Digitale Identiteit: een nieuwe balans

Job Spierings en Tom Demeyer

waag
technology & society

Digitale Identiteit: een nieuwe balans
Job Spierings en Tom Demeyer

Het Digitale Identiteit team van Waag:
Coen Bergman, Gijs Boerwinkel, Tom Demeyer, Dick van Dijk,
Jimena Gauna, Thijs van Himbergen, Amalie Hovgesen,
Ivonne Jansen-Dings, Max Kortlander, Joost Mollen,
Denise Op den Kamp, Alain Otjens, Laurie Skelton, Job Spierings,
Socrates Schouten, Marleen Stikker, Judith Veenkamp.

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No. 732546.

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Vereniging van Nederlandse Gemeente

decode

waag

Inhoudsopgave

Maak je schepels en mudden om mee te meten, dan zul je met schepels en mudden worden bedrogen.
Maak je weegschalen en gewichten om mee te wegen, dan zul je met weegschalen en gewichten worden bedrogen.
Maak je insignes en zegels om mee te waarmerken, dan zul je met insignes en zegels worden bedrogen.
Bevorder je menslievendheid en gerechtigheid om de wereld in rechte banen te leiden, dan zul je met menslievendheid en gerechtigheid worden bedrogen.
Hoe weet ik dat dit zo is? Steel een riemgesp en je wordt terechtgesteld! Steel een land en je wordt een edelman!

ANONIEM, 3e eeuw v. Chr.

Wat is het wegingskader?

Kun je online kenbaar maken wie je bent en wat je wilt?

Als die eerste vraag (wie?) niet goed beantwoord kan worden, zijn er drie reacties mogelijk:

- We proberen het maar gewoon in de hoop dat het meestal goed gaat. De gevolgen van identiteitsfraude of misverstanden/misbruik bij machtiging nemen we voor lief en lossen we later wel op.
- We vermoeden dat het niet goed kán gaan, en doen daarom maar niks. Het is voor een gemeente bijvoorbeeld 'onmogelijk' om een burger telefonisch te helpen, omdat de identiteit niet kan worden vastgesteld.
- We verliezen overzicht, vertrouwen en handelingsperspectief en haken af. Mensen zeggen: "we zijn onze privacy toch al kwijt" of: "Facebook/DigiD/ze weten toch al alles van je".

We lijken onszelf veroordeeld te hebben tot technologie die ondoorzichtig, onbetrouwbaar, onveilig en onvoldoende is. Burgers geven tamelijk unaniem aan dat ze controle, overzicht en vertrouwen verliezen. Overheden stellen vast dat zij een ander, uitgebreider begrip van Digitale Identiteit nodig hebben om complexere en persoonlijker digitale diensten te kunnen leveren. Uit oogpunt van dienstverlening, beleidsimpact of kostenbesparing. Het wegingskader Digitale Identiteit heeft tot doel gezamenlijk en geordend na te kunnen denken over ethiek, waarden en normen voor Digitale Identiteit. Het wil bijdragen aan het debat en de visievorming op dit onderwerp en streeft naar een integere toepassing van nieuwe technologie in de maatschappij door inzicht te geven in ethische dilemma's en mogelijke strategieën om hiermee om te gaan.

Het wegingskader:

- ordent de input uit het Digitale Identiteitslab en combineert dit met bestaande frameworks voor waarden en technologie;
- geeft een kader waarin technische *requirements* logisch en herleidbaar volgen uit een set waarden en normen.

Voor wie?

In eerste instantie is dit wegingskader bedoeld voor de deelnemers van het Digitale Identiteitslab. Daarnaast voor alle medewerkers van overheden, bedrijven en organisaties die zich willen verdiepen in nieuwe vormen van digitale identiteit en het delen van persoonlijke data.

Het Digitale Identiteitslab

Het wegingskader is gebaseerd op de diverse inbreng tijdens en rond het Digitale Identiteitslab. Dit vond plaats van juni - december 2018 en bestond uit een aantal design sprints, meetups en interviews waarin concepten zijn opgehaald, onderzocht en getest in gemeentelijke context. Waag organiseerde het Digitale Identiteitslab in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en de Vereniging Nederlandse Gemeenten.

In het Digitale Identiteitslab hebben we onderzoek gedaan naar welke waarden en normen van belang zijn. Naar wat mensen zeggen als je met hen over dit onderwerp in gesprek gaat. Met ontwerpers en bouwers van alternatieve systemen voor digitale identiteit en het delen van persoonlijke data hebben we ontwerpprincipes benoemd. Met verschillende gemeenten hebben we uitgezocht hoe nieuwe vormen van digitale identiteit werken in uiteenlopende use cases. Met ontwikkelaars en architecten van nieuwe, open-source systemen hebben we lange gesprekken gevoerd over decentrale oplossingen, *side-channel attacks* en het voorkomen en opsporen van fraude.

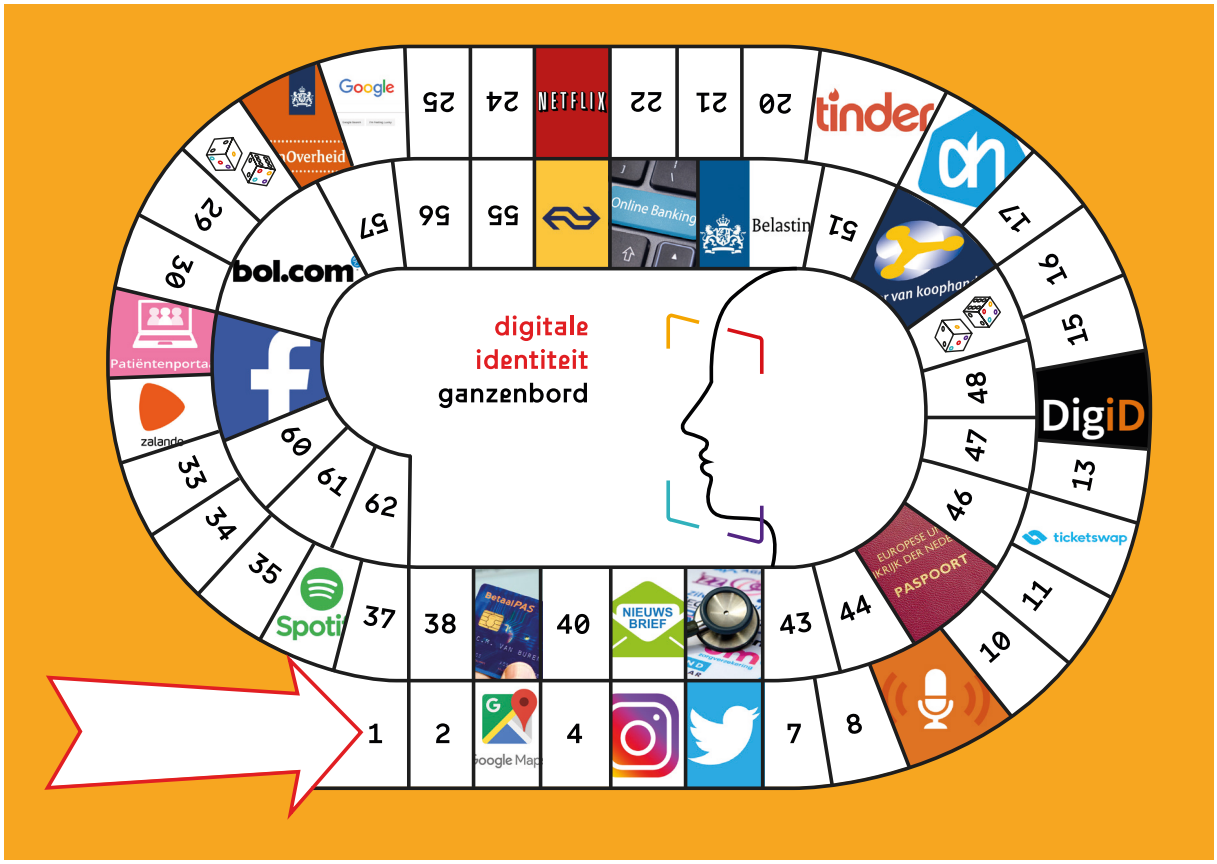
De resultaten hiervan zetten we als volgt op een rij:

- Na een inleiding volgt een overzicht van de actuele problemen met digitale identiteit.
- We doen verslag van de waarden die in het lab naar voren komen, de relatie met digitale identiteit en geven een aantal goede ontwerpprincipes die nu al worden ingezet: *users as designers*, webrichtlijnen, 6 pilaren van Tada!, BurgerServiceCode.

- We hebben vijf principes benoemd die juist nu nieuw en urgent zijn: omdat de technologie beschikbaar is, de noodzaak en impact hoog.

Ook benoemen we vragen die om nader onderzoek en verkenning vragen: waarbij de technologie er nog niet is, de vraag van de gebruiker nader onderzoek vergt of de impact van ontwikkelingen nog niet echt beoordeeld kan worden.

Zie de toelichting bij bronnen voor een compleet overzicht van evenementen en het gebruikte materiaal.



Het digitale identiteit ganzenbordspel

Inleiding

Met de komst van het internet heeft iedereen ook een digitale identiteit gekregen: we moeten aan de aanbieder van informatie of diensten steeds weer laten weten wie we zijn. Dat doen we vaak zonder er goed over na te denken. We maken een profiel aan bij een aanbieder van online winkelen, bij een sociaal media platform of een andere nieuwe app. Voor de aanbieders is het daardoor bekend wie we zijn en wat we doen. Om met de overheid digitaal te communiceren is ook een digitale identiteit nodig, in de meeste gevallen is dat DigiD.

Bedrijven en overheden hebben het ontwerp van digitale identiteit geoptimaliseerd vanuit het eigen blikveld. Webshops hebben niet alleen belang bij de verificatie om zeker te zijn dat er betaald wordt, het is steeds aantrekkelijk geworden om zoveel mogelijk gegevens te verzamelen. Die gegevens zijn namelijk geld waard, waardoor het speelveld op het internet fundamenteel is veranderd. Eerst was het vraagstuk 'on the internet nobody knows you're a dog'[1]: er kon vrijelijk anoniem gesurft worden op het internet. Nu is het probleem dat alles bekend is over de gebruiker en dat die informatie ongekende effecten heeft op wat iemand wel en niet te zien krijgt op het internet.

Als we vanuit het belang van het individu kijken, zou digitale identiteit er dan hetzelfde uitzien als hij nu is? Is het nodig dat de aanbieder van een stappenteller-app al jouw bewegingen verzamelt in een database ? Willen we dat onze betaalgegevens kunnen worden gedeeld met zorgverzekeraars? Is het handig om tientallen gebruikersnamen en wachtwoorden te onthouden? Willen we ons met onze biometrie identificeren? Hoe hard is het onderscheid tussen attributen van identiteiten die 'publiek' en 'privaat' zijn, of tussen 'burger' en 'bedrijf'? Is het voor iedereen begrijpelijk hoe DigiD werkt ? Hoe blijven we soeverein en houden we controle over onze eigen data.

"On the Internet, nobody knows you're a dog."

In het Digitale Identiteitslab zijn we met een grote verscheidenheid aan deelnemers de verschillende perspectieven expliciet gaan maken. De inzet is om ontwerpprincipes te formuleren die recht doen aan het belang van de burger in relatie tot de zekerheid die overheid, bedrijven en samenleving over zijn identiteit nodig hebben. Waar is bij gemeentelijke dienstverlening behoefte aan? Wat zijn de verschillen tussen de use-cases? Hoe reageren burgers op prototypes/tests met nieuwe tools? Kunnen we balans brengen tussen grondrechten van privacy en zelfbeschikking met de noodzaak om je digitaal te kunnen identificeren?

Marleen Stikker

1 https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog

Probleemstelling: wat is er mis met digitale identiteit?

In de meetups, design sprints en gesprekken tijdens het Digitale Identiteitslab kwamen heel veel verschillende problemen naar voren. We tellen er acht, op verschillende onderdelen en niveaus. Onderstaand zetten we ze op een rij.

1. Onveilig

Identiteitsfraude is een groeiend probleem: Volgens het ministerie van BZK zijn in Nederland zo'n 500 mensen per dag slachtoffer van een vorm van identiteitsfraude. Er zijn in 2017 liefst 10.000 datalekken gemeld, onder meer bij gemeenten. Wereldwijd werden miljarden gebruikersnamen en andere persoonlijke data gestolen. In de media[2] struikel je bijkans over berichten over datalekken, hacks en misbruik van persoonlijke gegevens.

"Op zich heb ik er niet zoveel problemen mee maar ze moeten er geen misbruik van kunnen maken."

2. Onzeker

Het is dus niet zo vreemd dat zowel gebruikers als dienstverleners voortdurend onzeker zijn: Komt deze bestelling écht bij die winkel terecht? Is de klant echt wie zij lijkt te zijn? Controleurs hamsteren data en transactiegegevens waarmee profielen worden aangelegd die het mogelijk maken outliers (een teken van fraude) vast te stellen. Gebruikers overzien door de vele checks en balances het bos niet meer en hebben als uitgangspunt het vermoeden dat bijvoorbeeld 'DigiD toch alles van je weet'. Dit is de kern van een panopticon: het vermoeden van controle is voldoende om mensen hun gedrag aan te laten passen, waarmee vrijheid van gedrag of beweging wordt ingeperkt.

2 https://www.fastcompany.com/90272858/how-our-data-got-hacked-scandalized-and-abused-in-2018

"Ik denk dat de meeste mensen, ik ook, eigenlijk wel anoniem willen blijven. Maar in deze tijd kan je eigenlijk bijna niet meer anoniem blijven. Dat ze dingen weten over jou, wie je bent en via Google kunnen zien wie je bent. Dat is wel raar vind ik. Maar het hoort er nu eenmaal bij. Het is 2018, je doet er niks aan."

"Ik ben me bewust van hoe complex het is, hoe internet ons leven beïnvloedt en nieuwe vormen geeft, wat geweldig is. Maar ook hoe we soms grip kwijtraken. De media staan vol van wie en waar die data heen gaat."

3. Ontbrekende dienstverlening

Stel: je hebt moeite om rond te komen en wilt weten wanneer een bedrag wordt bijgeschreven of afgeboekt. Je belt met de helpdesk bij de gemeente: maar die mag je niks concreets zeggen, want ze kunnen aan de telefoon je identiteit niet vaststellen. Voor veel mensen is een persoonlijk kort telefoongesprek veel toegankelijker dan het raadplegen van een online website. Van gezondheidszorg tot buurtregisseur, van jeugdhulp tot woningbouw en schuldhulpverleners: al deze diensten zitten vol met ideeën en plannen waarmee zij hun taak beter, persoonlijker en efficiënter kunnen uitvoeren. Maar: zonder een digitale identiteit die voor hun specifieke doelgroep werkbaar, betrouwbaar en veilig is, blijft het bij plannen, kleinschalige pilots en frustraties. Vervolgens wordt de overheid vaak verweten verkokerd te opereren en elke poging tot een holistische aanpak in de kiem te smoren.

4. Black box: onwetendheid

In moderne ontwerpmethodes is het mantra 'de gebruiker centraal'. Onbedoeld wordt het controleren van identiteit bij dit *user centric design* alleen als hobbel gezien en niet als moment om een gebruiker controle te geven en een bewuste afweging en keuze te laten maken. Identiteitscontrole wordt zoveel mogelijk verborgen of onzichtbaar gemaakt. Als voorbeeld: in de welwillende dienstverlening naar gemeenten maakt DigiD het aansluiten van diensten op haar systeem zo makkelijk mogelijk. Inzicht in of begrip van technologie is voor gemeenten

maar heel beperkt nodig. Nu gemeenten worden uitgenodigd om over te stappen op beter beveiligde versies van DigiD is het lastig om hen van het belang daarvan te overtuigen.

Een betrokken, kritisch gebruik wordt daarmee onbedoeld ontmoedigd of onmogelijk gemaakt: er is geen verweer mogelijk tegen 'the system says no', omdat er geen argumenten uitgewisseld kunnen worden. Een gedegen functioneel en technisch begrip van digitale identiteit en beveiliging is dus een voorwaarde om lokale overheden te bewegen veiliger technologie te gebruiken. Min of meer magisch, op de achtergrond werkende processen ontmoedigen begrip en reflectie en daarmee betrokkenheid. Dat maakt de samenleving kwetsbaar. Dat infrastructuur, code, beheersovereenkomsten en andere informatie alleen inzichtelijk zijn voor een klein groepje ingewijden maakt de black box groter en moedigt onverschilligheid aan.

Sinds de invoering van de nieuwe wetgeving AVG/GDPR[3] geldt de wettelijke opdracht privacy vanaf het allereerste begin van een systeem expliciet te ontwerpen. Dit heet privacy-by-design en het is belangrijk omdat je sommige ontwerpkeuzes achteraf domweg niet meer veilig en transparant kúnt maken.

5. Centralisatie en surveillance

Leveranciers van digitale identiteit reageren op de onveiligheid en onoverzichtelijkheid door systemen te bouwen die ze zoveel mogelijk zélf controleren en beheersen. Daarin voeren ze een voortdurende surveillance uit door alle transacties en activiteit te traceren en vast te leggen. Maar het centraliseren van kwetsbare, cruciale infrastructuur introduceert een heel nieuw veiligheidsrisico: niet alleen is bij storingen, misbruik of hacks direct het hele systeem gecorrumpeerd, het maakt het systeem ook aantrekkelijker en waardevoller voor misbruik en inbraken. Dit is zichtbaar in de diverse hacks en manipulaties op het Facebookplatform[4] en de rapportages van de Autoriteit Persoonsgegevens (AP) waar alleen al in de eerste helft van 2018 8.898 datalekken werden gemeld[5].

Door centralisatie en het aan gebruikers aanbieden van 'black boxes' is het praktisch onmogelijk geworden systemen te leveren die qua governance en techniek voldoen aan deze regels. Uit oogpunt van controle en beheersing wordt zoveel vastgelegd en gevolgd dat er weer complexe systemen en bestuurlijk toezicht nodig is om aan wetgeving te voldoen. Het eenvoudigweg technisch of met versleuteling afdwingen van doelbinding of het beperken van bepaalde transacties is niet mogelijk.

"Ik vind het een beetje dubbel. Enerzijds doe ik niks verkeerd, dus denk ik als ik niks verkeerds doe, wat maakt het uit? ik ben een hardwerkend persoon. Maar aan de andere kant het feit dat je niet weet wat men daar allemaal mee kan gaan doen? Je kunt misschien wel weten aan wie je het hebt gegeven, maar niet wat zij daar dan weer mee gaan doen. Dat stukje vind ik een beetje vervelend. Ik ben voor de rest niet geheimzinnig maar ik heb ook niet de behoefte om al mijn gegevens overal te laten."

6. Geen ruimte voor alternatieven

De marktmacht van grote 'Log-in Providers' (Facebook, Yahoo, Google) is aanzienlijk en ontneemt zuurstof aan alternatieve businessmodellen en technologieën. Een kleine ondernemer die een webshop begint of een sportclub die een onderlinge competitie wil delen hebben de keuze tussen het zelf opzetten en beheren van een database met email/wachtwoordcombinaties (kwetsbaar) of het implementeren van een inlogmogelijkheid met Facebook. De kennis, ervaring en investeringen van de overheid op het gebied van *online identity management* zijn op geen enkele manier maatschappelijk inzetbaar.

7. Businessmodel

Wie heel veel data over digitale identiteiten en hun gedrag heeft, kan geautomatiseerd profielen samenstellen.

3 AVG en GDPR zie: https://nl.wikipedia.org/wiki/Algemene_verordening_gegevensbescherming

4 Zie: https://krebsonsecurity.com/2018/09/facebook-security-bug-affects-90m-users/

5 https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/meldplicht_datalekken_halfjaarrapportage_q1_en_q2_2018_algemeen.pdf

Toegang tot deze profielen is een business-model met hoge marges: voor advertenties, gedragsbeïnvloeding, profilering van verzekerden, kredietwaardigheid. De maatschappelijke impact van deze businessmodellen is internationaal onderwerp van verhit gesprek en onderzoek in politieke debatten, referenda en verkiezingen. Dat een enkele burger hier of daar met reclame om de tuin wordt geleid is hoogstens onbehoorlijk of ongewenst.

Maar hier zijn niet te negeren signalen dat er maatschappelijke-ontwrichting-as-a-service geleverd kan worden. Ook op nationale schaal is elke dataset op basis van digitale identiteit altijd kwetsbaar voor oneigenlijk of commercieel hergebruik (als jij iemand bent die iedere 2 jaar een nieuw paspoort aanvraagt kunnen we je beter ook geen krediet/woning/online rating geven).

8. Bestuurlijk en juridisch vacuüm (‘empty chair’)

Een fundamenteel deel van de maatschappelijke infrastructuur is onder beheer van partijen die buiten de eigen democratisch gelegitimeerde jurisdictie of zelfs buiten elke betekenisvolle invloedssfeer vallen.

De facto en zelfs de jure ontbreekt dan de mogelijkheid om verhaal te halen, in beroep te gaan of enige maatschappelijke regie te hebben. Opgeslagen data kan fout of achterhaald zijn of worden gedeeld met verkeerde partijen. Politieke afwegingen worden zo buiten een politieke sfeer gemaakt op basis van private randvoorwaarden en infrastructuur, terwijl deze standaarden wel ons dagelijks leven beïnvloeden.

‘Empty chair’: Mark Zuckerberg ontbreekt bij een hoorzitting van het Britse Lagerhuis in november 2018 - foto: Gabriel Sainhas.

Van waarden naar techniek

Digitale, persoonlijke diensten zijn aantrekkelijk: het is fijn als taken efficiënter en effectiever uitgevoerd kunnen worden. Efficiëntie en effectiviteit zijn voor de overheid zelfs een beginsel van 'goed openbaar bestuur'. Maar uit het voorgaande overzicht van actuele problemen met digitale identiteit blijkt dat er van alles gebeurt waar de meeste mensen het mee oneens zullen zijn, of waar zij zich ongemakkelijk over zullen voelen. Allerlei publiek gedeelde waarden die wij belangrijk vinden komen in het gedrang:

- Voortdurende monitoring bedreigt privacy.
- Bij gedragssturing dreigt manipulatie.
- Bij profilering dreigt discriminatie.
- Black-box systemen zijn niet toegankelijk voor democratische controle.
- Complexiteit sluit mensen buiten.
- Uitsluiting leidt tot ongelijkheid.
- Onoverzichtelijkheid beperkt keuzevrijheid en zelfbeschikking

Welke waarden vinden we dan belangrijk?

Om dit te onderzoeken gingen we in het Digitale Identiteitslab de straat[6] op, organiseerden we meet-ups over ontwerpprincipes[7] en waarden[8], expertsessies[9] en organiseerden we design sprints. In een design sprint werd in korte tijd door een multidisciplinair team digitale identiteit onderzocht door samen een prototype te ontwerpen voor een specifieke casus.

Wat noemen mensen spontaan als je vraagt wat ze belangrijk vinden bij het delen van persoonlijke data op het internet? Ze noemen vooral: vertrouwen, transparantie, gemak en heel vaak: controle en privacy.

Een paar citaten uit de interviews die we hielden:

"Dat de burger zijn autonomie kan blijven behouden, dus ook op internet."

"Vertrouwen, alles begint met vertrouwen."

"Zelfcontrole: en dan wil ik ook doelen op de privacy. Dat vind ik heel belangrijk. Dat ik zelf een beetje de baas blijf over mijn eigen identiteit."

"Privacy is de belangrijkste. Omdat je er vanuit wil kunnen gaan dat andere partijen je privacy waarborgen en die niet zullen schenden."

"Privacy, dat je daar zelf controle over hebt."

"Privacy: ik wil niet dat iemand zomaar, zonder dat ik het doorheb, al mijn gegevens kan pakken. Komt ook weer terug op dat autonomie."

"Ik denk dat de meeste mensen, ik ook, eigenlijk wel anoniem willen blijven. Maar in deze tijd kan je eigenlijk bijna niet meer anoniem blijven."

"In principe zou je zo min mogelijk willen delen. Je zit eigenlijk niet op het internet om te delen - tenminste: niet om het te delen met ongevraagde partijen. In principe zou je zo min mogelijk aan zo min mogelijk partijen data willen weggeven."

Tijdens de meetup 'designing personal data'[10] werden de waarden transparantie, toegang, controle en integriteit genoemd.

Waardenladders in design sprints

Elke design sprint startte met een waardenladder[11]: een methode waarmee de waarden van deelnemers vanaf het begin expliciet worden gemaakt en tijdens het hele ontwerpproces zichtbaar blijven. Dat leverde bij twee sprints de volgende lijstjes op:

6 https://digitaleidentiteit.waag.org/artikel/video-serie/
7 https://digitaleidentiteit.waag.org/artikel/jouw-digitale-identiteit/
8 https://digitaleidentiteit.waag.org/artikel/stel-je-bouwt-een-digitale-tool-op-basis-van-een-waarde/
9 https://digitaleidentiteit.waag.org/wp-content/uploads/sites/6/Verslag-Expertsessie-Fieldlab-24-09-2018.pdf
10 https://digitaleidentiteit.waag.org/artikel/jouw-digitale-identiteit/
11 https://ccn.waag.org/navigator/tool/values-tree

Designsprint 'een rijbewijs als attribuut op je telefoon'

- Transparant (systeem)
- Veilig (techniek/data)
- Privacy
- Gemak
- Vrijheid/zelf-soeverein
- Autonomie /(zelf)controle
- Betrouwbaarheid (correct & juist)

Designsprint 'data delen bij aanvragen van hypotheek'

- Eigen regie
- Transparantie
- Gemak
- Betrouwbaarheid
- Inclusiviteit
- Data-minimalisatie

Belangrijke, breed gedeelde normen en waarden zijn ook vastgelegd in wetten en verdragen: de grondwet, het Europees Verdrag voor de Rechten van de Mens en de sustainable development goals van de VN. Twee artikelen uit de Nederlandse grondwet gaan direct over privacy en persoonlijke data. Artikel 10 gaat over privacy:

Artikel 10[12]
1. Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op eerbiediging van zijn persoonlijke levenssfeer.

2. De wet stelt regels ter bescherming van de persoonlijke levenssfeer in verband met het vastleggen en verstrekken van persoonsgegevens.

3. De wet stelt regels inzake de aanspraken van personen op kennisneming van over hen vastgelegde gegevens en van het gebruik dat daarvan wordt gemaakt, alsmede op verbetering van zodanige gegevens.

En artikel 11 over het lichaam:

Artikel 11[13]
Ieder heeft, behoudens bij of krachtens de wet te stellen beperkingen, recht op onaantastbaarheid van zijn lichaam.

Er wordt in juridische context rond dit artikel expliciet een koppeling gemaakt met het voorgaande artikel, dat de privacy van burgers beschermt. Met de in 2018 ingevoerde Algemene verordening gegevensbescherming (AVG)[14] heeft de wettelijke bescherming van persoonlijke data in Europa een enorme boost gekregen. Deze wetgeving is internationaal voorbeeldstellend en zou een voorbode kunnen zijn van een nieuw Europees zelfvertrouwen in het digitale domein.

De focus van de wet richt zich nog wel vooral op het beschermen van individuen. In een speech van oktober 2018 'Putting Dignity back into Digital' zei de Europese GDPR-tsaar Butarelli daarover:

"Another thing is clear. The GDPR is about the rights of the individual. But the more personal data processing affects the collective interest, the less we can look to the GDPR for answers."
(Butarelli, 2018)[15]

Macht en autonomie

Waarom wordt in elk lijstje hierboven, naast privacy, ook controle genoemd? Mensen willen autonoom handelen: zelf kunnen beslissen over hun leven en handelen, zelf te beslissen om hulp te bieden, of om hulp te vragen. En autonomie vereist macht. In de online wereld ervaren mensen dagelijks dat ze misschien wel rechten hebben, iets zouden moeten kunnen doen of mogen - maar dat het niet lukt. Of dat er wordt gedaan alsof je een keuze hebt. Waar is bij de pop-up op deze website de knop 'niet akkoord'?

12 http://wetten.overheid.nl/jci1.3:c:BWBR0001840&hoofdstuk=1&artikel=10&z=2017-11-17&g=2017-11-17
13 http://wetten.overheid.nl/jci1.3:c:BWBR0001840&hoofdstuk=1&artikel=11&z=2017-11-17&g=2017-11-17
14 https://www.autoriteitpersoonsgegevens.nl/nl/over-privacy/wetten/algemene-verordening-gegevensbescherming-avg
15 https://www.privacyconference2018.org/system/files/2018-10/Choose%20Humanity%20speech_0.pdf

Digitale identiteit regelt de toegang tot diensten waarmee we ons recht kunnen halen en aan onze plichten kunnen voldoen. Als dat systeem niet goed functioneert heeft dat grote gevolgen: als je een verzekering aansprakelijk wil stellen, belastingaangifte wil doen, in bezwaar gaat, studiefinanciering wil of hulp voor je moeder of zoon wilt aanvragen. Nu deze diensten steeds meer en soms uitsluitend online beschikbaar zijn, wordt digitale identiteit een steeds belangrijker poortwachter.

Dat in gesprekken en waardenladders controle, eigen regie, autonomie, vrijheid en soevereiniteit zo vaak terugkomen laat zien dat mensen zich op deze onderdelen bedreigd voelen door de oprukkende technologie en digitale diensten.[16]

Zelfbestuur

Zonder macht is er geen autonomie. Iets bezitten terwijl je machteloos bent is betekenisloos. Daarom staan er bijvoorbeeld in elk Nederlands paspoort de volgende drie zinnen:

Dit paspoort is eigendom van de staat der Nederlanden. De houder is verplicht het paspoort zorgvuldig te bewaren. Het mag slechts ter beschikking gesteld worden gesteld indien daartoe een wettelijke verplichting bestaat.

Hiermee beschermt de overheid haar burgers door iets niet te geven, maar uit te lenen. Een bedrijf kan niet in zijn voorwaarden opnemen dat je een paspoort moet afgeven en daarmee iemand verplichten zijn identiteit af te geven. De overheid beschermt de burger ten opzichte van partijen die een machtspositie hebben. Zo mogen we bijvoorbeeld ook niet onze eigen nieren verkopen, want in artikel 11 van de grondwet is de integriteit van het lichaam vastgelegd.

Daarom geldt 'data beschikbaar is data kwetsbaar'. Als burgers meer controle en regie over hun data krijgen, zonder dat hun autonomie daarbij evenredig versterkt wordt is het onvermijdelijk dat deze data in handen komt van allerlei derde partijen en zo vooral de positie van de grote, commerciële ICT spelers zal versterken.[17]

Om autonomie (begrepen als zelfbestuur) te realiseren zijn er twee dingen nodig: individuele capaciteit en een ondersteunende omgeving:[18]

Individuele capaciteit:
- je moet iets weten
- je moet een beslissing kunnen nemen
- je moet iets kunnen doen

Ondersteunende omgeving:
- die je hiertoe in staat stelt
- en enige beperking/beheersing oplegt

Omdat individuele (en steeds vaker ook collectieve) autonomie als gevolg van nieuwe technologie onder druk staat, stelt Rinie van Est van het Rathenau instituut vier acties voor. Twee om het collectief handelingsperspectief te vergroten, aangevuld door twee nieuwe mensenrechten:[19]

1. Vergroot publieke en politieke bewustwording.
2. Ontwikkel technologisch burgerschap: burgers zijn weerbaar en geïnformeerd en zij kunnen deelnemen aan de besluitvorming rondom technologie.
3. Het recht om niet gemeten, geanalyseerd of gecoached te worden.
4. Het recht op betekenisvol menselijk contact en menselijke controle.

16 Susskind onderscheid vier bronnen van macht voortkomend uit digitale technologie:
1. Informatie controle: wat weet je?
2. Perceptie controle: hoe beoordeel je dat?
3. Aandacht controle: waar richt je je aandacht op?
4. Decision making: wat doe je uiteindelijk?
Een berucht voorbeeld is de beweging 'Black Lives Matter': op sociale media werd dit vooral een provocatief en te ridiculiseren onderwerp, in plaats van een roep om zorg en aandacht. Zie: Jamie Susskind, 'Future Politics: Living Together in a World Transformed by Tech' (2018).

17 Bart Jacobs, presentatie 'About Self-Sovereignty', Pl.lab yearly meeting, Utrecht, 14/12/2018 op http://www.cs.ru.nl/B.Jacobs/TALKS/pilab-jacobs-2018-4up.pdf.

18 Rinie van Est, presentatie: 'Freedom in the robot age - The struggle for our intimacy', Jaarcongres Pl.lab, Utrecht 14 December 2018.

19 https://www.rathenau.nl/nl/digitale-samenleving/technologisch-burgerschap-de-democratische-uitdaging-van-de-eenentwintigste

Ethisch ontwerpen

"From my perspective, ethics come before, during and after the law. It informs how laws are drafted, interpreted and revised. It fills the gaps where the law appears to be silent. Ethics is the basis for challenging laws. Remember that slavery was legal. Child labour and censorship are still legal in many jurisdictions. We tackle these injustices on the basis of ethics."
(Butarelli, 2018)[20]

Systemen worden ontwikkeld vanuit ontwerpprincipes, die gelegitimeerd zijn door bovenliggende waarden. In veel gevallen is dit een impliciet of zelfs verborgen proces. Diensten en software worden ontwikkeld met schijnbaar neutrale doelen: 'gemak bieden', 'vraag en aanbod bij elkaar brengen'. Door de ogenschijnlijke neutraliteit wordt dan een kritische reflectie over waarden en maatschappelijke impact vermeden. Als het systeem schaal krijgt en gevolgen maatschappelijk zichtbaar worden, wordt het kritisch gesprek noodgedwongen aangezwengeld door groepen die zich benadeeld voelen. Voor een open, gelijkwaardige dialoog is dat natuurlijk verre van ideaal: posities zijn ingenomen, belangen geschaad en er is altijd een underdog.

Spreken over de waarden en normen die van belang zijn doe je dus vanaf het allereerste ontwerp, tijdens de ontwikkeling en tijdens het gebruik. Wat voor de wet geldt in het citaat hierboven ("ethics come before, during and after the law") geldt niet alleen voor het ontwerp maar ook voor implementatie en technologie. Een goed systeem dwingt gebruikers tot bepaald moreel wenselijk gedrag, bevordert bepaalde gewenste maatschappelijke verhoudingen en bemoeilijkt onwenselijkheden.

Bij aanvang van een project een rijtje mooie woorden op een flip-over zetten en er vervolgens nooit meer op terugkomen heeft natuurlijk weinig betekenis. Elke Identity Provider zal oprecht en met de hand op zijn hart verzekeren dat 'eerlijkheid' aan de grond van zijn ontwerp, bedrijf en persoonlijkheid staat.

Maar: details zijn belangrijk: wat is de use case, de doelgroep, context, implementatie, technologie? Een waardegedreven ontwerp kwalificeert en kwantificeert hoe de waarden en normen op al deze onderdelen zijn vertaald.

Bestaande toetsingskaders en richtlijnen

Er bestaan diverse goede toetsingskaders en richtlijnen die ethical driven design faciliteren en structuur geven. Veel dingen gaan al wél goed. Bij al deze raamwerken geldt: het is nooit een eenduidig of eenmalig afvinklijstje. Het geeft handvatten voor ontwerpers, bouwers, bestuurders en gebruikers om aannames expliciet te maken, te testen en er discussie over te voeren.

Een goed ontwerper stelt de mens integraal en expliciet centraal. Zowel uit oogpunt van veiligheid als inclusiviteit. Dat betekent dat ook het gewenste en het te verwachten gedrag van de mensen in het systeem wordt ontworpen.

- Hoe makkelijk kun je iemand even te hulp schieten?
- En omgekeerd: als je om hulp vraagt, kom je dan in een belastend doolhof van processen tot wederzijdse machtiging, of kijk je even mee op mijn telefoon?
- Begrijp je wat er gebeurt?
- Kun je nog terug?
- Is er ruimte voor 'professional discretion'? Artsen kunnen lichtelijk van de wet afwijken in 't belang van hun patiënt, bijvoorbeeld.

Traditioneel verhoudt de rigide werkelijkheid van wetgeving en overheidsregisters zich moeizaam tot een diffuus, onvoorspelbaar leven van alledag waarin het gaat om kennis, ervaring, contact en elkaar terzijde staan. Kunnen nieuwe systemen ook fysiek, tastbaar, overdraagbaar en tactiel verstaanbaar zijn?

We noemen deze richtlijnen omdat ze zonder uitzondering van toepassing zijn op Digitale Identiteit. De rest van dit wegingskader focust op waarden, ontwerpprincipes en technologie die specifiek en urgent zijn voor digitale identiteit en niet in de bestaande kaders worden genoemd.

20 https://www.privacyconference2018.org/system/files/2018-10/Choose%20Humanity%20speech_0.pdf

- De **BurgerServiceCode** is een gedragscode met tien kwaliteitseisen voor de relatie tussen burger en overheid in de moderne (digitale) samenleving. Deze eisen zijn geformuleerd als rechten van burgers en daarbij behorende plichten van overheden.[21]
- **DigiToegankelijk**: de formele toegankelijkheidseisen en webrichtlijnen die voor overheden verplicht zijn.[22]
- In Amsterdam is een publiek debat gevoerd over publieke waarden in relatie tot de digitale samenleving. Dit heeft geleid tot het manifest **'Tada, duidelijk over data'**, dat inmiddels een plaats heeft gekregen in het coalitieakkoord van het Amsterdams gemeentebestuur: De 6 pilaren van het data-manifest.[23]
- Voor een goede **analyse** van de verhouding tussen (lokaal) bestuur, de rechtsstaat en de borging van publieke waarden in rechten en beginselen (o.m. op basis van de algemene beginselen van behoorlijk bestuur en de 'Code goed openbaar bestuur') zie het essay 'Waardig digitaal overheidsbestuur' van Maaike Kamps.[24]
- **Public Spaces**: een coalitie van Nederlandse publieke organisaties heeft zich in 2018 verenigd om een nieuw digitaal sociaal platform te ontwikkelen. De waarden en principes waar dat platform aan moet gaan voldoen zijn gepubliceerd in een blog van Laurens de Knijff.[25]
- **Cities Coalition for Digital Rights** (Amsterdam, Barcelona, New York): Drie steden verenigden zich rond vijf principes om mensenrechten op het internet te waarborgen. Omdat de stad als democratisch instituut qua schaal het dichtste bij de mensen staat vinden ze dat ze daarin een bijzondere opdracht hebben.[26]
- **De zeven wetten** voor digitale identiteitssystemen van Kim Cameron: Machines moeten stap voor stap het vertrouwen van de mensen winnen (zie ook de bijlage).[27]
- **NL Digibeter**: Agenda voor Digitale Overheid van het Ministerie van Binnenlandse Zaken.[28]

Bijna alles kan stapsgewijs

Door het gebruiken van een of meerdere richtlijnen worden waarden en de operationalisering daarvan in de nieuwe en eigen context actueel en concreet. Het grote voordeel van softwareontwikkeling: klein beginnen, en heel stapsgewijs uitbreiden en opschalen is heel goed mogelijk.

Vertrouwen: relaties of transacties?

Je bent vader, zoon, vriend en collega. In elke context laat je iets anders zien van jezelf. Bovendien verandert je identiteit door tijd en plaats: op vakantie ben je een 'ander mens', je bent niet meer een kind van 8. We schakelen tussen deze fluïde identiteiten op basis van context, relatie en gevoel. Soms gaat het mis, tijdens de karaoke aan het eind van de kerstborrel bijvoorbeeld. De schade is dan te overzien (veel collega's waren al naar huis). En zolang het niet op video staat, kan het materiaal ook niet hergebruikt worden door derden.

21 https://www.digitaleoverheid.nl/document/burgerservicecode/
22 https://www.digitoegankelijk.nl
23 https://tada.city
24 https://waag.org/nl/article/waardig-digitaal-overheidsbestuur
25 https://medium.com/publicspaces/manifesto-f67efae6b622
26 https://citiesfordigitalrights.org/#declaration
27 https://msdn.microsoft.com/en-us/library/ms996456.aspx
28 https://www.digitaleoverheid.nl/nldigibeter/

Vertrouwen baseren we in de gewone wereld vooral op tijdsduur en nabijheid/tegenwoordigheid.[29] Mensen en organisaties die je lang kent, waar je meer ervaring en interactie mee hebt vertrouw je ook meer. Kortom: vertrouwen is gekoppeld aan relaties. Daarnaast gaat vertrouwen per definitie gepaard met kwetsbaarheid en geheimhouding. Bij mensen die je goed kent laat je meer van jezelf zien. En andersom. Een toename van vertrouwen gaat dus hand in hand met een toename van kwetsbaarheid.

In de technische architectuur van identiteitssystemen zijn deze verbanden precies zo aanwezig, zoals blijkt uit deze mooie technische definitie van vertrouwen:[30]

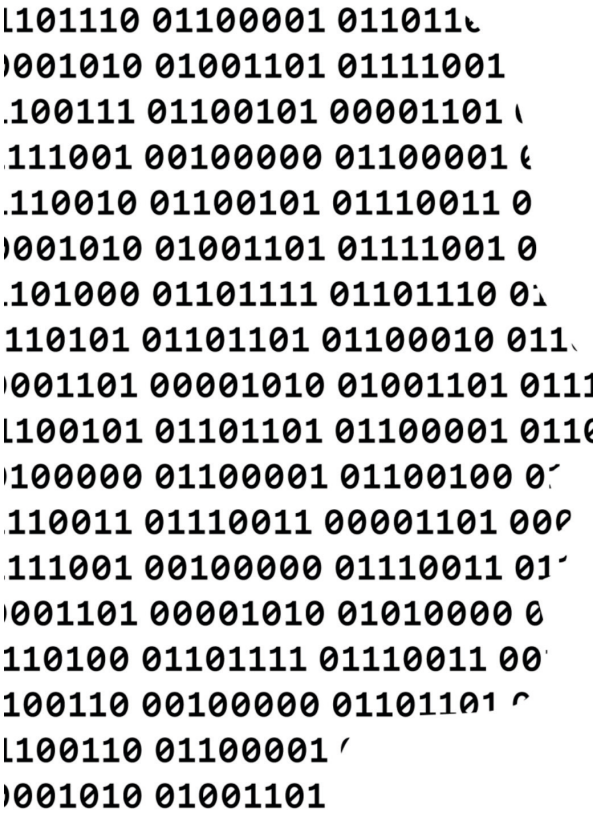
"When an actor trusts another actor, he or she is willing to assume an open and vulnerable position. He or she expects the other to refrain from opportunistic behaviour even if there is the possibility to show this behaviour. In more technical terms, entity A trusts entity B if B can break the security or privacy policy of A without A's cooperation or knowledge."

Maar online zijn we onze veiligheidskleppen kwijt. Contexten lopen makkelijk en ongemerkt door elkaar, 'op je gevoel' werken heeft geen betekenis en relaties ook niet. In de digitale wereld is de bandbreedte voor communicatie veel smaller en tijd is er nauwelijks. Noodgedwongen reduceren machines onze identiteit tot een set transacties. We kunnen niet langer 'spelen' met onze identiteit. Als we online eenmaal écht vertrouwen hebben, heeft dat even makkelijk exponentiële consequenties:

"Familiarity on WhatsApp breeds trust, which most of the time is a pretty great social good. But in fast-moving situations with high stakes — natural disasters, wars, terrorist attacks or elections — trust on WhatsApp is turned on its head, becoming a key force behind viral falsity" *(Farhad Manjoo, NY Times)*[31]**.**

Echt, persoonlijk en nabij vertrouwen dat in de tijd is opgebouwd kan op een digitaal platform in 1 stap en 1 milliseconde verworden tot een verontrustend gerucht. Dat ik jou echt en blindelings vertrouw, wil niet zeggen dat wat jij zegt en ik vervolgens doorstuur ook waar is. Waar we offline bij het doorvertellen van anekdotes nuances toevoegen (of nieuwe feiten verzinnen), is online elk filter verdwenen.

Vertrouwen werkt online dus anders dan offline.



29 Caroline Nevejan, 'Presence and the Design of Trust', http://www.nevejan.org/presence/
30 https://arxiv.org/pdf/1101.0427.pdf
31 https://www.nytimes.com/2018/10/24/technology/fixing-whatsapp-disinformation-human-nature.html

Nieuwe technologie voor digitale identiteit

In reactie op de genoemde maatschappelijke en operationele problemen zijn er diverse initiatieven die nieuwe oplossingen presenteren voor digitale identiteit en het delen van persoonlijke data. Een aantal van deze initiatieven hebben we in het Digitale Identiteitslab nader bekeken, onder meer in de design sprints en in expertgesprekken. Het gaat om:

Forus	forus.io[32]
IRMA	privacybydesign.foundation/irma[33]
It's Me	itsme.be[34]
Decode	decodeproject.eu[35]
Trustchain	tudelft.nl/technology-transfer[36]

Zoals te verwachten bij nieuwe technologie zijn er onderling verschillen in technologische en functionele rijpheid. Alle ontwerpteams waren beschikbaar voor vragen en uitleg maar de mate waarin bijvoorbeeld ontwerpkeuzes en broncode expliciet open en toegankelijk zijn verschilt. Op basis van de pilots, documentatie en gesprekken noemen we hier de interessantste punten die uit dit materiaal naar voren kwam.

Definities: een aantal hier gebruikte termen zijn in de bijlage kort gedefinieerd.

Zorg: balans tussen gemak, zorgplicht en autonomie

Voor een veel te groot deel van de Nederlandse bevolking is DigiD nu te complex. Er is een grote behoefte aan diensten, applicaties en technologie die toegankelijk en begrijpelijk zijn. Tegelijkertijd is technologie ingewikkeld en vereist autonomie een zeker begrip en handelingsperspectief. Alle experts van de oplossingen die wij spraken zijn bezorgd over het spanningsveld dat dit oplevert.

De grens tussen overheid en niet-overheid is vanuit het gezichtspunt van een dienstverlener vaak glashelder. Voor gebruikers en andere betrokkenen is dat praktisch bijna nooit zo.

Dataminimalisatie door attributen

Digitale identificatie moet niet plaatsvinden door zoveel mogelijk data te verzamelen, maar door aan gebruikers zo min mogelijk data te vragen. Soms is er niet meer nodig dan 'deze persoon is ouder dan 18'. De data die gevraagd wordt moet dan wel betrouwbaar zijn. Dit kan door het het toepassen van 'Attribute Based Credentials' (ABC). Bijkomend voordeel is dat data eenvoudig tussen contexten gedeeld kunnen worden (bijvoorbeeld een inkomen delen met een woningcorporatie). Alle oplossingen die we in het lab zagen gebruiken een vorm van ABC (al kan bij de oplossingen met gesloten broncode niet gezien worden wat men daar precies onder verstaat).

Decentralisatie

Om verantwoordelijkheid en risico te spreiden worden verschillende vormen van decentralisatie voorgesteld. Bijvoorbeeld door de cruciale data op hardware van de gebruikers op te slaan. Op die manier heeft de gebruiker niet alleen juridisch maar ook technisch zoveel mogelijk controle. Daarnaast kan in de architectuur voorkomen worden dat er een makelaar of broker nodig is voor een transactie. In een decentraal systeem is een derde partij niet nodig, dus kan er daar ook geen profiel worden opgebouwd van gedrag of metadata.

Conceptueel zou ook het hele ecosysteem van digitale identiteit decentraal worden georganiseerd (DECODE en diverse Self Sovereign Identity initiatieven).

Voorkom surveillance

Door het systeem zo te bouwen dat geen van de daarin betrokken partijen ongewenst het gebruik van de andere partijen in het systeem in kaart kunnen brengen wordt een surveillancemodel voorkomen.

32 https://forus.io
33 https://privacybydesign.foundation/irma/
34 https://www.itsme.be
35 https://www.decodeproject.eu
36 https://www.tudelft.nl/technology-transfer/

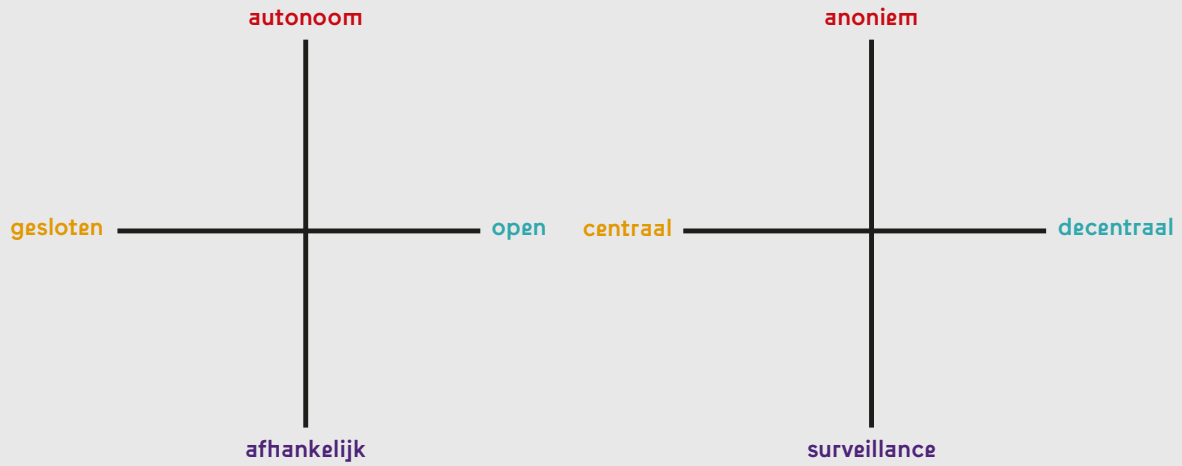
Bijvoorbeeld door *credentials* blind te ondertekenen. Dan kan een uitgever na uitgifte van een credential niet nagaan waar dit credential allemaal gebruikt wordt, zelfs niet als de uitgever samenspant met alle controleurs. Dit heet *issuer unlinkability*.

Er is regie nodig

De wens om meer en diverse spelers een rol te laten spelen in digitale identiteit en het infrastructurele maatschappelijke belang van digitale identiteit maken dat veel sprekers vragen om een andere rol van de overheid. Die beperkt zich tot nu tot teveel tot het uitzetten van aanbestedingen (voor eigen diensten) en het van afstand toezien op de markt. Maar de marktverhoudingen zijn nogal in het nadeel van partijen die juist maatschappelijk van belang kunnen zijn.

Kaartjes gebruikt tijdens de interviews

Wegingskader digitale identiteit



Op basis van de uitkomsten van het Digitale identiteitslab en wat we daarin verzameld hebben over technologie en uitgangspunten presenteren we hier vijf ontwerpprincipes voor digitale identiteit.

Elk principe is geordend langs een as, voorzien van een aantal uitgangspunten of vragen. Deze kunnen helpen om te bepalen waar een dienst of applicatie zich op deze as bevindt.

Vragen kunnen gesteld worden vanuit het perspectief van verschillende betrokkenen.
De burger/eerstelijns gebruiker die een dienst van de overheid wil gebruiken; de applicatiebeheerder bij gemeente of andere instelling; en vanuit een algemeen maatschappelijk oogpunt over de infrastructuur.

Twee kaders zijn maatschappelijk, twee technisch georiënteerd. De vijfde is overkoepelend. De eerste vier kaders vormen samen twee kwadranten, waarin antwoorden verzameld kunnen worden. Het is zo een instrument waarmee dilemma's bij gesprekken over digitale identiteit inzichtelijk gemaakt kunnen worden.

Aanpasbaarheid/flexibiliteit technologie en infrastructuur

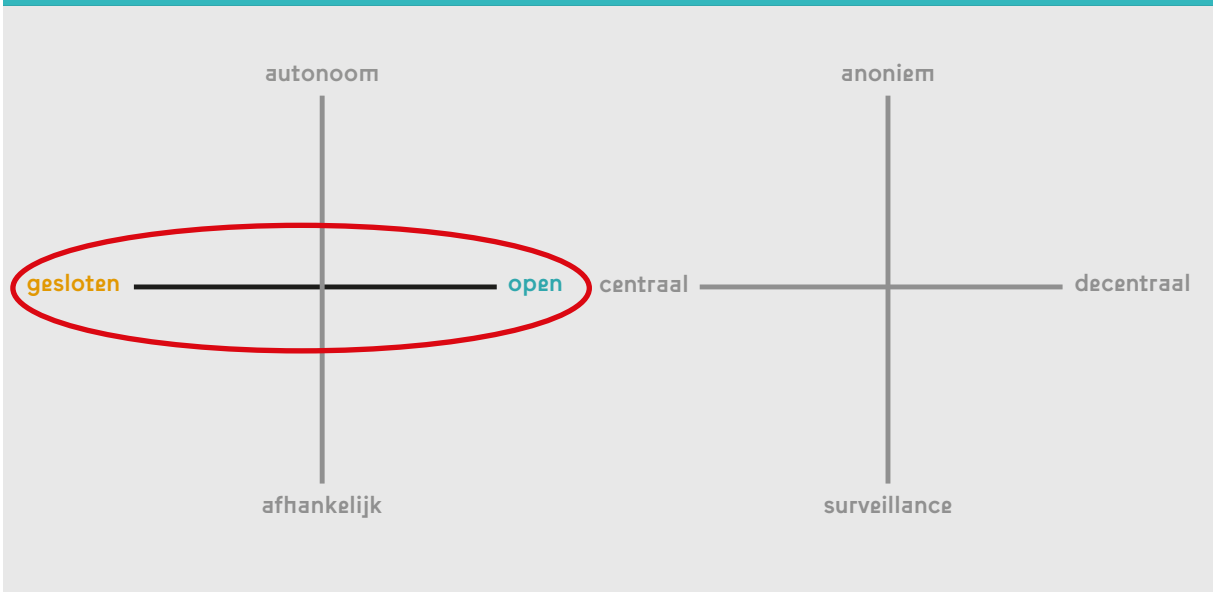
Een aandachtspunt bij de afweging is nog het volgende. Als overheid, dienstverlener of burger wil je zo vrij mogelijk zijn om op deze ontwerpprincipes een positie te kiezen. Want wat gepast en nodig is, is heel erg contextafhankelijk: minderjarigen hebben meer bescherming en zorg nodig, terwijl financiële of medische transacties een heel andere insteek vereisen. In het ontwerpen van een applicatie, user-interface en eventuele bijbehorende hardware voor de gebruiker zijn die overwegingen goed mee te nemen, maar de onderliggende, complexe en kostbare technologie en infrastructuur is véél minder flexibel.

Privacy by Design vereist daarom maximale aandacht voor anonimiteit en pseudonimiteit in de ontwerpfase van deze infrastructuur. Achteraf op onderdelen functionaliteit toevoegen (zoals bijvoorbeeld features voor criminaliteitsbestrijding) is gemakkelijker dan het omgekeerde; het is vrijwel onmogelijk een systeem privacy-vriendelijk maken dat by design elke transactie vastlegt, bijvoorbeeld. Als op élke straathoek in de stad vier camera's de windrichtingen filmen, kun je niet meer anoniem over straat. Als er nérgens camera's hangen, kun je altijd nog apparatuur plaatsen waar het écht nodig is.

Voor het ontwerp van de onderliggende governance, technologie en infrastructuur voor digitale identiteit moet dus gewerkt worden met technologie en infrastructuur die zoveel mogelijk autonomie garandeert, terwijl in de applicatielaag toepassingen kunnen worden aangeboden die deze autonomie beperken waar dit vanwege zorgplicht, fraudebestrijding of dienstverlening nodig is. Weergegeven op de as tussen surveillance en anoniem is achteraf maatwerk en aanpassing van boven naar beneden veel eenvoudiger. De beweging van omlaag naar omhoog is vrijwel onmogelijk:

Hierna lichten we de vijf principes stuk voor stuk toe.

1. Van transparantie naar dialoog



"As commodity technology starts to really drive the evolution of our daily lives and more of our personal data, our industry and our economy is on the internet, we will repeatedly run into challenges of how to explain complex and subtle technical concepts to non-experts. That's likely to cover everything from how the internet economy could affect personal privacy through how the mass of data our smart stuff will be generating affects national security to how agencies charged with public protection can do their job in a way that meets the public's expectation. To do that, we need to have open and honest conversations between experts that can inform the public debate about what's right and we'll need a framework in which to do that."
(Ian Levy, Crispin Robinson (GCHQ) in een essay over cryptografie en veiligheid)[37]

Gesloten

- 'Lege stoel' & black box
- Proprietary code
- Ver weg, niet bereikbaar
- Gesloten code, organisatie, verdienmodel
- Ongelijke informatiepositie
- Gesprek niet mogelijk of niet zinvol
- Beroep niet mogelijk of niet zinvol

Open

- Open code, organisatie
- Transparant verdienmodel
- Gesprek zinvol
- Gelijkwaardige dialoog
- Beroep mogelijk en zinvol

Veel online diensten zoals Software-as-a Service werken op basis van Continuous Integration (CI): meerdere mensen kunnen tegelijkertijd werken aan dezelfde codebase en veranderingen kunnen vrijwel direct online gezet worden naar test- en productieomgevingen. De codebase is dan voortdurend in ontwikkeling.

37 https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate

Parallel daaraan is bij de ontwikkeling van maatschappelijke fundamentele software 'Conversational Integration' nodig: een voortdurend gesprek over ethiek, functionaliteit en technologie. Een gesprek vereist dat diensten, applicaties en hun aanbieders aan een aantal eenvoudige maar fundamentele eisen voldoen.

Wat is daarvoor nodig?

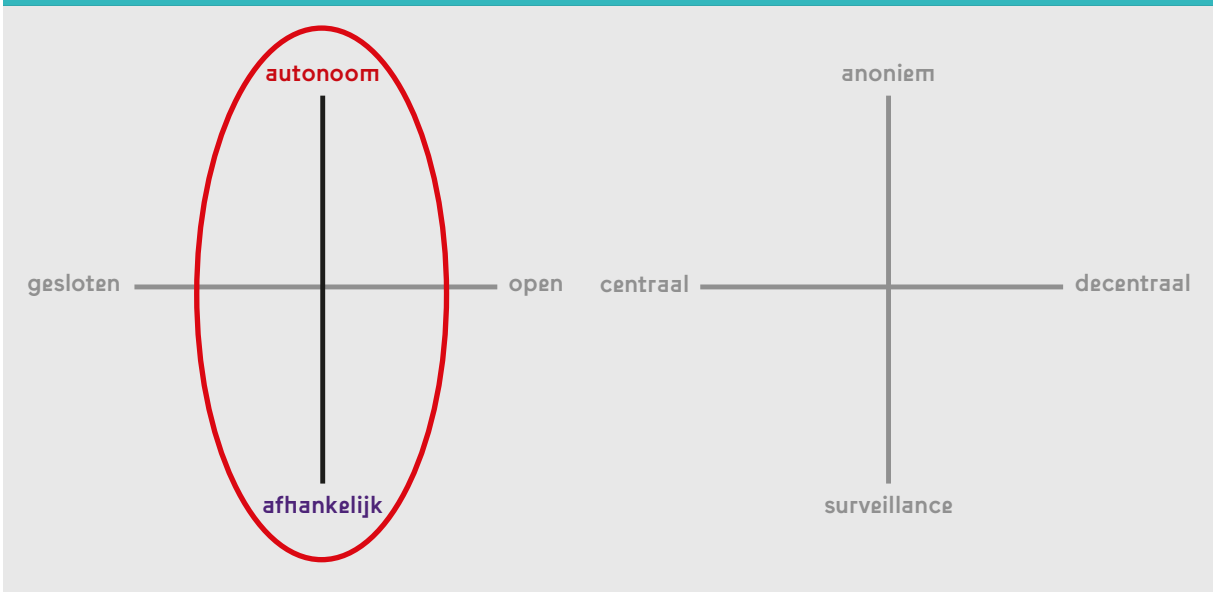
- Ontwerpers, beheerders en bestuurders zijn voor dit gesprek beschikbaar, bereikbaar en nabij (zie ook de empty chair[38]).
- Zij maken hun ethische, functionele en technische keuzes expliciet en geven aan hoe stakeholders in de maatschappij invloed kunnen hebben op hun ontwerpstrategieën.
- Dienstverleners zijn specifiek over de data die zij nodig hebben en vragen niet meer dan strikt noodzakelijk.
- Gebruikers moeten kunnen inzien en beoordelen of partijen gerechtvaardigd zijn de data op te vragen en dit ook redelijkerwijs nodig hebben.
- Ontwikkelproces, ontwerpen, informatiearchitectuur, algoritmen, documentatie en codebases zijn beschikbaar onder open licenties. Zij worden actief en kwalitatief beheerd. Zo vertrouwen we zo min mogelijk op toezeggingen en beweringen.
- Iedere burger kan vrij toe- en uittreden tot dit gesprek en heeft recht van spreken.
- In uitzonderlijke gevallen (bestaande overeenkomsten/licenties, verdragen/wetgeving, migratietrajecten) kan er sprake zijn van proprietary technologie en gesloten broncode. Dit is uit oogpunt van vertrouwen en veiligheid nadelig, omdat die dan uitsluitend gebaseerd is op audits van controlerende instanties.

Voorbeelden van openheid van ethiek, functionaliteit en technologie:

- Altijd hulp kunnen vragen of suggesties kunnen doen bij een balie in de buurt (functionaliteit, zie ook regel 1 van de BurgerServiceCode).
- Aanmelden voor een bijeenkomst over inclusiviteit van digitale identiteit (ethiek).
- Het zelf kunnen lezen van de broncode en er op een meetup over discussiëren (technologie).

38 De beroemde foto bij dit artikel https://www.politico.eu/article/facebook-privacy-mark-zuckerberg-facebook-britain-hearing-fake-news-damian-collins-misinformation-london/

2. Vergroot het begrip



"... dan ben je in een winkel geweest, en dan krijg je een appje "hoe vond je de winkel? hoe vond u de klantenservice?" en toen dacht ik: hè, hoe weten ze dat nou?"
(Interview tijdens het lab).

Autonoom

- UI/UX verduidelijkt rechten
- Controle expliciet
- Technologisch burgerschap
- Vrijheid (en zelfredzaamheid)

Afhankelijk

- Uit handen nemen
- UI/UX verdwijnt: 'magische interactie'
- Gezichtsherkenning op afstand
- Ontzorgen
- Ontlasten
- Manipulatie

Deze as vertegenwoordigt een klassiek ontwerpdilemma: streven naar gemak en toegankelijkheid kan betrokken, kritisch gebruik ontmoedigen. Terwijl begrip, reflectie en betrokkenheid voor gebruikers juist gereedschappen zijn om handelingsperspectief te vergroten, te doorzien wat er misgaat en zelf in te grijpen. Magische, verborgen processen voor digitale identiteit leiden tot onbegrip en misverstand op het moment dat zaken niet werken zoals verwacht.

Het is beter als de user-interface en -experience van applicaties gebruikers uitnodigt zich te realiseren en verdiepen in wat er gebeurt. Het stimuleert 'technologisch burgerschap' - in het algemeen en vooral bij politici, bestuurders en ambtenaren. Een 'technologisch burger' is geïnformeerd over de werking van technologie, kan kritisch reflecteren over die werking en de betekenis daarvan voor zijn leefwereld, en kan op basis daarvan kiezen welke technologie hij wel of niet kan of wil gebruiken.

In het ontwerp van applicaties en diensten moet in user-journey, -interactie en -experience over dit dilemma worden nagedacht. Door een ondersteunende omgeving te bieden kan de individuele en collectieve capaciteit tot autonomie worden vergroot. Bescherming moet geboden worden tegen misverstanden en misbruik.

Een voorbeeld biedt het ontwerp voor een interface voor het toepassen van een smart-rule bij het delen van data:

Interface voor het toepassen van een smart-rule bij het delen van data (concept uit project Decode).
Vragen die op deze as spelen zijn:

Autonomie faciliteren

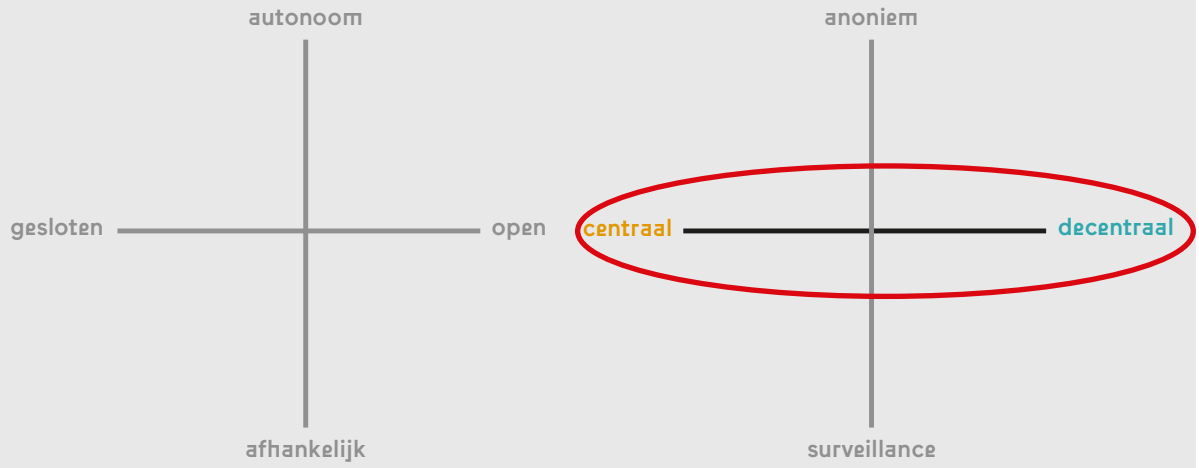
- Hoe kunnen momenten van keuze en controle aan de gebruiker worden gecommuniceerd?
- Waar en op welk moment staat een gebruiker hiervoor open?
- Hoe kun je gebruikers helpen glashelder onderscheid te maken tussen contexten, zodat er niet per ongeluk data uit verkeerde context wordt gedeeld? Ontwikkel een model van het aantal nog werkbare (of: benodigde) aantal identiteiten. Bijvoorbeeld over meerdere applicaties, of meerdere applicatie-contexten.
- Kunnen er ook verrassende, speelse of artistieke vormen ontwikkeld worden? Inspiratie bieden concepten zoals Erratic appliances[39] (huishoudelijke apparaten gaan zich onvoorspelbaar/onhandig gedragen als energiegebruik te hoog is) of Adversarial Design[40] (waarbij het politiek perspectief expliciet wordt gemaakt in het ontwerp naar voren komen).

Risico's beperken

- Een soepel, betrouwbaar systeem voor digitale identiteit introduceert een risico op 'overidentificatie': waardoor je overal en nergens met geverifieerde informatie moet inloggen, en partijen dit kunnen gebruiken om een real-name-policy[41] af te dwingen.
- Kun je mogelijkheden bieden om, bijvoorbeeld in verschillende veiligheidsniveaus, een advies (aan de gebruiker/burger) of verplichting (aan alle partijen) om (in verbinding met het protocol) te beperken in welke contexten welke credentials mogen worden gebruikt. (bijv: een lijst BSN-verwerkers, beheerd door een aparte identiteit, opgenomen in de schemadefinitie)?
- Kun je een beleid opstellen en handhaven op acceptanten van het middel: standaard om alle aanwezige credentials vragen zou niet mogen kunnen. Het hanteren van dataminimalisatie dient afgedwongen te kunnen worden.
- Complexe transacties die meerdere credentials vergen: hoe houd je die overzichtelijk? De UI zou automatisch moeten bepalen welke minimale set aan credentials nodig is, en die voorleggen aan de gebruiker.

39 http://dru.tii.se/static/erratic.htm
40 https://en.wikipedia.org/wiki/Adversarial_Design
41 https://en.wikipedia.org/wiki/Facebook_real-name_policy_controversy

3. Spreid verantwoordelijkheid & risico



Centraal

- Eén dienst voor alle gevallen
- Data Lake
- 'ID-provider' is essentiële stap
- Broker/centrale hub

Decentraal

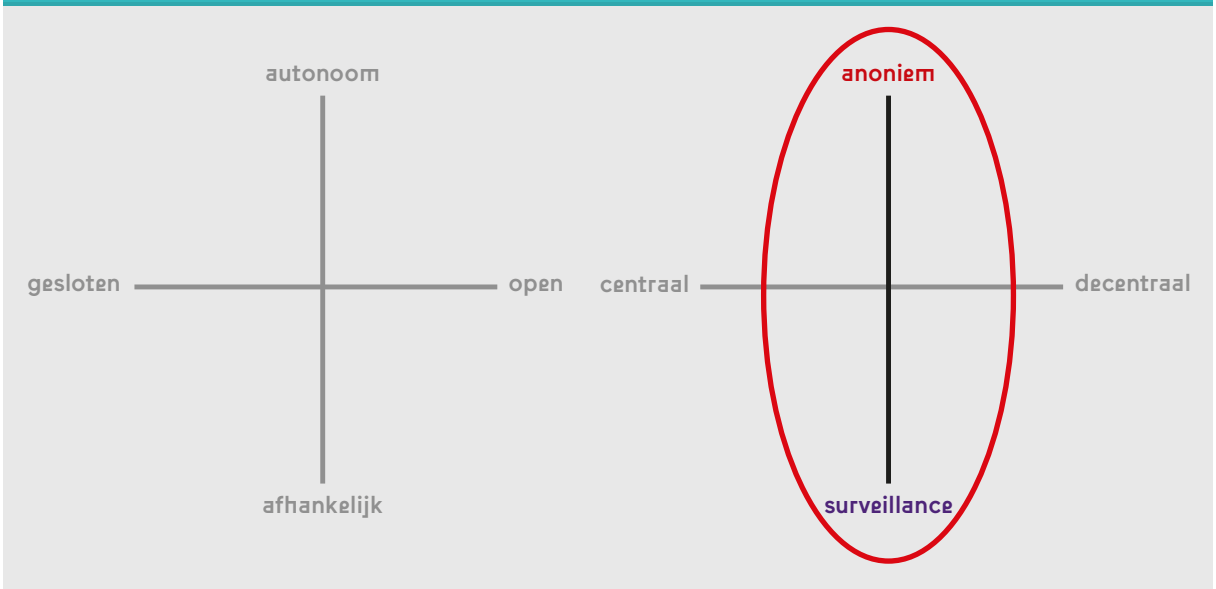
- Meerdere aanbieders
- Federatieve opzet
- Gebruiker is essentiële stap
- Gescheiden verstrekken en gebruiken
- Data verspreid / bij bron

Spreid en beperk zowel de verantwoordelijkheid als het risico door Digitale Identiteit technisch, juridisch en bestuurlijk decentraal te organiseren.

Wat is daarvoor nodig?

- Decentraliseer het opslaan en controleren van data. Technisch op hardware van gebruikers. Op die manier heeft de gebruiker niet alleen juridisch maar ook technisch zoveel mogelijk controle.
- Een decentrale architectuur waarbij er geen makelaar of broker nodig is voor een transactie.
- De gebruiker controleert het delen van gegevens. Dit wordt technisch afgedwongen doordat een credential niet zonder private key herbruikbaar is.
- Geen enkele uitgever of controleur kan zich voordoen als een van haar gebruikers.
- Technische systemen mogen nooit informatie vrij kunnen geven zonder toestemming van de gebruiker.
- De gebruiker is zelf altijd een essentieel onderdeel van de stap die toegang verleent.
- Het verstrekken van attributen/credentials is juridisch en technisch hard gescheiden van het gebruik van attributen/credentials.
- Technisch en qua governance kunnen alle rollen in het systeem door meerdere, juridisch en technisch gescheiden partijen worden vervuld.
- Public/private key encryption wordt state-of-the-art geïmplementeerd. Private-keys zijn altijd verspreid over meer dan 1 fysiek apparaat, zodat een aanvaller met alleen toegang tot dit ene apparaat nooit de sleutel daaraan kan onttrekken (voorbeelden zijn een yubi-key, IRMA key-sharing server).

4. Niet traceerbaar voor derden



"De digitale soevereiniteit van burgers omvat het recht zelf te besluiten in welke relatie je wat van jezelf prijsgeeft." *(Marleen Stikker)*

Anoniem

- Alleen traceren waar zorgplicht, fraude-bestrijding of dienstverlening dit vereist
- Pseudonieme attributen
- non-linkability
- Altijd mogelijk een niet identificerend/ gepseudonimiseerd attribuut te delen.
- Uitgevers van attributen kunnen technisch/ operationeel beperkingen stellen aan het hergebruik (Het BSN-nummer kan alleen opgevraagd door overheids-partijen).

Surveillance

- Alle transacties en activiteit gelogd
- Identificerende attributen verplicht
- Transactie onmogelijk zonder 3e partij

Uit oogpunt van dataminimalisatie bestaat digitale identiteit uitsluitend op basis van (combinaties van) eigenschappen d.m.v. Attribute Based Credentials[42]. Een transactie vindt plaats tussen twee partijen. Het gebruik van deze attributen/credentials is technisch nooit traceerbaar door een derde partij. Een 'derde partij' wil hier zeggen: elke partij die feitelijk geen cruciale rol speelt in de transactie. Bij sommige transactie is er sprake van een legitieme derde partij (bij het kopen van een huis: notaris, hypotheekverstrekker).

Traceren is ook onmogelijk als uitgever (issuer) en controleur (verifier) samenspannen, of bij herhaald gebruik van de credential in sessies bij dezelfde controleur (non-/unlinkability). Bijvoorbeeld door credentials blind te ondertekenen: de uitgever krijgt dan de uiteindelijke vorm van de credential niet te zien. Die is alleen bij de gebruiker bekend.

42 https://privacypatterns.org/patterns/attribute-based-credentials

Dus met anoniem bedoelen we hier niet dat de deelnemers aan een transactie anoniem zijn, maar dat het voor derden die geen onderdeel zijn van de transactie niet mogelijk is om mee te kijken naar of in de transacties, zelfs niet op het niveau van metadata.

De beslissing om toegang te geven of toestemming te verlenen wordt niet gemaakt op basis van een identifier (naam, BSN, telefoonnummer), maar op basis van kennis van de privésleutel die hoort bij het account waar toegang toe gevraagd wordt (een identifier is altijd bekend bij meer dan 1 persoon en dus te achterhalen). Waar nodig kan een credential identificerende attributen bevatten.

Omdat er niet getraceerd kan worden, kan nergens een profiel ontstaan op basis van gegevens die niet voor een partij bestemd is. Partijen krijgen uitsluitend de data die zij nodig hebben. Data die nodig is om de transactie te valideren maar inhoudelijk niet nodig is voor de andere partij wordt versleuteld als Zero Knowledge Proof gedeeld.

Om phishing te voorkomen moeten partijen zich altijd naar de gebruiker identificeren (mutual authentication).

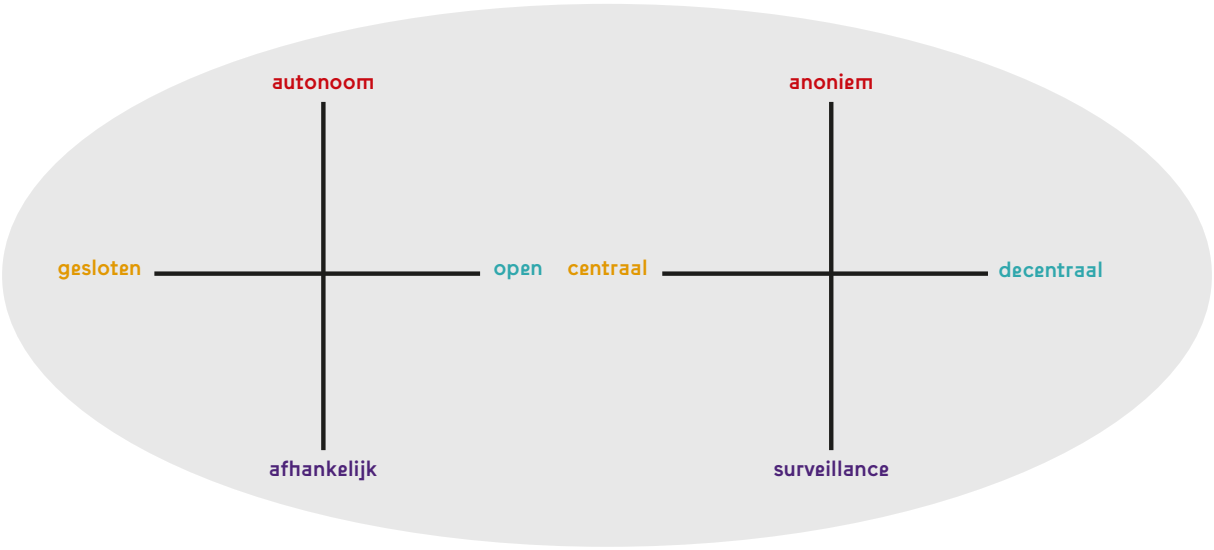
De uitgever (issuer) van een credential kan een credential technisch functioneel intrekken (dus aangeven dat een eerder uitgegeven credential niet langer als geldig moet worden beschouwd). Bijvoorbeeld door de ongeldigheid daarvan te publiceren of de automatische verlenging ervan stop te zetten, zonder dat andere eisen in het geding komen.

Uitgevers en controleurs kunnen een wettelijke, maatschappelijke of morele plicht hebben om transacties te volgen. Denk aan zorgplicht, fraudebestrijding of aansprakelijkheid. In die gevallen moet tracering als maatwerk mogelijk zijn.

Voor het verbeteren van dienstverlening kunnen sessies worden georganiseerd waarbij onderzoekers (fysiek, dus expliciet aanwezig) met gebruikers meekijken, om zo dienstverlening te verbeteren.

5. Regie en democratische controle

Regie en democratische controle

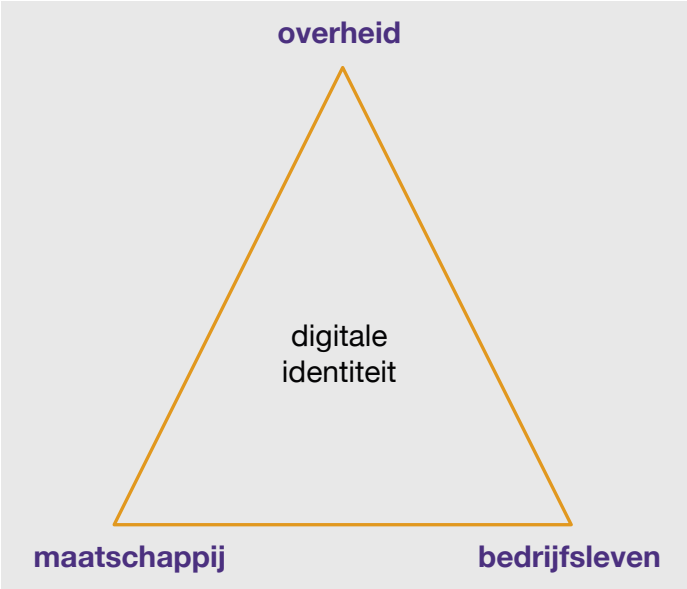


"The first element of trust is correct legal space. Which makes sure what are the rights of everybody using the system." *(Kersti Kaljulaid, Estland)*[43]

Als er een gemeentehuis is, moet er natuurlijk ook een weg zijn náár het gemeentehuis. Die weg moet duurzaam en veilig zijn en kostenefficiënt worden aangelegd. Maar in het denken over mobiliteit en infrastructuur staat dit operationele detail natuurlijk niet centraal. Op strategisch niveau ontwikkelen belanghebbenden en beleidsmakers een samenhangend beleid. Collectieve belangen van bedrijfsleven, automobilisten, fietsers, milieubeweging worden vertegenwoordigd en er zijn processen en instituties die voertuigen en chauffeurs toetsen en toelaten. Pas als het ambtelijk en democratisch proces voltooid is, kan er een aanbestedingsprocedure volgen. Of kan een fabrikant zijn goedgekeurde auto aanbieden. Het ontwikkelen en gebruiken van infrastructuur is gevat in wetten, regels en verkeerslessen voor jonge fietsers.

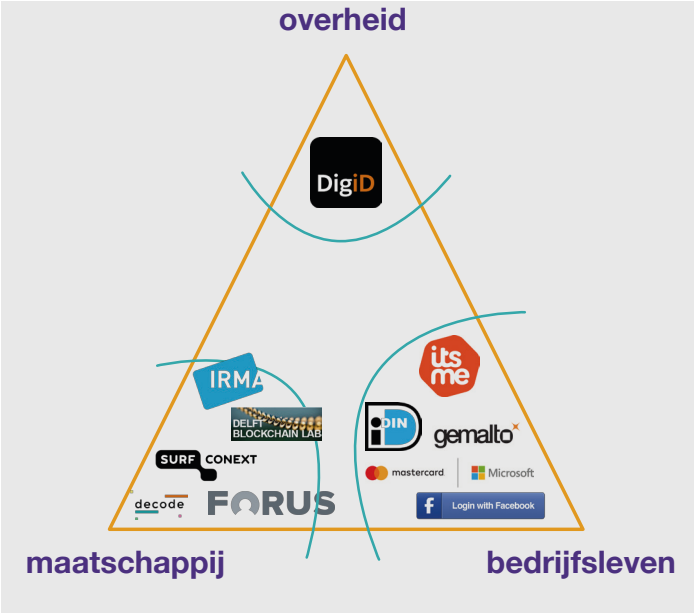
In het domein van verkeer en infrastructuur stelt de overheid juridische kaders, heeft de regie en biedt democratische controle. Daardoor kunnen burgers, bedrijven, stichtingen en belangenverenigingen elk zowel een rol spelen op strategisch als operationeel niveau. Een mobiliteitsstrategie voor 2030 heeft een ander proces dan een aanbestedingsprocedure voor het onderhoud van een rotonde.

43 In: https://www.vpro.nl/programmas/tegenlicht/kijk/afleveringen/2018-2019/verovering-van-ons-dna.html

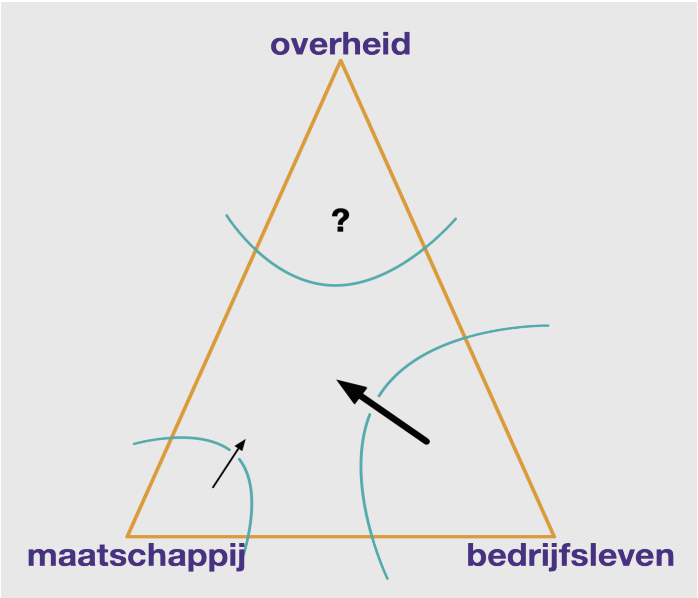


Als we op strategisch niveau naar digitale identiteit kijken zien we dat het een domein is waar belangen van overheid, bedrijfsleven en maatschappij samenkomen. Tussen deze belangen bestaat er zowel synergie als conflict en over de dilemma's die dit oplevert moeten afwegingen worden gemaakt. In een model kunnen we de ruimte van dit domein weergeven:

De belangen van overheid en bedrijfsleven zijn gevestigd en worden goed gearticuleerd. Maar belangen, ideeën en oplossingen die uit de maatschappij als geheel komen hebben geen vanzelfsprekende plaats. Het domein digitale identiteit wordt in rap tempo ingenomen door het bedrijfsleven, weergegeven in het model:



De overheid koopt digitale diensten in voor zichzelf, maar onttrekt zich aan het hebben van een visie, beleid of regie op de maatschappelijke functie van digitale identiteit. Er worden alleen op operationeel niveau diensten afgenomen. Op strategisch niveau wacht de overheid af. Met andere woorden: er wordt wel een weg aangelegd, maar alléén naar het gemeentehuis.



Digitale identiteit is complex en fundamenteel voor het maatschappelijk functioneren. We zien dat vanuit haar opdracht en machtspositie de overheid hierin een sterke en beslissende stem heeft. Ook marktpartijen zijn online en in het gesprek duidelijk aanwezig. Voor belangen, wensen en alternatieven die vanuit publieke context worden ontwikkeld is, zeker in formele zin, geen tot weinig plaats. Denk aan universitaire initiatieven als IRMA, Trustchain en Conext, de identiteitsservice van Surfnet. Beleid staat of valt met implementatie en dat vereist strategische en operationele controle. Het is daarom onwaarschijnlijk dat de overheid regie en democratische controle op deze publieke ruimte kan uitoefenen met alleen een aanbesteding voor een 'veilig inlogmiddel'. Het aantonen van een toegangsrecht gebeurt niet af en toe, maar voortdurend. Omdat dit proces bepaalt wie op welke manier economische, democratische en sociale mogelijkheden kan benutten, is Digitale Identiteit te beschouwen als een nutsvoorziening. De overheid en maatschappij hebben de taak belang en impact van infrastructuur te begrijpen en een working model te hebben waarmee zij op de werking kunnen reflecteren.

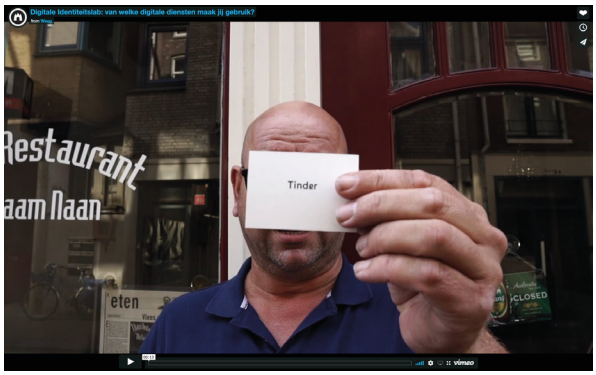
Een van de meest wezenlijke kenmerken van digitale identiteit is dat gebruikers in milliseconden veranderen van rol, functie, verantwoordelijkheid of vertegenwoordiging. Organisatorische of juridische verkokering speelt per definitie geen vanzelfsprekende rol meer. Dat stelt hoge eisen aan alle onderdelen van het systeem. De vele contexten en gelaagdheid waarin digitale identiteit een rol speelt maakt het onmogelijk één, allesomvattende oplossing te ontwerpen. De eisen tussen contexten zijn onderling vaak tegenstrijdig. Naast verschillende aanbieders zullen er deels ook verschillende systemen nodig zijn om tegenstrijdige features te kunnen leveren.

Politiek en bestuur zullen het voortouw moeten nemen in het vormen van democratisch gelegitimeerde controle en regie op deze nieuwe publieke ruimte. Zij kan daarbij het ontstaan van een maatschappelijke middenveld faciliteren, waarbij stakeholders zich rond belangen en functies kunnen verenigingen.

Bij het Digitale Identiteitslab waren op alle momenten veel en diverse partijen aanwezig die hier een rol willen en kunnen spelen.

Digitale Identiteit: de video's

Op de website en het videokanaal[44] van het Digitale Identiteitslab verzamelden we alle video's, die mede als input dienden voor het wegingskader.



44 https://vimeo.com/channels/digitaleidentiteit

Definities

Attribuut (eigenschap)
Een afzonderlijke eigenschap die iets zegt over een ding of persoon. Attributen voor geboortedatum, leeftijd of een leeftijdscategorie zeggen allemaal iets over je leeftijd maar de eerste geeft veel meer kwetsbare persoonlijke data vrij dan de laatste.

Attribute Based Credential
Attribute Based Credentials (ABC) zijn een vorm van credentials die het mogelijk maakt om zonder aanvullende informatie over iemand te onthullen (zero-knowledge eigenschap) een recht of kenmerk betrouwbaar aan te tonen. Bijvoorbeeld aantonen 'ik ben ouder dan 18', zonder dat mijn geboortedatum ook getoond wordt.

Credential
Een of meer attributen (eigenschappen) die als digitale set, digitaal ondertekend zijn. Bijvoorbeeld: Een door de RDW digitaal ondertekende verklaring dat de eigenaar van de credential rijvaardig is voor rijbewijs B en jonger is dan 70 jaar.

Controleur (verifier)
Instelling, bedrijf of mede-burger die van een gebruiker een credential vraagt, ontvangt, en de geldigheid verifieert.

Gebruiker (user)
Burger die persoonlijke gegevens die op hem/haarzelf betrekking hebben via een digitaal systeem wil of moet delen. Of dit als gemachtigde voor iemand anders wil moet doen.

(Digitale) identiteit
De volgende definities kwamen we tegen:

Van Dale: iden·ti·teit (de; v)
1 gelijkheid: je identiteit bewijzen, bewijzen dat je de persoon bent voor wie je je uitgeeft
2 eigen karakter

NRC Handelsblad[45]: Een online paspoort om te bewijzen wie we zijn.

RVIG[46]: DigiD staat voor digitale identiteit en wordt gebruikt om in te loggen bij websites van de overheid en instellingen.

VNG[47]: inloggen bij een bank, een telefoonprovider, bol.com, de Sociale Verzekeringsbank of bij een gemeente.

Tom Demeyer (CTO, Waag): De digitale identiteit van een persoon wordt gevormd door de digitaal gefaciliteerde relaties, expressies en transacties van die persoon. Vaak zijn deze direct gerelateerd aan de fysieke persoon zelf, maar hij bestaat ook als puur digitale entiteit. Een overleden persoon bestaat wellicht alleen nog digitaal, maar digitaal en fysiek kan ook helemaal samenvallen. In de relatie tussen fysieke en digitale wereld is elke gradatie mogelijk.

Data over een persoon kan gezien worden als de administratie van zijn relaties en handelen aan de éne kant, en als een administratie óver zijn relaties en zijn handelen aan de andere kant.

In de relatie met de overheid wordt deze administratie meestal gevoerd vanuit een juridisch mandaat (BSN, rijbewijs, strafblad); daarnaast zijn er zorgrelaties (medisch dossier), transacties (koopgedrag, museumbezoek, gaming, datingsites), expressieve uitingen op social media. Verder zijn er natuurlijk partijen die via aggregatie van deze bronnen weer nieuwe data genereren over een persoon.

Al deze data vormen tezamen een machine-readable versie van die persoon, en zijn een hanteerbare representatie van haar digitale identiteit.

Edwin Schuijt: De digitale identiteit van personen wordt vormgegeven door:[48]
- alle (digitale) gegevens die ons beschikbaar worden gesteld (BSN, IBAN),
- gegevens die we zelf beschikbaar stellen (koopgedrag, social media gebruik, gaming, dating)
- en gegevens die door systemen worden gemaakt (trackers, patroonherkenning, gedragsvoorspelling).

45 https://www.nrc.nl/nieuws/2018/10/04/iedereen-een-identiteits-app-of-twee-a2150911

46 https://www.rvig.nl/digitale-identiteit
47 https://vng.nl/samen-organiseren/digitale-identiteit
48 N.a.v meetup 'designing personal data' sept. 2017

Straatinterviews:[49]

- Poeh, moeilijk. ehh?
- Dat is de identiteit waarmee ik op het internet aanwezig ben.
- Al je gegevens, al je persoonlijke gegevens komt op internet te staan.
- Wie jij bent, wat je leuk vindt, waar je over nadenkt, allemaal verzameld, digitaal.
- Hetgene over jezelf, persoonlijke informatie op het internet. In ieder geval digitaal, op je computer.
- Anything which is presented about myself, my phone number, my bank account number, anything else which I want to give to the government digitally is called digital identity of myself.
- Ik denk dat het met DigiD te maken heeft. Dat je via internet je wachtwoorden kan doen.
- Mijn identiteit, maar dan digitaal. Dus online.
- Wie je online bent, eigenlijk.
- Wat ik daar achterlaat, wat voor gegevens ik daar moet geven aan instanties, hoe ik het zelf gebruik.

Schema
Structuur die definieert welke attributen en credentials in een decentraal systeem kunnen bestaan, hoe ze benoemd worden en welke publieke sleutels daarbij horen. Daarbij hoort ook overzicht van uitgevers, metadata en andere technische of menselijke afspraken zoals key size of naamgeving.

Schema manager
Dienst, organisatie of software die het beheer van een schema regelt, beheert en beschikbaar maakt.

Uitgever (issuer)
Instelling, bedrijf of mede-burger die aan een gebruiker een credential verstrekt.

Zero Knowledge Proof
Een cryptografische techniek waarmee een gebruiker aan een andere partij (de controleur) betrouwbaar kan bewijzen dat hij iets weet of heeft, zonder te onthullen wat dat precies is. Bijvoorbeeld aantonen dat je mag rijden op een bepaald moment, zonder informatie van het rijbewijs zelf te delen.

49 Alle interviews staan op https://digitaleidentiteit.waag.org/artikel/video-serie/

Bijlage: BurgerServiceCode

De BurgerServiceCode[50] is een gedragscode met tien kwaliteitseisen voor de relatie tussen burger en overheid in de moderne (digitale) samenleving. Deze eisen zijn geformuleerd als rechten van burgers en daarbij behorende plichten van overheden.

1. Keuzevrijheid contactkanaal
Als burger kan ik zelf kiezen op welke manier ik met de overheid zaken doe. De overheid zorgt ervoor dat alle contactkanalen beschikbaar zijn (balie, brief, telefoon, e-mail, internet).

2. Vindbare overheidsproducten
Als burger weet ik waar ik terecht kan voor overheidsinformatie en -diensten. De overheid stuurt mij niet van het kastje naar de muur en treedt op als één concern.

3. Begrijpelijke voorzieningen
Als burger weet ik onder welke voorwaarden ik recht heb op welke voorzieningen. De overheid maakt mijn rechten en plichten permanent inzichtelijk.

4. Persoonlijke informatieservice
Als burger heb ik recht op juiste, volledige en actuele informatie. De overheid levert die actief, op maat en afgestemd op mijn situatie.

5. Gemakkelijke dienstverlening
Als burger hoef ik gegevens maar één keer aan te leveren en kan ik gebruik maken van pro-actieve diensten. De overheid maakt inzichtelijk wat zij van mij weet en gebruikt mijn gegevens niet zonder mijn toestemming.

6. Transparante werkwijze
Als burger kan ik gemakkelijk te weten komen hoe de overheid werkt. De overheid houdt mij op de hoogte van het verloop van de procedures waarbij ik ben betrokken.

7. Digitale betrouwbaarheid
Als burger kan ik ervan op aan dat de overheid haar digitale zaken op orde heeft. De overheid garandeert vertrouwelijkheid van gegevens, betrouwbaar digitaal contact en zorgvuldige elektronische archivering.

8. Ontvankelijk bestuur
Als burger kan ik klachten of meldingen en ideeën voor verbeteringen eenvoudig kwijt. De overheid herstelt fouten, compenseert tekortkomingen en gebruikt klachten om daarvan te leren.

9. Verantwoordelijk beheer
Als burger kan ik prestaties van overheden vergelijken, controleren en beoordelen. De overheid stelt de daarvoor benodigde informatie actief beschikbaar.

10. Actieve betrokkenheid
Als burger krijg ik de kans om mee te denken en mijn belangen zelf te behartigen. De overheid bevordert participatie en ondersteunt zelfwerkzaamheid door de benodigde informatie en middelen te bieden.

50 https://www.digitaleoverheid.nl/document/burgerservicecode/

Bijlage: The Laws of Identity

Volgens Kim Cameron (2005).[51]

1. User Control and Consent
Technical identity systems must only reveal information identifying a user with the user's consent.

2. Minimal Disclosure for a Constrained Use
The solution that discloses the least amount of identifying information and best limits its use is the most stable long-term solution.

3. Justifiable Parties
Digital identity systems must be designed so the disclosure of identifying information is limited to parties having a necessary and justifiable place in a given identity relationship. The identity system must make its user aware of the party or parties with whom she is interacting while sharing information. The justification requirements apply both to the subject who is disclosing information and the relying party who depends on it.

4. Directed Identity
A universal identity system must support both 'omni-directional' identifiers for use by public entities and 'unidirectional' identifiers for use by private entities, thus facilitating discovery while preventing unnecessary release of correlation handles.

5. Pluralism of Operators and Technologies
A universal identity system must channel and enable the inter-working of multiple identity technologies run by multiple identity providers. It would be nice if there were one way to express identity. But the numerous contexts in which identity is required won't allow it.

6. Human Integration
The universal identity metasystem must define the human user to be a component of the distributed system integrated through unambiguous human-machine communication mechanisms offering protection against identity attacks.

7. Consistent Experience Across Contexts
The unifying identity metasystem must guarantee its users a simple, consistent experience while enabling separation of contexts through multiple operators and technologies.

51 Volledige versie: https://msdn.microsoft.com/en-us/library/ms996456.aspx

Bijlage: manifest Tada!

Online versie en toelichting: tada.city[52].

01. **Inclusief.** Onze digitale stad is inclusief. We houden rekening met de verschillen tussen individuen en groepen, zonder gelijkwaardigheid uit het oog te verliezen.

02. **Zeggenschap.** Data en technologie moeten bijdragen bij aan vrijheid van bewoners. Data zijn dienend. Om het leven vorm te geven naar eigen inzicht, zelf informatie te verzamelen, kennis te ontwikkelen, ruimte te vinden om jezelf te organiseren.

03. **Menselijke maat.** Data en algoritmen hebben niet het laatste woord. menselijkheid gaat altijd voor. We laten ruimte voor onvoorspelbaarheid. Mensen hebben het recht om digitaal vergeten te worden. Zo blijft er altijd ruimte voor een nieuwe, schone start.

04. **Open en transparant.** Welke data worden verzameld? Waarvoor? En met welke uitkomsten en resultaten? Daarover zijn we altijd transparant.

05. **Legitiem en gecontroleerd.** Bewoners en gebruikers hebben zeggenschap over de vormgeving van onze digitale stad. De overheid, maatschappelijke organisaties en bedrijven faciliteren dit. Zij monitoren de ontwikkeling en de maatschappelijke gevolgen.

06. **Van iedereen – voor iedereen.** Data die overheden, bedrijven en andere organisaties uit de stad genereren en over de stad verzamelen zijn gemeenschappelijk bezit. Iedereen kan ze gebruiken. Iedereen kan er voordeel van hebben. Hier maken we gezamenlijk afspraken over.

52 https://tada.city

Bronnen

Design sprints
- Digitale identiteit en digitale participatie[53]
- Design Sprint Rijvaardigheid
- Design Sprint Koopwoning

Meetups
- Lancering Identiteitslab[54] 4 juli, Utrecht
- Meetup Designing personal data ownership[55], De Waag, 27 september 2018
- Meetup Digitale Identiteitslab @Logius, 8 donderdag november 2018
- Meetup en panel: Private Screening ID2020, De Waag, 3 december 2018
- Meetup: Principes in technologie[56], Greenhost, donderdag 13 december 2018

Interviews
Opgenomen[57] in de zomer van 2018.

Gesprekken
- Expertsessie[58] tijdens VNG Fieldlab Common Ground: Tom Demeyer, Denis Roio, Timen Olthof. Zwolle, 24 september 2018.
- Update eID: Sybren van Dam, Wouter Diephuis, Stephan Klaassen, Jorgen Bogaard, Job Spierings. BZK Den Haag, 30 november 2018.
- Technologie en architectuur digitale identiteit: Sietse Ringers, Tomas Harreveld (IRMA/St. PbD), Timen Olthof (VNG), Tom Demeyer, Job Spierings, Amsterdam, 21 november 2018.
- Technologie en architectuur digitale identiteit: Johan Pouwelse, Quinten Stokkink (TU Delft), Timen Olthof (VNG), Tom Demeyer, Job Spierings, Delft, 29 november 2018.
- Panel: reflectie op screening ID2020: Roos Groothuizen, Jason Pridmore, Wouter Welling Marleen Stikker, De Waag, 3 december 2018.
- Expertpanel sprint Rijvaardigheid: Jan Smits, Paul Korremans, Robert Glas, Donovan Karamat Ali & Rob de Werd. Almere, 27 november 2018.
- Expertpanel sprint Koopwoning: Donovan Karamat Ali, Vincent Böhre, Robert Glas, Allard Keuter, Jan Smits, Wouter Welling, Jeroen Dijkgraaf en Henk Heerink. Utrecht, 4 december 2018.

Publicaties

Digitale Identiteit
- Christopher Allen Sovereign Identity. http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html
- Alpár, Hoepman, Siljee, 'The Identity Crisis', 2011. https://arxiv.org/abs/1101.0427
- Kim Cameron et al, 'Proposal for a Common Identity Framework: A User-Centric Identity Metasystem', 2008. Kim Cameron: https://msdn.microsoft.com/en-us/library/ms996456.aspx https://www.identityblog.com/wp-content/resources/2018/eic2018_06_cameron.mp4)
- Dramaturgie https://en.wikipedia.org/wiki/Dramaturgy_(sociology)
- The Economist 'Making you you. Establishing identity is a vital, risky and changing business', 18 dec. 2018. https://www.economist.com/christmas-specials/2018/12/18/establishing-identity-is-a-vital-risky-and-changing-business.
- Interactionisme https://nl.wikipedia.org/wiki/Interactionisme
- Bart Jacobs, 'De overheid als verschaffer en beschermer van digitale identiteiten', in: RegelMaat 2015 (30). https://repository.ubn.ru.nl//bitstream/handle/2066/141407/141407.pdf
- Jansen-Dings, Demeyer, 'Organiseren gebruikersperspectief doorontwikkeling eID', Waag Society, 2015.
- Tommy Koens and Stijn Meijer, 'Matching Identity Management Solutions to Self-Sovereign Identity Principles' 2018. https://www.slideshare.net/TommyKoens/matching-identity-management-solutions-to-selfsovereign-identity-principles
- Dirk Schravendeel, 'PBLQ Whitepaper: Naar een inlogstelsel voor de informatiesamenleving. Kies nu de juiste scope en doelstelling voor het eID programma'. https://www.pblq.nl/sites/default/files/2018-05/PBLQ-Whitepaper-naar-een-in-

53 https://digitaleidentiteit.waag.org/artikel/alleen-inwoners-mogen-digitaal-meebeslissen/
54 https://digitaleidentiteit.waag.org/wp-content/uploads/sites/6/Inbreng-Digitale-Identiteitslab.pdf
55 https://digitaleidentiteit.waag.org/artikel/jouw-digitale-identiteit/
56 https://digitaleidentiteit.waag.org/artikel/stel-je-bouwt-een-digitale-tool-op-basis-van-een-waarde/
57 https://digitaleidentiteit.waag.org/artikel/video-serie/
58 https://digitaleidentiteit.waag.org/wp-content/uploads/sites/6/Verslag-Expertsessie-Fieldlab-24-09-2018.pdf

logstelsel-voor-de-informatiesamenleving-.pdf
- VNG Greenpaper: 'Regie op gegevens? Durf te Doen! Verkenning van de mogelijkheden van persoonlijk datamanagement: digitale gegevensuitwisseling tussen (overheids-) partijen onder regie van de burger in een veilige en betrouwbare omgeving', 2017. https://www.digitaleoverheid.nl/document/greenpaper-regie-op-gegevens-durf/
- Steve Wilson, 'The Authentication Family Tree', presentatie CIS 2014 Modern Identity Revolution, Monterey, California 22 July 2014. http://lockstep.com.au/library/identity_authentication/authn-family-tree https://www.slideshare.net/CloudIDSummit/cis14-authentication-family-tree-111-annotated-steve-wilson

Technologie en begrippen

De online open gepubliceerde documentatie van de tools zoals besproken in de tekst.

- De blog van Jaap-Henk Hoepman http://blog.xot.nl en reacties daarop: https://www.cs.ru.nl/E.Verheul/presentations/Reactie_column_FD.pdf https://www.cs.ru.nl/E.Verheul/presentations/The_Dutch_eID.pdf https://www.cs.ru.nl/E.Verheul/presentations/IRMA_federated.pdf
- Carl M. Ellison, 'The nature of a useable PKI', 1999. http://www.sciencedirect.com/science/article/pii/S1389128698000188
- P-2-P verification o.b.v. threshold credentials o.b.v. Coconut. Toelichtend blog van Alberto Sonnino (UCL). https://www.benthamsgaze.org/2018/03/09/coconut-threshold-issuance-selective-disclosure-credentials-with-applications-to-distributed-ledgers/ en het onderliggende artikel: https://arxiv.org/abs/1802.07344
- P. Otte, et al., 'TrustChain: A Sybil-resistant scalable blockchain, Future Generation Computer Systems' (2017). http://dx.doi.org/10.1016/j.future.2017.08.048
- Stokkink, Pouwelse, 'Deployment of a Blockchain-Based Self-Sovereign Identity', 2018. https://arxiv.org/abs/1806.01926
- Pfitzman en Hansen, 'Anonymity, Unlinkability, Unobservability, Pseudonymity, and Identity Management – A Consolidated Proposal for Terminology', 2005. http://dud.inf.tu-dresden.de/Anon_Terminology.shtml
- Enige vragen over 'It's me' in Knack (2018). https://datanews.knack.be/ict/nieuws/je-hele-online-identiteit-in-een-app-wat-zou-er-kunnen-mislopen/article-opinion-859559.html?cookie_check=1546248501

Ethiek en beleid

- Maaike Kamps, 'Waardig digitaal overheidsbestuur. Over een integere omgang met sensor- technologie, big data, algoritmen en het Internet of Things', Waag, Amsterdam November 2018. https://waag.org/nl/article/waardig-digitaal-overheidsbestuur
- Over de balans tussen versleuteling, recht en (staats)veiligheid: https://www.lawfareblog.com/principles-more-informed-exceptional-access-debate
- Giovanni Buttarelli, 'Choose Humanity: Putting Dignity back into Digital', Opening Speech of Debating Ethics Public Session of the 40th Edition of the International Conference of Data, 24 October 2018. https://www.privacyconference2018.org/system/files/2018-10/Choose%20Humanity%20speech_0.pdf
- Rinie van Est, presentatie: 'Freedom in the robot age - The struggle for our intimacy', Jaarcongres PI.lab, Utrecht 14 December 2018.
- Caroline Nevejan, 'Presence and the Design of Trust', 2007. http://www.nevejan.org/presence/
- Caroline Nevejan, "Democracy by Design", presentatie 17 juni 2018.
- De Data Detox Kit, 2018. https://data-detox.nl
- Ernevi et al, 'Erratic Appliances and Energy Awareness', [DOI 10.1007/s12130-007-9007-7], 2007. https://link.springer.com/article/10.1007%2Fs12130-007-9007-7
- Jaap-Henk Hoepman, 'Privacyontwerpstrategieën (Het Blauwe Boekje)', 2018. https://www.cs.ru.nl/~jhh/publications/pds-boekje.pdf
- Mireille Hildebrandt, 'The Magic of Data

Driven Regulation', presentatie voor UNSW Sydney, 2018. https://www.youtube.com/watch?v=kHtF-VdK1LWg

- Gedicht pagina 2: vertaling uit het Chinees: Kristofer Schipper. Uit: 'Zhuang Zi: de volledige geschriften. Het grote klassieke boek van het taoïsme, vertaald en toegelicht door Kristofer Schipper', augustus, 2007.