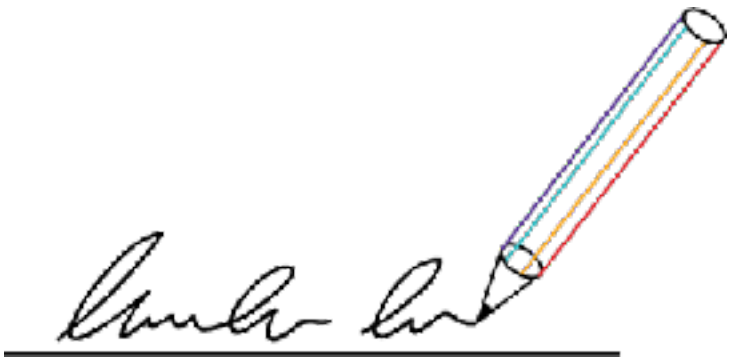
waag
technology & society

digitale identiteitslab

verzamelde inbreng

Datum	3 augustus 2018
Versie	1.0
Autheurs	Job Spierings

0. inhoudsopgave



1. inleiding

Hoe maak je online kenbaar wat je wil? En hoe kunnen anderen er dan vanuit gaan dat jij dat écht bent en dat dit écht jouw wil is?

Nu het Identiteitslab ruim een maand onderweg is, hebben we al veel informatie en input verzameld. Zowel tijdens diverse sessies en gesprekken als uit eerdere documentatie (zie kader). Deze inbreng wordt hier geordend en vormt de basis voor het vervolg van het lab.

Eén van de drie doelen van het Identiteitslab is het:

"**testen van de bruikbaarheid en geschiktheid van verschillende identiteitsconcepten en bijbehorende tools.**"

Dit gaan we doen in de volgende stappen:

1. Samen bepalen en vormgeven wat we belangrijk vinden omtrent digitale identiteit (kaders, principes, criteria, functionele eisen).

2. Een aantal geschikte concepten voor digitale identiteit selecteren.

3. Op verschillende voorwaarden testen bij de deelnemende gemeenten.

4. Opschaling onderzoeken en uitkomsten evalueren.

5. Opleveren als toetsingskader (en mogelijk herhalen).

De verzamelde inbreng biedt zowel inzicht in wat de nu betrokken stakeholders belangrijk vinden als welke aspecten nog nader onderzoek vergen omdat ze een blinde vlek zijn of anderszins vragen oproepen. Het is daarmee vooral een startpunt voor het gesprek in het identiteitslab. Op sommige, zo niet alle onderdelen (cryptografie, technologie, wetgeving, ethiek) is extra vakinhoudelijke expertise en afweging op een later moment natuurlijk noodzaak.

Door met zoveel verschillende mensen het onderwerp te bekijken worden op een heel natuurlijke manier maatschappelijke waarden en principiële visies gekoppeld aan

Bronnen

- Workshops tijdens BZK Congres "Eén Bij maakt nog geen Honing" op 7 juni, Nieuwegein
- Lancering Identiteitslab 4 juli, Utrecht
- Kickoff kerngroep op 12 juni, Amsterdam
- Project Decode (www.decode-project.eu)
- Greenpaper Regie op Gegevens (sep. 17)

ontwerpeisen en technische randvoorwaarden.

In de werkelijkheid werkt dit natuurlijk ook zo: iedere online transactie tussen burger en overheid heeft de kans het wereldbeeld van partijen te bevestigen (als de transactie voor iedereen slaagt) of te verstoren (als verwachtingen niet waar worden gemaakt).

De grote en kleine, fundamentele en praktische onderwerpen die naar voren zijn gebracht worden hier gegroepeerd.

Eerst worden de meest genoemde maatschappelijke waarden op een rij gezet, gevolgd door een overzicht van veelgestelde vragen.

Daarna volgt een lange lijst van functionaliteit en technische eisen. Die lijst bevat natuurlijk heel veel waarden en hier en daar ook wel een normatieve opmerking. Het onderwerp leent zich ook goed voor het impliciet verankeren van waardensystemen.

Opvallend: vrijwel in alle gesprekken en groepen wordt er (zelfs stilzwijgend) vanuit gegaan dat Digitale Identiteit wordt vervangen door een systeem dat werkt met het uitwisselen van (al dan niet geverifieerde) eigenschappen (Attribute Based Credentials).

2. Wat betekent digitale identiteit?

Waarden en principes: technologie is niet neutraal. Aan het begin van een ontwerpproces maken we inzichtelijk vanuit welke waarden stakeholders opereren.

Op een aantal momenten is expliciet gesproken over de waarden die deelnemers van belang vonden. Daarnaast kwamen waarden ook impliciet naar voren, als men spreekt over de 'betaalbaarheid' of de zorg uitspreekt dat 'veel mensen de regie op eigen gegevens misschien wel niet aankunnen'.

Digitale Identiteit gaat verder dan een begrip als Personal Data Management. Het omvat het geverifieerd, digitaal kenbaar maken wat iemand wil. Daarmee kun je ook geautomatiseerd overeenkomsten sluiten die de toegang regelen tot data die gaan over jou, of de naasten rondom jou. Basisregistraties en overheidsverificatie bieden een centraal punt van vertrouwen in een omgeving waar dat vertrouwen juist een schaars en vaak geschonden goed is.

Daarom zal Digitale Identiteit bepalend zijn voor de fundamenten van online zelfbeschikkingsrecht en het handelings-perspectief van burgers.

gemak

Als betrokkenen praten over welke waarden zij belangrijk vinden staat (gebruiks)gemak met stip op 1 als meest genoemd. Het kan zijn dat denken over digitale applicaties bestaande ergernissen met computers oproept, maar er wordt ook vaak naar verwezen vanuit het oogpunt van gelijkwaardigheid en inclusiviteit: slechte of onhandige software sluit vooral mensen uit.

De principes van agile softwareontwikkeling worden veel genoemd: "Stel vragen vanuit echte gebruikers en echte usecases/ transacties" en "draagvlak en gebruik gaan hand in hand".

(zelf)controle

Mensen zeggen: "ik bepaal zelf wat mijn digitale ID is" en "ik wil zijn wie ik ben – en niet wie anderen zeggen dat ik ben".
Ook wordt gewezen op het belang van de scheiding van contexten: "Betrouwbaar maar niet Herleidbaar".

> "Maak per oplossing helder wiens belang gediend wordt."

vertrouwen en legitimiteit

Georganiseerd vertrouwen en betrouwbaarheid is niet alleen een centrale functionaliteit van Digitale Identiteit: het strekt zich ook uit over alle onderdelen van de architectuur, wetgeving, governance en het businessmodel. Kan je er als gebruiker vanuit gaan dat die onderdelen die je niet direct overziet of waarneemt, toch voldoende begrijpt of kunt controleren om te beoordelen of ze werken volgens de gedeelde waarden?

Sommigen vragen: beschrijf (vooraf): “Wat is vertrouwen, hoe ontstaat dit en hoe kun je dat bevorderen of tot een bewust proces maken?” Rechtszekerheid en Informatiebeveiliging ook in het economisch verkeer is essentieel.

vrijheid en autonomie

Veel genoemd: het recht om vergeten te worden en de angst gedwongen te worden een systeem te gebruiken waarvan de belangen en waarden niet met die van jezelf overeenkomen.

Mag ik niet meedoen?
Mag ik liegen?

transparantie

Transparante en inzichtelijkheid zijn een belangrijke bouwsteen voor vertrouwen. Het laat zien welke verantwoordelijkheden wanneer van toepassing zijn. Waar je op mag rekenen en waar je eigen verantwoordelijkheid begint.

respectvol

Is er respect voor het individu, gaan rechtvaardigheid en menselijke maat boven de rigide consequenties van het systeem?

verantwoordelijkheid & behulpzaamheid

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?

Traditioneel verhoudt de rigide werkelijkheid van wetgeving em overheidsregisters zich moeizaam tot een samenleving waarin kennis, ervaring en elkaar terzijde staan diffuus en onvoorspelbaar zijn.

Veel mensen spreken de hoop uit dat nieuwe systemen ook fysiek, tastbaar, overdraagbaar en tactiel verstaanbaar zijn.

Omdenken

Er is ruimte om een vooruitstrevende positie in te nemen. Dit geef Nederland de kans om zich op dit onderwerp internationaal een voortrekkersrol toe te bedelen, bijvoorbeeld door voor te stellen om de Universele Verklaring van de Rechten van de Mens te ‘updaten’ met een ‘digitale vertaling’ van deze grondrechten.

(Greenpaper regie op gegevens)

3. Vragen:

Deelnemers hebben allerlei vragen: veel daarvan gaan over verschuivende taken, rollen en verantwoordelijkheden.

Wat is de rol van de overheid?

- Wat moet de overheid minimaal aanbieden?
- Wat moet de overheid minimaal begrijpen?
- Publieke of private infrastructuur? Wat moet overheid beheersen en wat kan “de markt” doen?
- Wie bepaalt de werkelijkheid?
- Welke eisen stel je aan toegankelijkheid tot deze middelen voor de private markt? Gaan zij attributen verzamelen (attribute hoarding)?
- Kun je de betrouwbaarheid van partijen inzichtelijk maken?
  - Keurmerk?
  - OF: deze webwinkel schendt 4 van de 12 principes?

Wat is de rol van de burger?

- Vertrouwen wij mensen met hun eigen data?
- Self sovereign, wat is “zelf in controle zijn”, kunnen we dat meten?
  - Wat is regie?
  - Wat is “ter inzage”?
- Kun je opnieuw beginnen? Bijvoorbeeld je ID resetten?

Welke stakeholders betrek je hoe en wanneer?

- Bijvoorbeeld opsporingsdiensten, “Europa”
- Verschillende ID-ketens
- Partijen buiten de overheid, private partijen, ook internationaal.

Wat is een trusted 3rd party?

- Notaris, overheid, bedrijven?
- Kan iedereen een eigenschap verifiëren van iemand anders? Mijn lidmaatschap van het buurtcomité of de voetbalclub?

Welk proces is er nodig?

- Faciliteer flexibiliteit/inspelen op veranderende eisen?
  - Meet wie er niet meedoet!
  - Zorg voor ruimte bij uitvoerende partijen
  - Toets je kader permanent op leefwereld
  - "Permanent beta"
- Wat zijn huidige problemen met eID?
- Borg het burgerperspectief bij ontwerp en gebruik
- met elkaar formeel vaststellen dat er experimenteerruimte is, bv. beleid of wetten vaststellen met 80% zekerheid of zaken die nog niet volledig uitgewerkt zijn (omdat tot meer snelheid te komen om in te spelen op veranderingen)

4. Functie & techniek

Functionele en technische eisen: welke eisen /uitgangs-punten stel jij aan een digitale identiteitsoplossing?

In een gesprek over waarden en principes die van toepassing zijn op digitale identiteit (DI) komen als vanzelf heel veel voorbeelden, ideeën en vragen naar voren. Vaak geformuleerd als specifieke eisen en wensen.

Uit lange lijsten, flip-overs, aantekeningen en collecties post-its komen de volgende zeven categorieën naar voren:

1. Functionaliteit: wat moet ik met DI kunnen?
2. Onder welke ethiek, wetgeving en governance valt DI?
3. Wat is voor veiligheid, bescherming en betrouwbaarheid van belang?
4. Is DI toegankelijk en inclusief?
5. Wanneer is DI gebruiksvriendelijk?
6. Waar moet technologie van DI aan voldoen?
7. Hoe komen we daar (operationalisering en efficiëntie)?

Hieronder worden (vrijwel) alle opmerkingen van deelnemers weergegeven, zo volledig als in de sessie genoteerd. Waar zinvol voorafgegaan door een korte samenvatting.

> "Ik wil zijn wie ik ben en niet wie anderen zeggen dat ik ben."

1. Functionaliteit

Waar iedereen het voor het oog nu al over eens is: authenticatie en autorisatie moet plaats gaan vinden op basis van eigenschappen (attributen). Vaak worden al specifieke oplossingen of apps genoemd. Sowieso hebben veel mensen één oplossing voor alle gevallen.

Daarbij noemt men vervolgens ook:

- "Ik wil dat het makkelijk is zelf te kiezen wat ik met wie deel."
- "Ik wil die toegang ook weer kunnen opheffen."
- "Doelbinding kunnen meegeven"
- "Ik wil meerdere digitale ID's kunnen hebben"
- "Ik bepaal zelf wat mijn digitale ID is"
- Scheiding van contexten: "Betrouwbaar maar niet Herleidbaar"
- "Ik wil zijn wie ik ben en niet wie anderen zeggen dat ik ben"
- "identiteit is altijd context gerelateerd. probeer helderder te maken: in deze

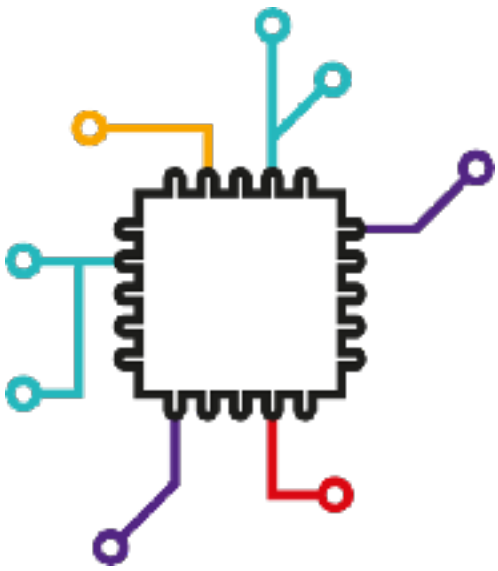
context geef ik dit van mezelf prijs, in deze context dit. een identiteitsbijsluiter."

Ook duidelijk: de eigenschappen (attributen) moeten in veel gevallen geverifieerd kunnen worden. Dat roept voor de hand liggende vragen op: wat vinden we dat (legitieme) eigenschappen zijn, hoe kun je die verifiëren en wie doet dat?

Eén deelnemer geeft vier categorieën:
- Kenmerken (gelaat/uiterlijk)
- Familie/gezinssamenstelling
- Werk(geschiedenis)
- Financiën

Maar kunnen foto's en andere data dan tekst ook een eigenschap vormen?
Is een eigenschap zinvol te anonimiseren en is dat hetzelfde als het opknippen van een attribuut?

Vanuit het DECODE project komt het concept "peer-to-peer verification met treshold credentials": dat maakt het mogelijk dat iedereen onder af te spreken voorwaarden elkaars eigenschappen kan verifiëren. In een gedistribueerde architectuur kan dergelijke p-2-p verificatie technisch verankerd worden.



Andere functionaliteit:
- Zowel binnen als buiten de overheid (niet iedereen) in meerdere rollen (zakelijk, privé, voetbalclub).
- Transparant inzicht hebben in wie welke data van mij beheert en raadpleegt: welke gegevens van mij gaan waar naartoe?
- kan ik zelf bepalen wie mij kan traceren?
- Zelf mijn gegevens beheren.
- Gegevens zijn makkelijk aan te passen en te wissen ('mogelijk tenzij…')
    - CRUD en versiebeheer (Create/Read/Update/Delete)
- Machtigingen geven en ontvangen aan mijn naasten om een deel van mijn data te kunnen gebruiken.
- Een testament kunnen meegeven: wat gebeurt er met mijn data na mij overlijden?
- Kan authenticatie ook op basis van biometrische gegevens?
- Een fysiek "iets" waarmee ik dit 'on the spot' kan doen.
- Soepele interacties met dienstverleners.
- Privacy: Vergeten kunnen worden.
- Privacy: Derden mogen mijn gegevens niet delen.

2. Ethiek, wetgeving en governance

De eisen focussen zich hier op drie thema's:

Angst voor monopolisering: hetzij afgedwongen gebruik van één overheidsapp, hetzij die van een softwaregigant.

Wetgeving aanpassen aan nieuwe mogelijkheden: geen kopie paspoort meer hoeven bewaren; maar ook: hoe verloopt de inspectie dan? En het borgen van rechten om vergeten of niet getraceerd te worden.

Roep om gebruik van open source software, open standaarden en wees interoperabel.

- Oplossingen moeten aansluiten bij wetgeving, en wetgeving dient misschien

aangepast te worden aan nieuwe usecases en oplossingen. Kopie van ID bewaren van iedere gast/medewerker is niet meer nodig.
- IE / Licenties: open source (nee tenzij).
- Bepaalde onderdelen (versleuteling) dient hoe dan ook FOSS.
- Interoperabiliteit en gebruik en ontwikkeling van open standaarden is vereist.
- Eigendom van en verantwoordelijkheden over de attributen: hoe liggen die en hoe maak je dat helder in de interfaces?
- Verantwoordelijkheden, kosten en opbrengsten: inzichtelijk, duurzaam en met juiste escalatie-mogelijkheden.
- gebruiker, eigenaar en alle andere rollen zijn aanspreekbaar.
- Ik wil dat mijn gegevens niet in handen komen van één centrale partij waarvan de belangen niet overeen komen komen met die van mij. Variatie in niet monopoliserende toepassingen, ook voor dataopslag en zowel centraal als decentraal.
- Dit is een nutsvoorziening, dus geen monopolisering vanuit tech-giganten.
- Zowel publieke als private toepassingen.
- Niet getraceerd kunnen worden, ook niet bij herhaald gebruik.
- Ik wil vrijheid in het beheer van mijn digitale identiteit.
- Rechtvaardigheid en menselijke maat blijven randvoorwaardelijk. ethische toetsing is ergens geborgd, middel ontwikkelen om ethische vraagstukken te bespreken die we nu nog niet kunnen voorzien, borgen dat deze vraagstukken op de juiste plek kunnen oppakken en borgen.

3. Veiligheid, betrouwbaarheid

Dit wordt vooral geadresseerd door duidelijk te maken wie waarvoor verantwoordelijk is. En helder te laten zij hoe die verantwoordelijkheid genomen wordt (of afgedwongen kan worden. Er wordt gesuggereerd om ketens te visualiseren, zo kunnen gebruikers zien bij wie ze terecht kunnen (en misschien ook zien wat de status van hun reclamatie is).

Het hanteren van Privacy-by-Design is niet alleen nodig op applicatieniveau maar bij het ontwerp en bouw van de hele stack, inclusief gedistribueerde en gefedereerde onderdelen.

Daarnaast noemt men dat het systeem crisisbestendig moet zijn in het geval van conflict of natuurramp.

Én: ondanks de vereiste betrouwbaarheid wenst men ook dat nieuwe use cases, hardware of bijzondere gevallen soepel in het systeem ontworpen en getest kunnen worden.

- Passende betrouwbaarheid voor elke use case, zo laag als mogelijk (spaarkaart), zo hoog als nodig (medisch dossier). Per attribuut te bepalen.
- Helder moet zijn wie in welk proces regie heeft of kan pakken. De oplossing mag niet een postbode zijn die elke transactie faciliteert.
- Vraag: wil je dit koppelen aan DNA? => Nee (waarom niet?).
- Integriteit van de keten moet bewaakt. Wie beheert/beschermt wat:
    - Visualiseer de keten en verantwoordelijkheden;
    - Fouten, disputen, reclamaties: proces inrichten;
    - Reclameren bij een trusted 3rd party?
    - Vaststellen van eigenschappen: hoe gaat dat?
- Misbruik, manipulatie, oneigenlijk gebruik:
    - Hanteer dreigingsmodellen voor alle deelnemers.
    - Alleen geverifieerde attributen of ook ongeverifieerde?
    - Preventie, Fraude.

    - faciliteer vertrouwen op platformen als Marktplaats.
    - Zorg dat opsporingsdiensten betrokken zijn.
- Voorkom het vermengen van digitale en fysieke middelen (niet).
- Welke onderdelen/transacties wil je onweerlegbaar en op neutrale grond vastleggen (bijv. op een distributed ledger)?
- Ik wil een oplossing met keurmerk.
- Crisisbestendig: qua energiegebruik, afhankelijkheid en kwade actoren.
    - “de overheid is eigenaar van het systeem, wat als de russen komen?"
- Robuustheid en beveiliging:
    - Architectuur, cloud, lokale opslag vs. “kluisjes” vs ...
- Privacy by design: ethiek, waarden zijn meegenomen in het ontwerp van de gekozen oplossingen.
    - Verandering met behoud van waarden moet mogelijk zijn.
- Nieuwe use/“edge”cases, technologie, hardware, domeinen en doelen. Die wil je kunnen onderzoeken, stapsgewijs testen en invoeren. Daar is proces voor nodig op al deze elementen.

4. Toegankelijk en inclusief

Meest gehoord: Biedt ook een fysiek alternatief. Misschien dat computers in het algemeen en internet in het bijzonder een efemere indruk achterlaten: tijdelijk en van onduidelijke bestendigheid. Iets wat je vast kunt houden, bedienen en uit kunt lenen geeft (letterlijk) meer houvast en vertrouwen.

- Online/digitaal maar ook fysiek, “analoog” mogelijk. Interactiemodel en verificatie ook afhankelijk van gekozen context en proces.
- Hoe kun je machtigingen inrichten, ook tussen privaat en publiek?
- Eenduidigheid (iDin, DigiD, eHerkenning, etc.), interoperabel.
- Kan “iedereen” in principe een identiteit hebben? Wie is “iedereen”?
- Hoe bescherm je gebruikers tegen misbruik/manipulatie/perverse prikkels (bijv. door private partijen)?
- Onvoorziene situaties en noodprocedures: Drager kwijt ==> uitwijkmogelijkheden, herstellen.

5. Gebruiksvriendelijk

Met afstand het meest en snelst genoemd. Maar gemak, privacy, regie: het zijn eisen met deels tegengestelde belangen. Die wil je wegen, en die weging kan in de tijd veranderen.

Zijn er meerdere niveaus van handelingsperspectief aan te bieden? Bijvoorbeeld een stevige basis met veilige defaults, maar veel vrijheid, keuze, flexibiliteit voor wie en waar gewenst en mogelijk.

Er zijn voor het domein van UI/UX goede en voorgeschreven testen, ook voor bijvoorbeeld minder-valide gebruikers. Digitale Identiteit

is straks echter een web aan systemen. Om daar de gebruiksvriendelijkheid te beoordelen is een concept als het **Frictie-Coëfficient** misschien een goed model : “The “Technical friction coefficient” is how hard it is, at a technical level, to engage in a new social network.” (Morgan Gangwere (4 April 2018, zie https://hackernoon.com/my-journey-into-mastodon-three-ish-days-of-overcoming-friction-d8d80285c23c (acc. 23/7/2018)).

- Kan ik ook iets ondertekenen met mijn e-mailadres? Welke kanalen lenen zich niet voor digitale identiteit? Burger mag zelf het kanaal kiezen, “hij moet het overal doen”, locatie-onafhankelijk.
- Hoe geef je burger inzicht in vastgelegde gegevens?
- Kunnen burger en instantie het proces inrichten, overzien en beheersen?
- Zijn fundamentele maar abstracte concepten voor "iedereen” begrijpelijk? (eigenschappen delen, instanties machtigen jouw informatie met andere instantie te delen)

6. Technologie

Het gebruikte systeem moet uit zichzelf transparant zijn en transparantie bevorderen. Vragen als “Hoe werkt het?” en “hoe werkt het voor mij?" worden in een natuurlijke flow beantwoord.

Alle gebruikers moeten een zinvol “working model” kunnen opbouwen van architectuur, verantwoordelijkheden en (in techniek verankerde) machtsrelaties, zodat zij kritische vragen kunnen stellen en daarmee betekenisvol hun democratisch recht kunnen uitoefenen.

Publieke waarden zijn verankerd in de technologie. Technologie ‘enabled’

> “Geen logboek maar functioneel in het moment.”

gelijkwaardigheid (niet zozeer gelijkheid) tussen deelnemers. Bijvoorbeeld doordat sleutelfuncties gedistribueerd of gefedereerd kunnen zijn (vgl. niemand 'controleert' email).

De overheid staat voor het gebruik van een full public stack. Gedistribueerd en waar nodig gecentraliseerd.

- (Inter)operabiliteit.
- Gebruik open standaarden.
- Sluit aan/volg/stuur internationale ontwikkelingen, standaarden en best practices op Europees en groter niveau.
- Minimalisering van dataopslag “bij de bron”.
- “Mijn” data zijn individueel versleuteld en ik heb de sleutels.

7. Operationalisering en efficiëntie

Hoewel dit nu nog opvallend weinig wordt genoemd is het voor de overheid natuurlijk cruciaal: is het uitvoerbaar en betaalbaar?

Opschaalbaarheid /Implementatietijd / Total Cost of Ownership.

5. Resultaten & vervolg

Wat moet het Identiteitslab opleveren volgens de bevraagde stakeholders?

Er zijn een paar duidelijke categorieën, die zich uitstrekken van het heel fundamentele tot zeer praktische.

Origineel: Biedt straks een plek aan waar je naar toe kan als er iets is met je digitale identiteit (bijv. Logius, gemeente).

Concrete oplossingen voor de burger

Om met dat laatste te beginnen, een enkeling vraagt specifiek om “(meerdere) werkende digitale oplossingen voor digitale identiteit die iteratief ontworpen en getest zijn samen met de burger.” Of, misschien haalbaarder, een “kleine oplossing, ontwikkeld met de burger, met werkende authenticatie-mechanismen.”

Verder wordt gedacht aan het beschrijven van een datamodel. En de technologie die ons soevereiniteit kan bieden is er immers al, het lab kan antwoord bieden op de vraag: willen we dat?

Strategisch resultaten

Deze richten zich op kennisvergroting en draagvlak voor de gevonden aanpak bij tamelijk specifieke doelgroepen.

Het ontwikkelen van een langetermijn-visie, een stip op de horizon, die de publieke rol (van de samenleving) op het gebied van de digitale identiteit tov partijen als Facebook versterkt.

In deze visie komen we tot een gedeeld begrippenkader rondom identiteit en identificeren: wat verstaan we daaronder, en onder digitale identiteit? Wat is dat wel, en wat niet? Het begrippenkader kan ook gebruikt worden voor gemeenschappelijke afspraken.

De uitkomsten zijn transparant, deelbaar en bieden deskundigheidsbevordering voor Tweede Kamerleden, het Rijk en lokale overheid. Ze vergroten ook het maatschappelijk bewustzijn door te delen wat er voor ontwikkeling gaande is en de burger/gebruiker vanaf het begin te betrekken bij het ontwerp en ontwikkelproces. Het geeft ook het maatschappelijk perspectief op digitale identiteit een steviger rol naast het individuele perspectief.

Best practices kunnen er onderdeel van zijn, evenals een richting voor aanpassingen op/ toekomst van DigiD.

Pilots

Er is een grote behoefte aan tastbare ervaringen en het concreet testen van oplossingen. Veel mensen hebben ook ideeën hoe, waar en met welke specifieke tool die zouden kunnen plaatsvinden.

Aansluiten bij bestaande contexten wordt vaak genoemd als belangrijk (zoals het VNG/ common ground gedachtegoed; Regie op

Gegevens). Ook wordt gevraagd om duidelijke principes als kader voor de pilots, en onderlinge afstemming tussen de tests, showcases, pilots.

Een voorbeeld is het verzoek ervaring op te doen met het dienstverleningsproces: wat moet er door worden “gekopt” als een tool op operationeel niveau wordt ingezet?

Duidelijk is de wil om te leren van (andere) experimenten en partijen, belangen niet voorop te stellen: “nu experimenteren, later meningen vormen”.

Inzicht in de opgave

Samengevat: wat komt eraan en waar moeten we ons op voorbereiden? Iemand vraagt om een “Definitie van wat eID van de overheid en andere partijen in de samenleving vraagt.” Deze stakeholders komen misschien niet direct op de inhoud van een ethiek- en ontwerp sessie af, maar willen wel graag weten hoe de roadmap voor de komende jaren eruit ziet en hoe zij zich daar op voor kunnen bereiden.

Misschien is enige concurrentie tussen gemeentes onderling nu juist goed? Houdt hierbij ook rekening met de wet markt en overheid.

Identiteitslab kan helpen vast te stellen wat de burger wil of wenst. Dit inzicht in behoefte van eindgebruikers (alle actoren) en prioritering hiervan kan als een top 5 aangeven wat als eerste kan worden opgepakt.

Framework/kader/programma van eisen

Identiteitslab dient een diverse groep mensen te betrekken bij het vaststellen en kadreren van ethische vragen volgens veel stakeholders.

> “Biedt straks een plek aan waar je naar toe kan als er iets is met je digitale identiteit.”

Daarin komen fundamentele (filosofische) uitgangspunten, waarden en grondslagen aan bod. Ook kan er opnieuw worden nagedacht over de rol van de overheid. Hoe creëren we een nieuw sociaal waardekader, waarin bijv. ook de commons (als ruimte tussen het publieke en private) benoemd worden? Hoe houden we balans tussen big brother en het individu? Wat is het kader wat we nodig hebben om de functioneren in de digitale wereld?

Kortom: lastige vragen en de daarop verzamelde antwoorden. Misschien in de vorm van een ‘position paper’: een waarden manifest. Een overzicht van de balans tussen allerlei waarden en hoe je die balans wil inrichten.

Het ethisch framework kan als rode draad worden gebruikt voor het vervolg en het resultaat zijn van een dialoog en samenwerking tussen alle verschillende stakeholders.

Daarnaast moet het framework requirements bevatten en ingaan op mogelijke business cases of verdienmodel. Het forceren van keuzen wordt ook genoemd, net als het onderscheid tussen theoretische en praktische problemen.

Een open en gedetailleerde technische vergelijking van verschillende oplossingen en hun impact op de waarden en beleid.

Voor commerciële partijen is het goed als er daarbij een consensus ontstaat over verantwoordelijkheden en duidelijkheid wat de overheid wil doen (en wat niet).

Wettelijk kader

Hoe kan identiteitslab bijdragen aan een toekomstig wetgevingsproces? Komt er een wet op de digitale identiteit?

Velen vragen om een (wettelijke) verankering van de plicht om waar beschikbaar/mogelijk gebruik te maken van open standaarden, een uniforme werkwijze en open source software. Ook voor de algemene infrastructuur is open source en interoperabiliteit een must.

Alle systemen moeten met elkaar kunnen praten en alle partijen, publiek, privaat, civiel kunnen de infra gebruiken.

Netwerkfunctie invullen

Er zijn niet alleen veel “oplossingen” voor digitale identiteit, er zijn ook heel veel initiatieven om te ontwikkelen, ontwerpen en testen. Is er een plek waar een inventarisatie beschikbaar is? Waar inzicht is in de al beschikbare “body of knowledge” die er al is? De komende jaren gaan meer partijen meer pilots doen met uiteenlopende use cases. Hoe organiseren we daarbij shared learning?

Partijen uit verschillende sectoren bij elkaar brengen, gezamenlijke ontwikkelprojecten faciliteren en kijken welke casussen relevant zijn. Dus: uitwisseling van kennis is hier essentieel. Evenals inzicht in wat we kunnen leren van andere landen.

Documenteer methode beleidslab

Zorg dat we aan het eind weten wat in deze werkvorm (identiteitslab) wel en niet werkt. Bijvoorbeeld door bij te houden hoe de uitkomsten wel of niet tot aanpassing leidt in beleid of wetgeving.

Het format van deze samenwerkingsvorm zou herhaalbaar gemaakt kunnen worden voor andere vraagstukken.