale assistent – voor mensen waarschijnlijk in de vorm van een smartphone app – maakt het de eindgebruiker eenvoudig en zorgt te allen tijde voor verantwoord beheer van identifiers, sleutels en gegevens. Het data-subject behoudt het inzicht en de regie op gegevens. Wanneer dienstverleners om gegevens vragen, ziet het subject altijd in een vertrouwde en consistente interface welke gegevens met wie gaan worden gedeeld. Van het subject zal enkel worden gevraagd om dit verzoek toe te staan of te weigeren. Niet alleen het subject heeft zo'n assistent, maar ook alle uitgevers en controleurs van gegevens. Hun agents faciliteren efficiënte en veilige datadeling waarin de herkomst en integriteit zijn geborgd. Ook standaardiseren ze de communicatie met de agent van het subject. Op deze wijze wordt het subject de verbindende factor tussen de uitgever van een gegeven (zoals een overheidsregister) en de controleur van dat gegeven (zoals een dienstverlener).

Doordat agents efficiënte en veilige datadeling realiseren en breed inzetbaar zijn, wordt de frictie van datadelen (tijd, kosten en moeite) aanzienlijk verminderd. Tegelijkertijd krijgt het data-subject vanuit die positie inzicht in en grip op de gedeelde data en is hij of zij daarbij volledig onafhankelijk van intermediairs. Zo heeft geen enkele derde partij meer inzicht in die gegevens of wat het data-subject daarmee doet. Doordat de technologie bij alle data-subjecten is belegd ontstaat een decentraal netwerk zonder centrale zwaktepunten. Dat maakt een digitale identiteitsinfrastructuur niet alleen robuust, maar ook beter schaalbaar. Daarmee is een win-winsituatie te creëren voor zowel dienstverleners als afnemers. Tenminste, dat is het streven.

Het woord "soeverein" verdient nadere toelichting. Soevereiniteit doet denken aan onbegrensde zeggenschap over de gegevens, ze zo aanpassen als gewenst, wat niet past in de huidige maatschappij. Toch wordt soevereiniteit in SSI niet zo bedoeld. Het idee van SSI is namelijk dat het data-subject actief de regie voert over de eigen gegevens. Over sommige van die gegevens zal men zelf iets verklaren, maar de meeste gegevens zullen uit vertrouwde bronnen van derden komen zoals overheidsregisters, banken, werkgevers en andere organisaties en mensen. Met SSI kan het data-subject die gegevens niet onopgemerkt aanpassen, maar verkrijgt het subject (net als met een fysiek paspoort of waardepapier) de werkelijke grip op wie dat gegeven inziet en wanneer.

Een veelgehoord bezwaar is dat mensen en organisaties niet in staat zouden zijn om dergelijke technologie en/of gegevens op een verantwoorde manier te beheren. Oftewel dat SSI alleen werkt voor een kleine groep privacy-experts. Het hoeft echter niet complex te zijn: de software neemt alle complexe taken uit handen en geeft in een begrijpelijke interface precies de informatie die nodig is. Toch brengt SSI naast vrijheid en controle ook een

Terug naar inhoudsopgave

nieuwe mate van verantwoordelijkheid. We moeten voorzichtig zijn als we mensen de volle verantwoordelijkheid geven over hun eigen privacy en (cyber)veiligheid. Het is daarom van belang om de technologie zo in te richten dat deze standaard voldoende bescherming biedt.

De ontwikkeling van, en aandacht voor, Self-Sovereign Identity is de afgelopen jaren sterk toegenomen. Diverse grote (consortia van) bedrijven zijn bezig met de ontwikkeling van de technische oplossingen, waarvan sommige al nagenoeg klaar lijken te zijn. Het lijkt onomkeerbaar dat een vorm van SSI in de nabije toekomst deel uit gaat maken van de maatschappij. Daarom is het van groot belang dat we in staat zijn deze ontwikkelingen op waarde te schatten, waar nodig bij te sturen en er vooral van te profiteren.

Het Dutch Self-Sovereign Identity Framework

Met het Dutch Self-Sovereign Identity Framework beoogt de Dutch Blockchain Coalition een gedeeld vertrekpunt voor alle belanghebbenden neer te zetten: waar hebben we het over en waar willen we naar toe? Met dat vertrekpunt kunnen ontwerpkeuzes worden gemaakt, onderbouwd en op waarde worden geschat. Daarbij onderkennen we ook de risico's, waarbij benadrukt moet worden dat we op dit moment nog niet alle risico's kunnen overzien. Toch geloven we in de enorme potentie van (de filosofie van) Self-Sovereign Identity, voor mens én organisatie, voor economie en maatschappij.

Dit visiedocument is als volgt gestructureerd:

- **Hoofdstuk 2** formuleert een gedeeld vertrekpunt: "Waar hebben we het over?". We staan allereerst stil bij de breedte en diversiteit van de context waarin de digitale identiteitsinfrastructuur een rol moet gaan spelen. Vervolgens analyseren we die context en zetten we de mogelijke functies van een infrastructuur uiteen.
- **Hoofdstuk 3** formuleert een kader van relevante waarden om de ontwikkeling van een infrastructuur op waarde te kunnen schatten en ontwerpkeuzes te kunnen maken. Daarmee kan tevens vastgesteld worden of wij – als dienstverleners, afnemers en andere belanghebbenden in de brede diversiteit van organisaties en sectoren – het eens zijn over de gewenste uitkomsten.
- **Hoofdstuk 4** betoogt de verbindende en controlerende rol van het subject, het idee van Self-Sovereign Identity, afgezet tegen alternatieve inrichtingen van een digitale identiteitsinfrastructuur.
- **Hoofdstuk 5** gaat in op de vraag hoe het subject die verbindende en controlerende rol kan gaan spelen. Zonder specifieke technologieën en ontwikkelingen te bespreken, schetsen we een oplossing en kaarten relevante ontwerpkeuzes, risico's en open vragen aan.
- **Hoofdstuk 6** bespreekt de vervolgstappen: "Hoe nu verder?".
- **Hoofdstuk 7** bevat een begrippenlijst.

Dit visiedocument is een leidraad en geen handleiding. Het is tevens een levend document dat aangepast wordt en groeit met voortschrijdend inzicht.

Terug naar inhoudsopgave

2 Een gedeeld vertrekpunt

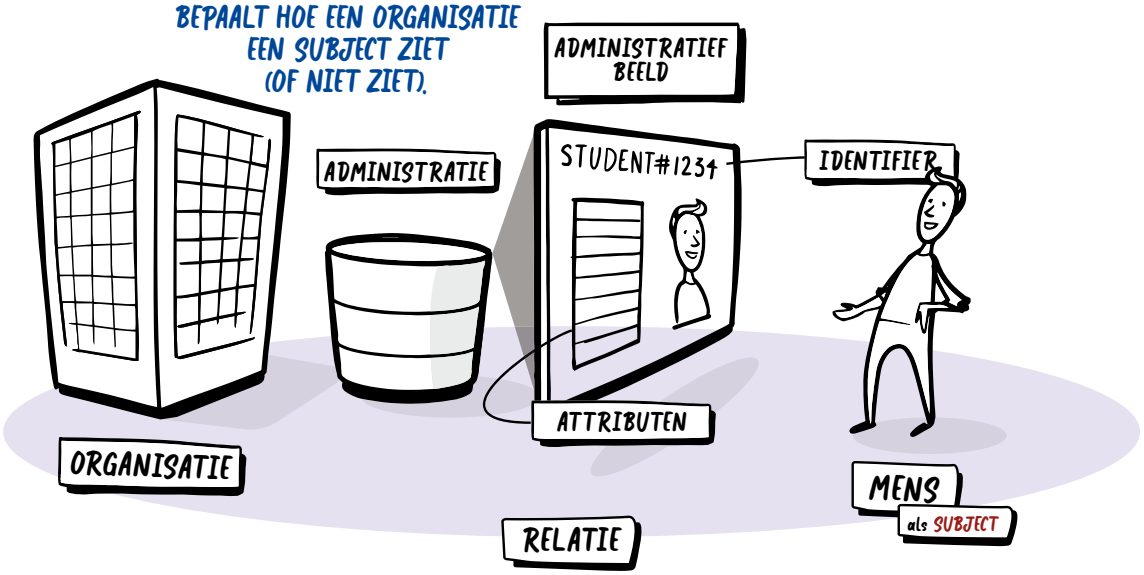
Het doel van dit visiedocument is het vaststellen van een gedeeld vertrekpunt voor alle belanghebbenden – met uiteenlopende achtergronden en expertises – van de beoogde digitale identiteitsinfrastructuur; waar hebben we het over en waar willen we naar toe? Met dat vertrekpunt kunnen ontwerpkeuzes worden gemaakt, onderbouwd en op waarde worden geschat. Dit hoofdstuk beschrijft de context en problematiek vanuit verschillende invalshoeken, los van technische, juridische en beleidsmatige details.

2.1 Van 'Identiteit' naar Administratieve Beeldvorming

Het begrip 'identiteit' kan tot verwarring leiden. Verschillende disciplines die in dit stuk zijn samengebracht hanteren namelijk verschillende definities. In de informatiewetenschappen kan identiteit verwijzen naar een set gegevens die een mens, organisatie of ding beschrijft. In het recht kan identiteit verwijzen naar de officiële registratie van een mens of organisatie, zoals vastgelegd in een burgerregister of handelsregister. In de sociale wetenschappen gaat het over het volledige en unieke *zijn* van de mens, hetgeen nooit in *gegevens* te vatten is. Zo zijn er nog vele definities en conceptualisaties te benoemen.

Het is in deze context productiever om te spreken van 'beeldvorming'. Mensen en organisaties vormen namelijk *beelden* van elkaar, op basis waarvan ze elkaar interpreteren en beoordelen. Dit beeld kan mentaal of emotioneel zijn, maar ook *administratief:* een **ADMINISTRATIEF BEELD** (zie Figuur 1). Elke partij heeft weer een *ander* beeld van dezelfde mens of organisatie, ingevuld met andere aspecten, andere **ATTRIBUTEN**. Om subjecten uit elkaar te kunnen houden en te kunnen identificeren kan aan elk subject een uniek identificerend nummer of gegeven worden toegekend, een **IDENTIFIER**[2]. Mensen (en organisaties) komen doorgaans in veel van die administraties voor, zoals in het personeelsbestand van hun werkgever, het klantenbestand van hun bank en het burgerregister van hun overheid.

FIGUUR 1:
EEN ADMINISTRATIEF BEELD BEPAALT HOE EEN ORGANISATIE EEN SUBJECT ZIET (OF NIET ZIET).



[2] Een identifier kan ook een (gebruikers)naam, of e-mailadres zijn. Een identifier is elk attribuut of combinatie van attributen die (in een bepaalde context) uniek is en daarmee gebruikt kan worden om te identificeren.

Terug naar inhoudsopgave

Het is essentieel om te onderkennen dat een administratief beeld altijd een *versimpeling* is en mogelijk onjuist of verouderd. De aanwezigheid van het administratief beeld moet niet verward worden met het feitelijke *bestaan* van de mens of organisatie – 'ik sta geregistreerd, dus ik ben'. Wanneer het administratief beeld in processen en organisatieculturen ten onrechte voor absolute waarheid wordt aangenomen, kan dit ernstige gevolgen hebben.

De administratieve beelden – en de processen waarmee die beelden tot stand komen, veranderen en worden gebruikt – zijn instrumenteel voor veilige en efficiënte dienstverlening. Ze zijn tevens waardengeladen; ze hebben *impact* op dienstverleners, dienstafnemers en andere betrokkenen. De ontwerpvraag die volgt is: **Hoe kan een digitale identiteitsinfrastructuur deze administratieve processen, en daarmee de dienstverlening, ondersteunen op een manier die recht doet aan de waarden van alle betrokkenen?**

2.2 Een waardengevoelig ontwerp

Het ontwerp van een digitale identiteitsinfrastructuur is waardengevoelig. In hoofdstuk 3 wordt dieper ingegaan op de waarden die hiermee zijn gemoeid. Hieronder volgt een korte samenvatting, zodat de lezer deze waarden in het achterhoofd kan houden.

Allereerst is van belang dat het administratieve beeld een bepaalde functie vervult, een **NUT** heeft, zoals het beveiligen, ondersteunen of personaliseren van de dienstverlening. Die functie bepaalt eveneens de vereiste **BETROUWBAARHEID** van de informatie. Het verstrekken van een lening heeft bijvoorbeeld een hoger risico dan het verstrekken van een klantenkorting en vraagt daarom om meer betrouwbare informatie. Tevens moet het beeld **REPRESENTATIEF** zijn: een nauwkeurige beschrijving van het data-subject; niet alleen voor effectieve dienstverlening maar ook voor een eerlijke behandeling van de beschreven mens of organisatie.

(Administratieve) beeldvorming staat per definitie op gespannen voet met **PRIVACY**. Privacy wordt breed omschreven als 'het (recht om) met rust gelaten (te) worden, om ongestoord je eigen gang te kunnen gaan'. Eén vorm van privacy, de ***INFORMELE* PRIVACY**, betreft de bescherming van persoonsgegevens. Vanuit dit oogpunt hebben anderen juist zo *min mogelijk* kennis over het data-subject. Per toepassing zal een afweging gemaakt moeten worden tussen het nut, de betrouwbaarheid en de (informationele) privacy. Naast primaire (persoons)gegevens moet ook **METADATA** (met wie en wanneer mensen en organisaties communiceren en zakendoen) worden beschouwd als gevoelig, bijvoorbeeld omdat het veel kan zeggen over het gedrag of karakter van een subject. Het zijn juist de metadata die het meest interessant zijn voor gerichte advertenties. Omdat administratieve beeldvorming de communicatie tussen mensen en organisaties ondersteunt, is ook de **COMMUNICATIEPRIVACY** relevant: het vertrouwelijk kunnen communiceren zonder dat anderen daar weet van hebben. Aanvullend speelt **FRAGMENTATIE** een belangrijke rol: Omdat met één infrastructuur een veelvoud aan toepassingen en contexten wordt bediend bestaat het risico dat de (meta)data en het gedrag van het subject uit al deze losse contexten aan elkaar te relateren valt, wat tot een onwenselijk omvangrijk beeld kan leiden.

Veel (vitale) processen zijn afhankelijk van deze administratieve beelden. Wanneer de nodige systemen of gegevens niet **BESCHIKBAAR** zijn, kan dit ernstige gevolgen hebben voor mensen en organisaties.

Terug naar inhoudsopgave

Doorgaans worden efficiënte en moeiteloze processen gezien als wenselijk. Vanuit dat oogpunt wordt **FRICTIE** beschouwd als een negatieve waarde en is het streven om zo gemakkelijk, goedkoop en snel mogelijk informatie te kunnen verzamelen over data-subjecten. Critici wijzen er echter op dat frictie ook een positief effect heeft: De benodigde moeite, kosten en tijd zorgen ervoor dat er minder gegevens worden gedeeld en dat mensen zich niet voor elk wissewasje hoeven te bewijzen.

Omdat de administratieve beeldvorming onvermijdelijk impact heeft op de voorgenoemde waarden is het van belang dat de betrokkenen, in het bijzonder het data-subject, **CONTROLE** kan hebben op (het gebruik van) administratieve beelden. Controle is nader te specificeren in **KENBAARHEID**, **ZEGGENSCHAP** en **GRIP**. Kenbaarheid is de mate van inzicht in (het gebruik van) gegevens. Zeggenschap is een bepaald *recht* om inspraak te hebben in het gebruik. En grip is het daadwerkelijk beschikken en bepalen over gegevens.

2.3 De toepassingsruimte: eilanden ondersteunen en verbinden

Om een breed inzetbare digitale identiteitsinfrastructuur te kunnen realiseren is het zinvol om een beeld te vormen van de toepassingsruimte. De toepassingsruimte strekt zich uit in diverse richtingen: over mensen en organisaties, over domeinen en sectoren, over landen en jurisdicties en ook over tijd. Allerlei culturele, organisatorische, politieke, juridische en economische 'eilanden' vallen daarmee binnen de toepassingsruimte. Ieder met eigen opvattingen, problemen en waarden. Het is niet alleen uitdagend om elk van die eilanden met één infrastructuur te *ondersteunen,* maar vooral uitdagend om ze te *verbinden*.

Naast internet en telefonie zijn er niet veel infrastructuren die opereren op deze schaal. De grootte van de toepassingsruimte hangt af van de flexibiliteit en sociale, technische en economische toegankelijkheid van de infrastructuur - en andersom. Waar de grens ook ligt en hoe groot de toepassingsruimte ook is, het ontwerp van een infrastructuur vergt een ruimere blik dan de eigen organisatie, ruimer dan het eigen domein en de eigen expertise.

2.4 Een model van de toepassingsruimte

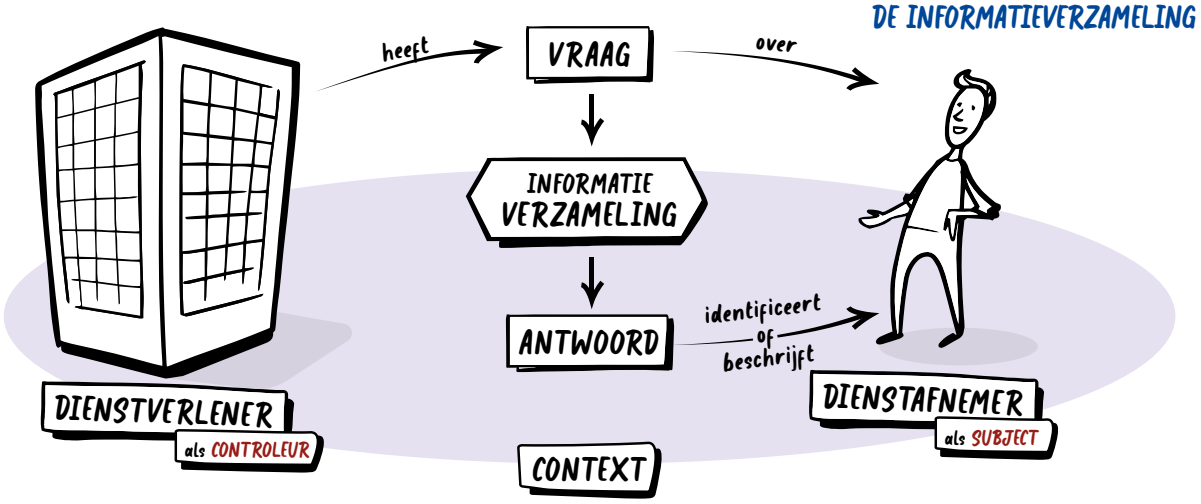
Ontwerpen voor die toepassingsruimte werkt niet door een oplossing eerst op één eiland te realiseren en daarna te proberen om die te vertalen naar het volgende eiland. In plaats daarvan moet een andere aanpak worden gehanteerd: een **generiek model** maken van de toepassingsruimte, op basis van kennis en ervaring uit de verschillende 'eilanden'. Op basis van dat model kan men vervolgens oplossingen ontwikkelen, die in specifieke toepassingen uitproberen en met de nieuwe inzichten het generieke model aanscherpen. Het model én de oplossing zijn in constante ontwikkeling. Deze aanpak heeft de laatste twee decennia onder andere geleid tot innovaties die zich nu onder de noemer Self-Sovereign Identity scharen, maar ook tot vele van de inzichten die in dit visiedocument zijn beschreven. Het generieke model van dit visiedocument heeft niet als doel om alle expertise te vatten, maar juist om los van die details – disciplineoverstijgend – het eens te worden over waar we staan en waar we heen willen.

Terug naar inhoudsopgave

2.5 De informatieverzameling: van vraag naar antwoord

Figuur 2 toont schematisch de toepassing van identiteitsinformatie in dienstverlening. Dienstverlener en dienstafnemer hebben een gezamenlijk doel: de dienst. Vanwege dat doel heeft de dienstverlener een **INFORMATIEVRAAG** over de dienstafnemer. In deze context nemen beiden een nieuwe rol aan: de dienstverlener handelt als **CONTROLEUR**, de dienstafnemer als **SUBJECT**[3] . Merk op dat de rollen ook omgekeerd kunnen zijn: de dienstáfnemer kan willen vaststellen dat de dienstverlener wel is wie hij zegt te zijn. In verdere discussie beschouwen we de controleur als de partij die de vraag heeft, en subject als de partij over wie die vraag gaat.

FIGUUR 2:
DE INFORMATIEVERZAMELING



De informatievraag kan *identificerend* zijn (zoals "welke klant heb ik aan de lijn?") of *beschrijvend* ("is deze gebruiker bevoegd?" of "waar woont deze persoon?"). Wat volgt is een proces van **INFORMATIEVERZAMELING**: de controleur kan *zelf* iets observeren ("de klant oogt 18+") of zal de informatie moeten halen uit de eigen administratie, (die van) het subject of (die van) een derde partij. Dit verzamelingsproces resulteert in een **INFORMATIEANTWOORD**, dat wederom *identificerend* ("Henk") en/of *beschrijvend* ("ja, 18+") kan zijn. Dat antwoord kan vervolgens door de controleur worden gebruikt.

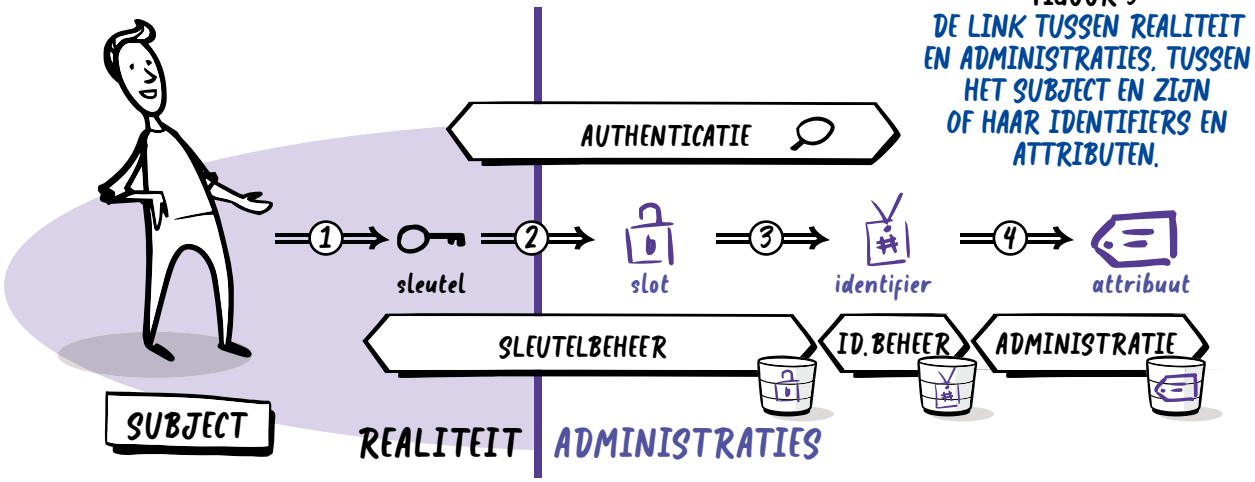
De **CONTEXT** waarin deze vraag, verzameling en antwoord een rol spelen is de interactie, of **TRANSACTIE**, tussen controleur en subject. Dat kan in een fysieke context zijn, aan de balie of aan de deur, of in communicatie op afstand, per post, telefonisch of elektronisch.

2.6 Link tussen realiteit en administraties

Om de gewenste informatie te kunnen verzamelen wordt één of meer administraties geraadpleegd. Daarbij is het van belang dat de link tussen de realiteit (de mens of organisatie in de rol van subject) en administratie (de administratieve beelden over dat subject) eerst gemaakt en later geverifieerd kan worden. Die link is geïllustreerd in Figuur 3.

[3] Voor de herkenbaarheid wordt het data-subject afgebeeld als mens. Een organisatie kan echter ook de rol van data-subject aannemen.

Terug naar inhoudsopgave



FIGUUR 3:
DE LINK TUSSEN REALITEIT EN ADMINISTRATIES, TUSSEN HET SUBJECT EN ZIJN OF HAAR IDENTIFIERS EN ATTRIBUTEN.

Er zijn diverse methoden om deze kloof tussen realiteit en administraties te overbruggen. Veelgebruikte methoden zijn gebaseerd op aspecten van de realiteit die kunnen worden *geobserveerd* (zoals vingerafdrukken, DNA, gezichten), *verzonnen* (zoals wachtwoorden en PIN-codes) of *gemaakt* (zoals paspoorten en SIM-kaarten). Een kopie, afgeleide of ander referentiemateriaal van die sleutels (hier als 'slot' gesymboliseerd) wordt vastgelegd in administraties om de link tussen realiteit en administraties tot stand te brengen.

De 4 schakels tussen de 5 elementen van deze link (mens, sleutel, slot, identifier en attribuut) beïnvloeden de betrouwbaarheid van de informatie. In de creatie en het beheer van deze link onderscheiden we drie beheersactiviteiten: sleutelbeheer, identifierbeheer en administraties. Authenticatie, de vierde activiteit, stelt ten tijde van de informatieverzameling vast of de link correct is. Deze vier activiteiten worden hieronder kort toegelicht.

2.6.1 Administratie

De verzamelterm **ADMINISTRATIE** wordt in dit document gebruikt om te verwijzen naar het geheel aan processen en systemen dat zich bezighoudt met het vastleggen en beheren van gegevens. Die processen en systemen zijn gespecialiseerd op de specifieke toepassing waarvoor ze zijn ontwikkeld. Er zijn immers wezenlijke verschillen tussen het burgerregister en het handelsregister en tussen de administratie van de voetbalclub en patiënten-dossiers. Het administratief beeld, zoals geïntroduceerd in Figuur 1, is het geheel aan attributen dat een partij aan één data-subject kan relateren. Naast persoonsgegevens als naam en geboortedatum, kunnen daaronder ook verbanden met andere zaken worden verstaan, zoals de eigendom van een auto of huis, een arbeidsrelatie met een bedrijf, et cetera.

Om culturele, organisatorische, politieke, juridische en economische barrières te kunnen overbruggen zal een digitale identiteitsinfrastructuur los moeten staan van de inhoud, vorm en betekenis van gegevens. Pogingen om deze inhoud, vorm en betekenis te standaardiseren vallen dan ook buiten de scope van deze visie. Een administratie wordt in deze beschouwing enkel gezien als een black-box waaruit antwoord kan worden gegeven op informatievragen.

Terug naar inhoudsopgave

2.6.2 Identifierbeheer

Onder **INDENTIFIERBEHEER** verstaan we het aanmaken, onderhouden en vernietigen van identifiers. Het doel is om binnen een bepaalde context naar individuele entiteiten te kunnen verwijzen, die te kunnen identificeren. Zo kent de Nederlandse overheid aan iedere burger één Burgerservicenummer (BSN) toe, kennen e-mailproviders één of meer e-mailadressen toe, en kan men op sociale media een eigen gebruikersnaam kiezen. Het identifierbeheer borgt, afhankelijk van het doel, bepaalde voorwaarden zoals *inclusiviteit* (alle personen een identifier), *singulariteit* (elk persoon heeft maar één identifier), *uniciteit* (elke identifier wordt maar door één persoon gebruikt) en *herleidbaarheid* (de identifier is terug te leiden naar de fysieke persoon).

Het gebruik van identifiers heeft invloed op de privacy. Wanneer één identifier door vele organisaties, in vele toepassingen en/of voor een lange periode wordt gebruikt, ontstaat het risico dat een omvangrijk beeld van (het gedrag van) het subject gemaakt wordt. Een beeld dat mogelijk misbruikt kan worden. Dit is één van de redenen om het gebruik van het BSN te beperken. Deze privacy-impact is te reduceren door wegwerpidentifiers te gebruiken of een ander pseudoniem te hanteren voor elk van de partijen waarmee het subject communiceert. Daarmee wordt het lastiger voor partijen om hun administraties aan elkaar te linken, of dat criminelen dat doen in het geval van datalekken.

Identifiers zijn een onmisbare schakel in de link tussen realiteit en administraties. Zonder identifier is de mens onzichtbaar en daardoor uitgesloten van (vitale) dienstverlening. Tevens is het gebruik van identifiers waardengevoelig. Een digitale identiteitsinfrastructuur kan het identifierbeheer ondersteunen door verschillende vormen van (pseudonieme) identificatie te standaardiseren.

2.6.3 Sleutelbeheer

Onder **SLEUTELBEHEER** valt het toekennen en intrekken van sleutels waarmee personen (of organisaties) kunnen bewijzen bij hun identifiers te horen. Sleutelbeheer moet verlies van sleutels, evenals onrechtmatig gebruik van sleutels voorkomen. Wanneer het subject de sleutels verliest heeft hij of zij geen toegang meer tot een identifier en alle waarde die daar in administraties aan is gekoppeld. In zo'n geval moet het subject bewijzen dat hij of zij bij de identifier hoort, zónder de sleutels te kunnen laten zien. Een digitale identiteitsinfrastructuur zou het sleutelbeheer in deze uitdagingen kunnen ondersteunen.

2.6.4 Authenticatie

AUTHENTICATIE heeft als doel om tijdens een transactie vast te stellen dat een persoon hoort bij een bepaalde identifier (dat hij is wie hij zegt dat hij is). De persoon presenteert dan de eerder vastgelegde sleutel. Als deze sleutel overeenkomt met het referentiemateriaal dan is de kans groot dat die persoon het rechtmatige data-subject is. De kwaliteit en beveiliging van de activiteiten sleutelbeheer en authenticatie vormen samen de authenticatiezekerheid, ook bekend als 'Level of Assurance' (LoA). Zonder (geslaagde) authenticatie zou identiteitsfraude kunnen plaatsvinden, wat de controleur, het werkelijke subject en/of andere belanghebbenden kan schaden.

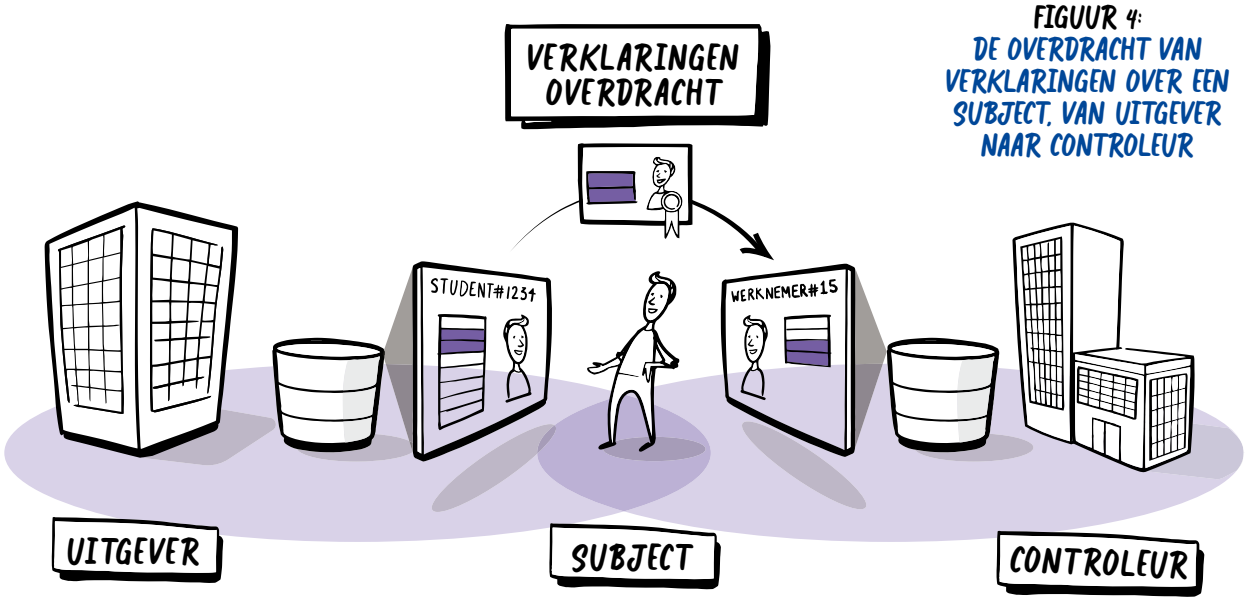
Terug naar inhoudsopgave

Normaliter worden deze links beheerd door één of meer organisaties, wat subject en controleur afhankelijk maakt van die organisaties. Zonder die link is het subject praktisch onzichtbaar, zoals de vluchtelingencrisis pijnlijk duidelijk maakt[4]. Indien mogelijk is deze link echter gegarandeerd en onder volledige controle van het subject; een taak die bij de digitale identiteitsinfrastructuur belegd zou kunnen worden. Zo vestigt hij of zij namelijk zelf, bij wijze van spreken, een vaste voet in de 'administratieve wereld'.

Kader 1. Een voorbeeld van de link tussen subject en administraties
Puk wil online zorgkosten declareren bij haar zorgverzekeraar. De zorgverzekeraar moet weten met welke verzekerde hij te maken heeft (identificeren) en gebruikt daarvoor DigiD. DigiD is verantwoordelijk voor het **SLEUTELBEHEER** en heeft eerder aan Puk twee middelen (**SLEUTELS**) heeft uitgegeven: een combinatie van gebruikersnaam en wachtwoord en de DigiD app. Het **IDENTITEITENBEHEER** valt onder verantwoordelijkheid van de Basisregistratie Personen (BRP). De BRP heeft aan Puk een BSN toegekend. De zorgverzekeraar voert een eigen **ADMINISTRATIE** waarin Puks **IDENTIFIER** (het BSN, of een afgeleide daarvan) is gekoppeld aan **ATTRIBUTEN**, zoals haar polis of betaalgeschiedenis. Door in te loggen met DigiD (**AUTHENTICATIE**) weet de zorgverzekeraar bij welke **IDENTIFIER** Puk hoort en dus bij welk **ADMINISTRATIEF BEELD**. Op basis van dat beeld worden de diensten verleend.

2.7 Verklaringenoverdracht

In sommige gevallen kan de controleur zijn informatievraag niet zelf beantwoorden, maar een andere partij wél. Aldus ontstaan **IDENTITEITSKETENS**, waarbij diverse **KETENPARTIJEN** informatie uitwisselen over hetzelfde subject. Wanneer een partij informatie over een subject deelt, geeft het in feite een **VERKLARING** uit. Die partij neemt daardoor de rol van **UITGEVER** aan, zie Figuur 4.



FIGUUR 4:
DE OVERDRACHT VAN VERKLARINGEN OVER EEN SUBJECT, VAN UITGEVER NAAR CONTROLEUR

[4] Vluchtelingen die naar Europa komen zonder identificatiemiddelen kunnen moeilijk, of helemaal niet, gebruik maken van vitale dienstverlening. Bron: UNHCR (https://www.unhcr.org/)

Terug naar inhoudsopgave

Zo is een gemeente uitgever van fysieke verklaringen in de vorm van een paspoort, rijbewijs of identiteitskaart. Hoewel de informatie en toepassing ver uiteenlopen zijn er bij **VERKLARINGENOVERDRACHT** grote overeenkomsten te bespeuren. We benoemen drie grote uitdagingen:

1. **Logistiek:** hoe komt de verklaring van de uitgever veilig bij de controleur?
2. **Autorisatie van de uitgever:** hoe kan de controleur *vertrouwen* op de verklaring van de uitgever?
3. **Autorisatie van de controleur:** hoe komt de verklaring alleen bij bevoegde controleurs voor het toegestane gebruik?

2.7.1 Logistiek

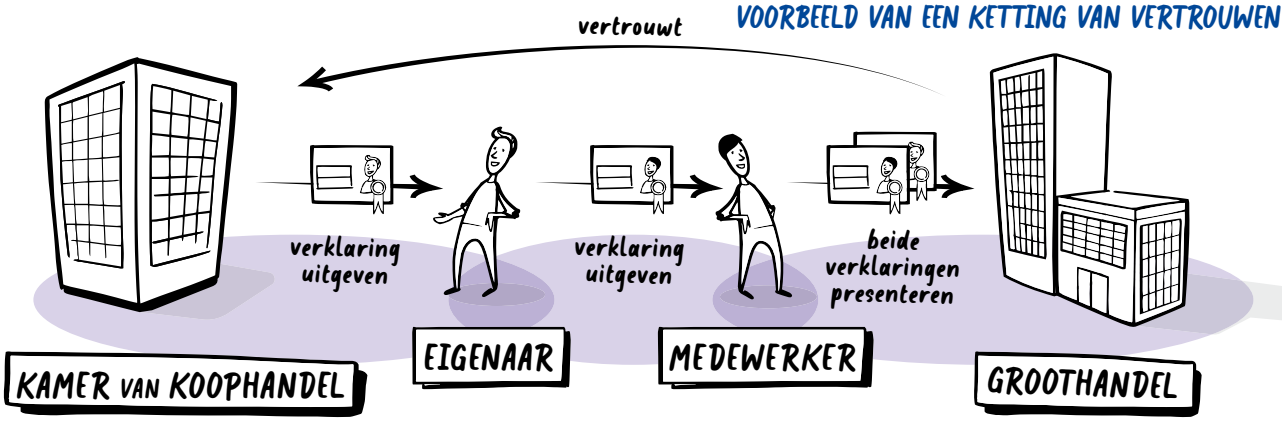
Om een informatievraag te kunnen beantwoorden moeten verklaringen van een uitgever naar een controleur worden getransporteerd. Dit kan bijvoorbeeld rechtstreeks, of via een bemiddelaar (zoals een gegevenskluis of -sluis) of via het subject (zoals met fysieke documenten het geval is). Het logistieke ontwerp heeft invloed op veel waarden van subject en controleur als het afhankelijkheden van (en mogelijk surveillance en controle door) derden introduceert. Een digitale identiteitsinfrastructuur kan de logistiek onder andere ondersteunen door de verklaringenoverdracht te standaardiseren en de benodigde communicatiekanalen te hergebruiken. Dit kan de frictie voor verklaringenoverdracht aanzienlijk verminderen.

2.7.2 Autorisatie van de uitgever

De toegevoegde waarde van een verklaring volgt uit wie hem uitgeeft. Zo mag de Kamer van Koophandel verklaringen (uittreksels) uitgeven die stellen wie de eigenaar is van een bedrijf. En elke Nederlandse universiteit mag een WO-diploma uitgeven. In de basis is de controleur verantwoordelijk voor het (direct of indirect) autoriseren van de uitgever. Alvorens de controleur een verklaring gebruikt zal het de herkomst van die verklaring moeten verifiëren én moeten bepalen of het verklaringen van die uitgever wil accepteren.

Uit deze behoefte ontstaat een nieuwe informatievraag: wie (of wat) is de uitgever? Het antwoord op die vraag kan wederom door een andere uitgever worden vastgesteld, en worden bewezen met een verklaring. Zo kan een **VERTROUWENSKETEN** ontstaan, een aaneenschakeling van partijen die elkaar vertrouwen die eindigt bij een **VERTROUWENSANKER**, een partij die door de controleur rechtstreeks of impliciet wordt vertrouwd. Het volgende voorbeeld (ook weergegeven in Figuur 5) illustreert hoe zo'n vertrouwensketting in het zakelijke verkeer kan werken:

FIGUUR 5:
VOORBEELD VAN EEN KETTING VAN VERTROUWEN



Terug naar inhoudsopgave

Kader 2. Versimpeld voorbeeld van een ketting van vertrouwen
Pim werkt voor Puk en gaat namens Puk BV naar de groothandel. De groothandel wil vaststellen dat Pim bevoegd is om op rekening van Puk BV te kopen. Pim toont daarvoor een machtiging (verklaring) van Puk. De volgende vraag is of de uitgever van die verklaring zélf wel bevoegd is. Met een verklaring van de KVK, een uittreksel uit het handelsregister, kan worden aangetoond dat Puk de eigenaar is van Puk BV. Omdat de groothandel de KVK rechtstreeks vertrouwt is de KVK in dit voorbeeld het vertrouwensanker en is de vertrouwensketting gesloten.

2.7.3 Autorisatie van de controleur

Omdat de verklaringen (gevoelige) gegevens bevatten moeten deze niet in verkeerde handen vallen. Voorafgaand aan elke overdracht moet worden bepaald *wie* de controleur is en of deze controleur bevoegd is om de gegevens in de verklaring op de beoogde manier te verwerken. Die verantwoordelijkheid kan onder meer liggen bij de uitgever, bij een eventuele bemiddelaar (kluis of sluis) en/of bij het subject.

Uitgevers zullen doorgaans een zorgplicht hebben richting het subject van de verklaring en daardoor (mede) verantwoordelijk zijn voor de autorisatie van de controleur. Het kan echter ook onwenselijk zijn dat de uitgever kennis heeft van individuele transacties tussen subject en controleur. Zo kan men met een fysiek identiteitsbewijs elke kroeg of casino betreden zonder dat de uitgever (de gemeente) daar zicht op heeft. In het digitale domein ligt dat echter anders. Wanneer iemand ergens inlogt met DigiD, registreert DigiD de metadata van die inlogpoging en kan de overheid in theorie meekijken op het onlinegedrag.

In veel gevallen kan een subject ook zeggenschap hebben over wie zijn of haar gegevens mag inzien en daardoor grip willen hebben op de verklaringen die hem of haar betreffen. Een digitale identiteitsinfrastructuur kan helpen zowel uitgever als controleur te autoriseren voor het respectievelijke uitgeven en gebruiken van verklaringen. Tevens kan zo'n infrastructuur borgen dat het subject de regie houdt op verklaringen die hem of haar betreffen.

Terug naar inhoudsopgave

2.8 Op naar een digitale identiteitsinfrastructuur

Een digitale identiteitsinfrastructuur kan dienstverlening aanzienlijk verbeteren door het voor mensen en organisaties eenvoudig te maken om elkaar op hoogwaardig niveau te *identificeren* en te *beschrijven*. Het raakvlak tussen uitgever, subject en controleur (verklaringenoverdracht) en het raakvlak tussen administraties en subjecten (sleutelbeheer en authenticatie) lenen zich er goed voor om gestandaardiseerd te worden. Twee *functionele* idealen volgen uit de voorgaande analyse:

1. Idealiter biedt de infrastructuur aan subjecten ten minste één (pseudonieme) link met administraties, zodat zij zich daar – onafhankelijk van derden – kenbaar kunnen maken.
2. Idealiter biedt de infrastructuur elke partij, inclusief subjecten zelf, de kans om moeiteloos eigen verklaringen uit te geven en die van anderen te verifiëren, terwijl het subject de controle kan hebben over de verklaringenoverdracht.

De rest van dit visiestuk bouwt voort op de algemene beschrijving van de context die hierboven is gegeven en geeft vorm en richting aan een digitale identiteitsinfrastructuur.

Terug naar inhoudsopgave

3 Gedeelde waarden

Om de ontwikkeling van een digitale identiteitsinfrastructuur in goede banen te leiden en op waarde te schatten is het nodig om vast te stellen wat we verstaan onder waardevol. Welke normen moeten te allen tijde worden gebord? En welke vrijheid moeten de gebruikers van de infrastructuur hebben om zelf de gewenste balans tussen waarden te vinden? Het vorige hoofdstuk introduceerde 9 relevante waarden. Om tot een gewogen waarden en normenkader te komen is meer onderzoek en overweging nodig. Dit hoofdstuk is een eerste aanzet tot een gezamenlijk kader, in de vorm van overwegingen onder elk van de 9 waarden.

3.1 Nut: een nuttig antwoord

De inzet van identiteitsmiddelen dient altijd een bepaald doel. Zo wil een dienstverlener diensten personaliseren, of beschermen tegen ongeautoriseerde afnemers. Dat doel wordt allereerst vertaald in een bepaalde informatievraag, zoals 'is het subject 18 jaar of ouder?' of 'kan het subject deze huursom betalen?'. Vervolgens wordt bepaald welke gegevens, uit welke bron, *antwoord* op die vraag moeten geven (zoals een identiteitsbewijs). Het nut is de mate waarin de controleur iets met het antwoord kan.

a) Het antwoord op de informatievraag – het resultaat uit authenticatie of verklaringenoverdracht – dient alleen het beoogde doel.

3.2 Informationele Privacy: een minimaal antwoord

Informationele Privacy gaat over de bescherming van (persoons)gegevens en staat per definitie op gespannen voet met de behoefte om iemand te identificeren (of te beschrijven) ten einde een dienst te verlenen. Er dient altijd een afweging te worden gemaakt tussen het nut en de impact op de privacy. Daarbij spelen, zoals ook in de privacyverordening AVG is vastgelegd, onder meer de volgende twee principes een rol: **proportionaliteit** houdt in dat het doel opweegt tegen de impact op de privacy. **Subsidiariteit** houdt in dat wanneer hetzelfde doel te bereiken is met een alternatief middel dat minder impact op de privacy heeft, dat alternatief moet worden gebruikt. De beoogde digitale identiteitsinfrastructuur realiseert zo'n alternatief. Overwegingen:

a) De uitgever van een verklaring bepaalt de (hoeveelheid) informatie die zo'n verklaring bevat. De huidige fysieke waardepapieren, welke veelal een verzameling van gegevens bevatten, kunnen één-op-één als digitale verklaring worden uitgegeven. Het grote voordeel van digitale verklaringen is dat ze veel goedkoper zijn. Een digitale handtekening, die de integriteit en authenticiteit van de verklaring borgt, is immers goedkoop te zetten. Dat maakt het mogelijk op attribuutniveau (of zelfs kleiner) verklaringen uit te geven. Ook andere mechanismen die de hoeveelheid overgedragen informatie kunnen beperken, zoals Zero-Knowledge Proofs (ZKPs) kunnen worden ingezet. Naast het faciliteren van granulariteit is het ook denkbaar dat een infrastructuur stimuleert of zelfs helpt afdwingen dat gegevensdeling tot een minimum wordt beperkt.

Terug naar inhoudsopgave

b) Het is niet te garanderen wat een partij doet met bepaalde informatie nadat het die heeft geleerd. Een infrastructuur kan echter wel helpen om vast te leggen welke partij om welke gegevens heeft gevraagd op welk moment, en welke gegevens vervolgens al dan niet zijn verstrekt. Dergelijke verslaglegging kan dienen als bewijs in geval van een dispuut. Dit kan tevens een afschrikkende werking hebben; zowel tegen onrechtmatige gegevensverzoeken als tegen onrechtmatig gebruik van verkregen gegevens.

c) Ook de impact op de informationele privacy te reduceren is, wordt het subject alsnog gevraagd te bewijzen dat hij of zij aan bepaalde criteria voldoet. Het wegnemen van de bezwaren van informationele privacy kan juist tot gevolg hebben dat meer van dit soort controles worden opgeworpen. Dit kan privacy in de bredere definitie schaden.

3.3 Representativiteit: een nauwkeurig antwoord

Voor een eerlijke behandeling is het van belang dat de informatievraag, en het antwoord, representatief zijn voor het subject. Dekt het antwoord de hele lading? Het gevaar van een (administratief) beeld is dat het in processen de echte mens vervangt. Oftewel dat het administratieve beeld als absolute waarheid wordt aangenomen. In werkelijkheid is het antwoord op de informatievraag nooit een 'gegeven' (onweerlegbaar feit)[5], maar altijd een verklaring van een bepaalde partij. Overwegingen:

a) Heeft het subject zicht op de gegevens en voor welke doeleinden deze worden gebruikt? Kan het daarover oordelen en invloed op uitoefenen?

3.4 Controle op het antwoord én de verzameling

Het is van belang dat het subject een bepaalde mate van controle heeft op het gebruik van zijn/haar administratieve beelden. Die beeldvorming heeft namelijk invloed op hoe het subject wordt behandeld (in dienstverlening) en op de privacy. Overwegingen:

a) Het subject moet zicht hebben op het gebruik van zijn/haar administratieve beelden. Het moet onder andere duidelijk zijn wie welke (meta)data heeft verkregen en voor welke doeleinden. Deze **KENBAARHEID** is de basis voor invloed die het subject indirect (bijvoorbeeld via een rechter) danwel direct (door eigen handelen) kan uitoefenen op identiteitstransacties. Deze informatie moet begrijpelijk gemaakt worden. Terwijl volledige transparantie richting het subject moet zijn geborgd is het ook van belang het subject niet te overbelasten.

b) De mate van **ZEGGENSCHAP** die het subject heeft over een bepaalde gegevensstroom, verschilt per context. 'Toestemming' is slechts één van de mogelijke juridische gronden waarop een organisatie gegevens van het subject mag verwerken. Echter, los van de juridische grond is het belangrijk de autonomie van het subject te respecteren. Ook al heeft een organisatie het recht bepaalde verklaringen te ontvangen, het is aan het subject om die verklaringen over te dragen. Dit is vergelijkbaar met grip op geld: ook al heeft iemand een schuld uitstaan, de schuldeiser mag dit geld niet zomaar afnemen. Wanneer het subject daadwerkelijk **GRIP** heeft op sleutels (en daarmee identifiers) en gegevens zijn daarmee zowel kenbaarheid als zeggenschap in bepaalde mate geborgd.

[5] Hoewel het in wetgeving misschien precies zo behandeld wordt is het belangrijk te blijven erkennen dat het in werkelijkheid niet zo is.

Terug naar inhoudsopgave

c) Wanneer de grip op attributen en identifiers feitelijk bij het subject ligt moet alsnog worden overwogen of het subject die daadwerkelijk kán beheersen. (Sommige) uitgevers van verklaringen hebben een bepaalde zorgplicht; een verantwoordelijkheid om het subject te beschermen tegen onrechtmatig of anderzijds schadelijk gebruik van hun gegevens. Bij het toekennen van controle zal moeten worden gelet op de kennis en kunde die het subject nodig heeft om de consequenties te overzien en verstandige beslissingen te maken, in de algemeenheid maar ook in specifieke contexten. De algemene beheersing zou onder andere kunnen worden verhoogd door een consistente en vertrouwde interface aan te bieden en op transactieniveau (automatisch) te adviseren. De gebruikers van de digitale identiteitsinfrastructuur moeten de ruimte hebben om de gewenste balans tussen bescherming en autonomie te vinden.

d) Indien toestemming de juridische basis is waarop gegevens zijn verstrekt is het van belang dat het subject het overzicht behoudt van alle eerder verleende toestemming. Tevens is het van belang dat het subject die toestemming met minimale moeite direct kan intrekken.

3.5 Betrouwbaarheid: een betrouwbaar antwoord

De identifiers en attributen van het subject kunnen een aantrekkelijk doelwit zijn voor identiteitsfraudeurs. Een foutieve authenticatie kan leiden tot substantiële schade voor zowel controleur als subject, maar ook voor derden. Daarnaast moet het subject ook kunnen vaststellen dat de controleur betrouwbaar is en de juiste organisatie is voor de betreffende transactie. Overwegingen:

a) In beginsel moet niemand anders dan het rechtmatige subject kunnen bewijzen bij zijn of haar identifiers te horen. Wanneer de digitale identiteitsinfrastructuur het mogelijk (en makkelijk) maakt dat mensen en organisaties hun eigen sleutels kunnen maken en beheren, kan een hoge mate van zekerheid worden gerealiseerd in identiteitstransacties. Daartoe is het van belang dat de betrokken partijen die sleutels ook zelfstandig, zonder tussenkomst van een derde, kunnen verifiëren.

b) Wanneer authenticatie standaard wederzijds is, is het subject er altijd zeker van aan wie hij zich authenticeert, danwel aan wie hij gegevens presenteert. Dit verlaagt onder andere de kans op phishing.

c) De betrouwbaarheid van een verklaring bestaat uit de integriteit, authenticiteit en de mate waarin de verklaring aan het subject is verbonden (subject-binding). Wanneer deze kwaliteiten in de verklaring zelf zijn geborgd, zoals ook een fysiek paspoort voorzien is van echtheidskenmerken, wordt de verklaring mobiel en behoudt deze waarde ongeacht externe factoren. De verklaring bevat dan zelf het bewijs van echtheid; waardoor het niet nodig is om contact op te nemen met de uitgever van de verklaring.

d) Het is echter wel mogelijk dat verklaringen hun geldigheid verliezen nadat ze zijn uitgegeven. Bijvoorbeeld doordat het oorspronkelijke gegeven is veranderd (zoals een adreswijziging) of doordat achteraf bleek dat de verklaring ten onrechte was uitgegeven. Samengevat kan de status van een verklaring veranderen nadat het is uitgeven en die status kan relevant zijn voor de controleur. De digitale identiteitsinfrastructuur moet de communicatie van status faciliteren zonder dat daarbij een inbreuk wordt gemaakt op de privacy, controle of andere hier besproken waarden. De overwegingen omtrent statuswijziging vragen om meer verdieping.

Terug naar inhoudsopgave

3.6 Beschikbaarheid: altijd een antwoord

Veel essentiële processen zijn afhankelijk van authenticatie en verklaringenoverdracht. Wanneer de nodige systemen niet beschikbaar zijn, kan dit ernstige gevolgen hebben voor mensen en organisaties. Een storing van of aanval op DigiD bijvoorbeeld zou een groot deel van de (digitale) communicatie tussen burgers en overheid lamleggen. Ook wanneer de nodige gegevens verloren raken of hun waarde verliezen – zoals diploma's die niet meer te verifiëren zijn als de onderwijsinstelling stopt – is dat problematisch voor het subject. Overwegingen:

a) Het streven naar een breed gebruikte digitale identiteitsinfrastructuur heeft als gevolg dat deze een kritieke en daarmee onmisbare rol krijgt in de dienstverlening. Wanneer (delen van) de infrastructuur niet-beschikbaar raken, hebben mensen en organisaties geen toegang meer tot (vitale) dienstverlening. Het is onacceptabel om centrale zwaktepunten in het systeem te introduceren.
b) Het is belangrijk voor subjecten dat hun toegang tot administratieve beelden, tot identifiers en attributen, zo lang beschikbaar blijft als zij dat wensen. Dit geldt ook voor ingetrokken of gerectificeerde verklaringen, met dien verstande dat de intrekking of rectificatie voor controleurs altijd zichtbaar is (een subject kan een ongeldige verklaring niet presenteren als zijnde geldig). Welke factoren bedreigen de beschikbaarheid van identifiers en attributen? Welke maatregelen neemt de digitale identiteitsinfrastructuur tegen deze bedreigingen?

3.7 (Communicatie)privacy: geen lekkage van (meta)data

Authenticatie vereist ten minste communicatie tussen het subject en de controleur; bij verklaringenoverdracht is ook nog een bron betrokken. Afhankelijk van de opzet van de infrastructuur zijn meer partijen actief tijdens een transactie, zoals gegevensverwerkers, datakluizen en -sluizen. Het is voor het subject van belang dat zo min mogelijk partijen kennis hebben van (1) de informatie die wordt gecommuniceerd (informationele privacy), (2) de metadata van die communicatie – wie met wie communiceert en wanneer (metadata/communicatieprivacy) en (3) de relatie tussen het subject en controleur. Overwegingen:

a) Bij de ontwikkeling van een digitale identiteitsinfrastructuur moet worden gestreefd naar een zo minimaal mogelijke impact op de (communicatie)privacy. De rol- en taakverdeling van de infrastructuur draagt hier aanzienlijk aan bij. Welke inzicht in (meta)data volgt uit ieder van de toegewezen rollen? Is het bijvoorbeeld mogelijk dat partijen bemiddelen als gegevenskluis of -sluis? Heeft de uitgever van verklaringen inzicht in hoe de verklaringen worden gebruikt en/of met wie ze worden gedeeld? Dergelijk inzicht (of toezicht) kan ook als noodzakelijk worden bestempeld; bijvoorbeeld vanuit een zorgplicht. De vraag is echter of dergelijke belangen (de bescherming van subjecten) ook met andere, minder invasieve, middelen te realiseren zijn (het principe van subsidiariteit). Het streven is dat enkel de noodzakelijk betrokken partijen kennis krijgen van de relatie dan wel communicatie (metadata) tussen subject en controleur.
b) Ongeacht de keuze is het van belang dat op systeemniveau en transactieniveau transparant is welke partijen betrokken zijn en welke mate van inzicht zij genieten in transacties. Alleen met deze kennis kunnen mensen en organisaties hun eigen privacy beschermen.

Terug naar inhoudsopgave

3.8 Frictie: moeiteloos een antwoord

Doorgaans worden efficiënte en moeiteloze processen gezien als wenselijk. Vanuit dat oogpunt is het streven dan ook om authenticatie en verklaringenoverdracht zo gemakkelijk, goedkoop en snel mogelijk te maken. Critici wijzen er echter op dat frictie ook een positief effect heeft[6]: De benodigde moeite, kosten en tijd zorgen ervoor dat er minder gegevens worden gedeeld en dat mensen zich niet voor elk wissewasje hoeven te bewijzen. Frictie kan dus een natuurlijk middel zijn om de privacy (informationeel, maar ook rust) van subjecten te beschermen. Het is echter een middel waar men weinig controle over heeft: het benadeelt alle toepassingen, niet alleen de onwenselijke toepassingen van authenticatie en verklaringenoverdracht. Een universele oplossing kan de moeite, kosten en tijd significant verlagen, maar vereist dan een nieuwe vorm van (kunstmatige) frictie om dit negatieve effect te voorkomen. Overwegingen:

a) In de basis is het gewenst om het gebruik van een gedegen identiteitsinfrastructuur, waarin de relevante waarden zijn geborgd, zo toegankelijk mogelijk te maken. Dit voorkomt dat partijen terug moeten vallen op ongunstiger alternatieven.
b) Tegelijkertijd is het van belang dat het mensen (en organisaties) niet té eenvoudig wordt gemaakt dat ze zich niet meer bewust zijn van de informatieverzameling (en beoordeling) die plaatsvindt, of dat men zich te makkelijk in riskante praktijken mengt. De digitale identiteitsinfrastructuur moet zichtbaar en/of kenbaar zijn.
c) Voor de inzet van een digitale identiteitsinfrastructuur moet worden onderzocht wat het effect van deze frictievermindering is én moet worden gezocht naar manieren om de daaruit volgende risico's (zoals overvraging) te beperken. Het afzien van digitalisering van informatievergaring is daar nadrukkelijk een afweging in.

3.9 Fragmentatie: informatie zoveel mogelijk gescheiden

Iedere organisatie (of ander mens) waarmee het subject een relatie heeft zal een eigen beeld van dat subject hebben; de administratieve beeldvorming is dus **gefragmenteerd** over al die organisaties (en mensen). Deze fragmentatie is natuurlijk omdat beeldvorming in de basis subjectief en persoonlijk is en in de aard van elke relatie en context weer andere zaken relevant zijn. **Fragmentatie** kan enerzijds worden beschouwd als een *positieve waarde*. Het andere uiterste is een alomvattend beeld van het subject, wat kan worden gebruikt om het subject te targeten of anderzijds te manipuleren. Zo'n alomvattend beeld is tevens een aantrekkelijk doelwit voor hackers. Anderzijds kan fragmentatie een *negatieve waarde* zijn, wanneer het de controleur weerhoudt om een nuttig of representatief beeld te vormen. Overwegingen:

a) Wordt fragmentatie bedreigd? Riskeren van nature gescheiden administraties door een partij aan elkaar te worden geknoopt? Bijvoorbeeld doordat gegevens uit verschillende administraties via één knooppunt worden gecommuniceerd?
b) Wordt correlatie (van transacties en/of administratieve beelden) actief bestreden? Bijvoorbeeld doordat voor iedere relatie standaard een uniek pseudoniem wordt gebruikt, in plaats van één identifier in allerlei contexten te gebruiken. En (voor wie) is de uitgifte van een verklaring te correleren met de presentatie van die verklaring?

[6] https://philipsheldrake.com/2020/11/the-dystopia-of-self-sovereign-identity-ssi/

Terug naar inhoudsopgave

4 Een gedeeld mechanisme

Hoofdstukken 2 en 3 schetsen een enorme gezamenlijke uitdaging: een digitale identiteitsinfrastructuur met grote potentie voor zowel dienstverleners als afnemers, voor zowel mensen als organisaties. **Eén infrastructuur die culturele, organisatorische, politieke, juridische en economische 'eilanden' verbindt én waarbij het subject de controle heeft over de informatie-uitwisseling die hem of haar betreft.** Die toepassingsruimte is veel groter dan waar eerdere vertrouwensnetwerken of afsprakenstelsels voor zijn ontwikkeld. Het is *terra incognita* - onbekend terrein.

In het huidige digitale domein spelen vertrouwensdiensten een belangrijke rol. Figuur 6 toont voorbeelden waarin authenticatie bemiddeld wordt door uiteenlopende diensten of toepassingen, zoals een authenticatiedienst (1), verklaringenoverdracht rechtstreeks tussen bron en controleur plaatsvindt (2) ofwel bemiddeld wordt door een gegevenskluis of -sluis (3). De afhankelijkheid, invloed en surveillance die deze vormen introduceren – evenals het gebrek aan controle door het subject – maakt dat deze vormen inbreuk maken op de waarden die in het vorige hoofdstuk zijn besproken. **Hoe kunnen al die eilanden verbonden worden zonder rechtstreekse communicatie of bemiddeling door vertrouwensdiensten?**

Het lijkt een logische stap om *het subject zelf* die eilanden te laten verbinden. 'Hij of zij' is immers de enige overeenkomst tussen alle informatievragen die over 'hem of haar' gaan. Dit is in overeenstemming met het SSI-gedachtegoed. Dit idee is niet vreemd: met fysieke paspoorten overbrugt het subject per slot van rekening óók al die eilanden. Maar de aard van het *digitale* domein is veel complexer, gevaarlijker en vooral ongrijpbaarder; waar men in de fysieke wereld een uniek en herkenbaar mens voor zich ziet die een legitiem paspoort toont met daarop zijn of haar gezicht, ziet men in de digitale wereld enkel een reeks nullen en enen binnenkomen. Het zijn de natuurwetten die de fysieke realiteit beperken en daarmee transparanter en voorspelbaarder maken. Ze vormen een onvrijwillig contract tussen alle mensen (en organisaties), wat niet gehandhaafd hoeft te worden omdat het onmogelijk is om die wetten te overtreden – ongeacht opzet of onkunde. Natuurwetten vormen een **MECHANISME** dat in het digitale domein ontbreekt.

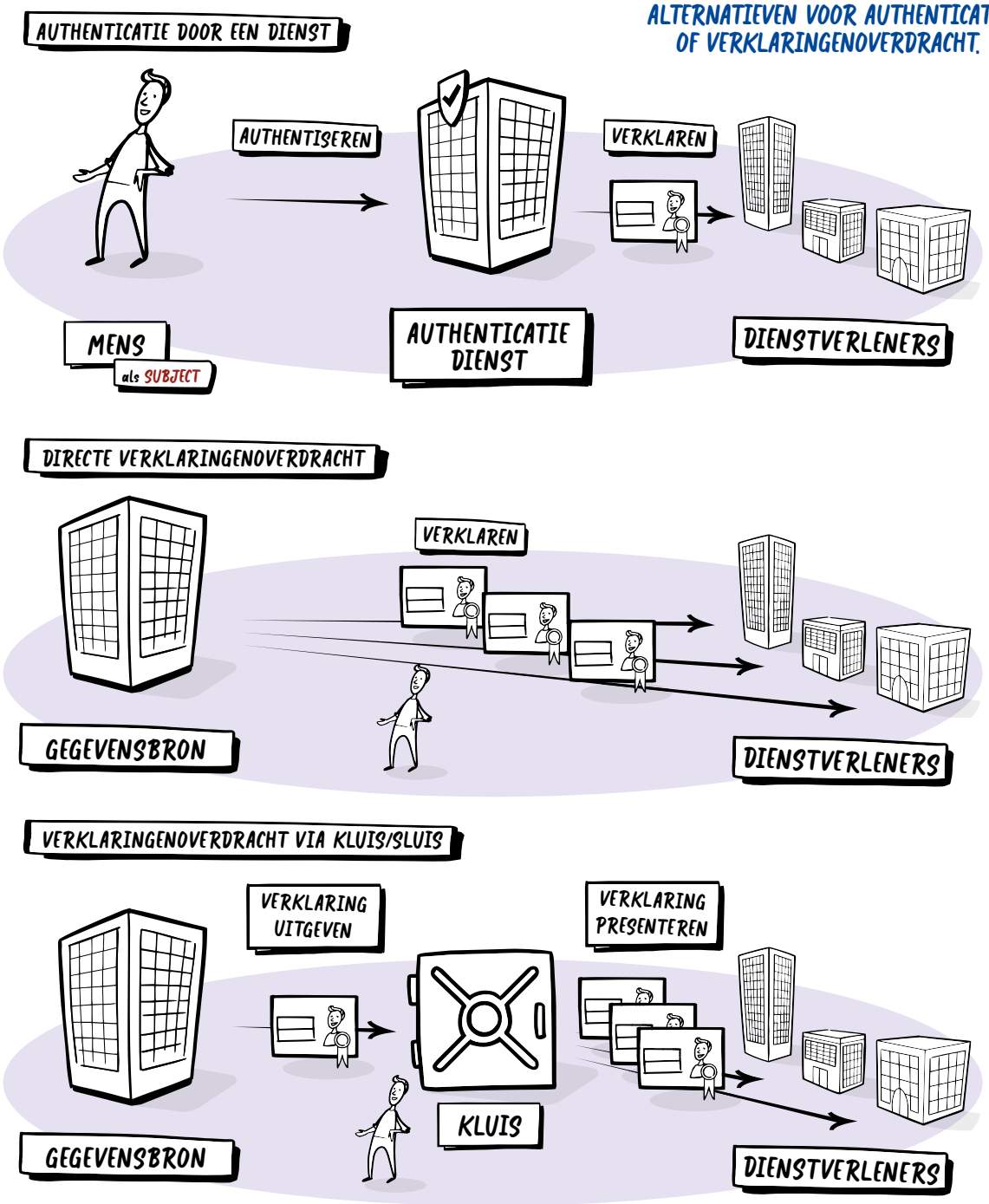
Door technologische ontwikkelingen die de laatste jaren zijn samengekomen onder de noemer Self-Sovereign Identity, lijken we nu een equivalent mechanisme te kunnen realiseren in de digitale wereld. **Met een transparant en voorspelbaar mechanisme kan *het subject zelf* de centrale rol spelen in de informatie-uitwisseling.** Controleurs kunnen het subject rechtstreeks en onafhankelijk raadplegen. Iedereen krijgt hetzelfde mechanisme, in de vorm van standaarden en software, waarmee verklaringenoverdracht en authenticatie gemeengoed worden. **Dit netwerk van mechanismen vormt een gedecentraliseerde digitale identiteitsinfrastructuur.**

Om het mechanisme te ontwerpen – of een reeds ontworpen mechanisme in praktijk te brengen – moeten gegarandeerd kunnen worden dat het (alleen) de gewenste uitkomsten realiseert. De enorme potentie van en grote vraag naar Self-Sovereign Identity komt namelijk met een groot risico: **RECENTRALISATIE**. Als de controle over de informatie-uitwisseling, in plaats van gedistribueerd over subjecten, toch in de handen valt van een kleine groep organisaties – bijvoorbeeld van big tech, big finance of big telco – wordt een averechts effect bereikt. Een ongekende concentratie van macht en surveillance is dan het gevolg. **Wellicht is de grootste uitdaging van Self-Sovereign**

Terug naar inhoudsopgave

Identity het blijvend garanderen van decentralisatie - dat ieder subject de sleutelpositie blijft vormen in zaken die hem of haar betreffen. Die uitdaging is enerzijds technisch en organisatorisch – zorgen dat decentralisatie *kan* – maar vooral ook juridisch en beleidsmatig – zorgen dat decentralisatie *gebeurt*. Ook tijdelijk, bijvoorbeeld in de opstartfase, kan het riskant zijn om centrale componenten toe te staan. **In elk detail van het technisch, juridisch en beleidsmatig ontwerp moet de onafhankelijkheid van het subject worden geborgd.**

FIGUUR 6:
ALTERNATIEVEN VOOR AUTHENTICATIE OF VERKLARINGENOVERDRACHT.



Terug naar inhoudsopgave

5 Hoe dan? Een gedeeld bouwplan

Het vorige hoofdstuk bepleit dat het subject centraal moet staan. Het moet zelfstandig aan authenticatie en verklaringenoverdracht kunnen doen om zekerheid te hebben dat zijn waarden zijn geborgd. Tegelijkertijd is het onredelijk om van ieder mens en organisatie te verwachten dat zij zich continu actief met deze zaken gaan bemoeien, of dat zij voldoende kennis en kunde hebben om dit gevoelige en belangrijke proces helemaal zelfstandig goed te regelen en/of te doorlopen. Hoe maken we het tóch mogelijk dat (nagenoeg) ieder mens of organisatie de verbindende en controlerende factor kan zijn?

Het antwoord hierop is om ieder mens en iedere organisatie te voorzien van een nieuw stuk gereedschap: een digitale assistent, in Self-Sovereign Identity ook wel een *agent of wallet*[7] genoemd. Die digitale assistent komt waarschijnlijk in de vorm van een smartphone app en helpt mensen en organisaties om hun identifiers, sleutels en gegevens verantwoord te beheren. De assistent zorgt ervoor dat het subject het inzicht behoudt, evenals de regie op gegevens. Controleurs kunnen het subject via zijn of haar digitale assistent vragen om allerlei gegevens. Door dit altijd in een vertrouwde en consistente interface te presenteren, raakt het subject vertrouwd met dit soort transacties. Van het subject zal enkel worden gevraagd om dit verzoek toe te staan of te weigeren. Wanneer 'toestemming' de juridische grond voor dit dataverzoek is, kan het subject geïnformeerd en onbeïnvloed toestemming verlenen voor de gegevensverwerking en op elk gewenst moment die toestemming weer intrekken. Op de achtergrond zorgt de assistent voor de nodige veiligheidscontroles om het subject tegen onrecht en fouten te beschermen. Ook kan het andere taken, zoals het doorspelen van gegevenswijzigingen (bijvoorbeeld adreswijzigingen) automatiseren. In die zin is de digitale assistent een vertrouwensdienst, maar dan transparant en voorspelbaar en onder de volledige controle van het subject[8].

Niet alleen het subject heeft zo'n assistent, maar de uitgevers en controleurs ook. Hun *agents* faciliteren efficiënte en veilige datadeling waarin de herkomst en integriteit zijn geborgd. Ook standaardiseren ze de communicatie met de *agent* van het subject. Als deze agents voldoende generiek zijn, kunnen ze in heel veel sectoren significante waarde toevoegen. Het volgende voorbeeld illustreert de enorme potentie van zo'n assistent.

[7] Het begrip 'wallet' wordt veelal gebruikt om de gelijkenis met de fysieke portemonnee – met daarin onder andere identiteitsbewijzen – te suggereren. Omdat deze analogie onvoldoende recht doet aan de (reken)kracht en functionaliteit van de software, gebruiken we hier het begrip 'agent' of 'digitale assistent'.

[8] Om deze transparantie en voorspelbaarheid te garanderen is het nodig om de broncode van de digitale assistent te openbaren; én toezicht op de (door)ontwikkeling van deze broncode in te richten. Dit maakt digitale assistenten openlijk verifieerbaar. Dit is een grote stap voorwaarts maar we moeten er rekening mee houden dat slechts weinigen zelf in staat zijn de integriteit van de broncode te verifiëren. De rest zal alsnog op de software(leverancier) moeten vertrouwen of op derden die de broncode hebben gecontroleerd.

Terug naar inhoudsopgave

Kader 3. Voorbeeld Gegevensoverdracht bij het huren van een huis

Pim wil een huis huren. De woningcorporatie heeft één vraag: gaat Pim de huur betalen? Omdat dat niet te voorspellen is, baseren ze zich op twee aspecten: heeft Pim voldoende inkomen of vermogen? En heeft Pim in het verleden altijd netjes zijn schulden betaald?

Het is niet ongebruikelijk dat verhuurders tientallen documenten van verschillende instanties opvragen, om antwoord te geven op deze simpele ja/nee-vragen. Het gevolg is dat verhuurders onnodig veel persoonlijke informatie krijgen. Ook is het proces voor beiden een flinke last: Pim moet handmatig alle documenten bij alle bronnen ophalen en de verhuurder moet deze verifiëren en beoordelen. En dan is er ook nog de vraag wat er gebeurt met die documenten nadat is vastgesteld of Pim de huur inderdaad met voldoende zekerheid kan opbrengen of niet.

Als de gegevensbronnen, de verhuurder en Pim allemaal een *agent* hebben gaat dit proces van meerdere dagen – of zelfs weken – naar enkele seconden. De *agent* van de verhuurder stuurt een gedetailleerd gegevensverzoek naar de agent van Pim, waarin staat welke verklaringen van welke instanties nodig zijn, en waarom. Pim's agent kan direct (op afstand) die instanties raadplegen en de gevraagde verklaringen op zijn smartphone verzamelen. Met Pim's toestemming en bevestiging worden de verklaringen aan de verhuurder gepresenteerd. Pim heeft – met gezichtsherkenning, een wachtwoord of een ander middel – bewezen dat hij achter de knoppen zit en hoort bij die verklaringen. Binnen enkele seconden, met minimale inspanning van alle partijen én behoud van privacy en zelfbeschikking, is het registratieproces voltooid en kan Pim huren of niet.

Dit voorbeeld toont aan dat de potentie van breed beschikbare *agents* enorm is. Het is aannemelijk dat alle betrokken partijen erop vooruitgaan, en de kosten aanzienlijk worden verlaagd. De maatschappelijke en economische voordelen rechtvaardigen een flinke inspanning in de ontwikkeling, regulering en inzet van deze *agents*.

Het voorbeeld van Pim is nu al te realiseren met reeds beschikbare technologie. De ontwikkelingen en experimenten zijn in volle gang, maar er zijn nog vele vragen te beantwoorden. Vooral op de domeinen beleid, wetgeving en ethiek is veel inspanning vereist om zeker te stellen dat deze fundamentele technologie – kritieke infrastructuur in wording – alleen *gewenste* uitkomsten realiseert. Dit hoofdstuk bespreekt enkele fundamentele ontwerpkeuzes om het inzicht te bieden dat voor verantwoorde ontwikkeling noodzakelijk is.

5.1 Voorwaarde: exclusief bezit van apparaten

De agent is het 'besturingsinstrument': de software die alles uitvoert en bijhoudt voor het subject en hem als het ware 'vertegenwoordigt'. De *agent* kan het subject vertegenwoordigen in een breed scala aan scenario's. De agent verzamelt, bewaart en deelt allerlei persoonlijke informatie en heeft ook zicht op de metadata: met wie en wanneer het subject transacties doet. Het heeft daarmee een bijzonder intieme kijk op het subject. Tevens beheert de agent de sleutels van het subject, waarmee het subject zich authenticeert, en mogelijk ook allerlei

Terug naar inhoudsopgave

documenten en wilsuitingen ondertekent. De *agent* is daarmee niet alleen het digitale gezicht, maar ook de digitale stem van het subject. Omdat de *agent* ongekend veel macht en zicht over de gegevens en sleutels van het subject heeft, is het essentieel dat die *agent* te allen tijde onder exclusieve controle van het subject blijft. Dat kan alleen wanneer ook het apparaat waarop die *agent* is geïnstalleerd – en waarop de identifiers, sleutels en gegevens zijn opgeslagen – onder exclusieve controle[9] van het subject is.

Deze voorwaarde roept een aantal aandachtspunten op, waarvan er hier drie worden uitgelicht: inclusie, verlies en diefstal, recentralisatie.

5.1.1 Inclusie

Niet iedereen heeft een smartphone, of een ander eigen apparaat. Niet iedereen is oud genoeg, jong genoeg, of anderzijds in staat om er één te bedienen. Niet iedereen kan (of wil) een smartphone betalen of gebruiken. Soms is de smartphone van de werkgever, en het bezit dus niet exclusief. Deze voorwaarde – exclusief bezit van een persoonlijk apparaat – riskeert dat deze mensen worden uitgesloten.

Enerzijds hebben alle technologische ontwikkelingen simpelweg met deze uitdaging om te gaan. Het zou een gemiste kans zijn om de rest van de samenleving de enorme potentie te ontzeggen. Ook zou het onterecht zijn om met dit bezwaar de vertrouwensdienst opnieuw centraal te zetten; als dat het probleem al oplost, zijn de risico's enorm. De vraag zal moeten zijn hoe mensen zonder smartphone alsnog de vruchten kunnen plukken.

Eén antwoord is (gedeeltelijke) vertegenwoordiging. De *agent* van een ouder of voogd kan bewijzen dat die ouder of voogd bevoegd is om een kind in bepaalde zaken te vertegenwoordigen. Dit is niet beperkt tot ouder-kind relaties: wat de technologie betreft kan ieder mens, organisatie (of ding) vertegenwoordigd worden door ieder ander mens of organisatie.

Toch is een regulier alternatief – bijvoorbeeld bestaande uit fysieke (of telefonische) loketten, begeleiding en ondersteuning, en de menselijk maat – nodig om ervoor te zorgen dat iedereen mee kan doen.

5.1.2 Verlies en diefstal

Uiteraard is een smartphone, of ander apparaat, gevoelig voor diefstal, schade of verlies. Om hiertegen te beschermen moeten de identifiers en gegevens goed worden geback-upt. Ook moeten sleutels buiten de telefoon om gedeactiveerd kunnen worden om te voorkomen dat iemand anders met die sleutels identiteitsfraude kan plegen. Een *noodplan* voor scenario's zoals diefstal, schade en verlies valt buiten de scope van dit visiedocument. Het is echter een essentieel vraagstuk, één dat voornamelijk maar niet uitsluitend technisch benaderd moet worden. De uitdaging is om maatregelen te nemen die simpelweg werken zonder dat het subject er wat aan doet, zonder terug te vallen op centrale oplossingen.

[9] Met dien verstande dat de beveiliging van een smartphone ook nooit waterdicht is.

Terug naar inhoudsopgave

5.1.3 Recentralisatie

Niets aan het (technisch) ontwerp van agents weerhoudt mensen om hun agent onder te brengen in de cloud. Bij een vertrouwensdienst dus. Velen zullen het als een voordeel ervaren, onbewust van – of ongeïnteresseerd in – het gevaarlijke gehalte van macht en toezicht die ze daarmee overhandigen. Voor grote techbedrijven kan dit lucratief zijn; ze kunnen goedkoop of zelfs gratis een erg aantrekkelijke *cloud agent* aanbieden, en geld verdienen aan het inzicht in gedrag en relaties, misschien zelfs de persoonlijke gegevens, die ze daarmee vergaren. Zo wordt juist het averechts effect bereikt: alle gegevens en transacties waar een *agent* mee gemoeid is zijn dan ondergebracht bij één en dezelfde partij. Ook als de dienst door een non-profit of overheidsorganisatie wordt aangeboden blijven de risico's bestaan. Commerciële overname of privatisering zou uitgesloten moeten zijn. Maar zo'n centrale dienst, in welke vorm dan ook, blijft een aantrekkelijk doelwit voor (staats)hackers: is het niet voor de diefstal van sleutels en (meta)gegevens, dan is het wel om deze kritieke infrastructuur plat te leggen.

Niet alleen de subjecten zijn kwetsbaar. Wanneer gegevensbronnen en dienstverleners hun koppeling met SSI uitbesteden dreigt dezelfde centralisatie. Zo ontstaat de schijn van een decentraal netwerk, waar in feite een kleine groep verwerkers weer de macht hebben. Deze technologie heeft grote potentie om de controle terug te geven aan het subject, maar ook om hem die te ontnemen.

Recentralisatie is een reëel gevaar. Dit vereiste een actieve zoektocht naar oplossingen. Want een nieuw - en in vele opzichten beter systeem, mag niet als gevolg hebben dat we van de regen in de drup raken.

5.2 Authenticatie met Agents

Het subject moet kunnen bewijzen te horen bij de identifiers en attributen die daadwerkelijk bij hem of haar horen. Dat moet te allen tijde kunnen en niemand anders dan het subject moet dat kunnen. Bij het ontwerpen van een digitale identiteitsinfrastructuur is het noodzakelijk om te kijken welke factoren deze uitgangspunten kunnen bedreigen. Zoals in hoofdstuk 4 is beargumenteerd, vormen tussenpersonen een dergelijk risico vanwege de afhankelijkheidsrelatie, invloed en surveillance die daarmee kunnen ontstaan. De eerste vraag is dus hoe de dienstverlener het subject kan authenticeren met behulp van hun agents en zonder tussenkomst of afhankelijkheid van een derde partij. Omdat dit niet in alle gevallen mogelijk blijkt, volgt een tweede vraag: hoe een digitale identiteitsinfrastructuur moet omgaan met situaties waarin het niet mogelijk is zonder derde partij te authenticeren. Een diepgaande analyse van deze twee ontwerpvragen valt buiten de scope van dit document. Deze sectie geeft echter inzicht in enkele belangrijke afwegingen.

5.2.1 Volledig controle over identifiers

Wanneer het subject volledige controle wil hebben over identifiers en verklaringen zal hij of zij deze identifiers zelf moeten kunnen aanmaken. Bij e-mailproviders is het vaak mogelijk om zelf een e-mailadres te kiezen, zolang deze niet al bezet is. Het identifierbeheer is dan bij de e-mailprovider belegd - die provider neemt daarmee de rol van identity provider aan. Het subject, de persoon achter het e-mailadres, is echter altijd afhankelijk van de

Terug naar inhoudsopgave

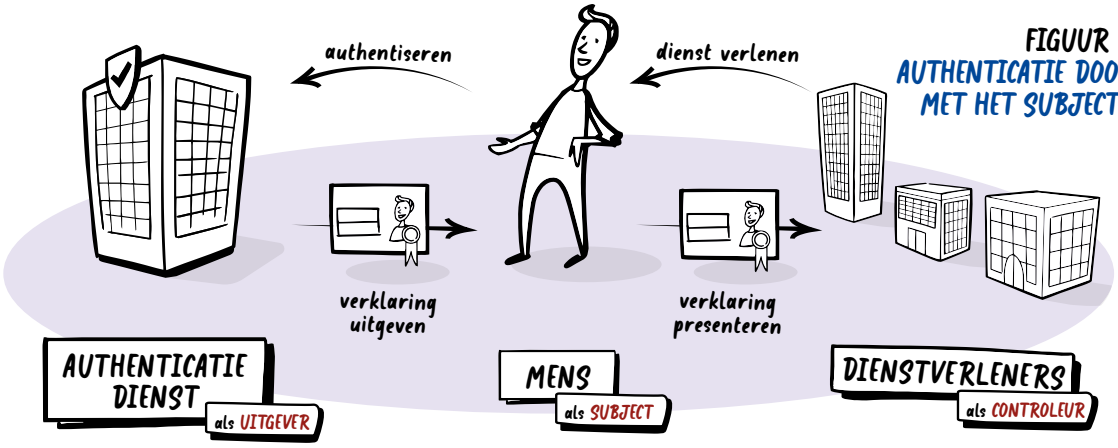
e-mailprovider om te bewijzen 'wie' hij of zij is. Eén alternatief is om de identity provider te vervangen door een gedistribueerd register (blockchain). Het proces verloopt globaal als volgt:

1. Het subject claimt een nog vrije identifier en registreert dit in het gedistribueerde register.
2. Eveneens genereert het subject eigen cryptografische sleutels en koppelt, in het register, de verificatiesleutel (publieke sleutel) aan de gekozen identifier.
3. Wanneer de controleur het subject wil controleren presenteert het subject zich met de in stap 1 gekozen identifier.
4. De controleur raadpleegt het register en vindt daar de verificatiesleutel waarmee hij het subject kan authenticeren.
5. Zolang het subject beschikt over de geheime sleutel, die wiskundig met de verificatiesleutel is verbonden, kan hij bewijzen eigenaar te zijn van de identifier.

Uiteraard worden deze taken verzorgd door de agents van controleur en subject. Mens noch organisatie hoeft in principe weet te hebben van de onderliggende technologie. Het grote voordeel van deze oplossing is dat het register niet zomaar te manipuleren is, en dat controleur en subject rechtstreeks kunnen authenticeren zonder tussenkomst van een derde. Dit alternatief – zelf geclaimde identifiers vastgelegd in een gedistribueerd register – is met de huidige technologie te faciliteren. De toepasselijkheid van die technologie hangt echter af van de eisen die de controleur stelt aan de identificatie. Voor gevallen waarin een zelf geclaimde identifier niet geschikt of onvoldoende is, kan het identiteiten- en/of sleutelbeheer (daarnaast) bij een externe partij worden belegd.

5.2.2 Authenticatie met derden

Wanneer een derde partij wordt betrokken in de authenticatie wordt het subject (en de controleur) van die partij afhankelijk. Echter door het subject centraal te zetten is het mogelijk dat subject de controle van en controle over het authenticatieproces te geven, en te voorkomen dat de authenticatiedienst zicht heeft op individuele transacties of relaties tussen het subject en de controleur. Figuur 7 illustreert hoe authenticatie door een derde kan werken: door gebruik te maken van verklaringenoverdracht.



FIGUUR 7:
AUTHENTICATIE DOOR EEN DERDE MET HET SUBJECT CENTRAAL

De authenticatiedienst kan op de gebruikelijke manier (met een wachtwoord, een SMS, of ander middel) het subject authenticeren en vervolgens een verklaring afgeven aan het subject dat hij op dát tijdstip zich heeft geauthenticeerd. Het subject kan die verklaring doorspelen aan de controleur die, indien dit tijdig gebeurt, erop kan vertrouwen dat het juiste subject achter de *agent* schuilgaat.

Terug naar inhoudsopgave

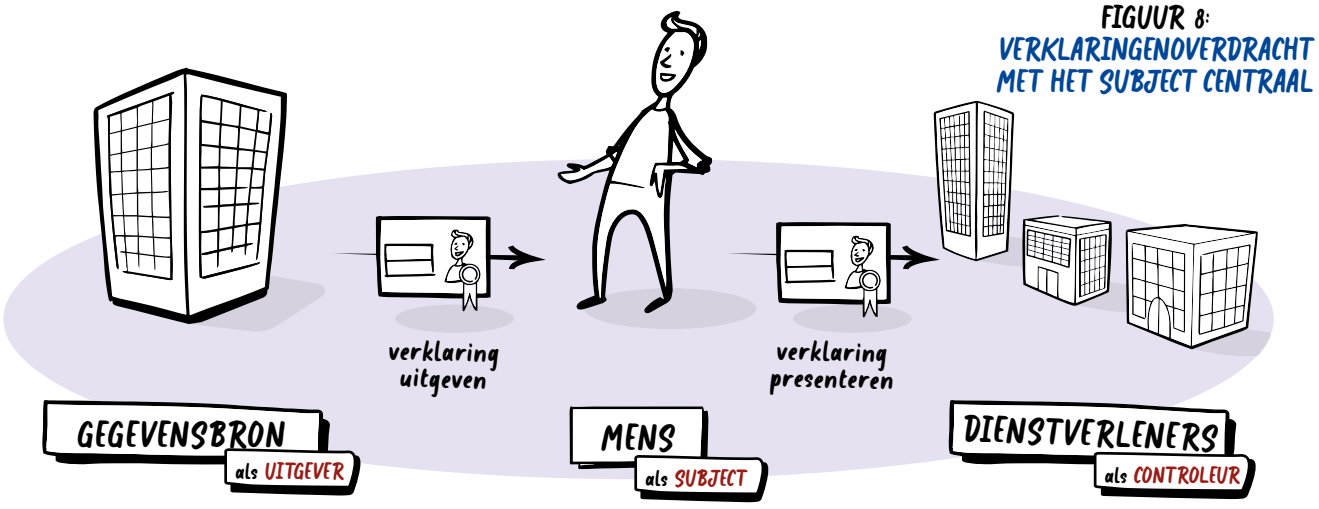
5.2.3 (Door)ontwikkeling van mechanische identificatie en authenticatie

De voorgaande twee secties illustreren twee mogelijkheden waarmee het subject zich bij controleurs kan authenticeren. Een combinatie van deze methoden kan ook toegevoegde waarde bieden. De voorkeur ligt echter bij de mechanische oplossing omdat deze onafhankelijk en transparant is. Om de ontwikkeling van dit mechanisme te stimuleren is het allereerst nodig in kaart te brengen welke eisen controleurs aan identificatie en authenticatie kunnen stellen en met welke mechanische middelen aan die eisen kan worden voldaan.

5.3 Verklaringenoverdracht met Agents

Om geschikt te zijn voor een scala aan toepassingen moet het netwerk van agents voldoende generiek worden ontworpen in plaats van voor een specifieke (set van) use case(s). Om deze reden is de probleemanalyse uit hoofdstuk 2 zo algemeen ingestoken.

Als het subject wettelijk of moreel gezien zeggenschap heeft over die datadeling dan is het wenselijk om het subject daarover werkelijke **regie** te geven en, zoals betoogd in hoofdstuk 3, centraal te zetten in het proces van verklaringenoverdracht (zie Figuur 8). Dat betekent dat de uitgever de verklaringen aan het subject geeft, en dat het subject die naar eigen inzicht met elke gewenste controleur kan delen. Ditzelfde patroon is te herkennen in het voorbeeld van Pim: hij verzamelt de verklaringen van de verschillende instanties en presenteert die aan de woningcorporatie.



FIGUUR 8:
VERKLARINGENOVERDRACHT MET HET SUBJECT CENTRAAL

Hieronder worden een drietal belangrijke aandachtspunten besproken

1. Is dataminimalisatie te garanderen?
2. Is het een goed idee om het subject regie op gegevens te laten voeren?
3. En hoe kunnen we verklaringen intrekken als ze niet meer actueel zijn?

Terug naar inhoudsopgave

5.3.1 Dataminimalisatie

Per toepassing zal moeten worden afgewogen of het nut van de informatieoverdracht opweegt tegen de privacy-impact. Ten behoeve van de privacy moet alleen de minimaal vereiste data worden gedeeld voor de minimaal benodigde tijdsduur. Een interessante ontwerpvraag is of het structureel – mechanisch – te garanderen is dat altijd enkel de minimale informatie wordt gedeeld.

De opvatting heerst dat ja/nee vragen per definitie een minimale impact op de privacy hebben. Het spel Twenty Questions (In Nederland: Wie is het?) illustreert goed waarom dit geen veilige aanname is: de uitdaging is om met maximaal twintig ja/nee vragen te bepalen wie iemand is. Ook zijn ja/nee vragen voor veel toepassingen te beperkend: bijvoorbeeld bij het doorgeven van een adres.

De (ontwikkelaar van de) agent kan niet van tevoren oordelen over de inhoud, over de afweging tussen privacy en nut, omdat dit contextueel en subjectief is. Die afweging wordt per geval door de betrokken partijen, uitgevers, subjecten en controleurs, gemaakt. Er zijn echter wel mechanismen te ontwerpen om die partijen bij die afweging te ondersteunen, zoals besproken in de volgende secties.

5.3.2 Regie op Gegevens: een goed idee?

Het subject voert, binnen zekere grenzen, de regie op gegevens; wanneer een partij om gegevens vraagt is het aan het subject om toegang te verlenen of te weigeren. De agent kan op consistente wijze aan het subject duidelijk maken *wie* vraagt om *welke* gegevens, en *waarom*. Het subject kan toestemming verlenen en die later op elk gewenst moment, vanuit de agent, intrekken. Toch blijft het risico dat het subject een onverstandige keuze maakt en te veel of te gevoelige gegevens deelt met de verkeerde partij. Dit kan uitgevers, die een zorgplicht hebben jegens het subject, weerhouden om hem of haar regie te geven over (gevoelige) gegevens. Om de kans op onverstandige datadeling te verminderen en tóch regie op gegevens te realiseren kunnen twee middelen worden ingezet: **regieondersteuning** en **regiebeperking**:

1. **Regieondersteuning:** de *agent* adviseert het subject over de datadeling, bijvoorbeeld door te melden dat de controleur al dan niet in een lijst met vertrouwde partijen staat, of al dan niet aan de gestelde eisen voldoet. Dergelijk advies kan in verschillende gradaties van ernst voorkomen: informerend, waarschuwend of alarmerend. Het blijft echter een advies waardoor het subject, met enige moeite, er alsnog voor kan kiezen om door te gaan.
2. **Regiebeperking:** de *agent* weigert het verzoek, ongeacht de wens van het subject, wanneer de controleur niet kan aantonen dat het aan de gestelde voorwaarden voldoet.

Uitgevers kunnen per (type) verklaring specificeren aan welke eisen controleurs moeten voldoen om die verklaring in te zien en of die eisen adviserend of beperkend zijn; bijvoorbeeld: het BSN mag alleen aan overheidsorganisaties worden getoond. Uitgevers moeten daarbij uiteraard rekening houden met de belangen van het subject en de toepasselijke wetgeving. Wanneer agents deze ondersteuning dan wel beperking zelfstandig kunnen toepassen, wordt recht gedaan aan de zorgplicht van uitgevers, en daarmee de barrière voor adoptie verlaagd.

Terug naar inhoudsopgave

5.3.3 Actualiteit

De meeste gegevens zijn veranderlijk. Verklaringen gebaseerd op veranderlijke gegevens zijn altijd momentopnamen. Verandert een gegeven, dan zijn eerder uitgegeven verklaringen mogelijk nog wel relevant, maar niet meer actueel. Bijvoorbeeld, een verklaring over het eigendom van een bedrijf is niet meer actueel nadat dat eigendom wordt verkocht, maar mogelijk nog wel relevant voor bijvoorbeeld de belastingdienst. Controleurs moeten in veel gevallen wel de actualiteit van het gegeven kunnen controleren, maar kan daarvoor niet contact opnemen met de uitgever. Daarmee zou de uitgever immers kennis krijgen van de transactie tussen subject en controleur, wat schadelijk is voor de privacy. Echter, wanneer verklaringen eenmaal zijn uitgegeven heeft een uitgever daar geen controle meer over. Het kan het subject niet dwingen de verklaring te verwijderen of aan te passen. Hoe kan de controleur dan toch met zekerheid de actualiteit van de verklaring vaststellen?

Een eerste optie is om verklaringen telkens te vernieuwen. Wanneer het subject een (te) oude verklaring toont, zou de controleur het subject kunnen verzoeken dat gegeven opnieuw bij de uitgever op te halen. Als het gegeven inmiddels is veranderd dan krijgt het subject geen nieuwe verklaring mee. Het probleem met deze optie is dat de verklaringen binnen enkele seconden hun waarde verliezen en het subject wederom afhankelijk is van een uitgever die meewerkt, beschikbaar is en blijft bestaan.

Een alternatief is om de intrekking van verklaringen publiekelijk te vereeuwigen in een **revocatieregister**. Op dit openbare register publiceert de uitgever een verwijzing naar elke uitgegeven verklaring die het heeft ingetrokken, zonder daarbij de identiteit van het subject bekend te maken. Blockchaintechnologie wordt momenteel gezien als de oplossing voor dit probleem. De ontwikkeling en operatie van dit revocatieregister is een aparte zorg naast de ontwikkeling van agents.

Terug naar inhoudsopgave

6 En nu?

Dit visiedocument beoogt een gezamenlijk vertrekpunt te zijn voor eenieder die zich beleidsmatig én operationeel met decentrale digitale identiteit bezighoudt in Nederland. Dit document is daarmee een leidraad en geen handleiding. Het schrijft niet voor hoe een oplossing er uit moet zien maar het helpt wel bij het nadenken over de keuzes die in het ontwerp van een identiteitssysteem aan de orde komen. Het visiedocument is ook een levend document. Dat wil zeggen dat het aangevuld en aangepast zal worden naar aanleiding van praktische invulling van SSI en andere decentrale digitale identiteitssystemen. Met gedeelde waarden, een gedeeld mechanisme en een gedeeld bouwplan kunnen we aan de slag.

Praktische invulling is dan ook een belangrijke volgende stap. Enerzijds in het ontwerp van infrastructuur zoals het Dutch Trust Network (DTN) anderzijds in het ontwerp van hoger gelegen delen van de technologie-stack zoals agents/wallets. Daadwerkelijke invulling gebaseerd op casussen zoals het opzetten van een BV, het uitwisselen van gegevens over verkregen diploma's en certificeringen of een andere invulling van KYC/AML zal nuttige inzichten opleveren aan de hand waarvan dit document verder in- en aangevuld kan worden.
Ook zijn er meer fundamentele vragen die het waard zijn om te onderzoeken. De samenwerking met kennispartners van DBC is daarbij onontbeerlijk.

In Europees verband willen we het gedeelde vertrekpunt gebruiken om bijvoorbeeld eSSIF en EBSI te helpen maar ook het recent door de Europese Commissie aangekondigde framework voor Europese Identiteit. Want één ding staat vast: we zijn het eens over het vertrekpunt, maar de praktijk zal met verschillende middelen ingevuld worden.

Inhoudelijke reacties op dit document zijn zeer welkom en kunnen in schriftelijke vorm verstuurd worden naar dssif@dutchblockchaincoalition.org. Meepraten kan ook door partner[10] te worden van de Dutch Blockchain Coalition en deel te nemen aan werkgroepen en of andere bijeenkomsten.

[10] Partnerschap van DBC staat open voor iedere Nederlandse organisatie uit overheid, bedrijfsleven of kennisinstellingen. Voor meer informatie zie https://dutchblockchaincoalition.org/over-dbc

Terug naar inhoudsopgave

7 Begrippenlijst

- **Administratief Beeld** – Een set gegevens / attributen die een partij heeft over een bepaald subject, gekenmerkt door één of meer identifiers.
- **Administratieve Beeldvorming** – De handelingen / processen waarmee administratieve beelden tot stand komen.
- **Afnemer | Controleur (Verifier)** – (Rol) Een partij die bepaalde gegevens vraagt of gebruikt.
- **Afsprakenstelsel** – Een verzameling van afspraken die een netwerk van partijen in staat stelt om bepaalde diensten te verlenen.
- **Agent** – Een softwareapplicatie die een partij (in de rol van uitgever, subject en/of controleur) vertegenwoordigt in identiteitstransacties. Synoniemen: wallet, digitale assistent.
- **Attribuut** – Een bepaald gegeven van een subject.
- **Authenticatie | Authenticeren** – Een proces waarin wordt vastgesteld of een bepaalde partij bij een (geclaimde) identifier hoort.
- **Bron** – Synoniem voor Issuer.
- **Cloud Agent** – Een agent die in de cloud wordt gehost, in tegenstelling tot een agent die lokaal op een eigen smartphone draait.
- **Communicatieprivacy** – Het vertrouwelijk kunnen communiceren zonder dat derden weten wat er wordt gecommuniceerd of dát wordt gecommuniceerd.
- **Controleur** – Synoniem voor Afnemer.
- **Dataminimalisatie** – Het tot een minimum beperken van de hoeveelheid informatie die wordt gedeeld en/of verwerkt.
- **Data-subject** – (Rol) De partij over wie bepaalde gegevens gaan neemt. Synoniem: Subject.
- **Decentralisatie** – Het verspreiden van macht en kennis over verschillende actoren opdat het niet door één actor kan worden misbruikt of er bezwaarlijke afhankelijkheidsrelaties ontstaan.
- **Digitale assistent** – Synoniem voor Agent.
- **Digitale Identiteitsinfrastructuur** – De verzameling afspraken en voorzieningen die gezamenlijk en generiek authenticatie en verklaringenoverdracht mogelijk maken.
- **Fragmentatie** – De toestand waarin informatie zoveel mogelijk is verspreid; om te voorkomen dat één actor een bezwaarlijke hoeveelheid informatie verkrijgt.
- **Frictie** – Weerstand in brede zin (moeite, tijd en geld) die partijen ervan weerhoudt om aan authenticatie of verklaringenoverdracht te doen.
- **Gedistribueerd Register (Blockchain)** – Een database / register dat gedistribueerd is over meerdere actoren waarbij de integriteit van het register door de technologie is geborgd.
- **Gegevensbron** - Synoniem voor Issuer.
- **Gegevenskluis** – Een dienst(verlener) die gegevens van één of meer uitgevers bewaart en, onder regie van het subject, die gegevens aan controleurs toont.
- **Gegevenssluis** – Een dienst(verlener) die gegevens van één of meer uitgevers, onder regie van het subject, doorsluist aan controleurs. In tegenstelling tot een gegevenskluis bewaart de gegevenskluis dus geen gegevens.
- **Gegevensverwerker** – (Rol) Een partij die gegevens verwerkt. Synoniem: Verwerker.
- **Identificeren / Identificatie** – Het bekend maken van een identifier van een mens of organisatie.
- **Identifier** – Een gegeven of combinatie van gegevens die uniek naar een subject verwijst.
- **Identifierbeheer** – Het aanmaken, onderhouden en vernietigen van identifiers.
- **Identiteitsfraude** – Het (onrechtmatig) voordoen als een andere persoon of organisatie.
- **Identiteitsketen** – Een keten van organisaties die identiteitsgegevens uitwisselt.
- **Identiteitssysteem** – Een informatiesysteem waarin identiteitsgegevens worden beheerd.
- **Identity Provider** – Een dienstverlener die identifiers beheert en subjecten authenticeert.
- **Issuer** – (Rol) Een partij die bepaalde gegevens / verklaringen uitgeeft. Synoniemen: Bron, Gegevensbron, Uitgever.

Terug naar inhoudsopgave

- **Metadata** – Gegevens die de karakteristieken van bepaalde gegevens of processen beschrijven.
- **Revocatieregister** – Een register waarin wordt gepubliceerd welke uitgegeven verklaringen zijn ingetrokken, en dus niet meer geldig zijn.
- **Self-Sovereign Identity (SSI)** – Beoogd ontwerp voor identiteitssystemen waarbij de kennis van en macht over gegevens enkel bij het data-subject ligt. Dit kan worden gerealiseerd door ieder subject te voorzien van een agent/wallet.
- **Sleutelbeheer** - Het toekennen en intrekken van sleutels waarmee personen (of organisaties) kunnen bewijzen bij hun identifiers te horen.
- **Soevereiniteit** – In de context van SSI: de mogelijkheid van het data-subject om actief zelf de regie te voeren over de eigen gegevens. Soevereiniteit omvat niet het aanpassen van verklaringen van derden, maar wel grip op wie die verklaringen inziet en wanneer.
- **Subject** – Synoniem voor Data-subject.
- **Uitgever** – Synoniem voor Issuer.
- **Verifier** – Synoniem voor Afnemer.
- **Vertrouwensanker** – Een partij die men van nature vertrouwt.
- **Verwerker** – Synoniem voor Gegevensverwerker.
- **Wallet** – Synoniem voor Agent.

Terug naar inhoudsopgave

Kernpartners

Partners

Dutch Blockchain Coalition

connect and create

info@dutchblockchaincoalition.org

www.dutchblockchaincoalition.org