



Universiteit
Leiden
The Netherlands

Samen bouwen aan vertrouwen in technologische innovatie aan de hand van Self-Sovereign Identity (SSI)

Oers, Marcia van

Citation

Oers, M. van. (2023). *Samen bouwen aan vertrouwen in technologische innovatie aan de hand van Self-Sovereign Identity (SSI)*.

Version: Not Applicable (or Unknown)

License: [License to inclusion and publication of a Bachelor or Master Thesis, 2023](#)

Downloaded from: <https://hdl.handle.net/1887/3656369>

Note: To cite this publication please use the final published version (if applicable).



**Universiteit
Leiden**

**SAMEN BOUWEN AAN VERTROUWEN
IN TECHNOLOGISCHE INNOVATIE
AAN DE HAND VAN SELF-SOVEREIGN IDENTITY (SSI)**

MASTER MANAGEMENT VAN DE PUBLIEKE SECTOR
Strategie, Advisering en Verandermanagement

Marcia van Oers

Begeleider en eerste lezer: Prof.dr.ing. A.J. Klievink

Tweede lezer: Dr. Alex Ingrams

07 augustus 2023

Inhoudsopgave

Voorwoord	4
1 Inleiding	8
1.1 <i>Aanleiding</i>	8
1.1.1 Over SSI	8
1.1.2 Risico's in beeld en het belang van vertrouwen.....	9
1.1.3 Digitalisering en de ontwikkeling richting quadruple helix	11
1.1.4 Probleemstelling	12
1.2 <i>Onderzoeksvraag</i>	14
1.3 <i>Relevantie</i>	15
1.3.1 Wetenschappelijke relevantie	15
1.3.2 Maatschappelijke relevantie.....	16
1.4 <i>Leeswijzer</i>	19
2 Theoretisch kader	20
2.1 <i>Digitale en collaboratieve innovatie</i>	22
2.1.1 Digitale technologie door de overheid in drie fasen	22
2.1.2 Digitale innovatie en haar speelvelden	23
2.1.3 Collaboratieve innovatie	24
2.2 <i>Self-sovereign identity; een disruptieve technologie</i>	25
2.2.1 Digitale soevereiniteit	25
2.2.2 Self-sovereign Identity (SSI)	26
2.2.3 SSI: een disruptieve technologie.....	28
2.2.4 Impact van disruptie	29
2.3 <i>Governance & samenwerking</i>	29
2.3.1 New Public Management.....	29
2.3.2 Publiek-Private Samenwerking.....	30
2.3.3 Triple helix & quadruple helix samenwerking.....	30
2.3.4 Governance	31
2.3.5 New Public Governance	32
2.3.6 Collaborative governance	33
2.4 <i>Publieke waarden & ethiek</i>	35
2.5 <i>Vertrouwen, risico & vertrouwensmodellen</i>	36
2.5.1 Definities van vertrouwen.....	36
2.5.2 Soorten vertrouwen.....	38
2.5.3 Risico in relatie tot vertrouwen.....	39
2.5.4 Vertrouwensmodellen.....	40
2.5.5 Leiderschap in relatie tot vertrouwen.....	42
2.6 <i>Policy & polity</i>	43
2.6.1 De veranderende samenleving met digitale technologie als sturende kracht	43
2.6.2 Beleid en de rol van de overheid.....	44
3 Methoden	46
3.1 <i>Onderzoekstype</i>	46
3.2 <i>Onderzoeksontwerp</i>	47
3.2.1 Kwalitatieve vragenlijst	48
3.2.2 Het samenstellen van de online vragenlijst.....	48
3.3 <i>Onderzoekseenheden & selectie</i>	52

3.4	<i>Dataverzameling & data-analyse</i>	52
3.5	<i>Betrouwbaarheid & validiteit</i>	53
3.5.1	Betrouwbaarheid.....	53
3.5.2	Validiteit.....	54
4	Resultaten & analyse	55
4.1	<i>Resultaten onderzoek</i>	56
4.2	<i>Analyse</i>	68
4.2.1	Digitale & collaboratieve innovatie.....	68
4.2.2	SSI: een disruptieve technologie.....	70
4.2.3	Governance & samenwerking.....	71
4.2.4	Publieke waarden & ethiek.....	74
4.2.5	Vertrouwen, risico & vertrouwensmodellen.....	75
4.2.6	Policy & Polity.....	77
5	Conclusies, aanbevelingen & discussie	79
5.1	<i>Conclusies en aanbevelingen</i>	79
5.2	<i>Discussie</i>	86
5.2.1	Reflectie op wetenschappelijke en maatschappelijke relevantie.....	86
5.2.2	Reflectie op onderzoeksmethodiek.....	88
5.3	<i>Slotwoord</i>	90
6	Referentielijst	94
7	Bijlagen	111

Voorwoord

“Change is not a threat, it's an opportunity.

Survival is not the goal, transformative success is” – Seth Godin

Veiligheid als voorwaarde voor vrijheid

Het streven naar een zo veilig en rechtvaardig mogelijke samenleving is voor mij een belangrijke waarde. Sterker nog; veiligheid zie ik als een voorwaarde om in vrijheid te kunnen leven. Waar veiligheid in het geding komt, staat ook onze vrijheid op het spel. Dat bewees COVID-19, de pandemie die voor flink wat opschudding in de wereld gezorgd heeft.

Turbodigitalisering en digitale transformatie

De pandemie zorgde ook voor turbo-digitalisering en versnelde (digitale) transformatie. “COVID-19 heeft de digitalisering van processen in een stroomversnelling gebracht” (Van Houten, 2021). En masse bewogen we van ‘offline’ op kantoor werken naar online thuiswerken en digitale systemen werden hier met straaljagersnelheid op aangepast. Hoewel het leek alsof de wereld buiten tot stilstand kwam, veranderde er immens veel. Het gedrag van een volledige samenleving bleek bijzonder adaptief, maar zoals het een verandering beaamt, nooit zonder weerstand. En zeker ook niet altijd met vertrouwen als fundament.

Veranderen met het oog op vooruitgang

“There is nothing permanent, except change” waren ooit de woorden van de Griekse filosoof Heraclitus. Voor iemand die in de richting Strategie, Advisering en Verandermanagement afstudeert, durf ik te constateren dat ik een periode vol veranderingen - in de algemene zin van het woord - als iets moois zie. Een periode waarin iedereen; overheid, bedrijfsleven, wetenschap en burgers, wel moet contempleren over nieuwe kansen met het oog op de toekomst, met daarin een belangrijke rol voor zowel mens als technologie. En daar vooral op dient te acteren in een samenleving die continu in verandering is, *“alles stroomt”* aldus Heraclitus. Momenteel richting een ‘smart society’ met een aaneenschakeling van disruptieve innovaties en dataficering.

Openheid, eerlijkheid en vertrouwen in verbinding

Het vertrekpunt van mijn onderzoek zou je gelijk kunnen trekken aan een welbekende uitspraak van Socrates: ‘Ik weet dat ik niets weet’.

In mijn optiek leveren nieuwsgierigheid, een open blik, respect en luisteren naar alle perspectieven ‘ergens in het midden’ ruimte en informatie op waar verbinding gemaakt kan worden. Vertrouwen is daarbij een onmisbaar fundament. Ik vraag mij nog steeds dagelijks af of er een formule is, of misschien zelfs een ‘gulden middenweg’, om een toekomst te kunnen bouwen vanuit vertrouwen. Waarbij mens en technologie elkaar harmonieus versterken, zonder dat wat we in bestuurskundige termen ‘de bedoeling’ noemen, uit het oog te verliezen. En is ‘de bedoeling’ nog wel helder, zou een volgende vraag kunnen zijn. Werken aan deze thesis riep bij mij verschillende vragen op waar, zeker op voorhand, geen eenduidig antwoord op mogelijk is. Daarom kan ik oprecht zeggen dat dit thema mij zowel heeft doen versnellen als stilstaan. Want geef er maar eens antwoord op... Hoe zetten we samen, vanuit veiligheid en vertrouwen, koers naar een gezonde maatschappelijke ‘BV Nederland’ als onderdeel van ‘Holding de Aarde’, waarin een belangrijke rol voor digitale innovatie is weggelegd? Eén van die talrijke technologische innovaties is Self-Sovereign Identity (SSI), oftewel digitale identiteit, waarbij de burger de regie krijgt over eigen data. Nederland zet grote stappen richting deze ontwikkeling. Met veel kansen die processen kunnen vereenvoudigen en versnellen, maar ook veel kritische kanttekeningen vanuit burgers en de Kamer. Dat we samen vooruit willen is een gegeven. Maar hoe? En welke waarden zijn daarbij leidend?

Waar sta ik ten opzichte van SSI?

Tijdens dit onderzoek heb ik mezelf veelvuldig afgevraagd hoe ik persoonlijk sta tegenover nieuwe technologieën als SSI en waar deze toe gaan leiden. Toen ik aan deze masterstudie begon, stonden innovatie- en veranderprocessen hoog bij mij in het vaandel, veelal gekoppeld aan veiligheid. Vaak kunnen processen beter en sneller vooruit en (nieuwe) technologie kan daaraan bijdragen. Toen ik een aantal jaar geleden als beleidsmedewerker op Sint Maarten werkte, vond ik het gebrek van DigiD op het eiland bijzonder. Ik stond urenlang met een stapeltje papieren te wachten bij het Belastingkantoor en bij de bank. Er komt nu nog post van deze instanties aan bij mijn oude werkgever, die zij vervolgens de oceaan over sturen. Dat kan efficiënter, effectiever en privacy-technisch ook zeker veiliger. Anno 2023 komt er ook daar stap voor stap verandering in (digitale) systemen. En dat is in mijn optiek mooi, mits we altijd veranderen en vooruitgaan met in ons hart en hoofd humaniteit als grondbeginsel, - en daarmee in verbinding blijven staan met wat voor ons bestaan essentieel is.

Persoonlijke transformatie

Wanneer gesproken wordt over verandermanagement, kan ik beamen dat dit thesis-proces mij heeft getransformeerd. Dat heeft tijd en ruimte nodig gehad. Privé heb ik het nodige meegemaakt en naast mijn studie was ik fulltime werkzaam binnen alle lagen van het ‘Huis van Thorbecke’. Hierdoor heb ik een langere periode nodig gehad voor deze thesis; maar deze periode heeft me doen groeien in alle facetten. Persoonlijke ontwikkeling is voor mij het grootste goud dat er is. Dit onderzoekstraject heeft veel licht geworpen op mijn persoonlijke kernwaarden en ethiek en het besef dat ik mij volledig inzet voor (een duurzame) ontwikkeling van de maatschappij. Vanuit autonomie, maar altijd in verbinding. Mijn ‘bedoeling’. Samen bouwen (creëren) en verbinden zijn voor mij al enige tijd mijn drijfveren en sleutel tot persoonlijk leiderschap. Maar daar hoorde nog een stap voor: verkennen. Dat heb ik tijdens dit thesis-proces volop gedaan in de vorm van exploratief onderzoek. Verkennen, creëren, verbinden vormen voor mij voortaan mijn persoonlijke leiderschapsmodel om op volle kracht vooruit te kunnen gaan. Nu en in de toekomst. Soms leidt vertraging dus ook tot fundamentele inzichten.

Dankwoord

Dit onderzoek is tot stand gekomen onder begeleiding van professor Klievink. Ik wil hem bedanken voor het geduld, de sturing en de feedback. Het onderzoek is opgehangen aan een capstone rondom quadruple helix-samenwerking met Digicampus; een organisatie die tot doel heeft de burger meer regie te geven, interactie met de overheid makkelijker te maken evenals verantwoord datadelen. Daarbij wil ik in het bijzonder professor Bharosa bedanken, voor de waardevolle input aan de start van mijn proces, zodat ik meer richting kon geven aan mijn onderzoeksvraag aan de hand van actuele innovaties binnen het Nederlandse publieke landschap. Ook wil ik mijn studiebegeleider Jolanda den Heijer bedanken voor de altijd positieve stimulans en fijne gesprekken.

Een blik op de onbekende toekomst

Zoals gezegd, heb ik tijdens dit proces bij veel zaken de nodige vraagtekens geplaatst; het vergt een blik op de nog onbekende toekomst. Met als belangrijkste vraag: wat gaan digitale ontwikkelingen als deze uiteindelijk op macroniveau voor ons als mens betekenen? Waar komen we uit, al deze micro-ontwikkelingen bij elkaar opgeteld? Het vergt een helder, open vizier op alle (ethische) perspectieven die we kunnen verzamelen, op basis waarvan de juiste overwegingen gemaakt dienen te worden.

Dit onderzoek hoopt, op micro-niveau, een iets beter beeld te schetsen van wat er, vanuit de overheid, nodig is om tot veilige en betrouwbare (mogelijke) adoptie van nieuwe technologische ontwikkelingen als SSI over te gaan, waar burgers met een gerust hart achter kunnen staan. Het brengt in kaart wat er aan perspectieven zijn rondom digitale identiteit en wat er nodig kan zijn om samen verder te bouwen aan vertrouwen. Daarmee hoop ik een heel klein (kiezel)steentje bij te kunnen dragen aan de missie om Nederland beter voor te bereiden op een veilige, toekomstbestendige maatschappij waarin de mens (en alles wat leeft) centraal blijft staan. En waarbij een weloverwogen inzet van innovatie en technologie mogelijkerwijs handvatten bieden om daar samen – in verbinding - verder aan te bouwen, vanuit vertrouwen.

Veel leesplezier!

1 Inleiding

“When written in Chinese, the word 'crisis' is composed of two characters. One represents danger and the other represents opportunity.” - John F. Kennedy

1.1 Aanleiding

1.1.1 Over SSI

Nederland zet momenteel de toon wanneer het aankomt op de ontwikkeling van de innovatie Self Sovereign Identity (SSI) vanuit het Europees Self-Sovereign Identity Framework (ESSIF); de term SSI staat ook wel bekend als digitale identiteit. De verwachting is dat Nederland één van de eerste landen kan zijn die SSI voor elkaar heeft met een grote mate van betrouwbaarheid (Jacobs, 2021). SSI oftewel digitale identiteit is één van de grote thema's van de European Coalition of the Willing, waarin acht EU-lidstaten samenwerken en waar voormalig staatssecretaris Raymond Knops (BZK) initiatiefnemer van is (Digitale Overheid, 2020). Belangrijk daarbij is om te weten dat er niet langer wordt gekeken naar enkel een nationale digitale infrastructuur maar naar een globale infrastructuur waarbij samenwerkingen tussen overheden en private sectoren worden aangemoedigd. Een samenwerking aan een grensoverschrijdende pilot om identiteitsgegevens tussen Nederland en Duitsland te delen is op 23 september 2021 ondertekend (iBestuur, 2021). Een SSI-wallet is vergelijkbaar met een digitale portemonnee en zorgt voor snelle en eenvoudige online toegang tot belangrijke diensten, waarbij burgers zich online kunnen identificeren zonder daarvoor een beroep te moeten doen op commerciële aanbieders. Toegang wordt verstrekt tot online diensten uit EU-lidstaten (Europees Parlement, 2023). Je kunt daarmee bijvoorbeeld een bankrekening openen, een hypotheek regelen, geboorteakten aanvragen, inschrijven voor een universiteit binnen de EU, een auto huren met een digitaal rijbewijs, inchecken bij een hotel en belastingaangifte doen (Europees Parlement, 2023). Daarbij is het de eindgebruiker, de burger, die de regie voert over zijn of haar gegevens. Elke burger krijgt de 'sleutel' tot een eigen digitale identiteit. Met de invoering van een digitale identiteit wordt de administratie via blockchaintechnologie op verschillende computers gevoerd, waardoor extra veiligheid gegarandeerd is (Dutch Blockchain Coalition, 2022).

De eerste versie van de ‘wallet’ wordt open source ontwikkeld. Open source houdt in dat de broncode openbaar is, zodat iedereen het kan controleren en zorgt ervoor dat het ontwerp en de wallet transparant zijn (iBestuur, 2022).

1.1.2 Risico’s in beeld en het belang van vertrouwen

De speculatie over de komst van SSI brengt veel teweeg. Mogelijke risico’s worden volop uitgelicht. Er bestaan talrijke definities van het construct risico, maar voor dit onderzoek gaan we in op de algemene definities die hierover bestaan. Volgens Vlek (1990, in Hanekamp, 1999, p. 6) vallen hieronder: “de mogelijkheid van een ongewenst gevolg; een verzameling van mogelijke ongewenste gevolgen en gebrek aan veronderstelde beheersbaarheid.” Risico’s gaan gepaard met vertrouwen en verwachtingen; ze zijn zelfs bepalend voor vertrouwen (Bouckaert and Van de Walle, 2001 in Colesca, 2009; Nordheim et al., 2019). Vertrouwen wordt ook wel “het magische elixir voor burgerlijke verbondenheid” genoemd en is een belangrijk element in een (samenwerkings)relatie, omdat het openheid en informatiedeling bevordert. Met burgerlijke verbondenheid (‘civic engagement’) wordt bedoeld “een positieve kracht die sociaal vertrouwen, normen en waarden verrijkt” (Geys & Murdoch, 2010 in AlAwadhi, 2019, p. 3162).

Eén van de eerste geluiden die over SSI naar buiten komt, is dat de digitale coronapas een eerste opstapje zou zijn voor de invoering van een digitaal identiteitsbewijs. “De lobby voor een coronapas en een ‘QR-maatschappij’ wordt aangevoerd door de ‘digital identity industry’ en die boekt resultaat: de Europese Commissie verwacht de coronapas uit te breiden tot een volmaakte digital wallet”, zo schrijven Van Roermund et al. (2021). In India werd in 2009 het grootste eID-systeem ter wereld ingevoerd; Aadhaar. Een digitaal systeem, waarbij systeemfouten zijn geconstateerd waar inwoners van India de dupe van zijn geworden (Raju et al. 2017). Als we in Nederland aan systeemfouten denken, denken we al snel aan de toeslagenaffaire die tot veel gedupeerden geleid heeft.

Het eindrapport SSI Speelveldanalyse (BZK, 2021) schetst dat een veelvoud aan databronnen het voor burgers moeilijk maakt om overzicht te bewaren waar data allemaal voor gebruikt wordt. Hoogleraar privacy en identiteit Bart Jacobs van de Radboud Universiteit in Nijmegen vreest dat data wordt opgeslagen om burgers politiek en commercieel te kunnen sturen.

Hij verstuurde in 2019 een brandbrief naar Knops die toendertijd vervangend minister was van Binnenlandse Zaken en Koninkrijksrelaties (BZK) met de uitnodiging een politieke keuze te maken voor een decentrale architectuur en geen centrale architectuur. Bij een centrale architectuur worden de gegevens door één partij verzameld en opgeslagen, bij een decentrale architectuur is dat over het algemeen niet zo. Hoewel de techniek decentraal werkt, lijkt de macht gecentraliseerd te worden door diegene die het contract heeft opgesteld (Naves et al. 2019; Van Roermund et al., 2021).

Blockchain is een decentraal netwerk dat transacties op een permanente manier registreert. Daarmee is de beveiliging goed, maar het is permanent en onveranderlijk en daarmee ‘in strijd met het principe van opslagbeperking.’ Volgens de AVG-wet moet data verwijderd worden, zodra deze niet langer nodig is of wanneer mensen hun toestemming intrekken. Dat kan bij blockchain niet (Van Roermund et al., 2021, p. 13).

Hoogleraar aan Harvard, Elizabeth Renieris, ziet identiteit als een universeel grondrecht dat niet te kapitaliseren is. Wie (eigen) data bezit, kan deze verkopen aan bedrijven, met als mogelijk gevolg het einde van anonimiteit (Van Roermund et al., 2021).

Mart Kaevats, nationaal digitaal adviseur van de regering van Estland zegt in een artikel van iBestuur zich vooral zorgen te maken over integriteit. Dat iemand een bepaalde bloedgroep heeft, is niet privacygevoelig, maar het wordt een probleem als iemand deze door een hack verandert in een andere bloedgroep. Hij geeft aan dat de architectuur inrichten het makkelijkste is. “Het moeilijkste is om de mindset en de cultuur te veranderen. Er moet een vorm van vertrouwen ontstaan zoals die bestaat in een zwerm vogels of een school vissen.” Kaevats stelt dat ‘zwermgedrag’ ook geldt voor de integriteit van (eigen) data, waar iedereen zelf verantwoordelijk voor is; “de eigen eieren liggen in het eigen mandje. Als er een ei breekt (bijvoorbeeld door een hack), dan is alleen het ei in dat mandje gebroken en zijn alle andere eieren in ieders eigen mandje nog heel.” Belangrijk is dat de burger op de hoogte moet worden gebracht als het ei in zijn of haar mandje gebroken is. In dat opzicht wordt nog naar oplossingen gezocht (Trommel, 2021).

Ook in de Tweede Kamer worden er zorgen geuit over digitale identiteit. Een aantal moties werden ingediend, waaronder de motie van ChristenUnie-Kamerlid Ceder en D66-Kamerlid Dekker-Abulaziz (Motie 21501-33-932, 2 juni 2022). Daarin stellen zij dat de Europese digitale identiteit nu en in de toekomst niet mag leiden tot dataconcentratie, waarbij bij de Europese Unie, staten of bedrijven een grote hoeveelheid centrale data samenkomt.

Het raamwerk voor een Europese digitale identiteit mag volgens de Kamerleden in de toekomst niet leiden tot een directe of indirecte verplichting voor mensen die hier geen gebruik van willen of kunnen maken. Hiervoor zouden gelijkwaardige alternatieven geboden moeten worden voor mensen die geen gebruik willen of kunnen maken van de wallet door zowel overheden als bedrijven. Een tweede motie van Ceder en mede-ondertekenaars (Motie 21501-33-933, 2 juni 2022) gaat over de gevaren voor burgers en risico's van misbruik door een uniek en blijvend identificatienummer in het raamwerk voor een Europees digitaal identiteitsbewijs. Rond 16 februari 2023 rommelt het in de Tweede Kamer en de media, want staatssecretaris Van Huffelen (digitalisering) heeft een Kamermotie van de Europese digitale identiteit genegeerd (Tweedekamer.nl). De motie van (inmiddels oud-Kamerlid) Leijten (SP) pleitte voor het niet instemmen met het Europese voorstel voor een Europese digitale identiteit. Deze motie werd op 1 december 2022 door de Kamermeerderheid aangenomen. Van Huffelen legde als reden voor het negeren voor de aangenomen motie uit dat ze het belangrijk vindt dat Nederland een betrouwbare onderhandelingspartner wil zijn in Brussel (Tweedekamer.nl). Omtzigt reageerde op 16 februari 2023 op Twitter dat een dergelijke handeling zeer ernstig is in een democratie.

1.1.3 Digitalisering en de ontwikkeling richting quadruple helix

Digitalisering is door de COVID-19-pandemie in een versnelling gekomen. Er wordt zelfs gesproken over 'turbo-digitalisering' (Mühlhoff, 2020). Diensten binnen de publieke dienstverlening worden steeds meer gedecentraliseerd en de burger wordt digitaal en autonoom, ook wanneer het op eigen data-beheer aankomt. Deze diensten raken de kwaliteit van het leven van burgers. Daarmee zijn het vaak niet enkel producten die worden afgenomen, maar juist interacties waarin dezelfde cliënten het proces meebepalen. Lipsky (1980, p. 40-48) concludeert: "Vraag is niet alleen onderdeel van een transactie tussen burgers en overheid, maar is ook een transactioneel concept" (Van Delden, 2009, p.14.). Burgers en overheid beïnvloeden elkaar dan over en weer. Op het gebied van SSI werken overheid, wetenschap en bedrijfsleven met elkaar samen in een zogeheten triple helix-context (Dutch Blockchain Coalition, 2023). Innovaties uit de triple helix sluiten niet altijd aan bij de eisen en behoeften van de samenleving. Naast overheid, wetenschap en bedrijfsleven, krijgt de mens, in de rol van burger, een steeds centralere rol in de 'super smart society', waarin duurzame oplossingen geproduceerd worden richting diverse behoeften en sociale problemen aan de hand van technologische vooruitgang (Yıkılmaz, 2020).

Wanneer burgers een sterkere stem krijgen, onder andere in het ontwerpen van publieke diensten van de toekomst, spreekt men van een quadruple helix (Carayannis et al., 2022). De quadruple helix omarmt het maatschappelijk middenveld om de kloof tussen innovatie en de samenleving te overbruggen (Cavallini et al., 2016). Het is bij aanvang van dit onderzoek niet uit field- en desk-research op te maken of SSI in de verkenningsfase vorderingen maakt richting een quadruple helix-context van samenwerken met burgers. Er lijkt kennis te ontbreken over de betrokkenheid, verbinding en mate van vertrouwen die burgers ervaren bij de invoering bij SSI.

1.1.4 Probleemstelling

Diverse studies bewijzen dat vertrouwen een belangrijke factor is om e-government diensten te kunnen accepteren, adopteren en implementeren. (Colesca, 2009; Horsburgh et al., 2011; Parent et al., 2005; Alzahrani et al., 2017). SSI is een vorm van e-government. Silcock (2001) omschrijft een elektronische overheid (e-government) als “een ecosysteem dat een complex socio-technisch¹ systeem is waarin burgers, bedrijven en overheidsinstellingen worden opgenomen, die elektronische platforms gebruiken om waarde te creëren en distribueren naar deelnemers aan het systeem” (Fan et al., 2022, p. 2). Vertrouwensissues rondom nieuwe systemen kunnen adaptatie in de weg staan. Colesca (2009, p. 13) concludeert dat “burgers vertrouwen moeten hebben in het e-government-proces wil e-government haar doelstellingen kunnen behalen en een hoge kwaliteit en geïntegreerde publieke diensten kunnen aanbieden. Zonder vertrouwen, zal er geen participatie zijn aan e-government diensten. Daarom is het belangrijk dat de standpunten van de burgers serieus genomen worden. Hebben zij het gevoel dat hun standpunten niet serieus genomen worden, dan zal toekomstige participatie voor lange tijd uitgesloten worden. Het vertrouwen terugwinnen zal dan heel veel moeite gaan kosten.” Ook het vertrouwen in de overheid en in technologie zijn significante factoren om tot adoptie van digitale diensten over te kunnen gaan (AlAwadhi, 2019). In het Eindrapport SSI Speelveldanalyse (BZK, 2021) is te lezen dat op het gebied van vertrouwen en governance versplintering merkbaar is en bevestigt dat er binnen deze context een uitdaging bestaat om de adoptie van SSI op gang te krijgen. Vooral aan de kant van Issuers, Holders en Verifiers².

¹ Met socio-technisch wordt bedoeld een benadering van organisatorische ontwerpen die focust op de interactie tussen mensen en technologie.

² Deze term wordt verder uitgelegd onder paragraaf 2.2: Self Sovereign Identity: een disruptieve technologie.

“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.” (Eindrapport SSI Speelveldanalyse, BZK, 2021, p. 37). In wetenschappelijke literatuur is weinig bekend over vertrouwenspercepties waarbij e-government en burgerlijke verbondenheid centraal staan. Bovendien is “burgerlijke verbondenheid niet alleen een resultaat van vertrouwen, maar kan deze ook leiden tot het vergroten van vertrouwen” (Ekman & Amna, 2012 in AlAwadhi, 2019, p. 3162)

Er worden in de inleiding risico's rondom SSI geschetst, die veelal gerelateerd zijn aan het beschermen van publieke waarden voor burgers als privacy, integriteit en veiligheid. Publieke waarden worden onder andere gedefinieerd als: “duurzame opvattingen over de vormgeving van en bezigheden in de samenleving die al dan niet nastrevenswaardig worden beschouwd voor het voortbestaan van die samenleving, het welbevinden van haar leden en in samenhang daarmee, de aard en het gedrag van degenen – de publieke functionarissen – die deze waarden moeten behartigen” en samengevat betreffen ze het “algemeen belang en het idee van een goede samenleving” (Rutgers, 2011, p. 6).

Onderzoek stipt aan dat publieke waarden meegenomen moeten worden in risicomanagement en dat er systematisch aandacht uit moet gaan naar het beheersen van risico's die met publieke waarden gemoeid zijn. (Bok et al., 2021). Mulder (2019) vindt dat risicomanagement rondom de inzet van nieuwe technologie beter vervangen kan worden door professionalisering van publiek innovatiemanagement en een visie nodig heeft die richting geeft aan nieuwe manieren waarop de overheid publieke waarde levert aan de samenleving, ethische grenzen bewaakt en eisen aan samenwerking met derden (zoals techbedrijven) stelt. Mulder stelt dat er een nieuwe strategie nodig is, waarbij de verandering van ‘oud’ naar ‘nieuw’ noodzakelijk is. Daarbij wordt gekeken naar de rol van de overheid (‘polity’) en beleidsvorming (‘policy’). In dit onderzoek specifiek vanuit burgerperspectief en rondom het thema vertrouwen in SSI. Wanneer er intensief gestuurd wordt op datgene wat nodig is in de samenwerking, kan dit vertrouwen opbouwen (Ysa et al., 2014). De (leiderschaps)rol van de overheid is daarmee van invloed op vertrouwensmanagement (Paliszkiewicz et al., 2015). Leiderschap is noodzakelijk voor het creëren en behouden van duidelijke basisregels, het opbouwen van vertrouwen, faciliteren van dialoog en het verkennen van wederzijdse winst. Het betrekken van belanghebbenden en hen in staat stellen om mee te denken, kunnen een uitwerking zijn van leiderschap (Ansell & Gash, 2008). Dit onderzoek kan potentieel bijdragen aan het vergroten van de slagingskans van mogelijke implementatie van SSI (of andere nieuwe innovaties). Hoe?

Door burgers actief mee te laten denken over de gewenste rol van de overheid, over (rand)voorwaarden die het vertrouwen in SSI kunnen versterken en over het beschermen van publieke waarden en minimaliseren van risico's.

1.2 Onderzoeksvraag

De in de inleiding omschreven achtergrondinformatie en probleemstelling hebben geleid tot het formuleren van een onderzoeksvraag. Voor dit onderzoek is gekozen om een prescriptieve vraagstelling te hanteren met als doel tot aanbevelingen ter verbetering van de huidige situatie te komen (Van Thiel, 2015). Op basis van de uitkomst van het onderzoek zouden beleidsaanbevelingen gedaan kunnen worden richting nieuw beleid rondom de mogelijke introductie en adaptatie van een nieuwe technologie als SSI met als focus: het vertrouwen in SSI vergroten van de toekomstige 'holders' van SSI, oftewel burgers. SSI brengt tal van nieuwe mogelijkheden met zich mee en kan vereenvoudiging en versnelling bieden ten opzichte van de huidige bestaande systemen. Echter brengt het ook de nodige optelsom aan uitdagingen met zich mee aangaande risico's en vertrouwen. Belangrijke publieke waarden als vrijheid, inclusiviteit, soevereiniteit, privacy en integriteit liggen onder het vergrootglas en dienen beschermd te worden. Hoe gaan we nu samen vooruit? Niet alleen vanuit overheid, wetenschap en bedrijfsleven, maar met burgers inclusief; vanuit het quadruple helix-perspectief. Dit gegeven heeft geleid tot de volgende onderzoeksvraag:

Wat kan de overheid bieden om samen met quadruple helix actoren verder te bouwen aan vertrouwen van burgers in de (mogelijke) komst en adaptatie van Self-Sovereign Identity (SSI)?

Om de onderzoeksvraag te kunnen beantwoorden, worden een aantal deelvragen ingezet.

Deelvragen:

- I Hoe omschrijft de literatuur vertrouwen?*
- II Welke theoretische concepten vormen een basis om te bouwen aan vertrouwen?*
- III Welke publieke waarden spelen een rol bij het verstevigen van een vertrouwenspositie?*
- IV Welke risico's zijn er te signaleren rondom SSI aangaande deze waarden?*

- V Hoe zien burgers hun eigen rol als ‘Holder’ van de digitale identiteit in relatie tot de Identifier en Verifier op het gebied van vertrouwen en wat denken zij vanuit die positie nodig te hebben vanuit de overheid?*
- VI Welke waarde-creërende oplossingen kunnen vanuit de overheid - en vanuit de samenwerking van de quadruple helix - geboden worden om het vertrouwen in SSI (digitale identiteit) te vergroten en adaptie van SSI succesvol te maken?*

1.3 Relevantie

1.3.1 Wetenschappelijke relevantie

Veel beleidsproblemen rondom digitale transformatie zijn uitdagend en worden vanwege hoge niveaus van complexiteit, onzekerheid, afhankelijkheid en adaptatie aangeduid als een ‘wicked problem’; een maatschappelijk probleem waarover kennis ontbreekt en waarbij partijen moeilijkheden ervaren bij het interpreteren van de aard van het probleem, de oplossingen en wie de problematiek aan moet pakken. Dat is mede te wijten aan de verschillende prioriteiten en belangen die betrokken publieke en private partijen hebben (Rittel & Webber, 1973; Van Bueren et al. 2003; Klijn & Koppenjan, 2016). Deze problemen spelen zich af in een omgeving met grote onzekerheid in relatie tot de aard van de risico’s voor het individu en de maatschappij (Van Bueren, 2003). Vaak zijn traditionele strategieën vanuit publiek management onvoldoende toereikend voor een dergelijke uitdaging (Fountain, 2019). Er zijn geen kant-en-klare oplossingen en wat er precies nodig is om dergelijke problemen aan te vliegen is onbekend of onstabiel (Churchman, 1967). Om deze problemen te kunnen tackelen, is leiderschap van invloed. “Wicked problems dagen leiders uit om meerdere belanghebbenden met verschillende perspectieven en op verschillende niveaus met elkaar te verbinden, maar ook om managementstrategieën te bouwen die kunnen omgaan met een hoge mate van onzekerheid, dynamische ontwikkelingen en ambiguïteit” (Fountain, 2019, p. 7). In deze thesis wordt onderzocht wat er nodig is vanuit de (rol van de) overheid rondom de mogelijke implementatie van SSI. Hieruit kunnen theoretische aanvullingen rondom vertrouwen en leiderschap voortvloeien in relatie tot SSI die mogelijk ook van invloed zijn op de implementatie en adaptatie van andere nieuwe publieke technologieën en systemen.

Wetenschappelijk onderzoek kan ook een licht werpen op de veranderende rol van de (decentraliserende) overheid en kennis verschaffen dat kan dienen als input voor toekomstig beleid aangaande SSI. Gezien het feit dat het hier om een nieuwe technologie gaat waar in de literatuur nog niet veel over bekend is, kan gesproken worden van een wetenschappelijk kennisgat, waarbij nieuwe kennis mogelijk kan leiden tot het versterken van vertrouwen in nieuwe e-diensten zoals SSI waardoor (digitale) vooruitgang kan plaatsvinden (Nordheim, 2019). Door burgers mee te laten denken over mogelijke (waarde-creërende) oplossingen om het vertrouwen in nieuwe technologieën als SSI te vergroten, kan er ook een ontwerpdoelstelling aan het onderzoek gehangen worden die kan leiden tot “aanbevelingen ter verbetering van een situatie” (Van Thiel, 2015, p. 27). Dit verkleint mogelijk ook het gat tussen wat er top-down bedacht wordt en “wat er in de echte wereld ontstaat” en kan bijdragen aan relevante zaken rondom “de rol die we digitale systemen toedichten in het werk van de overheid” (Klievink, 2021, p. 8). Het kan nieuw licht werpen op bestaande en gewenste werkwijzen en systemen. Deze aanbevelingen kunnen als theoretische aanvullingen in verder onderzoek toegepast worden. Burgers hebben een belangrijke bijdrage wanneer het gaat om collaboratieve innovatie in de publieke sector. Deze rol is onder-getheoretiseerd volgens Hartley (2014), waardoor het verder conceptualiseren van die rol in publieke innovatieprocessen wetenschappelijk relevant is (Agger en Lund, 2017).

1.3.2 Maatschappelijke relevantie

Veiligheid als basis met vertrouwen als kern

De piramide van Maslow (1943) geeft aan dat de meest belangrijke interne behoefte, na de primaire basisbehoefte van de mens, veiligheid en zekerheid is (Finkbeiner et al., 2010). Veiligheid wordt omschreven als het omgekeerde van risico; hoe lager het risico, hoe hoger de veiligheid wordt ervaren (Balderson, 2016). Ook veiligheid is een veelomvattend begrip en kent diverse vormen. Zo gaat fysieke veiligheid over “het beschermen van het eigen lichaam en de directe omgeving van personen, terwijl sociale veiligheid te maken heeft met het beschermen van de positie en levensomstandigheden van personen” (Bauman, in Schuilenburg 2009, p. 9). Ook kan er verschil gemaakt worden tussen objectieve veiligheid; hoe vaak een gevaarlijke situatie wel of niet voorkomt (meetbaar). Statistieken van incidenten, bijvoorbeeld rapporten van de politie, geven een beeld van de objectieve veiligheid (Bruls, 2001 in De Meij, 2010).

Subjectieve veiligheid gaat over het veiligheidsgevoel dat mensen ervaren (niet meetbaar); de beleving van veiligheid (De Meij, 2010). Beide vormen van veiligheid zijn toepasbaar op SSI; zo is het mogelijk dat een hack ‘objectief’ waargenomen wordt en data in verkeerde handen is gevallen. Anderzijds kunnen burgers een onveilig gevoel beleven (‘subjectief’) omdat zij weten dat een systeem mogelijk vatbaar is voor een hack, waardoor hun privacy in het geding is omdat er mogelijk persoonlijke gegevens in verkeerde handen kunnen vallen. De term maatschappelijke veiligheid is ook van toepassing op dit onderzoek, oftewel: “de maatschappelijke vaardigheid om kritische sociale functies te behouden om het leven en de gezondheid van burgers te beschermen en om aan de basisvereisten van de burgers in diverse stressvolle situaties te kunnen voldoen” (Olsen et al., 2007, p. 69). Ook tijdens de Coronacrisis is gebleken dat het voor de maatschappij van wezenlijk belang is om veiligheid en zekerheid zo goed mogelijk te garanderen (Rijksoverheid, 2020). Het zorgdragen voor de veiligheid van de samenleving ligt voor een groot deel bij de overheid (Boutellier, 2007). Met de komst van SSI komt data meer bij de burgers te liggen. Het is daarbij van belang dat de veiligheid van die data, en daarmee ook van de identiteit van burgers, zo goed mogelijk beschermd blijft, en dat nagedacht wordt over hoe objectieve en subjectieve veiligheid vergroot kunnen worden. De komst van SSI, en daarmee de decentralisering van data en de regie die de burger heeft over de eigen digitale identiteit, zorgt voor nieuwe uitdagingen betreffende publieke waarden als privacy, inclusiviteit, veiligheid en vertrouwen. Dit onderzoek brengt het subjectieve sentiment, dat wat burgers ervaren, in kaart, brengt de nieuwe uitdagingen beter in beeld en kan inzicht geven in hoe deze waarden beter beschermd kunnen worden vanuit het perspectief van de burger.

Aandacht voor de rol van de overheid en burger bij technologische innovaties

Mulder (2019) stelt dat ‘welke rol het bestuur heeft wanneer het gaat over hoe de samenleving omgaat met technologische veranderingen’ de brandende vraag is die politici en beleidsmakers bezig moet houden. Hoe de samenleving omgaat met eigen databeheer in relatie tot (cyber)veiligheid en wat de rol van burger en overheid zou moeten zijn in een maatschappij waarin de burger op steeds autonomere wijze data en digitale identiteit uitwisselt, vergt meer onderzoek. Dit onderzoek is een voorbereiding op een steeds autonomer functionerende data-gedreven maatschappij.

Verbeterde samenwerking door inzicht in burgerperspectief

en focus op de triple en quadruple helix

Wat heeft de burger van de overheid en andere actoren nodig om vol vertrouwen de toekomst tegemoet te zien in het kader van SSI? Kan er bijvoorbeeld door een betere samenwerking met de burger (quadruple helix) een steviger partnership gecreëerd worden? Dit onderzoek kan mogelijk leiden tot nieuwe inzichten over de ontwikkelingen van triple naar quadruple helix-samenwerking en optioneel bijdragen aan versterkte samenwerking tussen alle actoren. Wanneer men elkaar beter vindt en versterkt, kan dat ook positief uitwerken op andere maatschappelijke (beleids)uitdagingen en opgaven.

Het fundament voor bouwen aan vertrouwen versterken

Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK) heeft als beleidsverantwoordelijke voor de Nederlandse (digitale) identiteitsinfrastructuur, een visie gepubliceerd over de rol van en houding met betrekking tot digitale identiteit in Nederland. Hierin schetst Knops dat de overheid een actieve rol voor zichzelf ziet in het creëren van vertrouwen in de digitale wereld voor burgers en bedrijven en dat het beschikken over een betrouwbare (bron-)identiteit cruciaal is. Dit “door een zorgvuldige identificatie, betrouwbare authenticatie en gecontroleerde autorisatie mogelijk te maken. Dit vertrouwen is essentieel voor economische en sociale ontwikkeling” (*Kamerstukken II, 2020/21, 26643, nr. 743: p. 4*) Knops geeft aan dat Nederland bij de landen hoort die vooroplopen, maar het beter kan en moet. Daarom wil hij gezamenlijk bouwen aan vertrouwen in de digitale wereld door een betrouwbare digitale identiteit infrastructuur in te richten (*Kamerstukken II, 2020/21, 26643, nr. 743*). Een vraag kan zijn of dit de enige pijler is waarop dit vertrouwen in de digitale wereld berust of dat er andere aandachtspunten zijn om het fundament van vertrouwen rondom SSI te verstevigen, zoals systeemvertrouwen. Een gebrek aan vertrouwen kan voor burgers, bedrijven en overheden een aanleiding zijn om te aarzelen of weigeren om transacties digitaal uit te voeren en van nieuwe diensten gebruik te maken. Ook wanneer burgers de mogelijkheid krijgen om zelf de regie te voeren over een gezaghebbende bron van identiteitsgegevens. Dit kan adoptie van SSI in de weg staan en weerstand vergroten tegen nieuwe technologieën. Door burgers te laten meedenken over het onderwerp (en ontwerp), kunnen nieuwe mogelijkheden ontstaan die, indien verder onderzocht en juist geïmplementeerd, het vertrouwen van de burger in SSI kunnen versterken.

Vraagstukken rondom het aanjagen van adoptie beantwoorden

De vragenlijsten vanuit het Eindrapport SSI (2021) indiceren dat er vraagstukken rondom (grootschalige) adoptie van SSI bestaan, en dat gezien wordt als een relevante nieuwe onderzoeksvraag. Het rapport onderschrijft ook dat de focus in eerste instantie primair ligt op het verkennen van functionele mogelijkheden en gewenste technische implementatie en dat er pas na deze experimenten aandacht komt voor het aanjagen van adoptie.

Er is nog weinig aandacht voor het aanjagen van adoptie rondom SSI, omdat SSI zich nog in de experimentele fase met initiatieven bevindt, maar ook door een ingewikkelde adoptiedynamiek tussen Issuers, Holders en Verifiers (SSI Speelveldanalyse, 2021, p. 20). Er wordt gesproken over een uitdaging om de adoptie van SSI aan de kant van Issuers, Holders en Verifiers op gang te krijgen. Dit onderzoek kan mogelijk inzicht geven in de ingewikkelde adoptiedynamiek tussen Issuers, Holders en Verifiers, met als uitgangspunt vertrouwen, en zo de knelpunten binnen het adoptieproces van SSI, in elk geval vanuit de rol van de burger, zichtbaar maken. Dit helpt in het proces van het maken van de juiste afwegingen die nodig zijn rondom de (mogelijke) implementatie van SSI. Ook wordt benadrukt dat dit vraagstuk een relevante nieuwe onderzoeksvraag is, waar dit onderzoek aan kan bijdragen. Hoewel er steeds meer aandacht komt voor de relaties tussen het bouwen van vertrouwen in e-government, de adoptie en het gebruik van e-government diensten en de betrokkenheid van burgers hiermee, is er volgens AlAwadhi (2019), behoefte aan uitbreiding van kennis binnen deze context. Deze kennis koppelen aan SSI zou meerwaarde bieden om op dit specifieke thema maatschappelijke vooruitgang te kunnen boeken.

1.4 Leeswijzer

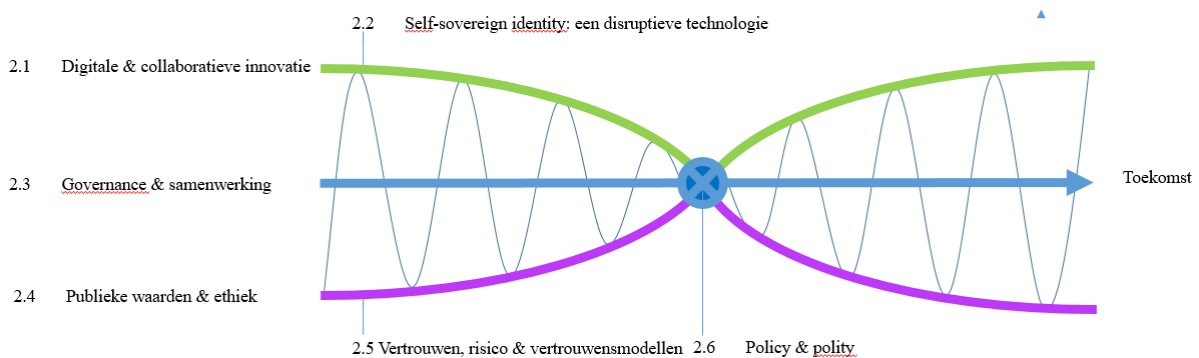
Dit onderzoek kent een theoretisch kader (2), methoden (3), resultaten en analyse (4) conclusies, aanbevelingen en discussie (5), referentielijst (6) en bijlagen (7).

2 Theoretisch kader

Het theoretisch kader gaat in op de gewenste rol van de overheid ('polity') in relatie tot vertrouwen in SSI en daarbij mogelijk passende beleidsoplossingen ('policy').

Overheid en beleid hebben zich door de jaren heen ontwikkeld. Om te begrijpen welke ontwikkelingen vooraf zijn gegaan aan waar 'we' nu staan op het gebied van overheid en beleidsvorming, is de achtergrond in beeld gebracht in een drietal informatiesporen die een onderzoekslens vormen om richting te geven aan dit onderzoek en de structuur ervan. Deze informatiesporen zijn van belang om te begrijpen welke belangrijke routes, die elkaar onderling raken, genomen zijn om vanuit de overheid tot hedendaagse beleidsvorming rondom SSI te komen. Digitale & collaboratieve innovatie (2.1), governance en (quadruple helix) samenwerking (2.3) en publieke waarden & ethiek (2.4) zijn allen onmisbare onderdelen om de beleidsmotor 'policy & polity' (2.6) rondom vertrouwen in SSI te begrijpen en laten draaien. Vanuit dat punt, die kern, kunnen de rol van de overheid en haar beleid nu verder vormgegeven worden richting de toekomst.

Om de samenhang van de theorie in beeld te brengen, is een model opgezet, dat ook gekoppeld wordt aan de structuur van het onderzoek:



Afbeelding 1: Het theoretisch kader inzichtelijk gemaakt.

Policy & polity (2.6) als het vertrekpunt 'nu' vanuit voorgaande sporen: beleid ('policy') en de rol van de overheid ('polity') maken verbinding met alle informatiesporen om verdere ontwikkeling mogelijk te maken om samen te kunnen bouwen aan vertrouwen in een mogelijke komst en adaptatie van een disruptieve technologie als SSI.

De informatiesporen die hieraan verwant zijn en qua achtergrond en historie van waarde zijn om inzicht te krijgen in de (gewenste) overheidsrol en tot beleidsvorming te kunnen komen, zijn:

2.1 Digitale & collaboratieve innovatie; groene informatiespoor: beschrijft de ontwikkeling in de tijd van digitale technologie: van automatisering en digitalisering richting dataficering op het beleidsniveau nu. Ook digital en smart government, e-governance en de smart society worden beschreven en er wordt uitleg gegeven over de ontwikkeling van triple helix en de kenniseconomie, naar quadruple helix en de kennismaatschappij en kennisdemocratie en Industry 5.0.

2.2 Self-sovereign identity, een disruptieve technologie: beschrijft het begrip soevereiniteit en geeft achtergrondinformatie over SSI als disruptieve technologie en de technische infrastructuur om een beter inhoudelijk begrip van SSI als technologie te krijgen.

2.3 Governance & samenwerking; blauwe informatiespoor: beschrijft de overheidsontwikkelingen van New Public Management, Publiek-Private Samenwerking, de triple en quadruple helix samenwerking, governance (New Public Governance en collaborative governance en de context van het samenwerkingsproces) door de tijd heen. Deze paragraaf maakt de achtergrond en (samenwerkings)mogelijkheden vanuit governance-perspectief inzichtelijk.

2.4 Publieke waarden & ethiek; paarse informatiespoor: legt uit wat publieke waarden zijn en welke publieke waarden SSI wil dienen. De publieke waarden die voor burgers van belang zijn in relatie tot vertrouwen in SSI, komen in de vragenlijst en in de resultaten daarop in hoofdstuk 4 uitvoerig aan bod.

2.5 Vertrouwen, risico & vertrouwensmodellen: vertrouwen is binnen de onderzoeksvraag het te onderzoeken concept. Het concept wordt hier nader uitgelegd en gekoppeld aan vertrouwensmodellen die in de literatuur te vinden zijn. Vertrouwen en risico hebben beiden invloed op gedrag; die relatie wordt uitgelegd (Gefen et al., 2003). De vertrouwensmodellen wijzen op de karakteristieken van vertrouwensmanagement en vertellen dat leiderschap van invloed is op vertrouwensmanagement. Dit onderzoek zal de gewenste rol van de overheid in relatie tot vertrouwen in SSI onder de loep nemen en bekijken welke karakteristieken van vertrouwensmanagement potentieel verbeterd kunnen worden.

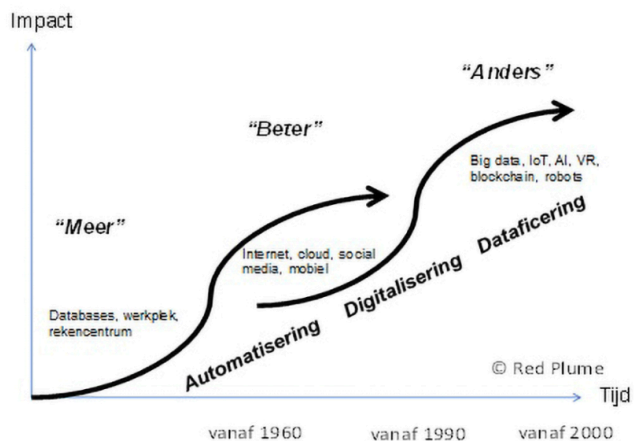
2.1 Digitale en collaboratieve innovatie

2.1.1 Digitale technologie door de overheid in drie fasen

Mulder (2019) omschrijft drie fasen in het gebruik van digitale technologie door de overheid: de periode van automatisering (vanaf 1960), digitalisering (vanaf 1990) en dataficering (2000). Deze drie technologiegolven leverden drie digitale landschappen op:

automatisering van de back-office, digitalisering van de frontoffice en dataficering van de out-of-office, ook wel de wereld buiten de overheid genoemd (Mulder e.a., 2017).

Maes (2017) vertaalt de drie fasen respectievelijk naar ‘meer, beter en anders’ waarbij meer en beter goed aansluiten bij de filosofie van New Public Management, waarbij bezuinigen en hervormen en dienstverlening vanuit klantperspectief centraal zijn komen te staan (Politt e.a., 2007). Het ‘anders’ kenmerkt zich door een shift in mindset, leren en experimenteren, ‘game changers’ met een ecosysteem en de samenleving als uitgangspunt. Blockchain-technologie speelt een belangrijke rol in het tijdperk van dataficering (Maes, 2017).



Afbeelding 2: Historische drie fasen van inzet van digitale technologie (Red Plume in Mulder, 2019, p. 60)

	Meer	Beter	Anders
Inzet ICT	Automatisering	Digitalisering	Dataficering
Scope ICT	Backoffice	Frontoffice	Out-of-office
Managementfocus	Control/efficiency	Aanpassing/gebruik	Leren/experimenteren
Organisatie-aanpassing	Herstructurering	Procesinrichting	Shift in 'mindset'
Innovaties	Goedkoper/snel	Betere diensten	'Game changers'
Ontwerpfocus	Eenheid/silo	Proces/keten	Ecosysteem
Scope	De organisatie	De overheid	De samenleving
Middelpunt	Medewerker	Klant	Mens
Strategie	Optimalisatie	Innovatie	Transformatie

Afbeelding 3: Managementmodellen en technologielandshappen meer, beter en anders (Maes, 2017 en Red Plume in Mulder, 2019, p. 61)

2.1.2 Digitale innovatie en haar speelvelden

Decentralisatie en privatisering, toenemende complexiteit van de netwerksamenleving en technologische ontwikkelingen veranderen niet alleen de mogelijkheden, maar ook de verwachtingen die burgers van de overheid hebben. Aanpassingen en vernieuwing is noodzakelijk, oftewel innovatie van de overheid (Osborne & Brown, 2005).

Anderson et al. (2014) zien innovatie als “het proces van leren en betekenis geven om te komen tot een nieuwe manier van (samen)werken.”

Innovatie als resultaat kan bestaan uit nieuwe producten, nieuwe processen of een nieuwe inrichting van governance³ (Anderson et al., 2014). Schumpeter (1942) beschrijft innovatie als “een proces van creatieve destructie waar nieuwe combinaties of bestaande bronnen worden verkregen.”

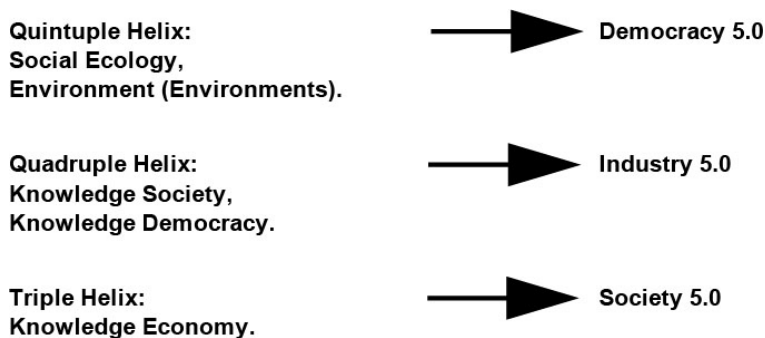
Technologie wordt steeds toegankelijker voor iedereen en de decentralisatie van technologie zorgt voor een shift in het informatie-evenwicht tussen overheid en samenleving. “Waar tot nu toe de overheid de beschikking had over de meeste data, gaat de samenleving zelf meer eigen data verzamelen. Deze decentralisatie van de macht over technologie en data komt momenteel samen met de noodzaak om wereldwijd maatschappelijke problemen op te lossen en de groeiende onvrede over het klassieke beleid en bestuur van de overheid. Dit kan weleens ruimte creëren voor een fundamentele heroriëntatie op de rol en het functioneren van de overheid en leiden tot radicaal andere manieren om publieke waarde te leveren” (Mulder, 2019, p. 62). Er zijn verschillende speelvelden van verandering rondom digitale innovatie:

- ➔ Digital government; het applicatielandschap van de overheid;
- ➔ E-governance; digitale dienstverlening tussen overheid, burgers en bedrijven en ketenuitwisseling tussen overheden. Hier gaat het om nieuwe technologie zoals blockchain en nieuwe werkwijzen zoals design thinking waarbij de gebruiker centraal staat;
- ➔ Smart government; waarbij de overheid slimme technologie inzet op eigen werkprocessen;
- ➔ Smart society; waarbij overheid en samenleving steeds meer met elkaar vervlochten raken, door dataficering waarbij processen en data meer en meer over de grenzen gaan

³ Governance als begrip wordt uitgelegd in paragraaf 2.3.4. pagina 31

van bestaande organisaties en instituties. Het speelveld ligt hier buiten de grenzen van bureaucratie en de sociale impact is groot (Mulder, 2019).

‘Super-smart society’, of ‘Society 5.0’ volgt vier perioden op: de jagers society, de agrarische society, de industriële society en de informatie society. “Het doel van de smart society is een maatschappij waarin de mens centraal staat en waar producten en diensten worden verstrekt om aan verschillende potentiële behoeften te voldoen en tegelijkertijd de economische en sociale kloven weg te nemen zodat alle mensen een comfortabel en gezond leven kunnen leiden” (Yikilmaz et al. 2020, p. 95). In relatie tot de quadruple helix wordt vaker gesproken over de Industry 5.0 en, bij de uitbreiding naar de quantuple helix, over Democracy 5.0. De quadruple helix draagt vooral bij in de dimensie van democratie, of de context van democratie, voor kennis. Uitgangspunt is dat de kennis- en innovatie-evolutie afhankelijk zijn van de democratie en kennisdemocratie (Carayannis & Campbell, 2002). Industry 5.0 is waarde-gedreven en wordt (vertaald) omschreven als “het herkennen van de kracht van de industrie om maatschappelijke doelstellingen te behalen die verder gaan dan banen en groei, om een weerbare verstrekker van welvaart te worden, door productie de grenzen van onze planeet te laten respecteren en het welzijn van degene die in de industrie werkzaam is in het hart van het productieproces te plaatsen” (Xu et al., 2021, p. 533).



Afbeelding 4: De Multi-Level Helix Structuur van het Quintuple helix framework (Carayannis & Campbell, 2022, p. 70)

2.1.3 Collaboratieve innovatie

Hartley et al. (2013, p. 822) omschrijven collaboratieve innovatie als “een complex en iteratief proces waarbij problemen worden aangeduid; nieuwe ideeën worden ontwikkeld en gecombineerd; prototypes en pilots worden ontworpen, getest en aangepast; en nieuwe oplossingen worden geïmplementeerd, verspreid en geïmplementeerd.”

Innovaties zijn veranderingen die breken met gevestigde werkwijzen en mindsets van een organisatie of organisatieniveau (Hartley et al. 2013).

Burgers hebben een belangrijke bijdrage wanneer het gaat om collaboratieve innovatie in de publieke sector (Agger en Lund, 2017). Co-productie wordt vaak in dezelfde context als collaboratieve innovatie genoemd. Co-creatie (Bason, 2010) en co-design, waarbij o.a. design thinking kan worden ingezet, is een uitgangspunt om burgers als publieke consumenten beter te betrekken in de productie van nieuwe publieke diensten en zo te kunnen bijdragen aan publieke waarde creatie (Prahalad & Ramaswamy, 2002). Moore omschrijft publieke waarde⁴ als: “de som van individuele voldoening die kan worden geproduceerd door een bepaald sociaal systeem of het overheidsbeleid” (Moore, 1995 p.52). Bozeman & Jørgensen (2007) en Talbot (2006) in Jellema (2021) vullen dit aan door de publieke waarde “een bijdrage aan de publieke sfeer” te noemen, “die in samenspel met de overheid en netwerkpartners wordt gerealiseerd door het gesprek aan te gaan.”

2.2 Self-sovereign identity; een disruptieve technologie

Om het concept Self-Sovereign Identity (SSI) uit te kunnen leggen, is het van belang het begrip soevereiniteit onder de loep te leggen.

2.2.1 Digitale soevereiniteit

Het begrip soeverein wordt in de Van Dale aangegeven als ‘oppermachtig’, ‘onafhankelijk’ en ‘onafhankelijke machthebber’ (Van Dale, 2022). Absolute soevereiniteit is vastgesteld door filosoof Thomas Hobbes (1588-1679), die in zijn werk Leviathan stelde dat burgers automatisch al hun rechten overdragen aan de staat. Leviathan is in het Oude Testament een zeemonster die een enorme macht voorstelt. Die rol zag Hobbes ook voor de staat weggelegd. In de moderne democratische staatsfilosofie is het zo dat burgers die soevereiniteit alleen overdragen in de mate waarin dat nodig is voor de rechtsstaat (Ensie, 2021). Digitale soevereiniteit wordt door Pohle & Thiel (2020) beschreven als “de mogelijkheid van individuen om over te gaan tot actie en keuzes te maken op een bewuste, opzettelijke en onafhankelijke manier, waarbij het doel is om controle te krijgen over hun data, device, software, hardware en andere technologieën” (Couture & Toupin, 2019 p.12). Identiteitsmanagement is daarbij de sleutel. Zelf-soevereiniteit kan gezien worden als

⁴ Zie voor een aanvulling van het begrip publieke waarde paragraaf 2.4, pagina 34

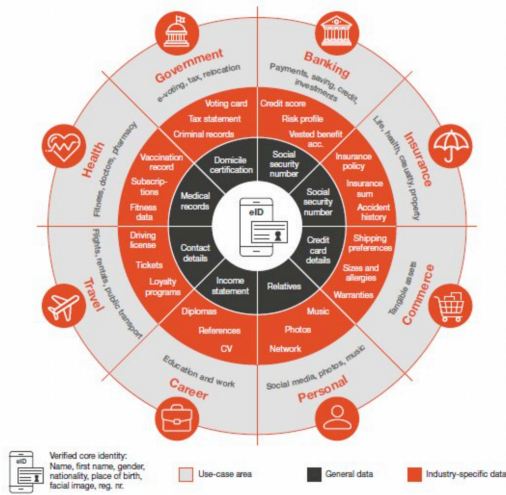
decentralisatie van macht, wat ook aansluit bij het idee van een gedecentraliseerde overheid. (Ishmaev, 2020). De burgers gaan zelf zorgdragen voor hun digitale identiteit.

2.2.2 Self-sovereign Identity (SSI)

Self-Sovereign Identity wordt omschreven als “een subtype van gedecentraliseerde identiteit (DID) waar de gebruikers controle over hun identificatoren hebben maar ook over de gegevens die daaraan gekoppeld zijn” (Komorowski et al. 2021). Self-sovereign Identity (SSI afgekort) staat voor een permanente identiteit die wordt beheerd en gecontroleerd door een persoon of entiteit waar deze identiteit aan toebehoort, zonder de behoefte om op een externe administratieve autoriteit te leunen en zonder de mogelijkheid dat de identiteit weggenomen kan worden. Daarvoor is nodig: de interoperabiliteit van gebruikersidentiteiten over meerdere locaties met instemming van de gebruiker, maar ook gebruikerscontrole van die digitale identiteit en volle gebruikersautonomie (Domingo, 2020). In de Kamerbrief van 12 oktober 2021 betreffende Domein Toegang onderschrijft Knops SSI als “een nieuwe manier van denken over digitale identiteit, gestoeld op het principe dat individuen controle zouden moeten hebben over hun digitale identiteit en de gerelateerde gegevens. De burger krijgt zelfbeschikking over de gegevens” (Knops, 2021). Dit zou passen binnen het beleid dat de praktische toegang tot de digitale dienstverlening behelst, evenals de inclusieve toegankelijkheid van inlogmiddelen. PwC schaal SSI onder de noemer Identity & Access Management en omschrijft dit als “een discipline die het mogelijk maakt dat de juiste individuen op de juiste momenten toegang hebben tot de juiste bronnen, op de juiste manier, om de juiste redenen en met de mogelijkheid om te rapporteren rondom deze toegang” (PwC.com, 2023). Met een digitale identiteit, ook wel eID genoemd, kunnen burgers bij overheden, banken en bedrijven met een unieke identificatiecode, gekoppeld aan persoonsgegevens, hun identiteit kenbaar maken (Van Roermund et al., 2021). Het Kamerstuk van 11 februari 2021 omschrijft digitale identiteit als een verzameling gegevens die een entiteit (persoon of organisatie) in het digitale domein representeren.

“Voorbeelden hiervan zijn: naam, geboortedatum, adres; statische identificerende gegevens, identifiers (bijvoorbeeld BSN, rekeningnummer, KvK nummer of telefoonnummer); biometrie (zoals een gezicht of vingerafdruk); certificaten (zoals diploma's of rijvaardigheid); dynamische attributen zoals digitale transacties (zoals een bankafschrift)” (*Kamerstukken II*, 2020/21, 26643, nr. 743: p. 7). In de schets die PwC van de eID (digitale identiteit) gemaakt heeft, zijn diverse informatiebronnen te identificeren, zowel zakelijk als privé. Deze kunnen allemaal deel uit gaan maken van de wallet, vergelijkbaar met een digitale portemonnee.

Denk daarbij aan: overheidsinformatie, financiële informatie, verzekeringsinformatie, commerciële informatie, persoonlijke informatie, informatie over carrière en opleidingen, reisinformatie en gezondheidsinformatie (Van Roermund et al.,2021).



Afbeelding 5: Schets digitale identiteit, PwC (Van Roermund et al.,2021)

De uitwisseling van gegevens loopt van partijen die ze in de vorm van credentials uitgeven (Issuers), via een digital agent (zoals een wallet) van betrokkenen (Holders) en onder hun nadrukkelijke controle terechtkomen bij partijen die credentials willen gebruiken oftewel die deze gegevens nodig hebben (Verifiers) (Eindrapport SSI Speelveldanalyse, BZK, 2021, p. 10).



ISSUERS; partijen die gegevens in de vorm van credentials uitgeven, via bijvoorbeeld een wallet van betrokkenen.



VERIFIERS; partijen waar de gegevens in de vorm van credentials terechtkomen omdat ze de gegevens willen gebruiken of nodig hebben.



HOLDERS; de individu of het bedrijf over wie de data gaat. Bijvoorbeeld de burger in kwestie.

Veel transacties vinden plaats tussen Issuer en Verifier. De Holder moet er dan op vertrouwen dat daadwerkelijk niet meer gedeeld wordt dan eventueel aan hen inzichtelijk is gemaakt (Eindrapport SSI Speelveldanalyse, BZK, 2021, p. 51).

Autonomie wordt gezien als een beslissend element van zelf-soevereiniteit.

Warr (2007) omschrijft autonomie als ‘een mogelijkheid voor persoonlijke controle’ (Warr, 2007, p. 83). Om autonomie te bewerkstelligen moet een SSI overdraagbaar zijn; het mag niet in beheer zijn op basis van slechts één site, provider of locatie. Hiervoor is een ecosysteem nodig dat de acquisitie en opname faciliteert van attributen, en vertrouwen verspreid tussen entiteiten die gebruik maken van deze identiteiten (Satybaldy et al., 2020). Omdat er sprake is van digitale processen gebeurt verificatie door inzet van een vertrouwensdienst. Onderdelen van vertrouwensdiensten zijn versleuteling, digitale ondertekening en authenticatie. Digitale certificaten vormen de basis van veilige digitale verbindingen en de beveiliging van digitale informatie. Privacy en autonomie hebben een raakvlak: “Privacy vertegenwoordigt de controle van transacties tussen een persoon of meerdere personen en een ander of anderen, met als ultieme doel autonomie te vergroten en/of kwetsbaarheid te minimaliseren” (Margulis, 1977, p.10).

2.2.3 SSI: een disruptieve technologie

Moderne disruptieve technologieën als SSI creëren een nieuwe werkelijkheid voor ons als burgers. Dit roept sturingsvragen rondom waarden als integriteit (Torenvlied & Ossewaarde, 2020). Onder een disruptieve technologie wordt verstaan: “een innovatie die de manier waarop consumenten, industrieën of bedrijven opereren aanzienlijk verandert.

Een disruptieve technologie veegt de systemen of gewoonten die het vervangt weg omdat het kenmerken heeft die overduidelijk superieur zijn” (Goede, 2007, p. 15). Disruptieve innovatie is een vorm van innovatie die “zorgt voor een radicale verandering van de status quo (Nagy, Schuessler en Dubinsk, 2016 in Knaapen, 2019, p. 19).

2.2.4 Impact van disruptie

Blockchaintechnologie, waar ook SSI op gebaseerd is, kent disruptieve effecten (Frizzo-Barker, 2021). Door de cryptotechnologie blockchain worden nieuwe decentrale modellen van dienstverlening mogelijk die voor ontwrichting (disruptie) kunnen zorgen.

Als eerste-orde-impact kan de disruptie van het werkproces genoemd worden. Zo komt het databeheer meer in de handen van burgers te liggen. Een digitale wallet kan ook een proces als een e-commerce registratie ontwrichten.

Bijvoorbeeld wanneer op een e-commerce website snel een aankoop kan worden gedaan zonder registratie, omdat de digitale wallet direct identiteitsinformatie ontsluit die opgeslagen is in de verifieerbare identiteit (Sedlmeir et al., 2021). De tweede orde-impact is het managen van de impact die de disruptie teweegbrengt. Processen gaan anders lopen en dat heeft ook impact op de manier van identiteit beheren en de (cyber)veiligheid en weerbaarheid van de burger (Mulder, 2019).

2.3 Governance & samenwerking

2.3.1 New Public Management

Vanaf het begin van de jaren tachtig deed New Public Management (NPM) haar intrede, waarbij de overheid zich meer ging focussen op het beleid en de uitvoering aan andere publieke en private partijen over ging laten ter bevordering van efficiëntie en effectiviteit. Er ontstond decentralisering van overheidstaken. Decentralisatie zorgt ervoor dat de nationale regering vaak sterk afhankelijk van de decentrale overheden is, omdat steeds meer taken en activiteiten van nationaal niveau worden overgedragen aan decentrale (bestuurs)lagen. Hierdoor bestaat de assumptie dat de staat uitgehold wordt en het publieke domein ‘leeg’⁵ raakt; taken van de overheid verschuiven immers door naar private individuen en partijen. Het vergt een nieuwe manier van besturen: multi-level governance. Dit brengt andere uitdagingen met zich mee. Taken zijn niet meer zo makkelijk te scheiden zoals het geval was ten tijde van de drie-kringenleer⁶. Termen als privatisering, verzelfstandiging en uitbesteding en handelen op basis van ‘performance’ wonnen met de decentralisatie aan terrein (Hood, 1991; Klijn & Twist, 2007).

⁵ ‘Hollow crown’

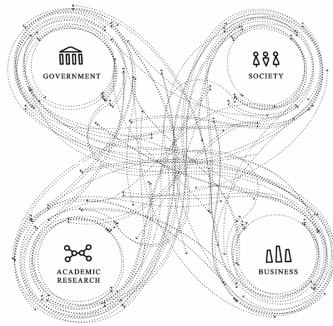
⁶ De drie kringen zijn Rijk, provincies en gemeenten.

2.3.2 Publiek-Private Samenwerking

Samenwerking tussen overheid en externe partijen is een middel dat door overheden steeds meer ingezet wordt om complexe problematiek aan te kunnen pakken. Klijn en Twist (2007, p.2) omschrijven publiek-private samenwerking (PPS) als “een min of meer duurzame samenwerking tussen publieke en private actoren waarin gemeenschappelijke producten en/of diensten worden ontwikkeld en waarin risico’s, kosten en opbrengsten worden gedeeld.”

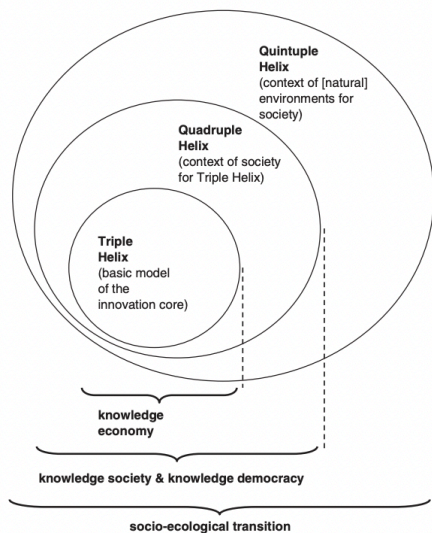
2.3.3 Triple helix & quadruple helix samenwerking

In de context van PPS kan ook gekeken worden naar triple helix samenwerking; “een tijdelijk samenwerkingsverband tussen drie of meer organisaties die middelen, risico’s en opbrengsten delen om individuele organisatiedoelen, gezamenlijke samenwerkingsdoelen en maatschappelijke doelen te realiseren” (Vos & De Vries, 2016). Onderdeel van die samenwerking zijn tenminste één publieke organisatie (overheid), kennisorganisatie (wetenschap) en private onderneming (bedrijfsleven). Naast de triple helix samenwerking zijn ook de quadruple en quintuple helix te onderscheiden, waarbij de quadruple helix de maatschappij (‘civil society’), en daarmee de burgers, in account neemt en de quintuple helix tevens de natuurlijke omgeving meeneemt (Carayannis et al. 2012). In dit onderzoek is ervoor gekozen de quadruple helix als uitgangspunt te nemen, omdat de burger met de komst van SSI een belangrijke rol krijgt in het zelfstandig beheren van data en de daarbij behorende risico’s zoals privacy en veiligheid om de hoek komen kijken. Dit model integreert niet alleen het belang van de maatschappij, maar voegt de democratie-dimensie toe om kennis te promoten en kennisproductie en innovatie aan te jagen (Carayannis & Campbell, 2022). Co-ontwikkeling en co-evolutie van kennisdiversiteit en heterogeniteit in een kennismaatschappij en kenniseconomie en de kwaliteit van democratie in een gevorderde kennisdemocratie zouden daarbij een rol spelen (Campbell, 2019 in Carayannis & Campbell, 2022). Daarbij is co-creatie tussen overheid, universiteiten, bedrijven en burgers vereist om het ‘leren’ te faciliteren waarmee ‘wicked problems’ mogelijk aangesproken kunnen worden (Bharosa, 2020). Collaboratieve innovatie, verwachtingen, verbeteren van producten (in dit geval: diensten) en nieuwe organisatorische ontwerpen zijn vier dimensies die Caruso (2018) toeschrijft aan ‘de stem van de maatschappij’ die van belang is in de quadruple-helix samenwerking (Steenkamp, 2019).



Afbeelding 6: *Het Quadruple helix model aangenomen door Fraunhofer (2016), ontwikkeld door Carayannis & Campbell (2009) in Schütz et al. (2019, p. 129)*

De quadruple en quintuple helix innovatiesystemen bieden volgens Carayannis en Campbell (2018) een referentie voor beleid en strategie en hoe beleidsinnovatie mogelijk is voor het verbeteren en vooruitgang van een duurzame ontwikkeling. Onderstaande afbeelding illustreert de ontwikkeling van kenniseconomie (triple helix), naar kennis amenleving & kennisdemocratie (quadruple helix) en socio-ecologische transitie (quintuple helix).



Afbeelding 7: *Het Quintuple helix innovatie-model: global warming als uitdaging en drijfveer voor innovatie. (Carayannis et al., 2012, p. 4)*

2.3.4 Governance

In de 14^e eeuw werd de term ‘governance’ uitgelegd als een actie, methode of functioneren van besturen (Halfani et al. 1994).

De term kent een brede set aan definities waaronder ‘de som van de vele wegen die individuen en instituties, zowel publiek als privaat, bewandelen om hun gemeenschappelijke doelstellingen (‘common affairs’) te managen’ (Weiss, 2000) en ‘het samenstel van mechanismen, dat nodig is om ‘het besturen beheersbaar te houden’ (Anderson et al. 2014). Stoker (2006) benoemt de regels en formulieren die collectieve besluitvorming begeleiden; waarbij ‘governance’ niet draait om de beslissing van een individu maar van een groep. Graham et al. (2003) zien governance als de interactie tussen structuren, processen en tradities die bepalen hoe macht en verantwoordelijkheden worden uitgevoerd, beslissingen worden gemaakt en de mate waarin burgers en stakeholders daarin kunnen beïnvloeden. Governance zou gaan over macht, de relatie en verantwoordelijkheid. Daarmee roept het vragen op over wie invloed uitoefent, wie de beslissingen maakt en hoe de beslissingsbevoegden verantwoordelijk worden gehouden (Mayer et al. 1995).

2.3.5 New Public Governance

Ondernemerschap en competitie zijn belangrijke (PPS) drijfveren voor innovatie, maar New Public Governance stelt dat samenwerking de superieure drijfveer van publieke innovatie is (Osborne, 2010). Publieke innovatie is te definiëren als een, min of meer, intentionele inzet om nieuw publiek beleid, diensten, organisaties en procedures te ontwerpen, realiseren en verspreiden die de gevestigde praktijken en het conventionele denken in een bepaald domein ontwrichten (Sørensen & Torfing, 2016). Samenwerking produceert innovatie door gemeenschappelijk en transformatief leren en het genereren van support voor het realiseren van nieuwe disruptieve ideeën (Roberts, 2000).

Wanneer samengewerkt wordt aan complexe problematiek, komt New Public Governance om de hoek kijken. New Public Governance erkent een meervoudige staat, waarbij meerdere wederzijds afhankelijke actoren in netwerken opereren en gezamenlijk een bijdrage leveren aan publieke diensten (Osborne, 2010). “New Public Governance gaat niet zoals bij New Public Management uit van rationeel handelen, maar van organische relaties als basis voor coördinatie” (Osborne, 1997, p. 319).

2.3.6 Collaborative governance

Ansell & Gash (2007) omschrijven in de context van publiek-private samenwerking de term ‘collaborative governance’: *‘a governing arrangement where one or more public agencies directly engage non-state stakeholders in a collective decision-making process that is formal, consensus-oriented, and deliberative and that aims to make or implement public policy or manage public programs or assets’* (Ansell & Gash, 2007, p.544). Collaborative governance, oftewel netwerksamenwerking, is een vorm van besturen waarbij belanghebbenden worden betrokken bij het samenwerkingsproces. Het heeft de potentie om innovatie van publieke diensten te versnellen. Een raamwerk om *collaborative governance* te onderzoeken, is het raamwerk van Ansell en Gash (2007). Startcondities, faciliterend leiderschap en institutioneel ontwerp vormen daarin de context van het samenwerkingsproces (‘collaboration process’).

Startcondities

Startcondities en randvoorwaarden kunnen de samenwerking versterken of ontmoedigen. De onbalans tussen middelen, macht en kennis, de prikkel om te participeren en een voorgeschiedenis van samenwerking of conflict geven samen vorm aan de startcondities (Ansell & Gash, 2008).

Faciliterend leiderschap

Leiderschap wordt als een cruciale component gezien die partijen bij elkaar brengt en in moeilijke tijden hun door het samenwerkingsproces heen sleept. De faciliterende leider heeft de taak om stakeholders bij elkaar te brengen en integriteit in het samenwerkingsproces te verzekeren. Als stakeholders in de samenwerking er niet uitkomen, kan de leider optreden als een mediator (Ansell & Gash, 2008).

Institutioneel ontwerp

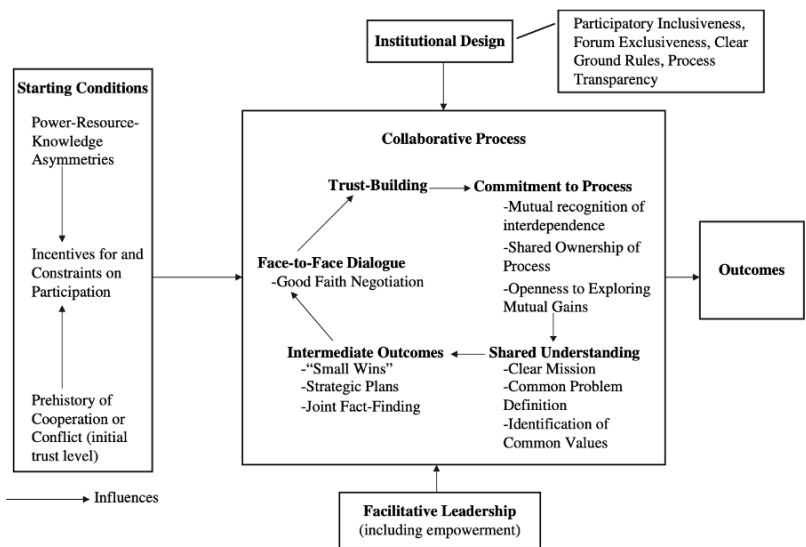
Heldere basisregels zijn van essentieel belang voor de legitimiteit van het samenwerkingsproces. Inclusiviteit en transparantie zijn belangrijke pijlers om bij te dragen aan een succesvolle ‘collaborative governance’ (Ansell & Gash, 2008). Wanneer belanghebbenden niet kunnen deelnemen, worden hun belangen onvoldoende vertegenwoordigd. Openheid en toegang tot samenwerking is belangrijk (Koppenjan & Klijn, 2004).

Koppenjan & Klijn (2004) concluderen ook dat het neerzetten van regels en standaarden voor belanghebbenden het vertrouwen kunnen verhogen, omdat het een goede basis voor alle actoren vormt om op de juiste manier te handelen.

Resultaten

De resultaten van het alsmaar doorlopende samenwerkingsproces zijn afhankelijk van: bouwen aan vertrouwen; communicatie; betrokkenheid bij het proces; wederzijds begrip; tussenliggende uitkomsten en dialoog (Ansell en Gash, 2007). De factor die het meest kritiek is voor succesvolle samenwerking, is vertrouwen (Dunn-Cavelty, 2009).

A Model of Collaborative Governance



Afbeelding 8: Model van Collaborative Governance, Ansell & Gash, 2008, p.550.

Vanuit een netwerkbenadering bekeken (ten opzichte van een centralistisch model) is er vertrouwen en samenspel nodig in plaats van centrale regie en is meer-richtingsverkeer (brengen en halen) de sleutel; het tegenovergestelde van eenrichtingsverkeer en top-down (Brennenraedts et al., 2020)

Centralistisch model	Netwerkbenadering
Eén dominant belang (bijv. nationale veiligheid)	Grote variëteit aan (organisatie) belangen
Centrale regie gewenst	Vertrouwen en samenspel nodig
Formele afspraken noodzakelijk	Informele netwerken, energie en initiatieven vormen de basis
Eenrichtingsverkeer (topdown)	Meer-richtingsverkeer (brengen en halen)
Verplichtend/afdwingbaar door overheid	Vrijwillig/eigenaarschap bij organisaties
Stabiele omgeving	Dynamische omgeving

Afbeelding 9: Centralistisch model vs. Netwerkbenadering, Brennenraedts et al., p.44.

2.4 Publieke waarden & ethiek

“Een waarde is alles wat een mens interesseert.” (Perry, 1968 in Rutgers, 2011)

In het kader van dit onderzoek is het van belang de publieke waarden en ethiek aan te stippen, omdat in de introductie al helder werd dat er zorgen bestaan dat publieke waarden, zoals privacy, voldoende gewaarborgd worden met de komst van SSI.

Ethiek probeert volgens Leppens (2010, p. 5) “criteria vast te stellen om te kunnen beoordelen of een handeling als goed of fout kan worden gekwalificeerd, en om de motieven en consequenties van deze handeling te kunnen evalueren.” Termen die vaak verband houden met ethiek zijn “keuzevrijheid, verantwoordelijkheid, waarheid, aanvaardbaarheid, universaliteit en doel en middelen” (Leppens, 2010, p. 5).

Publieke waarden worden door Bozeman gedefinieerd als de waarden waarover een normatieve overeenstemming bestaat aangaande “de rechten en voorrechten die een burger (al dan niet) toekomen, de verplichtingen van burgers aan de samenleving, de staat en aan elkaar en de principes waarop bestuur en beleid gebaseerd dienen te zijn” (Rutgers, 2011, p. 6). Benington (2011) omschrijft een publieke waarde als: “dat wat het publiek waardeert en dat wat waarde toevoegt aan een publieke omgeving; een democratische ruimte die inclusief is, maar niet samenvalt met de staat” (Andrews, 2019, p. 298). Uit het Kamerstuk ICT (Den Haag, 2021) blijkt dat er aantoonbare kansen liggen om vanuit de overheid belangrijke publieke waarden beter te dienen, waar SSI aan kan bijdragen: “De overheid kan door op te treden als gezaghebbende bron van een betrouwbare digitale identiteit het vertrouwen in het digitaal verkeer vergroten; zelfstandigheid en autonomie van burgers bevorderen; het grondrecht op privacy (beter) waarborgen; het verdienvermogen van Nederland versterken helpen burgers en bedrijven digitaal zaken te doen en administratieve lasten en onnodige kosten te verminderen; cyberveiligheid van burgers en bedrijven bevorderen; door een duidelijke basis van de digitale identiteit infrastructuur kan de overheid een betrouwbare partner zijn voor andere partijen die innovaties willen toevoegen aan dit domein; veilige gegevensuitwisseling; identiteitsfraude tegengaan” (*Kamerstukken II, 2020/21, 26643, nr. 743: p. 3*) Publieke waarden als inclusiviteit en veiligheid kunnen beter georganiseerd worden wanneer leveranciers in de markt gebruik maken van geaccepteerde standaarden en onderdeel zijn van governance-raamwerken waarin goed toezicht op geleverde kwaliteit bestaat (Digitale Overheid, 2020). Rutte-IV, dat op 10 januari 2022 beëdigd werd, wilde een mensgericht digitaal beleid nastreven (Rijksoverheid, 2022).

Dit uit zich het meest nadrukkelijk in het streven mensen een “*eigen online identiteit en regie over hun eigen data*” te geven (Den Boer, 2021). In het coalitieakkoord werd opgenomen het voortouw te nemen en: “in Europees verband in te zetten op versterking van de samenwerking tussen lidstaten op het gebied van digitalisering, onder meer op mensgerichte inzet van kunstmatige intelligentie, digitale ethiek, ontwikkeling van digitale identiteit en cybersecurity en open source” (Coalitieakkoord 2021-2025, 2021, p.30).

In Nederland zal de Wet digitale overheid (Wdo) de basis vormen voor 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 in SSI Speelveldanalyse (BZK, 2021) en met ‘regie op gegevens’ één van de speerpunten van voormalig kabinet Rutte-III. Daarin heeft de overheid speciale aandacht voor ‘regie op de eigen gegevens’ voor kwetsbare en niet-digivaardige burgers, omdat regie op gegevens voor hen zowel kansen als risico's creëert.

2.5 Vertrouwen, risico & vertrouwensmodellen

Met vertrouwen als belangrijk onderzoekselement in deze thesis, is het van belang de definitie van dit begrip te conceptualiseren. Yousafzai et al. (2003, p. 850) verzamelde een aantal definities van vertrouwen, die hieronder uiteengezet zijn in een tabel.

2.5.1 Definities van vertrouwen

850

S.Y. Yousafzai et al. / Technovation 23 (2003) 847–860

Table 1
Definitions of trust

Study	Definition of trust
Rotter (1967)	Trust is “the belief that a party’s word or promise is reliable and a party will fulfil his/her obligations in an exchange relationship”.
Morgan and Hunt (1994)	Trust occurs “when one party has confidence in an exchange partner’s reliability and integrity”.
Mayer et al. (1995)	Trust is “the willingness of a party to be vulnerable to the actions of another party based on the expectation that the other will perform a particular action important to the trustor, irrespective of the ability to monitor or control that other party”.
Rousseau et al. (1998)	Trust is a “psychological state comprising the intention to accept vulnerability based upon positive expectation of the intentions or behaviour of another”.
Gefen (2000)	Trust on an online vendor is the “willingness to make oneself vulnerable to actions taken by the trusted party based on the feeling of confidence and assurance”.
Ba and Pavlou (2002)	Trust is “the subjective assessment of one party that another party will perform a particular transaction according to his or her confidant expectation, in an environment characterised by uncertainty”.

Afbeelding 10: Definities van vertrouwen (Yousafzai et al., 2003, p. 850)

Vertrouwen wordt ook wel als ‘de lijm en het lubricant’ van samenwerking beschreven. De sociale lijm in relaties, groepen en sociale kringen. (Huxham & Vangen, 2004).

Vertrouwen faciliteert de samenwerking en houdt deze samenwerking tegelijkertijd bij elkaar (Bryson et al., 2006, pp. 46-47). Het begrip vertrouwen wordt gezien als een belangrijke voorwaarde voor een succesvolle samenwerking (Huxham & Vangen, 2004). Het zorgt voor wederzijds begrip en uiteindelijk ook een betere inzet van partijen in de samenwerking. Vertrouwen kan uiteindelijk de transactiekosten van de samenwerking verlagen, zorgt voor investering in relaties en stimuleert leren, kennisdeling en innovatie (Emerson et al., 2012, p. 13). Een belangrijke voorwaarde voor vertrouwen, zijn openheid en eerlijkheid in de communicatie (AlAwadhi, 2019; Laan & Sijpersma, 2006). Opvallend aan het rijtje met vertrouwensdefinities is dat vertrouwen vaak wordt gelinkt aan ‘kwetsbaar zijn’ aan de acties van een andere te vertrouwen partij: Mayer et al. (1995, p. 712) zien vertrouwen als “de bereidheid van een partij om kwetsbaar te zijn jegens de acties van een andere partij, gebaseerd op de verwachting dat de andere partij een bepaalde handeling zal uitvoeren richting de vertrouweling, ongeacht of die partij in staat is de andere partij te monitoren of controleren.” Belangrijk is dat de andere partij niet zal reageren op een manier die schadelijk is voor de vertrouwende partij, zal handelen op een wijze die voordelig is voor de vertrouwende partij en op voorspelbare en wederzijds geaccepteerde wijze handelt (Paliszkievicz, 2010). Ba en Pavlou (2002) sluiten daarop aan en verwoorden vertrouwen als “een subjectieve beoordeling van een partij, dat de andere partij een bepaalde transactie uitvoert volgens een verzekerde verwachting, in een omgeving die wordt gekarakteriseerd door onzekerheid” (Yousafzai et al. 2003, p.850).

Vertrouwen is nodig in onzekere situaties, omdat vertrouwen risico’s veronderstelt en kwetsbaarheid vereist van de partijen die in vertrouwen worden genomen; vaak vervangt vertrouwen risico’s, al zal diegene die vertrouwt risico dragen (Hosmer, 1995; Bouckaert and Van de Walle, 2001 in Colesca, 2009). Onder risico’s schaal Vlek (1990, in Hanekamp, 1999, p. 6) “de mogelijkheid van een ongewenst gevolg; een verzameling van mogelijke ongewenste gevolgen en gebrek aan veronderstelde beheersbaarheid.” Risico’s gaan gepaard met vertrouwen en verwachtingen; risico’s zijn bepalend voor vertrouwen (Bouckaert and Van de Walle, 2001 in Colesca, 2009; Nordheim et al., 2019). Vertrouwen kan beschreven worden als “de intentionele en gedragsmatige bereidheid om kwetsbaarheid op te schorten op basis van positieve verwachtingen over een tegenpartij onder condities van risico, afhankelijkheid en onzekerheid” (Oomsels, 2016, p. 3).

Dat een bepaalde partij zich aan zijn woord of belofte houdt en haar verplichtingen nakomt in een wederkerige relatie, aldus Rotter (1967). Vertrouwen is noodzakelijk wanneer er een interactie is tussen twee kanten en tenminste één van die kanten een risico voorziet (McKnight & Chervany, 2002). “Afhankelijkheid tussen partijen is belangrijk, omdat het bouwen aan vertrouwen anders onnodig zou zijn” (Ansell & Gash, 2007, p. 560). Vertrouwen is een betekenisvolle factor in het proces van samenwerken, en vertrouwen behouden vereist het maken van concrete afspraken, oppert Van den Brink (2017).

Het vertrouwen werd met de introductie en uitbreiding van internet een meer prominente zorg. Dat kwam mede door het kwijtraken van de face-to-face interactie die het risico en belang van vertrouwen vergrootte (Pavlou, 2003). Vertrouwen verwijst naar een afhankelijkheid in het vermogen en de integriteit of het karakter van een persoon of een zaak en betekent dat degene die het vertrouwen verleent erop kan vertrouwen dat degene die het vertrouwen verkrijgt zal zorgen voor de belangen of voordelen van degene die het vertrouwen verleent, en dat degene die het vertrouwen verleent vertrouwt op het resultaat dat wordt verstrekt door de in vertrouwen genomen persoon of instantie, ook al is het resultaat niet direct zichtbaar (Kini en Choobineh, 1998). Vertrouwen helpt om een relatie tussen twee partijen te bouwen of behouden (Zaltman en Moorman, 1988).

2.5.2 Soorten vertrouwen

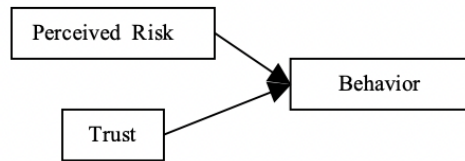
De Mul (2016) onderstreept drie soorten vertrouwen: basaal vertrouwen (‘basic trust’); interpersoonlijk vertrouwen en systeemvertrouwen. Basaal vertrouwen heeft een blind karakter, dat zelfs wanneer het wordt beschadigd, vaak nog standhoudt. Het is bijvoorbeeld het vertrouwen van een kind dat het, als vanzelfsprekend, door zijn of haar ouders gevoed wordt. Interpersoonlijk vertrouwen speelt vaak tussen personen. Het is geen vanzelfsprekendheid zoals basaal vertrouwen vaak is, maar is gebaseerd op (gemeenschappelijke) ervaringen. Deze vorm van vertrouwen is minder diep verankerd dan basaal vertrouwen en brengt een groter bewustzijn van mogelijke risico’s met zich mee. De derde vorm van vertrouwen is systeemvertrouwen; ook wel onpersoonlijk vertrouwen of omgevingsvertrouwen genoemd. Het systeemvertrouwen heeft betrekking op een functionerend systeem of een institutie, zoals de overheid. Dit vertrouwen bestaat uit twee dimensies: structurele zekerheid en situationele normaliteit. Bij structurele zekerheid is de verwachting dat succes een waarschijnlijkheid is omdat er bepaalde voorwaarden gecreëerd zijn, zoals beloften, contracten, regels en garanties. Bij situationele normaliteit is de verwachting dat succes waarschijnlijk is, omdat de situatie normaal is.

Dat houdt in dat iets goed gaat omdat het in eerdere vergelijkbare situaties ook goed gegaan is (Yousafzai et al., 2003). Binnen systeemvertrouwen speelt ook interpersoonlijk vertrouwen een rol. Zo zijn het diverse ambtenaren die ervoor zorgen dat het systeemvertrouwen tot stand komt, in stand gehouden wordt, of hersteld dient te worden. Het bewustzijn van de risico's is hier minder dan bij interpersoonlijke interacties. Zo lang het systeem functioneert, is er weinig aan de hand. Crasht het systeem, dan worden burgers met de neus op de feiten gedrukt. Voorbeelden hiervan zijn de toeslagenaffaire en het neerhalen van de MH17. Opmerkelijk aan deze vorm van vertrouwen is dat wanneer deze vorm van vertrouwen beschadigd wordt, we vaak snel met de vinger naar de verantwoordelijken wijzen. Dat is vaak de overheid, die als belangrijkste taak heeft om te waken over onze veiligheid. Bij interpersoonlijk vertrouwen zijn we juist geneigd eerst onze eigen goedgegeloofigheid als 'verantwoordelijk' aan te wijzen (De Mul, 2016).

Vertrouwen is ook afhankelijk van de vertrouwdheid die we hebben met de omgeving (De Mul, 2016). Sec gezegd: we voelen ons veiliger en meer vertrouwd in onze eigen leefomgeving dan in een vreemde stad. Verandering van spijs doet wellicht niet alleen eten, maar ook vrezen. Een onbekende weg bewandelen, brengt onzekerheden en risico's met zich mee. Andere kernwoorden die meerdere malen worden benoemd in de omschrijving van vertrouwen zijn betrouwbaarheid, integriteit en het wederzijds voldoen aan (positieve) verwachtingen (Yousafzai et al, 2003).

2.5.3 Risico in relatie tot vertrouwen

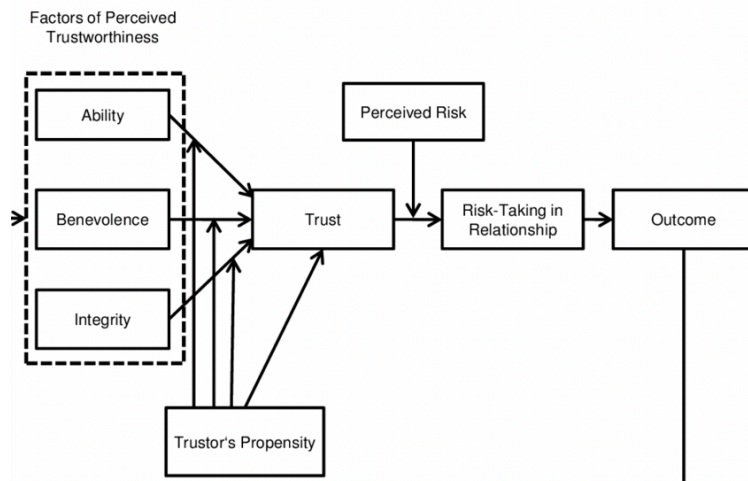
Vertrouwen zou niet nodig zijn geweest als er geen risico's hadden bestaan en wanneer acties met complete zekerheid genomen kunnen worden. Het element risico geeft het vertrouwensdilemma het basiskarakter. Dat is wat Johnson-George en Swap (1982) benadrukken. Veel onderzoek naar vertrouwen sluit het helder krijgen van de relatie tussen vertrouwen en risico uit (Yousafzai et al., 2003). Mayer et al. (1995) geven aan dat het onzeker is of risico een antecedent van vertrouwen is, vertrouwen is, of een uitkomst van vertrouwen is. Het artikel van Olson & Olson (2000) conceptualiseert vertrouwen als "de consequentie van het waargenomen risico (Olson & Olson in Gefen, 2003, p.8)." Het vertrouwen is groter wanneer de inzet laag is en het potentiële verlies minuscule is (Gefen, 2003). Ook controle speelt een rol, omdat controle en risico met elkaar samenhangen. Wanneer er meer controle is, is er sprake van minder risico (Das & Teng, 2001 in Geutjes, 2013).



Afbeelding 11: De perceptie van het risico en het begrip vertrouwen hebben een onafhankelijke invloed op gedrag (Gefen et al., 2003, p. 6)

2.5.4 Vertrouwensmodellen

2.5.4.1 Model of trust (Mayer, 1995)



Afbeelding 12: Naar een formatief meetmodel voor vertrouwen. (Mayer, Davis and Schoorman, 1995, p. 715)

Vertrouwensmanagement kent de volgende karakteristieken:

- het *vermogen* ('ability') (kennis, vaardigheden, gedrag en kwalificatie) die leiden tot verbeterd vertrouwen;
- *welwillendheid* ('benevolence'); het kunnen tonen van empathie en compassie en
- *integriteit*; het tonen van eerlijkheid en morele en ethische beginselen.

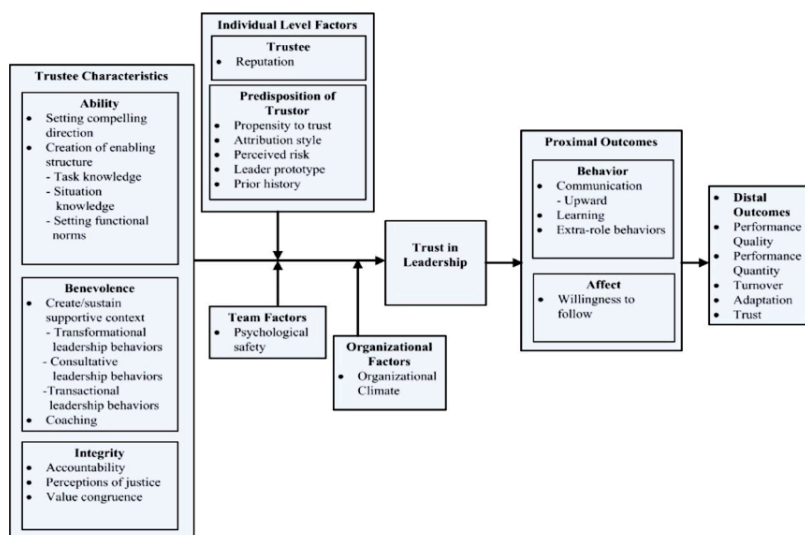
Daarnaast zijn van belang communicatie, congruentie, consistentie, afhankelijkheid, openheid, betrouwbaarheid en transparantie (Paliszkievicz et al., 2015).

Het *vermogen* wordt ook wel omschreven als de groep van vaardigheden, competenties en karakteristieken die een partij in staat stellen om invloed te hebben in een bepaald domein (Mayer et al., 1995).

Welwillendheid betekent ook dat degene die vertrouwd wordt, het voordeel van degene die het vertrouwen verleent, meeneemt wanneer er besluiten genomen moeten worden inzake de informatie van degene die het vertrouwen verleent (Lee & Turban, 2001).

Een veelgebruikte definitie voor *integriteit* is “het handelen overeenkomstig de (daarvoor) geldende morele waarden en normen en de daarmee samenhangende (spel)regels” (Huberts, 2015, p. 15). Huberts (2015) identificeert zes verschillende visies op integriteit: als heelheid, als professionele verantwoordelijkheid, als specifieke waarde of als ideaal en het dient overeen te stemmen met zowel wet- en regelgeving als met normen en waarden (Huberts, 2005). Waar integriteit, welwillendheid en vermogen heel erg inzetten op het menselijke aspect, worden de aspecten betrouwbaarheid (‘reliability’), functionaliteit en behulpzaamheid geassocieerd met technologie (McKnight et al., 2017 in Zarifis et al., 2022).

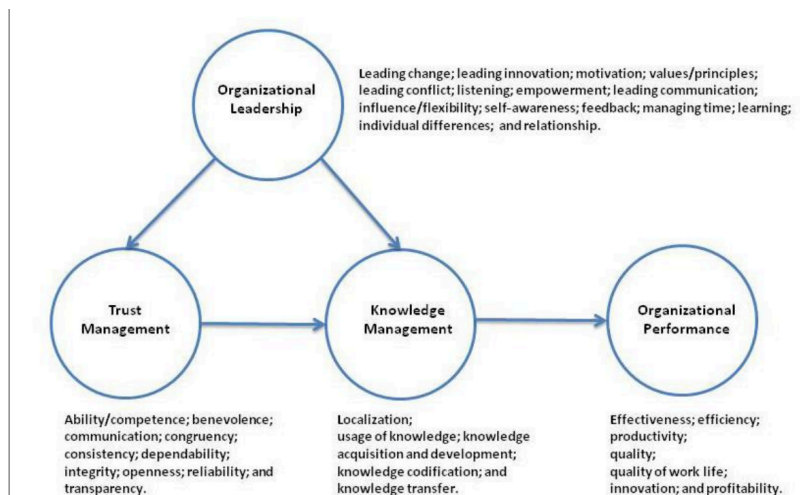
2.5.4.2 Trust in leadership model (Burke et al., 2007)



Afbeelding 13: Multi-level framework voor het begrijpen van vertrouwen in leiderschap (Burke et al., 2007, p. 613).

2.5.4.3 *Model for Achieving Successful Organizational Performance*
(Paliszkiewicz et al., 2015)

Met het ‘model of trust’ (Mayer, 1995) en ‘trust in leadership’ framework (Burke et al. 2007) als basis, ontwikkelde Paliszkiewicz et al. (2015) het ‘Model for Achieving Successful Organizational Performance’ dat het effect van vertrouwensmanagement op kennismanagement meet en vervolgens kennismanagement op de prestatie van de organisatie meet; maar ook het effect van leiderschap op vertrouwens- en kennismanagement meet. Leiderschap wordt in dit onderzoek meegenomen om de relatie tot vertrouwensmanagement in kaart te kunnen brengen. Leiderschap is cruciaal voor het omarmen, empoweren en betrekken van stakeholders en ze richting samenwerking te laten bewegen (Vangen & Huxham, 2003).



Afbeelding 14: *Model voor het bereiken van succesvolle organisatorische prestatie*
(Paliszkiewicz et al., 2015, p.23)

2.5.5 Leiderschap in relatie tot vertrouwen

In de inleiding werd het al aangestipt: leiderschap is noodzakelijk voor het creëren en behouden van duidelijke basisregels, opbouwen van vertrouwen, faciliteren van dialoog en het verkennen van wederzijdse winst (Ansell & Gash, 2008).

Wanneer er intensief wordt gestuurd op datgene wat nodig is in de samenwerking, kan dit vertrouwen opbouwen (Ysa et al., 2014). Wanneer naar vertrouwen en samenwerking gekeken wordt, kan “vertrouwen alleen ontwikkeld worden door samenwerking, dat op haar beurt weer afhankelijk is van vertrouwen,” (Dunn-Cavelty & Suter, 2009, p. 182). Zij concluderen dat vertrouwen tussen partners en/of partijen het sleutelaspect is voor succesvolle samenwerking. Om gezamenlijk vertrouwen op te bouwen zijn zaken belangrijk als het investeren in de relatie, het vergroten van transparantie, begrip hebben voor de uitdagingen waar elke partij voor staat en erop vertrouwen dat er positieve winst te behalen is voor alle partijen (Carr, 2016). Wederkerig vertrouwen (‘mutual trust’) wordt aangestipt als belangrijker dan controle en regulatie (Dunn-Cavelty & Suter, 2009).

Het omarmen van belanghebbenden (stakeholders) en ze in staat stellen mee te denken en te betrekken kunnen een uitwerking zijn van leiderschap (Ansell & Gash, 2008). Volgens Paliszkievicz et al. (2015) kent leiderschap vijftien karakteristieken: het leiden van verandering, het leiden van innovatie, motiveren, het besteden van aandacht aan waarden, durf om het conflict aan te gaan, luistervaardigheid, empowerment, communicatie, bereidheid om feedback te geven en ontvangen, invloedrijkheid en flexibiliteit, zelfbewustzijn, het vermogen om te leren, timemanagement, diversiteit en inclusie en het vermogen om relaties te bouwen en onderhouden.

2.6 Policy & polity

2.6.1 De veranderende samenleving met digitale technologie als sturende kracht

De samenleving staat voor ingrijpende veranderingen, door de snelle ontwikkelingen van technologie. Het World Economic Forum spreekt zelfs van een nieuwe, vierde, industriële revolutie, waarbij digitale technologie de sturende kracht is (Mulder, 2019; WEF, 2018).

Koppenjan en Klijn (2004) vatten de steeds complexer wordende samenleving samen in een aantal uitgangspunten, waaronder het ontstaan van nieuwe onzekerheden door ontwikkeling van kennis en technologie, het vervagen van grenzen door toegenomen globalisering en een hiërarchische relatiestructuur die verandert in horizontale netwerken. Alle betrokken partijen; publiek en privaat staan kriskras met elkaar in verbinding. Deze netwerksamenwerking kenmerkt zich dan ook door het ontbreken van duidelijke grenzen (Castells, 2000). De rol van de overheid en het beleid van de overheid dienen zich aan te passen op deze ontwikkelingen om mee te kunnen bewegen.

2.6.2 Beleid en de rol van de overheid

Volgens Mulder (2019) bekleedt de overheid twee belangrijke rollen:

de eerste is een beleidsmatige rol (het beleid van de overheid; ‘policy’). De tweede rol gaat in op de transformatie van de rol van de overheid (als institutionele entiteit) en het functioneren ervan: ‘polity’. Met beleid wordt bedoeld: “alle voornemens, keuzes en acties van één of meer bestuurlijke instanties gericht op de sturing van een bepaalde maatschappelijke ontwikkeling” (Map en ’t Hart, 2011, p. 16). Wanneer men spreekt over het vormen van beleid, gaat het om het bespreken, analyseren en onderhandelen om tot plannen en programma’s te komen.

Daarbij gaan diverse partijen aan de slag om elkaar te overtuigen van hun visie om sturing te geven aan maatschappelijke ontwikkelingen die tot politieke beslissingen leiden (MAP en ’t Hart, 2011). Bij een quadruple helix-benadering worden ook de burgers daarbij betrokken en kunnen zij een bijdrage leveren door hun visie kenbaar te maken en mee te denken tijdens het proces. Volgens Mulder (2019) is het de vraag hoe de overheid ervoor zorgt dat de samenleving en economie de nieuwe technologie oppakken en daarbij naar kansen en mogelijkheden enerzijds en risico’s en bedreigingen anderzijds kijkt. Tijdens dit onderzoek wordt in de vragenlijst aan burgers gevraagd naar hun visie op SSI en de kansen, mogelijkheden, risico’s en bedreigingen die er in hun optiek kunnen ontstaan. Zij krijgen een mogelijkheid om mee te denken richting beleid en bijbehorende beleidsinstrumenten die kracht bij kunnen zetten. Een beleidsinstrument is een middel dat wordt ingezet om beleid te voeren en kan communicatief en informatief, financieel-economisch of juridisch van aard zijn (Van Damme & Pattyn, 2015).

De overheid is een institutionele entiteit (‘polity’). Volgens Mulder (2019) onderschatten bestuurders de impact van nieuwe technologie en het effect dat nieuwe technologie heeft op het functioneren van de overheid. De transformatie van de rol en het functioneren van de overheidsinstantie zelf, zijn hier aan de orde.

De overheid kan vanuit haar rol op diverse wijzen aansturen. Toch kunnen er grofweg drie basisstrategieën onderscheiden worden met het oog op beleidsvoering: sturing volgens de logica van hiërarchie (macht en eenzijdig overheidsoptreden), de markt (geld) of het netwerk (samenwerking). Een gecombineerde strategie is tevens een optie (Van Damme & Pattyn, 2015). De vraag vanuit de rol van de overheid is welke nieuwe beleidsmodellen mogelijk zijn en organisatievormen aansluiten (Mulder, 2019). In Reijmerink (2003) worden vier beleidsmodellen onderscheiden: rationeel, incrementeel, synoptisch en gemengd. Bij een rationeel beleidsmodel wordt het probleem gedefinieerd dat opgelost moet worden en daarna worden top-down oplossingen bedacht.

Vaak wordt het proces lineair doorlopen en is er één actor met volledige macht. Bij een incrementele benadering, worden vaak meerdere actoren betrokken, waardoor er met meerdere doelen rekening gehouden kan worden. In kleine stappen vooruit wordt toegewerkt naar een verandering. Vaak zijn de volgorde van stappen uit de beleidscyclus chaotisch (non-lineair). Geen van de actoren heeft exclusieve macht (Snijkers, 2005). In een synoptisch model wordt het hele proces lineair en volledig doorlopen en is er vaak één actor met macht waarbij een acceptabele beslissing goed genoeg is. Bij een gemengd beleidsmodel wordt er strategisch gekozen uit de volgorde van de stappen in de beleidscyclus en bestaan er meerdere actoren met beperkte beslissingsmacht. Over de belangen van stakeholders is te onderhandelen (Reijmerink, 2003).

De relatie tussen overheid en burger is de afgelopen jaren complexer geworden en dat heeft implicaties voor het voeren van beleid. Een overheid die hiërarchisch en eenzijdig optreedt is steeds minder vanzelfsprekend. De kennis en capaciteiten van burgers is enorm toegenomen en een burger die geïnformeerd is zal sneller overheidsautoriteit – en optreden ter discussie stellen. Ook zal er eerder protestgedrag ontstaan vanuit burgers, wanneer er een indruk bestaat dat belangen in het geding zijn. Bovendien heeft er verschuiving plaatsgevonden van de maatstaven die een burger inzet bij de waardering van beleid en beleidsprocessen (Bekkers & Ringeling, 2003). Naast de vraag of de overheid wel doet wat wettelijk afgesproken is (legaliteitsnormen genoemd), is er meer aandacht voor democratische en integriteitsnormen. Heeft de overheid alle belangen meegenomen in haar besluitvorming, is er sprake van transparantie en worden keuzes gemotiveerd? (Popelier et al. 2008 in Van Damme & Pattyn, 2015).

Dat leiderschap en beleid een effect hebben op vertrouwen en vertrouwensmanagement - en samenwerking (co-creatie) en leren kan bevorderen - is in de voorgaande theorie aangeduid (in o.a. de vertrouwensmodellen van Burke et al. 2007 en Paliszkievicz et al., 2015). Welke gewenste (leiderschaps)rol en bijbehorende (beleids)acties burgers voor de overheid zien, is relevant om samenwerking met alle quadruple helix-actoren en vertrouwen in SSI mogelijk(er)wijs te kunnen bevorderen. Deze vraag wordt in dit onderzoek gesteld om mogelijk aanbevelingen te kunnen doen die inzicht geven in het verbeteren richting een vertrouwen-bevorderende rol en antwoord hoopt te geven op de overkoepelende onderzoeksvraag.

3 Methoden

Wat kan de overheid bieden om samen met quadruple helix actoren verder te bouwen aan vertrouwen van burgers in de (mogelijke) komst en adaptatie van Self-Sovereign Identity (SSI)?

Bij de gestelde onderzoeksvraag is gezocht naar een passende onderzoeksmethode.

3.1 Onderzoekstype

Gekozen is voor een exploratief onderzoek dat kwalitatief van aard is. Een dergelijk kwalitatief onderzoek is “interpreterend, waarbij empirische gegevens op een controleerbare wijze worden verzameld, geanalyseerd, en gerapporteerd” (Zwieten & Willems, 2004; Plochg & Van Zwieten, 2007, p. 77). De onderzoeksfasen kunnen daarbij door elkaar heen lopen. Een bijkomend voordeel aan kwalitatief onderzoek is dat er “met een open blik bestudeerd kan worden” (Boeije, 2005, p. 148). Door inzet van een vrij globale onderzoeksvraag, kan flexibel ingespeeld worden op dat wat empirisch wordt waargenomen (Plochg & Van Zwieten, 2007). De verkennende (deel)vragen die gesteld zullen worden, zijn open en veronderstellen dat er nog niet voldoende kennis over bestaat in het onderzoeksdomein (Van Thiel, 2015). Het doel van dit onderzoek is om op breed niveau meer inzicht te verkrijgen in het fenomeen ‘vertrouwen in SSI’ in relatie tot de (gewenste) rol van de overheid en de inzet van beleid; ook om (quadruple helix) samenwerking te bevorderen. Hierbij staan centraal: het exploreren van meningen, opvattingen, ervaringen, waarden en belangen vanuit het perspectief van de burgers ten opzichte van de verschillende participerende actoren uit de quadruple helix: wetenschap, overheid en bedrijfsleven. Het stimuleren van vertrouwen en meer inzicht verkrijgen in gewenst leiderschap en beleid, in relatie tot de komst van de (mogelijk) nieuwe technologie SSI, worden hierbij in acht genomen (Plochg en Van Zwieten, 2007). In de onderzoeksfase worden de vragen zo ingezet dat er ruimte ontstaat om vanuit openheid op zoek te gaan naar verbetermaatregelen (aangaande de rol van de overheid) en mogelijkheden voor de (mogelijke) komst en adaptatie van SSI, waardoor er raakvlakken zijn met een ontwerpvraag (Van Thiel, 2015); de hoofddoelstelling blijft echter exploratief. Het onderwerp raakt zowel inductief als deductief onderzoek. Deductief onderzoek zoekt naar een verklaring in de bestaande theorie (Van Thiel, 2015).

In dit geval wordt bestaande literatuur en wetenschappelijke theorie gebruikt om de basis van begrippen als vertrouwen, samenwerking en leiderschap in kaart te brengen. Omdat SSI een nieuw thema is en daar nog weinig informatie over bestaat, is inductief verkennend onderzoek leidend, waarbij nieuwe informatie wordt verzameld (Van Thiel, 2015).

3.2 Onderzoeksonwerp

Zowel desk- als fieldresearch worden ingezet; waarbij deskresearch (bureau-onderzoek) zich richt op bestaande data en fieldresearch (veldonderzoek) uitgaat van het verzamelen van nieuwe data. Deskresearch is uitgevoerd door wetenschappelijke literatuur op Google Scholar te bestuderen op diverse momenten tussen 2020 en 2023. Dit heeft theoretische constructen en (vertrouwens)modellen en begrippen inzichtelijk gemaakt rondom thema's die samenhangen met SSI en vertrouwen en onderling vaak ook verband met elkaar houden. Denk aan thema's als digitale en collaboratieve innovatie, governance, leiderschap, samenwerkingsontwikkelingen, publieke waarden en ethiek, risico en vertrouwensmodellen. Het doel hiervan is om een stevige achtergrond neer te kunnen zetten en te begrijpen welke (bestuurskundige) ontwikkelingen een rol gespeeld hebben om te komen tot waar we anno 2023 op het gebied van beleid en de rol van de overheid staan in relatie. Ook in relatie tot SSI. Een stukje historie van bestuurskundige ontwikkelingen is in kaart gebracht (zoals decentralisering, publiek-private samenwerking en New Public Management). Dit om governance en leiderschap in de loop der tijd beter te kunnen begrijpen en in verband te kunnen brengen met vooruitstrevende disruptieve, technologische ontwikkelingen als SSI. Omdat SSI een nieuwe technologie is en daarover nog weinig bekend is danwel gepubliceerd is binnen de wetenschap, wordt de literatuur waar nodig aangevuld met bevindingen uit de media zoals (online) kranten en bestuurskundige literatuur (zoals iBestuur). Vervolgens wordt een kwalitatieve online vragenlijst, die veelal bestaat uit open vragen, als fieldresearch ingezet om nieuwe onderzoeksresultaten en invalshoeken te genereren die kunnen bijdragen aan het beantwoorden van de onderzoeksvraag. De literatuur wordt hierbij gebruikt als achtergrond om de empirische data, verkregen als respons op de vragenlijsten, te kunnen duiden.

3.2.1 Kwalitatieve vragenlijst

Een vragenlijst wordt vaak ingezet om feiten, gedrag, meningen, kenmerken of sociale verschijnselen in kaart te brengen. Vaak wordt er bij de inzet van een vragenlijst een steekproef getrokken om de doelgroep te kunnen onderzoeken. De vragenlijst legt de nadruk doorgaans op ontwikkelingen; (maatschappelijke) veranderingen die interessant zijn (Boeije et al., 2016). De (mogelijke) komst van nieuwe technologie als SSI, eveneens een verandering met impact, leent zich goed voor een vragenlijst en kan meningen en ideeën opleveren. Een kwalitatieve vragenlijst heeft als uitgangspunt zo veel mogelijk informatie te verzamelen rondom kennis, houding en gedrag van de doelgroep ten opzichte van het te onderzoeken fenomeen. In dit geval is er gekozen voor een gestructureerde online vragenlijst, waarbij de volgorde van vraagstelling vaststaat, waarbij zo veel mogelijk rekening is gehouden om de respondenten op logische, zelfstandige wijze door de vragenlijst te sturen. Boeije et al. (2016) noemt als voordelen van een online vragenlijst dat het snel is; er vaak minder fouten in een vragenlijst zitten door een juiste routing en er betere controle is op de consequenties van gegeven antwoorden (bijvoorbeeld minder onduidelijkheden in reacties op open vragen).

Hoewel online vragenlijsten veelal tot kwantitatief onderzoek behoren, kan met een kwalitatieve online vragenlijst, die voor dit onderzoek wordt uitgezet via LinkedIn, een gedeelte van de doelgroep snel en anoniem benaderd worden. In dit geval wordt er bij deelname aan het onderzoek wel om mailadressen gevraagd, omdat er een managementboek verloot wordt om meer mensen te bewegen de vragenlijst, waar met 20 vragen wat tijd en inzet voor vereist is, in te vullen en zo non-respons tegen te gaan en het responspercentage te verhogen. Een beloning koppelen om deelname aan het onderzoek te vergroten, leidt niet altijd tot een hogere respons, maar wordt wel ingezet om de motivatie voor deelname aan het onderzoek te verhogen (Dillman et. Al, 2000 in Van Thiel, 2015).

3.2.2 Het samenstellen van de online vragenlijst

Verskillende theoretische concepten staan met elkaar in verbinding als het gaat om vertrouwen en de (mogelijke) implementatie van een nieuwe technologie als SSI. De eerste twee deelvragen van het onderzoek zijn: wat is vertrouwen en welke theoretische concepten vormen een basis om te bouwen aan vertrouwen? Deze worden beantwoord aan de hand van literatuuronderzoek in het theoretisch kader. Het theoretisch kader vormt een onderzoekslens waaraan de vragen in de vragenlijst opgehangen worden.

Uit een uitgebreide eerste literatuurstudie naar verbanden met SSI, vertrouwen, ‘polity en policy’ en leiderschap, zijn de volgende onderwerpen naar voren gekomen: ‘samenwerking’ (‘collaboratie’ en ‘collaboratieve innovatie’), ‘vertrouwen’ en ‘soorten vertrouwen’, onder policy: ‘risico’s en bedreigingen’, ‘kansen en mogelijkheden’ en ‘communicatie’, onder polity: ‘rol van de overheid’, ‘vermogen, welwillendheid en integriteit’ (ABI-model) onder vertrouwensmodellen. ‘Publieke waarden’ (zoals ‘veiligheid’) zijn verweven door het volledige onderzoek. De quadruple helix richt zich op een samenwerking van verschillende actoren: de rol van overheid, wetenschap, bedrijfsleven en burgers (‘rol van de wetenschap’, ‘rol van de overheid’, ‘rol van het bedrijfsleven’, ‘rol van de burger’, ‘quadruple helix’). De definities van deze te onderzoeken concepten zijn uitgezet in het theoretisch kader en dienen als leidraad om meer inzicht te krijgen in dat wat er onder burgers speelt rondom de (mogelijke) komst en adaptatie van SSI en onderlinge samenhang te ontdekken. Er wordt ook wel gesproken van ‘sensitizing concepts’, oftewel “begrippen die de onderzoeker gevoelig maken voor bepaalde aspecten van de te onderzoeken werkelijkheid, deze zijn attenderend, richtinggevend en verkennend” (Smaling, 2021, p. 65-66). Vooral over de samenhang van de concepten in relatie tot SSI is nog weinig bekend en dit onderzoek zorgt voor precisering van zowel de inhoud van de concepten als de samenhang daartussen. De vragen die in de vragenlijst gesteld worden, refereren naar deze samenhangende concepten. Bij het opstellen van de vragenlijst worden de verschillende theorie-paragrafen als basis gebruikt. De vragen worden gestructureerd weergegeven in een tabel waarbij in de kantlijn begrippen gezet zijn, die aangeven waar deze vragen informatie over kunnen verzamelen. Elke paragraaf staat voor een informatiespoor zoals is weergegeven in afbeelding 1 op pp. 19-20, te weten:

informatiespoor 1: digitale & collaboratieve innovatie (2.1) en sub-spoor Self-Sovereign Identity: een disruptieve technologie (2.2); informatiespoor 2: governance & samenwerking (2.3); informatiespoor 3: publieke waarden & ethiek (2.4) & sub-spoor vertrouwen, risico en vertrouwensmodellen (2.5) en daar waar de sporen uitkomen; kern van het onderzoek: policy & polity (2.6).

De vragenlijst wordt opgemaakt in Google Forms en bestaat uit 20 vragen en zijn voor de onderzoeker genummerd ondergebracht onder de diverse informatiesporen en de ‘policy en polity’ kern. Bij het opstellen van de vragen wordt getracht zo min mogelijk te sturen en zo veel mogelijk open vragen te stellen, zodat er volop ruimte ontstaat voor respondenten om zo open en eerlijk mogelijk te antwoorden en eigen denkkraft om te zetten naar ideeën die mogelijkwjs bijdragen aan verbetering rondom de (mogelijke) komst en adaptatie van SSI.

Zo min mogelijk beïnvloeding en sturing stimuleert de betrouwbaarheid van het onderzoek. De respons van de respondenten wordt geanonimiseerd weergegeven in het onderzoek, mede om een open en veilige omgeving te kunnen garanderen waarbij respondenten kunnen aangeven waar zij in relatie tot SSI tegenaan lopen in termen van vertrouwen en leiderschap.

Hoofdstuk & paragraaf	Thema & vraagstelling	Open codes verbonden aan theoretisch kader
Informatiespoor 1:	Digitale & collaboratieve innovatie	
2.1	Digitale & collaboratieve innovatie	Collaboratieve innovatie
2.2	Self-sovereign identity: een disruptieve technologie	
	1) Ben je bekend met het begrip Self Sovereign Identity (SSI) oftewel digitale identiteit?	SSI; Communicatie/informatievoorziening
	2) Is er volgens jou voldoende informatie (kennis) beschikbaar om een houding ten opzichte van SSI te kunnen aannemen?	Communicatie/informatievoorziening
	3) Heb jij een bepaalde informatiebehoefte t.o.v. het onderwerp SSI om je beter geïnformeerd te voelen?	Communicatie/informatievoorziening
	4) Hoe sta je tegenover SSI op basis van de informatie die hierover bij jou bekend is?	Houding burgers t.o.v. kennis
	10) Heb jij in relatie tot SSI ergens zorgen over?	Zorgen en risico's; relatie tot vertrouwen
Informatiespoor 2:	Governance & samenwerking	
2.3	Governance & samenwerking	
	6) Vind je dat er naast de overheid andere partijen (wetenschap, burgers, bedrijfsleven) aan te wijzen zijn die kunnen helpen om vertrouwen in nieuwe technologie als SSI te verstevigen? Geef per tak aan hoe zij kunnen helpen.	Quadruple helix-werking; rollen; relatie tot vertrouwen
	6 a) Wat kan de wetenschap doen om jou te helpen om vertrouwen in nieuwe technologie als SSI te verstevigen?	Rol van de wetenschap; quadruple helix; relatie tot vertrouwen
	6 b) Wat kan het bedrijfsleven doen om jou te helpen om vertrouwen in nieuwe technologie als SSI te verstevigen?	Rol van het bedrijfsleven; quadruple helix; relatie tot vertrouwen
	6 c) Wat kunnen burgers en/of jijzelf doen om jou te helpen om vertrouwen in nieuwe technologie als SSI te verstevigen?	Rol van de burgers; quadruple helix; relatie tot vertrouwen
	7) Hoe denk jij dat de diverse partijen beter kunnen samenwerken om technologische innovaties als SSI beter te kunnen ondersteunen?	Quadruple helix-werking; samenwerking; relatie tot vertrouwen
	9) Digitale identiteit betekent ook dat je meer controle over je eigen databeheer krijgt. Hoe zie jij jouw eigen rol als burgers wanneer je beseft dat het beheer van jouw gegevens bij jou komt te liggen?	Rol als burgers; (zelf)vertrouwen in relatie tot autonoom databeheer
Informatiespoor 3:	Publieke waarden & ethiek	
2.4	Publieke waarden & ethiek	Vertrouwen, risico & vertrouwensmodellen
	16) Welke publieke waarden spelen voor jou een rol bij het verstevigen van een vertrouwenspositie bij het invoeren van een innovatie als SSI?	Publieke waarden; relatie tot vertrouwen
	17) Welke waarde is voor jou het meest belangrijk? En waarom?	Publieke waarden; persoonlijke waarden
	18) Signaleer jij risico's rondom SSI in relatie tot jouw waarden? Zo ja, welke?	Publieke waarden; risico's; zorgen
	19) Hoe zouden optionele risico's naar jouw mening geminimaliseerd kunnen worden om jouw waarden te beschermen?	Publieke waarden; veiligheid; beschermen van waarden; risico's

Hoofdstuk & paragraaf	Thema & vraagstelling	Open codes verbonden aan theoretisch kader
2.5	Vertrouwen, risico en vertrouwensmodellen	
	8) Hoe sta je qua vertrouwen tegenover digitale uitwisseling van (digitale) gegevens die voor jou belangrijk zijn?	Vertrouwen; digitalisering; data
	12) Hoe verwacht je dat de verschillende betrokken partijen met jouw (digitale) data omgaan?	Vertrouwen; rolverdeling; quadruple helix; data
2.6 De kern	Policy & polity	
	5) Wat kan de overheid volgens jou bieden om verder te bouwen aan vertrouwen van burgers rondom de mogelijke komst en ingebruikname van SSI?	Rol van de overheid; relatie tot vertrouwen
	11) Wat kan de overheid doen om ervoor te zorgen dat jij je veilig en gesterkt voelt in het beheren van jouw eigen gegevens en de (mogelijke) komst van SSI?	Rol van de overheid; polity; publieke waarden; veiligheid
	13) Wat vind je dat de overheid kan doen om erop toe te zien dat de uitrol en (mogelijke) ingebruikname van SSI goed verloopt? Welke rol kan de overheid hierin aannemen? Voorbeelden: * Wijze van communiceren veranderen; hoe zou je geïnformeerd willen worden? * Het (mogelijk) bestaan van bepaalde zorgen wegnemen; als deze bestaan, hoe kunnen deze weggenomen of verminderd worden? * Het opstellen van heldere kaders en regelgeving rondom SSI.	(Gewenste) rol van de overheid
	14) Waar zie je kansen en mogelijkheden rondom SSI? Beschrijf deze.	Policy; kansen & mogelijkheden
	15) Zie jij risico's en bedreigingen rondom SSI? Zo ja, welke?	Policy: risico's & bedreigingen
Algemeen	Aanvullingen op het onderzoek	
	20) Heb je nog vragen, opmerkingen of aanvullingen? Noteer ze dan hier.	Open

Boeije et al. (2016) onderscheidt drie typen vragen: open, gesloten en halfopen vragen. Volgens Boeije et al. (2016) stelt een onderzoeker open vragen om te achterhalen wat er aan antwoorden mogelijk is en wanneer men benieuwd is naar de associaties die de vraagstelling naar boven haalt. Singleton & Straits (2005) concluderen dat een open vraag de respondent ruimte geeft om een eigen antwoord te geven die kan leiden tot belangrijke informatie, denkprocessen, de kracht van mening of gevoelens en de hoeveelheid informatie. Als nadelig feit van open vragen wordt genoemd dat ze lastiger te coderen en te analyseren zijn en dit tijdrovend is (Singleton & Straits, 2005). In dit onderzoek zijn 16 open vragen gebruikt. Ook worden er vragen ingezet waarbij meerdere keuze-opties geselecteerd kunnen worden; bijvoorbeeld om de publieke waarden in kaart te brengen. Daar zit om uitsluiting van andere antwoorden te voorkomen altijd een 'open' invulveld als optie bij om zelf aan te kunnen vullen wanneer er informatie ontbreekt.

Open vragen	Open vragen met voorbeelden	Meerkeuze-vragen met open invulveld
3, 4, 5, 6, 7, 9, 11, 12, 14, 15, 17, 18, 19, 20	10, 13	1, 2, 8, 16

Er wordt rekening gehouden met een logische volgorde ('routing') in de vraagstelling om de respondent eenvoudig door de vragenlijst te begeleiden. Genoemd moet worden dat aan de begrippen SSI en digitale identiteit niet veel toelichting wordt gegeven aan respondenten om te polsen of men al bekend is met de termen. De keerzijde hiervan is dat het wellicht voor een aantal respondenten (te) moeilijk is om een goed beeld te schetsen van SSI of er (onbewust) verkeerde voorstellingen worden gemaakt.

De gehele vragenlijst is te vinden in hoofdstuk 7; bijlage 1.

3.3 Onderzoekseenheden & selectie

Bryman (2012) geeft aan dat een onderzoeksvraag een richtlijn kan zijn voor het selecteren van respondenten. Omdat het vertrouwen van burgers wordt getoetst rondom de (mogelijke) komst en adaptatie van SSI in Nederland, zijn burgers in Nederland de onderzoekseenheid. Daarbij wordt een steekproef toegepast, omdat de gehele populatie (alle personen als burger ingeschreven in Nederland) bereiken, niet haalbaar is, omdat het onwaarschijnlijk is dat iedereen participeert en omdat de looptijd van dit onderzoek daarvoor te kort is. Dat houdt in dat een selectie uit een populatie van onderzoekseenheden wordt onderzocht (Van Thiel, 2015). Voor dit onderzoek wordt zelfselectie toegepast. Zelfselectie houdt in dat de keuze om mee te doen aan het onderzoek volledig aan de individuen wordt overgelaten (Bethlehem, 2010). Het betreft vrijwillige deelname aan het onderzoek.

3.4 Dataverzameling & data-analyse

De bron die geselecteerd is voor het verzamelen van data, is het persoonlijke LinkedIn-profiel van de onderzoeker waaraan 1503 volgers gekoppeld zijn. Via het openstellen van een online vragenlijst (vragenlijst) op LinkedIn wordt van donderdag 8 juni tot en met zaterdag 17 juni 2023 gepoogd een grote gevarieerde doelgroep te bereiken en op deze wijze kwalitatieve data te verzamelen.

Zij die het bericht signaleren, krijgen de kans om mee te doen aan het onderzoek. Er wordt verder niet geselecteerd op sociaal-demografische gegevens om verdere representativiteit te verbeteren. Het onderzoek wordt op LinkedIn gedeeld in de vorm van een openbaar bericht, waar volgers via een directe link naar Google Forms toegang kunnen krijgen tot het onderzoek. Er is bewust een zo open, anoniem en veilig mogelijke ruimte gecreëerd op Google Forms. Het bovenhalen van een zo breed mogelijke informatiestroom die kan bijdragen aan het formuleren van een eerste antwoord op de onderzoeksvraag, is leidend in dit onderzoek.

Er wordt bij de analyse gebruik gemaakt van open en axiaal coderen en ‘pattern-matching’. Bij open coderen wordt een open en herhalende methode ingezet, “waarbij de onderzoeker zo veel mogelijk relevante trefwoorden in de kantlijn plaatst. Elk segment wordt gelezen vanuit elke afzonderlijke onderzoeksvraag” (Wester, 2004, p. 567). De diverse trefwoorden worden onderscheiden gebaseerd op de theorie en wat verkregen wordt uit fieldresearch en vervolgens geanalyseerd op raakvlakken. Elk segment wordt gelezen vanuit het perspectief van de respondent met als vraag wat dit verder nog naar boven brengt (Wester, 2004). Dit proces van analyseren wordt meerdere malen herhaald om de juiste informatie en verbindingen naar boven te halen. Bij axiaal coderen wordt gezocht naar patronen in gebruikte codes. Deze zijn op thematische wijze verder gecodeerd (Van Thiel, 2015). Door concepten als vertrouwen, governance en leiderschap en (quadruple helix) samenwerking in beeld te hebben gebracht in het theoretisch kader aan de hand van conceptualisaties uit de wetenschappelijke literatuur, en deze te verbinden aan antwoorden die door burgers op de vragenlijst gegeven worden, kan een eerste analyse worden gemaakt van overeenkomsten en verschillen die bestaan met de literatuur. Dit kan helpen bepaalde patronen inzichtelijk te maken. Het basismodel dat hiervoor gebruikt is, is ‘pattern-matching’ waarbij de aandacht gericht is op het bijeenbrengen van overeenkomstige resultaten rondom een bepaald begrip en het “geleidelijk opbouwen van een verklaring” (Yin, 2013 in Van Thiel, 2015, p.173).

3.5 Betrouwbaarheid & validiteit

3.5.1 Betrouwbaarheid

Kwalitatief onderzoek kan worden beoordeeld aan de hand van validiteit en betrouwbaarheid en geeft wat aan over de kwaliteit van het onderzoek. Bij prescriptief onderzoek zou men bij een betrouwbaar onderzoek met zekerheid aanbevelingen kunnen doen die effectief zijn (Van Thiel, 2015) en dat is de doelstelling van dit onderzoek.

Betrouwbaarheid kent als elementen nauwkeurigheid en “de consistentie waarmee variabelen worden gemeten” (Van Thiel, 2015, p. 60). Om de consistentie van het onderzoek te vergroten, worden er meerdere vragen ingezet waarbij dezelfde variabelen (zoals risico’s en zorgen rondom SSI) gemeten worden in de vragenlijst. “Herhaalbaarheid maakt onderzoek betrouwbaarder omdat je als onderzoeker dan zekerder bent van de juistheid van bevindingen” (Van Thiel, 2015, p. 61). De nauwkeurigheid van het onderzoek is vergroot door een ruime hoeveelheid open vragen te stellen en respondenten de gelegenheid te geven zoveel mogelijk variabelen in te geven en mee te laten wegen als meetbare waarde in het onderzoek. Ook bij gesloten vragen is de optie gegeven zelf een eigen respons in te vullen. Dit gaat eventuele exclusie van belangrijke (meetbare) resultaten tegen en vergroot daarom de betrouwbaarheid en openheid van het onderzoek. Vaak heeft de onderzoeker bij kwalitatief onderzoek een bepaalde invloed op onderzoeksresultaten (Plochg & van Zwieten, 2007, p. 89). Er wordt getracht dit zo veel mogelijk te voorkomen, door open antwoordmogelijkheden te bevorderen en bij de vraagstelling zo min mogelijk voorbeelden te vermelden die een sturende uitwerking kunnen hebben.

3.5.2 Validiteit

Validiteit kent twee varianten: interne en externe validiteit. Bij interne validiteit gaat het om de geldigheid van een onderzoek. Wordt er gemeten wat er gemeten moet worden? (Van Thiel, 2015). In dit kwalitatieve onderzoek staat het feitelijke meten niet centraal en zullen de onderzoeksresultaten meer het sentiment, dat wat er leeft ten opzichte van de vraagstelling, omhooghalen. Alle relaties en betekenissen die in de leefwereld van de respondenten (betrokkenen) relevant zijn, moeten zijn opgenomen in het onderzoeksmateriaal (Hak, 2004). Daarvoor wordt in dit onderzoek veel ‘open’ ruimte gecreëerd om de eigen beleving, gedachten en meningen in relatie tot SSI op te tekenen. Interne validiteit wordt vergroot door bij het maken van de vragenlijst, gebruik te maken van een grote hoeveelheid wetenschappelijke literatuur en onderzoekslens die begrippen en verbanden rondom de thema’s, die verband houden met de onderzoeksvraag, helder maakt. Hierdoor wordt de kans vergroot dat daadwerkelijk uitgevraagd wordt wat belangrijk is om de onderzoeksvraag te kunnen beantwoorden. De creatie van een onderzoekslens geeft structuur aan de context die nodig is om globaal in kaart te brengen wat er onder respondenten speelt in relatie tot de onderzoeksvraag. Zou slechts een klein onderdeel uitgelicht worden, dan zouden er mogelijk verbanden over het hoofd gezien kunnen worden die relevant zijn voor verder onderzoek.

Bij externe validiteit gaat het om de mate waarin het onderzoek generaliseerbaar is en de resultaten toepasbaar zijn voor andere personen (Van Thiel, 2015). Om de externe validiteit van het onderzoek te vergroten, is de opgestelde vragenlijst eerst als pilot toegestuurd aan een programmamanager van de SSI-community met het verzoek te bekijken of er vanuit zijn expertise nog relevante aanvullingen of onduidelijkheden waren. Zo kon ook de informatiebehoefte die vanuit hen bestond, gekoppeld worden aan het onderzoek. Eveneens hebben twee proefpersonen de vragenlijst kunnen invullen voor de start van het onderzoek om de helderheid in de vraagstelling te kunnen aanscherpen en onduidelijkheden eruit te filteren. Twee open vragen zijn naar aanleiding van de feedback op de pilot verduidelijkt met een aantal voorbeelden, zodat er denkrichtingen ontstaan voor de respondenten. Kanttekening daarbij is dat er een mogelijke onbedoelde vorm van sturing aan de antwoorden op de vragen gegeven wordt. Door de pilot-vragenlijst in te zetten, is de validiteit van het onderzoek vergroot.

4 Resultaten & analyse

Resultaten op dit deel van het onderzoek zijn verkregen via het uitzetten van een vragenlijst. De bevindingen uit deze vragenlijst zijn in paragraaf 4.1 resultaten beknopt opgesomd; de volledige bevindingen zijn in hoofdstuk 7, bijlage 2 te vinden en inclusief alle volledige reacties van de respondenten weergegeven om openheid van dit onderzoek te garanderen. In *cursief* is in paragraaf 4.1 onder elke vraag een korte samenvatting van de onderzoeksresultaten opgenomen. De quotes die in paragraaf 4.1 worden benoemd en tussen aanhalingstekens staan, zijn letterlijke uitdrukkingen van de respondent, volledig of deels weergegeven.

Paragraaf 4.2 bevat een analyse van de resultaten, al dan niet gekoppeld aan de daarvoor benaderde literatuur benoemd in het theoretisch kader. Analyse van de vragenlijstresultaten geeft idealiter een globaal beeld van wat de overheid kan bieden om het vertrouwen te verstevigen rondom de adaptatie van SSI en welke rolsverwachting er bestaat van overige quadruple helix-actoren, met als gewenste opbrengst: richtlijnen voor beleidsadvies en een conclusie op dit onderzoek. Er komt tevens een antwoord op de deelvragen binnen dit onderzoek uit voort. Voor het weergeven van de resultaten wordt gekozen voor een tekstuele uitwerking en een infographic, te vinden onder hoofdstuk 7 in bijlage 3.

Daarbij worden resultaten gecategoriseerd en op basis van patroon gematcht naar gewenste rollen van de vier quadruple helix-actoren, kansen en mogelijkheden, risico's en bedreigingen en zorgen en aanbevelingen op het vlak van informatievoorziening. Zo wordt overzicht gecreëerd van de onderzoeksresultaten die een subtiele basis kan leggen voor toekomstig onderzoek.

Aantal respondenten

Dertien respondenten namen deel aan het onderzoek; maar er zijn telkens maximaal 12 antwoorden op een vraag gekomen. Waarschijnlijk is één respondent direct afgehaakt. Hierdoor wordt gerekend op een totaal van twaalf respondenten op de kwalitatieve vragenlijst. Vaak zijn 12 tot 20 respondenten gebruikelijk bij kwalitatief onderzoek.

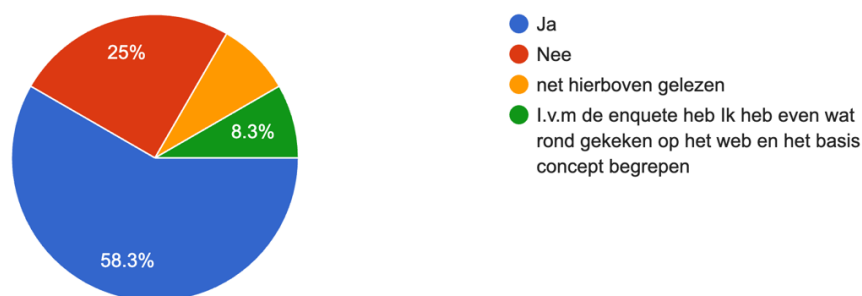
4.1 Resultaten onderzoek

Vraag 1 Bekendheid begrip SSI

Er is een relatief lage bekendheid met het begrip SSI:

Bij 41.7 procent van de twaalf respondenten is het begrip SSI/digitale identiteit niet of slecht bekend. 58.3 procent is wel bekend ermee.

1 - Ben je bekend met het begrip Self Sovereign Identity (SSI) oftewel Digitale Identiteit?
12 responses



Afbeelding 15: Terugkoppeling onderzoeksresultaten 'Bekendheid met begrip SSI'

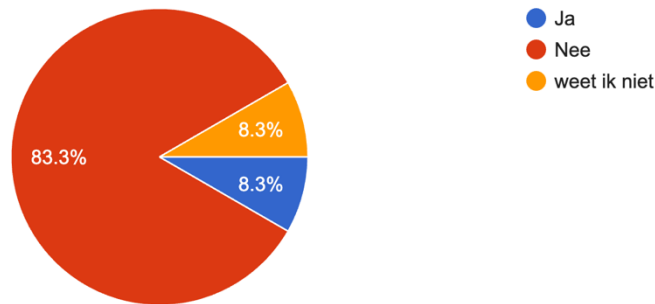
Vraag 2 Beschikbaarheid van informatie (kennis) om een houding t.o.v. SSI te kunnen aannemen

De beschikbaarheid van informatie rondom SSI wordt op dit moment als onvoldoende aangegeven door de respondenten:

Door 83.3 procent van de twaalf respondenten wordt de beschikbare informatie als onvoldoende aangegeven.

2) Is er volgens jou voldoende informatie (kennis) beschikbaar om een houding ten opzichte van SSI te kunnen aannemen?

12 responses



Afbeelding 16: Terugkoppeling onderzoeksresultaten 'Beschikbaarheid van info'

Vraag 3 Informatiebehoefte t.o.v. SSI

Er bestaat een informatiebehoefte t.o.v. SSI.

Dat uit zich in vragen waarop een antwoord gewenst is. Respondenten vragen om meer aandacht voor het onderwerp. Het onderzoek wijst ook aan waar specifiek informatie over gewenst is.⁷ Denk aan: “waarom SSI en hoe komt het tot stand, hoe kan ik het gebruiken, voor- en nadelen, kun je het ook in het buitenland gebruiken, wie beslist erover, stand van zaken, wat brengt het alle betrokken partijen.”

Vraag 4 Houding t.o.v. SSI op basis van de huidige bij de burger bekende informatie⁸

Er bestaan zorgen rondom de (mogelijke) komst van SSI die in relatie staan tot de houding van burgers en de informatie die hierover bij hen bekend is:

“Het geeft de houder te veel macht”, “eenzijdige controle door de overheid”, “geen duidelijkheid over mogelijke consequenties voor vrijheid.” “Het gebruik mag kritisch bekeken worden en aan banden worden gelegd.” “Handig, maar ook angst voor beperking.”

⁷ Waar specifiek informatie over gewenst wordt, is aan de hand van coderen concreet uiteengezet in de vorm van een infographic: onderzoeksresultaten SSI. Zie ook bijlage 3.

⁸ Tevens uiteengezet in de infographic onderzoeksresultaten SSI, bijlage 3.

“Beveiliging een uitdaging.” “Zorg voor eventuele achterdeurtjes en dat gebruikers de zwakste schakel zijn m.b.t. data security.” “Hopelijk minder omslachtig dan DigiD.”

Vraag 5 Gewenste rol van de overheid om verder te bouwen aan vertrouwen rondom SSI:⁹

De overheid kan haar rol verstevigen en vertrouwen opbouwen door een betere communicatie/informatievoorziening; zelfbeschikking over informatie; transparantie en openheid en het bieden van bescherming: “Een betere informatievoorziening rondom SSI”; “meer bekendheid genereren door inzet campagnes”; “informatie toegankelijk maken”; “volk betrekken bij keuzes (wellicht referenda)”; “veel zelfbeschikking geven aan burgers over (eigen) informatie”; “burgers moeten kunnen zien wie wat inziet”; “transparantie en openheid”; “open source”; “vertrouwen in de burger vanuit de overheid”; “overheidskennis en tempo proberen te verhogen” en “vanuit meer bewustzijn een sterke beschermer worden.”

Vraag 6 Gewenste rol die de overige quadruple helix-actoren (wetenschap, bedrijfsleven, burgers) kunnen aannemen om vertrouwen in SSI te verstevigen

a) Wetenschap

Van de wetenschap wordt verlangd om veiligheid te onderbouwen, leerstoelen in te richten, informatie te delen in bijvoorbeeld wetenschappelijke magazines en dit alles zo veel mogelijk vanuit het open-source-principe.

Genoemd zijn: “Open source”; “onderbouwen van veiligheid en hierover informeren;” “voorbeelden en voordelen schetsen van SSI”; “uitleggen hoe het werkt en wat er voor zorgt dat SSI veilig is”; “hoe je er zelf voor kunt zorgen dat je veilig met SSI omgaat”; “feiten geven m.b.t. het onderwerp”; “belang van menselijk contact aanstippen”; “onderzoeken publiceren”; “link leggen met populair-wetenschappelijke onderzoeken (bijv. Quest)”, “leerstoelen aanwijzen bij de universiteit”, “goede encryptie- en communicatie-protocollen ontwikkelen”, “SSI in het onderwijs inbedden.”

⁹ Zie tevens de infographic onderzoeksresultaten SSI, bijlage 3.

b) Bedrijfsleven

Het bedrijfsleven lijkt als actor in de quadruple helix de minst grote vertrouwenspositie t.o.v. SSI te hebben. Een positieve trigger kan zijn: weten hoe SSI een bedrijf helpt (belangen inzichtelijk maken) en wat hun voordelen zijn, zodat de gebruiker zelf kan bepalen of hij of zij openstaat voor het gebruik van SSI. Investeren in oplossingen en tools die linken aan de belangen van bedrijven en toezicht op wat er met gegevens gebeurt (ook als je geen klant meer bent). Ook genoemd werden: garanderen dat de identiteit niet gehackt kan worden. Bewijzen dat alleen met toestemming gegevens ingezien mogen worden, bewaren, etc. Open source. Zorgen voor gemak en community.

c) Burgers; eigen rol

Openheid en transparantie zijn essentieel; ook wanneer het gaat om het geven, delen en verduidelijken van informatie: “Medeburger helpen om SSI te begrijpen en vertrouwen”; “informatie opzoeken en goed doornemen”; “ervaringsverhalen delen en er over praten en verduidelijken”; “leren hoe anderen het gebruiken”; “goed onderscheid maken tussen fake-news/complotdenken en waarheidsgetrouwe informatie”; “mensen die nieuwsgierig zijn en voordelen zien, kunnen erover praten in hun netwerk (gebruikersgemak, voordelen, risico’s, wat het hen oplevert), zodat het anderen motiveert het ook uit te proberen.”

Vraag 7 Hoe diverse partijen beter kunnen samenwerken om technologische innovatie als SSI te kunnen ondersteunen

De volgende punten komen sterk naar voren:

1) Communicatie; informatievoorziening verstevigen vanuit openheid en transparantie; open source

Informatie geven helpt. Open source en openheid en transparantie worden meerdere malen benoemd. Er leven veel vragen die een antwoord nodig hebben (hoe het werkt, waarom het werkt, wat de voordelen zijn, wat het burgers, overheid, wetenschap en het bedrijfsleven brengt). Een oplossing die genoemd wordt: “Een platform online inrichten, conferenties houden, raamovereenkomsten sluiten.”

2) Een inclusieve samenwerking (collaborative governance) met heldere rolverdeling

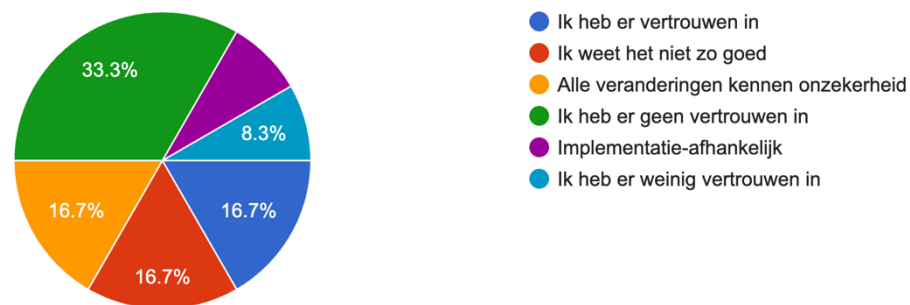
Een samenwerking “die ook gedeeld gaat worden met iedereen en niet alleen in hoger segment”: Sterk leiderschap en inzicht. “Zorg dat er duidelijke rollen zijn en dat velen kunnen deelnemen aan onderdelen van het systeem.”

Vraag 8 Houding ten opzichte van vertrouwen tegenover digitale gegevensuitwisseling van belangrijke gegevens

Het grootste deel van de twaalf respondenten heeft weinig tot geen vertrouwen in digitale gegevensuitwisseling en ongeveer een derde is hier onzeker over. Een kleinere groep heeft er wel vertrouwen in. Dat wijst erop dat er op het gebied van digitale gegevensuitwisseling verder gebouwd kan worden aan vertrouwen. 41.6 procent heeft weinig (8.3 procent) tot geen vertrouwen (+ 33.3 procent) in digitale gegevensuitwisseling van belangrijke (persoonlijke) gegevens. 16.7 procent heeft er wel vertrouwen in en de overige 33.4 procent is er onzeker over.

8) Hoe sta je qua vertrouwen tegenover digitale uitwisseling van (digitale) gegevens die voor jou belangrijk zijn?

12 responses



Afbeelding 17: Terugkoppeling onderzoeksresultaten ‘Vertrouwen t.o.v. digitale uitwisseling van gegevens’

Vraag 9 Rol als burger bij eigen databeheer

Hoewel eigen databeheer rondom SSI hopelijk “eenduidiger en overzichtelijker” wordt, lijkt er een vertrouwensissue bij burgers te zijn met betrekking tot eigen databeheer; ook is er onzekerheid over het kennisniveau van burgers om over te gaan tot het kunnen beheren van eigen data. “Eenduidiger en overzichtelijker,” dat zou een effect moeten zijn wanneer databeheer bij burgers komt te liggen.

Hoeveel kennis is er bij burgers nodig om dit systeem te kunnen beheren, is een vraag die uit het onderzoek naar voren komt. Meer eigen verantwoording, bewustwording en betrokkenheid worden genoemd. Betrokkenheid geeft vertrouwen en gevoel van zelfbeschikking en controle: “Dat ik kan bepalen wat anderen wel en niet van mij mogen weten, is fijn.” “Het is niet iets eenmaligs, je moet hier veelvuldig mee bezig zijn en af en toe kritisch bekijken of je bepaalde toestemmingen nog wil verlenen.” Bij de bespreking van de rol van de burger komt ook in de antwoorden naar voren dat er geen geloof is in eigen databeheer: “data laat overal sporen na, dus ik geloof niet in eigen beheer” en “Big Tech plukt alles uit de cloud” en “volgens mij krijg ik juist minder controle.”

Vraag 10 Geuite zorgen in relatie tot SSI

De geuite zorgen in relatie tot SSI hebben betrekking op een mogelijk laag systeemvertrouwen en weinig vaardigheid van de overheid op ICT-gebied in relatie tot nieuwe ontwikkelingen.

Het systeemvertrouwen (m.a.w. het vertrouwen in de overheid) en in de vaardigheid (‘ability’) van de overheid op ICT-gebied blijkt laag onder deze groep respondenten.

Zo zijn er zorgen m.b.t. “controle over uitwisseling, systeemvertrouwen en juiste implementatie. “De burger zou echt overal controle over moeten hebben.” “Totaal geen vertrouwen in de overheid.” En: “Mijn vertrouwen van de overheid op het gebied van ICT is vrij laag. Zo lang zij geen topontwerpers, systeemprogrammeurs en hackers aannemen tegen concurrerende topsalarissen... blijft de overheid op dit gebied een onbetrouwbare partij.”

Andere antwoorden van respondenten zijn: “dat het niet soepel zal lopen in het begin”, “te veel werk”, “zowel privacy als misbruik van gegevens lijken me belangrijk. Criminelen lopen altijd een stap voor op de overheid, dat is lastig te veranderen.” Uitgebreidere reacties: “Ik vertrouw er niet zo op dat het opschiet.” “Er is ook veel kwaliteit nodig om het op te zetten... gelijk doen op het niveau van de Europese Unie” en “Op het moment dat er veel juridische taal bij komt, vind ik het lastig. Dan denk ik, ik wijs alles af onder het mom ‘better safe...’

Ook vraag ik me af hoe het dan zit met de gegevens die je bewust verstrekt/zichtbaar maakt en hoe bedrijven daarmee omgaan.” Andere zaken die genoemd worden: “Alles” en “Al het bovenstaande” (wat als voorbeeld genoemd is in de vraagstelling: privacy; controle van gegevens; (zelf)controle op digitale gegevensuitwisseling en interoperabiliteit tussen systemen die met elkaar moeten communiceren; systeemvertrouwen; vertrouwen in de digitale infrastructuur en het kunnen van de overheid; vertrouwen in eigen online handelen). “Voorkom al te veel bureaucratie, maar houd democratische controle.”

Vraag 11 Wat de overheid doen kan om ervoor te zorgen dat jij je veilig en gesterkt voelt in het beheren van jouw eigen gegevens en de mogelijke komst van SSI

Duidelijk en transparant informeren aan de hand van een campagne; openheid van informatie en consequenties geven (transparantie); informatiehuishouding versterken (duidelijk zijn) en “goede tools creëren” en websites voorzien van informatie die daarbij ondersteunen.

Verdere tips zijn: “Creëer audit trails voor je eigen SSI”, “baken af waar gegevens voor gebruikt moeten worden” en “maak gebruik van open source en single use”.

Genoemd zijn: “Campagne om ideeën en voorbeelden te geven, consequenties toelichten en toelichten wat anderen eventueel kunnen doen (zowel goed als kwaad).” “Voorbeelden geven hoe jouw gegevens zo goed mogelijk te beheren en consequenties duidelijk maken van bepaalde keuzes die je digitaal maakt: ‘als je deze toestemming geeft, dan houdt dat in dat... voor de tijdsduur van...’ Dus consequenties van handelen toelichten en toelichten wat anderen eventueel kunnen doen (goed en kwaad).”

Vraag 12 Verwachting over de omgang met jouw (digitale)data door betrokken partijen

Over het algemeen verwachten respondenten dat overheden zich aan de regelgeving houden.

Er bestaat wel angst voor misbruik van gegevens en gegevens die in verkeerde handen vallen.

Beveiliging is van groot belang: Een aantal respondenten verwacht dat overheden zich aan alle AVG en privacywetgeving houden en niet meer dan nodig opvragen. “Dat er met zorg en ‘volgens afspraak’ met data wordt omgegaan, maar je moet er wel op toezien”. Een andere respondent vertrouwt met name overheidsinstanties wel “maar informatie mag niet in verkeerde handen komen.” Beveiliging van data wordt als belangrijk aspect aangewezen om misbruik te voorkomen. Er wordt door één respondent wel goede omgang verwacht met data binnen de EU, maar er bestaan twijfels over omgang met data buiten de EU. Vijf van de twaalf respondenten heeft weinig tot geen vertrouwen in de omgang met data of verwacht misbruik ervan, omdat er geld verdiend wordt aan data of omdat zij vrezen dat hackers een identiteit proberen over te nemen. Over commerciële partijen wordt door een respondent gezegd dat ze “zullen proberen meer data te verzamelen en te bewaren dan de bedoeling is.” Over vertrouwen in commerciële partijen wordt minder positief gedacht, omdat er geld aan verdiend kan worden.

Vraag 13 Wat de overheid kan doen om erop toe te zien dat de (mogelijke) uitrol en ingebruikname van SSI goed verloopt. Gewenste rol van de overheid.

Samengevat wordt over de gewenste rol van de overheid in relatie tot SSI genoemd: vanaf het begin de doelstelling helder formuleren, controleren (toetsen) en begrijpelijk informeren over SSI, transparant opstellen; geen belerende houding innemen en heldere kaders en goede afspraken en regels opstellen met balans als uitgangspunt: “Controlerend (toetsend) en informerend”, “Transparant opstellen, niet belerend zijn. Nationaal vs. EU scheiden is waarschijnlijk ook verstandig. Ben ik zelf geen voorstander van, maar voor mensen met een anti-EU-sentiment lijkt het me verstandig dat ik bijv. niet automatisch ook gegevens met EU- instanties deel als ik ze eigenlijk met NL-(semi)overheden wil delen”, “Heldere kaders, balans, goede afspraken en regels opstellen”, “Informatie die makkelijk te vinden en vooral te begrijpen is”. Een andere respondent noemt: “Overheids campagne (SIRE), nieuwskanalen (NOS, etc.), Rijksoverheid.nl.” Weer een andere respondent vult aan: “Website, spotjes (online) waarin voorbeelden en zorgen langskomen. Ook voorbeelden toelichten waarmee je als burger hier gebruik van zou kunnen maken met die overheid.” “Kaders en overzicht” en “Het opstellen van heldere kaders en regelgeving rondom SSI in Europees verband” worden benoemd. “Alle kritiek van alle partijen serieus nemen” is weer een andere opmerking, wat door dezelfde respondent wordt aangevuld met: “Niet zelf doordrukken van agenda’s buiten de Kamer om.” Weer een andere respondent zegt: “Niets, want er is geen draagvlak.” Een andere respondent haalt de uitrol van DigiD aan: “Die was niet geweldig, waar in eerste instantie alleen de overheid er gebruik van zou maken (belastingen, etc.) is het nu onmisbaar voor alle communicatie met de gezondheidszorg. Het moet vanaf het begin duidelijk zijn voor welk doeleinde dit gebruikt gaat/kan worden en in hoeverre het tot uitsluiting leidt, indien men er geen gebruik van maakt.”

Vraag 14 Kansen en mogelijkheden rondom SSI

SSI kan zorgen voor efficiëntere en snellere dienstverlening door de overheid. Gemak en het bevorderen van snelheid in het gebruik, zoals overstappen naar een andere bank of provider, spelen ook mee. SSI kan een kans zijn om proactief privacy-problemen op te lossen en identiteitsfraude te voorkomen. Een kwart van de twaalf respondenten zag geen kansen (wel bedreigingen). Respondenten noemden: “Minder naar het gemeentehuis, minder gedoe bij huur of (ver)koop van een huis. Overstappen van bank of provider zou makkelijker moeten zijn.” “Mogelijk maakt het bepaalde zaken gemakkelijker.”

“Mega kans wat betreft vertrouwen in overheid terugwinnen voor politiek. Ook kans om proactief privacy-problemen op te lossen.” “Als het goed aangepakt wordt, kan identiteitsfraude wellicht voorkomen worden.

Het kan zorgen voor efficiëntere en snellere dienstverlening door de overheid.”

“Contact met overheid.” “Ja, als deze DigiD vervangt en niet ernaast komt.”

“Voor minder bedeelden en gehandicapten.” Drie respondenten noemden: “geen kansen”, “nergens kansen” en “kansen zie ik niet, ik zie eerder bedreigingen.”

Vraag 15 Risico's en bedreigingen rondom SSI

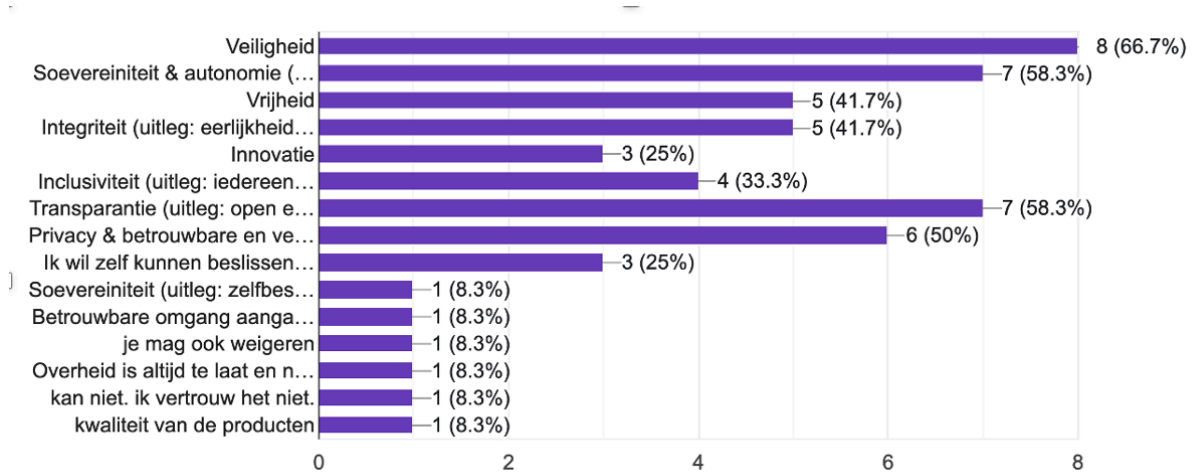
Er bestaan voor de respondenten risico's en bedreigingen rondom SSI: er is zorg over hacking, phishing en kwaadwillenden en toegang tot informatie die in verkeerde handen valt ook in relatie tot macht, invoering, implementatie en kosten van SSI, bureaucratie en toekomstbestendigheid van SSI (o.a. in relatie tot toekomstige technologieën zoals quantum computers). Ook zijn er zorgen over eigen databeheer:

“Hackers (buiten) en kwaadwillenden (binnen)” en tevens van een andere respondent: “Dat er hackers op af komen.” “ICT overheid en budget gaan nooit goed samen, dus invoering gaat miljarden kosten. Door alles te koppelen wordt het mogelijk om ook digitaal geld te koppelen, dan wordt het wel heel gevaarlijk als verkeerde personen aan de macht komen.”

Een andere respondent noemt: “Stel dat Hitler hier toegang toe had gehad?” en weer een andere respondent heeft het over “Informatie die in verkeerde handen valt. Cybercrime maar ook cyberwar.” “Ik vind het een heel eng idee hoe de overheid steeds meer ‘macht’ naar zich toetrekt en er een agenda uitgerold is en wordt. Met veel camera's, Iris-scans, overal je ID scannen en opgeven – zelfs bij museums.” “Alleen maar.” “Niet anders dan bij andere technologieën, wat betreft hacking, fishing, etc.” “Veel risico's: het schiet niet op. Te veel politiek gedoe en bureaucratie. Bij gebruik: mensen durven niet, worden defensief door geen informatie te delen.” “Winstbejag is het grootste doel. Aandeelhouders bepalen. Implementatie wordt niet serieus genomen. Te veel om op te noemen.” “Risico's en bedreigingen komen van 2 kanten: wie heeft regulier toegang tot welke data en hoe wordt dat door de gebruiker bepaald? Is het systeem toekomstbestendig? Denk aan quantum computers voor encryptie.” “Onwetendheid of onhandigheid bij mensen, waardoor zij onbewust te veel data met de verkeerde personen delen. Wat gebeurt er als een derde er met jouw identiteit vandoor gaat?”

Vraag 16 Publieke waarden die een rol spelen bij het verstevigen van een vertrouwenspositie bij het invoeren van een innovatie als SSI

Belangrijke waarden die een rol spelen bij SSI, zijn als volgt benoemd:



Afbeelding 18: Terugkoppeling onderzoeksresultaten 'Waarden die een rol spelen bij het verstevigen van een vertrouwenspositie'

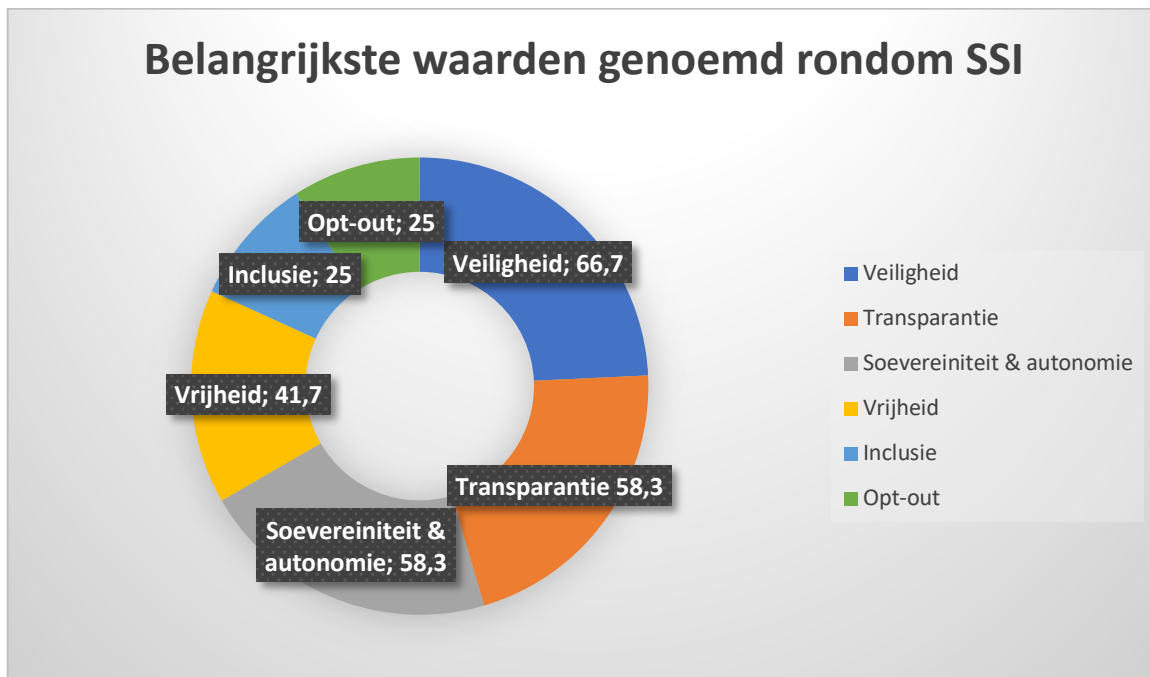
Veiligheid wordt door 66.7 procent van de twaalf respondenten benoemd als belangrijke Waarde die een rol speelt bij het verstevigen van een vertrouwenspositie.

Op de voet gevolgd door transparantie en soevereiniteit & autonomie (beiden 58.3 procent). Privacy wordt aangevinkt door de helft van de respondenten.

Vrijheid en integriteit zijn beiden door 41.7 procent van de respondenten aangevinkt.

Inclusiviteit is door een derde (33.3 procent) van de respondenten benoemd.

Innovatie en “Ik wil zelf kunnen beslissen om hier aan mee te doen en ook voor een opt-out kunnen kiezen zonder dat dit verdere consequenties op uitsluiting heeft” zijn door een vierde van de respondenten aangevinkt. Een vorm van exclusie zonder consequenties, lijkt gewenst. “Je mag ook weigeren,” schrijft één respondent. Een andere respondent geeft aan soevereiniteit belangrijk te vinden; en weer een andere respondent schrijft: “Overheid is altijd te laat en neemt contraproductieve beslissingen. Ze voeren een politieke daad uit en hollen achter WEF aan. De multinational met exorbitant winstbejag regeert.” Eén respondent schrijft “Kan niet, ik vertrouw het niet” en één respondent geeft “Kwaliteit van de producten” op. Een andere respondent kiest voor “Betrouwbare omgang aangaande mijn gegevens vanuit alle betrokken partijen.”



Afbeelding 19: Terugkoppeling onderzoeksresultaten 'Belangrijkste waarden rondom SSI'

Vraag 17 Belangrijke waarden gekoppeld aan SSI

Diverse waarden werden als belangrijk benoemd in relatie tot SSI. Veiligheid, vrijheid, autonomie, openheid en privacy werden o.a. benoemd:

“Veiligheid, omdat het gaat over mijn identiteit. Misbruik kan grote gevolgen hebben.”

“Kleine sociale netwerken en verbondenheid en een roverheid op afstand.”

“Soevereiniteit en autonomie. Past bij de samenleving. Niet i.v.m. individualisme maar om als individu aan een groep deel te nemen op eigen voorwaarden.” “Een keuze hebben en die is er in veel gevallen niet meer. Doe je niet mee, dan kan je bepaalde apps niet meer gebruiken of downloaden of plekken niet bezoeken.” In dezelfde lijn als de vorige reactie: “Opt-out zonder gevolgen.” “Openheid zodat ik het idee heb dat er geen addertjes onder het gras zijn.”

“Veiligheid, vrijheid en innovatie.” “Kwaliteit, het is anders denken en complex.” “Privacy & betrouwbare en veilige omgang met mijn gegevens vanuit alle betrokken partijen. Zonder vertrouwen is elk systeem gedoemd te mislukken.” “Privacy & betrouwbare en veilige omgang met mijn gegevens vanuit alle betrokken partijen. Er is niets zo vervelend als iemand anders mijn digitale identiteit overneemt.”

Vraag 18 Gesignaleerde risico's in relatie tot waarden en SSI

Op de vraag: signaleer jij risico's rondom SSI in relatie tot jouw waarden, wordt veelvuldig "ja" geantwoord. Op de vraag welke risico's worden gesignaleerd, zijn diverse antwoorden ontvangen. Een risico dat een aantal keer wordt benoemd, is de aandacht voor inclusie. "Ik zie niet echt in hoe het inclusiviteit verbetert." Maar ook het risico dat elk systeem kent. Bijvoorbeeld "als ik nu mijn paspoort kwijt ben, kan iemand daar online ook kwaad mee". Een aantal reacties duiden ook op respondenten die de mogelijkheid willen hebben tot exclusie van SSI, zonder consequenties. "Ik vind het belangrijk dat iedereen mee kan doen (laagdrempelig) en dat niet kiezen voor SSI ook mogelijk blijft zonder dat er consequenties aanzitten. Ik vermoed dat als SSI meer gebruikt wordt de niet-gebruiker toch gedwongen wordt mee te gaan doen." Verder werden "gebrek aan kwaliteit" en "de onduidelijkheid" als risico aangeduid. Overige reacties van respondenten: "Als je een niet welgevallige mening hebt, zoals de truckers in Canada, dan wordt je bankrekening bevroren." Eén respondent ziet geen risico's, een andere ziet ze overal. Twee respondenten zien minder risico's rondom waarden. Eén van hen vult aan: "Als het niet meer wordt dan een verbeterde DigiD, heb ik er geen probleem mee."

Vraag 19 Hoe optionele risico's geminimaliseerd kunnen worden om waarden te beschermen

Risico's kunnen geminimaliseerd worden door in te regelen hoe deelnemers aan het SSI-systeem gecontroleerd kunnen worden en wat de maatregelen zijn als misbruik geconstateerd wordt. Geen automatische data-uitwisseling mogelijk maken, tenzij daarvoor opt-in wordt gegeven, dat betekent het aanbieden van keuze-opties waarmee je als gebruiker zelf kunt kiezen welke data je wel en niet geeft, zonder dat daarvoor consequenties voor de gebruiker ontstaan. Een Europees topteam oprichten om SSI aan te vliegen is een andere gegeven oplossing. En open source kan risico's minimaliseren. Reacties van respondenten: "Weten hoe deelnemers gecontroleerd worden, wat er gebeurt als misbruik geconstateerd wordt." "Geen automatische data-uitwisseling tenzij daarvoor opt-in is gegeven. Niets o.b.v. opt-out. Het moet zijn alsof het een kluisje is dat bij mij thuis staat met mijn data erin. De overheid belt aan bij de voordeur, vraagt om data, ik beslis wat ik wel en niet geef, en doe het kluisje weer dicht." Keuze-opties zijn ook voor de volgende respondent van belang: "Door een keuze te hebben voor een andere mogelijkheid i.p.v. je kunt een app niet meer gebruiken etc. Je wordt nu gedwongen om persoonsgegevens vrij te geven." "Informatie inwinnen en doornemen." "Richt op Europees niveau een topteam in om dit in 5 jaar te realiseren."

“De bestaande vormen van communiceren met bedrijven en overheden zouden moeten blijven bestaan.” “Open source.” “Door de hoeveelheid beschikbare informatie in SSI te minimaliseren.” Andere reacties zijn: “Niet, kijk wat ze in China al doen.”

En: “Alle multinationals socialiseren.”

Vraag 20 Relevante vragen, opmerkingen en aanvullingen uit het onderzoek

Onderstaande opmerkingen duiden bij deze groep respondenten op zorg over de inzet van SSI in relatie tot ethiek. “Ik ben er helemaal klaar mee, met die opgelegde controle. Ontmenselijkt en dehumaniseert... Waar zijn we mee bezig.” “Zoals je leest, sta ik niet te springen om SSI ondanks dat het een deel van onze realiteit is. Het kan ons veel goeds brengen, maar dan wel onder strikte voorwaarden.”

4.2 Analyse

Paragraaf 4.2 bevat een analyse van de resultaten, waar mogelijk gekoppeld aan de theorie. De deelvragen uit dit onderzoek worden aan de hand van de resultaten uit de vragenlijst beantwoord. Deze vormen een basis om in hoofdstuk 5 de onderzoeksvraag te kunnen beantwoorden. Uiteindelijk brachten de onderzoeksresultaten SSI naar voren: ontwikkelpunten die relatie hebben tot SSI, de (gewenste) rol voor de overheid en de overig quadruple helix-actoren (wetenschap, bedrijfsleven, burgers) in relatie tot SSI; kansen en mogelijkheden; risico's en bedreigingen uiteindelijk thematisch gekoppeld aan het fenomeen 'zorgen over SSI'; en mogelijke vertrouwensissues (nader te onderzoeken).

4.2.1 Digitale & collaboratieve innovatie

Minimale informatievoorziening; lage betrokkenheid van burgers

Transformatieprocessen met mens en samenleving als middelpunt en scope, zijn uitgangspunt in een tijdperk waar dataficering en out-of-office centraal staan in het ICT-landschap (Maes, 2019). “Neem een persoon en vertaal deze in persoonsgegevens; de vertaling van de werkelijkheid in data,” zo omschrijft Van Nieuwenhoven (2019) dataficering. SSI, oftewel digitale identiteit, wordt (mogelijk) een open-source wallet waarin belangrijke gegevens van een persoon, online verzameld worden. In empirische studies is terug te vinden dat mensen er vaak huiverig voor zijn om persoonlijke informatie via internet te delen vanuit de angst dat (hun financiële) leven een open boek wordt in “het internet universum” (Bestavros, 2000).

Voor SSI komt diezelfde vrees terug in het onderzoek “dat (persoonlijke) informatie in verkeerde handen - of kwaadwillenden - valt” wordt meermaals benoemd.

Vertrouwen wordt vaak gelinkt aan burgerlijke verbondenheid (‘civic engagement’). In de inleiding werd vertrouwen als “het magische elixer” beschreven om die verbondenheid te bereiken (AlAwadhi, 2019).

Van de burgers die meededen aan het onderzoek, ervaren de meesten zich weinig betrokken bij de verkenningsfase waarin SSI zich bevindt. Deze conclusie wordt getrokken door inzicht uit het onderzoek dat de lage mate waarin de burgers zich geïnformeerd voelen over SSI onderstreept. Volgens Bryson et al. (2006, p. 46) wordt aan vertrouwen gebouwd, door informatie en kennis te delen, goede intenties te hebben, competenties te laten zien en te waarborgen dat partijen zich aan afspraken houden. Kennis is noodzakelijk om samen te kunnen werken. Daarom is het van belang om deze kennis te organiseren en faciliteren (Buuren 2014 in Van den Brink, 2017). Er worden in het onderzoek eveneens zorgen uitgesproken over het kennisniveau om autonoom met SSI aan de slag te gaan, wat er op kan duiden dat er in het proces aandacht moet zijn voor het vergroten van toepasbare kennis (eveneens informatie).

AlAwadhi (2019) noemt vertrouwen als belangrijke factor voor het accepteren en adopteren van e-government diensten. Daarvoor moet de dienst, zoals SSI, niet alleen eenvoudig bruikbaar zijn en tijd- en moeite-besparende voordelen opleveren. Er moet ook interactie zijn met burgers. Wanneer zij de juiste gereedschappen krijgen om hun standpunten en behoeften te uiten, gaan zij deel uitmaken van het (samenwerkings)proces. Daarmee vergroot je niet alleen het vertrouwen, maar uiteindelijk ook burgerlijke verbondenheid; betrokkenheid (AlAwadhi, 2019).

Om betrokkenheid met de innovatie te vergroten en bij te dragen aan publieke waarde creatie zijn collaboratieve innovatie en co-creatie belangrijke elementen in een quadruple helix-context waar burgers, wetenschap, bedrijfsleven en overheid met elkaar samenwerken. (Prahalad & Ramaswamy, 2002). De verkenningsfase rondom de mogelijke komst van SSI lijkt te duiden op een triple-helix samenwerking; respondenten voelen zich nog niet voldoende geïnformeerd en daarmee betrokken als partner in het proces.

4.2.2 SSI: een disruptieve technologie

Risico's & bedreigingen; kansen & mogelijkheden

SSI is een vorm van zelf-soevereiniteit, waarbij macht gedecentraliseerd wordt en burgers zelf zorgdragen voor hun digitale identiteit en bijbehorende data (Ishmaev, 2020).

Uit het onderzoek wordt duidelijk dat het voor respondenten niet helder is waar de macht ligt. Hoeveel macht de overheid en bedrijven potentieel in handen hebben, wordt als een risico gezien. Hieronder worden respectievelijk risico's en kansen die naar voren kwamen in het onderzoek uiteengezet:

- Uit het onderzoek blijkt dat er *controle, macht en privacy-issues* bestaan die aandacht en opheldering aan de hand van communicatie verdienen. Zo noemt een respondent dat hij of zij denkt juist “minder controle” te krijgen wanneer SSI er is; “de houder krijgt te veel macht.”
- “*De toekomstbestendigheid van het systeem*”.
- Niet alleen vanuit de overheid, maar ook vanuit de burger bestaat er een wens om *controle over uitwisseling van data en toezicht op data* binnen SSI te hebben.
- *Privacy-issues en beveiliging* worden als een *uitdaging* gezien. Zoals eerder benoemd bestaan er zorgen dat (persoonlijke) informatie in verkeerde handen valt. Respondenten geven aan risico te lopen door de gevoeligheid van (persoonlijke) informatie die wordt gedeeld. “Data laat overal sporen na.”
- De respondenten merken ook risico's op rondom *eigen handelen in relatie tot eigen databeheer*, waarbij onwetendheid en onhandigheid benoemd worden.
- Risico's die ook genoemd worden zijn *inclusiviteit en een optie tot exclusie* om mee te doen aan SSI, zonder dat daar consequenties aan zitten.
- “*Onduidelijkheid over SSI*” als risico. Wat gaat SSI teweegbrengen en zijn er consequenties m.b.t. vrijheid en beperking als belangrijke waarden?
- Diverse *zorgen rondom het proces en de (mogelijke) implementatie* van SSI komen naar voren. Ook de “kwaliteit van leveren” wordt genoemd.
- *Kosten*; een ander punt dat in het onderzoek naar voren is gekomen, is dat de invoering volgens een respondent miljarden gaat kosten en lang duurt.

Risico gaat hand in hand met vertrouwen, zo leerden we uit het theoretisch kader en van o.a. Vangen & Huxham (2003). Naast risico's, bedreigingen en zorgen, zijn er ook kansen & mogelijkheden in relatie tot SSI genoemd door de respondenten.

Zo kan het volgens hen

- zowel DigiD en het fysieke identiteitsbewijs vervangen;
- online zorgen voor betere bescherming en mogelijk identiteitsfraude voorkomen mits het goed ingeregeld wordt;
- meer snelheid en gemak verlenen bij het regelen van zaken, efficiëntere dienstverlening;
- het contact met de overheid verbeteren;
- privacy-problemen oplossen;
- het heft terug in handen van burgers geven en potentieel vertrouwen teruggeven aan mensen.

4.2.3 Governance & samenwerking

Relatie en dialoog met de burger; behoefte aan transparantie; gewenste rol bedrijfsleven, wetenschap en burgers

Wanneer je kijkt naar governance in ontwikkeling, kan opgemerkt worden dat de relatiestructuur verandert. Dat houdt in dat er in plaats van een top-down structuur steeds meer horizontale netwerken ontstaan, waarin samengewerkt wordt (Castells, 2000).

New Public Management zorgde vanaf de jaren tachtig voor decentralisering van overheidstaken (Hood, 1991; Klijn & Twist, 2007). New Public Governance gaat uit van een netwerkstructuur, waarin organische relaties de basis zijn; in tegenstelling tot rationeel handelen (Osborne, 1997). Het kan gezien worden als een deelmechanisme van publiek management, waarbij het doel is om aan verschillende behoeften van burgers te kunnen voldoen. Bij deze netwerkvorm staat de relatie centraal en bestaat er afhankelijkheid van vertrouwen en stabiliteit als basis. Het fundament van deze netwerkvorm bestaat niet uit regels, systemen en beperkingen. Hierdoor is er sprake van meer flexibiliteit; ook om mee te gaan met veranderingen (Xu et al. 2015). Een disruptief proces als SSI vereist een andere vorm van managen van de impact die de disruptie veroorzaakt (Mulder, 2019). Governance en leiderschap zijn daarbij belangrijke elementen.

Bij collaborative governance wordt op dusdanige wijze bestuurd dat belanghebbenden betrokken worden bij het samenwerkingsproces. Dit kan innovatie versnellen (Ansell & Gash, 2007).

Wanneer de voorhistorie tussen belanghebbenden antagonistisch is en daarmee strijdig, dient er veel tijd gestoken te worden in effectieve oplossingsmaatregelen rondom het bouwen aan vertrouwen (Ansell & Gash, 2008). Collaborative governance komt vaak voor uit het gebrek aan vertrouwen onder belanghebbenden. Het bouwen aan vertrouwen onder belanghebbenden is daarbinnen essentieel (Weech-Maldonado & Merrill 2000 in Ansell & Gash, 2008).

Wanneer het fundament van basisvertrouwen er is, zouden collaboratieve leiders moeten investeren in transparante communicatie, gedeeld eigenaarschap van het proces en overige strategieën die helpen om vertrouwen te verstevigen (Ansell & Gash, 2008). Ansell & Gash (2007) benoemen dat resultaten van collaborative governance afhankelijk zijn van de mate van bouwen aan vertrouwen; communicatie; betrokkenheid bij het proces; wederzijds begrip; tussenliggende uitkomsten en dialoog (Ansell & Gash, 2007). Op een groot deel van deze punten lijkt op basis van de onderzoeksresultaten verbetering mogelijk.

Uit het onderzoek blijkt dat er een grote behoefte bestaat aan open en transparante communicatie en heldere doelstellingen; maar er op dit moment een informatietekort is. Ook Nederlandstalige informatie over SSI is schaars, geeft een respondent aan. In dit onderzoek zijn behoeften en fundamentele waarden van een kleine groep burgers naar voren gekomen ten opzichte van de (mogelijke) invoering van SSI. Daarbij kan vanwege het informatietekort naar de burgers toe de vraag gesteld worden of de relatie en de dialoog met de burger in de verkennende fase van SSI voldoende centraal staat, of dat er meer aandacht gevestigd dient te worden op 'gedeeld eigenaarschap'. Zoals Dunn-Cavelty & Suter (2009) aangaven, wordt vertrouwen enkel ontwikkeld door samenwerking, waarbij samenwerking weer afhankelijk is van vertrouwen. Vertrouwen bouw je volgens Carr (2016) gezamenlijk op door te investeren in de relatie, transparantie te vergroten, begrip te hebben voor de uitdagingen van alle belanghebbenden en erop vertrouwen dat er positieve winst te behalen is voor alle partijen. Uit het onderzoek is ook op te maken dat er twijfels bestaan of SSI in ieders optiek een positieve winst zal kunnen bevorderen; een deel van de respondenten kijkt met wantrouwen toe naar de ontwikkelingen rondom SSI en ziet geen kansen rondom SSI. Diverse zorgen worden geuit, die te maken hebben met een laag vertrouwen in het systeem en andere actoren die deel uitmaken van het systeem (zoals verkoop van data door bedrijven), digitale systemen en de verantwoordelijkheid in relatie tot eigen databeheer ('gebruikersvertrouwen'). Dit betekent ook dat om tot een goed resultaat te komen niet alleen communicatie, tussenliggende uitkomsten en dialoog (benodigd voor wederzijds begrip) en gedeeld eigenaarschap aandacht nodig hebben. Ook bouwen aan vertrouwen vereist verdere aandacht.

Startcondities, faciliterend leiderschap en institutioneel ontwerp vormen de context van het samenwerkingsproces (Ansell & Gash, 2007) waarbinnen het bouwen aan vertrouwen een significante plek heeft.

Binnen het institutioneel ontwerp is het belangrijk om belanghebbenden te laten deelnemen aan het proces zodat hun belangen worden vertegenwoordigd (inclusiviteit), er moeten heldere basisregels zijn en er dient transparantie in het proces te zijn (Ansell & Gash, 2008). Transparantie behoort tot de drie meest genoemde belangrijke waarden in het onderzoek bij het verstevigen van de vertrouwenspositie (58.3 procent), naast veiligheid (66.7 procent) en soevereiniteit & autonomie (58.3 procent).

Er wordt door respondenten gewenst dat de overheid zich transparant opstelt qua houding. Eerlijkheid, openheid en transparantie zouden de boventoon moeten voeren in communicatie en er dient transparantie aanwezig te zijn tijdens het gebruik van SSI als systeem: “Kunnen zien wie wat inziet.”

Gewenste rol van bedrijfsleven, wetenschap en burgers

Tijdens dit onderzoek hebben respondenten een centrale rol gekregen om vanuit quadruple helix-context over de (gewenste en verwachte) rol van de vier betrokken actoren na te denken. Op de rol van de overheid (‘polity’) wordt verder ingegaan onder 5.1.6. Policy & Polity. De overige actoren zijn kort samengevat:

1) Bedrijfsleven

Het bedrijfsleven lijkt de minst grote vertrouwenspositie in relatie tot SSI te hebben. Gebrek aan vertrouwen is veelal te wijten aan het waargenomen gebrek aan controle over toegang die anderen hebben tot persoonlijke informatie. Informatiecontrole zoomt in op het waargenomen vermogen van de burger om het gebruik van persoonlijke informatie voor andere doelstellingen te kunnen controleren. Denk daarbij aan persoonlijke informatie die aan derden verkocht wordt door bedrijven, zonder dat burgers hier weet van hebben of toestemming voor hebben gegeven (Hoffman et al., 1999). Een positieve trigger die door een respondent benoemd wordt als oplossingsrichting: weten hoe SSI een bedrijf helpt, maak belangen en voordelen inzichtelijk, zodat de gebruiker zelf kan bepalen of hij of zij openstaat voor het gebruik van SSI. Investeren in oplossingen en tools die linken aan de belangen van bedrijven en toezicht houden op wat er met gegevens gebeurt (ook als je geen klant meer bent). In Estland kan men zien welke overheidsinstantie data raadpleegt en waarom.

Wanneer jouw privacy wordt geschonden, kun je daarmee naar de rechtszaal omdat Estland transparantie, privacy en integriteit als principes hanteert (Trommel, 2021). In dit geval kan de vraag ook toepasbaar gemaakt worden op het bedrijfsleven. Welk bedrijf raadpleegt data en waarom? Bart Jacobs gaf eerder in een interview aan dat het verstandig kan zijn de wallet niet alleen open source maar ook volledig non-profit te maken en commerciële partijen ervan uit te sluiten (Hartholt, 2021).

2) Wetenschap

Van de wetenschap wordt verlangd om veiligheid te onderbouwen, leerstoelen in te richten, informatie te delen in bijvoorbeeld wetenschappelijke magazines vanuit het open source-principe.

3) Burgers

Openheid en transparantie zijn essentieel in communicatie.
Het geven, delen en verduidelijken van informatie staan centraal.

4.2.4 Publieke waarden & ethiek

Deelvraag III:

Welke publieke waarden spelen een rol bij het verstevigen van een vertrouwenspositie?

In volgorde van belangrijkheid geven de volgende waarden uit het onderzoek in relatie tot SSI een antwoord op de deelvraag: veiligheid, transparantie, soevereiniteit & autonomie, vrijheid en inclusie en exclusie (onder exclusie wordt verstaan; de mogelijkheid tot opt-out zonder nadelige consequenties).

Deelvraag IV:

Welke risico's zijn er te signaleren rondom SSI aangaande deze waarden?

Op de vraag welke risico's worden gesignaleerd, kwamen diverse antwoorden binnen. Een risico dat een aantal keer wordt benoemd, is inclusie. "Ik zie niet echt in hoe het inclusiviteit verbetert" en "Ik vind het belangrijk dat iedereen mee kan doen" worden genoemd. Evenals de optie om niet mee te kunnen doen "dat niet kiezen voor SSI ook mogelijk blijft, zonder dat er consequenties aan zitten". Angst voor te veel controle van de overheid en voor misbruik van kwaadwillenden (veiligheid) komen ook terug in de antwoorden.

4.2.5 Vertrouwen, risico & vertrouwensmodellen

Vertrouwen is de meest kritieke factor voor succesvolle samenwerking (Dunn-Cavelty, 2009).

Leiderschap is van groot belang om partijen bij elkaar te brengen (Bryson et al. 2006; Ansell & Gash, 2007). Daarbij is vertrouwen van grote waarde in samenwerkingsverbanden.

Er is tijd voor nodig om te bouwen aan vertrouwen, maar het kan ook snel beschadigd worden (Ansell & Gash, 200; Emerson et al., 2012).

Om te kunnen bouwen aan vertrouwen is het belangrijk om vaak interactie te hebben (Vangen & Huxham, 2003, p.11). Naast vertrouwen hebben ook risico's invloed op het gedrag (Gefen et al. 2003). Meer risico's betekent een grotere mate van kwetsbaarheid. Vandaar dat ook kwetsbaarheid en vertrouwen aan elkaar gelinkt zijn (Gefen, 2000). Vertrouwen is noodzakelijk daar waar onzekerheid heerst, omdat vertrouwen risico's met zich meebrengt en kwetsbaarheid vereist van de partijen die in vertrouwen genomen worden (Hosmer, 1995).

Er werden door respondenten veel risico's en zorgen genoemd (zie ook hoofdstuk 7, bijlage 3) en op vier verschillende vertrouwensvlakken kwamen onzekerheden naar voren die duiden op verbetermogelijkheden om vertrouwen te verstevigen:

- systeemvertrouwen;
- vertrouwen in digitale gegevensuitwisseling;
- gebruikersvertrouwen;
- vertrouwen in het bedrijfsleven m.b.t. datagebruik.

Binnen het onderzoek werden vraagtekens geplaatst bij thema's als controle, macht en privacy-issues, gelinkt aan vertrouwen in de overheid als systeem en de (voor burgers onzichtbare) verkoop van data door het bedrijfsleven. Het grootste deel van de respondenten heeft volgens dit onderzoek weinig tot geen vertrouwen in digitale gegevensuitwisseling en ongeveer een derde van de twaalf respondenten is hier onzeker over. Een kleinere groep heeft er wel vertrouwen in. Gebruikersvertrouwen is ook een essentieel aspect voor nieuwe technologieën om succesvol geadopteerd te kunnen worden (Corritore, Kracher, & Wiedenbeck, 2003). Ook daar kwam onzekerheid over naar boven drijven in het onderzoek:

Deelvraag V:

Hoe zien burgers hun eigen rol als ‘Holder’ van de digitale identiteit in relatie tot de Identifier en Verifier op het gebied van vertrouwen en wat denken zij vanuit die positie nodig te hebben vanuit de overheid?

Een deelvraag die ingaat op gebruikersvertrouwen, leverde op:

- behoefte aan zelfcontrole over eigen data: “dat ik kan bepalen wat anderen wel en niet van mij mogen weten,” gevoel van zelfbeschikking; meer eigen verantwoording en bewustwording;
- verwachting om meer overzicht als gebruiker te krijgen;
- zorg over mate van kennis en continue alertheid bij de gebruiker: “je moet er mee bezig blijven en kritisch bekijken of je bepaalde toestemming wilt blijven verlenen;”
- weerstand; “ik doe niet mee” en “ik geloof niet meer zo in eigen beheer”, “ik geloof er niets van: Big Tech plukt alles uit de cloud.”

Als behoefte werd ‘kennis’ benoemd om met het juiste ‘gedrag’ het systeem te kunnen beheren, maar ook de mogelijkheid om zelf over eigen data te kunnen beschikken. Meer controle, betekent minder risico, concluderen Das & Teng (2001 in Geutjes, 2013).

Weerstand van respondenten kan een aanleiding zijn om na te denken of zorgen weggenomen kunnen worden door het versterken van het SSI-systeem en het verstrekken van informatie (‘kennis’) daarover en de dialoog over onzekerheden aan te gaan.

Vertrouwen kan gemanaged worden met vertrouwensmanagement.

Vertrouwensmanagement kijkt naar drie karakteristieken in de vorm van het ABI-model; het vermogen; de vaardigheden (‘ability’); welwillendheid (‘benevolence’) en integriteit (‘integrity’). De aspecten integriteit, welwillendheid en vermogen zijn van invloed op vertrouwen, maar ook op degene die vertrouwd wordt in het ‘Trust in leadership model’ van Burke (2007) en is daarom ook als leiderschapsmodel te gebruiken om vertrouwen daarin te begrijpen. Uit het onderzoek komen signalen dat er sprake is van een laag systeemvertrouwen waarin de ‘agenda’ niet helemaal vertrouwd lijkt te worden en er is een behoefte aan transparantie (ook met betrekking tot het communiceren van doelstellingen). Ook wordt er door een respondent twijfel uitgesproken over de ICT-vaardigheden (‘ability’) van de overheid.

Het tonen van eerlijkheid en morele en ethische beginselen duiden op integriteit (Paliszkievicz et al., 2015). Er wordt een grote mate van integriteit (en eerlijkheid, openheid en transparantie) verwacht vanuit de overheid aangaande SSI.

Zorgen over misbruik van gegevens en privacy die naar voren komen in het onderzoek zijn zorgen over integere omgang van data binnen het SSI-systeem. Door opkomende technologieën, is het makkelijker om data met derden te delen. Daarin ligt ook het risico op het verliezen van vertrouwelijkheid; een belangrijke factor in het bouwen aan vertrouwen (Culnan & Armstrong, 1998 in Mukherjee et al. 2003). Raakvlakken met welwillendheid ('benevolence') zijn in het onderzoek niet voldoende naar voren gekomen; een suggestie kan zijn om dit aspect in een volgend onderzoek beter uit te vragen onder respondenten.

In het 'model voor het bereiken van succesvolle organisatorische prestatie' komt vertrouwensmanagement ook aan de orde en zijn naast welwillendheid, integriteit en vermogen ook openheid en transparantie, afhankelijkheid, communicatie, congruentie en consistentie en betrouwbaarheid opgenomen als essentiële pijlers (Paliszkiewicz et al., 2015). Uit het onderzoek komen openheid en transparantie en communicatie als essentiële aandachtspunten naar voren; evenals *onafhankelijkheid* (autonomie) in de vorm van zelfbeschikking en controle over data en de mogelijkheid tot in- en exclusie aan het SSI-systeem. Betrouwbaarheid (vrij vertaald naar vertrouwen) vergt nader onderzoek op tenminste de vier soorten vertrouwen: systeemvertrouwen, vertrouwen in digitale gegevensuitwisseling, gebruikersvertrouwen en vertrouwen in het bedrijfsleven m.b.t. datagebruik. Congruentie en consistentie zijn niet naar voren gekomen in dit onderzoek en kunnen nader verkend worden in toekomstig onderzoek. Paliszkiewicz (2015) laat in het model zien dat leiderschap van invloed is op vertrouwensmanagement. Op gewenst leiderschap in de vorm van een duidelijke rol vanuit de overheid wordt verder ingegaan.

4.2.6 Policy & Polity

De verwachtingen die burgers van de overheid hebben, veranderen. Ook de overheid moet daar in haar rol en houding en inrichting van governance op innovatieve wijze in meegaan "om te komen tot een nieuwe manier van samenwerken" (Anderson et al. 2014).

Volgens Mulder (2019) valt de decentralisatie van de macht over data en technologie samen met de noodzaak om maatschappelijke problemen en de onvrede over het klassieke beleid en bestuur van de overheid op te lossen. Dit kan leiden tot heroriëntatie op de rol en het functioneren van de overheid (Mulder, 2019). De rol die de overheid kan innemen bij de (mogelijke) implementatie van SSI staat hier centraal, in een samenleving die steeds meer waarde-gedreven is (Carayannis & Campbell 2022).

Rol van de overheid ('polity')

Vanuit de rol van de overheid als institutionele entiteit ('polity') is gekeken naar de (gewenste) rol van de overheid in relatie tot nieuwe technologie; in dit geval SSI (Mulder, 2019). Dit haakt aan op *deelvraag VI*:

Welke waarde-creërende oplossingen kunnen vanuit de overheid - en vanuit de samenwerking van de quadruple helix - geboden worden om het vertrouwen in SSI (digitale identiteit) te vergroten en adaptie van SSI succesvol te maken?

Respondenten hielpen mee met het bedenken van oplossingsrichtingen die tegelijkertijd een aantal aanbevelingen markeren:

- Minimaliseer risico's door te beschermen en controleren (toetsen) als overheid;
- Creëer mogelijkheden voor burgers zelf om toegang te verlenen en weigeren; opt- in en opt-out; zelfbeschikking;
- Zorg voor in- en exclusie (mogelijkheid tot exclusie van SSI zonder consequenties);
- Bied opties als 'audit trails' om na te kunnen gaan wie data benadert of gedeeld heeft;
- Informeer open, transparant en begrijpelijk en zorg voor voldoende informatie om kennis te vergroten en betrokkenheid onder burgers te vergroten; zorg dat de doelstelling vanaf het begin helder is; zorg voor een transparante niet-belerende houding;
- Vergroot kennis bij de overheid en probeer het tempo te verhogen;
- Bied altijd voorbeelden met consequenties wanneer het data betreft.
Voorbeeld: "Als je deze toestemming geeft, dan houdt dat in dat.... voor de tijdsduur van..."
- Zorg voor heldere kaders in de vorm van regels en afspraken; zorg voor balans;
- Neem alle kritiek van alle betrokken burgers en partijen serieus;
- Denk (samen met alle actoren) na over de gewenste verbinding met de EU.

Beleidspectief ('policy')

Binnen 'policy' wordt gekeken naar het beleid van de overheid. Wanneer we naar beleidsvoering kijken, zien we de sturing volgens de logica van hiërarchie en markt steeds meer ruimte geven aan sturing volgens de logica van het netwerk of tenminste een gecombineerde strategie inzetten (Van Damme & Pattyn, 2015). In elk geval bestaat er een behoefte dat er geluisterd wordt naar input van alle betrokkenen binnen het netwerk en dat er op autonome wijze keuzes gemaakt kunnen worden rondom SSI (o.a. opt-in en opt-out) op basis van transparante input.

Kansen en mogelijkheden en risico's en bedreigingen zijn vanuit burgerperspectief in kaart gebracht, door respondenten hiernaar te vragen (Mulder, 2019). Er kan vanuit beleidsperspectief naar de uiteenzetting van resultaten gekeken worden. Het geeft een beeld welke onderwerpen aandacht nodig hebben om burgers gerust te stellen, te informeren, het systeem mogelijkverder te ontwikkelen en indiceert waar mogelijk voordelen voor burgers behaald kunnen worden in termen van efficiëntie. Een overzicht van de geschetste risico's, bedreigingen, kansen & mogelijkheden is weergegeven in bijlage 3.

Een beleidskans waar dit onderzoek licht op lijkt te werpen is: wees open en transparant over doelstellingen rondom SSI en communiceer hier op dezelfde wijze over via regelmatige interacties met betrokken actoren. Welk beleidsmodel daarvoor ingezet kan worden, is nader te onderzoeken. Bij de incrementele benadering, worden diverse actoren betrokken en wordt vaak in non-lineaire stappen richting een verandering gewerkt. Een gemengd model zou ook kunnen werken, waarbij de volgorde van de beleidsstappen strategisch wordt gekozen, meerdere actoren beperkte beslissingsmacht krijgen en de belangen onderhandelbaar zijn (Reijmerink, 2003). Door transparantie te vergroten, keuzes te motiveren en belangen van alle actoren te bespreken en mee te nemen in het besluitvormingsproces, kan voldaan worden aan democratische en integriteitsnormen die steeds meer aandacht krijgen, zoals Popelier et al. (2008) het omschrijven (Van Damme & Pattyn, 2015).

5 Conclusies, aanbevelingen & discussie

De gewenste leiderschapsrol en bijbehorende (door burgers gewenste) beleidsacties in relatie tot SSI komen hier samengevat aan bod. In paragraaf 5.1, de conclusies en aanbevelingen, wordt de onderzoeksvraag beknopt beantwoord aan de hand van drie overkoepelende ontwikkelpunten voor beleidsverbetering en concrete aanbevelingen voor nader wetenschappelijk onderzoek. In paragraaf 5.2 worden verdere beperkingen aan dit onderzoek in de discussie besproken.

5.1 Conclusies en aanbevelingen

In hoofdstuk 4 werden de deelvragen van dit onderzoek behandeld in de analyse om vervolgens een antwoord te kunnen geven op de onderzoeksvraag waarmee dit onderzoek geopend werd:

Wat kan de overheid bieden om samen met quadruple helix actoren verder te bouwen aan vertrouwen van burgers in de (mogelijke) komst en adaptatie van Self-Sovereign Identity (SSI)?

Een analyse van de onderzoeksresultaten over het onderzoeksonderwerp SSI in relatie tot vertrouwen doet, naar bevinding in dit onderzoek, stof opwaaien. Gefen (2003) leerde ons dat risico's en de mate van vertrouwen een effect hebben op gedrag. Er worden in relatie tot SSI veel risico's benoemd en er wordt niet altijd even makkelijk over de implementatie van SSI gedacht. Het vertrouwen lijkt niet altijd even aanwezig, en dat lijkt zich te uiten in de weerstand die in de vorm van houding en gedrag ten opzichte van SSI geboden wordt binnen dit kleinschalige onderzoek onder burgers. Daaruit maak ik voorzichtig op dat er werk te verrichten is om samen verder te kunnen bouwen aan vertrouwen om (mogelijke) nieuwe technologieën als SSI goed te kunnen laten landen. Aan de hand van de resultaten en analyse in hoofdstuk 4 kunnen conclusies worden getrokken en aanbevelingen worden gedaan die mogelijk het beleid ('policy') op dit vraagstuk kunnen verbeteren. De drie concrete ontwikkelpunten die uit dit onderzoek naar voren zijn gekomen, zijn: verstevig de rollen, geënt op de transformatie van de rol van de overheid vanuit 'policy-perspectief'; verbeter de communicatie/informatievoorziening en vergroot kennis over SSI en onderzoek nader hoe tenminste vier soorten vertrouwen te verstevigen. Hieronder worden deze conclusies en aanbevelingen uit het onderzoek verder toegelicht:

1) Verstevig de rollen

Er is gekeken naar gewenste rol van de vier quadruple helix-actoren.

In dit onderzoek zijn de vier quadruple-helix-rollen onder de loep genomen, de focus ligt in dit onderzoek echter op de rol van de overheid (zie voor een samenvatting van de overige gewenste rollen bijlage 3 en paragraaf 4.2.3).

Gewenste rol van de overheid

"Vertrouw maar verifieer" zei voormalig president van de Verenigde Staten Ronald Reagan ooit (Covey & Merrill, 2006). De overheid heeft als gewenste functie optreden als beschermer en controleur.

Cheskin (1999) concludeerde (destijds in relatie tot consumentenvertrouwen) dat de eerste meest noodzakelijke stap om vertrouwen te kunnen garanderen, is om ervoor te zorgen dat persoonlijke informatie bewaakt wordt. Hierop wordt aangevuld dat meer controle minder risico tot resultaat heeft (Das & Teng, 2001 in Geutjes, 2013). De overheid kan (technologische) mogelijkheden onderzoeken om burgers zelfbeschikking en eigen controle over data te geven. Zorg voor verificatiemogelijkheden en bied verificatie-diensten aan als ‘audit trails’ om na te gaan wie data benadert of gedeeld heeft. Bied mogelijk ook opties tot opt-in, zoals een respondent benoemde:

“Geen automatische data-uitwisseling tenzij daarvoor opt-in is gegeven, niets o.b.v. opt-out. Het moet zijn alsof het een kluisje is dat bij mij thuis staat met mijn data erin. De overheid belt aan bij de voordeur, vraagt om data, ik beslis wat ik wel en niet geef, en doe het kluisje weer dicht”; zorgdragen voor in- en exclusie van burgers (mogelijke exclusie of opt-out zonder consequenties); open en transparant en begrijpelijk communiceren; zorgen dat de doelstelling vanaf het begin helder is en niet-belerend opstellen maar transparant; kennis vergroten bij de overheid, op ICT-vlak en waar mogelijk het tempo verhogen; voorbeelden geven met consequenties wat data betreft; heldere kaders scheppen in termen van regels en afspraken; iedereen serieus nemen en daarop acteren en nadenken over de verbinding met de EU. Al deze zaken kunnen meegenomen worden in beleidsontwikkeling; maar ook om de verdere ontwikkeling van het SSI-systeem te kunnen optimaliseren, met bijvoorbeeld mogelijke functies waar burgers behoeften aan hebben om zelf te kunnen controleren en toezien en als burger keuzemogelijkheden en daarmee autonomie te behouden.

Samenwerking & interactie

- *Verricht verder onderzoek naar het bevorderen van een inclusieve samenwerking met burgers vanuit een netwerkbenadering;*

Vertrouwen speelt een rol in het begin van de samenwerking (Ansell en Gash, 2007). Kan de ontwikkeling van SSI al vanuit de verkenningsfase vanuit een quadruple-helix-perspectief benaderd worden? Bestaat er bij burgers behoefte om in een premature fase al betrokken te worden bij een ontwikkelproces rondom technologische innovatie en zo ja, hoe betrek je ze beter bij het proces? Wat is de gewenste interactievorm van burgers in relatie tot de overheid bij nieuwe ontwikkeltrajecten?

Bij netwerkbenadering staan vertrouwen en samenspel centraal en is er geen eenrichtingsverkeer maar meer-richtingsverkeer (brengen en halen) (Brennenraedts et al. p. 44). Co-creatie in relatie tot SSI, collaboratieve innovatie en collaborative governance bieden een startpunt voor verder onderzoek. Dit kan inzicht geven hoe bij burgers zowel betrokkenheid bij, als vertrouwen in, deze nieuwe technologie vergroot kunnen worden. Design-thinking inzetten kan tevens een mogelijkheid zijn om vanuit samenwerking van alle actoren onderzoek in te zetten naar verdere mogelijkheden tot implementatie van SSI.

- *Onderzoek de rol van burgers in relatie tot de quadruple helix.*

Het geven van betekenis aan complexe problemen wordt bevorderd wanneer verschillende actoren met verschillende kennisniveaus, ervaring en perspectieven met elkaar in contact zijn; dat bevordert nieuwe oplossingen. Het toetsen van deze oplossingen gaat beter wanneer verschillende actoren met verschillende achtergronden risico's en kansen bestuderen. Vanuit participatie en dialoog is er een grotere kans dat het invoeren van oplossingen geoptimaliseerd en gepromoot wordt door actoren die samenwerken en vaak ook ambassadeur worden van de oplossing waar zij zelf aan bijgedragen hebben (Bommert, 2010).

Een onderzoek kan zijn hoe je burgers beter vanaf de start meeneemt in het proces op basis van het raamwerk van Ansell & Gash (startcondities, faciliterend leiderschap en institutioneel ontwerp) (Ansell & Gash, 2008). Bijvoorbeeld door de startcondities op dit moment in de tijd te onderzoeken en wat er aan (faciliterend) leiderschap nodig is om elkaar te kunnen vertrouwen.

Leydesdorff & Etzkowitz (2003) in Carayannis & Campbell (2022, p. 69) vragen zich in de context van quadruple helix-samenwerking af of je 'het publiek' oftewel de burgers wel als een vierde pijler in de quadruple-helix moet opnemen, of dat de burgerlijke maatschappij als het fundament van de onderneming van innovatie gezien moet worden (als basis en niet als vierde pijler). Een uiting die verder uitgesloten is van de theorie binnen dit onderzoek, maar die benoemd wordt als aanbeveling, omdat het een interessant haakje kan zijn voor verder onderzoek.

Governance, leiderschap & bescherming van waarden

- *Onderzoek diverse vormen van leiderschap die een gunstig effect kunnen hebben op het vergroten van vertrouwen rondom mogelijke implementatie van nieuwe technologie.*

Bijgaande vormen komen niet (of niet uitgebreid) terug in het theoretisch kader, maar kwamen wel naar voren tijdens literatuuronderzoek en zijn interessant bevonden voor verdere studie; denk aan complexiteit-leiderschapstheorie, meta-governance & actor network theory als in te zetten leiderschapsmogelijkheden om vertrouwen mogelijk te verstevigen.

- *Bekijk welke leiderschapsrollen gunstig zijn voor een positieve uitwerking op het minimaliseren van de diverse vertrouwensissues die lijken te bestaan.*

Zo is de mediator “een leider die faciliteert door te helpen met bemiddelen en het voeden van relaties tussen belanghebbenden” (Ansell & Gash, 2012, p. 6). Deze wordt vaak ingezet als de belanghebbenden er samen niet uitkomen. De inzet van deze rol zou kunnen leiden tot het uitspreken van het conflict en het stabiliseren van voorwaarden zodat er een positieve interactie kan plaatsvinden en er kan worden gebouwd aan vertrouwen onder belanghebbenden (Ansell & Gash, 2008). De faciliterende leider heeft tot doel te verzekeren dat er integer gehandeld wordt in het samenwerkingsproces (Ansell & Gash, 2008). Wetenschappelijk onderzoek op dit thema in relatie tot SSI kan helpen vertrouwensissues op te lossen aan de hand van wenselijke leiderschapsrollen.

- *Houd belangrijke waarden die genoemd zijn continu in het vizier bij beleidsontwikkeling.*

Zorg ervoor dat de belangrijke waarden die uit het onderzoek naar voren zijn gekomen te allen tijde optimaal beschermd kunnen worden. Onderzoek hoe risico's, waarbij waarden in het geding komen, aangevlogen kunnen worden om ze te minimaliseren of als risico uit te sluiten. Leg uit hoe SSI als systeem die waarden beschermt of in de toekomst mogelijk kan gaan beschermen en hoe de overheid beschermt en daarop toeziet. Het is mogelijk om vertrouwen te versterken door de doelstelling - vanaf het begin - helder te formuleren en duidelijk te maken welke publieke waarde er wordt gecreëerd (Vangen & Huxham, 2003).

2) *Verbeter de communicatie/informatievoorziening en vergroot kennis over SSI (vanuit openheid & transparantie);*

Het onderzoek toont aan dat een groot deel van de respondenten onvoldoende bekend is met SSI, de beschikbaarheid van informatie rondom SSI op dit moment onvoldoende lijkt, en er een behoefte aan informatie en kennis bestaat. Communicatie, openheid en transparantie zijn

een onmisbaar aspect om aan vertrouwen te bouwen, zo blijkt uit de diverse vertrouwensmodellen. Informatie uitwisselen draagt bij aan het verstevigen van vertrouwen en dat is een groot aandachtspunt dat naar voren is gekomen in dit onderzoek (Paliszkiewicz et al., 2015 en Burke et al. 2007).

Respondenten ervaren onduidelijkheid over SSI en zitten met vragen die een antwoord nodig hebben (hoe het werkt, waarom het werkt, wat de voordelen zijn, wat het burgers, overheid, wetenschap en het bedrijfsleven brengt¹⁰). Probeer daar zo transparant mogelijk antwoorden op te formuleren. Zorg voor een betere informatievoorziening, neem burgers daarin mee vanaf de start en al in verkenningsfasen van (mogelijke) implementaties en licht ze stapsgewijs voor over de ontwikkelingen die er zijn. Zorg voor heldere, eenvoudige verwoording met inzet van de Nederlandse taal.

Het inzetten van heldere, open, eenvoudige communicatie en informatie rondom SSI - als beleidsinstrument - zou ook kunnen helpen om zorgen rondom de (mogelijke) komst van SSI te reduceren door concrete oplossingen aan te bieden op voorziene zorgen. Informeer duidelijk en transparant aan de hand van een campagne; geef openheid van informatie; bespreek consequenties (transparantie); voorzie websites van informatie die daarbij ondersteunt. Bouw diverse communicatiemomenten in om interactie te verhogen en burgers aangehaakt te houden op het proces. Wanneer samen kennis opgebouwd wordt, kan dit bijdragen aan een betere overeenstemming over een onderwerp of probleem en de mogelijke maatregelen (Hmelo-Silver & Barrows, 2008 in Van den Brink, 2017). Bovendien kan “het integreren van kennis voor nieuwe kennis zorgen” (Van den Brink, 2017, p. 18). Een aanbeveling kan zijn om naast het vergroten van interactiemomenten met alle belanghebbenden ook reflectiemomenten in te bouwen om te bespreken wat de effecten zijn of zijn geweest van een bepaalde keuze en op basis daarvan gezamenlijk nieuwe keuzes te maken en te motiveren. Zo kun je op non-lineaire wijze ook besluiten terug te gaan naar een andere stap binnen het beleidsproces en het kan lucht geven om te weten dat keuzes niet altijd definitief en onveranderlijk zijn.

¹⁰ Zie tevens hoofdstuk 7, bijlage 3 voor specifieke gewenste informatiebehoefte onder respondenten.

3) ***Onderzoek hoe het vertrouwen te verstevigen door nader onderzoek onder actoren op tenminste vier soorten vertrouwen: systeemvertrouwen; vertrouwen in digitale gegevensuitwisseling; gebruikersvertrouwen ('user trust') en vertrouwen in bedrijfsleven met betrekking tot datagebruik.***

Bouw dus niet alleen aan vertrouwen door inzet van een betrouwbare digitale infrastructuur zoals Knops eerder verwoordde (Kamerstukken II, 2020/21, 26643, nr. 743); maar aan vertrouwen in een bredere context.

- Bedenk als overheid, bij elke stap die gezet wordt, wat er aan communicatie, informatie, dialoog, interactie en systeemontwikkeling nodig is om het vertrouwen van burgers in (mogelijke) nieuwe technologieën als SSI te laten groeien en faciliteer daarin. Er zijn veel interacties nodig om vertrouwen op te kunnen bouwen (Vangen & Huxham, 2003, p. 11).
- Het verdient een aanbeveling om verder inhoudelijk onderzoek te doen naar SSI in relatie tot het ABI-model ('ability, benevolence & integrity') en vertrouwensmodellen.
- Wanneer onderzoek gedaan wordt naar het vertrouwen in het bedrijfsleven met betrekking tot data-gebruik; onderzoek dan ook of een oplossing zoals Jacobs (2021) deze aandraagt een mogelijkheid is; om de wallet volledig non-profit te maken en commerciële partijen ervan uit te sluiten (of op andere wijzen aan te haken, met bijvoorbeeld burgerlijke keuzes voor opt-in en opt-out). Meet vervolgens wat het mogelijke effect van een publieke portemonnee kan zijn op het vertrouwen in SSI (Hartholt, 2021).
- Weerstand van respondenten en wantrouwen ten opzichte van (mogelijke) implementatie van SSI, en mogelijk ten opzichte van het systeem, kan een aanleiding zijn om na te denken of zorgen weggenomen kunnen worden door het versterken van systemen en het verstrekken van informatie daarover en de dialoog over onzekerheden aan te gaan. Sluit daarbij niet uit, maar neem alle vormen van kritiek serieus mee in het 'open' gesprek. Het kan ook een aanbeveling zijn om leiderschap, vertrouwen en weerstand als gecombineerde variabelen in toekomstig onderzoek te integreren.

Volgens De Mul (2016) gaan systeemvertrouwen en interpersoonlijk vertrouwen vaak hand in hand. Worden leiders vertrouwd in hun leiderschap en functioneert het systeem, dan volgt er weinig weerstand. Wat is in relatie tot SSI de oorzaak van de waargenomen weerstand?

Verder verdient het een aanbeveling om verder kwantitatief onderzoek op het gebied van SSI in relatie tot vertrouwen te verrichten, met een grotere en gevarieerde groep respondenten.

In het coalitieakkoord ‘Omzien naar elkaar, vooruitkijken naar de toekomst’ staat beschreven: *“De sterke overheid die wij voor ons zien heeft oog voor de menselijke maat, is begrijpelijk, bereikbaar en aanspreekbaar door inwoners, en herstelt op die manier het vertrouwen”* (Rijksoverheid.nl, 2022). Groei daar naartoe ook in het kader van SSI, lijkt een samenvattende conclusie uit dit onderzoek, met toevoeging van de aanbeveling: doe dat open, transparant en met aandacht voor zowel inclusie als exclusie. Dat ‘we’ er nog niet zijn, heeft dit onderzoek duidelijk gemaakt. Het vertrouwensfundament om een mogelijk nieuwe technologie als SSI te kunnen implementeren vraagt, naast een goede communicatie/informatievoorziening, om versteviging. Het aannemen van een stevige leiderschapsrol is essentieel om te kunnen bouwen aan de (vertrouwens)relatie met burgers als betrokken partner. Voordat we op de top een vlag kunnen plaatsen, kan het nog wel even duren, want er bestaat geen korte weg voor dit “menselijk streven” (‘human endeavour’), volgens Ansell & Gash (2008). Laat het dan tenminste een weg vol interessante onderzoeken en opwaartse resultaten zijn waarbij burgers en hun waarden centraal staan.

5.2 Discussie

5.2.1 Reflectie op wetenschappelijke en maatschappelijke relevantie

In de aanleiding zijn een aantal zaken vermeld waaraan dit onderzoek zowel wetenschappelijk als maatschappelijk kan bijdragen. SSI is een onderwerp waarover kennis ontbreekt, ook omdat het een technologische innovatie betreft die nog niet geïmplementeerd is. Deze thesis heeft een kennisbijdrage geleverd, waardoor het kennisgat gedeeltelijk weer iets gedicht is en kansen, bedreigingen, risico’s en zorgen in kaart gebracht zijn die ook in toekomstig wetenschappelijk onderzoek meegenomen kunnen worden om tot verbeteringen te komen en meer inzicht te verschaffen in wat voor burgers noodzakelijk is om tot een (mogelijke) succesvolle implementatie van SSI-technologie te kunnen komen.

De rol die de overheid volgens burgers mag innemen rondom de implementatie van SSI is hier uitgebreid aan het licht gekomen. Dit kan bijdragen aan verdere beleidsstrategieën, zoals ook Mulder (2019) aanstipt. Er zijn verbanden gelegd tussen (mogelijke) implementatie van SSI-technologie en diverse soorten vertrouwen en leiderschap wat een verdere basis kan vormen voor nader wetenschappelijk onderzoek. Ook het gebruikersvertrouwen rondom eigen databeheer is in kaart gebracht en kan daarmee een bijdrage leveren aan een (toekomstige) maatschappij die steeds autonomer lijkt te gaan functioneren. Bovendien heeft het onderzoek een uitgebreide literatuurlijst op deze overkoepelende kennisdomeinen opgeleverd die zowel nuttig als tijdsbesparend kan zijn voor verder onderzoek. Burgers spelen een belangrijke rol om (mogelijke) implementatie van SSI mogelijk te maken en zijn een belangrijke partner om in elk geval qua communicatie aangehaakt te houden tijdens het gehele (mogelijke) adoptieproces om te kunnen bouwen aan vertrouwen. Daarbij is transparantie de sleutel. Onderzoekstechnisch gezien verdient het aandacht om de verschuiving van triple helix naar quadruple helix-samenwerking rondom dit onderwerp verder uit te kristalliseren en het belang van collaboratieve innovatie, met daarin een belangrijke rol voor burgers, wetenschappelijk verder te kunnen onderbouwen. Het onderzoek laat zien dat de mogelijke implementatie van SSI gekoppeld is aan publieke waarden en dat veiligheid, transparantie, autonomie, vrijheid en in- en exclusie een belangrijke rol spelen en beschermd dienen te worden, wat ook als een overheidstaak aangeduid wordt. Dit onderzoek heeft het sentiment, dat een kleine groep burgers ervaart, naar voren gebracht en een aantal uitdagingen belicht die gemoeid zijn met de (mogelijke) implementatie van SSI. Het subjectieve veiligheidsgevoel dat ervaren wordt, de beleving van veiligheid, wordt door een groot deel van de respondenten niet als optimaal ervaren in relatie tot SSI en kan een rol spelen in verder wetenschappelijk onderzoek om beter bij te kunnen dragen aan het ervaren van een veilig gevoel binnen de maatschappij, vooral in relatie tot technologische innovatie. Het fundament van vertrouwen verstevigen is essentieel voor de mogelijke adoptie van SSI; dit onderzoek heeft in dat kader kort aangestipt welke knelpunten er rondom vertrouwen bestaan en dat dit vertrouwen verstevigd dient te worden. Niet alleen vertrouwen aangaande SSI-technologie en digitale gegevensuitwisseling, maar ook het systeemvertrouwen, gebruikersvertrouwen en vertrouwen in het bedrijfsleven (één van de belangrijke vier actoren) vereisen meer aandacht en oplossingen om het vertrouwen te vergroten en (mogelijke) adoptie van SSI te vergemakkelijken. Het onderzoek draagt daarmee bij aan het oplossen van vraagstukken die rondom adoptie van SSI bestaan.

Hoewel het Eindrapport SSI (2021) duidelijk maakt dat er rondom SSI primair verkenning van mogelijkheden en gewenste technische implementatie ingezet is, stipt dit onderzoek aan dat er ook in het beginstadium vanuit burgers een beter ingerichte (Nederlandstalige) informatievoorziening gewenst is, die burgers geïnformeerd en betrokken houdt bij ontwikkelingen. AlAwadhi (2019) indiceerde een kennisbehoefte rondom het bouwen van vertrouwen in e-government en de adoptie van een e-governmentdienst in relatie tot betrokkenheid van burgers. Dit onderzoek heeft daar door burgers te betrekken, in zeer brede zin aan bijgedragen en gesignaleerd waar verder onderzoek op ingericht kan worden.

5.2.2 Reflectie op onderzoeksmethodiek

Hoewel er aan dit onderzoek slechts twaalf respondenten hebben meegewerkt, en het daarom geen representatieve afspiegeling van de volledige populatie van Nederland genoemd mag worden, werpt het licht op een gevarieerd aantal perspectieven die er bestaan rondom de komst van SSI oftewel digitale identiteit. Het doel van dit onderzoek was om meer inzicht te scheppen in de mogelijkheden die de overheid kan bieden om vanuit quadruple-helix-perspectief, en dus ook de burgers inclusief, te bouwen aan het vertrouwen van burgers rondom de mogelijke komst en adaptatie van Self-Sovereign Identity (SSI). Door de reacties van de respondenten op de vragenlijst die daarop ingezet heeft, is een fractie van het kennisgat rondom deze thematiek gedicht. Zoals meerdere malen aangehaald in deze thesis, gaat vertrouwen gepaard met risico's. Omdat er rondom dit thema zeer uiteenlopende invalshoeken bestaan (variërend van een nieuwe technologie die zaken sneller laat verlopen tot aan privacy-en veiligheidsissues), is het wijsheid ruimte te bieden aan alle opinies. Een opinie kent echter emotie en kan leiden tot bepaald gedrag. Het is echter de vraag hoe stevig het fundament is waarop de opinie berust. Hebben alle partijen de juiste informatie ontvangen om een opinie te kunnen vormen? Of is er sprake van onwetendheid door een gebrek aan kennis over SSI waardoor het lastig is een mening te vormen over complexe vragen? (Fresco, 2011). Wanneer op dit moment Self-Sovereign Identity benoemd wordt zonder uitleg; zal de (ongeinformeerde) burger niet weten wat hiermee bedoeld wordt. De vragenlijst die is ingezet tijdens dit onderzoek heeft slechts een korte samenvatting gegeven van het begrip 'SSI' waardoor de onderzoeksresultaten van een aantal respondenten berust op primaire ingevingen van burgers rondom de thematiek of op resultaten vanuit een online zoekmachine.

Er bestaat een kans dat de antwoorden die gegeven zijn, gefundeerd zijn op eerder gezette stappen vanuit de overheid (dat kan ook zijn onvrede over ander gevoerd beleid). Dit kan ervoor gezorgd hebben dat er startcondities bestaan die van invloed zijn op de beeldvorming rondom SSI en de overheid. Slechte startcondities kunnen de samenwerking ontmoedigen (Ansell & Gash, 2008). Heerst er bijvoorbeeld vanuit eerdere ervaring al wantrouwen, dan staat dit mogelijkwerwijs een implementatie van een nieuwe technologie in de weg. In dit kader zou ook gesproken kunnen worden over een mogelijke integriteitsparadox die resultaten kan beïnvloeden. Door veel focus te leggen op integriteitsgevallen, lijkt het alsof er meer integriteitsgevallen zijn, waardoor mensen weinig vertrouwen hebben in de overheid. Iemand die te maken heeft gehad met - een voorbeeld - de effecten van de toeslagenaffaire, heeft een ander beeld van de overheid, dan iemand die hier nooit eerder van gehoord heeft (Huberts en Lasthuizen, 2005; De Graaf en Huberts, 2011; Kaptein en Reenen, 2001). Het is ook een gegeven dat de respondenten zijn opgehaald uit het persoonlijke LinkedIn-netwerk van de onderzoeker; hierdoor is er kans op inclusie en exclusie van doelgroepen werkzaam binnen een bepaalde sector. Mogelijkwerwijs kunnen selectiebias of andere vormen van misrepresentatie van de populatie optreden. Daarbij gaat het erom dat het aantal en de soorten respondenten inhoudelijk representatief zijn (Hak, 2004). Zelfselectiebias treedt mogelijkwerwijs op als personen zichzelf aanmelden voor onderzoek, wat kan leiden tot vertekende data omdat het niet direct betekent dat de respondenten representatief zijn voor de gehele populatie. Het kan ook zo zijn dat een bepaalde doelgroep zich eerder geroepen voelt om mee te doen aan het onderzoek, bijvoorbeeld omdat er een duidelijke mening bestaat richting het onderzoeksonderwerp. Daarmee wil ik als subjectief voorbeeld omschrijven dat het mogelijk is dat iemand bijvoorbeeld een review geeft als iets juist heel slecht of heel goed gaat. En dat er een keuze kan zijn om niet deel te nemen, wanneer iets gemiddeld gaat of er een gemiddelde mening of interesse ten opzichte van het onderwerp bestaat. Omdat respondenten zelf de keuzemogelijkheid hebben om mee te doen aan het onderzoek, zou dat effect hier ook kunnen optreden. In een volgend onderzoek zou je randomisatie kunnen toepassen om dit tegen te gaan. Een andere bias die kan optreden is ‘undercoverage bias’ (ondervertegenwoordigingsbias) waar online vragenlijsten gevoelig voor zijn. Het sluit bijvoorbeeld mensen zonder internet uit (Scribber, 2023). Dit onderzoek, met een gering aantal respondenten, kan niet garant staan voor een goede afspiegeling van de samenleving, maar geeft wel een impressie van het sentiment dat er bestaat dankzij de variëteit van 20 vragen, op basis waarvan verder kwalitatief en kwantitatief onderzoek verricht kan worden.

In de onderzoeksresultaten in hoofdstuk 4 worden een aantal diagrammen weergegeven die verbonden zijn aan (kwantitatieve) percentages. De reden hiervoor is het snel, kort en overzichtelijk onderzoeksresultaten weer te geven. Omdat er slechts twaalf respondenten deelnamen aan dit onderzoek, moet gezegd worden dat deze percentages niet als representatief gezien mogen worden. Daarvoor is de steekproef te klein. Wanneer er een grootschaliger onderzoek gedaan wordt, kan er inhoudelijk ook meer gezegd worden over eventuele kwantitatieve percentages en verhoudingen. Op dit onderzoek werd door een respondent ook een kritische opmerking geplaatst: “De vragen zijn te sturend en de uitkomsten kunnen makkelijk voor onethische doeleinden ingezet worden.” Bij dit onderzoek is zo veel mogelijk gebruik gemaakt van open vragen om zo min mogelijk te sturen; maar zoals eerder benoemd, kan het geven van voorbeelden al een sturend effect hebben. Mijn intentie als onderzoeker was om burgers vanuit zoveel mogelijk openheid te laten reageren, zodat duidelijk wordt wat er bij hen speelt op het gebied van (mogelijke) implementatie van SSI, en het vergroten van vertrouwen daarin, en ze te laten meedenken over oplossingen die werkbaar zijn voor hen. Voor een volgend onderzoek zou het een idee zijn om voorafgaand een studie van de manier van vragenstellen te maken om de vragenlijst te kunnen optimaliseren.

5.3 Slotwoord

Wanneer we het hebben over het stellen van vragen, spreek ik graag met Gandhi’s woorden: “The power to question is the basis of all human progress.” Laten we vooral proberen om - onszelf en elkaar - de juiste vragen te blijven stellen, denkkracht te bundelen om (toekomst)scenario’s te schetsen en te blijven anticiperen op de vele kleine stappen die worden gezet richting een grote verandering. Een verandering waarin technologie een grote rol zal spelen en steeds meer de dialoog met ons aan zal gaan.

Aan het einde van mijn thesis-proces aangekomen, opperde iemand: heb je ChatGPT al eens gevraagd naar SSI? Ik had het systeem nog nooit gebruikt en het leek me een interessant experiment; een digitaal systeem mijn onderzoeksvraag opgeven.

Ik voerde op 20 juli 2023 mijn exacte onderzoeksvraag in op ChatGPT (in het Nederlands) en kreeg als (letterlijk) antwoord:

“Self-Sovereign Identity (SSI) is a concept that empowers individuals to have full control over their own digital identities, including how their personal information is shared and used.

Building trust among citizens and other stakeholders regarding the potential adoption of SSI requires collaboration among quadruple helix actors, which typically include government, industry, academia, and civil society. Here are some ways in which the government can work with these actors to foster trust and promote the adoption of SSI:

1. **Education and Awareness:** The government can lead public awareness campaigns and educational initiatives to inform citizens about the benefits of SSI, how it works, and how it enhances data privacy and security. This education should also address potential concerns and misconceptions related to SSI.
2. **Stakeholder Engagement:** Encourage active involvement and engagement of all quadruple helix actors in the development and implementation of SSI solutions. This ensures that diverse perspectives and expertise are considered, leading to more robust and inclusive solutions.
3. **Regulatory Framework:** The government can establish a clear and supportive regulatory framework for SSI, addressing issues such as data protection, consent, liability, and interoperability. A well-defined regulatory environment can provide businesses and citizens with confidence in adopting SSI.
4. **Pilot Projects and Demonstrations:** Support pilot projects and real-world demonstrations of SSI implementations in collaboration with different quadruple helix actors. These projects can showcase the benefits of SSI and address any challenges that may arise.
5. **Certification and Standards:** Encourage the development of industry standards and certification processes for SSI solutions. Standardization helps ensure interoperability, security, and trustworthiness of SSI systems.
6. **Privacy by Design:** Advocate for the adoption of privacy-by-design principles in the development of SSI solutions. This means embedding privacy and data protection measures into the core architecture of the system, ensuring user trust.
7. **Data Protection and Security:** Work with industry and academia to establish best practices for data protection and security in SSI systems. Regular audits and security assessments can help maintain the integrity and reliability of SSI implementations.
8. **Collaborative Platforms:** Create collaborative platforms or forums where quadruple helix actors can openly discuss concerns, share best practices, and collaborate on addressing challenges related to SSI.

9. User-Centric Design: Encourage SSI solutions that prioritize user experience and usability. A user-centric approach can enhance user trust and acceptance of SSI systems.
10. Legal Identity Support: Work towards providing legal recognition and support for SSI as a valid form of identity. Collaborate with civil society and industry to ensure SSI aligns with legal requirements and can be used in various contexts.
11. Digital Literacy Initiatives: Promote digital literacy programs to ensure that citizens are equipped with the knowledge and skills to use SSI effectively and responsibly.
12. Responsible Use of Data: Promote responsible data usage and emphasize the importance of data minimization and consent in SSI systems.

By working closely with quadruple helix actors and taking a comprehensive approach, the government can play a pivotal role in building trust and facilitating the successful adoption of Self-Sovereign Identity solutions for the benefit of citizens and society as a whole.”

(ChatGPT, persoonlijke communicatie, 20 juli, 2023)

Een behoorlijke denk- en verbindingskracht en goede aanvullingen; althans dat is mijn persoonlijke mening. Heel eerlijk; dergelijke kwalitatieve uitkomsten had ik nog niet verwacht. In de context van dit onderzoek vraag ik mijzelf voorzichtig af of het helix-model er in de toekomst wellicht een ‘digitale’ actor bij gaat krijgen, ‘wie of wat dat dan is’ en hoe we hier qua vertrouwen tegenaan gaan kijken en wat dit voor ons als mens - in welke rol dan ook - gaat betekenen. Er valt nog zo veel te onderzoeken. Mijn advies: elke medaille heeft een keerzijde; bekijk alle kanten vanuit een breed en open perspectief en blijf vooral zelf nadenken en voelen over maatschappelijke thema’s als technologische innovatie en de mogelijke effecten die de veranderingen op ons als mens kunnen hebben. De laatste dagen voor de uiterste inleverdatum van mijn scriptie was ik op reis in Bosnië. Daar sprak ik iemand die digitalisering onomkeerbaar noemde. Hij was daarnaast bewust uit ‘het systeem’ gestapt en zei: we creëren gewoon een parallelle wereld. Maar is dat wat we daadwerkelijk willen? We leven namelijk samen op het globale systeem dat we ‘de wereld’ noemen. Ik kan niet in een glazen bol kijken, maar als we de verbinding met elkaar verliezen en in opponenten gaan denken, ben ik bang dat we het zwaar gaan krijgen met z’n allen. Daarom stip ik hier in mijn persoonlijke pleidooi het belang van verbinding aan waarin ruimte mag zijn om te ontdekken hoe een ideale wereld er voor eenieder uit mag zien.

Daarmee refereer ik naar het coverbeeld van deze thesis. Kijkende naar de wereld, die deels in onze handen ligt, kun je jezelf de volgende vraag stellen: waar wil jij dat ‘jouw’ wereld naartoe groeit – ook in relatie tot digitalisering? Blijf daar met elkaar het gesprek over aan gaan. Samen in verbinding met alle quadruple helix-actoren zoals ChatGPT beaamt, met “het voordeel voor burgers en de maatschappij als geheel” als daadwerkelijke ‘bedoeling’.

6 Referentielijst

Agger, Annika & Lund, Dorthe. (2017). Collaborative Innovation in the Public Sector – New Perspectives on the Role of Citizens. *Scandinavian Journal of Public Administration*.

AlAwadhi, S. (2019, January). A proposed model of trust factors for e-government adoption and civic engagement. In *Proceedings of the 52nd Hawaii International Conference on System Sciences*.

Alzahrani, L., Al-Karaghoul, W., & Weerakkody, V. (2017). Analysing the critical factors influencing trust in e-government adoption from citizens' perspective: A systematic review and a conceptual framework. *International business review*, 26(1), 164-175.

Anderson, N., Potočnik, K. & Zhou, J. (2014) Innovation and Creativity in Organizations: A State-of-the-Science Review, Prospective Commentary, and Guiding Framework. *Journal of Management*, 40(5), 1297–1333

Andrews, L. (2019). Public administration, public leadership and the construction of public value in the age of the algorithm and 'big data'. *Public Administration*, 97(2), 296-310.

Ansell, C. Gash, A. (2007) Collaborative Governance in Theory and Practice, *Journal of Public Administration*

Ansell, C., & Gash, A. (2008). Collaborative governance in theory and practice. *Journal of public administration research and theory*, 18(4), 543-571. *n Research and Theory*, Volume 18, Issue 4, October 2008, Pages 543–571

Ansell, C., & Gash, A. (2012). Stewards, mediators, and catalysts: Toward a model of collaborative leadership¹. *The Innovation Journal*, 17(1), 2.

Ba, S., & Pavlou, P. A. (2002). Evidence of the effect of trust building technology in electronic markets: Price premiums and buyer behavior. *MIS quarterly*, 243-268.

- Balderson, D. (2016). Safety defined: A means to provide a safe work environment. *Professional Safety*, 61(05), 63-68.
- Bason, Christian. (2010). Leading public sector innovation: Co-creating for a better society.
- Bekkers, V. & Ringeling, A. B. 2003, "Vervlochten onderzoek: balans en perspectief," in Vragen over beleid. Perspectieven op waardering, V. Bekkers & A. B. Ringeling, eds., Uitgeverij Lemma, Utrecht. Hood, C. 1986, The tools of government Chatham House, Chatham.
- Bestavros, A., 2000. Banking industry walks 'tightrope' in personalization of web services. *Bank Systems and Technology* 37 (1), 54– 56.
- Boeijs, H. (2005). Analyseren in kwalitatief onderzoek. Denken en doen. Den Haag: Boom Lemma uitgevers.
- Bharosa, N., & Janssen, M. (2020). Digicampus-Preliminary Lessons from a Quadruple Helix Ecosystem for Public Service Innovation. In *EGOV-CeDEM-ePart-** (pp. 195-204).
- Boeijs, H., Tobi, H., Scheepers, P. (2016). *Onderzoeksmethoden, 9e dr.* Uitgeverij Boom.
- Bok, C., Brunsveld, N., Dijck, J. V., Prins, C., Jacobs, B., Skeikh, H. & Verstappen, J. (2021). Advies publieke waarden voor het onderwijs.
- Bommert, Ben. (2010). Collaborative Innovation in the Public Sector. *International Public Management Review · electronic Journal*.
- Boutellier, H. (2007) Nodale orde Veiligheid en burgerschap in een netwerksamenleving. Vrije Universiteit Amsterdam
- Bozeman, B., & Jørgensen, T.B. 2007. 'Public values. An Inventory'. *Administration and Society*, vol. 39, no. 3, p. 354-381.

Burke, C. S., Sims, D. E., Lazzara, E. H., & Salas, E. (2007). Trust in leadership: A multi-level review and integration. *The leadership quarterly*, 18(6), 606-632.

Brennenraedts, R., Bekkers, R., Kats, J., Hanswijk, M., Bakhyshev, R., Sahebali, W., Jansen, R. (2020). Informatie-uitwisseling landelijk dekkend stelsel cybersecurity. Eindrapport. WODC.

Bryman, A. *Social Research Methods by Alan Bryman (19-Jan-2012) Paperback*. (2021). Oxford; 4 edition (19 Jan. 2012)

Bryson, J. M., Crosby, B. C., & Stone, M. M. (2006). The design and implementation of Cross-Sector collaborations: Propositions from the literature. *Public administration review*, 66(s1), 44-55.

Carayannis, E.G., Barth, T.D. & Campbell, D.F. The Quintuple Helix innovation model: global warming as a challenge and driver for innovation. *J Innov Entrep* 1, 2 (2012).

Carayannis, E. G., & Campbell, D. F. (2018). *Smart quintuple helix innovation systems: How social ecology and environmental protection are driving innovation, sustainable development and economic growth*. Springer.

Carayannis, E.G., Dezi, L., Gregori, G. *et al.* (2022) Smart Environments and Techno-centric and Human-Centric Innovations for Industry and Society 5.0: A Quintuple Helix Innovation System View Towards Smart, Sustainable, and Inclusive Solutions.

Carr, M. (2016) Public-private partnerships in national cyber-security strategies. *International Affairs* 92: 1 (2016) 43-62

Castells, M. (2000) *The rise of the network society*. Oxford: Blackwell Publishers

Ceder, D. en Dekker-Abulaziz, H. (2 juni 2022). Motie 21501-33-932 van de leden Ceder en Dekker-Abdulaziz over de inzet voor het voorstel voor een raamwerk voor een Europese Digitale identiteit. [Kamerstuk] Geraadpleegd via <https://www.tweedekamer.nl/kamerstukken/moties/detail?id=2022Z11047&did=2022D22670>

Cavallini, S., Soldi, R., Friedl, J. & Volpe, M. (2016). Using the Quadruple Helix approach to accelerate the transfer of research and innovation results to regional growth. Brussels: European Union, Committee of the Regions.

Ceder, D. (2 juni 2022) Motie 21501-33-933 c.s. over het bezwaar tegen de introductie van een uniek en blijvend identificatienummer. [Kamerstuk] Geraadpleegd via:
<https://www.tweedekamer.nl/kamerstukken/moties/detail?id=2022D22672&did=2022D22672>

Cheskin (1999). Research and Studio Archetype. Ecommerce trust study. Redwood Shores, CA: Cheskin Research.

Churchman, C. W. (1967). Guest editorial: Wicked problems. *Management science*, B141-B142.

Colesca, S. E. (2009). Understanding trust in e-government. *Engineering Economics*, 63(3).

Corritore, C. L., Kracher, B., & Wiedenbeck, S. (2003). On-line trust: concepts, evolving themes, a model. *International journal of human-computer studies*, 58(6), 737-758.

Couture, S., & Toupin, S. (2019). What does the notion of “sovereignty” mean when referring to the digital?. *New media & society*, 21(10), 2305-2322.

Covey, S. R., & Merrill, R. R. (2006). *The speed of trust: The one thing that changes everything*. Simon and schuster.

Cucinotta D, Vanelli M. (2020) WHO Declares COVID-19 a Pandemic.

Geraadpleegd op 17 mei 2020 van:

<https://www.mattioli1885journals.com/index.php/actabiomedica/article/view/9397>

Culnan, Mary & Armstrong, Pamela. (1998). Information Privacy Concerns, Procedural Fairness and Impersonal Trust: An Empirical Investigation. *Organization Science*. 10. 10.1287/orsc.10.1.104.

Den Boer, R. (2021). Digitale media in het coalitieakkoord van Rutte IV.

Diggit Magazine. 16 december, 2021. Geraadpleegd via:

<https://www.diggitmagazine.com/blog/digitale-media-het-coalitieakkoord-van-rutte-iv>

De Meij, S., Beleid, M., Scriptiebegeleider, P., & Cachet, A. (2010). Subjectieve en objectieve veiligheid: een overbrugbare kloof?. *Erasmus University*.

De Mul, J. (2016). Gemedieerd vertrouwen in de overheid. Een wijsgerig-antropologisch perspectief op veiligheid en vertrouwen. In B. Haring, L. van Zoonen, V. Frissen, M. de Lange, C. Sigaloff, & W. Vrouwe (Eds.), *Essay Estafette, reflecties op de toekomst van de digitale overheid* (pp. 19).

Domingo, I. A. (2020). April 2020. SSI eIDAS Legal Report How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market.

Dunn-Cavelty, M., & Suter, M. (2009). Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection. *International Journal of Critical Infrastructure Protection*, 2(4), 179-187.

Digitale Overheid. (2020). *Regie op Gegevens – Digitale Overheid*.

Geraadpleegd via <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/regie-op-gegevens>.

Digitale Overheid. (2020). *European coalition of the willing - Digitale*

Overheid. Geraadpleegd via: <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/europa/european-coalition-of-the-willing/>

Dutch Blockchain Coalition. Blockchain & SSI. Geraadpleegd op 11 december 2022 van <https://dutchblockchaincoalition.org/nieuws/blockchain-en-ssi>

Ekman, J., & Amnå, E. (2012). Political participation and civic engagement: Towards a new typology. *Human affairs*, 22, 283-300.

Emerson, K., Nabatchi, T., & Balogh, S. (2012). An integrative framework for collaborative governance. *Journal of public administration research and theory*, 22(1), 1-29.

Europese digitale identiteit: eenvoudige onlinetoegang tot belangrijke diensten.

Geraadpleegd op 13 juli 2023 via:

<https://www.europarl.europa.eu/news/nl/headlines/society/20230302STO76818/europese-digitale-identiteit-eenvoudige-onlinetoegang-tot-belangrijke-diensten>

Fan, M., Epadile, M., Qalati, S. A., & Qureshi, N. A. (2022). The Effects of eGovernment Efficiency on Subjective Wellbeing. *Frontiers in Psychology*, 13, 768540.

Finkbeiner, M., Schau, E. M., Lehmann, A., & Traverso, M. (2010) Towards Life Cycle Sustainability Assessment. *Sustainability*. 2. 10.3390/su2103309.

Fountain, J. E. (2019). The wicked nature of digital transformation: A policy perspective. *Dubai Policy Review*, 1, 40-44.

Fresco, L. O. (2011). Feiten in overvloed. *Amsterdam: Vossiuspers UvA (Kohnstammlezing)*.

Frizzo-Barker, J., Chow-White, P. A., Adams, P. R., Mentanko, J., Ha, D., & Green, S. (2020). Blockchain as a disruptive technology for business: A systematic review. *International Journal of Information Management*, 51, 102029.

Gefen, David & Rao, Srinivasan & Tractinsky, N.. (2003). The Conceptualization of Trust, Risk and Their Relationship in Electronic Commerce: The Need for Clarifications. 10 pp.. 10.1109/HICSS.2003.1174442.

Geutjes, R. (2013). De rol van vertrouwen en communicatie binnen publiek-private samenwerking. Radboud Universiteit Nijmegen. Bestuurskunde Thesis.

Geys, B., & Murdoch, Z. (2010). Measuring the ‘bridging’ versus ‘bonding’ nature of social networks: A proposal for integrating existing measures. *Sociology*, 44(3), 523-540.

Graham, J., Plumptre, T. W., & Amos, B. (2003). *Principles for good governance in the 21st century* (Vol. 15, p. 6). Ottawa: Institute on governance.

- Goede, M. (2007) 365 dagen Bestuurskunde 360°. De Bestuurskundeacademie 2007.
- Hak, Tony. (2004) Waarnemingsmethoden in kwalitatief onderzoek. *Huisarts en Wetenschap*. 47. 205-212.
- Halfani, M. P., McCarney, P., & Rodriguez, A. (1994). Towards an understanding of governance: the emergence of an idea. *Urban research in the developing world*. Toronto: University of Toronto.
- Hanekamp, J. C., Deel, I. I., Normenstelsel, H., met Zand, B., & van Haren, W. (1999). Normering en risico in wetenschappelijk perspectief. *Stichting HAN*. Amsterdam.
- Hartholt, S. (2021). Is de Europese digitale identiteit echt het einde van de vrijheid? Geraadpleegd via: <https://www.agconnect.nl/artikel/de-europese-digitale-identiteit-echt-het-einde-van-de-vrijheid>
- Hartley, J., Sørensen, E. & Torfing, J. (2013) Collaborative innovation: A viable alternative to market competition and organizational entrepreneurship. *Public Administration Review*, 73, pp.821–830.
- Hartley, J. (2014) New development: Eight and a half propositions to stimulate frugal innovation. *Public Money & Management*, 34(3), pp.227–232.
- Hoffman, D. L., Novak, T. P., & Peralta, M. (1999). Building consumer trust online. *Communications of the ACM*, 42(4), 80-85.
- Holvast, E. (2021). *Metagovernance en een innovatieve binnenvaartsector, wat is er nodig?* *Public Administration*. 26 augustus 2021. Geraadpleegd via: <http://hdl.handle.net/2105/58397>
- Hood, C. (1991) A Public Management For All Seasons? *Public Administration*, 69: 3-19
- Horsburgh, S., Goldfinch, S., & Gauld, R. (2011). Is public trust in government associated with trust in e-government?. *Social Science Computer Review*, 29(2), 232-241.

Huberts, L. (2005) *Integriteit en integritisme in bestuur en samenleving. Wie de schoen past...* Amsterdam; Onderzoeksgroep Integriteit van Bestuur Vrije Universiteit Amsterdam.

Huberts, L. W. J. C., Hoekstra, A., & Gaisbauer, I. (2015). Integrity and integrity management in the Netherlands. Describing the scene, definitions, strategies and developments. In L. Huberts, & A. Hoekstra (Eds.), *Integrity management in the public sector: The Dutch approach* (pp. 9-29). The Hague: BIOS.

Huxham, C., & Vangen, S. (2004). Doing things collaboratively: realizing the advantage or succumbing to inertia?. *IEEE Engineering Management Review*, 32(4), 11-20.

iBestuur (24 september, 2021). Nederland en Duitsland werken samen aan een stelsel voor digitale identiteit. Geraadpleegd via:

<https://ibestuur.nl/artikel/nederland-en-duitsland-werken-samen-aan-stelsel-voor-digitale-identiteit/>

iBestuur (24 augustus, 2022). Staatssecretaris vraagt input over ontwikkeling digitale identiteit. Geraadpleegd via:

<https://ibestuur.nl/artikel/staatssecretaris-vraagt-input-over-ontwikkeling-digitale-identiteit/>

Ishmaev, G. (2021). Sovereignty, privacy, and ethics in blockchain-based identity management systems. *Ethics and Information Technology*, 23(3), 239-252.

Jacobs, B. (2021) Digitale identiteit als Nederlandse troefkaart in Europa. iBestuur. 15 juni 2021. Geraadpleegd via:

<https://ibestuur.nl/podium/digitale-identiteit-als-nederlandse-troefkaart-in-europa>

Jellema, T. D. (2021). *De invloed van het betrekken van de doelgroep bij publieke waarde (n) creatie op de legitimiteit en steun van maatschappelijke activiteiten van BVO's* (Master's thesis).

Johnson-George, C., & Swap, W. C. (1982). Measurement of specific interpersonal trust: Construction and validation of a scale to assess trust in a specific other. *Journal of personality and social psychology*, 43(6), 1306.

Kamerstukken II, 2020/21, 26643, nr. 743: p. 7, informatie- en communicatietechnologie (ICT), 2021. Geraadpleegd via <https://zoek.officielebekendmakingen.nl/kst-26643-743.pdf>

Kaptein, M., & Van Reenen, P. (2001). Integrity management of police organizations. *Policing: An International Journal of Police Strategies & Management*, 24(3), 281-300.

Kaptein, M., Huberts, L., Avelino, S., & Lasthuizen, K. (2005). Demonstrating ethical leadership by measuring ethics: A survey of US public servants. *Public Integrity*, 7(4), 299-311.

Kini, A., & Choobineh, J. (1998, January). Trust in electronic commerce: definition and theoretical considerations. In *Proceedings of the thirty-first Hawaii International conference on System sciences* (Vol. 4, pp. 51-61). IEEE.

Klijn, E. & Koppenjan, J. (2016) *Governance Networks in the Public Sector*. Leiden, Nederland: Taylor & Francis Ltd.

Klievink, B. (2021). *Hollen én stilstaan: hoe data en digitalisering de overheid veranderen*. Universiteit Leiden.

Knaapen, B., Lezer, E., & Homburg, V. (2019) *Innoveren door experimenteren?*

Knops, R., 11 februari 2021 – Visiebrief digitale identiteit. [Kamerstuk]

Kamerstukken II, 2020/21, 26643, nr. 743: p. 7, informatie- en communicatietechnologie (ICT), 2021. Geraadpleegd op diverse data via <https://zoek.officielebekendmakingen.nl/kst-26643-743.pdf> en via <https://open.overheid.nl/documenten/ronl-767b3b63-dc1b-4e0b-b16b-530c6a1702ef/pdf>

Knops, 12 oktober 2021 - Kamerbrief over voortgang domein Toegang, 12 oktober 2021. [Kamerbrief] Geraadpleegd via <https://open.overheid.nl/documenten/ronl-767b3b63-dc1b-4e0b-b16b-530c6a1702ef/pdf>

Komorowski, M., Claeys, L., & Van Dam, T. (2021). Digitale decentrale waardeoverdracht voor de publieke sector in Nederland. Een speelveldanalyse: hoe kunnen Distributed Ledger-technologieën zoals blockchain de publieke waarden beïnvloeden?.

Koppenjan, J., Klijn, E. (2004) Managing uncertainties in networks: A network approach to problem solving and decision making. London: Routledge

Klijn, E. H., & Van Twist, M. J. W. (2007). Publiek-private samenwerking in Nederland, Overzicht van theorie en praktijk.

Laan, A., & Sijpersma, R. (2006). *Bouwen op Vertrouwen*. (Publicatie / Economisch Instituut voor Bouwnijverheid, ISSN 0922-4483). Economisch Instituut voor Bouwnijverheid.

Lee, M. K., & Turban, E. (2001). A trust model for consumer internet shopping. *International Journal of electronic commerce*, 6(1), 75-91.

Leppens, P. (2010) Ethische modellen voor euthanasiebeslissingen.

Maes, R., 'Geen digitale transformatie zonder mentale transformatie. De nieuwe werkelijkheid van de informatiefprofessional', W. Brongeeest, M. Wesseling & E. de Vries (eds.), *De informatiefprofessional 3.0. Strategische vaardigheden die u connected houden*, Amsterdam: 2017, p. 15-26.

Map, B., & P 't Hart, M. J. W. (2011). *Openbaar Bestuur– Beleid, organisatie en politiek*.

Margulis, S. T. (1977). Conceptions of privacy: Current status and next steps. *Journal of Social Issues*, 33(3), 5-21.

Mayer, R., Davis, J., Schoorman, F. (1995). An integrative model of organizational trust. *The Academy of Management Review*, 20(3), 709–734

Mcknight, D. & Chervany, Norman. (2002). What Trust Means in E-Commerce Customer Relationships: An Interdisciplinary Conceptual Typology. *International Journal of Electronic Commerce*. 6. 35-59.

- Moore, M. (1995). *Creating Public Value: Strategic Management in Government*. Cambridge: Harvard University Press.
- Moorman, C., & Zaltman, G. (1988). The Role of Personal Trust in the Use of Research. *Journal of Advertising Research*, 28, 16-24.
- Mühlhoff, R. (2020) We Need to Think Data Protection Beyond Privacy Turbo-Digitization after Covid-19 will advance algorithmic social selection and the biopolitical shift of digital capitalism. Technische Universität Berlin
- Mulder, E. J. (2019). Digitale transformatie van de overheid vergt visie en beleid. *Bestuurswetenschappen*, 73(4), 57-66.
- Mukherjee, Avinandan & Nath, Prithwiraj. (2003). A Model of Trust in Online Relationship Banking. *International Journal of Bank Marketing*. 21. 5-15. 10.1108/02652320310457767.
- Naves, Jeroen & Audia, Benedetta & Busstra, Marjolein & Hartog, Koen & Yamamoto, Yoshiyuki & Rikken, Olivier & Heukelom-Verhage, Sandra. (2019). Legal Aspects of Blockchain. *Innovations: Technology, Governance, Globalization*. 12. 88-93.
- Nordheim, C. B., Følstad, A., & Bjørkli, C. (2019). An Initial Model of Trust in Chatbots for Customer Service – Findings from a Questionnaire Study. *Interacting with Computers*.
- Oomsels, P. (2016) Interorganisationeel vertrouwen in Vlaamse horizontale departementen: naar een managementmodel. *Vlaams Tijdschrift voor Overheidsmanagement*. 2016.
- Olson. J.S. & Olson, G.M. "i2i Trust in E-commerce," *Communications of the ACM*, 43(12), 2000: 41-44.
- Olsen, Odd Einar & Kruke, Bjørn & Hovden, Jan. (2007). Societal Safety: Concept, Borders and Dilemmas. *Journal of Contingencies and Crisis Management*. 15.

Osborne, S. P. (1997). Managing the coordination of social services in the mixed economy of welfare: competition, cooperation or common cause?. *British journal of management*, 8(4), 317-328.

Osborne, S. & Brown, K. (2005). *Managing Change and Innovation in Public Service Organizations*.

Osborne, S. (2010). *The new public governance: Emerging perspectives on the theory and practice of public governance*. Routledge.

Paliszkiewicz, J. O. (2010). The relationship between social perspective and knowledge management. *International Journal of Innovation and Learning*, 7(4), 450-466.

Paliszkiewicz, J., Gołuchowski, J. & Koohang, A. (2015) Leadership, trust, and knowledge management in relation to organizational performance: Developing an instrument. *Online Journal of Applied Knowledge Management*. 3. 19-35

Parent, M., Vandebek, C. A., & Gemino, A. C. (2005). Building citizen trust through e-government. *Government Information Quarterly*, 22(4), 720-736.

Pavlou, P.A. (2003) Consumer Acceptance of Electronic Commerce: Integrating Trust and Risk with the Technology Acceptance Model. *International Journal of Electronic Commerce*, 7, 101-134.

Ploch, T., & Van Zwieten, M. C. B. (2007) Kwalitatief onderzoek. *Handboek gezondheidszorgonderzoek*, 77-93.

Pohle, J., & Thiel, T. (2020) Digital sovereignty. *Pohle, J. & Thiel*.

Pollitt, C., Van Thiel, S., & Homburg, V. (Eds.). (2007). *New public management in Europe*. Basingstoke: Palgrave Macmillan.

Popelier, P., Van Gestel, R., Van Aeken, K., Verlinden, V., & Van Humbeeck, P. 2008, Consultaties in de wetgevingspraktijk. Een zoektocht naar internationale best practices. Politeia, Brussel.

Prahalad, C. K., & Ramaswamy, V. (2002). The co-creation connection. *Strategy and business*, 50-61.

Raju, R. S., Singh, S., & Khatter, K. (2017) Aadhaar card: challenges and impact on digital transformation. *arXiv preprint arXiv:1708.05117*.

Reijmerink, W. (2003). Use it or lose it. Kansen en strategieën voor kennis-effectief werken bij het Ministerie van VWS. Den Haag: Ministerie van VWS.

Rijksoverheid. Ministerie van Algemene Zaken. (2022). Coalitieakkoord “Omzien naar elkaar, vooruitkijken naar de toekomst. 15 december 2021. Geraadpleegd via <https://www.rijksoverheid.nl/regering/coalitieakkoord-omzien-naar-elkaar-vooruitkijken-naar-de-toekomst> en <https://open.overheid.nl/documenten/ronl-f3cb0d9c-878b-4608-9f6a-8a2f6e24a410/pdf>

Roberts, Nancy. (2000). “Wicked Problems and Network Approaches to Resolution.” *The International Public Management Review*. 2000, 1(1). Coping With Wicked Problems.

Rutgers, M.R. (2011) Het Pantheon van de Publieke Waarden. Rede uitgesproken bij de aanvaarding van het ambt van hoogleraar Filosofie van het Openbaar Bestuur aan de Universiteit van Amsterdam op vrijdag 11 februari 2011.

Satybaldy, A., Nowostawski, M., & Ellingsen, J. (2020). Self-sovereign identity systems: Evaluation framework. *Privacy and Identity Management. Data for Better Living: AI and Privacy: 14th IFIP WG 9.2, 9.6/11.7, 11.6/SIG 9.2. 2 International Summer School, Windisch, Switzerland, August 19–23, 2019, Revised Selected Papers 14*, 447-461.

Schuilenburg, M. (2009) De securisering van de samenleving. Over de relatie tussen veiligheidszorg, bestuur en quasistrafrecht. *Krisis*, 3, 6-22.

Schumpeter, J. (1942). *Capitalism, socialism and democracy*. New York, NY: Harper & Row.

Schütz, F., Heidingsfelder, M.L, Schrauder, M. (2019). *Co-shaping the Future in Quadruple Helix Innovation Systems: Uncovering Public Preferences toward Participatory Research and Innovation*, *She Ji: The Journal of Design, Economics, and Innovation*, Volume 5, Editie 2, 2019, pp. 128-146.

Schwab, K. (2017). *The Fourth Industrial Revolution*. World Economic Forum.
Geraadpleegd via: <https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab>

Scribber (2003). Scribbr. (n.d.). *Soorten Research Bias | Betekenis & Voorbeelden*. <https://www.scribbr.nl/category/onderzoeksbias/>

Sedlmeir, J., Smethurst, R., Rieger, A., & Fridgen, G. (2021). Digital identities and verifiable credentials. *Business & Information Systems Engineering*, 63(5), 603–613.
<https://doi.org/10.1007/s12599-021-00722-y>

Singleton, R., & Straits, B. (2005). *Approaches to social research* (4th ed.). New York, NY: Oxford University Press.

Smaling, A. (2021). Sensitizing concepts, wat kun je ermee?. *KWALON*, 26(1), 65-67.

Snijkers, K. *E-Government: ICT from a public management perspective*, Moscow State University, Moscow, Russia, 2005.

Sørensen, Eva & Torfing, Jacob. (2016). *Metagoverning Collaborative Innovation in Governance Networks*. *The American Review of Public Administration*. 47. 10.1177/0275074016643181.

Stoker, G. (2006). Public value management: A new narrative for networked governance?. *The American review of public administration*, 36(1), 41-57.

SSI Speelveldanalyse (1 oktober, 2021, versie 1.0). Innopay; TNO in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Geraadpleegd op verschillende data via <https://open.overheid.nl/documenten/ronl-9fa0e23a-0b04-442a-917b-36bce29403a8/pdf>

Steenkamp, R. J. (2019). The quadruple helix model of innovation for Industry 4.0. *Acta Commercii*, 19(1), 1-10.

Talbot, C. (2006). Applying public value to public administration reform in Macedonia. *Centre for Public Policy & Management, Manchester Business School. occasional paper.*

Torenvlied, R., & Ossewaarde, M. R. R. (2020). Toekomst van de Bestuurskunde in een ongekende hightech samenleving. *Bestuurskundige berichten*, 35(2), 2-4.

Trommel, S. (2021) iBestuur (23 december, 2021). Regeringsadviseur Estland: begin met een digitale identiteit. Geraadpleegd via: <https://ibestuur.nl/artikel/regeringsadviseur-estland-begin-met-een-digitale-identiteit/>

Van Bueren, E. M., Klijn, E. H., & Koppenjan, J. F. (2003). Dealing with wicked problems in networks: Analyzing an environmental debate from a network perspective. *Journal of public administration research and theory*, 13(2), 193-212.

Van Dale. Geraadpleegd in 2022 via: <https://www.vandale.nl/gratis-woordenboek/nederlands/betekenis/soeverein>

Van Damme, J., & Pattyn, V. (2015). Overheid in transitie (s)? Beleidsrollen en-instrumenten in een transitiecontext. *Vlaams Tijdschrift voor Overheidsmanagement*, 8(1), 5-9.

Van Delden, P. (2009). *Samenwerking in de publieke dienstverlening*. Eburon Uitgeverij BV.

Van den Brink (2017). Kennis, key in de digitale wereld.

Kwalitatief onderzoek naar de rol van leiderschap, vertrouwen en machtsverhoudingen in samenwerking. Masterscriptie. Universiteit Utrecht.

Vangen, S., & Huxham, C. (2003). Nurturing collaborative relations: Building trust in interorganizational collaboration. *The Journal of applied behavioral science*, 39(1), 5-31.

Van Houten, R. (2021, 21 oktober). *iBestuur magazine*. Editie 40, p. 11. NCSC-directeur Hans de Vries: 'Soms neem ik de ruimte om te doen wat niet mag'. Tevens online geraadpleegd op 19 juni 2023 via: <https://ibestuur.nl/artikel/ncsc-directeur-hans-de-vries-soms-neem-ik-de-ruimte-om-te-doen-wat-niet-mag/>

Van Nieuwenhoven, E. H. J. (2019). *Ongelofelijk politiek, maar onbegrijpelijk genoeg genegeerd. Een discoursanalyse op het snijvlak van de Nederlandse omgang met politiek, datatechnologie en toekomstliteratuur* (Master's thesis).

Van Roermund, J., Riva, C., Tinari, S. (2021). Wetenschappers waarschuwen voor een nieuwe digitale identiteit. Follow The Money. 12 december 2021.

Van Thiel, S. (2015). *Bestuurskundig onderzoek*. Uitgeverij Coutinho.

Vos, P. M., & de Vries, F. (2016). Waardecreatie in triple helix: Recepten voor triple helix samenwerking.

Warr, P. (2007). *Work, happiness, and unhappiness*. London: Lawrence Erlbaum Associates.

Weiss, T. G. (2000). Governance, good governance and global governance: conceptual and actual challenges. *Third world quarterly*, 21(5), 795-814.

Wester, F. P. J. F. (2004). Analyse van kwalitatief onderzoeksmateriaal. *Huisarts en wetenschap*, 47, 122-128.

Xu, R., Sun, Q., & Si, W. (2015). The third wave of public administration: The new public governance. *Canadian Social Science*, 11(7), 11-21.

Xu, X., Lu, Y., Vogel-Heuser, B., Wang, L. (2021). Industry 4.0 and Industry 5.0—Inception, conception and perception. *Journal of Manufacturing Systems*. Volume 61, 2021. P. 530-535.

Yikilmaz, İ. (2020). New era: The transformation from the information society to super smart society (society 5.0). *Data, Information and Knowledge Management; Mert, G., Şen, E., Yılmaz, O., Eds*, 85-112.

Yin, R., (2013, 5e druk). Case study research: design and methods. Thousand Oaks: Sage Publications.

Yousafzai, S. Y., Pallister, J. G., & Foxall, G. R. (2003). A proposed model of e-trust for *electronic banking*. *Technovation*, 23(11), 847-860.

Ysa, T., Sierra, V. & Esteve, M. (2014). Determinants of network outcomes: The impact of management strategies. *Public Administration*. Vol. 92, No 3, 2014 (636-655).

Zarifis, A., & Cheng, X. (2022). A model of trust in Fintech and trust in Insurtech: How Artificial Intelligence and the context influence it. *Journal of Behavioral and Experimental Finance*, 100739.

Zwieten, Myra & Willems, Dick. (2004). Waardering Van Kwalitatief Onderzoek. *Huisarts en Wetenschap*. 47. 38-43. 10.1007/BF03083653.

7 Bijlagen

Bijlage 1: Vragenlijst

Deze vragenlijst is uitgezet via Google Forms

Onderzoeksvraag: Wat kan de overheid bieden om samen* verder te bouwen aan vertrouwen van burgers rondom de komst en mogelijke ingebruikname van Self-Sovereign Identity (SSI)?
SSI vertaalt zich ook als digitale identiteit.

Dit onderzoek is een bestuurskundig onderzoek vanuit eigen initiatief, maar gekoppeld aan een masterthesis Management van de Publieke Sector aan de Universiteit Leiden. Er worden zo veel mogelijk open vragen ingezet om een goed beeld te kunnen krijgen van wat er speelt onder burgers in Nederland ten opzichte van deze (mogelijk) nieuwe technologie.**

Het doel: een advies kunnen geven om de rol van de overheid en de samenwerking tussen overheid, wetenschap, bedrijfsleven en burgers te verstevigen bij het invoeren van nieuwe ontwikkelingen, waarbij burgers zich gehoord en gesupport voelen en voldoende vertrouwen kunnen hebben in (mogelijke) invoering van nieuwe technologieën als SSI.

* Met gezamenlijk wordt gekeken naar het quadruple helix perspectief: de rol en samenwerking tussen overheid, wetenschap, bedrijfsleven en burgers.

** Het onderzoek bestaat uit 20 vragen; grotendeels open vragen.
Het onderzoek wordt geanonimiseerd uitgevoerd en opengesteld van 8 juni tot en met 17 juni 2023.

Ik verloot onder alle deelnemers 1 managementboek naar eigen keuze (met een maximale waarde van 40 euro incl. BTW). Daarvoor heb ik wel je mailadres nodig als je meewerkt, om je te kunnen bereiken indien je wint.

Self Sovereign Identity - Digitale Identiteit

(Informatie)kennis & houding



1 - Ben je bekend met het begrip Self Sovereign Identity (SSI) oftewel Digitale Identiteit?



Multiple choice

- Ja ×
- Nee ×
- Other... ×
- Add option



2) Is er volgens jou voldoende informatie (kennis) beschikbaar om een houding ten opzichte van SSI te kunnen aannemen?

- Ja
- Nee
- Other...

3) Heb jij een bepaalde informatiebehoefte t.o.v. het onderwerp SSI om je beter geïnformeerd te voelen?

Long answer text

4) Hoe sta je tegenover SSI op basis van de informatie die hierover bij jou bekend is?

Licht dit toe.

Long answer text

Vertrouwen & polity

5) Wat kan **de overheid** volgens jou bieden om verder te bouwen aan vertrouwen van burgers rondom de mogelijke komst en ingebruikname van SSI?

Long answer text

6) Vind je dat er naast de overheid andere partijen (wetenschap, burgers, bedrijfsleven) aan te wijzen zijn die kunnen helpen om vertrouwen in nieuwe technologie als SSI te verstevigen?

Geef per tak aan hoe zij kunnen helpen.

Zonder al te veel te willen beïnvloeden, een aantal suggesties:

- * Meer informatie verstrekken en je op bepaalde wijze meenemen in processen.
- * Beter inzicht verstrekken in wat de consequenties zijn.
- * Bijv. betrokkenheid vergroten, informatieproces optimaliseren, besluitvormingsproces.
- * Etcetera...

Probeer zo concreet mogelijk te verwoorden wat jou zou helpen.

6 a) Wat kan **de wetenschap** doen om jou te helpen om vertrouwen in nieuwe technologie als SSI te verstevigen?

Long answer text

6 b) Wat kan **het bedrijfsleven** doen om jou te helpen om vertrouwen in nieuwe technologie als SSI te verstevigen?

Long answer text

6 c) Wat kunnen **burgers en/of jijzelf** doen om jou te helpen om vertrouwen in nieuwe technologie als SSI te verstevigen?

Long answer text

7) Hoe denk jij dat de diverse partijen beter kunnen samenwerken om technologische innovatie als SSI beter te kunnen ondersteunen?

Long answer text

8) Hoe sta je qua vertrouwen tegenover digitale uitwisseling van (digitale) gegevens die voor jou belangrijk zijn?

- Ik heb er vertrouwen in
- Ik weet het niet zo goed
- Alle veranderingen kennen onzekerheid
- Ik heb er geen vertrouwen in
- Other...

9) Digitale identiteit betekent ook dat je meer controle over je eigen databeheer krijgt.

Hoe zie jij jouw eigen rol als burger wanneer je beseft dat het beheer van jouw gegevens bij jou komt te liggen?

Long answer text

10) Heb jij in relatie tot SSI ergens zorgen over?

Denk bijv. aan zaken in relatie tot:

- * privacy;
- * controle van gegevens;
- * (zelf)controle op digitale gegevensuitwisseling en interoperabiliteit tussen diverse systemen die met elkaar moeten communiceren;
- * systeemvertrouwen; vertrouwen in de overheid om het juiste te doen voor burgers ('benevolence' & integriteit);
- * vertrouwen in de digitale infrastructuur en het kunnen van de overheid ('ability');
- * vertrouwen in eigen online handelen.

Long answer text

11) Wat kan de overheid doen om ervoor te zorgen dat jij je veilig en gesterkt voelt in het beheren van jouw eigen gegevens en de mogelijke komst van SSI?

Long answer text

12) Hoe verwacht je dat de verschillende betrokken partijen met jouw (digitale) data omgaan?

Long answer text

13) Wat vind je dat de overheid kan doen om erop toe te zien dat de uitrol en (mogelijke) ingebruikname van SSI goed verloopt?

Welke rol kan de overheid hierin aannemen?

Voorbeelden:

- * Wijze van communiceren veranderen; hoe zou je geïnformeerd willen worden?
- * Het (mogelijk) bestaan van bepaalde zorgen wegnemen; als deze bestaan, hoe kunnen deze weggenomen of verminderd worden?
- * Het opstellen van heldere kaders en regelgeving rondom SSI.

Long answer text

14) Waar zie je kansen en mogelijkheden rondom SSI?
Beschrijf deze.

Long answer text

15) Zie jij risico's en bedreigingen rondom SSI?
Zo ja, welke?

Long answer text

16) Welke waarden spelen voor jou een rol bij het verstevigen van een vertrouwenspositie bij het invoeren van een innovatie als SSI?

- Veiligheid
- Soevereiniteit & autonomie (uitleg: zelfbeschikking over eigen gegevens)
- Vrijheid
- Integriteit (uitleg: eerlijkheid en oprechtheid staan hoog in het vaandel)
- Innovatie
- Inclusiviteit (uitleg: iedereen moet in staat zijn makkelijk mee te kunnen doen; digitalisering heeft conseq...
- Transparantie (uitleg: open en eerlijke communicatie zodat juiste keuzes gemaakt kunnen worden))
- Privacy & betrouwbare en veilige omgang met mijn gegevens vanuit alle betrokken partijen
- Ik wil zelf kunnen beslissen om hier aan mee te doen en ook voor een opt-out kunnen kiezen zonder dat d...
- Other...

17) Welke waarde is voor jou het meest belangrijk? En waarom?

Long answer text

18) Signaleer jij risico's rondom SSI in relatie tot jouw waarden? En zo ja, welke?

Long answer text

19) Hoe zouden optionele risico's naar jouw mening geminimaliseerd kunnen worden om jouw waarden te beschermen?

Long answer text

20) Heb je nog vragen, opmerkingen of aanvullingen? Noteer ze dan hier.

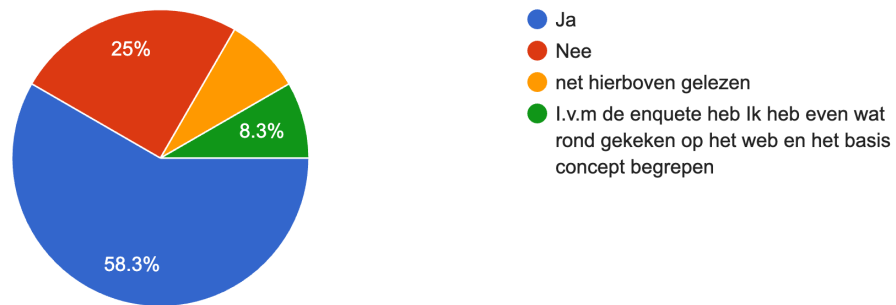
Long answer text

Bedankt voor het meewerken aan dit onderzoek!

Bijlage 2: Onderzoeksresultaten uit Google Forms (Juni 2023)

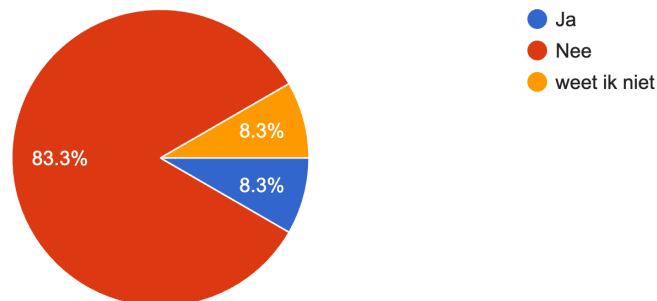
1 - Ben je bekend met het begrip Self Sovereign Identity (SSI) oftewel Digitale Identiteit?

12 responses



2) Is er volgens jou voldoende informatie (kennis) beschikbaar om een houding ten opzichte van SSI te kunnen aannemen?

12 responses



3) Heb jij een bepaalde informatiebehoefte t.o.v. het onderwerp SSI om je beter geïnformeerd te voelen?

12 responses

Ik weet dat SSI bestaat en ik vind het lastig een beeld te vormen hoe het mij in mijn dagelijkse leven kan ondersteunen. Waarom, waar en hoe kan ik het gebruiken? Wat zijn de voor- en nadelen tov 'normale' identificatie? Kan ik het ook in het normale leven gebruiken (op Schiphol of in het buitenland)? openbaring van besluiten in EU, hoe komt ssi tot stand, wie beslist hierover en hoe kan ik het besluit beïnvloeden?

Ik wil het gewoon niet, nooit

Nee, het is een globaal principe en erg afhankelijk van specifieke implementatie.

Niet perse

Dat het meer bekendheid heeft

nee

ik hoor en zie er weinig tot niets over dus meer aandacht er voor lijkt me aan te raden.

Wat is de stand van zaken en waarom neemt het zoveel tijd in beslag?

Het zou fijn zijn als de instanties die hiermee werken informatie op hun site erover zetten. Al is het maar een korte intro met een verwijzing naar een plek waar er meer informatie over te vinden is.

Niet meer

informatie op het web is voornamelijk in het Engels, de omschrijving in de Nederlandse Wikipedia is zeer summier

4) Hoe sta je tegenover SSI op basis van de informatie die hierover bij jou bekend is?

Licht dit toe.

12 responses

Afwachtend. Een paspoort, rijbewijs o.i.d. op mijn telefoon lijkt me handig voor als ik de documenten vergeet mee te nemen zodat ik me altijd kan identificeren. Online zie ik er nog weinig in.

Negatief. geen duidelijkheid over mogelijke consequenties voor mijn vrijheid. Stel dat ik tegen vaccinatie ben, kan de overheid mijn SSI dan op rood zetten. Of als ik een bepaalde mening heb. Nu zal dat niet zomaar vaart lopen, maar met corona hebben we ook vergaande vrijheid beperkende maatregelen opgelegd gekregen. maatregelen die we nooit gedacht hadden.

Zeer negatief. Eenzijdige controle door overheid. Onwenselijke contracten met WHO (one health doel is pure waanzin, genocide).

Erg positief over het concept omdat het het hef in eigen handen geeft bij mensen en ook het potentieel heeft om vertrouwen terug te geven aan mensen.

Het gebruik mag wat mij betreft erg kritisch worden bekeken en streng aan banden worden gelegd. In bepaalde mate kan het handig zijn maar ik vind het ook beperkend. Ik heb er een naar onderbuik gevoel bij

Positief en noodzakelijk, er mag veel meer aandacht voor zijn.

negatief, geeft de houder ervan te veel macht

ik kan dit moeilijk zeggen, maar ik denk dat die identiteit online in de plaats van een fysiek id-bewijs zal gelden (paspoort, rijbewijs etc). Dat lijkt me aangezien vrijwel alles digitaal gaat wel een goede aanvulling. Wel lijkt me de beveiliging etc. een uitdaging.

In deze tijd moet de overheid regelen dat je persoonsinformatie beschermd wordt en dat je controle houdt over het gebruik van de informatie. Ik sta er erg positief tegenover. Als een paar jaar vandaar antwoord vraag 3

Positief. Het lijkt me dat als ik dit als persoon goed regel ik online beter beschermd ben

Negatief, vertrouwen dat gegevens gekoppeld worden zonder dat ik het weet. Wat als ik niet eens ben met iets, dat op sociale media plaats en vervolgens bepaalde vrijheden moet inleveren.

Lijkt mij een soort DigiD 2.0, hopelijk minder omslachtig

5) Wat kan de overheid volgens jou bieden om verder te bouwen aan vertrouwen van burgers rondom de mogelijke komst en ingebruikname van SSI?

12 responses

Meer bekendheid aan geven door online campagnes.

de overwegingen aan het volk voorleggen en betrekken in de keuzes, misschien wel referenda. niet alleen in zee gaan met partijen zoals Amazon

Uit EU stappen. Uit Wef, uit Who. Bilderberg. Nutsvoorzieningen terug naar Nederlandse bedrijven.

Wetenschap weer onafhankelijk van subsidiegevers.

Heel veel zelfbeschikking over informatie. Transparantie. Kunnen zien wie wat inziet. De burger vertrouwen omdat wantrouwen richting de burger ook automatisch wantrouwen richting overheid kweekt.

Dit erg kritisch en met mate in te zetten.

Er openheid over geven en meer informatie die makkelijk toegankelijk is.

niet veel, het is wat het is

meer informatieverschaffing, een informatiecampaagne zowel online, als op tv, radio en kranten.

Er is een inhaalslag nodig om het gebrek aan veiligheid van persoonsgegevens te verminderen. Dat is een rol van de overheid omdat het om bescherming gaat van de persoonlijke levenssfeer. Dit gebeurt ook wel in europa. Er woedt een informatieoorlog en de overheid kan vertrouwen winnen voor burgers door zich als sterke beschermer op te stellen, Daarvoor is wel meer bewustzijn nodig. De huidige kennis en het tempo bij de overheid stellen niet gerust.

Informatievoorziening: wat is het, wat kun je ermee, voorbeelden en voordelen.

Open source maken. Het dient één doel. Niet meer.

Hangt er vanaf in hoeverre ik zelf mijn identiteit beheren kan.

6) Vind je dat er naast de overheid andere partijen (wetenschap, burgers, bedrijfsleven) aan te wijzen zijn die kunnen helpen om vertrouwen in nieuwe technologie als SSI te verstevigen? Geef per tak aan hoe zij kunnen helpen.

6 a) Wat kan de wetenschap doen om jou te helpen om vertrouwen in nieuwe technologie als SSI te verstevigen?

12 responses

Uitleggen hoe het werkt en wat er voor zorgt dat SSI veilig is en hoe je er zelf voor kunt zorgen dat je veilig met SSI omgaat.

Alles opensource maken

Huidige wetenschap is niet meer onafhankelijk en waardevrij. Atoomenergie is gewoon veilig en schoon. Waarom Afrikanen afbeulen voor lithium batterijen? Ze lopen achter klimaatgekte aan etc. Onze aarde is groot genoeg en wij willen GEEN volledige controle. De ijstijd kennen we, we weten toch dat de aarde wisselt van klimaten. Pas je aan.

Onderbouwing van bijv. veiligheid

Informereren maar vooral ook vertellen dat er niets gaat boven menselijk contact

Feiten geven m.b.t. het onderwerp

geldstromen van onderzoek inzichtelijk maken

onderzoeken publiceren, populair wetenschappelijke onderzoeken misschien ook (Quest enzo) leerstoelen hier over aanwijzen bij universiteiten.

Is er geen vertrouwen in de nieuwe technologie? Mensen als Bart Jacobs en Jose van Dijk zetten zich best in.

De wetenschap kan voorbeelden en voordelen schetsen van SSI.

Niets

Goede encryptie en communicatie protocollen ontwikkelen

6 b) Wat kan het bedrijfsleven doen om jou te helpen om vertrouwen in nieuwe technologie als SSI te verstevigen?

12 responses

Ik denk dat het bedrijfsleven achter staat bij mij als het gaat om vertrouwen te verstevigen. Wel zou ik positief getriggerd zijn als ik zou weten hoe SSI hen helpt. Als ik beter weet wat hun voordelen zijn, kan ik zelf een inschatting maken of ik open sta voor het gebruik van SSI.

Bewijzen dat zij allen met mijn toestemming mijn gegevens mogen inzien, bewaren etc. Dus ook dit opensource

Stoppen met die EU en WEF en hoax klimaatdoelen.

Het bedrijfsleven is erg ruim. Gaat het om Google, TUI vakantie reizen, de slager om de hoek?

Zorgen voor gemak maar ook community

Informatie geven m.b.t het eigen bedrijf

niks

hun belangen gaan inzien, investeren in oplossingen en tools die hiermee te maken hebben.

banken genieten op gebied van veiligheid vertrouwen en roeren zich ook wel

Het bedrijfsleven kan ook voorbeelden en voordelen schetsen van SSI, maar ik denk dat ik het bedrijfsleven wel minder vertrouw.

Afstand nemen hiervan

Harde garanties geven dat mijn identiteit niet gehackt kan worden

6 c) Wat kunnen burgers en/of jijzelf doen om jou te helpen om vertrouwen in nieuwe technologie als SSI te verstevigen?

12 responses

Ik denk dat je altijd een paar voorlopers hebt. Mensen die nieuwsgierig zijn en de voordelen zien. Als die er over praten (gebruiksgemak, voordelen, risico's, wat het hun oplevert)-in hun netwerk, dan steekt dat anderen weer aan om het uit te proberen. Meer mond op mond, eigenlijk.

geen idee

Geen junktroep aanbieden, dan stopt consumentisme onmiddellijk. Duurzamere artikelen aanbieden.

Wegwerp bannen. Schonere fabrieken als tataasteel.

Niet veel, het gaat puur om de implementatie. Verder helpen je medeburger het te begrijpen en vertrouwen wellicht? Maar dat kan ik alleen doen als het ook echt te vertrouwen is zonder dat er rare achterdeurtjes in zitten die afbreuk doen aan het principe en de manier waarop het wordt ingevoerd.

Vooraf met beiden benen op de grond blijven staan en goed te voelen wat klopt. SSI handig fit verkiezen boven mensen nee

De informatie opzoeken en goed doornemen

niks

meer er over lezen, in het onderwijs inbedden, goed onderscheid maken tussen fake-news/complotdenken en echte waarheidsgetrouwe informatie.

veel praten, verduidelijken. Vertrouwen uitstralen?

De eerste stappen zetten, ervaringsverhalen delen. Leren hoe anderen het gebruiken

Blijven verzetten zolang het niet democratisch, in alle openheid en transparantie gebouwd wordt.

Geen idee

7) Hoe denk jij dat de diverse partijen beter kunnen samenwerken om technologische innovatie als SSI beter te kunnen ondersteunen?

11 responses

Voor de grotere massa (niet de voorlopers) denk ik dat informatie (wat brengt het jou, wat brengt het de bedrijven, wat brengt het de overheid) helpt. Breed inzetten en vooral niet proberen af te dwingen.

opensource

Wij willen geen ssi. Dat is alweer het 'tegenovergestelde woord dan wat de praktijk zal zijn'. Net als WHO doel 'one health' dat wordt ons immuunsysteem om zeep geholpen. Hoe verzin je het 300 mrna prikken..., Pure genocide.

Open-source! Zie bijv. hoe het bedrijf Egeniq in de openbaarheid werkte aan de Covid QR-apps, het principe hieromheen was erg positief. Zeer aan te raden om hierover bij te lezen!

Dit gebeurt toch wel want er is veel geld mee geboeid.

Een samenwerking die ook gedeeld gaat worden met iedereen en niet alleen in hoger segment niet doen ik vind het een geheel schadelijk idee

een platform online inrichten, conferenties houden, raamovereenkomsten sluiten.

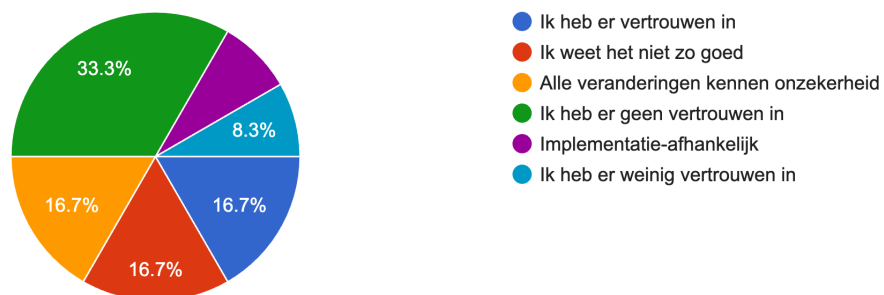
Sterk leiderschap en inzicht. Veel geld meebrengen. Zorg dat er duidelijke rollen zijn en dat velen kunnen deelnemen aan onderdelen van het systeem

er zullen altijd mensen zijn die voorlopers zijn. Die SSI met open armen ontvangen. De grote groep mensen die daarna komt hebben wat meer wantrouwen en die hebben (denk ik) feedback nodig over hoe het werkt, waarom het werkt en wat de voordelen zijn. En daarna zal de groep komen die niet/nauwelijks te overtuigen valt.

Geen idee

8) Hoe sta je qua vertrouwen tegenover digitale uitwisseling van (digitale) gegevens die voor jou belangrijk zijn?

12 responses



- 9) **Digitale identiteit betekent ook dat je meer controle over je eigen databeheer krijgt.**
Hoe zie jij jouw eigen rol als burger wanneer je beseft dat het beheer van jouw gegevens bij jou komt te liggen?

12 responses

Dat ik kan bepalen wat anderen wel en niet van mij mogen weten is fijn. Wel vind ik het lastig om te bedenken dat dit niet iets eenmaligs is (zoals het doorgeven of na mijn dood mijn organen gebruikt mogen worden). Dit is ws iets waar je meerdere keren mee bezig moet zijn en af en toe ook kritisch moet kijken of je bepaalde toestemmingen nog steeds wilt verlenen. En net als nu: wat doen bedrijven met jouw gegevens als je geen klant meer bent?

Wie zegt dat dit waar is? volgens mij krijg ik juist minder controle

Ik geloof er niks van. Big tech plukt alles uit de cloud. 6g is al in ontwikkeling.

Positief, het maakt je meer betrokken en geeft vertrouwen en gevoel van zelfbeschikking.

Fijn maar dat voelt ook al een illusie want data laat overal sporen na dus ik geloof niet meer zo eigen beheer.

Alles is al lang bekend.

Meer eigen verantwoording en bewustwording

irrelevant en niet nodig

net als nu bij mijnoverheid.nl, tijdig informatie aanleveren etc.

Dat is nu ook al zo. Het wordt wat eenduidiger en overzichtelijker lijkt me

Het idee controle te hebben over wat anderen wel en niet van mij mogen weten, vind ik fijn.

Ik hier tegen in opstand komen, ik doe niet mee

Hangt er vanaf hoeveel kennis hier voor nodig is. Verder denk ik dat gebruikers de zwakste schakel zullen zijn met betrekking tot data security.

10) Heb jij in relatie tot SSI ergens zorgen over?

Denk bijv. aan zaken in relatie tot:

- * **privacy;**
- * **controle van gegevens;**
- * **(zelf)controle op digitale gegevensuitwisseling en interoperabiliteit tussen diverse systemen die met elkaar moeten communiceren;**
- * **systeemvertrouwen; vertrouwen in de overheid om het juiste te doen voor burgers ('benevolence' & integriteit);**
- * **vertrouwen in de digitale infrastructuur en het kunnen van de overheid ('ability') ;**
- * **vertrouwen in eigen online handelen.**

10 responses

Alles

Controle over uitwisseling, systeemvertrouwen en juiste implementatie. De burger zou m.i. echt overal controle over moeten hebben. Tuurlijk kan dat betekenen dat de overheid een dienst niet kan verstrekken als ik niet X en Y meestuur, maar ik wil zelf heel specifiek bepalen of ik X en Y meestuur.

Al het bovenstaande

Dat het niet helemaal soepel zal lopen in het begin te veel werk

zowe privacy als misbruik van gegevens lijken me erg belangrijk. Criminelen lopen altijd een stap voor op de overheid, dat is lastig te veranderen.

Ik vertrouw er niet zo op dat het een beetje opschiet. Het bereiken van inzicht duurt zo lang. Geen idee waarom. En vervolgens gaat er weer veel geld en tijd over de balk om het te realiseren. Er is ook veel kwaliteit nodig om het op te zetten en ik zou zeggen gelijk doen op het niveau van de Europese unie.

Voorkom al te veel bureaucratie maar houd wel democratische controle

Op het moment dat er veel juridische taal bij komt, vind ik het lastig. Dan denk ik 'ik wijs alles af' (net als met cookies e.d.) onder het mom 'better safe...' Ook vraag ik me af hoe het dan zit met de gegevens die je bewust verstrekt/zichtbaar maakt en hoe bedrijven daarmee omgaan.

Totaal geen vertrouwen in de overheid

Mijn vertrouwen van de overheid op het gebied van ICT is vrij laag. Zolang zij geen top ontwerpers en systeem programmeurs en hackers aannemen tegen concurrerende topsalarissen (denk aan 2 a 3x een ministersalaris) blijft de overheid op dit gebied een onbetrouwbare partij.

11) Wat kan de overheid doen om ervoor te zorgen dat jij je veilig en gesterkt voelt in het beheren van jouw eigen gegevens en de mogelijke komst van SSI?

12 responses

In het portaal voorbeelden geven en consequenties duidelijk maken. "Als je deze toestemming geeft dan houdt dat in dat... voor de tijdsduur van". Duidelijke taal. en ook: wat gebeurt er als dit systeem gehackt wordt? of iemand achter jouw inloggegevens komt?

Afbakenen waar gegevens voor gebruikt mogen worden

Niks de overheid - ze brengen erin volk tot slavernij.

Transparantie. Audit-trails voor je eigen SSI.

Eerlijk, transparant en duidelijk zijn en vooral ook mensen blijven inzetten ipv alles over te laten aan SSI

Openheid van informatie

helemaal niks

goede informatievoorziening, goede tools/sites creëren.

daadkracht en kwaliteit leveren.

Campagne om ideeën te geven, voorbeelden te geven, consequenties toe te lichten en toe te lichten wat anderen dan eventueel ermee kunnen doen (zowel goed als kwaad).

Alles open source en single use

Zie boven

12) Hoe verwacht je dat de verschillende betrokken partijen met jouw (digitale) data omgaan?

12 responses

ik denk dat overheden zich aan alle privacywetgeving zullen houden. Ik vraag me af of bedrijven hier de mogelijkheid in zien om meer te vragen dan strikt noodzakelijk voor hun dienstverlening. een kwaadwillende medewerker kan (net als nu) veel schade aanrichten. En digitaal lijkt me het gemakkelijker om meer slachtoffers te maken.

Dat ze er misbruik van maken.

Geen vertrouwen in

Volgens de AVG; niet meer dan nodig opvragen.

Met zorg en aandacht

Met zorg!

niet

ik vertrouw overheidsinstanties wel, maar informatie mag niet in verkeerde handen komen. Beveiliging dus belangrijk.

volgens afspraak en daar moet je op toezien. Snap ik de vraag wel?

Binnen de EU ga ik ervanuit dat de betrokken partijen goed (veilig) met mijn data omgaan. Buiten de EU heb ik daar twijfels over.

Misbruik maken van mijn data. Dat ze geld verdienen aan mijn data. Dat ze een ongevallige mening afstraffen

Iedere commerciële partij zal proberen meer data te verzamelen en te bewaren dan de bedoeling is. Verder zullen hackers en landen zoals Rusland en China proberen je identiteit over te nemen

13) Wat vind je dat de overheid kan doen om erop toe te zien dat de uitrol en (mogelijke) ingebruikname van SSI goed verloopt? Welke rol kan de overheid hierin aannemen?

Voorbeelden:

- * Wijze van communiceren veranderen; hoe zou je geïnformeerd willen worden?
- * Het (mogelijk) bestaan van bepaalde zorgen wegnemen; als deze bestaan, hoe kunnen deze weggenomen of verminderd worden?
- * Het opstellen van heldere kaders en regelgeving rondom SSI.

12 responses

Controlerend (toetsend) en informierend.

geen idee

Refurfished: aivd hoort niet in een democratie

Transparant opstellen, niet belerend zijn. Nationaal vs EU scheiden is waarschijnlijk ook verstandig. Ben ik zelf geen voorstander van, maar voor mensen met anti-EU-sentiment lijkt het me verstandig dat ik bijv. niet automatisch ook gegevens met EU-instanties deel als ik ze eigenlijk met NL-(semi-)overheden wil delen.

Heldere kaders, balans, goede afspraken en regels opstellen

Informatie die makkelijk te vinden en vooral te begrijpen is

niets, want er is geen draagvlak

overheids campagne (SIRE), nieuwskanalen (NOS etc.), op Rijksoverheid.nl

kaders en toezicht. dit is erg precair

Het opstellen van heldere kaders en regelgeving rondom SSI in Europees verband. Via een website, spotjes (online) waarin voorbeelden en zorgen langskomen. Ook voorbeelden toelichten waarmee je als burger hier gebruik van zou kunnen maken mét die overheid.

Alle kritiek van alle partijen serieus nemen. Niet zelf doordrukken van agenda's buiten de kamer om

De uitrol van digid was nou niet echt geweldig, waar in eerste instantie alleen de overheid er gebruik van zou maken (belastingen etc) is het nu onmisbaar voor alle communicatie met de gezondheidszorg. Dus het moet vanaf het begin duidelijk zijn voor welke doeleinde dit gebruikt gaat/kan worden en in hoeverre het tot uitsluiting leidt indien men er geen gebruik van maakt.

14) Waar zie je kansen en mogelijkheden rondom SSI? Beschrijf deze.

12 responses

Minder naar het gemeentehuis, minder gedoe bij huren of (ver)kopen van huis. Overstappen van bank of provider zou makkelijker moeten zijn.

mogelijk maakt het bepaalde zaken makkelijker

Geen

MEGA kans wat betreft vertrouwen in overheid terugwinnen voor politiek. Ook kans om proactief privacy-problemen op te lossen.

Voor minder bedeelde en gehandicapten

Mezelf hierin verdiepen

nergens

als het goed aangepakt wordt kan het identiteitsfraude wellicht voorkomen. Ook kan het zorgen voor efficiëntere en snellere dienstverlening door de overheid.

er zijn genoeg mogelijkheden. Begin misschien met simpele dingen zoals het tool van jacobs (irma) om te melden dat je ouder bent dan 18.

Contact met overheid.

Kansen zie ik weinig eerder bedreigingen

Ja, als deze bv Digid vervangt en niet er naast komt.

15) Zie jij risico's en bedreigingen rondom SSI? Zo ja, welke?

12 responses

Hackers (buiten) en kwaadwillenden (binnen)

ICT overheid en budget gaan nooit goed samen, dus invoering gaat miljarden kosten. Door alles te koppelen wordt het mogelijk om ook digitaal geld te koppelen. dan wordt het wel heel gevaarlijk als verkeerde personen aan de macht komen.

Alleen maar

Niet anders dan bij andere technologieën wat betreft hacking, fishing, etc.

Zeer zeker. Ik vind het een heel eng idee hoe de overheid steeds meer 'macht' naar zich toetrekt en er een agenda uitgerold is en wordt. Met veel camera's, Iris scans, overal je ID scannen en opgeven zelfs bij het bezoeken van een museum.

Ja dat er hackers op af komen

Stel dat Hitler hier toegang toe had gehad?

informatie die in verkeerde handen valt, cybercrime dus maar ook zelfs cyberwar (Rusland!)

ja veel. het schiet niet op. te veel politiek gedoe en bureaucratie. Te domme mensen die het opzetten. Bij gebruik: mensen durven niet, gaan heel defensief worden door geen informatie te delen (en snijden zichzelf).

Winstbejag is grootste doel. Aandeelhouders bepalen. Implementatie wordt niet serieus genomen. Teveel om op te noemen

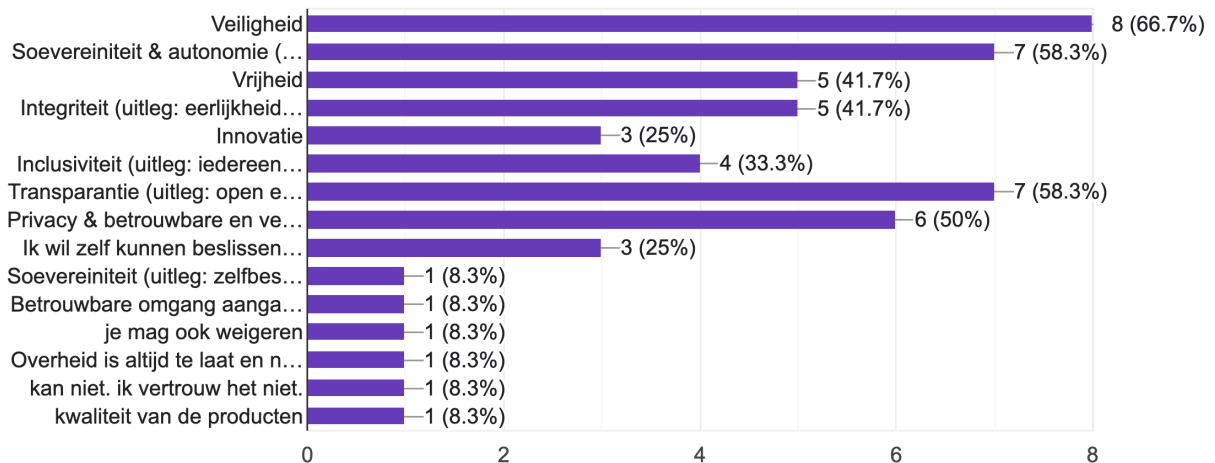
Onwetendheid of onhandigheid bij mensen waardoor zij per onbewust toch teveel data met de verkeerde personen delen. Wat gebeurt er als een derde er met jouw identiteit vandoor gaat?

Zie andere antwoorden

Risico's en bedreigingen komen van 2 kanten, wie heeft regulier toegang tot welke data en hoe wordt dat door de gebruiker bepaald. Is het systeem toekomst bestendig, denk aan quantum computers voor encryptie.

16) Welke waarden spelen voor jou een rol bij het verstevigen van een vertrouwenspositie bij het invoeren van een innovatie als SSI?

12 responses



17) Welke waarde is voor jou het meest belangrijk? En waarom?

12 responses

Veiligheid, omdat het gaat over mijn identiteit. Misbruik kan grote gevolgen hebben.

-

Kleine sociale netwerken en verbondenheid en een roverheid op afstand.

Soevereiniteit en autonomie. Past bij de samenleving. Niet ivm individualisme maar om als individu aan een groep deel te nemen op eigen voorwaarden.

Een keuze hebben en die is er ik veel gevallen niet meer. Doe je niet mee dan kan je bepaalde apps niet meer gebruiken of downloaden of plekken niet bezoeken.

Openheid zodat ik het idee heb dat er geen addertjes onder het gras zijn
irrelevant

veiligheid, vrijheid en innovatie.

kwaliteit, het is anders denken en complex

Privacy & betrouwbare en veilige omgang met mijn gegevens vanuit alle betrokken partijen. Zonder vertrouwen is elk systeem gedoemd te mislukken.

Opt out zonder gevolgen

Privacy & betrouwbare en veilige omgang met mijn gegevens vanuit alle betrokken partijen. Er is niets zo vervelend als iemand anders mijn digitale identiteit overneemt.

18) Signaleer jij risico's rondom SSI in relatie tot jouw waarden? En zo ja, welke?

12 responses

Ja, maar dat heeft elk systeem wel. Als ik mijn paspoort nu kwijtraak, kan iemand daar online ook kwaad mee.

ja, als je een niet welgevallige mening hebt, zoals de truckers in canada, dan wordt je bankrekening bevroren.

De nieuwe slavernij; ai is artificiele indoctrinatie; msm is verlengstuk van politici cq multinational.

Ik zie niet echt in hoe het inclusiviteit verbetert.

Ja zie bovenstaande.

De onduidelijkheid zijn voor mij nog risico

ja, zoals gezegd. Stel dat Hitler hier toegang toe had.

eigenlijk niet.

ja gebrek aan kwaliteit

Ik vind het belangrijk dat iedereen mee kan doen (laagdrempelig) en dat niet kiezen voor SSI ook mogelijk blijft zonder dat er consequenties aanzitten. Ik vermoed dat als SSI meer gebruikt wordt de niet-gebruiker toch gedwongen wordt mee te gaan doen.

Eigenlijk allemaal wel

Als het niet meer wordt dan een verbeterde DigiD heb ik er geen probleem mee.

19) Hoe zouden optionele risico's naar jouw mening geminimaliseerd kunnen worden om jouw waarden te beschermen?

12 responses

Weten hoe deelnemers gecontroleerd worden, wat er gebeurt als misbruik geconstateerd wordt.

-

Alle multinationals socialiseren.

Geen automatische data-uitwisseling tenzij daarvoor opt-in is gegeven. Niets obv opt-out. Het moet zijn alsof het een kluisje is dat bij mij thuis staat met mijn data erin. De overheid belt aan bij de voordeur, vraagt om data, ik beslis wat ik wel en niet geef, en doe het kluisje weer dicht.

Door een keuze te hebben voor een andere mogelijkheid ipv je kunt een app niet meer gebruiken etc. Je wordt nu gedwongen om persoons gegevens vrij te geven

Informatie inwinnen en doornemen

Niet, kijk wat ze in China al doen.

zie vorige vraag.

richt op europees niveau een topteam in om dit in 5 jaar te realiseren.

De bestaande vormen van communiceren met bedrijven en overheden zouden moeten blijven bestaan.

Open source

Door de hoeveelheid beschikbare informatie in een SSI te minimaliseren

20) Heb je nog vragen, opmerkingen of aanvullingen? Noteer ze dan hier.

10 responses

Poeh!!

-

Ik ben er helemaal klaar mee, met die opgelegde controle. Ontmenselijkt en de-humaniseert. Straks de drone die zijn slachtoffer target - waar zijn we mee bezig.

Succes! :)

Zoals je leest sta ik niet te springen om SSI ondanks dat het een deel van onze realiteit is. Het kan ons veel goeds brengen maar dan wel onder strikte voorwaarden

Nee.

De vragen zijn te sturend en de uitkomsten kunnen makkelijk voor onethisch doeleinden ingezet worden. Ik zou hier liever een keer een gesprek met je over hebben en begrijp goed dat het moeilijk voor je is om dit werk af te ronden.

nee, succes.

waarom is email adres een verplicht veld? Ik hoef geen boek namelijk ook al is dat heel aardig. Dus: wil je meedingen voor het boek geef dan je email adres. We hadden ook een 1malige sleutel kunnen bedenken om mij in dit geval te contacten... maar dan is zo'n team eerst nodig ;-) succes met de verwerking

Nee

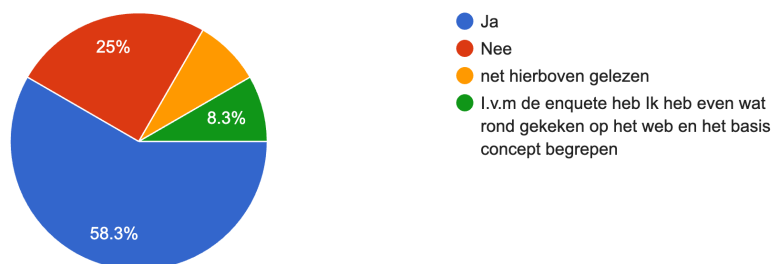
Volledig uitgeschreven analyse aan de hand van de vragenlijst

4.1 Bekendheid met het begrip SSI

Van alle respondenten zegt 58.3 procent bekend te zijn met het begrip SSI oftewel digitale identiteit. 25 procent is niet bekend met het begrip en het overige percentage (16.7 procent) heeft i.v.m. de vragenlijst op het web gekeken of het concept begrepen werd of uit de inleiding van de vragenlijst een interpretatie gemaakt.

1 - Ben je bekend met het begrip Self Sovereign Identity (SSI) oftewel Digitale Identiteit?

12 responses



Samengevat: meer dan de helft (58.3 procent) van de respondenten is bekend met SSI.

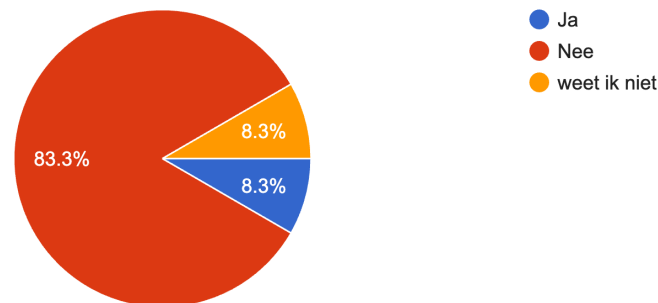
Bij 41.7 procent is SSI slecht of niet bekend.

4.2 Beschikbaarheid van informatie (kennis) om een houding t.o.v. SSI te kunnen aannemen

83.3 procent geeft aan dat er onvoldoende informatie (kennis) beschikbaar is om een houding ten opzichte van SSI te kunnen aannemen. 8.3 procent vindt dat er voldoende informatie beschikbaar is en 8.3 procent geeft ‘weet ik niet’ als respons.

2) Is er volgens jou voldoende informatie (kennis) beschikbaar om een houding ten opzichte van SSI te kunnen aannemen?

12 responses



4.3 Gewenste informatiebehoefte t.o.v. SSI

Gevraagd is ook naar of er een bepaalde informatiebehoefte van SSI bestaat om je als burger beter geïnformeerd te voelen. Deze open vraag leverde diverse antwoorden op. “Ik weet dat SSI bestaat en vind het lastig een beeld te vormen hoe het mij in mijn dagelijkse leven kan ondersteunen. Waarom, waar en hoe kan ik het gebruiken? Wat zijn de voor- en nadelen t.o.v. ‘normale’ identificatie? Kan ik het ook in het normale leven gebruiken (in Nederland of in het buitenland)?, openbaring van besluiten in EU, hoe komt SSI tot stand, wie beslist hierover en hoe kan ik het besluit beïnvloeden?” Er wordt gevraagd om “meer bekendheid” en “meer aandacht lijkt me aan te raden, want ik hoor en zie er weinig tot niets over.” Verder worden genoemd: “Informatie op het web is voornamelijk in het Engels, omschrijving in de Nederlandse Wikipedia is zeer summier.” Een andere respondent noemt: “Het zou fijn zijn als de instanties die hiermee werken informatie op hun site zetten erover. Al is het maar een korte intro met een verwijzing naar een plek waar er meer informatie over te vinden is.” “Wat is de stand van zaken en waarom neemt het zo veel tijd in beslag?” wordt ook gevraagd. Een drietal (25 procent) respondenten geeft aan geen informatiebehoefte te hebben. Eén van hen vermeldt: “Nee, het is een globaal principe en erg afhankelijk van specifieke implementatie.”

4.4 Houding t.o.v. SSI op basis van de huidige bij de burger bekende informatie

Hoe staan de respondenten tegenover SSI op basis van de informatie die bekend is?

Negatief wordt door 25 procent van de respondenten benoemd. Als toelichting wordt vermeld: “geeft de houder ervan te veel macht, eenzijdige controle door overheid (onwenselijke contracten met WHO) en geen duidelijkheid over mogelijke consequenties voor mijn vrijheid. (Stel dat ik tegen vaccinatie ben of een bepaalde mening heb, kan mijn SSI dan op rood gezet worden?) Nu zal dat niet zo’n vaart lopen, maar met corona hebben we ook vergaande vrijheid beperkende maatregelen opgelegd gekregen, die we nooit gedacht hadden.” Een andere respondent heeft een naar onderbuikgevoel bij SSI: “Het gebruik mag kritisch worden bekeken en streng aan banden worden gelegd. In bepaalde mate kan het handig zijn, maar ik vind het ook beperkend.” Een andere respondent is afwachtend. “Een paspoort, rijbewijs op mijn telefoon lijkt me handig voor als ik documenten vergeet mee te nemen, zodat ik me altijd kan identificeren. Online zie ik er nog weinig in.” Een zelfde antwoord wordt door een andere respondent gegeven: “Ik denk dat die identiteit online in plaats van een fysiek ID-bewijs zal gelden (paspoort, rijbewijs). Dat lijkt me aangezien vrijwel alles digitaal gaat, wel een goede aanvulling. Wel lijkt de beveiliging een uitdaging.” Vier respondenten (33 procent) zijn erg positief over het concept: “Omdat het heft in eigen handen geeft bij mensen, heeft het ook het potentieel om vertrouwen terug te geven aan mensen.” Een andere respondent is tevens positief en noemt het “noodzakelijk, er mag veel meer aandacht voor zijn.” Ook “het lijkt me dat ik dit als persoon goed regel, ik online beter beschermd ben” en “in deze tijd moet de overheid regelen dat je persoonsinformatie beschermd wordt en dat je controle houdt over het gebruik van de informatie; ik sta er erg positief tegenover” worden benoemd. Een andere respondent antwoordt: “Lijkt een soort DIGID 2.0; hopelijk minder omslachtig.”

4.5 Wat de overheid kan bieden om verder te bouwen aan vertrouwen rondom SSI

Op de vraag “Wat kan de overheid volgens jou bieden om verder te bouwen aan vertrouwen van burgers rondom de mogelijke komst en gebruik van SSI?” komt naar voren:

“Meer bekendheid aan geven door online campagnes,” “de overwegingen aan het volk voorleggen en betrekken in keuzes, misschien wel referenda”, “veel zelfbeschikking over informatie, transparantie, kunnen zien wie wat inziet.” Deze laatste zin wordt aangevuld met: “de burger vertrouwen omdat wantrouwen richting de burger ook automatisch wantrouwen richting overheid kweekt.” Openheid van informatie wordt door meer respondenten gewenst: “Er openheid over geven en meer informatie die makkelijk toegankelijk is”, “meer

informatieverschaffing, een informatiecampagne online, op tv, radio en in kranten”, “informatievoorziening: wat is het, wat kun je ermee, voorbeelden en voordelen”, “open source maken; het dient één doel, niet meer.” Andere antwoorden zijn: “Hangt er vanaf in hoeverre ik zelf mijn identiteit beheren kan” en “Er is een inhaalslag nodig om het gebrek aan veiligheid van persoonsgegevens te verminderen. Dat is een rol van de overheid omdat het om bescherming gaat van de persoonlijke levenssfeer... Er woedt een informatieoorlog en de overheid kan vertrouwen winnen voor burgers door zich als sterke beschermer op te stellen. Daarvoor is wel meer bewustzijn nodig. De huidige kennis en het tempo bij de overheid stellen niet gerust.” Een andere respondent vindt: “Uit de EU stappen, uit WEF, uit WHO, Bilderberg. Nutsvoorzieningen terug naar Nederlandse bedrijven” en weer een andere respondent schrijft: “Dit erg kritisch en met mate inzetten.”

4.6 Quadrupe helix actoren die kunnen helpen om vertrouwen in SSI te verstevigen

a) Wat de wetenschap kan doen om jouw vertrouwen in SSI te verstevigen

Genoemd worden: “Alles open source maken,” “uitleggen hoe het werkt en wat er voor zorgt dat SSI veilig is en hoe je er zelf voor kunt zorgen dat je veilig met SSI omgaat.” Veiligheid wordt in het kader van de wetenschap meer benoemt: “onderbouwing van veiligheid” en “goede encryptie- en communicatie-protocollen ontwikkelen.” Een andere functie is informeren: “informeren, maar ook vertellen dat er niets gaat boven menselijk contact”, “feiten geven m.b.t. het onderwerp”, “onderzoeken publiceren, populair wetenschappelijke onderzoeken (Quest), leerstoelen hierover aanwijzen bij universiteiten”, “voorbeelden en voordelen schetsen van SSI”. Wat niet direct een antwoord geeft op de gestelde vraag en wellicht duidt op weinig vertrouwen in de wetenschap: “geldstromen van onderzoek inzichtelijk maken” en “huidige wetenschap is niet meer onafhankelijk en waarde vrij”.

b) Wat het bedrijfsleven kan doen om jouw vertrouwen in SSI te verstevigen

Over het bedrijfsleven in relatie tot SSI wordt het volgende verwoord:

“Het bedrijfsleven staat achter bij mij als het gaat om vertrouwen verstevigen. Wel zou ik positief getriggerd zou zijn als ik zou weten hoe SSI hen helpt. Als ik beter weet wat hun voordelen zijn, kan ik zelf een inschatting maken of ik open sta voor het gebruik van SSI.”

“Het bedrijfsleven kan voorbeelden en voordelen schetsen van SSI, maar ik vertrouw het bedrijfsleven minder.” “Afstand nemen hiervan”.

“Hun belangen gaan inzien, investeren in oplossingen en tools die hiermee te maken hebben.”

“Harde garanties geven dat mijn identiteit niet gehackt kan worden.” En: “niks”. Hieruit lijkt het bedrijfsleven in relatie tot SSI en het vergroten van vertrouwen onder burgers beduidend minder vertrouwd te worden. Overige reacties lijken aan te sluiten op het concept open source en informatie delen o.a.: “Bewijzen dat zij alleen met mijn toestemming mijn gegevens mogen inzien, bewaren, etc. Dus ook dit open source,” en wat daarop aansluit “informatie geven m.b.t. het eigen bedrijf”. En: “zorgen voor gemak, maar ook community”.

c) Wat burgers en/of jijzelf kunnen doen om vertrouwen in SSI te verstevigen

Een aantal respondenten zegt niks of geen idee. Andere suggesties die worden gedaan:

“Je medeburger helpen het te begrijpen en vertrouwen wellicht? Maar dat kan ik alleen doen als het ook echt te vertrouwen is zonder dat er rare achterdeurtjes in zitten die afbreuk doen aan het principe en de manier waar op het wordt ingevoerd,” “de informatie opzoeken en goed doornemen”, “meer er over lezen, in het onderwijs inbedden, goed onderscheid maken tussen fake-news/complotdenken en waarheidsgetrouwe informatie”, “de eerste stappen zetten, ervaringsverhalen delen, leren hoe anderen het gebruiken”, “veel praten, verduidelijken, vertrouwen uitstralen?” “Vooral goed voelen wat klopt” wordt ook genoemd. “Er zijn altijd een paar voorlopers, mensen die nieuwsgierig zijn en voordelen zien. Als die er over praten (gebruikersgemak, voordelen, risico’s, wat het hun oplevert) in hun netwerk, dan steekt het anderen weer aan om het uit te proberen.” Een tegengeluid is er ook: “blijven verzetten zolang het niet democratisch is en in alle openheid en transparantie gebouwd wordt.”

4.7 Hoe diverse partijen beter kunnen samen werken om technologische innovatie als SSI te kunnen ondersteunen

“Voor de grote massa (niet de voorlopers) denk ik dat informatie (wat brengt het jou, wat brengt het de bedrijven, wat brengt het de overheid) helpt. Breed inzetten, niet afdwingen.”

“Open source” (meerdere malen benoemd). “Zie bijvoorbeeld hoe het bedrijf Egeniq in de openbaarheid werkte aan COVID QR-apps, het principe hieromheen was erg positief.” “Een samenwerking die ook gedeeld gaat worden met iedereen en niet alleen in hoger segment.”

“Een platform online inrichten, conferenties houden, raamovereenkomsten sluiten.”

Ook leiderschap wordt genoemd: “Sterk leiderschap en inzicht. Zorg dat er duidelijke rollen zijn en dat velen kunnen deelnemen aan onderdelen van het systeem.”

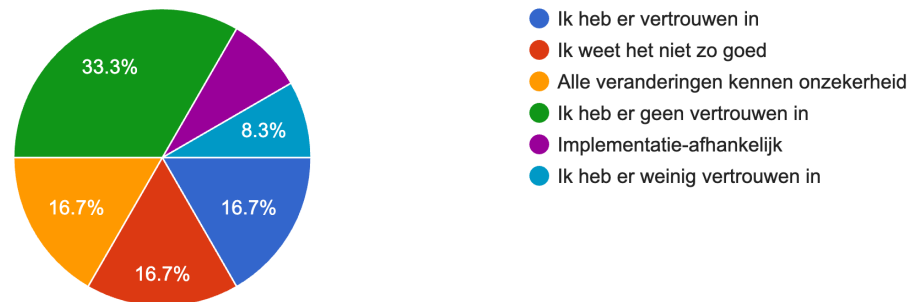
“Er zullen altijd mensen zijn die voorlopers zijn, die SSI met open armen ontvangen. De grote groep mensen die daarna komt hebben wat meer wantrouwen en die hebben (denk ik)

feedback nodig over hoe het werkt, waarom het werkt en wat de voordelen zijn. Daarna zal de groep komen die nauwelijks te overtuigen valt.”

4.8 Vertrouwen t.o.v. digitale uitwisseling van gegevens die voor jou belangrijk zijn?

8) Hoe sta je qua vertrouwen tegenover digitale uitwisseling van (digitale) gegevens die voor jou belangrijk zijn?

12 responses



Een derde van de respondenten heeft geen vertrouwen in digitale uitwisseling van gegevens die belangrijk zijn voor hen als burger. 16.7 procent weet het niet zo goed, 16.7 procent vindt dat alle veranderingen onzekerheid kennen, 16.7 procent heeft er wel vertrouwen in. 8.3 procent heeft er weinig vertrouwen in.

4.9 Rol als burger bij eigen databeheer

Hoe de eigen rol als burger wordt gezien wanneer je beseft dat het beheer van jouw gegevens bij jou komt te liggen: “Dat is nu ook al zo. Het wordt eenduidiger en overzichtelijker, lijkt me.” “Het idee controle te hebben over wat anderen wel en niet van mij mogen weten, vind ik fijn.” Dat haakt weer aan op zelfbeschikking, wat een andere respondent benoemt: “positief, het maakt je meer betrokken en geeft vertrouwen en gevoel van zelfbeschikking.”

“Dat ik kan bepalen wat anderen wel en niet van mij mogen weten, is fijn. Wel vind ik het lastig om te bedenken dat dit niet iets eenmaligs is... Dit is iets waar je meerdere keren mee bezig moet zijn, en af en toe ook kritisch moet kijken of je bepaalde toestemmingen nog steeds wilt verlenen. En net als nu: wat doen bedrijven met je gegevens als je geen klant meer bent?” “Hangt er vanaf hoeveel kennis hier voor nodig is. Verder denk ik dat de gebruikers de zwakste schakel zullen zijn met betrekking tot data security.”

“Meer eigen verantwoording en bewustwording”. Ook wordt genoemd: “Net als bij mijnoverheid.nl tijdig informatie aanleveren, etc.” Tegengeluid wordt ook gegeven:

“Fijn, maar dat voelt ook als een illusie want data laat overal sporen na dus ik geloof niet meer zo in eigen beheer.” “Ik geloof er niks van. Big Tech plukt alles uit de cloud. 6G is al in ontwikkeling”, “Wie zegt dat dit waar is? Volgens mij krijg ik juist minder controle.” Ook “irrelevant en niet nodig” en “ik doe niet mee” worden genoemd.

4.10 Zorgen in relatie tot SSI

Zorgen die betrekking hebben op SSI worden gedeeld. Het systeemvertrouwen (m.a.w. het vertrouwen in de overheid) blijkt laag, zo wordt meerdere malen benoemd door respondenten. “Controle over uitwisseling, systeemvertrouwen en juiste implementatie. De burger zou echt overal controle over moeten hebben. Tuurlijk kan dat betekenen dat de overheid een dienst niet kan verstrekken als ik niet X en Y meestuur, maar ik wil zelf heel specifiek bepalen of ik X en Y meestuur.” “Totaal geen vertrouwen in de overheid.” En: “Mijn vertrouwen van de overheid op het gebied van ICT is vrij laag. Zo lang zij geen top ontwerpers en systeemprogrammeurs en hackers aannemen tegen concurrerende topsalarissen ... blijft de overheid op dit gebied een onbetrouwbare partij.”

Andere antwoorden van respondenten zijn: “dat het niet soepel zal lopen in het begin”, “te veel werk”, “zowel privacy als misbruik van gegevens lijken met belangrijk. Criminelen lopen altijd een stap voor op de overheid, dat is lastig te veranderen.” Uitgebreidere reacties: “Ik vertrouw er niet zo op dat het opschiet. Het bereiken van inzicht duurt lang. Geen idee waarom. Vervolgens gaat er geld en tijd over e balk om het te realiseren. Er is ook veel kwaliteit nodig om het op te zetten... ik zou zeggen gelijk doen op het niveau van de Europese Unie” en “Op het moment dat er veel juridische taal bij komt, vind ik het lastig. Dan denk ik ‘ik wijs alles af’ onder het mom ‘better safe...’ Ook vraag ik me af hoe het dan zit met de gegevens die je bewust verstrekt/zichtbaar maakt en hoe bedrijven daarmee omgaan.”

Andere zaken die genoemd worden: “Alles” en “Al het bovenstaande” (wat als voorbeeld genoemd is in de vraagstelling: privacy; controle van gegevens; (zelf)controle op digitale gegevensuitwisseling en interoperabiliteit tussen systemen die met elkaar moeten communiceren; systeemvertrouwen; vertrouwen in de digitale infrastructuur en het kunnen van de overheid; vertrouwen in eigen online handelen).

Ook: “Voorkom al te veel bureaucratie, maar houd democratische controle” wordt benoemd.

4.11 Wat kan de overheid doen om ervoor te zorgen dat jij je veilig en gesterkt voelt in het beheren van jouw eigen gegevens en de mogelijke komst van SSI?

“Goede informatievoorziening, goede tools/sites creëren.” “”Duidelijke taal”, inzetten. In het kader van verdere informatievoorziening wordt genoemd: “Campagne om ideeën en voorbeelden te geven, consequenties toelichten en toelichten wat anderen eventueel kunnen doen (zowel goed als kwaad).” “Voorbeelden geven en consequenties duidelijk maken: ‘als je deze toestemming geeft, dan houdt dat in dat... voor de tijdsduur van...’ En: wat gebeurt er als dit systeem gehackt wordt of iemand achter jouw inloggegevens komt?”

Verder zou een rol van de overheid kunnen zijn het “afbakenen waar gegevens voor gebruikt mogen worden”. Transparantie komt meerdere malen terug in de antwoorden:

“Transparantie. Audit-trails voor je eigen SSI” en “Eerlijk, transparant en duidelijk zijn en vooral ook mensen blijven inzetten i.p.v. alles over te laten aan SSI” en “openheid van informatie”. Ook “open source” en “single use” worden hier genoemd. Een aantal keer wordt “niks” benoemd.

4.12 Verwachting over de omgang met jouw (digitale)data door betrokken partijen

“Ik denk dat overheden zich aan alle privacywetgeving houden. Ik vraag me af of bedrijven hier de mogelijkheid in zien om meer te vragen dan strikt noodzakelijk voor hun dienstverlening. Een kwaadwillende medewerker kan... veel schade aanrichten. En digitaal lijkt me het gemakkelijker om meer slachtoffers te maken.” “Volgens de AVG: niet meer dan nodig opvragen.” Twee respondenten antwoorden: “Met zorg (en aandacht)”. Een andere respondent verwacht dat er “volgens afspraak” met de data wordt omgegaan, maar “je moet er op toezien.” Er is bij een andere respondent vertrouwen dat “binnen de EU betrokken partijen goed (veilig) met data omgaan. Buiten de EU bestaan daar twijfels over.” Vijf van de twaalf respondenten heeft er “geen vertrouwen” in en/of verwacht dat er “misbruik van gemaakt zal worden”. Bijvoorbeeld “dat ze geld verdienen aan mijn data” en “iedere commerciële partij zal proberen meer data te verzamelen en te bewaren dan de bedoeling is. Verder zullen hackers en landen zoals Rusland en China proberen je identiteit over te nemen.” Een andere respondent vertrouwt overheidsinstanties wel, maar “informatie mag niet in verkeerde handen komen. Beveiliging is dus belangrijk.”

4.13 Wat de overheid kan doen om erop toe te zien dat de (mogelijke) uitrol en ingebruikname van SSI goed verloopt.

Welke rol kan de overheid hierin aannemen?

“Controlerend (toetsend) en informierend”, “Informatie die makkelijk te vinden en vooral te begrijpen is”. “Transparant opstellen, niet belerend zijn. Een andere respondent noemt: “Overheidscampagne (SIRE), nieuwskanalen (NOS, etc.), Rijksoverheid.nl.” Weer een andere respondent vult aan: “Website, spotjes (online) waarin voorbeelden en zorgen langskomen. Ook voorbeelden toelichten waarmee je als burger hier gebruik van zou kunnen maken met die overheid.” “Heldere kaders, balans, goede afspraken en regels opstellen”, “Kaders en overzicht” en “Het opstellen van heldere kaders en regelgeving rondom SSI in Europees verband” worden benoemd.

“Nationaal vs. EU scheiden is waarschijnlijk ook verstandig. Ben ik zelf geen voorstander van, maar voor mensen met een anti-EU-sentiment lijkt het me verstandig dat ik bijv. niet automatisch gegevens met EU-instanties deel als ik ze eigenlijk met NL-(semi)overheden wil delen”. “Alle kritiek van alle partijen serieus nemen” is weer een andere opmerking, wat door dezelfde respondent wordt aangevuld met: “Niet zelf doordrukken van agenda’s buiten de Kamer om.” Weer een andere respondent zegt: “Niets, want er is geen draagvlak.” Een andere respondent haalt de uitrol van DigiD aan: “Die was niet geweldig, waar in eerste instantie alleen de overheid er gebruik van zou maken (belastingen, etc.) is het nu onmisbaar voor alle communicatie met de gezondheidszorg. Het moet vanaf het begin duidelijk zijn voor welk doeleinde dit gebruikt gaat/kan worden en in hoeverre het tot uitsluiting leidt indien men er geen gebruik van maakt.”

4.14 Kansen en mogelijkheden rondom SSI

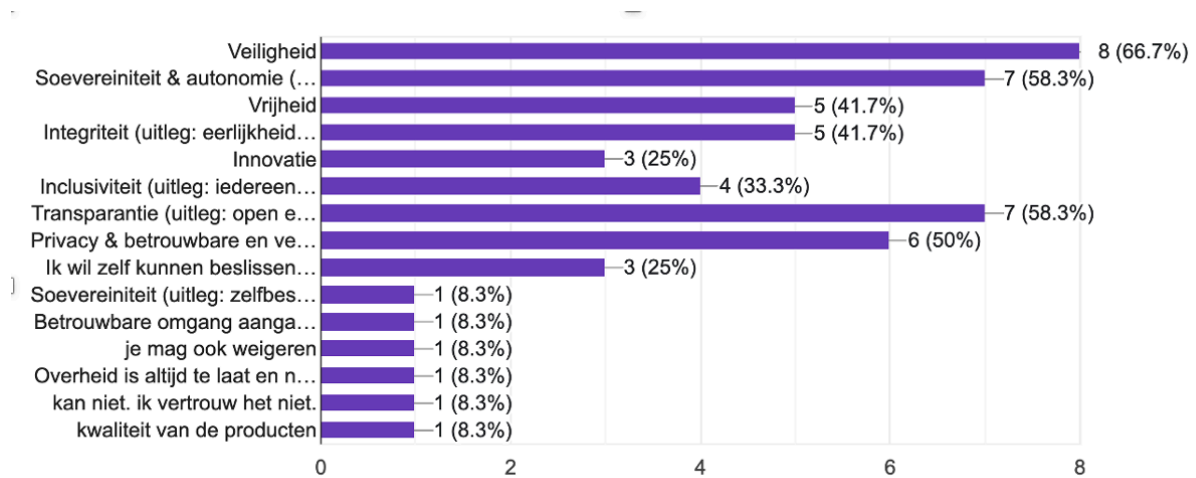
- “Minder naar het gemeentehuis, minder gedoe bij huur of (ver)koop van een huis. Overstappen van bank of provider zou makkelijker moeten zijn.”
- “Mogelijk maakt het bepaalde zaken gemakkelijker.”
- “Mega kans wat betreft vertrouwen in overheid terugwinnen voor politiek. Ook kans om proactief privacy-problemen op te lossen.”
- “Als het goed aangepakt wordt, kan identiteitsfraude wellicht voorkomen worden. Het kan zorgen voor efficiëntere en snellere dienstverlening door de overheid.”
- “Mezelf hierin verdiepen.”

- “Geen” en “nergens kansen” en “kansen zie ik weinig, eerder bedreigingen.”
- “Contact met overheid.”
- “Ja, als deze DigiD vervangt en niet ernaast komt.”
- “Voor minder bedeelden en gehandicapten.”

4.15 Risico’s en bedreigingen rondom SSI

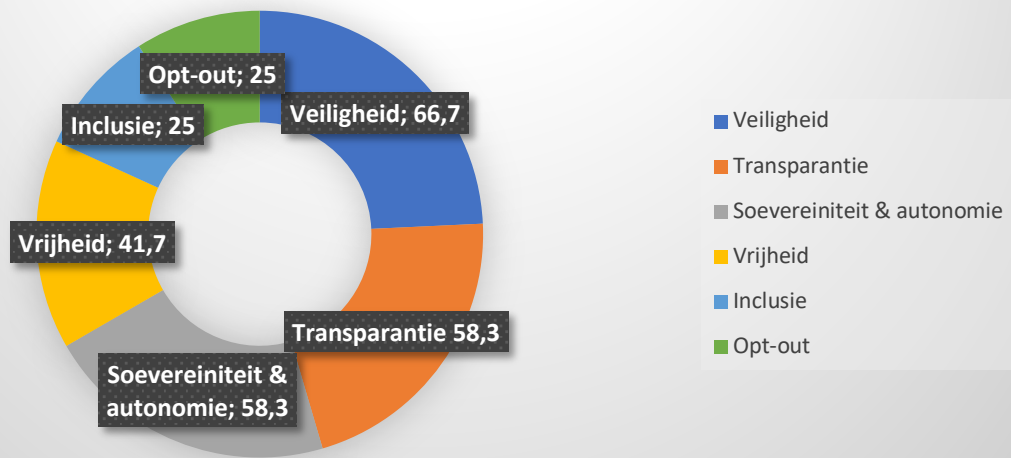
- “Hackers (buiten) en kwaadwillenden (binnen)” en tevens van een andere respondent: “Dat er hackers op af komen.”
- “ICT overheid en budget gaan nooit goed samen, dus invoering gaat miljarden kosten. Door alles te koppelen wordt het mogelijk om ook digitaal geld te koppelen, dan wordt het wel heel gevaarlijk als verkeerde personen aan de macht komen.”
Een andere respondent noemt: “Stel dat Hitler hier toegang toe had gehad?” en weer een andere respondent heeft het over “Informatie die in verkeerde handen valt. Cybercrime maar ook cyberwar.”
- “Risico’s en bedreigingen komen van 2 kanten: wie heeft regulier toegang tot welke data en hoe wordt dat door de gebruiker bepaald? Is het systeem toekomstbestendig? Denk aan quantum computers voor encryptie.”
- “Ik vind het een heel eng idee hoe de overheid steeds meer ‘macht’ naar zich toetrekt en er een agenda uitgerold is en wordt. Met veel camera’s, Iris-scans, overal je ID scannen en opgeven.”
- “Alleen maar.”
- “Niet anders dan bij andere technologieën, wat betreft hacking, fishing, etc.”
- “Veel risico’s: Het schiet niet op. Te veel politiek gedoe en bureaucratie. Bij gebruik: mensen durven niet, worden defensief door geen informatie te delen (en snijden zichzelf).”
- “Winstbejag is het grootste doel. Aandeelhouders bepalen. Implementatie wordt niet serieus genomen. Te veel om op te noemen.”
- “Onwetendheid of onhandigheid bij mensen, waardoor zij onbewust te veel data met de verkeerde personen delen. Wat gebeurt er als een derde er met jouw identiteit vandoor gaat?”

4.16 Waarden die voor respondenten een rol spelen bij het verstevigen van een vertrouwenspositie bij het invoeren van een innovatie als SSI



Veiligheid wordt door 66.7 procent van de respondenten benoemd als belangrijke waarde die een rol spelen bij het verstevigen van een vertrouwenspositie. Op de voet gevolgd door transparantie en soevereiniteit & autonomie (beiden 58.3 procent). Privacy wordt aangevinkt door de helft van de respondenten. Vrijheid en integriteit zijn beiden door 41.7 procent van de respondenten aangevinkt. Inclusiviteit is door een derde (33.3 procent) van de respondenten benoemd. Innovatie en ‘Ik wil zelf kunnen beslissen om hier aan mee te doen en ook voor een opt-out kunnen kiezen zonder dat dit verdere consequenties op uitsluiting heeft’ zijn door een vierde van de respondenten aangevinkt. 1 respondent geeft aan soevereiniteit belangrijk te vinden; 1 respondent geeft aan “Je mag ook weigeren”, 1 respondent schrijft op: “Overheid is altijd te laat en neemt contraproductieve beslissingen. Ze voeren een politieke daad uit en hollen achter WEF aan. De multinational met exorbitant winstbejag regeert.”, 1 respondent schrijft “Kan niet, ik vertrouw het niet” en 1 respondent geeft “Kwaliteit van de producten” op. 1 respondent kiest voor “Betrouwbare omgang aangaande mijn gegevens vanuit alle betrokken partijen.”

Belangrijkste waarden genoemd rondom SSI



4.17 Welke waarde is voor jou als respondent het meest belangrijk? En waarom?

- “Veiligheid, omdat het gaat over mijn identiteit. Misbruik kan grote gevolgen hebben.”
- “Kleine sociale netwerken en verbondenheid en een roverheid op afstand.”
- “Soevereiniteit en autonomie. Past bij de samenleving. Niet i.v.m. individualisme maar om als individu aan een groep deel te nemen op eigen voorwaarden.”
- “Een keuze hebben en die is er in veel gevallen niet meer. Doe je niet mee, dan kan je bepaalde apps niet meer gebruiken of downloaden of plekken niet bezoeken.”
- In dezelfde lijn als de vorige reactie: “Opt-out zonder gevolgen.”
- “Openheid zodat ik het idee heb dat er geen addertjes onder het gras zijn.”
- “Veiligheid, vrijheid en innovatie.”
- “Kwaliteit, het is anders denken en complex.”
- “Privacy & betrouwbare en veilige omgang met mijn gegevens vanuit alle betrokken partijen. Zonder vertrouwen is elk systeem gedoemd te mislukken.” En: “Er is niets zo vervelend als iemand anders mijn digitale identiteit overneemt.”

4.18 Gesignaleerde risico's in relatie tot waarden van respondenten

“Ja” wordt veelvuldig genoemd. “Ja, maar dat heeft elk systeem wel. Als ik mijn paspoort nu kwijtraak, kan iemand daar online ook kwaad mee.”

“Als je een niet welgevallige mening hebt, zoals de truckers in Canada, dan wordt je bankrekening bevroren.” “De nieuwe slavernij; AI is artificiële indoctrinatie; msm¹¹ is verlengstuk van politici cq multinational.” “Ja, zoals gezegd. Stel dat Hitler hier toegang toe had.” “Ik zie niet echt in hoe het inclusiviteit verbetert.” Een andere respondent schrijft: “Ik vind het belangrijk dat iedereen mee kan doen (laagdrempelig) en dat niet kiezen voor SSI ook mogelijk blijft zonder dat er consequenties aanzitten. Ik vermoed dat als SSI meer gebruikt wordt de niet-gebruiker toch gedwongen wordt mee te gaan doen.”

“De onduidelijkheid is voor mij een risico” en “Gebrek aan kwaliteit.”

“Eigenlijk allemaal wel.” Twee respondenten zien minder risico’s rondom waarden:

“Als het niet meer wordt dan een verbeterde DigiD, heb ik er geen probleem mee.”

“Eigenlijk niet.”

4.19 Hoe zouden optionele risico’s geminimaliseerd kunnen worden om jouw waarden te beschermen?

“Weten hoe deelnemers gecontroleerd worden, wat er gebeurt als misbruik geconstateerd wordt.” “Geen automatische data-uitwisseling tenzij daarvoor opt-in is gegeven. Niets o.b.v. opt-out. Het moet zijn alsof het een kluisje is dat bij mij thuis staat met mijn data erin. De overheid belt aan bij de voordeur, vraagt om data, ik beslis wat ik wel en niet geef, en doe het kluisje weer dicht.” Keuze-opties zijn ook voor de volgende respondent van belang: “Door een keuze te hebben voor een andere mogelijkheid i.p.v. je kunt een app niet meer gebruiken etc. Je wordt nu gedwongen om persoonsgegevens vrij te geven.” “Informatie inwinnen en doornemen.” “Richt op Europees niveau een topteam in om dit in 5 jaar te realiseren.”

“De bestaande vormen van communiceren met bedrijven en overheden zouden moeten blijven bestaan.” “Open source.” “Door de hoeveelheid beschikbare informatie in SSI te minimaliseren.” Andere reacties zijn: “Niet, kijk wat ze in China al doen.” En “Alle multinationals socialiseren.”

¹¹ Het nadeel van een vragenlijst is dat je niet door kunt vragen bij respondenten zoals bij een interview. Met ‘msm’ wordt naar alle waarschijnlijkheid ‘mainstream media’ bedoeld (Google, 2023).

4.20 Relevante vragen, opmerkingen en aanvullingen uit het onderzoek

“Ik ben er helemaal klaar mee, met die opgelegde controle. Ontmenselijkt en dehumaniseert... Waar zijn we mee bezig.” “Zoals je leest, sta ik niet te springen om SSI ondanks dat het een deel van onze realiteit is. Het kan ons veel goeds brengen, maar dan wel onder strikte voorwaarden.”

“De vragen zijn te sturend en de uitkomsten kunnen makkelijk voor onethische doeleinden ingezet worden.” Samenvattend: deze opmerkingen duiden bij deze groep respondenten op zorg over de inzet van SSI in relatie tot ethiek.

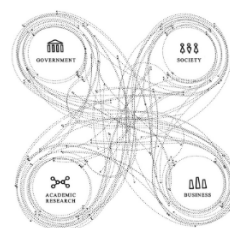
ONDERZOEKS RESULTATEN SSI

Overall ontwikkelpunten

Er zijn 3 ontwikkelpunten die veelvuldig naar voren komen in het onderzoek en die van invloed op de ontwikkelomgeving:

- 1) Verstevig de rollen vanuit quadruple helix perspectief; vergroot de betrokkenheid & samenwerking met burger
- 2) Verbeter de communicatie/informatievoorziening en vergroot kennis over SSI; zorg voor openheid & transparantie
- 3) Onderzoek hoe het vertrouwen te verstevigen door nader onderzoek onder actoren

Ontwikkelpunt 1: Verstevig de rollen Gewenste rol van de overheid



Overheid

Bescherm, controleer, informeer

Regel dat persoonsinformatie beschermd wordt en dat er controle is over informatie; controleer (toets) op correct dataverkeer en informeer hierover

Zorg voor transparantie in houding en bij het delen van informatie

Transparante, eerlijke doelstelling; vanaf de start transparantie geven aan de hand van communicatie; geen belerende houding, maar een transparante

Openheid van informatie

Open source; single use; goede tools/sites creëren. Audit-trails voor je eigen SSI

Verbeter de communicatie/informatievoorziening

Een betere informatievoorziening rondom SSI; meer bekendheid aan geven door campagnes; informatie toegankelijk maken; volk betrekken bij keuzes (wellicht referenda); informatie die makkelijk te vinden en te begrijpen is; communiceer direct of iets gaat leiden tot uitsluiting wanneer men er geen gebruik van wil maken

Geef veel zelfbeschikking aan burgers

Over (eigen) informatie; kunnen zien wie wat inziet; transparantie en openheid in systeem; open source; vertrouwen in de burger vanuit de overheid; biedt mogelijkheden tot inclusie (en exclusie op basis van eigen keuze);

Vergroot overheidskennis en verhoog ontwikkeltempo

Geef voorbeelden en verhelder consequenties

'Als je deze toestemming geeft, dan houdt dat in dat... voor de tijdsduur van...' Afbakenen waar gegevens voor gebruikt mogen worden

Balans, goede afspraken en regels opstellen

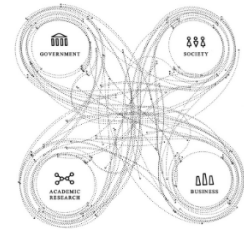
Neem alle kritiek van partijen serieus mee

Niet zelf doordrukken van agenda's buiten de Kamer om

Nadenken over verbinding met EU

Nationaal vs. EU scheiden kan verstandig zijn vs. het opstellen van heldere kaders, regelgeving en overzicht rondom SSI in Europees verband

Ontwikkelpunt 1: Verstevig de rollen Gewenste rol van de burgers



Burgers

- Help de medeburger SSI te begrijpen en vertrouwen
- De informatie opzoeken en goed doornemen; meer erover lezen
- Goed onderscheid (kunnen) maken tussen fake-news/complotdenken en waarheidsgetrouwe informatie
- Ervaringsverhalen delen; leren hoe anderen het gebruiken; veel erover praten, verduidelijken
- Mensen die nieuwsgierig zijn en voordelen zien, kunnen erover praten in hun netwerk (gebruikersgemak, voordelen, risico's, wat het hun oplevert), zodat het anderen motiveert het ook uit te proberen
- Voel goed wat klopt

Houding t.o.v. eigen rol rondom eigen databeheer SSI

Gevoel van zelfbeschikking geeft vertrouwen

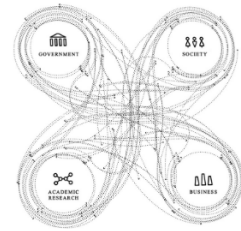
controle over wat anderen wel en niet van mij mogen weten, is fijn;
meer eigen verantwoording; betrokkenheid en bewustwording

Met SSI wordt het mogelijk eenduidiger en overzichtelijker

Veelgestelde vraag: hoeveel kennis is er voor nodig? (zie ook: zorgen)

Ontwikkelpunt 1: Verstevig de rollen

Gewenste rol van de wetenschap & het bedrijfsleven



Wetenschap

Open source

Onderbouw veiligheid en informeer hierover; leg uit hoe het werkt en wat er voor zorgt dat SSI veilig is en hoe je er zelf voor kunt zorgen dat je veilig met SSI omgaat; neem ook het belang van menselijk contact mee in de communicatie

Schets voorbeelden en voordelen van SSI

Focus op onderzoek en onderwijs

Onderzoeken publiceren;
ook focus op populair-wetenschappelijke onderzoeken (Quest);
leerstoelen aanwijzen bij de universiteit;
SSI in het onderwijs inbedden; feiten geven

Ontwikkel goede encryptie- en communicatie-protocollen



Bedrijfsleven

Open source

Verstevig vertrouwenspositie; die lijkt laag
Bedrijfsleven lijkt de minst grote vertrouwenspositie t.o.v. SSI te hebben. Vijf van de twaalf respondenten heeft er "geen vertrouwen" in en/of verwacht dat er "misbruik van gemaakt zal worden". Bijvoorbeeld "dat ze geld verdienen aan mijn data." "Iedere commerciële partij zal proberen meer data te verzamelen en te bewaren dan de bedoeling is." Wat doen bedrijven met je data? Daar is nu geen inzicht in, dus:

Maak inzichtelijk hoe SSI een bedrijf helpt (belangen inzichtelijk maken)
wat hun voordelen zijn, zodat de gebruiker zelf kan bepalen of hij of zij openstaat voor het gebruik van SSI en digitaal uitwisselen van data

Bewijs dat bedrijven alleen met mijn toestemming mijn gegevens mogen inzien, bewaren, etc. investeren in oplossingen en tools

Garandeer dat de identiteit niet gehackt kan worden

Zorg voor gemak en community

Kansen & mogelijkheden, risico's & bedreigingen en zorgen

Aangegeven door respondenten in de enquête



Kansen & mogelijkheden

- Kan een goede vervanging zijn voor de DIGID en het fysieke identiteitsbewijs
- Je geeft het heft terug in handen van burgers en dat heeft potentieel om vertrouwen terug te geven aan mensen; kans wat betreft vertrouwen in overheid terugwinnen voor politiek. Plus een kans om proactief privacy-problemen op te lossen
- Online beter beschermd (als je het zelf goed inregelt)
- Meer snelheid en gemak bij het regelen van zaken; efficiëntere en snellere dienstverlening (door de overheid): "minder naar het gemeentehuis, minder gedoe bij huur of (ver)koop van een huis en overstappen van een bank of provider zou makkelijker moeten zijn"
- Kan mogelijk identiteitsfraude voorkomen, als het goed aangepakt wordt
- Kan het contact met de overheid verbeteren
- Neem ook de kansen voor minder bedeelden en gehandicapten mee (inclusie)

Kansen & mogelijkheden, risico's & bedreigingen en zorgen



Aangegeven door respondenten in de enquête

Beveiliging een uitdaging: hacking, fishing & angst voor informatie in handen van kwaadwillenden

"Hackers (buiten) en kwaadwillenden (binnen)" en tevens van een andere respondent: "Dat er hackers op af komen." "Verder zullen hackers en landen zoals Rusland en China proberen je identiteit over te nemen." "Informatie mag niet in verkeerde handen komen. Beveiliging dus belangrijk." Een andere respondent noemt: "Stel dat Hitler hier toegang toe had gehad?" en weer een andere respondent heeft het over "Informatie die in verkeerde handen valt in relatie tot cybercrime maar ook cyberwar." "Door alles te koppelen wordt het mogelijk om ook digitaal geld te koppelen, dan wordt het wel heel gevaarlijk als verkeerde personen aan de macht komen." "Criminelen die voor lopen op de overheid." "Zorg voor eventuele rare achterdeurtjes." Maar ook: "Niet anders dan bij andere technologieën, wat betreft hacking, phishing, etc." En: "Als ik mijn paspoort nu kwijtraak, kan iemand daar online ook kwaad mee."

Invoering gaat miljarden kosten en duurt lang; zorg over gebrek aan kwaliteit

"ICT overheid en budget gaan nooit goed samen, dus invoering gaat miljarden kosten. Door alles te koppelen wordt het mogelijk om ook digitaal geld te koppelen, dan wordt het wel heel gevaarlijk als verkeerde personen aan de macht komen." "Veel risico's: Het schiet niet op. Te veel politiek gedoe en bureaucratie. Bij gebruik: mensen durven niet, worden defensief door geen informatie te delen (en snijden zichzelf)." "Het bereiken van inzicht duurt lang, geen idee waarom." "Implementatie wordt niet serieus genomen." "Gebrek aan kwaliteit." "Geld en tijd over de balk om het te realiseren."

Er heerst angst en wantrouwen; controle, macht en privacy-issues verdienen aandacht

"Ik vind het een heel eng idee hoe de overheid steeds meer 'macht' naar zich toetrekt en er een agenda uitgerold is en wordt. Met veel camera's, Iris scans, overal je ID scannen en opgeven – zelfs bij museums." "Eenzijdige controle door de overheid." "Winstbejag is het grootste doel. Aandeelhouders bepalen. Implementatie wordt niet serieus genomen." "Privacy en misbruik van data." "Geeft de houder te veel macht." "Het systeemvertrouwen (m.a.w. het vertrouwen in de overheid) lijkt laag; of laag in relatie tot ICT waardoor het een onbetrouwbare partij genoemd wordt."

Risico's m.b.t. het systeem SSI; is dit toekomstbestendig?

"Risico's en bedreigingen komen van 2 kanten: wie heeft regulier toegang tot welke data en hoe wordt dat door de gebruiker bepaald? Is het systeem toekomstbestendig? Denk aan quantum computers voor encryptie."

Risico's m.b.t. eigen handelen rondom data-beheer en controle door gebruiker

"Onwetendheid of onhandigheid bij mensen, waardoor zij onbewust te veel data met de verkeerde personen delen. Wat gebeurt er al een derde er met jouw identiteit vandoor gaat?" "Wie heeft toegang tot welke data en hoe wordt dat door de gebruiker bepaald?"

Risico's m.b.t. inclusiviteit en optie tot exclusie om mee te doen aan SSI

"Ik zie niet echt in hoe het inclusiviteit verbetert." Een andere respondent schrijft: "Ik vind het belangrijk dat iedereen mee kan doen (laagdrempelig) en dat niet kiezen voor SSI ook mogelijk blijft zonder dat er consequenties aanzitten. Ik vermoed dat als SSI meer gebruikt wordt de niet-gebruiker toch gedwongen wordt mee te gaan doen."

Onduidelijkheid als risico; ook m.b.t. vrijheid en beperking

"De onduidelijkheid is voor mij een risico." "Geen duidelijkheid over mogelijke consequenties voor vrijheid." "Handig maar ook angst voor beperking."

Kansen & mogelijkheden, risico's & bedreigingen en zorgen

Aangegeven door respondenten in de enquête



Proces & uitwerking SSI

- "Dat het niet soepel loopt in het begin."
- "Te veel werk."
- "Er is kwaliteit nodig om het op te zetten; waarom niet gelijk op het niveau van de EU?"
- "Hopelijk minder omslachtig dan een DIGID 2.0."
- "Lastig wanneer er juridische taal bij komt kijken. Dan wijs ik liever alles af."

Controle & toezicht op data

- Controle over uitwisseling, systeemvertrouwen en juiste implementatie.
- De burger zou echt overal controle over moeten hebben.
- Het gebruik mag kritisch bekeken worden en aan banden worden gelegd.
"Je moet er op toezien hoe er met je data wordt omgegaan."
- Er bestaat een zorg dat gebruikers zwakste schakel zijn m.b.t. data security.
- "Onduidelijkheid over hoe het werkt met gegevens die je bewust verstrekt/zichtbaar maakt. Hoe gaan bedrijven om met mijn gegevens?"

Wantrouwen eigen databeheer:

"Fijn, maar dat voelt ook als een illusie want data laat overal sporen na dus ik geloof niet meer zo in eigen beheer." "Ik geloof er niks van. Big Tech plukt alles uit de cloud. 6G is al in ontwikkeling", "Wie zegt dat dit waar is? Volgens mij krijg ik juist minder controle."

Hoeveel kennis is er voor nodig bij de gebruiker?

Hoe vaak moet je toestemmingen verlenen en hoe houd je daar overzicht op?

"Lastig om te bedenken dat dit niet iets eenmaligs is..."

Dit is iets waar je meerdere keren mee bezig moet zijn, en af en toe ook kritisch moet kijken of je bepaalde toestemmingen nog steeds wilt verlenen."

Ontwikkelpunt 2: Verbeter de communicatie/informatievoorziening

Uitgangspunt openheid & transparantie



Communicatie heeft in het proces rondom SSI meer aandacht nodig

Er bestaat een informatiebehoefte - in duidelijke, eenvoudige Nederlandse taal - waarin SSI op eenvoudige wijze uitgelegd wordt. Instanties die werken met SSI kunnen informeren over (de mogelijke ontwikkeling van) SSI op hun websites.

Vragen waarop een antwoord nodig is:

- Waarom is er SSI?
- Hoe komt SSI tot stand?
- Hoe en waarvoor kan ik SSI gebruiken?
- Waarom werkt SSI?
- Wat zijn de voor- en nadelen voor alle betrokken partijen: burgers, overheid, bedrijven, wetenschap? (Ook t.o.v. normale identificatie)
- Is SSI zowel in Nederland als in het buitenland veilig en bruikbaar?
- Wie beslist er over SSI?
- Kan ik besluiten over SSI beïnvloeden? Zo ja, hoe?
- SSI: wat is de stand van zaken in de ontwikkeling? En het tijdspad?
- Wat gebeurt er als SSI gehackt wordt of iemand achter jouw inloggegevens komt?

Ontwikkelsuggesties:

- Voorbeelden geven en consequenties duidelijk maken: 'als je deze toestemming geeft, dan houdt dat in dat... voor de tijdsduur van...'
- Campagne om ideeën en voorbeelden te geven, consequenties toelichten en toelichten wat anderen eventueel kunnen doen (zowel goed als kwaad). Overheids campagne (SIRE), nieuwskanalen (NOS, Rijksoverheid.nl). Website, spotjes (online) waarin voorbeelden en zorgen langskomen. Ook voorbeelden toelichten waarmee je als burger hier gebruik van zou kunnen maken met die overheid.
- Een andere respondent haalt de uitrol van DIGID aan: "Die was niet geweldig, waar in eerste instantie alleen de overheid er gebruik van zou maken (belastingen, etc.), is het nu onmisbaar voor alle communicatie met de gezondheidszorg. Het moet vanaf het begin duidelijk zijn voor welk doeleinde dit gebruikt gaat/kan worden en in hoeverre het tot uitsluiting leidt indien men er geen gebruik van maakt."

Ontwikkelpunt 3: Onderzoek hoe het vertrouwen te verstevigen door nader onderzoek onder actoren



Samen bouwen begint vanuit vertrouwen

De antwoorden uit het onderzoek lijken te duiden op weinig systeemvertrouwen onder de kleine groep respondenten; ook het vertrouwen in eigen databeheer is nog niet optimaal evenals het vertrouwen in digitale gegevensuitwisseling van persoonsgegevens. Het vertrouwen in het bedrijfsleven m.b.t. het gebruik van data van burgers lijkt erg laag; uit het onderzoek blijkt dat er veel vraagtekens bestaan wat een bedrijf doet met data van derden en er bestaat een wens daar inzicht in te verkrijgen. Zelfcontrole over eigen data en helder inzicht in wat er met eigen data gebeurt, zijn wensen. Op deze punten ligt een aanbeveling tot verder onderzoek om vertrouwen te kunnen verstevigen en te onderzoeken of SSI als systeem kan bijdragen aan deze vertrouwensvormen, wanneer het aan bepaalde wensen/eisen voldoet.



Systemvertrouwen



Vertrouwen in digitale gegevensuitwisseling



Gebruikersvertrouwen / 'user trust'



Vertrouwen in bedrijfsleven m.b.t. datagebruik