Bezoekverslag eYou in the EU

Connecting consumers in a digital world

Datum
27 juni 2016

Classificatie
Publiek

Auteur
Esther Makaay

Blad
1/4

Contact
T 026 352 55 00
support@sidn.nl
www.sidn.nl

Bezoekadres
Meander 501
6825 MD Arnhem

Postadres
Postbus 5022
6802 EA Arnhem

Via participatie in IDnext was SIDN betrokken bij eYou in the EU, dat georganiseerd werd in het kader van het Nederlandse voorzitterschap van de EU. We hebben een kort verslag gemaakt, omdat we denken dat deze onderwerpen interessant zijn voor een veel breder publiek dan enkel de aanwezige bestuurders en beleidsmakers.

Europese eIDAS-programma

Het programma had een sterke focus op eID-ontwikkelingen in diverse landen en de stand van zaken rondom het Europese eIDAS-programma. Vertegenwoordigers van onder andere Oostenrijk, België, Spanje, Estland en het Verenigd Koninkrijk deelden hun lokale ervaringen met het implementeren van eIDAS.
Lidstaten mogen hun nationale eID schemes tot 2018 vrijwillig aanmelden voor gebruik. 13 lidstaten hebben aangekondigd dit te doen en een 10-tal werkt er nog aan. Vanaf 2018 zijn de alle landen vervolgens verplicht om online authenticaties voor overheidsdiensten van deze aangemelde eIDs te accepteren.

Digital single market

Het overkoepelende thema van de dag was het Europese streven naar een ‘digital single market’, wat geen sinecure is met 28 lidstaten met ieder hun eigen aanpak en ideeën. De basis hiervoor is vertrouwen: in de technologie, de systemen, maar vooral in de afspraken die gemaakt moeten worden (en gehandhaafd!). eIDAS is hierbij een uniek project, omdat het internationaal voor juridische interoperabiliteit zorgt.
Om dit in een breder perspectief te plaatsen, was er in het programma volop ruimte voor ondersteunende, alternatieve en disruptieve ontwikkelingen vanuit de private sector.

Martijn Kaag van Connectis is ervan overtuigd dat federatieve oplossingen de enige manier zijn om echte wereldwijde oplossingen te leveren voor een ‘digital single market’: herbruikbare identiteiten voor real-time cross-border veilige transacties in allerlei vormen. Met een overzicht van de geschiedenis van federaties (van X.500 en MS Passport via Kim Cameron’s 7 Laws of Identity naar huidige grootschalige implementaties zoals OpenID, SURFconext en eHerkenning) laat hij zien dat de technologie en standaarden inmiddels volwassen zijn. De ontbrekende schakel wordt nu ingevuld door eIDAS: het eerste bindende afsprakenstelsel voor cross-border identificatie en authenticatie.

Maar eIDAS is nog niet geïmplementeerd. Om adoptie van eIDAS aan te jagen, werkt Connectis samen met de overheid aan een project waarmee op korte termijn meer dan 70 gemeentes, meer dan 1.000 services en meer dan 25 identity providers aangesloten worden op eIDAS. (www.eidas2018.eu)

Frankrijk heeft (net als Nederland overigens) nog geen nationale elektronische identiteit. Uit frustratie over de moeizame ontwikkelingen is een klein team de uitdaging aangegaan om met weinig geld en in korte tijd een alternatieve oplossing te vinden voor digitale transacties. Charles-Henri Menseau presenteerde 'AliceM', een demo waarmee op basis van de chip in het ePassport of een identiteitskaart een digitale identiteit aan een telefoon met NFC gekoppeld kan worden. Hiermee kan vervolgens, met een hoog vertrouwensniveau, authenticatie plaatsvinden of kunnen digitale handtekeningen gemaakt worden. De Franse overheid investeert nu in een vervolg hierop. Misschien dat andere Europese landen hier ook in geïnteresseerd zijn?

Trusttester

TNO heeft onderzocht dat één van de obstakels voor het succes van eID-stelsels dataverstrekking is: beheerders van data zijn terughoudend met het verstrekken van hun data of het geven van toegang daartoe aan derde partijen. (Naast de strikte privacyregelgeving is er vaak sprake van waardevermindering van data en ziet men risico's rondom het verstrekken van validiteit of garanties op de inhoud.)
Op basis van dit gegeven hebben ze een systeem gebouwd dat gebaseerd is op validatie van data zonder verstrekking: TrustTester.
TrustTester is een afsprakenstelsel waarmee data veilig (en traceerbaar) gevalideerd kan worden zonder dat de data zelf uitgewisseld wordt met andere partijen in het stelsel (het is een 'zero-knowledge' oplossing waarbij geen enkele partij meer leert dan wat ze al wisten of wat hen door hun gebruikers verteld wordt). TNO werkt momenteel aan een pilot voor hypotheekoffertes met het UWV en een grote bank. Gebruikers kunnen bij de bank hun inkomen opgeven en validatie van dit gegeven verkrijgen zonder dat er persoonlijke- of inkomensgegevens worden uitgewisseld. SIDN is betrokken bij dit initiatief.

Data-overload

Watson-ambassadeur Nicky Hekster van IBM heeft een hele persoonlijke motivatie om te werken aan innovatie in de gezondheidszorg: Wat is er belangrijker dan gezondheid? Dit werd eenvoudig gedemonstreerd door aan het publiek te vragen te gaan staan en dan te gaan zitten als ze iemand kennen met diabetes, hart- en vaatziekten, kanker… Het duurde niet lang voordat iedereen weer in zijn stoel zat.
De gezondheidszorg heeft te maken met data-overload. Nog los van de groeiende hoeveelheid academische, klinische en genetische gegevens, verzamelen mensen tegenwoordig terabytes aan informatie met wearables en gezondheids-apps.

Door al deze data op te slaan en te gebruiken, kunnen nieuwe inzichten en individueler gerichte zorg ontstaan. Dit is mogelijk met Watson Health Cloud, gebaseerd op het Watson Cognitieve Technologie Platform. Watson begrijpt natuurlijke taal, kan redeneren en evalueren, leren en aanpassen, begrijpt en interacteert met individuen en kan 800 miljoen A4-pagina's per seconde verwerken. Watson werd beroemd door het winnen van de Amerikaanse spelshow Jeopardy (waar de antwoorden gegeven worden, en de spelers de bijbehorende vraag moeten bedenken) van de beste menselijke deelnemers.

De Watson Health Cloud integreert en verrijkt data en content aangeleverd door partners in het ecosysteem, waardoor bewijs-gebaseerde analyse en inzichten verkregen kunnen worden, onder data-stewardship op privacy en security.
De eerste voorbeelden van services die gebaseerd zijn op dit platform zijn een persoonlijke diabetes-coach op de smartphone die een hypoglycemische coma 3 uur van tevoren kan voorspellen (huidige norm is een half uur) en een platform dat astmapatiënten helpt met respirator-gebruik door het combineren van real-time inhalatorgegevens met longfunctiemonitoring.

Privacy staat centraal

Bij al deze ontwikkelingen staan security en privacy natuurlijk centraal. In één van de break-out sessies werd een solide basis gegeven voor deze onderwerpen.
Jaap-Henk Hoepman, onder meer directeur van het Privacy & Identity Lab, presenteerde een praktische aanpak voor privacy in ontwikkeling van systemen en concepten: op basis van onderzoek door de Radboud Universiteit is er een model gemaakt met daarin acht strategieën voor privacy-by-design. Vier ervan zijn gericht op de data zelf:

- Minimalisatie (verzamel geen data van alle personen, of verzamel zo min mogelijk data per persoon)
- Separatie (sla data op verschillende plaatsen op)
- Aggregatie (gebruik generieke data over groepen heen)
- Verbergen (zorg dat niet alle data zichtbaar is, bijvoorbeeld met encryptie en toegangsbeperkingen)

De andere vier hebben te maken met het proces:

- Informatie (de betrokkene moet weten wanneer zijn data verwerkt wordt)
- Controle (de betrokkene hoort controle te hebben over wanneer en hoe dat gebeurt)
- Aantonen (compliancy aan beleid, regels en wetgeving)
- Handhaven (van de privacypolicy)

De werking van deze strategieën werd geïllustreerd met verschillende voorbeelden van een alternatieve aanpak voor sociale netwerken, cloud storage en eID-oplossingen.
En Hoepman maakte een bijzonder punt van eerlijk ontwerp: ontwerp systemen die werken als geadverteerd en je niet verrassen of beschadigen (achteraf).

Sterke authenticatie

Jens Bender van BSI stelde een intrigerende vraag: *wat bedoelen we als we het hebben over 'sterke authenticatie'?*
Europese en overheidsregelgeving en -wetgeving noemen betrouwbaarheid en security, maar de bewoording over hoe dit bereikt zou moeten worden is zeer impliciet. De technologie praat over 'sterke authenticatie' en tegenwoordig wordt dat simpelweg vertaald naar 2-factor authenticatie.
Jens presenteerde een analyse van de verschillende type authenticatiefactoren (bezit, kennis en biometrie) en de diverse aspecten die relevant zijn voor deze typen. Bijvoorbeeld of een factor gebruikt wordt met symmetrische authenticatie (zoals een wachtwoord dat lokaal bekend is bij de

gebruiker, maar ook extern bij de systemen van een provider) en hoe herroeping uitgevoerd kan worden.
Zijn aanbevelingen:

- Een combinatie van factoren (zoals bij 2FA) moet gebruikmaken van de verschillende sterke punten van de factoren.
- Geen één aanval zou effectief mogen zijn tegen beide gebruikte factoren.
- Herroeping is een hard requirement, liefst onafhankelijk van een service provider.
- Een gebruiker moet het merken als zijn middelen gecompromitteerd zijn.
- En het ontstaan van 'privacy hot spots' moet natuurlijk vermeden worden.

Mens-gebaseerde trust

In haar afsluitende keynote presenteerde Benita Matofska, oprichter van The People Who Share, nog een perspectief op vertrouwen: mens-gebaseerde trust. The People Who Share is een sociale organisatie die bedrijven en individuen helpt om toe te treden tot de Sharing Economy, een systeem gebaseerd op het delen van allerlei soorten middelen die je maar kunt bedenken. En het is groot: de waarde van de groei van de Sharing Economy is geschat op $15 miljard over de eerste 7 jaar, waarmee de gezamenlijke groei van Facebook, Google en Yahoo ($11 miljard) ruim overtroffen wordt. Er zijn meer dan 9.000 platformen, toepassingen en projecten en het behelst alle denkbare sectoren: privaat, publiek, liefdadigheid en sociaal. Al 28% van de wereldwijde volwassen bevolking participeert en naar verwachting verdubbelt dit aantal het komende jaar.
Echter, vertrouwen is de grootste drempel voor delen en dit leidt tot de opkomst en noodzaak van mens-gebaseerde trusttechnologieën. Voorbeelden hiervan zijn Veridu, wereldwijde identiteits-verificatie gebaseerd op je digitale footprint, of HooYu, peer-to-peer identiteits-bevestiging. Het is belangrijk dat deze nieuwe typen technologie aangemoedigd worden: in de toekomst moeten onze steden 70 procent meer mensen huisvesten. De noodzaak om middelen te delen is enorm. We moeten onze steden ombouwen tot 'smart, sharing cities'. Trusttechnologie stelt ons in staat om veilig contact aan te gaan met vreemden en ongebruikte bezittingen te delen, wat onze steden en onze economie op grote schaal verandert.

Aansluitend werd in Den Haag op 15 en 16 juni de conferentie Trust in the Digital World georganiseerd. Hier was gedurende twee dagen tijd om nog verder op alle onderwerpen in te gaan.