SSI Speelveldanalyse

Een verkenning van het Nederlandse SSI speelveld, toekomstige ontwikkelrichtingen, impact op publieke waarden en de rol van de Nederlandse overheid

1 oktober 2021
Versie 1.0

In opdracht van:

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Uitgevoerd door:

INNOPAY | TNO

Inhoudsopgave

1 Managementsamenvatting

Wereldwijd, en ook in Nederland, wordt gewerkt aan manieren om geverifieerde gegevens digitaal uit te wisselen op manieren die de privacy en autonomie ten aanzien van (ter beschikking stellen van) deze gegevens voor burgers en bedrijven verbeteren en transparantie en inclusiviteit verhogen. Het is mogelijk om administratieve processen en dienstverlening efficiënter, goedkoper en ook kwalitatief beter te maken. Eén van deze manieren van digitale gegevensuitwisseling, die we Self-Sovereign Identity (SSI) noemen, kenmerkt zich doordat gebruikers zelf gegevens bij de bron ophalen en deze vervolgens onder eigen controle en regie veilig kunnen opslaan. Bovendien kan de gebruiker deze gegevens delen met anderen wanneer ze dat nodig vinden. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) ziet deze ontwikkelingen en herkent de relevantie ervan voor de eigen uitdagingen op het gebied van digitale identiteit en digitale gegevensuitwisseling. Met betrekking tot deze ontwikkelingen wil BZK een standpunt bepalen betreffende wat te doen, en op welke manier. Daarmee beantwoordt ze tevens de steeds luider wordende oproep vanuit Europa en de private sector aan de Nederlandse overheid om een duidelijk standpunt in te nemen ten aanzien van verdergaande digitale gegevensuitwisseling. Om dit te kunnen doen heeft BZK gevraagd om aanbevelingen voor vervolgstappen, gebaseerd op een speelveldanalyse.

In dit verkennende onderzoek analyseren INNOPAY en TNO de huidige initiatieven rondom digitale gegevensuitwisseling aan de hand van drie analyses: **(A)** Het Nederlandse SSI speelveld, **(B)** (inter-)nationale ontwikkelingen en **(C)** toekomstige ontwikkelrichtingen en impact op publieke waarden. Elke deelanalyse levert conclusies op over SSI en digitale gegevensuitwisseling, gevolgd door aanbevelingen aan de opdrachtgever.

Deel A - Het Nederlandse SSI speelveld

De analyse van het Nederlandse SSI speelveld geeft vier conclusies:

- Er lopen veel SSI experimenten in Nederland, maar het landschap is gefragmenteerd.
- Kritieke massa is (nog) niet gerealiseerd door individuele leveranciers van SSI oplossingen.
- SSI gedachtegoed is (nog) niet volwassen genoeg voor grootschalig gebruik in de maatschappij.
- Beperkte beschikbaarheid brondata en beperkte herbruikbaarheid in andere domeinen vormt barrière voor waardecreatie.

De experimenten laten de potentie van SSI al goed zien, maar er is weinig samenwerking tussen de verschillende initiatieven wat leidt tot een gefragmenteerd speelveld in zowel de private als de publieke sector. Er bestaan verschillende ideeën over wat de beste invulling van SSI is, ook omdat bepaalde concepten die hiervoor nodig zijn nog onvoldoende zijn uitgewerkt. Organisaties focussen zich nog vooral op de ontwikkeling van het eigen product en in mindere mate op samenwerking en interoperabiliteit met andere initiatieven. Ook zijn partijen nog terughoudend met het ontsluiten (en gebruiken) van gegevens via SSI, wat ook verklaart waarom er nog geen kritieke massa is ontstaan.

Deel B - (Inter-)nationale ontwikkelingen
De analyse van (inter-)nationale ontwikkelingen geeft twee conclusies:

- Het is onduidelijk hoe de verschillende juridische kaders (in ontwikkeling) zich tot elkaar (gaan) verhouden
- Grote commerciële partijen kunnen sneller bewegen dan wetgevende ontwikkelingen waardoor zij de markt kunnen domineren en verstoren

De partijen in het speelveld geven aan dat het ontbreken van duidelijkheid rondom de (aankomende) juridische kaders een rem is op verdere opschaling van SSI. Dit komt omdat de kaders over verschillende aspecten van digitale gegevensuitwisseling gaan. Daarnaast kunnen partijen die veel gebruikers hebben (grote tech-bedrijven) het speelveld grootschalig betreden. Wanneer de juridische kaders doorgevoerd zijn is er mogelijk al concurrentie ontstaan waar potentieel nieuwe wetgevende trajecten voor nodig zijn om de macht in te dammen.

Deel C - Toekomstige ontwikkelrichtingen en impact op publieke waarden
De analyse van toekomstige ontwikkelrichtingen en de impact op publieke waarden geeft twee conclusies:

- 'Digital agent' en 'Data bij de bron' zijn twee verschillende interactievormen die beide gefaciliteerd moeten worden
- Een geconsolideerde markt voor digitale gegevensuitwisseling heeft positieve effecten op de publieke waarden voor burgers, bedrijven en overheid

Een consolidatie op de markt van digitale gegevensuitwisseling kan gedicteerd worden door grote tech-bedrijven, maar ook worden gerealiseerd door actief samen te werken aan een publiek-privaat gedragen oplossing. Afhankelijk van de mate waarin de overheid de maatschappelijke waardes wil realiseren, zal ze dit aan de markt overlaten, of zelf actief aan de ontwikkeling en consolidatie bijdragen, en wellicht een coördinerende rol nemen.

Aanbevelingen aan de opdrachtgever
Om de bijdragen van het digitaal kunnen uitwisselen van geverifieerde gegevens op verschillende publieke waarden te helpen realiseren, kan de overheid het volgende doen:

1. **Stel geïntegreerde visie op voor het Nederlandse landschap van digitale identiteit en gegevensuitwisseling en koppel dat aan een ambitieuze uitvoeringsagenda**
   Ontwikkel een breed gedragen visie op de gewenste rol van SSI in het bredere landschap van digitale identiteit en digitale gegevensuitwisseling, rekening houdend met Europese ontwikkelingen rondom de EU Digital Identity Wallet. Zorg daarnaast voor een ambitieuze uitvoeringsagenda zodat gebruikers, private en publieke partijen op de kortst mogelijke termijn daadwerkelijk de maatschappelijke waarde van digitale gegevensuitwisseling kunnen realiseren.
2. **Stuur op consolidatie van het speelveld rond digitale gegevensuitwisseling via een Publiek Private Samenwerking**
   Breng de kennis en expertise van de 90+ partijen die al experimenteren met SSI bij elkaar en werk toe naar een geharmoniseerd en interoperabel speelveld voor digitale gegevensuitwisseling dat klaar is voor verdere opschaling. Deze *best practices* zullen via deze publiek private samenwerking ook hun weg moeten vinden

naar de gremia die in Europa werken aan de verdere detaillering van de EU Digital Identity wallet.

3. **Doorbreek als overheid het kip-ei probleem voor digitale gegevensuitwisseling door als 'first mover' zelf pro-actief brondata aan te bieden en te consumeren**
   Start met het beschikbaar stellen van brondata via 'digital agents' en/of 'data bij de bron' interactiemodellen, en gebruik brondata voor validatie binnen en en optimalisatie van eigen bedrijfsprocessen. Dit om de realisatie van de maatschappelijke waarde van digitale gegevensuitwisseling voor de Nederlandse economie op gang te brengen.

2 Inleiding

Dit document beschrijft de resultaten van een onderzoek in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) naar het Nederlandse Self-Sovereign Identity (SSI) speelveld, uitgevoerd door INNOPAY en TNO. Het onderzoek beschrijft de huidige situatie van het Nederlandse SSI speelveld, identificeert mogelijke ontwikkelrichtingen voor de toekomst en verkent de impact hiervan op publieke waarden. Deze inzichten leiden tot aanbevelingen aan BZK voor vervolgstappen in het bepalen van beleid rondom digitale gegevensuitwisseling en SSI.

2.1 Aanleiding

Sinds enkele jaren is een nieuwe manier van denken over digitale identiteit sterk in opkomst. Self-Sovereign Identity (SSI) is gebaseerd op het principe dat individuen (en organisaties) controle zouden moeten hebben over hun digitale identiteit en daaraan gerelateerde gegevens, mits zij daartoe gerechtigd zijn[1][2]. Deze controle en de mogelijkheid om gegevens ter beschikking te kunnen stellen, biedt potentieel verschillende voordelen: optimalisatie van (administratieve) processen waarbij burgers niet langer 'ingewikkelde' elektronische formulieren[3] hoeven in te vullen, het verlagen van validatiekosten (> 1 miljard euro/jaar voor de Nederlandse economie, meerdere miljarden/jaar voor EU[4]), het verhogen van data-kwaliteit, dataminimalisatie en controle over privacy, vergroten van autonomie en transparantie in het digitale domein en het stroomlijnen van dienstverlening[5].

Hoewel de genoemde potentiële voordelen van SSI niet uitsluitend door middel van SSI te realiseren zijn, kan SSI wel een belangrijke katalysator zijn om deze voordelen te realiseren. Deze aantrekkelijke beloftes rondom SSI zorgen de afgelopen jaren voor veel aandacht en activiteit rondom het onderwerp SSI en digitale gegevensuitwisseling. Binnen overheid, bedrijfsleven en kennisinstellingen is inmiddels een verscheidenheid aan SSI-initiatieven, producten en standaarden in ontwikkeling.

Recent heeft het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK), als beleidsverantwoordelijke voor de Nederlandse (digitale) identiteitsinfrastructuur, een visie gepubliceerd over de rol van en houding met betrekking tot digitale identiteit in Nederland[6]. Hierin schetst staatssecretaris Knops dat de overheid een actieve rol voor zichzelf ziet in het creëren van vertrouwen in de digitale wereld voor burgers en bedrijven en het beschikken over een betrouwbare (bron-)identiteit is hierbij cruciaal. In deze visiebrief Digitale Identiteit staat niet omschreven hoe de overheid aankijkt tegen de ontwikkelingen op het gebied van Self-Sovereign Identity en hoe zich dat verhoudt tot de visiebrief op Digitale Identiteit. Wel merkt de overheid dat hier vanuit de markt steeds meer behoefte aan is.

BZK heeft INNOPAY en TNO daarom gevraagd inzicht te bieden in de huidige staat van het Nederlandse SSI speelveld, wat de relatie is met digitale identiteit, en hoe dit speelveld zich

[1] INATBA (2020)
[2] Sovrin Foundation (2021)
[3] Nationale Ombudsman (2019)
[4] Pascal Wissink, "SSI savings on a European scale", private analysis TNO
[5] SSIF (2021)
[6] Visiebrief digitale identiteit (2021)

lijkt te gaan doorontwikkelen. Op basis van deze inzichten doen wij aanbevelingen aan BZK waarmee zij haar eigen standpunt en beleid rondom SSI kan bepalen en verder concretiseren.

2.2 Doelstelling

Het doel van dit onderzoek is om het Nederlandse SSI-speelveld in kaart te brengen om zo eventuele lacunes te identificeren die wel ingevuld moeten zijn om maatschappelijke baten en waarden van SSI te waarborgen en te versterken. Dit moet leiden tot aanbevelingen over welke rol(len), taken en acties de overheid in het SSI-speelveld op zich zou kunnen nemen. Dit onderzoek geeft antwoord op de volgende vragen:

1. Hoe ziet het SSI-ecosysteem van Nederland er momenteel uit en hoe kan het worden gekarakteriseerd?
2. Welke spelers/partijen zijn actief in dit ecosysteem en welke producten/diensten leveren ze?
3. Welke (inter-)nationale ontwikkelingen/initiatieven en partijen hebben invloed op het Nederlandse SSI-ecosysteem, hoe wordt deze invloed uitgeoefend en wat betekent dit concreet?
4. Wat zijn de mogelijk ontwikkelingsrichtingen van het SSI-ecosysteem en welke toekomstscenario's zijn hierbij te bedenken?
5. Welke impact hebben mogelijke toekomstige ontwikkelrichtingen van het SSI-ecosysteem op de publieke waarden?
6. Welke rol(len), taken en acties zou de overheid nu en in de toekomst op zich kunnen nemen in het SSI-ecosysteem om maatschappelijke baten te realiseren en publieke waarden te waarborgen en te versterken?

2.3 Aanpak

In dit onderzoek hebben wij allereerst een analyse gemaakt van het Nederlandse SSI speelveld op basis van deskresearch, input van marktpartijen via een online enquête en enkele interviews met stakeholders en experts in het SSI speelveld. Op basis van deze input hebben we twee ontwikkelrichtingen rondom het thema digitale gegevensuitwisseling opgesteld, wat resulteerde in vier toekomstscenario’s. Deze toekomstbeelden hielpen ons om in dialoog met de opdrachtgever gevoel te krijgen voor welke impact deze toekomstige ontwikkelrichtingen kunnen hebben op verschillende publieke waarden. Op basis van de inzichten uit de verschillende onderdelen in dit onderzoek hebben wij enkele aanbevelingen voor vervolgactiviteiten geformuleerd.

Uitgangspunt voor de gekozen diepgang per onderwerp is altijd geweest dat BZK graag een breed en verkennend onderzoek wilde. Het is dan ook nadrukkelijk niet de opdracht geweest om een uitputtende lijst met detailinzichten te geven, maar om in de breedte relevante topics te identificeren die als input dienen voor nader te bepalen vervolgactiviteiten.

De onderzoeksaanpak en tussentijdse uitkomsten van dit onderzoek zijn steeds besproken en gevalideerd met opdrachtgever BZK en een externe begeleidingscommissie met vertegenwoordigers van BZK en de Dutch Blockchain Coalition.

2.4 Leeswijzer

Dit rapport bestaat uit drie onderzoekende delen (A, B en C) en aanbevelingen aan de opdrachtgever.

- **Hoofdstuk 3** geeft de context van dit onderzoek en gaat in op de relatie tussen digitale gegevensuitwisseling en SSI.
- **Hoofdstuk 4 (deel A)** geeft inzicht in het Nederlandse SSI speelveld. Het schetst een overzicht van de verschillende partijen die actief zijn in het SSI speelveld en beschrijft enkele observaties over hun rol. In dit hoofdstuk worden onderzoeksvraag 1 en 2 beantwoord.
- **Hoofdstuk 5 (deel B)** beschrijft (inter-)nationale ontwikkelingen op het gebied van wet- en regelgeving, SSI-trends en andere Europese en wereldwijde ontwikkelingen rondom data delen en digitale identiteit. In dit hoofdstuk wordt onderzoeksvraag 3 beantwoord.
- **Hoofdstuk 6 (deel C)** introduceert mogelijke toekomstige ontwikkelrichtingen voor het Nederlandse SSI speelveld en geeft een overzicht van relevante publieke waarden die in dit hoofdstuk afgewogen worden tegen de genoemde mogelijke toekomstige ontwikkelrichtingen. In dit hoofdstuk worden onderzoeksvraag 4 en 5 beantwoord.
- **Hoofdstuk 7** vat de conclusies van de onderzoekende hoofdstukken 4, 5 en 6 samen.
- **Hoofdstuk 8** omschrijft de aanbevelingen voor de opdrachtgever. Dit beantwoordt de 6^{e} en laatste onderzoeksvraag.

3 Context - SSI en digitale gegevensuitwisseling

Het is moeilijk om een goede definitie van Self-Sovereign Identity (SSI) te geven – daarover bestaat sinds het ontstaan van de term nog altijd geen consensus. Wij zullen ons in dit rapport dan ook niet wagen aan het formuleren van dé (zoveelste) definitie van SSI.

Als startpunt van de verdere speelveldanalyse, bouwen wij voort op datgene over SSI wat in de markt niet ter discussie lijkt te staan, namelijk dat:

- SSI te maken heeft met een digitale uitwisseling van gegevens over individuen, organisaties, 'things', enzovoorts, waarbij deze gegevens voorzien zijn van bewijzen over zaken als: herkomst, integriteit en dergelijke.
- De uitwisseling van deze gegevens loopt van partijen die ze in de vorm van credentials uitgeven (*Issuers*), via een digital agent (bijvoorbeeld een *wallet*) van betrokkenen (*Holders*) (individuen maar ook wel organisaties) en onder hun expliciete controle terecht komen bij partijen die deze gegevens nodig hebben (*Verifiers*).
- Dit alles gebeurt zonder dat een *Issuer* weet heeft van waar (aan welke *Verifier*) de *Holder* zijn credentials toont.

Het hebben van een Self-Sovereign Identity is geen doel op zich, het is bedoeld om iets mogelijk te maken. Het is van belang om je te realiseren dat de voordelen die worden toegedicht aan SSI (zie ook 2.1) gerealiseerd worden binnen de context van digitale gegevensuitwisseling, of ook wel: (elektronische) business transacties. Voor het mogelijk maken van deze (elektronische) business transacties, is een belangrijke uitdaging dat *Verifiers* met de data waarover zij kunnen beschikken (door SSI of bijvoorbeeld het in dit hoofdstuk geïntroduceerde alternatief van rechtstreeks data bij de bron halen) hun dienstverlening daadwerkelijk optimaliseren.

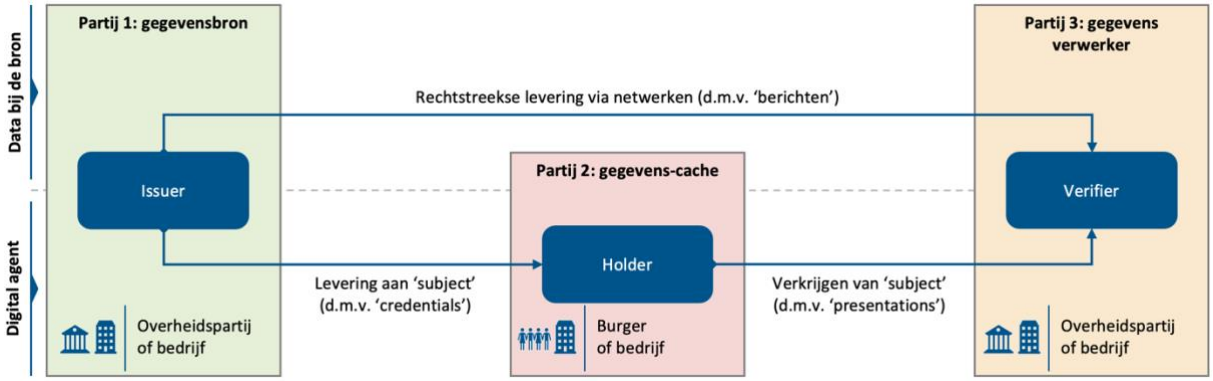
Besluitvorming over deze digitale gegevensuitwisseling vergt niet alleen gegevens over de digitale (bron-)identiteit van de gebruiker, maar ook andere gegevens die mogelijk niet strikt gaan over je identiteit (bijvoorbeeld je inkomen, vaccinatiebewijs of de WOZ-waarde van je huis). Welke gegevens dat precies zijn en wanneer deze voldoende 'gekwalificeerd' (valide) zijn om voor dat doel te worden gebruikt, bepaalt uiteindelijk de partij die deze gegevens uitvraagt, de *Verifier*[7]. Een *Verifier* zal willen kunnen besluiten of ze deze gegevens kunnen en willen gebruiken, gegeven de risico's van hun business transactie. In het aanvraagproces van een hypotheek zal een hypotheekverstrekker bijvoorbeeld met enige mate van zekerheid digitaal willen kunnen vaststellen dat zaken als inkomensgegevens, een werkgeversverklaring, waardering van het huis inderdaad zijn uitgegeven door een specifieke bronhouder. En een werkgever zal bij het digitaal uitwisselen van credentials als een universitair diploma willen kunnen vaststellen door welke universiteit die diploma is uitgegeven en dat er niet met die diploma geknoeid is.

Zoals we in Figuur 1 laten zien kan zo'n digitale gegevensuitwisseling via het voor SSI kenmerkende 'digital agent' interactiemodel plaatsvinden. Binnen de SSI community is een

[7] Feitelijk is dit een ongelukkige term omdat het niet om verifiëren gaat (= vaststellen dat de gegevens authentiek, tijdig en structureel in orde zijn). Om niet teveel af te wijken van veelvuldig voorkomend taalgebruik gaan wij hier in dit rapport in mee.

wallet een veel voorkomende digital agent, maar ook digitale kluizen of andere personal data management oplossingen kunnen gebruikt worden. Zeker voor (cloud) agents die niet direct op bijvoorbeeld de smartphone of een ander lokaal device opereren, is het wel van belang dat er voldoende waarborgen zijn voor hoe met transacties, kennis of metadata over deze transacties en gegevensuitwisseling omgegaan wordt (bijvoorbeeld welke informatie, attributen of keys worden er in de cloud opgeslagen). Deze waarborgen, die wellicht niet allemaal technisch afgedwongen kunnen worden, kunnen bijvoorbeeld door certificering hard gemaakt worden.

Naast data ophalen via een digital agent kan een *Verifier* gegevens ook rechtstreeks bij de bron ophalen, waarbij afhankelijk van de gevoeligheid van de data mogelijk wel consent van het individu nodig is (en dus: een voldoende betrouwbare digitale identiteit van de gebruiker). Deze twee methoden zijn niet de enige manier van gegevensuitwisseling (denk aan het posten van een brief), maar wel de twee meest relevante methoden om digitaal gegevens uit te wisselen samen met hun 'kwalificaties'. Deze kwalificaties, zoals 'assurances' en 'proofs', worden altijd meegestuurd.



Figuur 1 Twee manieren van digitale gegevensuitwisseling: 'digital agent' en 'data bij de bron'

Gegeven de scope van de opdracht van dit onderzoek zoomen wij nu in hoofdstuk 4 eerst verder in op partijen die zich in het SSI speelveld bezig houden met 'digital agent' oplossingen. Dit onderzoek betreft immers een SSI Speelveldanalyse. Vanaf hoofdstuk 6, wanneer we de blik naar de toekomst richten zal ook het 'data bij de bron' model weer terugkomen. Dit doen we niet om tot een waardeoordeel te komen over in hoeverre het voor SSI kenmerkende 'digital agent' interactiemodel beter of slechter is dan het 'data bij de bron' model. Dit doen we om in te kunnen schatten hoe de toekomstscenario's (incl. bijbehorende interactiemodellen) uitpakken voor verschillende publieke waarden.

4 Deel A - Het Nederlandse SSI speelveld

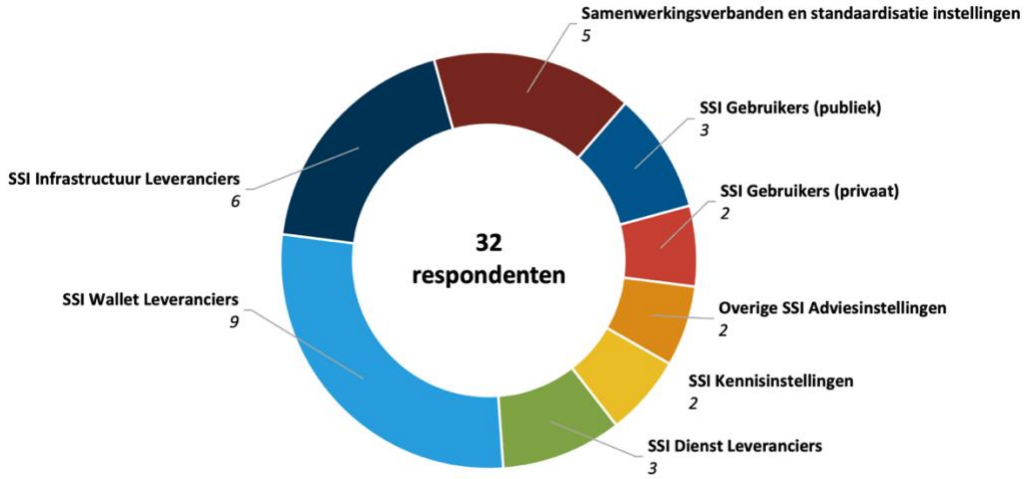
Dit onderzoek beoogt om breed inzicht te bieden in de huidige staat van het Nederlandse SSI speelveld. In dit hoofdstuk laten wij daarom zien welke partijen er in het Nederlandse SSI speelveld actief zijn, welke producten/ diensten zij leveren en hoe deze partijen zich tot elkaar verhouden.

4.1 Aanpak

Op basis van deskresearch, aangevuld met input van de opdrachtgever en begeleidingscommissie hebben wij een longlist van partijen samengesteld die een rol spelen in het 'Nederlandse' SSI speelveld. Hierbij hebben we gekeken naar bedrijven, organisaties en initiatieven op het gebied van SSI die:

1. Zélf actief zijn op de Nederlandse markt óf
2. Een duidelijke invloed hebben op partijen die op de Nederlandse markt actief zijn.

Om meer inzicht in de karakteristieken van het Nederlandse SSI speelveld te creëren zijn uit deze longlist, 50+ partijen geselecteerd die via een online enquête bevraagd zijn over o.a. hun rol in het speelveld en hun verwachtingen over hoe dat speelveld zich in de toekomst zal ontwikkelen. De partijen zijn geselecteerd op basis van hun activiteiten in het Nederlandse speelveld en mate van volwassenheid en/of activiteit. Daarnaast zijn er ook een aantal internationale spelers gevraagd om de enquête in te vullen omdat deze spelers al lange tijd in het wereldwijde speelveld betrokken zijn en gezien worden als voorlopers op het gebied van SSI. Van de 50+ uitgenodigde partijen hebben 32 partijen de enquête ingevuld (zie Figuur 2 voor de verdeling per categorie).



Figuur 2 Verdeling reacties enquête per categorie

Appendix 9.1 heeft een totaaloverzicht van alle partijen die actief zijn op het Nederlandse SSI speelveld. Appendix 9.2 geeft een overzicht van de partijen die uitgenodigd zijn om de enquête in te vullen.

4.2 Overzicht totale Nederlandse SSI speelveld

Onderstaand overzicht laat zien dat ruim 90 organisaties direct of indirect actief zijn in het Nederlandse SSI speelveld[8].

Figuur 3 Het Nederlandse SSI speelveld

We hanteren in het overzicht van het Nederlandse SSI speelveld de volgende categorisering:

Categorie	Omschrijving	Voorbeelden
SSI Gebruikers	SSI Gebruikers zijn partijen die credentials uitgeven (*Issuer*), opvragen, ontvangen of verwerken (*Verifier*), en hiervoor 'SSI technologie' gebruiken. Ook burgers en bedrijven die optreden als *Holder* in transacties zijn SSI Gebruikers, maar deze dragen behalve volume niet direct iets bij aan het speelveld en zijn daarom niet meegenomen	SSI Gebruikers kunnen zowel private als publieke partijen zijn. Denk aan: banken en verzekeraars die hun klanten laten inloggen met behulp van SSI-credentials, of gemeentes en uitvoerings-organisaties die credentials uitgeven zoals VOGs, uittreksels van burgerlijke stand etc.
SSI Leveranciers	SSI Leveranciers zijn partijen die 'SSI technologie' maken en/of aanbieden, of partijen die gerelateerde diensten leveren (denk aan: technologie die SSI Gebruikers kunnen gebruiken voor het uitgeven, opvragen, ontvangen of verwerken van credentials.	Dit kunnen zowel infrastructuur leveranciers zijn (zoals Ledger Leopard), wallet leveranciers (zoals Datakeeper, IRMA, OCTKO, Schluss) of dienstleveranciers die zich richten op het breder faciliteren van SSI Gebruikers (zoals Signicat en TNO's eassi gateway).

[8] Appendix 9.1 bevat een grotere versie van deze overzichtsplaat

SSI Kennisleveranciers	SSI Kennisleveranciers zijn partijen die actief kennis ontwikkelen op het gebied van SSI met als doel deze kennis (open) beschikbaar te maken, of andere partijen te adviseren op het gebied van SSI, bijvoorbeeld op gebied van Governance, Risk en Compliance.	Denk aan kennisinstellingen zijn zoals TU Delft, Radboud, TNO en overige (advies)instellingen zoals Deloitte, Pels Rijcken, Innovalor en Innopay.
Samenwerkingsverbanden en standaardisatie instellingen	Samenwerkingsverbanden zijn partijen die met elkaar samenwerken om bepaalde (SSI) doelen te realiseren, zoals SSI adoptie of interoperabiliteit. Ook standaardisatieinstellingen verbinden partijen en zorgen ervoor dat zij komen tot afspraken die worden vastgelegd in normen, richtlijnen en standaarden.	Voorbeelden hiervan zijn eSSIF-Lab (samenwerkingsverband) en W3C (standaardisatieinstelling).

Tabel 1 Categorisering partijen in Nederlandse SSI speelveld

Een organisatie kan uiteraard in verschillende categorieën vallen, maar wij hebben er uit praktische overwegingen voor gekozen om organisaties in te delen in de categorie waarin ze het meest actief zijn. Wij realiseren ons dat er ook andere categoriseringen van het SSI speelveld mogelijk zijn, ieder met haar eigen voor- en nadelen.

De hier gekozen categorisering biedt het door BZK gewenste inzicht in de breedte van het Nederlandse SSI speelveld. Het helpt enerzijds onderscheid te maken tussen gebruikers van SSI die als *Issuer* of *Verifier* van credentials optreden, als ook leveranciers die als faciliterende partij optreden. Daarnaast geeft deze categorisering inzicht in welke partijen en organisaties zich op een wat hoger abstractieniveau bezighouden met SSI zoals kennisinstellingen en partijen die consulting diensten bieden, bijvoorbeeld op het gebied van governance, risk en compliance. Verder is het goed om op te merken dat eindgebruikers (burgers/ consumenten) in dit overzicht ontbreken, dit viel buiten scope van dit onderzoek.

Dit overzicht schetst uiteraard een momentopname van het Nederlandse SSI speelveld (peildatum: juli 2021). Het SSI speelveld is nog volop in beweging. Het is goed denkbaar dat zich over enige tijd nieuwe partijen in het Nederlandse SSI speelveld gaan begeven of zich juist terugtrekken uit dit speelveld. Ook is het goed denkbaar dat sommige van de getoonde partijen in andere of juist in minder categorieën actief zullen zijn. Denk bijvoorbeeld aan partijen die tijdelijk een wallet bieden voor test- of demodoeleinden, of partijen die vanuit een kennis- of adviesrol instappen als leverancier van een SSI dienst voor gebruikers.

4.3 Analyse van het huidige Nederlandse SSI speelveld

Kijkend naar het Nederlandse SSI speelveld en de input die partijen over dit speelveld via de enquête gegeven hebben, vallen vooral de volgende zaken op:

1. Partijen hebben wisselende denkbeelden over wat SSI is of zou moeten zijn
2. Veel focus op controle consument/ burger als SSI Gebruiker met nog weinig aandacht voor (informatie-) behoeftes Issuers & Verifiers
3. Grote diversiteit in technische inrichting en standaarden
4. Beperkte adoptie van SSI wallets
5. SSI Leveranciers hebben nog geen positieve business case
6. Gefragmenteerde SSI initiatieven binnen de Nederlandse overheid

In de volgende paragrafen zullen wij deze observaties verder duiden.

4.3.1 Wisselende denkbeelden over wat SSI is of zou moeten zijn

Uit de analyse van de enquêtes komt naar voren dat er verschillende denkbeelden over SSI bestaan. Dit betreft niet alleen de interpretatie van de term SSI, maar ook over nut en noodzaak van SSI voor de Nederlandse samenleving.

Figuur 4 Verschillende definities van Self-Sovereign Identity volgens respondenten enquête

Zoals te zien is in Figuur 4 refereren veel partijen in de enquête aan de 10 principes uit de SSI visie van Christopher Allen[9], de 12 principes van Sovrin[10] (of een selectie uit deze principes) en bepaalde technische inrichtingen waar partijen minimaal aan moeten voldoen.

Uit de enquêteresultaten maken wij op dat SSI voor sommigen echt een principekwestie is, terwijl anderen vooral de nadruk leggen op de doelstellingen die je met SSI kunt bereiken (denk aan: privacy, grip op gegevens door gebruikers, etc.) waarbij het minder van belang is of je dat door middel van 'zuiver' SSI of een andere invulling van digitale identiteit bereikt. Het is een implementatiekeuze of je het mitigeren van afhankelijkheden en risico's van digitale gegevensuitwisseling zoveel mogelijk in techniek wilt regelen, of dat je dit borgt in beleid, processen en/ of afspraken.

Uit de enquête blijkt verder dat er verschillende opvattingen bestaan over hoe SSI principes in de praktijk in diensten en producten het beste vorm kunnen krijgen, en of alle principes in de Nederlandse maatschappij wel relevant zijn.

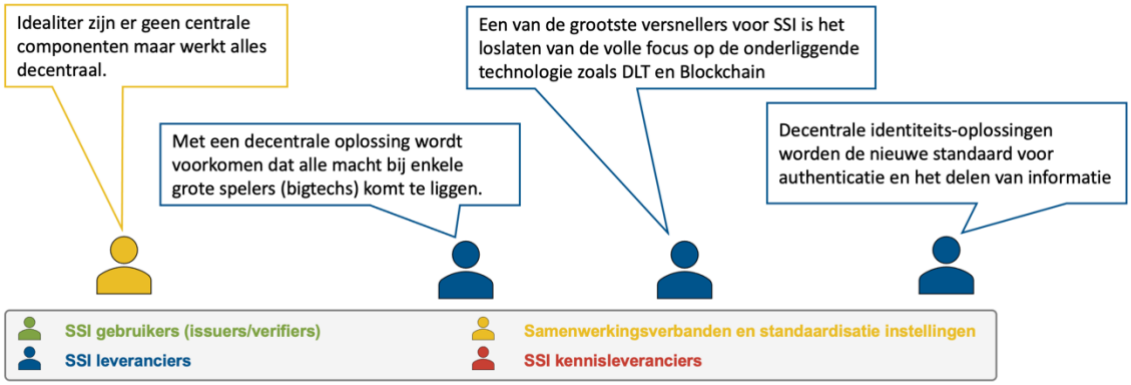
[9] The Path to Self-Sovereign Identity (2016)
[10] Sovrin Foundation (2021)

We zien dat het verschil in opvattingen zich vooral richt rondom enkele thema's:

(De)centralisatie

Partijen in het speelveld verschillen van mening of de data/metadata die voor de verificatie van credentials nodig is al dan niet op een blockchain of Distributed Ledger Technology (DLT) moet staan. Respondenten op de enquête onderbouwen hun standpunt om wel of geen blockchain/DLT te gebruiken niet echt met argumenten. Over het algemeen is er wél consensus om geen persoonsgegevens op te slaan op de blockchain/DLT.

Daarnaast zijn er ook discussies in het speelveld over identiteit attributen en of deze zoveel mogelijk uit verschillende bronnen moeten komen om een goed, compleet beeld van een identiteit te geven, of dat juist een verzameling van identiteit attributen vanuit één bron betrouwbaarder is.



Figuur 5 Standpunten respondenten SSI speelveld enquête over decentralisatie

Data opslag

Een belangrijk punt voor veel SSI initiatieven is waar de data van consumenten (e.g. credentials) wordt opgeslagen. Wij zien dat spelers met een meer idealistische kijk op SSI implementaties, vinden dat data lokaal opgeslagen moet staan voor de gebruiker, op een hardware device waar de eigenaar te allen tijde zelf beschikking over heeft (in tegenstelling tot bijvoorbeeld een cloud oplossing). Andere initiatieven vinden dat de opslag van data ook door een (centrale) organisatie gedaan kan worden, zolang de gebruiker maar altijd regie houdt over deze gegevens. Ook werd een aantal keer de opvatting "mits op de juiste manier geïmplementeerd" genoemd.

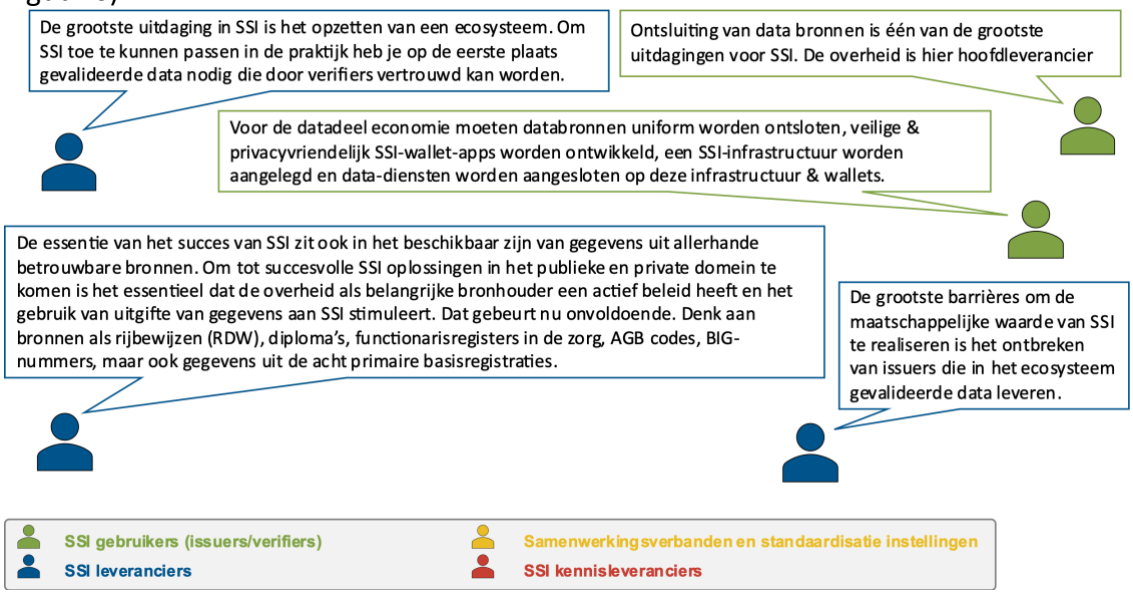
4.3.2 Veel focus op controle consument als SSI Gebruiker met nog weinig aandacht voor (informatie-) behoeftes van Issuers & Verifiers

In het Nederlandse SSI speelveld is, zo blijkt uit de enquêtes, bij het gros van de partijen veel aandacht voor de consument of burger als gebruiker. Verschillende producten zoals o.a. de wallet leveranciers van Schluss, OCKTO en IRMA focussen in hun proposities op de behoefte van de gebruiker om regie te kunnen voeren over welke gegevens hij/ zij deelt met partijen. Deze producten gaan uit van principes als privacy-by-design, data minimalisatie en strakke controle over digitale datauitwisseling via een digital agent van de consument. Deze partijen geven aan dat gebruikers deze regie over hun gegevens zelf willen, of op zijn minst zouden

moeten willen. Of dit inderdaad het geval is, komt uit de reacties op de vragenlijst verder niet naar voren.

Er is in het SSI speelveld nog weinig aandacht voor het perspectief van bedrijven en medewerkers die handelen namens hun bedrijf (vertegenwoordigen). Ook is er weinig aandacht voor oplossingen waarmee burgers kunnen handelen namens een andere burger (guardianship). Slechts twee partijen geven aan hiermee bezig te zijn.

Opvallend is dat er in het Nederlandse SSI speelveld nog weinig aandacht is voor de behoeftes van de andere actoren dan de eindgebruiker, terwijl Issuers en Verifiers uiteraard wel nodig zijn om digitale gegevensuitwisseling via een digital agent mogelijk te maken. Echter zijn er beperkte incentives voor Issuers om mee te doen. Een issuer kan een vergoeding vragen voor het uitgeven van credentials, maar burgers hebben over het algemeen een lage willingness to pay voor identity producten. Issuers kunnen de vergoeding niet vragen aan verifiers omdat er geen contact is tussen Issuers en Verifiers. Daardoor is het voor Issuers (die niet ook verifyen) minder interessant om credentials uit te geven als er onduidelijke vergoeding of waarde tegenover staat. Wij zien dus ook weinig partijen die als Issuer claims of credentials ter beschikking stellen in de markt, terwijl de beschikbaarheid van credentials juist essentieel is voor elke use case om transacties van de juiste data te kunnen voorzien. Dit werd ook een aantal keer als barrière voor SSI-adoptie genoemd (zie Figuur 6).



Figuur 6 Meningen over het beschikbaar stellen van gegevens

In meerdere gevallen noemen respondenten dat de overheid een cruciale rol speelt (of zou kunnen spelen) als Issuer van credentials uit betrouwbare bronnen. Verschillende marktpartijen wachten op deze bruikbare geverifieerde data vanuit de overheid om eigen oplossingen en diensten aan te kunnen bieden.

4.3.3 Grote diversiteit in technische inrichting en standaarden

Er gaan veel technische keuzes vooraf aan elke digitale gegevensuitwisseling in een transactie met behulp van een digital agent. Wij zien in het Nederlandse SSI speelveld sterke verschillen in deze technische inrichting.

Aan de hand van de informatie-, data- en netwerklaag geven we enkele voorbeelden van verschil in de technische inrichting. Daarnaast geven een aantal partijen aan de Trust over IP stack[11] te volgen, die ruimte biedt voor verschillende implementaties in de verschillende lagen.

Informatielaag
De diverse SSI Leveranciers binnen het Nederlandse speelveld gebruiken veelal eigen schema's voor de data die in credentials beschreven staan. SSI Gebruikers die van verschillende SSI Leveranciers gebruik willen maken, moeten deze verschillende schema's kunnen interpreteren om te weten wat deze data betekent. Het al dan niet definiëren van schema's voor digitale gegevens kan een keuze zijn van een groep partijen die nauw samenwerken en vergelijkbare credentials zouden uitgeven.
Met andere woorden, als een credential door verschillende Issuers geleverd kan worden en deze Issuers elk een eigen datamodel hanteren voor het beschrijven van de inhoud van credentials, dan moeten Verifiers verschillende 'dialecten' kunnen interpreteren om credentials van verschillende Issuers te kunnen gebruiken. Stel dat verschillende gemeentes WOZ waarde credentials uitgeven (waar de schrijfwijze bijvoorbeeld 'WOZ-waarde', 'wozwaarde' of 'Waardering Onroerende Zaken' kan zijn, of de waarde uitgedrukt is in EUR, Euro of €) dan moeten banken de verschillende dialecten kunnen interpreteren voordat ze deze credentials optimaal kunnen gebruiken.

Ook kan dit probleem andersom voorkomen. Als Verifiers of Holders credentials in een bepaald format verwachten, dan moeten Issuers deze credentials in verschillende vormen kunnen verstrekken of toestaan dat er vertaling plaats kan vinden.

Datalaag
Er bestaan verschillende invullingen voor hoe credentials vormgegeven worden en informatie die via het netwerk verstuurd wordt, wordt verpakt. Voorbeelden hiervan zijn bijvoorbeeld data formatting van berichten (JSON, JSON-LD) of standaarden voor de credential zelf (Verifiable Credentials en de verschillende vormen daarbinnen, of bijvoorbeeld Attribute Based Credentials). Binnen het Nederlandse speelveld worden zowel VCs gebruikt, als ook ABCs.

Netwerklaag
Partijen in het Nederlandse SSI speelveld gebruiken een grote diversiteit aan protocollen en onderliggende infrastructuur voor de daadwerkelijke uitwisseling van gegevens. Sommige leveranciers maken bijvoorbeeld gebruik van open standaard blockchain of distributed ledger technologie (bijv. Hyperledger Aries, Sovrin), terwijl andere oplossingen juist proprietary netwerkinrichting (bijv. IRMA) toepassen.
We merken op dat, hoewel diverse partijen aangeven zich te conformeren aan de ToIP stack, weinig tot geen onderscheid gemaakt wordt in twee technische layers

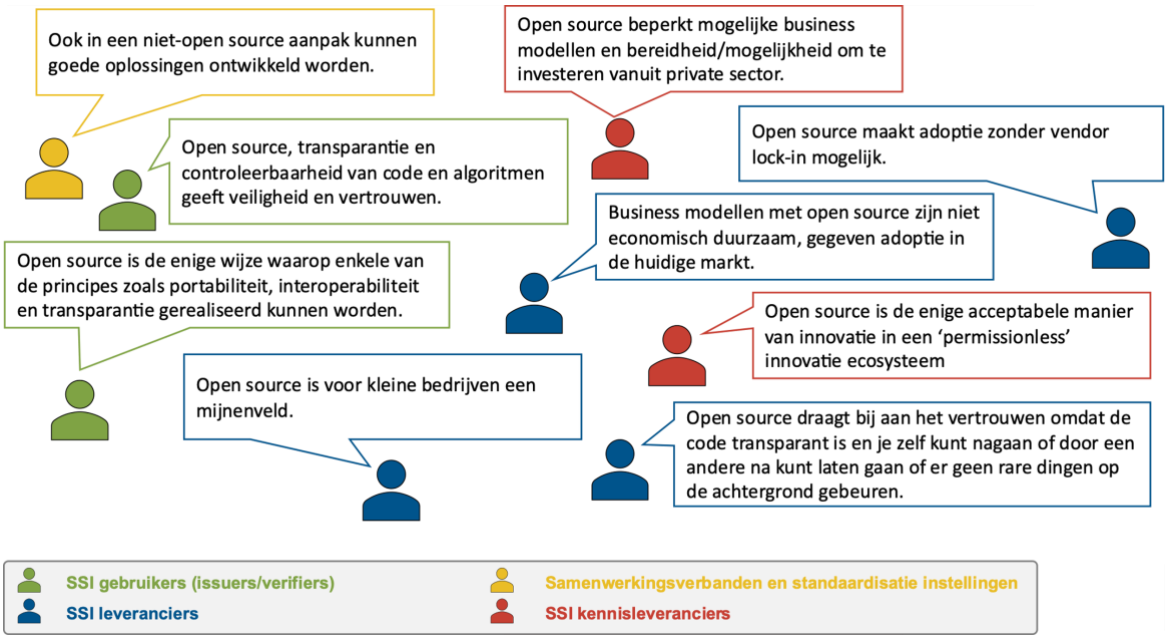
[11] The Trust over IP Stack December 2019, IEEE Communications Standards Magazine 3(4):46-51/ DOI: 10.1109/MCOMSTD.001.1900029

welke ToIP gebruikt om een netwerk te omschrijven, namelijk Layer 1 Public Utilities en Layer 2 DIDComm Peer to Peer Protocol.

Voor een architectuur/infrastructuur in opkomst zoals SSI is het op zich logisch dat er niet direct 'best practices' bestaan voor de verschillende architectuurlagen. Partijen geven aan momenteel verschillende technische invullingen te gebruiken in demonstrators en proofs of concepts, waarna moet blijken wat in welke context wel of niet werkt. Of hier verdere convergentie zal ontstaan zal ook sterk afhangen van verdere internationale ontwikkelingen bij o.a. Europese lidstaten, consortia en standaardisatie instellingen, geven verschillende respondenten aan. Zie voor meer detail ook de (inter-)nationale ontwikkelingen zoals beschreven in hoofdstuk 0.

Opvattingen over open source

Naast verschillende opvattingen over hoe bepaalde technische componenten worden ingericht, zijn er ook wisselende meningen over of, en hoe deze componenten beschikbaar gesteld worden. We zien een aantal partijen die vinden dat alles rondom SSI 'by design' open source moet zijn en open source ontwikkeld moet worden. Maar er zijn ook partijen die open source niet als must beschouwen, en zelfs als beperking zien voor businessmodellen en bereidheid om te investeren.



Figuur 7 Meningen over open source van respondenten enquête

4.3.4 Beperkte adoptie van SSI wallets

De adoptie van SSI oplossing is nog beperkt. SSI wallets zoals de Trinsic wallet, esatus wallet, Datakeeper (Rabobank), Connect.Me (van Evernym), Gataca en IRMA hebben tussen de 10 en 10.000 downloads. Hiernaast bestaan er ook digitale identiteit initiatieven die niet specifiek voor SSI ontworpen zijn. Hoewel deze initiatieven niet direct met elkaar te vergelijken zijn, maakt dit wel inzichtelijk dat de adoptie van SSI wallets nog beperkt is. Zo is de Belgische Itsme app meer dan 3,5 miljoen gedownload[12,13]. De DigiD app was in 2019 al 6

[12] Itsme 2021
[13] NB: Itsme heeft voornamelijk Belgische gebruikers maar is aan het uitbreiden in Nederland

miljoen keer gedownload[14]. Ook het verschil in adoptie is groot als we de SSI wallets vergelijken met Itsme en DigiD op Actieve gebruikers per maand (zie Figuur 8).

Het aantal maandelijks actieve gebruikers bij de meest gebruikte SSI wallets samen zit onder de 10.000[15]. De DigiD app heeft ongeveer 1,8 miljoen maandelijks actieve gebruikers[16]. Itsme had in augustus 2021 iets minder dan 1 miljoen maandelijks actieve gebruikers.

Figuur 8 Actieve gebruikers per maand van apps

We zien verschillende oorzaken voor deze beperkte adoptie van SSI wallets:

In experimenten nog weinig aandacht voor adoptie
Veel van de SSI initiatieven op de Nederlandse markt bevinden zich nog in experimentele fase en kennen als gevolg daarvan ook nog een beperkt aantal (actieve) gebruikers. In deze experimenten ligt de focus veelal op het verkennen van de functionele mogelijkheden en gewenste technische implementatie in de vorm van demonstrators en proofs of concept. Pas als uit deze experimenten duidelijk wordt óf en zo ja, hoe SSI een oplossing kan bieden voor een specifieke digitale gegevensuitwisselings use case, en partijen besluiten dit op grotere schaal te gaan gebruiken, zal de aandacht naar het aanjagen van adoptie verschuiven. Uit de vragenlijsten blijkt dat veel respondenten wel bezig zijn met vraagstukken rondom (grootschalige) adoptie, en dat ze dit zien als een relevante nieuwe onderzoeksvraag.

Kip-ei probleem Issuers, Holders, Verifiers
De adoptiedynamiek tussen Issuers, Holders en Verifiers kenmerkt zich door netwerkeffecten: het invullen van een van deze rollen wordt waardevoller naarmate er ook een bepaalde kritische massa van andere rollen aanwezig is in het speelveld. Maar bij gebrek aan kritieke massa in deze drie rollen, wie beweegt dan eerst? Dit is een traditioneel kip-ei probleem. Een aantal respondenten geeft aan dat het een uitdaging is om de adoptie van SSI aan de kant van Issuers, Holders en Verifiers op gang te krijgen.

[14] Logius 2020
[15] Apptopia 2021
[16] Apptopia 2021

Fragmentatie in technische implementatie en gebrek aan interoperabiliteit
In voorgaande paragraaf bespraken wij al de grote diversiteit in technische inrichting. Interoperabiliteit tussen deze verschillende technische implementaties ontbreekt nog, wat betekent dat partijen die verschillende technische inrichtingen hebben, niet digitale gegevens met elkaar kunnen uitwisselen.

Afhankelijkheden van providers in het IT landschap
In veel contexten maken potentiële Verifiers en Issuers gebruik van standaard softwarepakketten. Denk aan een leerlingvolgsysteem, huisarts informatiesysteem en een notarieel administratiesysteem. Deze potentiële doelgroepen (leraren, huisartsen en notarissen) kunnen vaak niet zelfstandig keuzes maken over het toepassen van bepaalde diensten en services in het door hen gebruikte softwarepakket. Zij zijn afhankelijk van wet- en regelgeving, en accreditaties welke al dan niet toegekend worden aan diensten en services. Dit zou ertoe kunnen leiden dat softwareleveranciers relatief weinig aanleiding hebben om kostbare vernieuwingen door te voeren aangezien overstappen voor hun klanten erg onaantrekkelijk is.

4.3.5 SSI Leveranciers hebben nog geen positieve business cases

De relatief lage adoptie en de kip-ei problematiek maakt het voorlopig moeilijk voor SSI Leveranciers (bijvoorbeeld Wallet leveranciers) om tot een positieve businesscase te komen. Dat wil zeggen dat leveranciers van SSI oplossingen voldoende omzet uit het gebruik van de dienst genereren en dit niet hoeven te compenseren uit subsidie, investering of omzet van andere diensten. Het gaat hier om partijen die gegevens issuen en/of verifiën, producten en diensten voor Holders faciliteren of de onderliggende technische infrastructuur leveren.

Waarde ontstaat over het algemeen niet in het direct delen van (identiteits)gegevens zelf, maar in wat daar vervolgens mee gedaan of gerealiseerd kan worden. Bij gebrek aan een community waarin data voldoende beschikbaar is (credentials die ge-issued kunnen worden en Holders die de data daadwerkelijk delen), zijn dienstverleners terughoudend om als Verifier in te stappen en gebruik te maken van SSI. Voorlopig maakt het merendeel van leveranciers in het SSI speelveld gebruik van subsidies of investering vanuit innovatiebudgetten, of verwerkt de kosten in een breder portfolio van diensten en services die worden aangeboden.

Het blijkt voor SSI Leveranciers lastig om de problematiek rondom kritieke massa in Issuers, Holders en Verifiers op te lossen. In de praktijk zien wij dat huidige implementaties zich momenteel voornamelijk rondom individuele use cases afspelen. Hoewel ze misschien ontworpen zijn voor generiek gebruik, is het momenteel zo dat SSI Gebruikers voor vrijwel elke gebruikssituatie een eigen applicatie of implementatie nodig hebben. Het nettoresultaat is een diversiteit aan oplossingen met elk een eigen kleine gebruikersgroep. Hoewel een beperkte groep betrokkenen misschien waarde uit een dergelijke gefragmenteerde situatie weet te realiseren, is het realiseren van brede maatschappelijke waarde uitdagend.

4.3.6 Gefragmenteerd landschap van SSI-initiatieven binnen de Nederlandse overheid

Niet alleen private partijen maar, ook diverse overheidsorganen zijn actief op het gebied van SSI. Een aantal voorbeelden van zulke SSI-initiatieven[17] zijn bijvoorbeeld:

Overheidsorganisatie(s)	Omschrijving
Belastingdienst	De Belastingdienst heeft een visie opgesteld rondom SSI. De Belastingdienst is in de opstartfase voor SSI use cases. Vanaf september 2021 worden twee use cases opgestart: 'BV in a day' en 'Zonnepanelen BTW teruggave'.
BZK en RvIG	BZK en RvIG zijn bezig met de digitale bronidentiteit. Dit is een manier om vanuit de overheid een digitaal identificatiemiddel aan burgers toe te kennen als digitaal equivalent van een paspoort, die de burger via een wallet kan delen in interactie met derden. Daarnaast wil BZK een EBSI ESSIF compliant wallet als prototype opzetten als volgende stap in innovatie. RvIG is ook betrokken bij Digital Travel Credentials initiatieven vanuit de International Civil Aviation Organization (ICAO)
DUO	DUO werkt aan een diploma use-case. Verder is DUO betrokken bij het EBSI-diplomaprogramma[18], wat gelieerd is aan (onder andere) Europass, en is DUO betrokken bij EMREX, waarbij studenten hun (studie)gegevens voor verschillende doeleinden in verschillende landen kunnen gebruiken.
Gemeentes (o.a. Utrecht en Heerlen)	De gemeenten Utrecht en Heerlen werken aan schuldhulpverlening voor kwetsbare gebruikers in het financiële domein. Met gebruik van IRMA kan een burger zich makkelijker identificeren en authentiseren, waardoor de burger eerder en beter geholpen wordt.
KvK	De KvK is betrokken bij diverse SSI-initiatieven waaronder Techruption en de Dutch Blockchain Coalition, bijvoorbeeld rond use cases als 'ZZP in a day' en 'BV in a day' in samenwerking met de Belastingdienst.
SVB, SZW, UWV, VNG en gemeentes (o.a. Enschede)	SVB, SZW, UWV, VNG en gemeenten werken aan het programma Toekomst Werk en Inkomen. Het doel van het programma is om burgers meer regie te geven op diensten die zij afnemen van overheids- en private partijen. Enerzijds door de burgers te informeren over hun rechten, anderzijds door de burgers gegevens digitaal beschikbaar te stellen voor dienstverlening richting andere publieke of private partijen.
VNG, RDW, CJIB (de Blauwe Knop)	VNG en RDW hebben de Blauwe Knop geïntroduceerd om mensen te helpen met regie op hun gegevens en inzichten te geven in hun schulden. Zo kan de overheid effectievere schuldhulpverlening bieden. Andere organisaties die zijn aangesloten bij de Blauwe Knop zijn CAK, CJIB en de gemeenten Tilburg en Boxtel.
VWS	VWS is verantwoordelijk voor de CoronaCheck app waarmee gebruikers (inter-)nationaal kunnen aantonen of zij gevaccineerd zijn, negatief getest zijn op corona, of recent corona hebben gehad. De use case heeft veel raakvlakken met het SSI gedachtegoed: de uitgever van de QR code ziet niet wanneer deze gescand is en door wie. Wel ligt er een centrale database aan ten grondslag, waardoor het niet als decentrale SSI oplossing gezien kan worden.

Tabel 2 Overzicht SSI initiatieven Nederlandse overheid

De SSI-initiatieven van de genoemde overheidsorganisaties zijn veelal nog onderzoekend van aard en richten zich vaak op één specifieke use case. Burgers/ ondernemers die gebruik maken van de genoemde SSI-initiatieven van de Nederlandse overheid zullen op dit moment veelal per initiatief over een aparte wallet app moeten beschikken om een specifiek

[17] Zoals reeds beschreven verschilt de interpretatie van wat wel of niet SSI is in de markt, niet elk initiatief in deze lijst zal door een breed publiek als SSI initiatief worden gezien

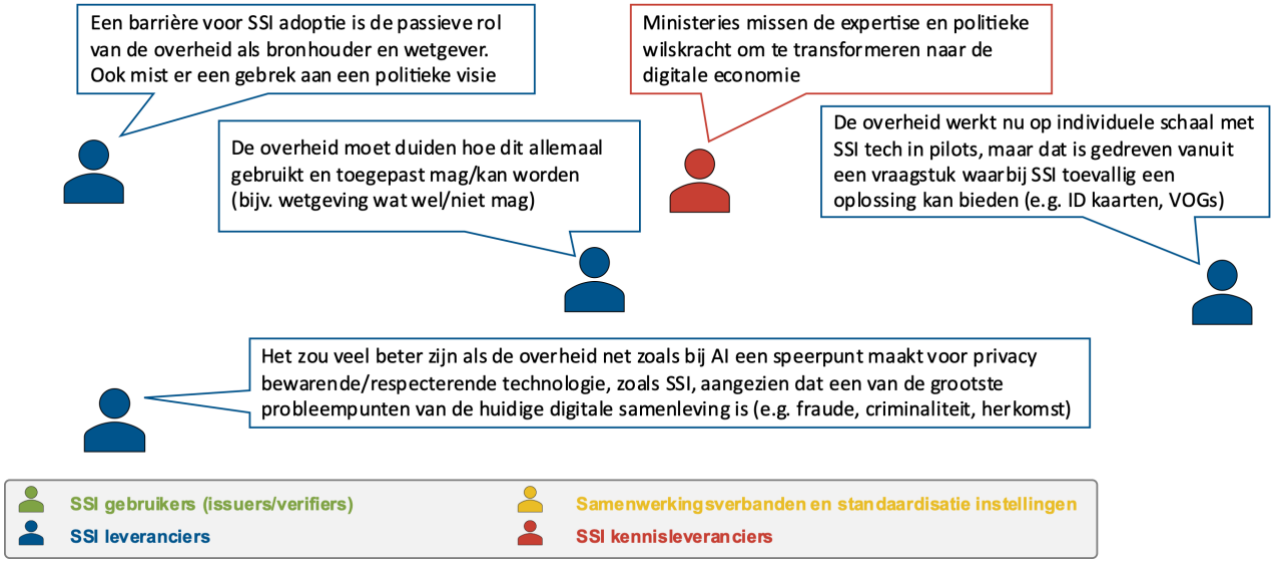
[18] EBSI4be (2021)

identificatiemiddel, diploma, coronabewijs of ander bewijsmiddel in op te kunnen slaan en deze te kunnen delen met partijen die voor deze use case als Verifier optreden.

De initiatieven zijn bovendien veelal opgezet binnen de beperkte scope en visie van de eigen overheidsorganisatie en niet gebaseerd op algemeen geldend overheidsbeleid. Zo bestaat er nog geen brede visie en kaders van de Nederlandse overheid voor overheidsorganisaties over het issuen en verifiëren van credentials en de daarvoor geschikte standaarden, technologieën en producten.

Wij zien dus ook binnen het overheidsdomein fragmentatie in SSI-initiatieven ontstaan. Deze fragmentatie kan leiden tot aansluitingsproblemen tussen verschillende overheidsorganen. Desondanks is het goed dat de overheid veel experimenteert. Experimenteren helpt de overheid om later, als bijvoorbeeld Issuer en/of Verifier in een meer volwassen markt, goed om te gaan met digitale gegevensuitwisseling.

Deze fragmentatie wordt ook opgemerkt door de private partijen die actief zijn in het Nederlandse SSI speelveld. Deze fragmentatie wordt zelfs regelmatig genoemd als barrière voor verdere SSI adoptie in Nederland. De overheid zou volgens de respondenten niet alleen een eenduidige visie op SSI en gewenste implementatie, standaarden etc. moeten hebben, maar ook concreet moeten stimuleren dat SSI initiatieven binnen de overheid conform deze visie uitgewerkt en uitgevoerd worden.



Figuur 9 Reacties uit de enquête over de rol van de overheid

4.4 Conclusies over het Nederlandse SSI speelveld

In dit hoofdstuk hebben wij een overzicht gegeven van de huidige staat van het Nederlandse SSI speelveld. We hebben laten zien welke partijen er in het Nederlandse SSI speelveld actief zijn, welke producten/ diensten zij leveren en hoe deze partijen zich tot elkaar verhouden. De inzichten van de analyse van het Nederlandse SSI speelveld vatten wij samen in vier conclusies die de eerste twee onderzoeksvragen beantwoorden:

1. **Er lopen veel SSI experimenten in Nederland, maar het landschap is gefragmenteerd**
2. **Kritieke massa is (nog) niet gerealiseerd door individuele leveranciers van SSI oplossingen**

3. **SSI gedachtegoed is (nog) niet volwassen genoeg voor grootschalig gebruik in de maatschappij**
4. **Beperkte beschikbaarheid brondata en beperkte herbruikbaarheid in andere domeinen vormt barrière voor waardecreatie**

4.4.1 Er lopen veel SSI experimenten in Nederland, maar het landschap is gefragmenteerd

Kijkend naar het Nederlandse SSI speelveld zien wij dat er opvallend veel activiteit is. Veel verschillende partijen (soms in een cluster met andere partijen) experimenteren voor het faciliteren digitale gegevensuitwisseling binnen hun use cases met het gebruik van verschillende SSI principes, architecturen, infrastructuren, technologieën en diensten.

Dit levert een gefragmenteerd landschap op, vooral op de volgende thema's:

- **De opvattingen over wat SSI wel/ niet is of zou moeten zijn:** Er is veel discussie over de beste of meest zuivere SSI inrichting. Spelers in het speelveld vinden van zichzelf allemaal dat ze "SSI zijn" en soms ook dat andere partijen "geen SSI zijn".
- **Opvattingen over wat de nut en noodzaak van SSI is**: Voor sommigen is de nut en noodzaak van SSI een principekwestie waarbij traditionele invulling van digitale identiteit volledig zou moeten verdwijnen. Anderen richten zich vooral op het realiseren van waarde voor de burger en de Nederlandse economie waarbij de precieze gekozen inrichting (SSI of niet) van ondergeschikt belang is.
- **Diversiteit aan technische inrichting zonder interoperabiliteit**: Rondom verschillende oplossingen wordt vooral gekeken naar de technische werking binnen de eigen use case, hierbij is nog weinig oog voor interoperabiliteit met andere oplossingen in andere domeinen.

Sommige partijen binnen het SSI speelveld werken aan een generieke functioneel bouwblok (zoals een DIDComm service of een credential back up service) voor SSI, met relatief weinig concrete use cases en betrokken partijen. Daar tegenover staan partijen die een single use case uitwerken en proberen om vanuit daar een springplank te zijn naar opschaling in gebruikers en toepassingen. Daarbij is het logisch dat nu nog verschillende technische inrichtingen bekeken worden. Dat er nu een zekere mate van fragmentatie is op met name technisch vlak, is dan ook niet heel verwonderlijk.

Ook de Nederlandse overheid draagt bij aan de fragmentatie in het speelveld doordat verschillende overheidsorganisaties zonder onderlinge coördinatie experimenteren met SSI-achtige producten. Dit maakt het voor andere spelers in het SSI speelveld alleen maar extra onduidelijk wat de positie en de rol van de overheid is en wat toekomstbestendige inrichtingskeuzes zijn.

In het gefragmenteerde Nederlandse SSI speelveld ontbreekt het nu aan samenhang. Er kan niet gesproken worden van één ecosysteem, partijen concentreren zich rondom verschillende eigen use cases en vormen daarmee verschillende ecosystemen naast elkaar, die vaak ook verschillende, onderling niet-interoperabele technologie gebruiken.

4.4.2 Kritieke massa is (nog) niet gerealiseerd door individuele leveranciers van SSI oplossingen

Het resultaat van het gefragmenteerde landschap zoals geschetst in paragraaf 4.4.1 is een hoeveelheid aan eilandjes die voor hun specifieke digitale gegevensuitwisselings use case voor dezelfde uitdaging staan om kritieke massa te organiseren in het samenspel tussen Issuers, Holders en Verifiers.

Zolang deze fragmentatie in de SSI markt blijft, zal het voor partijen een uitdaging blijven om netwerkeffecten en groei van hun SSI initiatief rondom de rollen (Issuer, Holder, Verifier) te realiseren, waardoor de maatschappelijke waarde van digitale gegevensuitwisseling niet ten volle gerealiseerd wordt. Dit vergt samenwerking en coördinatie, tussen zowel publieke en private partijen.

4.4.3 SSI gedachtegoed is (nog) niet volwassen genoeg voor grootschalig gebruik in de maatschappij

De fragmentatie komt voort uit de verschillende ideeën over de beste invulling van SSI Leveranciers, bijvoorbeeld op het gebied van technische inrichting en semantiek. Uit de verschillende experimenten (demonstrators en proof of concepts) is nog geen technische inrichting gekomen waaraan de initiatieven zich in de nabije toekomst zullen conformeren. Bovendien zijn nog niet alle functionele componenten voldoende uitgewerkt. Er is consensus in de markt dat voor een goed functionerend SSI ecosysteem in de Nederlandse maatschappij enkele concepten nog verder onderzocht, ingevuld en geïmplementeerd moeten worden (denk bijvoorbeeld aan zaken als onder curatele of bewind staan, of beperkte handelingsbekwaamheid waardoor mensen een vertegenwoordiger nodig hebben). Typisch zijn dit concepten die niet puur technisch van aard zijn, maar waar juist governance een groot vraagstuk is. Dit maakt dat de initiatieven momenteel nog ongeschikt zijn voor grootschalig gebruik in de maatschappij.

4.4.4 Beperkte beschikbaarheid brondata en beperkte herbruikbaarheid in andere domeinen vormt barrière voor waardecreatie

Zowel overheid als private partijen bezitten (registers met) brondata die, wanneer een gebruiker hier bijvoorbeeld over zou kunnen beschikken via een digital agent waardevol is voor optimalisering bedrijfsprocessen in het private en publieke domein.

Digitale gegevensuitwisseling is sterk afhankelijk van de beschikbaarheid van geverifieerde data. Diverse partijen onderzoeken zelfstandig of in samenwerkingsverbanden hoe digitale gegevensuitwisseling al dan niet via SSI op een verantwoorde manier kan gebeuren.

Echter, zolang de daadwerkelijke brondata die via deze systemen ter beschikking moet worden gesteld niet wordt aangeboden, kan er geen waarde uitwisseling plaatsvinden. De overheid heeft beschikking over zeer diverse datasets over burgers en bedrijven en wordt door spelers in het SSI Speelveld gezien als belangrijke potentiële Issuer voor digitale gegevensuitwisseling.

5 Deel B – (Inter-)nationale ontwikkelingen

Het Nederlande SSI speelveld groeit niet alleen, maar wordt ook beïnvloed door verschillende nationale en internationale ontwikkelingen. Dit hoofdstuk geeft inzicht in de meest relevante (inter-)nationale ontwikkelingen, om vervolgens te duiden hoe dit van invloed is op het Nederlandse SSI speelveld.

5.1 Aanpak

Wij hebben meerdere nationale en internationale ontwikkelingen geanalyseerd op basis van deskresearch, input van de opdrachtgever en begeleidingscommissie, eigen betrokkenheid bij internationale initiatieven (zoals ESSIF en EBSI) en enquêteresultaten. De opdrachtgever en de begeleidingscommissie hebben inzichten geleverd over de huidige status van verschillende wet- en regelgeving. De inzichten zijn aangevuld met reacties van respondenten van de enquête en interviews met marktpartijen.

5.2 Nationale wet- en regelgeving

5.2.1 Wet Digitale Overheid (WDO)

De Wet digitale overheid (WDO) legt de basis voor verdere digitalisering van de overheid. In de WDO wordt vastgelegd waar publieke en private eID-middelen aan moeten voldoen om ingezet te kunnen worden als identificatiemiddel voor online overheidsdienstverlening, dit is in lijn met de Europese eisen aan inlogmiddelen zoals beschreven in de eIDAS-verordening (zie paragraaf 5.3.1).

De voorbereidingen voor de WDO lopen al sinds 2016[19] en het wetsvoorstel is mede naar aanleiding van vragen vanuit Eerste en Tweede Kamer al verschillende keren gewijzigd. De Staatssecretaris voor Binnenlandse Zaken heeft in juni 2021 een aangepast voorstel van de WDO ingediend bij de Tweede Kamer[20]. Na goedkeuring van het wetsvoorstel door het parlement is de verwachte inwerkingtreding van WDO op zijn vroegst voorzien in 2022.

Terwijl het goedkeuringsproces van WDO loopt, zijn er ook al uitbreidingen op de Wet digitale overheid in ontwikkeling, die de wettelijke verankering van de volgende onderwerpen zal regelen:

- Het kader voor het verantwoord delen van digitale persoonsgegevens met partijen binnen en buiten de overheid (regie op gegevens);
- Het beleggen van de verantwoordelijkheid voor het stelsel van basisregistraties en het bewaken van de werking daarvan, waaronder het correct (en verplicht) gebruik van authentieke gegevens in het stelsel;
- Het verder naar elkaar toegroeien van het burger- en bedrijvendomein tot een integraal stelsel van digitale toegang.

Met name de onderwerpen ‘regie op gegevens’ en het hergebruik van authentieke gegevens uit de diverse basisregistraties raken aan Self-Sovereign Identity.

[19] Voortgang Wet Digitale Overheid
[20] Eerste Kamer (2021)

5.2.2 Regie op Gegevens (RoG)

In de beleidsbrief 'Regie op gegevens' uit juli 2019[21] schrijft staatssecretaris Knops (Min. BZK) dat een burger zijn eigen gegevens bij de overheid moet kunnen inzien en wijzigen en dat hij moet kunnen weigeren om gegevens op te geven als de overheid deze zelf al heeft. Regie op gegevens betekent óók dat een burger de gegevens die de overheid over hem heeft (denk aan: adres, leeftijd, inkomen etc.) zélf digitaal moet kunnen delen met dienstverleners van buiten het overheidsdomein zoals zorgverleners, onderwijsinstellingen, woningcorporaties of schuldhulpverleners. Deze partijen zouden zo administratieve rompslomp kunnen beperken en betere diensten kunnen leveren aan hun klanten.

De begrippen ‘Regie op gegevens’ en ‘digitale identiteit’ zitten erg dicht tegen elkaar aan. Niet voor niets is ‘digitale identiteit’ in de visie op digitale identiteit omschreven als “een verzameling van betrouwbare gegevens die een entiteit (persoon, organisatie, object of apparaat) representeren in het digitale domein”. Hierbij gaat het meestal om een beperkte set min of meer statische identiteitsgegevens, die min of meer overeenkomen met de identiteitsgegevens op een fysiek paspoort.

'Regie op gegevens' als beleidsdoelstelling beoogt o.a. gegevens van burgers uit basisregistraties, maar ook gegevens uit andere registraties zoals de Belastingdienst of de RVO, beschikbaar te maken en eventuele barrières hiervoor weg te nemen. Dit heeft als doel dat de burger deze gegevens onder zijn regie veilig kan delen met andere partijen zowel binnen als buiten het overheidsdomein. Het delen van gegevens onder regie van de burger kan op verschillende manieren plaatsvinden: een bronhouder kan deze gegevens rechtstreeks aan de burger verstrekken, een burger kan deze gegevens verstrekken aan derden, of een bronhouder verstrekt deze gegevens aan derden in opdracht van de burger.

Ongeacht het interactiemodel voor digitale gegevensuitwisseling is het hebben van een (betrouwbare en herbruikbare) digitale identiteit randvoorwaardelijk om regie op gegevens voor de burger mogelijk te maken. Staatsecretaris Knops doet hierbij geen uitspraak of dit al dan niet een Self-Sovereign Identity zou moeten zijn.

Regie op gegevens voor burgers is één van de speerpunten van kabinet Rutte-III en daarom werkt het Ministerie van BZK in het programma 'Regie op gegevens' langs diverse actielijnen aan de realisatie van de beleidsdoelstellingen op dit vlak. Hierbij is onder andere aandacht voor het wegnemen van bestaande juridische barrières en wettelijke verankering in de wet Digitale Overheid. Ook heeft de overheid speciale aandacht voor 'digitale inclusie oftewel 'Regie op de eigen gegevens' voor kwetsbare en/of niet-digivaardige burgers, omdat regie op gegevens voor hen zowel kansen als risico's creëert.

[21] Beleidsbrief Regie op Gegevens (2019)

5.3 Internationale wet- en regelgeving

5.3.1 eIDAS

Op Europees niveau raakt het onderwerp digitale identiteit aan het onderdeel elektronische identificatie (eID) in de eIDAS-verordening[22]. De eIDAS-verordening verplicht lidstaten onder meer om elkaars inlogmiddelen te accepteren in de grensoverschrijdende digitale dienstverlening tussen overheden en burgers en bedrijven.

De Europese Commissie heeft in juni 2021 een herziening van de eIDAS verordening voorgesteld[23] met als belangrijkste nieuwigheid dat alle burgers en bedrijven in de EU recht zullen krijgen op een Europese portemonnee voor digitale identiteit (EU Digital Identity Wallet).

De Europese portemonnee voor digitale identiteit is een persoonlijke digitale portemonnee waarmee burgers zich digitaal kunnen identificeren en hun identiteitsgegevens en officiële documenten elektronisch kunnen opslaan en beheren. Met deze portemonnee zullen burgers hun identiteit kunnen bewijzen als dat nodig is om online toegang te krijgen tot diensten, digitale documenten te delen (denk aan: rijbewijs, doktersvoorschriften of diploma's) of simpelweg een specifiek persoonlijk kenmerk te bewijzen, zoals hun leeftijd, zonder dat ze hun identiteit of andere persoonlijke details hoeven prijs te geven. Volgens de verordening zullen burgers altijd en overal volledige zeggenschap houden over de gegevens die zij beheren en delen met andere partijen.

Voor dit initiatief bouwt de Europese Commissie voort op de bestaande eIDAS-verordening. Parallel aan het wetgevingsproces werkt de Commissie met de lidstaten en de private sector samen aan technische aspecten van de Europese digitale identiteit. Het is de ambitie van de Commissie om in oktober 2022 een toolbox met technische standaarden te publiceren, waarna proefprojecten kunnen starten.

Het voorstel voor de herziening van de eIDAS-verordening spreekt nergens expliciet over Self-Sovereign Identity, maar het voorstel ademt op verschillende punten wel het SSI gedachtegoed. Zo spreekt het voorstel over de term 'wallet', focust het voorstel op de gebruiker die via zijn wallet controle zou moeten krijgen over zijn digitale 'gegevens' en zou de gebruiker middels 'selective disclosure' ook slechts delen van zijn identiteitsgegevens moeten kunnen prijsgeven aan partijen die daar om vragen.

Nog niet alles is duidelijk is rondom de herziene eIDAS verordening. Verschillende vragen blijven onbeantwoord zoals:

- Op basis van welke standaarden wordt internationale interoperabiliteit geborgd?
- Vallen de APIs tussen deze wallets en validerende partijen ook binnen deze verordening?

Desondanks zetten verschillende landen al wel de eerste stappen richting gebruik van een dergelijke wallet. Eind 2020 initieerde Duitsland de eerste use case voor gebruik van het

[22] EUR-Lex (2014)
[23] European Commission (2021)

European Digital Identity Initiative[24]. Binnen deze use case kunnen zakenreizigers inchecken bij een hotel met gebruik van een credential gebaseerd op hun ID bewijs. Eind juli 2021 maakten Duitsland en Spanje bekend te gaan samenwerken rondom de SSI wallets[25]. Hiertoe is een Memorandum of Understanding getekend, deze is open voor andere landen om aan te sluiten. Ook Nederland is sinds september aangesloten bij deze samenwerking. Binnen de samenwerking zullen best practices gedeeld worden, op technisch, operationeel en regelgevend niveau, en zal cross border interoperabiliteit worden geborgd.

5.3.2 Open Banking en 'Revised Payment Services Directive' (PSD2)

Sinds 2019 is in Europa de *Revised Payment Services Directive*[26] (PSD2) van kracht. Naast herzieningen van afspraken omtrent betalingsverkeer is een belangrijke pijler van deze wet de bepalingen rondom '*Access to accounts*'. Access to accounts, ofwel 'toegang tot rekeningen', maakt het mogelijk dat derde partijen rechtstreeks bij banken data van de consument (bijvoorbeeld transactiegeschiedenis) kunnen opvragen of betalingen initiëren. Dit is onderdeel van de grotere 'Open Banking' beweging waarbij burgers hun financiële data en -dienstverlening niet meer exclusief via hun banken aangeboden krijgen. Derde partijen kunnen op basis van bijvoorbeeld APIs deze data opvragen en dienstverlening initiëren, waarmee zij bankzaken verder kunnen integreren in eigen dienstverlening naar burgers toe. PSD2 en Open Banking zijn geen voorbeelden van SSI en het 'Digital Agent' interactiemodel. PSD2 en Open Banking zijn wel voorbeelden van een grote Europese beweging omtrent het veilig en met controle organiseren van digitale gegevensuitwisseling, op basis van data bij de bron ophalen.

5.4 Andere internationale ontwikkelingen

5.4.1 Standaardisatie en grote consortia

Wereldwijd zijn er verschillende partijen die samenwerken aan standaardisatie van de verschillende componenten en manieren van digitale gegevensuitwisseling. Typisch is er samenhang tussen deze standaardisatiegremia, al kent ieder zijn eigen focus. Tabel 3 beschrijft een aantal van deze consortia.

Consortium	Omschrijving
Trust over IP[27]	ToIP focust zich op de gehele architectuur rondom een privacy-vriendelijke, veilige en betrouwbare communicatie. Verschillende werkgroepen houden zich bezig met andere lagen van deze architectuur, maar ook met onderwerpen zoals terminologie en samenwerking binnen ecosystemen. Dit is een wereldwijd consortium en valt onder de Linux Foundation.
EBSI-ESSIF	ESSIF is een van de use-cases van EBSI (European Blockchain Services Infrastructure), die beoogt SSI te gebruiken voor 'cross-border interaction', integratie met eIDAS, e-delivery, 'once-only', en 'to preserve European/democratic values in the implementation of SSI'[2829]
eSSIF-Lab[30]	eSSIF-Lab is een EU cascaded funding project, met focus op een open en betrouwbare digitale identiteitoplossing voor sneller en veiligere digitale gegevensuitwisseling.
W3C[31]	W3C is een internationale gemeenschap dat zich richt op standaardisatie voor het World Wide Web. Ook is hier plaats voor standaarden binnen de onderste lagen in de

[24] Bundeskanzleramt (2021)
[25] Die Bundesregierung (2021)
[27] Trust over IP Foundation (2021)

	SSI architectuur, zoals DIDs. W3C specificeert ook een veel-gebruikt datamodel voor Verifiable Credentials.
Hyperledger[32]	Hyperledger is een open source community die zich bezighoudt met de ontwikkeling frameworks, tooling en libraries voor blockchain oplossingen. Binnen de wereldwijde SSI community wordt vooral gekeken naar Aries, Fabric, Indy, Ursa.

Tabel 3 Consortia op het gebied van SSI

5.4.2 Internationale initiatieven

Ook buiten Europa wordt toegewerkt naar de eerste digitale gegevensuitwisselingen op basis van digital agents. Een voorbeeld hiervan is de Good Health Pass (GHP), een consortium dat toewerkt naar interoperabele digitale gezondheidsverklaringen om internationale reizen weer mogelijk te maken[33]. Dit initiatief is opgestart in 2020, naar aanleiding van de Covid-19 pandemie en maakt gebruik van diverse SSI concepten. De credentials van de GHP worden geaccepteerd door andere organisaties die ook bezig zijn met internationaal reizen zoals de International Civil Aviation Organisation (ICAO), International Air Transport Association (IATA), de Collaborative Arrangement for the Prevention and Management of Public Health Events in Civil Aviation (CAPSCA) en de Airport Council International (ACI).

Daarnaast hebben Big Tech spelers ook veel invloed op het SSI speelveld. Zo is Apple actief betrokken bij de ontwikkeling van ISO standaard 18013-5 mDL (mobile driver's license)[34]. Apple heeft recent aangekondigd dat mensen rijbewijzen en ID kaarten kunnen toevoegen aan hun Apple wallet[35]. In eerste instantie introduceert Apple de functie in meerdere staten van de Verenigde Staten. Het is aannemelijk dat Apple deze functie op een later tijdstip ook zal willen introduceren in Europese landen. Ook Google erkent de use case van mobiele rijbewijzen en ePaspoorten[36]. Het is daarom ook zeer aannemelijk dat Google bezig is met een eigen poging om rijbewijzen en paspoort te koppelen aan Google Pay. Microsoft is actief betrokken bij de Decentralized Identity Foundation (DIF), de W3C Credentials Community Group en andere bredere identiteits-communities. Naast de betrokkenheid in deze communities heeft Microsoft recent Azure AD verifiable credentials geïntroduceerd. Deze credentials bieden een platform om digitaal verifiable credentials te valideren[37].

5.5 Analyse (inter-)nationale ontwikkelingen

Wij zien dat er zowel nationaal als internationaal veel ontwikkelingen zijn op het gebied van digitale gegevensuitwisseling. Binnen en buiten Nederland zien wij wet- en regelgeving ontstaan. Deze wet- en regelgeving ontwikkelen door en hebben veel invloed heeft op digitale gegevensuitwisseling. Het ontbreekt echter nog aan een scherp overzicht hoe deze verschillende nationale en internationale wet- en regelgevingen zich tot elkaar (gaan)

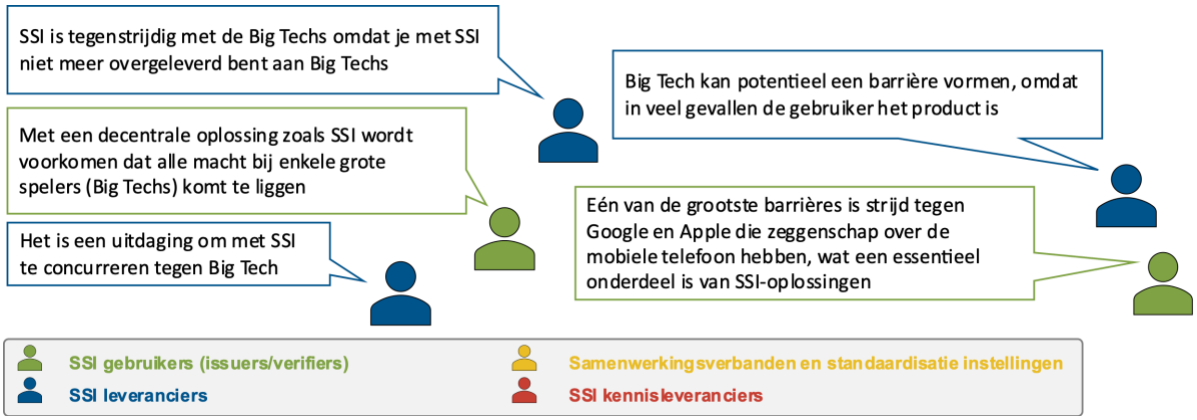
[27] Trust over IP Foundation (2021)
[28] Decentralized Identity Foundation (2020)
[29] ESSIF (2019)
[30] ESSIF Lab (2021)
[31] W3C (2021)
[32] Hyperledger (2021)
[33] Good Health Pass (2021)
[34] ISO (2021)
[35] Apple (2021)
[36] Google (2021)
[37] Microsoft (2021)

verhouden. Marktpartijen benoemen dit ook als één van de barrières voor het realiseren van de maatschappelijke waarde van SSI (zie Figuur 10). Doordat dit overzicht mist, zullen SSI Gebruikers langer in een exploratieve fase blijven omdat ze (nog) niet willen committeren aan SSI oplossingen.

Ook moet de mogelijke impact van de eIDAS revisie niet onderschat worden. Zeker gezien het beoogde dwingende karakter van de eIDAS revisie (o.a. verplichting voor lidstaten tot het aanbieden van wallet(s) in tegenstelling tot de mogelijkheid om identiteitsmiddelen te notificeren zoals in de huidige eIDAS verordening), kan deze wetgeving grote veranderingen in de lidstaten als gevolg hebben (vergelijkbaar met de impact van het genoemde PSD2 op het Europese betaallandschap). Dit kan in een hoog tempo innovatie en vernieuwing teweegbrengen, waarbij Nederland bijtijds in moet stappen om te voorkomen dat zij slechts gedicteerd krijgt wat de te volgen standaarden zijn.

Figuur 10 Reacties uit de enquête over de onduidelijkheid rondom wet- en regelgeving

Er zijn ook andere internationale ontwikkelingen die invloed hebben op het Nederlandse speelveld. Het belangrijkste hier is de invloed van Big Tech. Veel respondenten ervaren Big Tech spelers als een bedreiging voor het SSI denkbeeld en het succes van SSI initiatieven (zie Figuur 11). Dit komt onder andere doordat Big Tech spelers over voldoende financiële middelen beschikken om snel producten en diensten te ontwikkelen en introduceren aan consumenten. De machtsongelijkheid groeit verder doordat Apple en Google 'zeggenschap' hebben over mobiele telefoons en de daarbij horende app stores, die beiden essentieel zijn voor SSI initiatieven.



Figuur 11 Reacties uit de enquête over de strijd met Big Tech

5.6 Conclusies (inter-)nationale ontwikkelingen

Er zijn veel nationale en internationale ontwikkelingen en initiatieven die het Nederlandse SSI speelveld beïnvloeden. De inzichten van de analyse vatten wij samen in twee conclusies die de derde onderzoeksvraag beantwoorden:

- **Het is onduidelijk hoe de verschillende juridische kaders zich tot elkaar (gaan) verhouden**
- **Grote commerciële partijen kunnen sneller bewegen dan wetgevende ontwikkelingen waardoor zij de markt kunnen domineren en verstoren**

5.6.1 Het is onduidelijk hoe verschillende juridische kaders zich tot elkaar (gaan) verhouden

Voor spelers in het (SSI) speelveld is er onduidelijkheid op het gebied van wet- en regelgeving. Voor marktpartijen is er onduidelijkheid over de richting van de overheid. Ook missen marktpartijen duidelijke kaders in wet- en regelgeving wat wel en niet mag en missen marktpartijen duidelijke tijdslijnen voor wet- en regelgeving. De onduidelijkheid remt de adoptie van SSI oplossingen in de markt. SSI Gebruikers (e.g. banken, verzekeraars) experimenteren met SSI, maar zullen zonder duidelijkheid op het gebied van wetgeving zeer terughoudend zijn met het omarmen van huidige SSI oplossingen.

5.6.2 Grote commerciële partijen kunnen sneller bewegen dan wetgevende ontwikkelingen waardoor zij de markt kunnen domineren en verstoren

In het digitale domein beweegt de wereld snel. De ontwikkelsnelheid bij individuele organisaties is vaak hoger dan het tempo van grootschalige wetgevende veranderingen, die vaak jaren kosten om te realiseren. Grote commerciële partijen (zoals Big Techs) kunnen sneller bewegen, waardoor (wetgevende) ambities van de lidstaten worden ingehaald en overbodig worden gemaakt.

6 Deel C – Toekomstige ontwikkelrichtingen en impact op publieke waarden

In de vorige hoofdstukken hebben wij de huidige staat van het SSI Speelveld in Nederland laten zien. Ook schetsten wij een aantal (inter-)nationale ontwikkelingen die van invloed zijn op de verdere doorontwikkeling van dit speelveld. In hoofdstuk 6 onderzoeken wij aan de hand van enkele toekomstscenario's hoe dit SSI Speelveld zich verder zou kunnen doorontwikkelen, om vervolgens te kunnen wegen welk effect deze ontwikkelrichtingen zouden hebben op publieke waarden. Deze inzichten zullen richting geven voor Min BZK voor toekomstige beleidskeuzes op het gebied van digitale identiteit en regie op gegevens.

6.1 Aanpak

Er bestaat binnen de Nederlandse overheid geen formele en uitputtende lijst van publieke waarden. In overleg met opdrachtgever Min BZK is daarom een lijst samengesteld van verschillende publieke waarden die zij het meest van belang achten om vanuit haar maatschappelijk rol te borgen. Als input voor het overzicht met publieke waarden gebruikten wij ook (overheids-)publicaties, zoals de visiebrief Digitale Identiteit[38] en het wegingskader Digitale Identiteit[39].

Vervolgens hebben wij op basis van enquêteresultaten en inzichten uit de analyse van internationale ontwikkelingen, gecombineerd met input van opdrachtgever en begeleidingscommissie twee ontwikkelrichtingen rondom het thema digitale gegevensuitwisseling opgesteld. Dit resulteerde in vier toekomstscenario's.

We doen hierbij nadrukkelijk geen poging om de toekomst te voorspellen en spreken ook geen waardeoordeel uit over de verschillende scenario's. De scenario's schetsen slechts plausibele toekomstbeelden. Dit moet de opdrachtgever helpen om gevoel te krijgen voor hoe een dergelijk toekomstscenario mogelijk zou uitwerken op verschillende actoren zoals burgers, bedrijven en SSI Leveranciers en wat de impact van deze scenario's op verschillende publieke waarden zou zijn.

6.2 Publieke waarden

Het ministerie van BZK is beleidsverantwoordelijk voor onderwerpen als digitale identiteit en digitalisering. Bij het maken van beleidskeuzes op deze onderwerpen zal Min BZK altijd rekening moeten houden met impact op publieke waarden, zoals privacy, veiligheid en autonomie. Waar mogelijk en passend bij haar rol, zal BZK gunstige effecten op publieke waarden willen stimuleren en negatieve effecten zoveel mogelijk willen voorkomen. Soms is het onvermijdelijk dat een positief effect op de ene publieke waarde, een negatief effect op de andere publieke waarde zal hebben. De overheid zal de impact op publieke waarden steeds zorgvuldig en in samenhang met elkaar moeten afwegen, alvorens te kunnen besluiten hoe het daar mee om wil gaan.

Tabel 4 schetst het overzicht van publieke waarden dat de basis vormde in de verdere analyse van de verschillende toekomstscenario's:

[38] Visiebrief digitale identiteit (2021)
[39] Wegingskader digitale identiteit – Waag (2019)

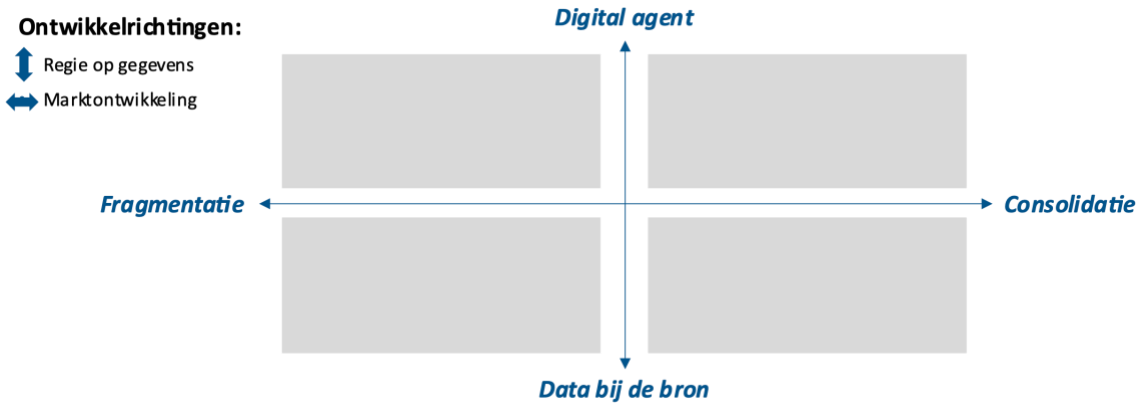
Publieke waarden	Omschrijving
Privacy	Privacy gaat over afscherming van personen, groepen en (commerciële of niet-commerciële) organisaties van bespieding en beïnvloeding, en omvat het recht om vertrouwelijk te communiceren en om niet onnodig/ongewenst lastig te worden gevallen
(cyber)Veiligheid	Het beschermen van personen, groepen en organisaties tegen identiteitsfraude en het waarborgen van de cybersecurity van digitale en fysieke systemen
Autonomie en regie op gegevens	Zeggenschap personen, groepen en organisaties over gegevens die op henzelf betrekking hebben, inclusief de mogelijkheid om deze gegevens te corrigeren, te verwijderen of te (her)gebruiken waar zij dat willen
Inclusiviteit	De mate waarin personen en groepen kunnen deelnemen aan de diverse digitale ecosystemen
Decentralisatie van kennis en macht	Overdracht van kennis en bevoegdheden naar lagere organen, vermindering van centrale aansturing (van bijvoorbeeld overheden, organisaties en samenwerkingsverbanden)
Transparantie	De mate waarin personen, groepen en organisaties zicht hebben op welke gegevens die op henzelf betrekking hebben voor welk doel gebruikt worden
Innovatie/verdienvermogen	De mate waarin commerciële en niet-commerciële organisaties in staat zijn om diensten te verbeteren, kosten te verlagen en uiteindelijk winstgevend te opereren
Gelijke concurrentievoorwaarden	De eerlijke machtsverhouding in de relaties tussen burgers en organisaties en tussen organisaties onderling
Adequate overheidsdienstverlening	De mate waarin de overheid haar dienstverlening efficiënt, kwalitatief hoogwaardig en effectief uitvoert. Deze dienstverlening bestaat vooral uit het nemen van en communiceren over besluiten
Zorgplicht van de overheid tegenover burgers/bedrijven	De plicht van de overheid om zorgvuldig om te gaan met de belangen van burgers en bedrijven en die te beschermen wanneer burgers en bedrijven dat zelf niet (goed) kunnen
Betrouwbare overheid	De mate waarin de overheid haar werk op een voorspelbare, consistente en samenhangende wijze uitvoert, en dit doet volgens de regels van de wet c.q. andere overheidsuitspraken

Tabel 4 Overzicht van publieke waarden

6.3 Ontwikkelrichtingen en toekomstscenario's

Ontwikkelrichtingen geven aan waar het Nederlandse speelveld voor digitale gegevensuitwisseling zich in de toekomst naartoe kan bewegen. Op basis van de verzamelde input hanteren wij de volgende twee ontwikkelingen als basis voor de toekomstscenario's om de ontwikkeling van het speelveld te duiden:

1. Regie op gegevens: 'Data bij de bron' versus 'Data via een digital agent'
2. Marktontwikkeling: 'Fragmentatie versus consolidatie van een markt'



Figuur 12 Ontwikkelrichtingen van het Nederlandse speelveld

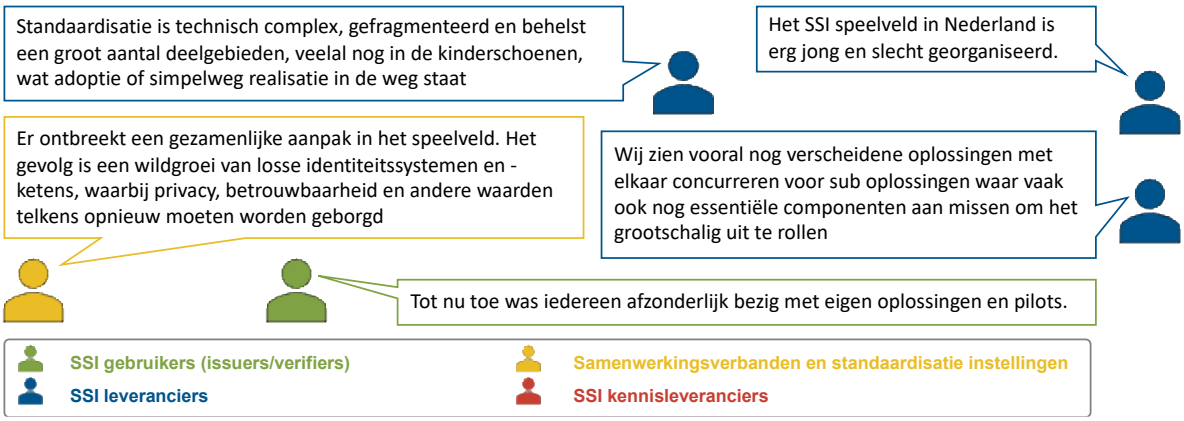
6.3.1 Ontwikkelrichting: Regie op gegevens

Zoals eerder geschetst, is het hebben van een Self-Sovereign Identity geen doel op zich; het gaat erom wat je ermee mogelijk maakt: betrouwbare, digitale gegevensuitwisseling onder regie van de gebruiker.

Je kunt deze regie op gegevens faciliteren via een digital agent (bijv. een wallet), zodat de burger zelf de beschikking heeft over zijn identiteitsgegevens en zelf kan bepalen met wie hij deze gegevens deelt in een digitale transactie. Zoals we in hoofdstuk 3 schetsen, is men het er inmiddels over eens dat dit de 'SSI' manier van digitale gegevensuitwisseling is. Wanneer je SSI in deze context van digitale gegevensuitwisseling beschouwt, dan is er ook een grote tegenhanger waarneembaar: het digitaal uitwisselen van gegevens door deze rechtstreeks bij de bron op te vragen (eenmalig of doorlopend), altijd met consent van de gebruiker. (Denk aan: Open Banking/PSD2 in hoofdstuk 5.3.2). We noemen deze vorm van 'regie op gegevens' hier 'Data bij de bron'.

6.3.2 Ontwikkelrichting: Marktontwikkeling

Respondenten van de enquête benoemen ook veelvuldig de noodzaak tot consolidatie of het oplossen van fragmentatie om maatschappelijke baten van SSI te kunnen benutten. (Zie Figuur 13). In deze analyse beschouwen we 'de markt' als de markt voor Issuers, Holders en Verifiers.



Figuur 13 Enkele reacties uit enquête over Marktontwikkeling

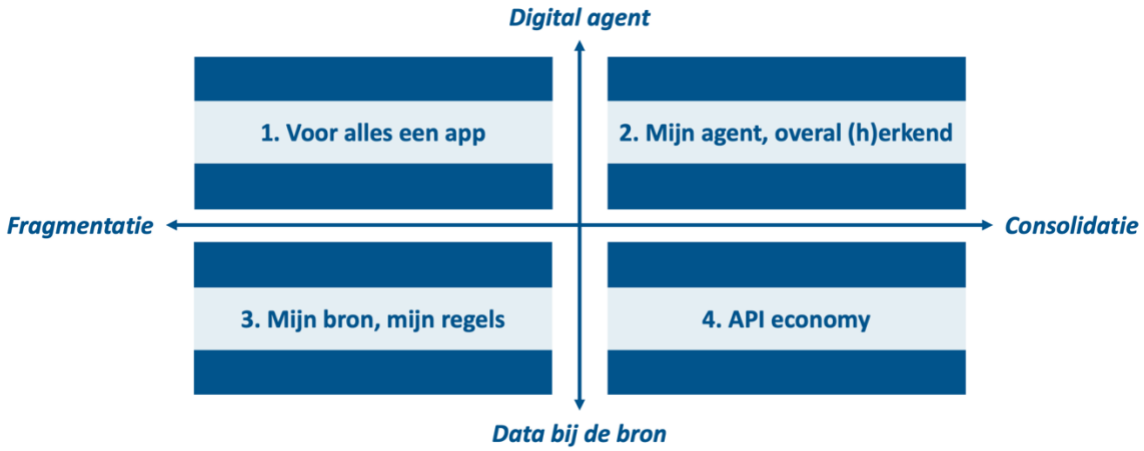
Het spanningsveld tussen fragmentatie en consolidatie is een steeds terugkerend thema in de ontwikkeling en opschaling van digitale ecosystemen, en daarmee niet uniek voor dit speelveld. In nieuwe of onvolwassen markten verkennen verschillende organisaties wat een goede productinrichting is, onderzoeken zij technologische mogelijkheden en klantbehoeften, met fragmentatie als gevolg. Tegenover deze versnipperde en gefragmenteerde ontwikkeling, staat consolidatie; een markt waarin dienstverlening, producten en technologie juist goed op elkaar aansluiten Consolidatie van de markt betekent in het algemeen dat gebruikers minder verschillende dienstverleners, producten en technologieën nodig hebben.

Consolidatie en fragmentatie kunnen ieder een gunstig of juist negatief effect hebben op publieke waarden en de spelers in het speelveld, wat het een geschikt onderwerp maakt om als ontwikkelrichting te beschouwen in dit verkennende onderzoek.

6.3.3 Toekomstscenario's

De toekomstscenario's vormen we door de twee uitersten van deze trends op een as te zetten en de assen met elkaar te confronteren. Dit heeft geleid tot de volgende 4 toekomstscenario's:

1. **Voor alles een app**
2. **Mijn agent, overal (h)erkend**
3. **Mijn bron, mijn regels**
4. **API economy**



Figuur 14 Toekomstscenario's voor het Nederlandse speelveld

Scenario 1: 'Voor alles een app'

In dit scenario gebruiken en ontwikkelen partijen ieder hun eigen, proprietary SSI oplossingen, wat een gefragmenteerd en versplinterd landschap oplevert. Het ontbreekt aan interoperabititeit tussen SSI oplossingen, waardoor iedere consument, organisatie en overheidsinstelling tientallen digital agents en SSI Leveranciers moet gebruiken, die ieder op hun eigen wijze credentials uitgeven, opslaan, verifiëren en verzenden. Burgers hebben zelf de regie over wanneer ze welke data met wie delen, zonder dat de Issuer hier weet van heeft, maar zijn voor specifieke use cases wel gebonden aan specifieke wallets. De huidige digitale sleutelbos wordt zo een sleutelbos van apps/digital agents.

Voor elke wallet die een partij zijn burgers of klanten toestaat te gebruiken, moet hij de juiste soort credential en protocol kunnen gebruiken en dus implementeren. Hetzelfde geldt voor partijen die credentials willen gebruiken (Verifiers): zij zullen het type credential en protocol moeten implementeren van alle wallets die ze klant/burger toestaan te gebruiken. Ook op gebied van vertrouwen en governance is de versplintering merkbaar. Verifiers vertrouwen bijvoorbeeld sommige Issuers niet als betrouwbare databronnen, of digital agents accepteren verzoeken van bepaalde Verifiers niet omdat deze niet onder passend toezicht vallen.

Scenario 2: 'Mijn agent, overal (h)erkend'

In dit scenario heeft een flinke consolidatieslag plaatsgevonden in het SSI speelveld. Er ontstaat een breed ecosysteem waarin verschillende partijen goed op elkaar aansluiten en interoperabel zijn, zowel technisch als op governance niveau. Burgers genieten van een hoge mate van regie op gegevens en soevereiniteit. Met één of enkele digital agents hebben zij grote keuzevrijheid in producten die zij overal kunnen gebruiken. Er is geen, of slechts een lage mate van lock-in. Met behulp van hun digital agents kunnen burgers bijna overal makkelijk terecht, burgers kunnen bijvoorbeeld gemakkelijker online formulieren invullen, zonder dat partijen die deze gegevens als Issuer aan de burger verstrekt hebben, weten dat deze data daarvoor gebruikt worden. Daar tegenover staat wel "opstartmoeite" voor de burgers, zij zullen credentials bij bronnen moeten ophalen, beheren en beschikbaar maken via hun agent voordat zij kunnen participeren in digitale gegevensuitwisseling. Hoewel dit proces uiteindelijk grotendeels geautomatiseerd kan worden, moeten burgers nog wel onboarden bij agents en databronnen om deze uitwisseling mogelijk te maken.

Iedere partij heeft de keuze uit SSI wallets/producten/diensten, op de achtergrond zorgen gemeenschappelijke afspraken over bijvoorbeeld infrastructuur, standaarden, semantiek en aansprakelijkheid ervoor dat de SSI wallets/producten/diensten frictieloos met elkaar samenwerken (interoperabiliteit). Daarnaast werken de Europese overheden samen door dezelfde standaarden te gebruiken waardoor internationale samenwerking mogelijk is vanwege cross-border interoperabiliteit. Voor partijen in de validerende rol zullen meer soorten gegevens potentieel[40] beschikbaar komen die bovendien van hogere kwaliteit zijn. Dat drukt de kosten voor het verkrijgen/gebruiken van deze data. Door standaardisatie wordt het eenvoudiger om credentials afkomstig uit verschillende databronnen te verifiëren. Als Issuer zullen partijen merken dat het eenvoudig is om credentials aan

[40] Het feit dat gegevens in principe ontsloten zijn betekent niet dat iedereen daar zonder meer toegang toe heeft. Het besluit om gevraagde gegevens daadwerkelijk te leveren ligt bij de partij van wie ze worden verkregen: bij 'digital agent' is dat de burger, bij 'data bij de bron' is dat de bronhouder.

eenieder beschikbaar te stellen die ze daarvoor in aanmerking vinden komen. Voor alle partijen geldt dat er geen, of een lage mate van 'vendor lock-in' is van technologie (door de open standaarden).

Scenario 3: 'Mijn bron, mijn regels'

Er is een grote wildgroei aan producten en diensten op gebied van digitale identiteit en digitale gegevensuitwisseling waarbij data direct bij de databron wordt opgehaald. Elke consument heeft een steeds groter wordend aantal digitale identiteiten (accounts), elk voor een ander doel en andere dienst. De burger moet per databron en per Verifier aangeven of deze toegang kan krijgen tot de brondata. Dit zou een eenmalige of doorlopende toestemming kunnen zijn. Door de hoge mate van concurrentie zullen producten/diensten 'gratis' zijn voor de burger. In de praktijk betaalt de burger met zijn data. De burger kan verder te maken krijgen met voor hem/haar onbekende dienstverleners die om consent vragen voor data transacties, wat voor vragen of onzekerheid bij de burger kan zorgen.

Elke databron maakt gebruik van verschillende standaarden voor het ontsluiten van data, wat integratie voor Verifiers tijdrovend en complex maakt. Issuers die data beschikbaar stellen, hebben mogelijk inzicht in transacties, weten precies welke andere partijen gebruik van maken van deze data. Zij kunnen zo eenvoudig een verdienmodel op basis van transactievolume creëren. Verifiers zullen per databron die zij bevragen, aanpassingen moeten maken om te voldoen aan de integratiestandaarden van de 'issuer', wat een barriere vormt voor opschaling. Wanneer de 'verifiers' de brondata kunnen gebruiken voor hun besluitvorming, kan dit wel een hogere mate van zekerheid opleveren.

Scenario 4: 'API economy'

In dit scenario blijven er enkele betrouwbare partijen over die namens een burger data ophalen bij de bron, om door andere partijen te gebruiken in hun bedrijfsprocessen. Iedere burger, organisatie en overheidsinstelling heeft keuze uit diverse digitale identiteit producten, die elk een eigen level of assurance bieden. Om dit mogelijk te maken, wordt gebruik gemaakt van standaarden en koppelingen zoals APIs. Afsprakenstelsels regelen de afspraken en standaarden op technisch vlak, governance en vertrouwensniveau.

Burgers kunnen kiezen voor een handvol digitale identiteit producten. Omdat er relatief weinig concurrentie is, zou het kunnen dat burgers betalen (met geld) om gebruik te kunnen maken van een dienst die geleverd wordt door zo'n betrouwbaar merk. De burger wordt niet lastiggevallen met producten of inspanning voor het beheren van zijn eigen data. Dit gaat allemaal buiten de burger om en hij/zij hoeft alleen zo nu en dan consent te geven voor specifieke transacties.

6.4 Analyse toekomstige ontwikkelrichtingen en toekomstscenario's en impact op publieke waarden

In bijlage 9.3 staat een totaaloverzicht staan van de impact van de verschillende toekomstscenario's op de verschillende publieke waarden zoals genoemd in Hoofdstuk 6.2. We beperken ons hier tot de belangrijkste inzichten uit deze analyse. We zullen de impact op publieke waarde duiden aan de hand van de ontwikkelrichtingen.

6.4.1 Regie op gegevens

Binnen de ontwikkelrichting ‘Regie op gegevens’ onderscheiden we zoals gezegd twee archetype interactievormen: via een ‘digital agent’ en ‘data bij de bron’. In de praktijk zien we dat de gewenste interactievorm vooral afhangt van de context waarin digitale gegevensuitwisseling plaats vindt. Beide interactievormen zullen in de toekomst naast elkaar bestaan en aanbieders van geverifieerde data zullen moeten bepalen voor welke interactievorm(en) het logisch is om de data aan te bieden.

Voor situaties waar bijvoorbeeld de overheid tegelijkertijd issuer en verifier van dezelfde data is, is direct data ophalen bij de bron laagdrempeliger voor de burger (wat niet betekent dat dit in de huidige praktijk overal zo werkt, reeds bekende data wordt nog vaak dubbel gevraagd). Of in noodsituaties, waar de burger niet in staat is om zijn digital agent te gebruiken, kan het essentieel zijn om data (bijvoorbeeld medische gegevens) bij de bron op te halen.

Met betrekking tot de publieke waarden zien we vooral voor publieke waarden als autonomie en privacy voordelen bij ‘digital agents’ ten opzichte van ‘data bij de bron’. Deze toegenomen autonomie en bescherming van de gebruiker tegen “meekijken” schuren wel met publieke waarden als zorgplicht wat bemoeilijkt wordt wanneer burger en bedrijf zeer autonoom handelen. Echter, dit geldt met name voor smartphone-based wallets. Wanneer een burger gebruik maakt van een cloud-based wallet, is het mogelijk dat er “meegekeken” wordt door de wallet leverancier, afhankelijk van de technische inrichting (er bestaan praktijkvoorbeelden van identiteitsoplossingen waar met de juiste certificeringen aangetoond kan worden dat confidentialiteit gewaarborgd blijft in een cloud opstelling).

Ook de publieke waarde Inclusiviteit staat onder druk in een door ‘digital agents’ gedomineerd landschap. Voordat dit breed inzetbaar is voor alle burgers in de Nederlandse maatschappij (ook voor laaggeletterden, digibeten, etc) zullen er nog onopgeloste issues en aandachtspunten rondom gebruiksvriendelijkheid en toegankelijkheid opgelost moeten worden. Het gaat daarbij niet alleen om het goedkeuren of consent geven voor een transactie, maar ook de bredere participatie in het ecosysteem. Denk hierbij aan de huidige complexiteiten van onboarden voor SSI oplossingen en een onderwerp als guardianship, waarin iemand digitaal namens een ander kan handelen, een thema dat op zichzelf weer schuurt met SSI gedachtegoed over volledig autonoom handelen door burger en bedrijf.

6.4.2 Marktontwikkeling

Elke (digitale) markt, waarin dienstaanbieders de competitie met elkaar aangaan, kent schommelingen tussen fragmentatie en consolidatie van diensten. Deze marktontwikkeling heeft een dynamisch karakter, door de tijd heen zal er altijd tussen fragmentatie en consolidatie heen en weer bewogen worden. Met als kanttekening dat fragmentatie eenvoudig kan ontstaan en consolidatie een grote inspanning van actoren vraagt om te realiseren. Voor de individuele organisatie lijkt het wellicht beperkte moeite om zijn eigen implementatie op een opportuun moment aan te passen naar meer gangbare standaarden. Echter, wanneer meerdere organisaties deze aanpak hanteren wordt het collectief al complex om een gangbare standaard te kiezen. En wanneer dit probleem zo groot geworden is dat de markt collectief vastzit in fragmentatie, dan is er een marktfalen ontstaan waar ook individuele partijen niet eenvoudig met aanpassingen aan de eigen

implementatie uit los kunnen komen. Het oplossen van fragmentatie is daarmee niet een individuele aangelegenheid en 'slechts' kostenimpact, maar een gezamenlijke inspanning van betrokkenen in een markt die coördinatie vergt.

Fragmentatie is, zeker in vroegere fases van productvolwassenheid prettig, omdat het ruimte biedt voor experimenten en verkenning. Hiermee wordt onderzocht wat 'best practices' zijn om invulling te geven aan producten, waarna de mogelijkheid bestaat om te consolideren. In een te vroeg stadium consolidatie afdwingen geeft het risico dat er zwaar wordt ingezet op sub-optimale oplossingen. Wanneer een markt een periode van consolidatie heeft gekend, zullen er altijd weer dienstverleners opstaan die nieuwe richtingen en concepten gaan verkennen, wat een nieuwe beweging richting fragmentatie inzet. Partijen in de markt zelf kunnen gezamenlijk consolidatie realiseren, alternatief kan wetgeving of overig overheidsbeleid een belangrijke drijfveer zijn tot consolidatie.

Met betrekking tot de publieke waarden zien we voor burger en bedrijf over het algemeen positieve impact voor de scenario's die op een geconsolideerde markt zijn gebaseerd. De gevraagde inspanning of diversiteit aan benodigde producten/implementaties neemt af, waardoor burger en bedrijf gemakkelijker van dienstverlening gebruik kunnen maken. Publieke waarden als (cyber)veiligheid zijn veel beter te organiseren wanneer leveranciers in de markt gebruik maken van geaccepteerde standaarden en onderdeel zijn van governance raamwerken waarin goed toezicht op geleverde kwaliteit bestaat.

Tegenover het geleverde gemak voor burger en bedrijf, drukken geconsolideerde markten wel op het verdienvermogen van leveranciers. Het basisproduct van 'digitale gegevensuitwisseling' mogelijk maken wordt dusdanig generiek door standaarden, dat marges daarin teruglopen en verdienmodellen in de bredere context van gegevensuitwisseling gevonden moeten worden. In een meer gefragmenteerde markt is er voor leveranciers veel meer vrijheid om te experimenteren en onderscheidend vermogen te leveren.

6.5 Conclusies toekomstige ontwikkelrichtingen en impact op publieke waarden

Op basis van het bestuderen van twee ontwikkelrichtingen voor digitale gegevensuitwisseling en de impact op publieke waarden in verschillende toekomstscenario's, trekken wij twee conclusies die de vierde en vijfde onderzoeksvraag beantwoorden:

- **'Digital agent' en 'Data bij de bron' zijn twee verschillende interactievormen die beide gefaciliteerd moeten worden**
- **Een geconsolideerde markt voor digitale gegevensuitwisseling heeft positieve effecten op de publieke waarden voor burgers, bedrijven en overheid**

6.5.1 'Digital agent' en 'Data bij de bron' zijn twee verschillende interactievormen die beide gefaciliteerd moeten worden

'Digital agent' en 'Data bij de bron' interactiemodellen kennen elk andere relevante use cases. Zo kan een 'Digital agent' bijvoorbeeld relevant zijn voor het laten zien van een digitaal paspoort. Voor het hergebruik van BRP-informatie binnen de overheid kan 'Data bij de bron' relevant zijn. Issuers en Verifiers moeten daarom begrijpen wanneer een bepaalde

interactievorm wenselijk is voor de toepassing waarbinnen digitale gegevensuitwisseling plaats vindt.

6.5.2 Een geconsolideerde markt voor digitale gegevensuitwisseling heeft positieve effecten op de publieke waarden voor burgers, bedrijven en overheid

Over de breedte van de publieke waarden is er voor burger, bedrijf en overheid positieve impact in een geconsolideerde markt. Een geconsolideerde markt zorgt ervoor dat barrières om samen te werken worden weggenomen en dat partijen die nu willen werken richting adoptie daar de ruimte voor krijgen. Het wordt gemakkelijker voor burgers en bedrijven om gebruik te maken van dienstverlening. Ook zijn publieke waarden zoals (cyber)veiligheid veel beter te organiseren in een geconsolideerde markt.

7 Overzicht conclusies

De eerder in dit rapport genoemde conclusies vatten wij hier nogmaals samen. Per conclusie verwijst A, B of C naar het analysedeel waaruit de conclusie afkomstig is.

A	**Er lopen veel SSI experimenten in Nederland, maar het landschap is gefragmenteerd:** De diverse SSI Er is opvallend veel activiteit in het Nederlandse SSI speelveld. Veel verschillende partijen (soms in een cluster met andere partijen) experimenteren voor het faciliteren digitale gegevensuitwisseling binnen hun use cases met het gebruik van verschillende SSI principes, architecturen, infrastructuren, technologieën en diensten. Het ontbreekt alleen aan samenwerking tussen de initiatieven, wat resulteert in een gefragmenteerd landschap.
A	**Kritieke massa is (nog) niet gerealiseerd door individuele leveranciers van SSI oplossingen:** Zonder samenwerking (bijvoorbeeld om te komen tot technische standaarden en afsprakenstelsels) tussen de clusters binnen het gefragmenteerde landschap, ontstaat er geen kritieke massa voor oplossingen. In het bijzonder zijn binnen een cluster veelal de drie verschillende rollen (issuer, holder, verifier) vaak niet alle drie ingevuld. Zolang dit landschap gefragmenteerd blijft, zal het uitdagend blijven om netwerkeffecten en groei te realiseren. Dit maakt het ook moeilijk om de maatschappelijke waarde van digitale gegevensuitwisseling ten volle te benutten.
A	**SSI gedachtegoed is (nog) niet volwassen genoeg voor grootschalig gebruik in de maatschappij:** De fragmentatie komt voort uit de verschillende ideeën over de beste invulling van SSI oplossingen, bijvoorbeeld op het gebied van technische inrichting en semantiek. Er is consensus in de markt dat voor een goed functionerend SSI ecosysteem, de invulling van enkele concepten nog verder onderzocht, ingevuld en geïmplementeerd moeten worden. Dit maakt dat de initiatieven momenteel nog ongeschikt zijn voor grootschalig gebruik.
A	**Beperkte beschikbaarheid brondata en beperkte herbruikbaarheid in andere domeinen vormt barrière voor waardecreatie:** Zowel overheid als private partijen bezitten brondata die waardevol is voor het optimaliseren van bedrijfsprocessen, zowel in het private als het publieke domein. Omdat brondata uit het ene domein niet zomaar gebruikt kan worden in het andere domein, is er een drempel om bedrijfsprocessen anders in te richten. De overheid kan een cruciale rol hebben door wet- en regelgeving te versnellen, en dan ook data beschikbaar te stellen.
B	**Het is onduidelijk hoe de verschillende juridische kaders zich tot elkaar (gaan) verhouden:** Voor spelers in het (SSI) speelveld is er onduidelijkheid op het gebied van wetgeving van onder andere WDO, RoG en de EU Identity Wallet (bijvoorbeeld tijdslijnen en reikwijdte van wetgeving). Deze onduidelijkheid remt de adoptie van SSI oplossingen. Partijen die nu experimenteren met SSI zullen terughoudend zijn met verdere opschaling, totdat duidelijk wordt of de ontwerpkeuzes die zij nu maken toekomstbestendig zijn en ook passen binnen de (toekomstige) geldende juridische kaders.
B	**Grote commerciële partijen kunnen sneller bewegen dan wetgevende ontwikkelingen waardoor zij de markt kunnen domineren en verstoren:** In het digitale domein beweegt de wereld snel. De ontwikkelsnelheid bij individuele organisaties is vaak hoger dan het tempo van grootschalige wetgevende veranderingen, die vaak jaren kosten om te realiseren. Grote commerciële partijen (zoals Big Techs) kunnen sneller bewegen, waardoor (wetgevende) ambities van de lidstaten worden ingehaald en overbodig worden gemaakt.
C	**'Digital agent' en 'Data bij de bron' zijn twee verschillende interactievormen die beide gefaciliteerd moeten worden:** 'Digital Agent' en 'Data bij de Bron' interactiemodellen kennen elk andere relevante use cases. Issuers en Verifiers moeten daarom begrijpen wanneer een bepaalde interactievorm wenselijk is voor de toepassing waarbinnen digitale gegevensuitwisseling plaats vindt.
C	**Een geconsolideerde markt voor digitale gegevensuitwisseling heeft positieve effecten op de publieke waarden voor burgers, bedrijven en overheid:** Over de breedte van de publieke waarden is er voor burger, bedrijf en overheid positieve impact in een geconsolideerde markt. Een geconsolideerde markt zorgt ervoor dat barrières om samen te werken worden weggenomen en dat partijen die nu willen werken richting adoptie daar de ruimte voor krijgen. Het wordt gemakkelijker voor burgers en bedrijven om gebruik te maken van dienstverlening. Ook zijn publieke waarden zoals (cyber)veiligheid veel beter te organiseren in een geconsolideerde markt.

8 Aanbevelingen

In dit hoofdstuk doen wij een aantal aanbevelingen voor vervolgactiviteiten aan opdrachtgever BZK die bijdragen aan het bereiken van de stip op de horizon 'het realiseren van maatschappelijke waarde uit digitale gegevensuitwisseling'.

8.1 Stip op de horizon: realiseren maatschappelijke waarde van digitale gegevensuitwisseling

Zoals eerder gezegd, is het hebben van een Self-Sovereign Identity en een goed functionerend SSI-landschap geen doel op zich. Het is wél een manier om burgers en bedrijven regie te geven over hun (identiteits-)gegevens zodat zij autonoom kunnen handelen in een digitale context en zelf kunnen besluiten met wie en onder welke voorwaarden zij deze (identiteits-)gegevens delen met andere partijen.

De analyse in dit rapport heeft laten zien dat de techniek en het gedachtegoed rond SSI nog niet volwassen is en dat er ook nog veel onbeantwoorde vraagstukken zijn die verder uitgekristalliseerd moeten worden voordat SSI haar beloftes ten volle waar kan maken. Dat laat onverlet dat er in digitale gegevensuitwisseling ook nu al veel (onbenutte) maatschappelijke waarde zit, waarbij het in sommige use cases zinvol is dit via een digital agent te faciliteren, terwijl het in andere use cases wenselijk of zelfs noodzakelijk kan zijn om deze gegevens rechtstreeks bij de bron op te halen (evt. met consent van de gebruiker). De Nederlandse overheid kan als aanjager een belangrijke rol spelen om deze maatschappelijke waarde uit digitale gegevensuitwisseling daadwerkelijk te realiseren.

De Nederlandse overheid en het bedrijfsleven beschikken over tal van geverifieerde brongegevens over haar burgers en klanten, die wanneer deze gegevens herbruikbaar zouden zijn binnen de business processen van de overheid, en mogelijk ook het private domein processen efficiënt, uitlegbaar, gebruiksvriendelijk, transparant, betrouwbaar en schaalbaar kunnen maken en waarbij privacy en veiligheid geborgd zijn. Idealiter ontstaat er een geconsolideerde markt waarin het voor leveranciers aantrekkelijk is om interoperablele producten, diensten en onderliggende infrastructuur voor digitale gegevensuitwisseling te leveren. Dit vraagt om een infrastructuur die open en beschikbaar is voor gebruik door bedrijfsleven, overheid en burgers. En waarbij producten en diensten van verschillende leveranciers interoperabel zijn, waardoor de burgers en bedrijven geen lock-in ervaren.

8.2 Aanbevelingen

Als de overheid de beloftes van digitale gegevensuitwisseling wil waarmaken en een positieve impact op publieke waarden wil realiseren, adviseren wij de volgende concrete vervolgactiviteiten die we in de volgende paragrafen verder zullen uitwerken:

1. **Stel geïntegreerde visie op voor het Nederlandse landschap van digitale identiteit en gegevensuitwisseling en koppel dat aan een ambitieuze uitvoeringsagenda**
   Ontwikkel een breed gedragen visie op de gewenste rol van SSI in het bredere landschap van digitale identiteit en digitale gegevensuitwisseling, rekening houdend met Europese ontwikkelingen rondom de EU Digital Identity Wallet. Zorg daarnaast voor een ambitieuze uitvoeringsagenda zodat gebruikers, private en publieke partijen op de kortst mogelijke termijn daadwerkelijk de maatschappelijke waarde van digitale gegevensuitwisseling kunnen realiseren.

2. **Stuur op consolidatie van het speelveld rond digitale gegevensuitwisseling via een Publiek Private Samenwerking**
   Breng de kennis en expertise van de 90+ partijen die al experimenteren met SSI bij elkaar en werk toe naar een geharmoniseerd en interoperabel speelveld voor digitale gegevensuitwisseling dat klaar is voor verdere opschaling. Deze *best practices* zullen via deze publiek private samenwerking ook hun weg moeten vinden naar de gremia die in Europa werken aan de verdere detaillering van de EU Digital Identity wallet.
3. **Doorbreek als overheid het kip-ei probleem voor digitale gegevensuitwisseling door als 'first mover' zelf pro-actief brondata aan te bieden en te consumeren**
   Start met het beschikbaar stellen van brondata via 'digital agents' en/of 'data bij de bron' interactiemodellen, en gebruik brondata voor validatie binnen en en optimalisatie van eigen bedrijfsprocessen. Dit om de realisatie van de maatschappelijke waarde van digitale gegevensuitwisseling voor de Nederlandse economie op gang te brengen.

8.2.1 Stel snel een geïntegreerde visie op voor het Nederlandse landschap van digitale identiteit en gegevensuitwisseling en koppel dat aan een ambitieuze uitvoeringsagenda

Zoals in paragraaf 0 is beschreven, is een van de belangrijkste barrières om de maatschappelijke waarde van digitale gegevensuitwisseling te kunnen realiseren volgens marktpartijen het ontbreken van een duidelijke, eenduidige en breed gedragen visie van de overheid op Self-Sovereign Identity. In de in februari 2021 gepubliceerde visie over digitale identiteit onderschrijft staatssecretaris Knops weliswaar het belang van een betrouwbare identiteit voor het faciliteren van digitale gegevensuitwisseling, maar deze visiebrief is nog niet duidelijk over de rol van Self-Sovereign Identity en hoe dat past binnen de (toekomstige) (inter-)nationale juridische kaders voor digitale identiteit en digitale gegevensuitwisseling.

De recente ontwikkelingen in Europa, waar de Europese Commissie serieus vaart maakt met de uitwerking van een vernieuwde eIDAS verordening die sterk leunt op een SSI-achtig digital agent model voor digitale gegevensuitwisseling (ook wel: de EU Digital Identity wallet) dwingen de Nederlandse overheid om juist nú op dat onderwerp kleur te bekennen, of anders te volgen wat in de rest van Europa voor ons bepaald zal worden. Dit vraagt ook politieke urgentie op dit onderwerp, iets wat volgens marktpartijen ontbreekt getuige het feit dat de relevante juridische kaders rondom digitale identiteit en digitale gegevensuitwisseling al jaren in ontwikkeling zijn.

Een visiedocument en politieke urgentie alleen zijn niet voldoende om de maatschappelijke waarde uit digitale gegevensuitwisseling te kunnen realiseren. Dit heeft pas meerwaarde wanneer dit gecombineerd wordt met een ambitieuze uitvoeringsagenda die niet alleen beschrijft 'waar we heen willen' maar ook 'hoe we daar komen', 'wanneer' en 'met wie'. Dit vergt een gecoördineerde effort, zodat gebruikers, private en publieke partijen op de kortst mogelijke termijn daadwerkelijk de maatschappelijke waarde van digitale gegevensuitwisseling kunnen realiseren.

Als beleidsverantwoordelijke op de onderwerpen digitale identiteit en digitale gegevensuitwisseling adviseren we BZK om als onderdeel van die uitvoeringsagenda nadrukkelijk een coördinerende rol op te pakken binnen de verschillende geledingen van de Nederlandse overheid. Anders dan bij de verschillende (gefragmenteerde) SSI experimenten die nu ontstaan binnen de Nederlandse overheid, zou een gecoördineerde overheids-brede aanpak actief kunnen bijdragen aan verdere consolidatie en harmonisatie van de markt, wat van belang is om publieke waarden voor burgers, bedrijven en overheid maximaal te kunnen borgen.

8.2.2 Stuur op consolidatie van het speelveld rond digitale gegevensuitwisseling via Publiek Private Samenwerking

Zoals in paragraaf 6.5.2 is omschreven, heeft consolidatie van de markt voor digitale gegevensuitwisseling een positief effect op publieke waarden voor zowel burgers, bedrijven en overheid. Om te komen tot deze consolidatie en zo de gewenste netwerkeffecten te kunnen creëren, adviseren wij aan BZK om een Publiek Private Samenwerking (PPS) te organiseren, en daar zelf ook actief aan deel te nemen.

Zoals we in deze speelveldanalyse hebben kunnen zien is er al ongelofelijk veel activiteit op het gebied van Self-Sovereign Identity en digitale gegevensuitwisseling. Meer dan 90 partijen voeren in Nederland experimenten uit of zijn bezig dienstverlening te ontwikkelen en deze verder op te schalen. Deze partijen hebben vaak los elkaar al ongelofelijk veel kennis en expertise opgebouwd die relevant is om te komen tot breed gedragen best practices. Deze best practices die uit deze publiek private samenwerking voort komen, zullen ook hun weg moeten vinden naar de diverse gremia die in Europa werken aan de verdere detaillering van de EU Digital Identity wallet.

We adviseren om bij het opzetten van een publiek private samenwerking vooraf duidelijke doelstellingen te formuleren, en heldere afspraken te maken over hoe de overheid de resultaten van deze samenwerking gaat toepassen in de Nederlandse maatschappij. Ook kan dit ervoor zorgen dat deze PPS niet slechts een ‘praatgroep’ wordt. Dit vergt actieve coördinatie en gedegen stakeholdermanagement, omdat de verschillende deelnemende publieke en private partijen ieder vanuit een andere insteek en met andere (soms tegenstrijdige) belangen meedoen.

Om te komen tot breed gedragen en oplossingen is het van belang een open en inclusieve samenstelling van de publiek private samenwerking na te streven. Niet alleen (toekomstige) gegevensverbruikers (Verifiers) en uitgevers van gegevens (Issuers) moeten betrokken zijn, maar ook de SSI Leveranciers zouden een plek moeten hebben in een dergelijke samenwerking.

Een mooi voorbeeld van een succesvolle PPS op het gebied van SSI is het H2020 NGI eSSIF-Lab programma[41]. Hierin worden deelnemers gemotiveerd met een gedeeltelijke subsidie (“subgrant”) om SSI implementaties te bouwen (bijv. open source) en SSI technologie nuttig in te zetten in domein-specifieke use cases. Deze programma inrichting heeft als belangrijkste voordelen laagdrempeligheid en flexibiliteit in een snelbewegende markt.

[41] Zie ook https://essif-lab.eu/

Een PPS kan diverse resultaten opleveren. Allereerst wordt er natuurlijk gezamenlijk gewerkt aan het volwassener worden van de verschillende initiatieven rondom digitale gegevensuitwisseling. Daarnaast is er ruimte om nieuwe concepten nader te onderzoeken en, indien gewenst, op de juiste manier te implementeren. Concreet kan dit ertoe leiden dat er een open, geharmoniseerd, breed gedragen en interoperabel speelveld voor digitale gegevensuitwisseling ontstaat, dat klaar is voor verdere opschaling. Een overzicht van onderwerpen die een PPS kan uitwerken zijn omschreven in de appendix 9.4.

8.2.3 Doorbreek als overheid het kip-ei probleem voor digitale gegevensuitwisseling door als 'first mover' zelf pro-actief brondata aan te bieden en te consumeren

Start met het beschikbaar stellen van brondata via 'digital agents' en/of 'data bij de bron' interactiemodellen, en gebruik brondata voor validatie binnen en optimalisatie van eigen bedrijfsprocessen. Dit om de realisatie van de maatschappelijke waarde van digitale gegevensuitwisseling voor de Nederlandse economie op gang te brengen.

Zoals in paragraaf 4.3.4 beschreven, is de adoptie van SSI initiatieven in Nederland nog beperkt. Dit is deels toe te schrijven aan de experimentele fase waarin deze initiatieven zich bevinden, maar vooral ook door een ingewikkelde adoptiedynamiek tussen Issuers, Holders en Verifiers. Het invullen van een van deze rollen wordt pas waardevoller als er ook een bepaalde kritische massa van andere rollen aanwezig is in het speelveld, het zogenoemde netwerkeffect. In paragraaf 4.4.4 schetsen we, dat het succes van digitale gegevensuitwisseling in een Issuer, Holder, Verifier landschap sterk afhankelijk is van de beschikbaarheid van geverifieerde data.

De overheid heeft bijvoorbeeld in de vorm van diverse basisregistraties beschikking over zeer diverse datasets over burgers en bedrijven. Wanneer de overheid als first-mover deze binnen de geldende juridische kaders gekwalificeerde data beschikbaar stelt (zowel via digital agents als bij de bron, afhankelijk van de use case), kan het kip-ei probleem doorbroken worden en kan een netwerkeffect gecreëerd worden. Ook kan het uit om niet alleen de data zelf beschikbaar te stellen, maar ook een overzicht van de verschillende gegevens die de overheid heeft over burgers en bedrijven samen met de redenering aan de hand waarvan deze data is opgesteld. Mogelijk zijn er twee overzichten die gebruikt worden: een voor de overheid intern, en een die ook beschikbaar is voor private partijen.

De overheid zou niet alleen als *Issuer* kunnen optreden door het aanbieden van brondata, maar ook als *Verifier*, door het consumeren en valideren van gekwalificeerde brondata. Aan de andere kant consumeert de overheid ook data. Niet alleen uit eigen bron, maar typisch ook van private partijen. Ook hiervan kan een overzicht gemaakt worden: bijvoorbeeld welk type data benodigd is binnen overheidsprocessen, welke partijen dit kunnen aanleveren en welke *assurance* wordt gevraagd. Dit maakt het mogelijk dat private partijen ook brondata kunnen aanleveren op de manier dat de overheid dit kan verwerken, en versterkt het netwerkeffect.

Om te voorkomen dat data zonder duidelijke afzetmarkt beschikbaar wordt gesteld, of dat de overheid data wil gebruiken die niet beschikbaar is, is het wenselijk om te starten met enkele gebruikssituaties waar de overheid tegelijk uitgever en gebruiker van de data is. Dat

wil zeggen, start met use cases waar de overheid zelf een databehoefte heeft en waarin (een ander deel van) de overheid ook kan voorzien in de data. Aanvullend kunnen ook private partijen als Issuer of Verifier betrokken worden om zo de publiek-private samenwerking te stimuleren. Een voorbeeld kan bijvoorbeeld de overheid zijn die VOG-credentials uitgeeft waar private partijen gebruik van kunnen maken.

Concrete resultaten van deze vervolgstappen zijn burgers die daadwerkelijk kunnen digitaal regie kunnen voeren over hun gegevens in cont met de overheid, zowel via digital agents als bij de bron. Daarnaast zijn data beschikbaar en herbruikbaar in andere domeinen, zoals financiële organisaties, binnen de huidige juridische kaders.

8.3 Overige suggesties voor vervolgactiviteiten

Bovenop de aanbevelingen uit paragraaf 8.2 doen wij nog enkele aanvullende suggesties voor vervolgactiviteiten die bij kunnen dragen aan het realiseren van maatschappelijke waarde uit digitale gegevensuitwisseling:

1. **Drijfverenanalyse**
   Analyseer de drijfveren/incentives van betrokkenen in digitale gegevensuitwisseling, zodat mogelijk beleid marktwerking kan stimuleren (de markt in plaats van de overheid actief in behoefte van burger en bedrijf laten voorzien)
2. **Studie interactiemodellen**
   Voer een studie uit naar behoeftes in verschillende use cases voor digitale gegevensuitwisseling, en daarmee voorkeuren voor interactiemodellen (digital agents of data bij de bron en specifieke keuzes daarbinnen)
3. **Maatschappelijke kosten-baten analyse**
   Maak met behulp van een maatschappelijke kosten- en batenanalyse tastbaar wat de benefits van een geconsolideerde markt voor digitale identiteit en digitale gegevensuitwisseling zouden zijn, om zo beleidskeuzes op dit onderwerp beter te kunnen onderbouwen.

8.3.1 Drijfverenanalyse

Verschillende partijen kiezen verschillende manieren om digitale gegevensuitwisseling op in te richten. (denk aan: zuiver SSI, alle principes van Allen of Sovrin volgens de letter volgen, open source ja of nee etc) In dit rapport is een eerste analyse gedaan op de verschillende manieren naar die inrichting en laten we zien dat hier een grote diversiteit in is. Wij hebben geen analyse gedaan naar de motivatie achter die inrichtingskeuze. Een drijfverenanalyse helpt inzicht te krijgen in de onderliggende beweegredenen van partijen in het SSI Speelveld. Dit kan antwoorden geven waarom digitale gegevensuitwisseling (nog) niet grootschalig is uitgerold, binnen Nederland maar ook internationaal. Ook kan de overheid, wanneer drijfveren bekend zijn, juist met beleid zoveel mogelijk vrije marktwerking stimuleren (partijen niet direct forceren activiteiten te ontplooien in het speelveld, maar motiveren om vrijwillig stappen te zetten door drijfveren aan te spreken).

Om de motivatie van verschillende partijen in kaart te brengen, adviseren we om een drijfverenanalyse uit te voeren. Hierbij worden verschillende invalshoeken voor gebruik en aanbod van diensten in het speelveld tegen elkaar afgewogen. Het traditionele businessmodel (waarbij de verifier betaalt), de machtsongelijkheid tussen verifier en holder, het probleem van moral hazard bij verifiers en holders (nadelen van slechte datakwaliteit

worden afgewenteld op holders en geven de verifier minder incentive om hogere kwaliteit te eisen) en de productaansprakelijkheid van issuers.
Typische vragen die beantwoord zouden kunnen worden zijn:

- Wat zijn drijfveren voor partijen binnen het Nederlandse speelveld om een bepaalde rol daarin te vervullen?
- Hoe beïnvloeden deze verschillende drijfveren de dynamiek in het speelveld?
- Welke belemmeringen levert deze beïnvloeding op waardoor de Nederlandse maatschappij niet snel de voordelen ten volle kan benutten?
- Hoe kunnen die belemmeringen verminderd worden?

Resultaten van een drijfverenanalyse levert inzichten op over het gedrag dat partijen mogelijk vertonen onder verschillende voorwaarden. Deze inzichten helpen te begrijpen hoe partijen gemotiveerd kunnen worden om bepaalde activiteiten uit te voeren, welke drijfveren eventueel conflicterend gedrag veroorzaken en hoe een partij als de overheid bijvoorbeeld gewenst gedrag kan stimuleren ten bate van de Nederlandse samenleving.

8.3.2 Studie interactiemodellen

Zoals in paragraaf 6.5.1 is beschreven, zijn zowel digitale gegevensuitwisseling via een digital agent als bij de bron relevante manieren om data te delen. Welke manier het meest geschikt is, hangt af van de specifieke context. In de onderzoeksopdracht was nu geen ruimte om uit te zoeken welke wijze van gegevensuitwisseling binnen de welk type use case het meest relevant is.

Om meer duidelijkheid te krijgen bij welk type use cases welke manier van gegevensuitwisseling het best past, adviseren we om een studie uit te voeren naar de verschillende use cases voor gegevensuitwisseling, en te identificeren wat voor soort interactiemodel in bepaalde situaties gewenst is bijvoorbeeld door te kijken naar hoe publieke waarden geborgd kunnen worden. Aangezien digitale gegevensuitwisseling via ‘digital agents’ en ‘data bij de bron’ beiden naast elkaar kunnen bestaan, wil je weten wanneer welk interactiemodel of combinatie van interactiemodellen gewenst is. In deze studie kunnen parameters zoals recurring access, toegang zonder consent, noodsituaties, veiligheids/opsporingsdiensten meegenomen worden, om te bepalen in welke vorm en via welk interactiemodel de overheid data beschikbaar zou moeten stellen. Dit verschilt dan ook mogelijk per type data.

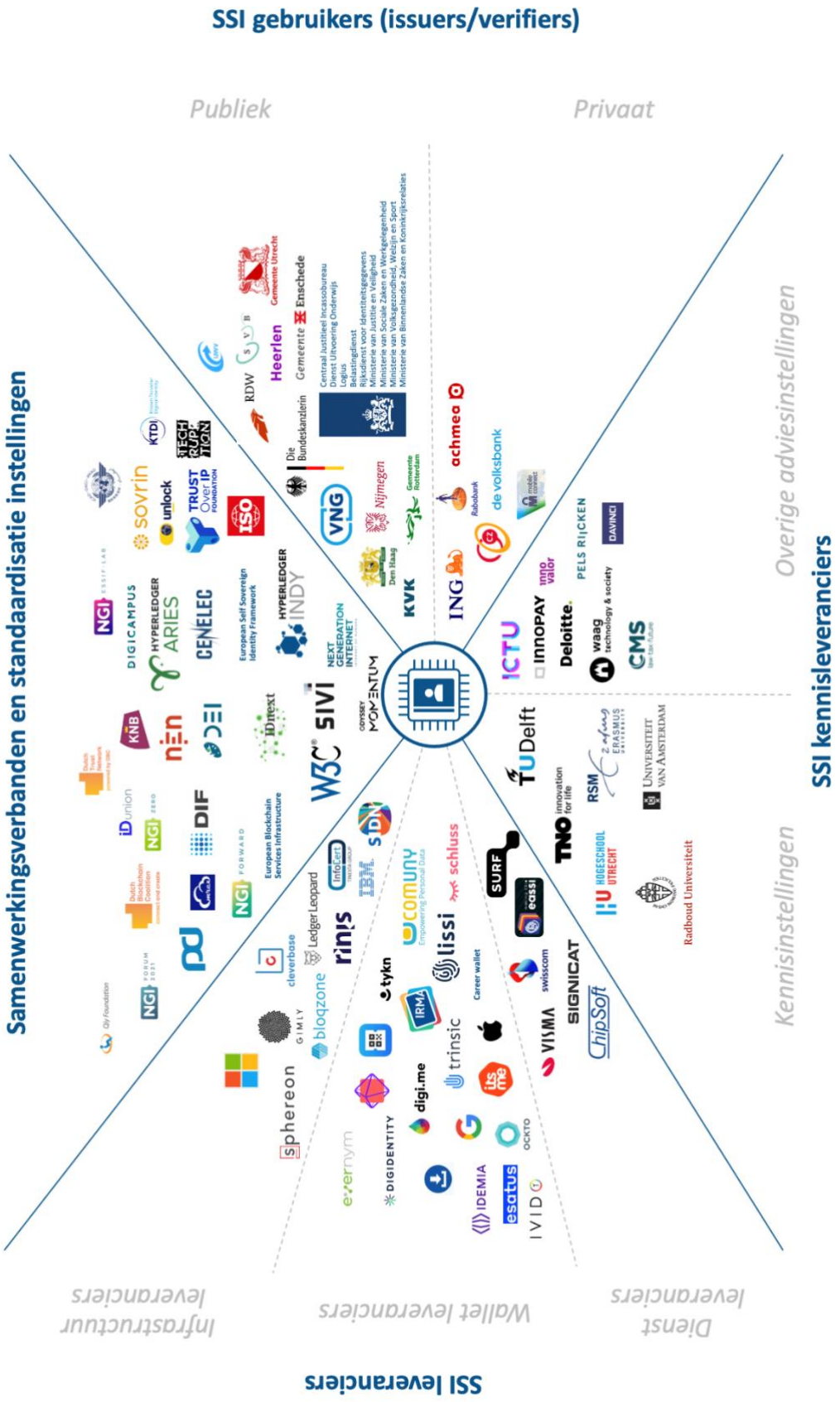
8.3.3 Maatschappelijke kosten-batenanalyse digitale identiteit en digitale gegevensuitwisseling

In deze speelveldanalyse spreken diverse partijen hoge verwachtingen uit over de financiële en maatschappelijk voordelen die we in Nederland zouden kunnen bereiken wanneer er een geconsolideerde markt voor digitale identiteit en digitale gegevensuitwisseling bestaat. Een grondige onderbouwing hiervoor ontbreekt echter.

Met behulp van een maatschappelijke kosten- en batenanalyse kan de overheid tastbaar maken wat de maatschappelijke waarde van een geconsolideerde markt voor digitale identiteit en digitale gegevensuitwisseling zou zijn, zodat zij beleidskeuzes op dit onderwerp beter kan onderbouwen.

9 Appendices

9.1 Longlist van het Nederlandse SSI speelveld



9.2 Shortlist SSI speelveld

Onderstaande partijen zijn uitgenodigd om de online vragenlijst in te vullen voor dit onderzoek.

Organisaties	
Achmea	IDEMIA
Apple	InnoValor
Bloqzone	IRMA
Bundeskanzler SSI	Itsme
Career wallet	Koninklijke Notariele Beroepsvereniging
CJIB	Ledger Leopard
Cleverbase	Microsoft
CMS	Ministerie van Volksgezondheid, Welzijn en Sport
CZ	Ockto
Deloitte	Quli
Digicampus / ICTU	Rabobank / Datakeeper
Digidentity	RvIG
Digime	Schluss
Digital Ecosystems Institute (DEI)	SIDN
DUO	Signicat
Dutch Blockchain Coalition	SIVI
Dutch Trust Network	Sphereon
Esatus AG	Stichting Rinis
Evernym	SURF
Gataca	Techruption
Gemeente Den Haag	TNO
Gimly	Trinsic
Google	TU Delft / Trustchain
HDN	Visma Connect
IBM	Volksbank
IDUnion	Zorginstituut Nederland

9.3 Analyse publieke waarden in toekomstscenario's

9.3.1 Publieke waarden in Scenario 1: 'Voor alles een app'

In het toekomstscenario 'Voor alles een app' is de markt gefragmenteerd en kunnen burgers en bedrijven data leveren aan wie ze dat willen, via een digital agent (bijvoorbeeld een wallet). Het effect hiervan op de publieke waarden is omschreven in Tabel 5.

Publieke waarden	Effect van toekomstscenario op publieke waarden	
Privacy	+	Omdat de digitale gegevensuitwisseling via agents verloopt, kunnen partijen alleen direct bij burgers/bedrijven aankloppen als zij data willen opvragen
	-	Door een veelvoud aan trust-implementaties (e.g. governance) vergroot de kans dat er ecosystemen ontstaan waarin dienstverleners minder zware privacyrichtlijnen hanteren waar burgers/bedrijven niet goed van op de hoogte zijn
(cyber)Veiligheid	+	Burgers/bedrijven krijgen dankzij agents beschikking over diensten die hen helpen bij het beschermen van hun persoonlijke gegevens

	-	Burgers zeggen over het algemeen gemakkelijk 'ja' in digitale context, omdat ze nauwelijks keuze krijgen of zo min mogelijk moeite willen doen[42]. Kwaadwillenden kunnen burgers eenvoudig bevragen/dwingen om allerlei verschillende soorten data te delen en krijgen daarmee ten onrechte beschikking over data
	-	Een gefragmenteerd landschap biedt ook ruimte aan SSI wallets waar security minder serieus genomen wordt
	?	Een gefragmenteerd landschap zorgt ervoor dat kwaadwillenden, net als Issuers en Verifiers, maar een beperkt bereik kunnen creëren met hun software implementatie
Autonomie en regie op gegevens	+	Burgers en bedrijven hebben regie op hun eigen data, bepalen zelf wanneer, met wie de data te delen.
	-	Burgers en bedrijven zijn benadeeld door fragmentatie: niet alle credentials mogen in alle wallets
Inclusiviteit	-	Er is een hoge mate van lock-in, voor bepaalde credentials of bepaalde diensten moeten steeds losse apps/accounts etc gebruikt worden. De digitaal literates kunnen hiermee uit de voeten, maar de meeste mensen snappen niet dat weer een andere app/account/agent nodig is. Dan wordt het allemaal niet makkelijker voor de mensen uit lagere sociaal economische delen van de maatschappij
	-	Het ophalen van credentials en deze beschikbaar maken in je digital agent vraagt hoge opstartmoeite van burger/bedrijf nog voordat eerste transacties uitgevoerd worden
Decentralisatie van kennis en macht	-	- In een gedecentraliseerde situatie waar overheidsinstellingen elk hun eigen SSI-achtige oplossing hebben, wordt samenwerking en uitwisseling van kennis sterk bemoeilijkt wat leidt tot minder digitale gegevensuitwisseling
Transparantie	-	In een gefragmenteerd landschap kan het per organisatie verschillen welke data zij voor vergelijkbare doeleindes willen ontvangen, voor partijen die data moeten aanleveren roept zulke inconsistentie vragen op en leidt tot wantrouwen
	-	Een veelvoud aan wallets maakt het voor burger/bedrijf complex om totaaloverzicht te bewaren over waar hun data allemaal precies gebruikt wordt
	-	Inzicht in transacties wordt bijgehouden in agents, aangezien door fragmentatie elke toepassing een eigen agent heeft is het totaaloverzicht over digitale gegevensuitwisseling ver te zoeken
Innovatie/ verdienvermogen	+	SSI Leveranciers hoeven zich niet te conformeren aan bijvoorbeeld standaarden of governance, waardoor zij alle vrijheid ervaren om met hun product te experimenteren en innoveren
	+	De grote productvrijheid en -onderscheid biedt het toekomstperspectief voor spelers in het speelveld dat zij het volgende dominante platform kunnen zijn, wat interesse en mogelijk investeringsaandacht trekt van commerciële investeerders
	+	Hoge mate van concurrentie dwingt SSI Leveranciers om te verbeteren/innoveren in dienstverlening om voorop te blijven lopen
	+	Het denkbaar dat een partij een configureerbare SSI-component maakt die de technische details van het kiezen van credential-types en protocollen 'onder de motorkap' verbergt, en toelaat dat de burger/consument maar 1 wallet nodig heeft die hij vrij mag kiezen. Een dergelijke component zou dezelfde impact voor SSI kunnen hebben als Adyen/Mollie-achtige oplossingen voor het betalingsverkeer.

[42] Vergelijk met een cookie wall: "accepteer onze cookies of ga ons instellingendoolhof in"

	-	Voor gebruikers van SSI zorgt hoge mate van fragmentatie voor verminderd bereik, wat zorgt voor de noodzaak voor meerdere implementaties tegelijk om voldoende waardevolle toepassingen te kunnen faciliteren
	-	Het verdienvermogen voor issuers is complex aangezien transacties met behulp van uitgegeven credentials buiten zicht gebeuren, mogelijk meermaals per credential. Zonder kennis van potentieel gebruiksvolume wordt het lastig om een investering te verantwoorden
Gelijke concurrentievoorwaarden	?	Afhankelijk van hoe beleid/wetgeving vormgegeven wordt, kunnen bedrijven/sectoren/domeinen elk eigen SSI producten verplicht stellen of producten verbieden waardoor het voor SSI Leveranciers moeizaam kan zijn nieuwe markten te betreden
Adequate overheidsdienstverlening	-	Wanneer de overheid gegevens beschikbaar stelt aan de burger in dienst digital agent, is het mogelijk dat dit in verschillende formats zal moeten, zodat burgers deze gegevens in een wallet naar keus kan opslaan. Dit kan ertoe leiden dat burgers een mindere kwaliteit ervaren van overheidsdienstverlening
Zorgplicht van de overheid tegenover burgers/bedrijven	-	Gegevens komen onder directe controle van burgers/bedrijven te staan. Zonder specifieke inspanning van de overheid zullen bepaalde groepen uit de maatschappij een prooi kunnen worden voor kwaadwillenden
	-	Een grote diversiteit aan dienstverleners in het speelveld maakt eventuele controle door overheid op kwaliteit van dienstverlening moeilijker
Betrouwbare overheid	?	Digital Agent implementaties van overheidsafdelingen zullen verschillen en steeds veranderen, voor partijen die op meer dan een enkele toepassing willen samenwerken met de overheid levert dit veel onzekerheid op over wat de partij kan verwachten

Tabel 5 Publieke waarden in 'Voor alles een app'

9.3.2 Publieke waarden in Scenario 2: 'Mijn agent, overal (h)erkend'

In het toekomstscenario 'Mijn agent, overal (h)erkend' is de markt geconsolideerd en kunnen burgers en bedrijven data leveren aan wie ze dat willen, via een digital agent (bijvoorbeeld een wallet). Het effect hiervan op de publieke waarden is omschreven in Tabel 6.

Publieke waarden		Effect van toekomstscenario op publieke waarden
Privacy	+	Omdat de digitale gegevensuitwisseling via agents verloopt, kunnen partijen alleen direct bij burger/bedrijf aankloppen indien zij data willen ophalen
	+	Discutabele trust-implementatie overleeft consolidatieslag niet, overgebleven SSI oplossingen bieden een hoge mate van privacy bescherming
	?	Commoditisering vergroot aantal transacties, hoeveelheid data die gedeeld wordt neemt toe
	?	In toekomst kunnen mogelijk protocollen geïmplementeerd worden om ook bij issuers en verifiers data te beschermen
(cyber)Veiligheid	+	Burgers/bedrijven krijgen dankzij agents beschikking over SSI producten die hen helpen bij het beschermen van hun persoonlijke gegevens
	-	Burgers zeggen over het algemeen gemakkelijk 'ja' in digitale context. Kwaadwillenden kunnen burgers eenvoudig bevragen/dwingen om allerlei verschillende soorten data te delen
	+	Een geconsolideerd landschap draagt bij aan grootschalige implementatiekansen van bijvoorbeeld cryptographically enforcable policies en revocation lists waarmee beter voorkomen kan worden dat data terecht komt bij partijen die hier geen beschikking over mogen hebben of onbetrouwbare data gedeeld wordt

	+	De verschillende wallets wie binnen het ecosysteem gebruikt worden, zijn allen gecertificeerd en voldoen aan een hoge mate van security specificaties
Autonomie en regie op gegevens	+	Burgers en bedrijven hebben regie op hun eigen data, bepalen zelf wanneer, met wie de data te delen
	+	Gegevens zijn herbruikbaar in verschillende domeinen omdat meer issuers/verifiers die met data kunnen omgaan
Inclusiviteit	+	Burgers, bedrijven en overheden ervaren een lage mate van lock-in
	+	Ook is het mogelijk dat partijen die het zelf niet kunnen, of niet mogen, deel uit maken van het digitale ecosysteem, wanneer guardianship / mandatering / delegeren goed wordt geïmplementeerd
	-	- Het ophalen van credentials en deze beschikbaar maken in je digital agent vraagt hoge opstartmoeite van burger/bedrijf nog voordat eerste transacties uitgevoerd worden
Decentralisatie van kennis en macht	+	Een decentrale aanpak is mogelijk met voldoende bereik (richting burgers, bedrijven en overheid) en effectiviteit (realisatie van digitale gegevensuitwisseling)
Transparantie	+	Via agent is inzichtelijk voor elke transactie welke gegevens gedeeld worden
Innovatie/ verdienvermogen	+	Prijzen per transactie zullen dalen vanwege commoditisering van SSI. Dit verbetert het verdienvermogen voor gebruikers, en leidt tot laagdrempelige optimalisatie van bijv. admin processen
	-	Het onderscheidend vermogen voor SSI Leveranciers staat onder druk wat het verdienvermogen kan verminderen
	-	Het verdienvermogen voor issuers is complex aangezien transacties met behulp van uitgegeven credentials buiten zicht gebeuren, mogelijk meermaals per credential. Dit maakt het lastig om een prijs op dienstverlening te zetten
Gelijke concurrentievoorwaarden	+	Consolidatie op standaarden, governance etc. maken de spelregels voor partijen om in te stappen in een markt heel helder, dit creëert een level playing field
Adequate overheidsdienstverlening	+	Burgers/bedrijven kunnen met eigen voorkeursproducten interacteren met overheid en krijgen geen aanvullende (betaalde) diensten opgelegd
	+	Overheid kan eigen admin/besluitvormingsprocessen voor burgers/bedrijven sterk optimaliseren op basis van SSI, er is minder noodzaak om als overheid intern verscheidenheid aan database integraties aan te leggen
Zorgplicht van de overheid tegenover burgers/bedrijven	-	Gegevens komen onder directe controle van burgers/bedrijven te staan. Zonder specifieke inspanning van de overheid zullen bepaalde groepen uit de maatschappij een prooi kunnen worden voor kwaadwillenden
	?	Partijen/overheid kunnen gevoelige credentials op een dusdanige manier uitgeven dat zij alleen door goedgekeurde partijen inzichtelijk kunnen worden gemaakt (Cryptographically enforceable policies)
Betrouwbare overheid	+	Doordat burger en bedrijf op een eenduidige manier digitale gegevensuitwisseling met de overheid kunnen doen, wordt de overheid consistenter en voorspelbaarder

Tabel 6 Publieke waarden in 'Mijn agent, overal (h)erkend'

9.3.3 Publieke waarden in Scenario 3: 'Mijn bron, mijn regels'

In het toekomstscenario 'Wilde westen' is de markt gefragmenteerd en wordt data direct opgehaald bij de bron, mogelijk zonder tussenkomst van burgers en bedrijven (eenmalig of doorlopend, maar altijd met consent). Het effect hiervan op de publieke waarden is omschreven in Tabel 7.

Publieke waarden		Effect van toekomstscenario op publieke waarden
Privacy	-	Partijen kunnen direct bij de bron aankloppen, voor data flows waar de Issuer geen authenticatie van de betreffende persoon doet neemt het risico dat onterecht data gedeeld wordt toe
	-	Burgers betalen niet voor het faciliteren van 'data bij de bron', in de praktijk leidt dit tot betalen met je data
(cyber)Veiligheid	-	Niet elke issuing databron hanteert zelfde security standaarden en slecht beveiligde databases kunnen datalekken veroorzaken
Autonomie en regie op gegevens	-	De versplintering van gegevens, verdeeld over bronnen met eigen authenticatie, maakt overzicht en effectief voeren van regie erg complex voor burger/bedrijf
	-	Afhankelijkheid van databron die gegevens vrij geeft is nadelig voor zelfstandigheid en zelfbeschikking van burgers op hun gegevens indien databron offline is
Inclusiviteit	+	Data bij de bron verlegt implementatiemoeite weg van burger/bedrijf naar partijen met veel brondata, dit maakt het erg laagdrempelig om mee te kunnen doen in een data ecosysteem
	-	Hoge concurrentie leidt tot 'gratis' dienstverlening richting burger/bedrijf. Vaak betekent dit een verborgen verdienmodel op data, gebruikers moeten dus met data betalen of kunnen niet meedoen
Decentralisatie van kennis en macht	?	In een sterk gefragmenteerd landschap is decentralisatie van onder andere kennis en macht bereikt, het is echter onduidelijk of dit als positief of negatief ervaren kan worden aangezien decentralisatie niet per se een doel op zich is
Transparantie	+	Data ophalen bij de bron geeft voor een Verifier het meest directe gevoel van zekerheid over de correctheid van data
	-	In een gefragmenteerd landschap kan het per organisatie verschillen welke data zij voor bepaalde doeleindes willen ontvangen. Onduidelijk waarom bepaalde informatie ergens nodig voor is
	-	Een veelvoud aan databronnen maakt het voor burger/bedrijf complex om totaaloverzicht te bewaren waar hun data allemaal precies gebruikt wordt
	?	Veel transacties vinden plaats tussen issuer en verifier. De partij over wie de data gaat moet er dan maar op vertrouwen dat daadwerkelijk niet meer gedeeld wordt dan eventueel aan hen inzichtelijk is gemaakt
Innovatie/ verdienvermogen	+	Elke leverancier van 'Data bij de Bron' oplossingen heeft volle vrijheid met inrichting van het product, er is volop ruimte om te innoveren op productgebied zonder rekening te houden met geldende industrie standaarden
	+	Grote productvrijheid en -onderscheid biedt het toekomstperspectief voor spelers in het speelveld dat zij het volgende dominante platform kunnen zijn, wat interesse en mogelijk investeringsaandacht trekt
	+	Elke transactie is inzichtelijk voor issuers, elke transactie is inspanning en dit volume kan de concrete basis zijn voor verdienmodellen
	-	Voor gebruikers zorgt de hoge mate van fragmentatie voor verminderd bereik. Dit kan potentieel verdienvermogen per implementatie omlaag brengen
Gelijke concurrentievoorwaarden	+	Er is veel ruimte voor partijen om eigen implementaties/producten vorm te geven en relevante doelgroepen aan te spreken met *tailored offerings*
Adequate overheidsdienstverlening	-	De overheid vraagt (nog steeds) regelmatig naar de bekende weg, gebruikt formulieren die (volgens de ombudsman) niet handig in te vullen zijn, heeft processen waarin wachttijden optreden als gevolg van het verzamelen en valideren van voor een besluit benodigde gegevens

Zorgplicht van de overheid tegenover burgers/bedrijven	+	Indien de overheid zelf als databron optreedt, kan zij zelf nog controle houden over al dan niet delen met discutabele partijen
	-	Wanneer de overheid als issuing bron versnipperd is (credentials zijn verspreid over diverse bronnen binnen de overheid), ontstaat er bij de overheid geen eenduidig beeld welke informatie verstrekt is of kan worden aan burger en bedrijf waardoor zij deze niet optimaal van dienst kunnen zijn
Betrouwbare overheid	?	In dit scenario is het niet voorspelbaar met welke technologie de verschillende overheden gaan werken. Waarschijnlijk wordt dit een lappendeken van technologieën die per overheid verschillen en niet interoperabel zijn

Tabel 7 Publieke waarden in 'Mijn bron, mijn regels'

9.3.4 Publieke waarden in Scenario 4: 'API economy'

In het toekomstscenario 'API economy' is de markt geconsolideerd en wordt data direct opgehaald bij de bron, mogelijk zonder tussenkomst van burgers en bedrijven (eenmalig of doorlopend, maar altijd met consent). Het effect hiervan op de publieke waarden is omschreven in Tabel 8.

Publieke waarden		Effect van toekomstscenario op publieke waarden
Privacy	+	Enkele betrouwbare merken dragen verantwoordelijkheid voor hun klanten (burgers/bedrijven). Een partij kan als 'betrouwbaar' worden gezien wanneer deze de klant goed informeert over welke data voor welk doel wordt gedeeld en de privacy van de klant waarborgt.
	-	Partijen kunnen direct bij de bron aankloppen, voor data flows waar de Issuer geen authenticatie van de betreffende persoon doet neemt het risico dat onterecht data gedeeld wordt toe
	-	Issuers kunnen in principe inzage hebben in frequentie van transactieverkeer, of zelfs in totaal transactiegedrag wanneer logs niet met bepaalde encryptie bewaard worden
(cyber)Veiligheid	+	De partijen hanteren hoge kwaliteit security standaarden in hun issuing rol om hun goede naam te beschermen
	+	Consolidatie vergroot de kans dat burgers/bedrijven gemakkelijk van hoog LoA authenticatie gebruik kunnen maken voor diverse toepassingen
	+	'Data bij de Bron' producten voor burger/bedrijf dragen zorg voor hun klanten en zorgen dat zij zich steeds bewust zijn van de data die ze op het punt staan ter beschikking te stellen
	-	Het ontstaan van enkele grote databases leidt tot aantrekkelijke hackersdoelwitten
Autonomie en regie op gegevens	+	Burgers/bedrijven zijn in staat om bij enkele partijen het overzicht te bewaren/inzien/bewerken van de gegevens die over hen beheerd worden
	-	Burgers en bedrijven zijn afhankelijk van databronnen die gegevens vrijgeven over hen, dit is nadelig voor zelfstandigheid en zelfbeschikking indien databron offline is of niet 24/7 beschikbaar is
Inclusiviteit	+	Data bij de bron verlegt implementatiemoeite weg van burger/bedrijf naar partijen met veel brondata, dit maakt het erg laagdrempelig om mee te kunnen doen in een data ecosysteem
	+	Burgers en bedrijven ervaren een lage mate van lock-in, dit betekent veel keuzevrijheid en men kan onderdeel van het systeem zijn met producten die bij de eigen voorkeur passen
Decentralisatie van kennis en macht	-	Het ontstaan van enkele grote betrouwbare merken leidt mogelijk tot gecentraliseerde kennis/macht

	+	Consolidatie in het landschap maakt een decentrale aanpak waarbij voldoende bereik en effectiviteit aanwezig is mogelijk
Transparantie	+	Data ophalen bij de bron geeft voor een Verifier het meest directe gevoel van zekerheid over de correctheid van data
	?	Veel transacties vinden plaats tussen issuer en verifier. De partij over wie de data gaat moet er dan maar op vertrouwen dat daadwerkelijk niet meer gedeeld wordt dan eventueel aan hen inzichtelijk is gemaakt
	?	Gebruiksgemak kan ontstaan door bijvoorbeeld voor-ingestelde consent, waardoor een deel van transacties zonder wetenschap van burger/bedrijf gaan plaatsvinden
Innovatie/ verdienvermogen	+	Elke transactie is inzichtelijk voor issuers, elke transactie is inspanning en dit volume kan de concrete basis zijn voor verdienmodellen
	+	Hoge mate van consolidatie maakt het voor verifiers met één of enkele implementaties mogelijk om een groot bereik te realiseren, verdienvermogen per implementatie neemt toe
	+	Burgers zijn in dit scenario bereid om te betalen voor betrouwbare merken (kleine selectie verifiers die data ophalen voor dienstverlening), om zo verdienmodellen op (persoonlijke) data te voorkomen
	-	Hoge mate van consolidatie en standaardisatie beperkt het onderscheidend vermogen voor leveranciers
	-	Betrouwbare merken zullen zich meer risicomijdend opstellen wat over het algemeen innoverend vermogen beperkt
Gelijke concurrentievoorwaarden	-	Het ontstaan van enkele grote betrouwbare merken maakt het in de praktijk lastig voor nieuwe partijen om daartussen te komen
Adequate overheidsdienstverlening	+	Met de juiste koppelingen tussen databases en oplossingen kan de overheid zonder tussenkomst van burger gegevens ophalen (geen noodzaak om te vragen naar data die al binnen de overheid bekend is)
Zorgplicht van de overheid tegenover burgers/bedrijven	+	Bij de bron kan controle worden uitgevoerd over de rechtmatigheid van uitgifte van gegevens over burgers/bedrijven.
Betrouwbare overheid	+	Consistentie in het ontsluiten van gegevens vanuit het overheidsdomein maakt het voor dienstverleners voorspelbaar om diensten te ontwerpen en ontwikkelen

Tabel 8 Publieke waarden in 'API economy'

9.4 Mogelijke onderwerpen voor een publiek-private samenwerking

Deze bijlage bevat een overzicht van mogelijke onderwerpen welke binnen een publiek-private samenwerking opgepakt kunnen worden. Deze onderwerpen zijn suggesties, en werden ofwel door één partij genoemd in de vragenlijst, ofwel zijn onderwerpen die INNOPAY/ TNO uit andere trajecten identificeren als belangrijk om nader te onderzoeken.

Inrichting infrastructuur voor digitale gegevensuitwisseling

Om tot een netwerkeffect te komen rondom digitale gegevensuitwisseling, is het nodig dat de onderliggende infrastructuur hier de mogelijkheden toe biedt. Hiervoor is het van belang dat dusdanig gestandaardiseerd is, dat partijen hiermee kunnen werken, en hun eigen producten/diensten kunnen aanbieden op deze infrastructuur. Binnen een PPS kan een dergelijke infrastructuur opgebouwd worden, nadat onderzocht is wat ermee gedaan moet worden, wie wat zal gebruiken, wie wat kan leveren en hoe dit gestandaardiseerd dient te worden.

Invulformulieren
Een belangrijk onderdeel van digitale gegevensuitwisseling is het invullen van digitale invulformulieren. Contact tussen burger en partij waar deze burger een dienst wil afnemen, verloopt veelal via een dergelijk formulier. Wanneer “digitale gegevensuitwisseling 2.0”, dat wil zeggen zoals wij het voor ons zien, in de praktijk wordt toegepast, dienen de huidige invulformulieren geüpdatet te worden. Een belangrijk onderdeel hiervan is niet alleen het mogelijk maken dat een formulier wordt ingevuld met behulp van “digital agent” of “data bij de bron”, maar dat ook de besluitvorming daarbij wordt geëvalueerd en verwerking daarvan.

Wet- en regelgeving
Wanneer over wordt gegaan naar een andere wijze van digitale gegevensuitwisseling, is het van belang dat dit wel voldoet aan (toekomstige) wet- en regelgeving. Het is voor burger, bedrijf en overheid niet alleen van belang om de juridische regelgeving te volgen, maar ook specifiek beleid van organisaties zelf. Daartoe dient bijvoorbeeld in kaart gebracht te worden op basis van welke regelgeving bepaalde bedrijfsprocessen verlopen en hoe deze processen zouden kunnen veranderen door gebruik van “digital agent” of “data bij de bron”.

Afsprakenstelsels
Een ander belangrijk punt om uit te werken in een publiek-private samenwerking zijn de afsprakenstelsels tussen overheid en bedrijfsleven, maar ook tussen verschillende private partijen onderling. Afsprakenstelsels gaan in op zaken als de balans tussen het collaboratief-competitief domein, aansprakelijkheid, gebruiksvoorwaarden, vastleggen van keuzes voor het gebruik van standaarden voor interoperabiliteit, beheer van infrastructuur en het waarborgen van het gelijke speelveld.

Concepten om verder uit te werken
Als laatste geven wij twee overzichten van verschillende concepten die nog verder uitgewerkt kunnen worden binnen een dergelijke publiek-private samenwerking. In Tabel 9 Overzicht van onderzoeksonderwerpen is een overzicht van deze concepten en wat wij daarmee bedoelen, in Tabel 10 wordt aangegeven hoe deze concepten bijdragen aan de publieke waarden zoals omschreven in Paragraaf 6.2. Deze bijdrage aan de publieke waarden is op basis van een inschatting door de auteurs gemaakt, deze inschatting is geen resultaat van enquêtes of impactanalyse op publieke waarden zoals uitgevoerd in deze SSI Speelveldanalyse.

Onderwerp	Omschrijving
Issuen van credentials	Het uitgeven van data, mogelijk via “digital agent” of “bij de bron”, over alle gegevens betreffende klanten, burgers, bedrijven, etc. Dit hangt samen met recht op inzage zoals omschreven in de GDPR
Purpose-binding	Wanneer een partij gegevens opvraagt (in presentation requests) moet het aannemelijk zijn dat deze gegevens voor een bepaald doel gebruikt worden. Ook voor presentation responses is dit van belang
Publicatie en transparantie van verifier besluitvorming	Wanneer een partij besluiten gaat nemen (in geval dat er een databehoefte bestaat voordat dienstverlening aangeboden kan worden), kan van tevoren een overzicht gegeven worden hoe deze besluitvorming gedaan zal worden, dit zorgt ook voor transparantie gedurende het proces. Opties hiervoor zijn 'credential-catalogue-alike' services (zie ook: transparantie), die het mogelijk zou kunnen

	maken voor een privacy-waakhond of consumentenorganisatie om te controleren op data minimalisatie
Verify-the-verifier'-achtige protocollen	Het is van belang dat de partij welke gevraagd wordt om data te tonen, ook de mogelijkheid heeft om na te gaan wie (en waarom) deze data opvraagt. Bovendien mag sommige data alleen gevalideerd worden door bepaalde partijen, dit kan (cryptografisch) ingeregeld worden. Daarnaast kunnen neutrale organisaties als de Consumentenbond die bijbehorende policies onderhouden om te voorkomen dat issuers op een oneigenlijke manier beperken waar credentials gebruikt kunnen worden.
Type-certificatie van wallets	Type-certificatie is het formeel vaststellen, door een daartoe geaccrediteerde auditor, dat alle producten van één soort voldoen aan een vastgestelde verzameling eisen, en de productie van die producten op precies dezelfde wijze gebeurt (en voldoen aan voor de productie vastgestelde eisen). Type-certificatie van wallets is één van de onderdelen die nodig zijn om te borgen dat zulke wallets op integere wijze omgaan met de aan hun toevertrouwde gegevens; jouw IT kan vaststellen aan welke security- of andere eisen de wallet voldoet (met wie jouw IT communiceert); jouw IT op betrouwbare/baarder wijze kan vaststellen namens welke partij de wallet component acteert.
Cryptographically enforceable policies	Niet alle informatie over een partij mag zomaar met elke willekeurige andere partij gedeeld worden, denk aan de BSN van een burger. Er zijn verschillende protocollen die het mogelijk maken om deze data alleen te kunnen ontsluiten op basis van een policy die aangeeft wie wel/niet gerechtigd is om deze informatie te gebruiken.
Online/remote integrity attestation services (RIAS)	Het idee is dat een SSI component zich bij een of meer zulke services aanmeldt zodra deze wordt gedeployed en zodanige gegevens hierover bij de RIAS worden geregistreerd dat, zodra de component (later) bij de RIAS om een (kortlevend) integriteits-credential vraagt, die laatste kan detecteren of zich veranderingen in de component hebben voorgedaan die diens integriteit aantasten, en zo niet, het gevraagde credential aanleveren.
(adequate) privacy-preserving revocation	Wanneer een partij bepaalde gegevens valideert, kan een van die controles bestaan uit het nagaan dat de informatie nog geldig is, en dat het credential niet revocated is. Dit werkt het liefst niet dmv CRLijsten of OCRProtocollen, maar wel volgens een methode die toelaat dat de verifier/validator de revocation van een credential kan controleren op het moment dat hij de gegevens eruit feitelijk gebruikt.
Type-specificatie van SSI componenten	Het gaat hierbij over het specificeren van de capabilities van een SSI component door de fabrikant/leverancier als een (in de component ingebakken) credential. Het gaat bijvoorbeeld om mogelijkheden om • de eindgebruiker te authentiseren (bijv. via vingerafdrukken, gezichtsherkenning, pin, ...), • het kunnen uitgeven van credentials die de component met een eigen sleutel ondertekent (bijv. voor het uitgeven van authenticatie-credentials waarin staat dat de eindgebruiker de eigenaar van de component is en de wijze waarop dat is vastgesteld) • via NFC paspoort of rijbewijs uit te lezen, • te communiceren (bijv. DIDCom), etc.
Type-certificatie van SSI componenten	Het gaat daarbij over certificatie van de een component tegen de (type)specificatie ervan; dat geldt vooral voor componenten die potentieel risicovolle handelingen uitvoeren, zoals het zetten van een digitale handtekening (dat gaat dan over issuer-componenenten, verifier-componenten (handtekening onder presentation requests) en wallets (handtekening onder presentaties), alsmede over componenten die 'op verzoek' een handtekening kunnen zetten.
Mechanismen voor data transformatie	Veel informatie die wel beschikbaar is behoeft een doorvertaling om operationeel bruikbaar te worden gemaakt. Twee voorbeelden: Een vonnis betreffende de onderbewindstelling van een zeker persoon, waarbij een deel van

	de bankrekeningen waarvan die persoon de houder is onder het bewind vallen, zou je bijvoorbeeld zodanig willen kunnen 'doorvertalen' dat de bewindvoerder over een credentials kan komen te beschikken die in een online sessie met de betreffende bank zonder verwijl toegang tot die rekeningen geven en de bewindvoerder in staat stellen over het geld te beschikken conform te condities van het vonnis.
Mandateren/delegeren	Het gaat hier om het verstrekken van een recht c.q. plicht tot het uitvoeren van zekere taken door een recht/plicht-hebbende aan een andere partij, die deze taken vervolgens namens de recht/plicht-hebbende (al dan niet onder eigen verantwoordelijkheid) gaat uitvoeren. Zo zou bijvoorbeeld het NHR de volgende functionaliteiten kunnen krijgen: - het registreren van mandaat/delegaat-types door (willekeurige) partijen, die daarmee aangeeft wat iemand met zo'n mandaat/delegaat bij die partij kan doen (bijv. een bankrekening inzien en/of geld overmaken), en evt. welke gegevens daarbij nodig zijn (bijv. een bankrekeningnummer); - het aanmaken van een mandaat/delegaat van een zeker type, door een (willekeurige) partij, die daarmee de benodigde taak-gegevens invult, en de identiteit van de gemandateerde/gedelegeerde partij - het uitgeven van credentials waarin zulke mandaten/delegaten zijn opgenomen, zodat iemand die gemandateerd/gedelegeerd is bij de betreffende partij (de bank bijvoorbeeld) kan laten zien dat hij gemandateerd is voor zekere taken (die de bank dus kent, want zelf gespecificeerd) door de mandaat/delegaat-gever.
Formulieren ver-SSI-en	Een van de ideeën rondom SSI is dat dit het invullen van allerlei formulieren kan vergemakkelijken. Dat betekent echter wel dat bij elk formulier een soort 'policy' moet worden opgesteld, op basis waarvan de it-verifier-component • om (specifieke gegevens uit) credentials kan vragen die met de vereiste assurances, bijv. omtrent de gegevensbron, de integriteit, etc. van de erin opgenomen gegevens; • de gegevens te controleren op validiteit voor het doel waarvoor ze worden gevraagd; • de gegevens te transformeren naar het formaat dat intern in de eigen organisatie wordt gebruikt (bijv. punten in komma's veranderen, tijdsnotaties, etc.), om daarmee het betreffende veld in het formulier in te kunnen vullen. De ontwerper van dergelijke formulieren hebben dan tools nodig waarmee ze kunnen ontdekken wie welke credentials uitgeeft, met welke assurances die komen e.d. Ook hebben ze tools nodig om de policy mee te kunnen specificeren en wel zodanig dat die policy door de SSI it (infra) componenten operationeel gebruikt kan worden.
Resultaten ver-SSI-en	Een van de ideeën rondom SSI is dat papieren die worden uitgegeven (diploma's, vergunningen, beschikkingen, enz.) ook als credential uitgegeven moeten kunnen worden. Dat houdt in dat een partij die dit doet over tools moet beschikken om • de structuur (het schema) van de credential mee vast te leggen en te documenteren • 'marketing-gegevens' erbij de geven (bijvoorbeeld of er sprake kan zijn van een liability, volgens welk (al dan niet gecertificeerd) proces de gegevens tot stand zijn gekomen, of zulke credentials wat kosten, of er revocation bij zit (en zo ja, welk smaakje), e.d.)
Privacy mechanismen	Er lijken mogelijkheden te zijn om de privacy niet alleen voor individuele burgers te verbeteren, maar ook structureel te verbeteren. Een voorbeeld zou kunnen zijn dat een verifier voor elke dienst die hij verleent publiceert op basis van welke gegevens hij dit doet. Dit is toetsbaar door de Autoriteit Persoonsgegevens. Operationeel kan bij een credential-uitvraag het doel waar de gegevens voor worden gebruikt (= een zekere dienst) worden meegestuurd, en die vraag worden vergeleken met de gepubliceerde gegevens, en als dit verschilt kan dit (bijv. bij de AP) worden gemeld en kan er actie volgen.

Tabel 9 Overzicht van onderzoeksonderwerpen

	Privacy	(Cyber)veiligheid	Autonomie en Regie op Gegevens	Inclusiviteit	Decentralisatie van kennis en macht	Transparantie	Innovatie/verdienvermogen	Gelijke concurrentievoorwaarden	Adequate overheidsdienstverlening	Zorgplicht van de overheid tov burgers/bedrijven	Betrouwbare overheid
Issuen van credentials	■		■				■				
Purpose-binding	■					■	■				
Publicatie en transparantie van verifier besluitvorming	■					■	■				■
Verify-the-verifier'-achtige protocollen	■	■					■			■	
Type-certificatie van wallets		■					■				
Cryptographically enforceable policies		■					■			■	
Online/remote integrity attestation services (RIAS)		■				■	■				
(adequate) privacy-preserving revocation		■					■		■		
Type-specificatie van SSI componenten		■	■				■				
Type-certificatie van SSI componenten		■					■	■		■	
Mechanismen voor data transformatie			■	■		■	■		■		
Mandateren/delegeren			■	■		■	■		■		
Formulieren ver-SSI-en			■			■	■				■
Resultaten ver-SSI-en			■			■	■				■
Privacy mechanismen	■		■				■				

Tabel 10 Bijdrage van onderzoeksonderwerpen aan publieke warden

9.5 Colofon

Dit onderzoek is in opdracht van BZK uitgevoerd door INNOPAY en TNO:

INNOPAY	TNO
Auteurs ▪ Christian van Ramshorst christian.vanramshorst@innopay.com ▪ Leon Kluiters	**Auteurs** ▪ Sterre den Breeijen sterre.denbreeijen@tno.nl
Reviewers ▪ Eefje van der Harst ▪ Vincent Jansen	**Reviewers** ▪ Rieks Joosten ▪ Oskar van Deventer
https://www.innopay.com/	https://www.tno.nl/

9.6 Dankwoord

Graag bedanken wij de volgende personen voor hun bijdrage aan dit rapport (in alfabetische volgorde):

- Cem Adiyaman
- Jacob Boersma
- Rein Schaafsma
- Tim Speelman
- Pieter Verhagen
- Peter Verkoulen
- Wouter Welling
- Paul Zeef