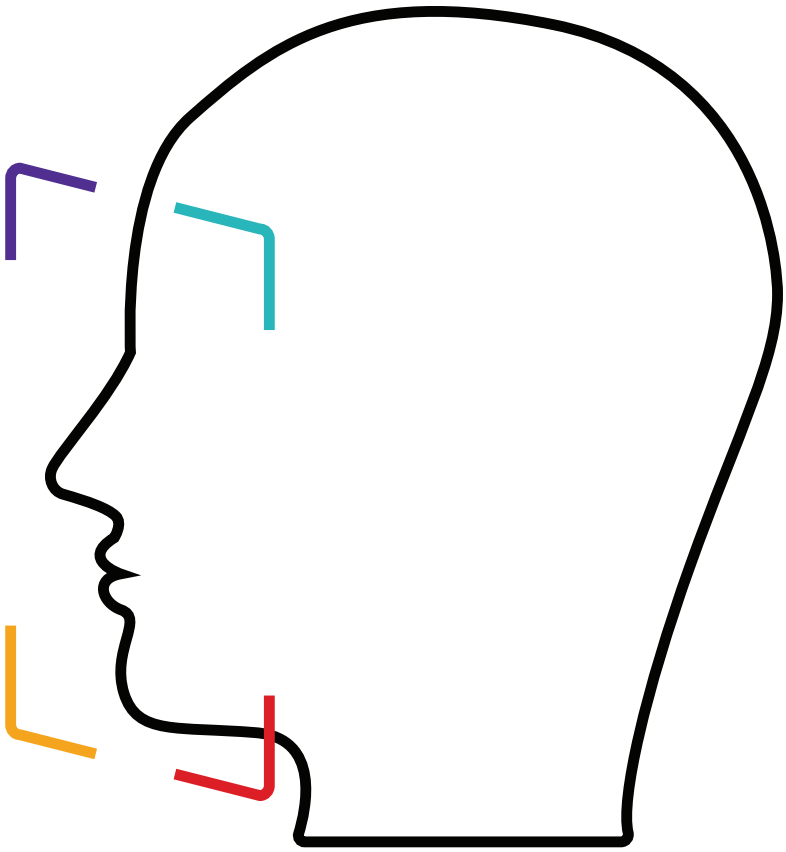
Smart Society Case #2

Digitale identiteit: verdeel en beheers

De opkomst van decentrale technieken om mensen hun identiteit veilig mee te laten bewijzen en beheren

November 2019



Auteurs:
Socrates Schouten
Teuntje Bril

Dienstverlening | ICT | Privacy | Digitale veiligheid

Het digitaliseren van overheidsdiensten belooft de mogelijkheid publieke diensten te verbeteren. Ook gemeentelijke dienstverlening gaat steeds meer digitaal en op maat. Voor de verschillende diensten moeten burgers zich digitaal melden, maar op het gebied van digitale identificatie stapelen zich momenteel risico's op. Er is behoefte aan een identificatiemiddel waarbij een persoon zichzelf (of eigenschappen van zichzelf, zoals leeftijd) kan aantonen zonder volledig identificeerbaar te zijn.

Inleiding

Om digitale dienstverlening mogelijk te maken is het noodzakelijk dat burgers zich digitaal kunnen identificeren. In de overheidscontext vervult op dit moment voornamelijk DigiD de rol van zo'n digitale identiteit.[1] DigiD is inmiddels door vrijwel alle volwassenen in gebruik: 13,6 miljoen Nederlanders hebben een DigiD en loggen hiermee 300 miljoen keer per jaar in. DigiD maakt het regelen van toegang tot overheidsdiensten in de kern veel makkelijker dan de ouderwetse papierwinkel.

Maar veel gemeenten lopen tegen nieuwe problemen aan door de overstap naar een centraal digitaal identificatiemiddel, bijvoorbeeld rondom het afgeven van machtigingen. Weliswaar bestaat de mogelijkheid derden, zoals zorgverleners,

toestemming te verlenen om digitale zaken te doen met de overheid, maar die machtigingsoptie schiet in veel contexten tekort.[2] Daarom worden in de praktijk DigiD's vaak uitgeleend. Dat deze praktijk niet alleen onwenselijk is, maar ook wettelijk verboden, blijkt voor de zorgverlener minder zwaar te wegen dan de noodzaak te kunnen handelen namens haar cliënt of familielid. Dit is maar één voorbeeld van een situatie waarin meer flexibiliteit van digitale identificatie gewenst is in de relatie tussen overheid en inwoner.

Ook buiten de overheid groeit de behoefte aan een betrouwbaar en flexibel online identificatiemiddel. Het aantal online transacties en via apps of internet georganiseerde diensten neemt al jaren stug toe, en zal dat voorlopig blijven doen. De wildgroei van paspoortkopietjes is gelukkig tot bedaren gekomen, maar naar privégegevens zoals adres en geboortedatum wordt om de haverklap gevraagd. En steeds vaker leunen webwinkels voor die informatie op Amerikaanse platformbedrijven zoals Google, Facebook en Paypal als intermediairs voor het inloggen en betalen door klanten.

Vanuit het oogpunt van veiligheid en democratische controle is dit echter een doodlopende weg. Er moeten manieren worden gezocht om de gegevens en privacy van burgers online beter te beschermen en je identiteit flexibeler te kunnen aantonen. Er worden momenteel diverse oplossingen uitgewerkt, die diversiteit in het identificatielandschap aanbrengen en heel anders met persoonsgegevens omgaan. Hoe werken deze oplossingen? Hoe zou een *betrouwbare en veilige digitale identiteit* er in de nabije toekomst uit kunnen zien?

Risico's van de huidige digitale identificatiemiddelen

DigiD is een digitale authenticatiedienst die gebruik maakt van het bestaande stelsel van 'basisregistraties', zoals paspoorten en rijbewijzen. Dat stelsel schiet tekort willen we het tempo van digitalisering en herorganisatie in de publieke sector bijbenen. Binnen de huidige mogelijkheden kunnen de vele verschillende databases die gemeenten en centrale overheid beheren niet continu worden gesynchroniseerd.[3] Dat leidt tot verveelvoudiging van data. De consequentie is niet alleen inefficiëntie, maar ook foutgevoeligheid. Door diverse databases met dezelfde persoonsgegevens aan te maken wordt meer informatie opgeslagen dan strikt noodzakelijk is, kunnen synchronisatiefouten optreden en neemt de kans op datalekken toe.

Een tweede issue: in sommige gevallen is DigiD een 'paardenmiddel'. DigiD is gekoppeld aan het burgerservicenummer, een hoogstpersoonlijke en veelomvattende *identifier*. In diverse contexten is deze mate van authenticatie onnodig zwaar,

Vraagstukken

Betrouwbaarheid en efficiëntie
Gemeentelijke databestanden die refereren naar de basisregistraties dupliceren informatie en kunnen niet continu worden gesynchroniseerd. Dat introduceert foutgevoeligheid. Hoe meer systemen en voorzieningen gekoppeld worden en door dezelfde trechters gaan, hoe groter het risico op systeemfalen ('omvallende dominostenen').

Flexibiliteit
De digitalisering 'dwingt' ons tot dynamischer werkwijzen. Binnen en buiten de overheid is de digitale identiteit daar nog niet toe opgewassen. DigiD kan alleen voor publieke diensten worden gebruikt; identificatie in andere contexten is nu een 'marktgoed' met weinig publieke controle. Een goed, wendbaar identificatiemiddel is inzetbaar in vele contexten en gaat uit van dataminimalisatie.

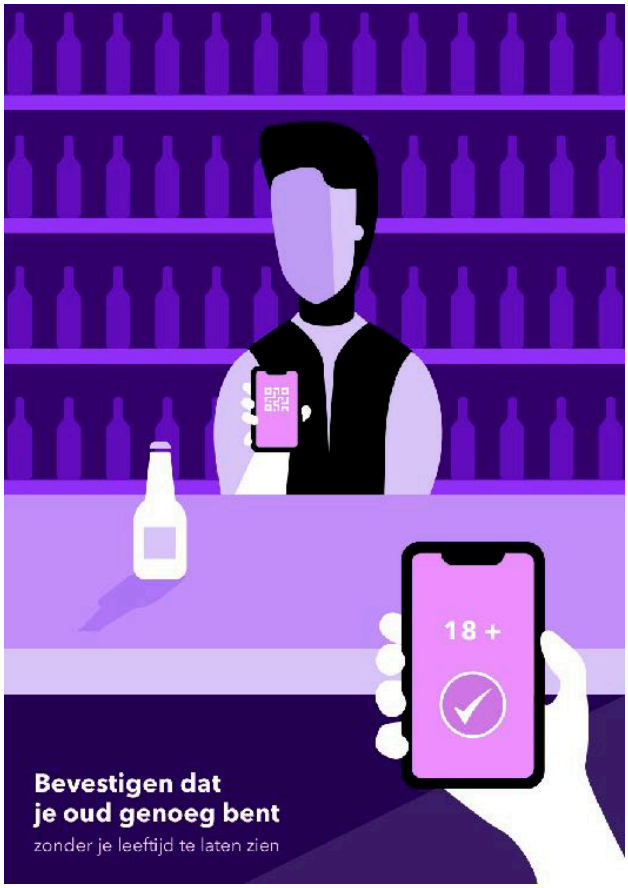
Controle en autonomie
Online ervaren mensen een gevoel van ongenoegen: 'ze weten alles van mij' en 'wie weet wie er allemaal meelezen'. Dit gebrek aan controle begint bij de digitale identiteit. Zou het helpen als een app je duidelijk maakt wat er met je gegevens gebeurt, wat je met wie deelt en welke rechten en plichten je hebt?

bijvoorbeeld als een inwoner een kapotte straatlantaarn wil melden bij de gemeente. Het gebruik van contextuele informatie is dan proportioneler en veiliger: woont of werkt deze persoon in de buurt? Hoe kunnen we haar bereiken voor vragen of feedback? Haar BSN en precieze identiteit is immers niet van belang. Een oplossing die de melder weliswaar kwalificeert, maar die enkel de hoogst noodzakelijke informatie verstrekt, geniet vanuit informatieveiligheid en gebruiksgemak dan de voorkeur. Door middel van onderstaande casus wordt uitgelegd waarom dat niet alleen 'eleganter' is maar ook wezenlijke (persoonlijke, bestuurlijke en maatschappelijke) risico's indamt.

Case: Aantonen dat je ouder dan 18 bent

28 maart 2019: Staatssecretaris Blokhuis meldt strenger te gaan handhaven op de aanschaf van alcohol door minderjarigen. Het moet onmogelijk worden om via internet toch aan alcohol te komen. De huidige werkwijze is dat een bezorger de leeftijd van de ontvanger moet controleren bij het afleveren van een bestelling met drank. Dat gebeurt maar één op de tien keer, blijkt uit onderzoek.[4] In diverse gemeenten spelen vergelijkbare problemen rondom minderjarigen met gokverslaving.

Denk bijvoorbeeld aan webwinkels die een manier zoeken om leeftijd vast te stellen bij alcoholverkoop. Hoewel bezorgers bij levering van alcohol om legitimatie moeten vragen, gebeurt dit maar weinig waardoor jongeren probleemloos alcohol kopen. Als de bezorger er wel om verzoekt, is het resultaat ook niet optimaal: wanneer je je paspoort of ander identificatiebewijs laat zien, toon je ook je naam, geboortedatum en andere gegevens. Zou het werken om je online te identificeren bij het plaatsen van de bestelling? Het middel DigiD is hiervoor in elk geval niet beschikbaar: het is te 'zwaar' voor deze situaties[5] en bovendien kan DigiD kan enkel door overheidsinstanties gebruikt worden voor een gelimiteerd aantal doeleinden.[6] Hier toont zich het gebrek aan een werkbaar, algemeen inzetbaar digitaal identificatiemiddel.



Afbeelding: Gemeente Amsterdam

Bij gebrek aan veilige en betrouwbare identificatie is het niet zo vreemd dat zowel gebruikers als dienstverleners voortdurend onzeker zijn: komt deze bestelling écht bij die klant terecht? De enige oplossing tegen deze onzekerheid lijkt nu het verzamelen van zoveel mogelijk gegevens: het hamsteren van data als substituut voor échte zekerheid. Op deze manier leggen verkopers klantprofielen aan die het mogelijk maken verdacht gedrag te signaleren. Een gevolg is evenwel dat aanbieders en dienstverleners steeds vaker grijpen naar uitgebreide, geautomatiseerde risicoanalyses om klanten al dan niet te bedienen.

Beschouwing

De meerderheid van de Nederlanders klikt online vrij argeloos op 'ik accepteer de voorwaarden'; privacy lijkt niet erg zwaar te wegen. Maar desgevraagd ervaren mensen vaak een sluimerend gevoel van ongenoegen:

'Ze weten toch al alles van mij,' en 'wie weet wie er allemaal meelezen'.[7] Terwijl we steeds meer persoonlijke informatie prijsgeven, is er een gebrek aan controle over het delen van zulke data: wat, met wie, en in welke context. Daarvoor zijn praktische oplossingen nodig.

Het herwinnen van controle over het gebruik van persoonlijke data begint bij de digitale identiteit. Daarmee kan men, in theorie, zelfs bij zeer alledaagse digitale handelingen beslissen om wel of geen data te delen. Het praktische ontwerp van zulke oplossingen is in volle gang. Inmiddels zijn er juridische, technische en ook bestuurlijke handvatten om een betere digitale identiteit vorm te geven. Hoe zien die eruit en wat is het handelingsperspectief voor een gemeente?

Op het juridische vlak is de Algemene Verordening Gegevensbescherming (AVG) een doorslaggevende factor. Sinds de bekrachtiging van de AVG geldt de wettelijke opdracht privacy vanaf het allereerste begin van een systeem expliciet te implementeren. Dit principe, *privacy-by-design*, is in de verordening opgenomen om te zorgen dat altijd rekenschap kan worden gegeven over de datastromen. Als dat niet inherent in het technische ontwerp zit, maar 'achteraf' wordt toegevoegd, is het risico op datalekken groot en is de 'accountability' niet te waarborgen. Voor de kwesties die spelen rondom digitale identiteit geldt hetzelfde: als deze niet voorafgaand goed georganiseerd worden, dreigen problemen achteraf moeilijk of niet oplosbaar te zijn.

Een tweede principe uit de AVG is *dataminimalisatie*. Dataminimalisatie betekent dat de hoeveelheid persoonsgegevens die verzameld en opgeslagen worden zoveel mogelijk wordt beperkt. Dat principe staat haaks op de verleiding die platformbedrijven nu vaak niet kunnen weerstaan: veel data inzamelen en combineren om klantprofielen mee op te bouwen. Ook webwinkels en andere dienstverleners kennen die verleiding, maar dan gemotiveerd om te trachten iemands identiteit te verzekeren – bij gebrek aan een betrouwbaar authenticatiemiddel.

Attribuutgebaseerde identiteit in de praktijk: de aanvraag van een sociale huurwoning

Als ik mij wil inschrijven bij een online site voor huurappartementen wordt me gevraagd aan te tonen dat ik over een passend inkomen beschik om de huur te kunnen betalen. Via een link op de website word ik naar de website van de Belastingdienst gestuurd.
De website van de Belastingdienst vraagt of ik een attribuut wil ontvangen dat zegt dat mijn verzamelinkomen vorig jaar hoger was dan €35.000. Ik klik op OK, log in en er verschijnt in het scherm een QR-code met de tekst: open uw Attributen App op uw telefoon en scan de QR-code. Ik scan de code en op mijn telefoon zie ik dat ik nu over een nieuw attribuut beschik: "Inkomen 2018 > €35.000". Dit attribuut is nu herbruikbaar, zodat deze stap in het vervolg kan worden overgeslagen. Terug op de website van de makelaar klik ik op de knop "minimuminkomen aantonen". Weer verschijnt er een QR-code met een verzoek: scan deze code om uw minimuminkomen aan te tonen. Met mijn telefoon scan ik de code en wordt mij gevraagd: wilt u het attribuut "Inkomen 2018 > €35.000,-" delen met makelaarskantoor Een Dak B.V.? Ik klik op 'Ja' en in mijn account verschijnt een groen vinkje. ✅

De technische belofte: attribuutgebaseerde identiteit

De principes van dataminimalisatie en privacy-by-design bieden samen een goede leidraad voor het ontwerp van identificatieroutines. Een praktische, technische uitwerking van deze principes vinden we in het model van *attribuutgebaseerde identiteit*: dan wordt niet iemands identiteit prijsgegeven maar slechts een 'attribuut' ofwel eigenschap gedeeld. In de genoemde casus zou dat als volgt werken. Bij de verkoop van alcohol, zo hebben we gezien, hoeft de verkoper enkel te weten dat de koper ouder dan

18 jaar is. In een ideaal geval krijgt de verkoper slechts een 'groen vinkje' te zien, die bewijst dat aan deze verkoopvoorwaarde is voldaan. Dat groene vinkje heeft dan bijvoorbeeld als betekenis: "De gemeente Aa en Hunze verklaart dat deze persoon ouders is dan 18 jaar". Met attribuutgebaseerde identiteit is het mogelijk je puur en alleen te 'identificeren' op dat ene gegeven (er wordt ook wel gesproken van 'betrouwbaarheid op het kleinst mogelijke gegeven').

Om uit te leggen hoe dit werkt, moeten we eerst een paar termen introduceren. Ten eerste maken we verschil tussen het brede begrip *identiteit* en het precieze begrip *eigenschap*. Je (digitale) identiteit gaat over het geheel van kenmerken die maken wie jij bent en hoe je daaraan herkenbaar bent. Een eigenschap is een enkel, specifiek stuk informatie over jouw persoon. De eigenschappen geboortedatum, leeftijd of leeftijdscategorie zeggen elk iets over je leeftijd. Maar de eerste geeft véél meer persoonlijke data vrij dan de laatste. In een online omgeving (webshops, online gokken) zou attribuutgebaseerde identiteit eenvoudig kunnen worden geregeld, maar ook in winkels, casino's en in de kroeg is meerderjarigheid te bewijzen via je smartphone. Het kader (op pagina 5) geeft een voorbeeld van hoe dit er in de praktijk voor een gebruiker uit zou kunnen zien.

eID: Rijksprogramma voor digitale identiteit

Het Ministerie van Binnenlandse Zaken werkt aan de uitbouw van digitale identificatie en aan de herziening van het stelsel van basisregistraties. In de nabije toekomst zal er een systeem van 'open erkenning' van authenticatie- en inlogmiddelen van kracht gaan, zodat er naast DigiD allerlei andere apps in gebruik kunnen worden genomen.[8] Er zijn voor de meeste contexten al apps beschikbaar, zowel van commerciële als niet-commerciële ontwikkelaars, en in diverse gemeenten vinden experimenten plaats met deze oplossingen. Hier behandelen we enkele van de belangrijkste ontwikkelingen voor de Nederlandse context.

eID ('elektronische identiteit') is een Rijksprogramma gericht op het verbeteren van de digitale interactie van burgers en bedrijven met de overheid. Dit programma omvat onder andere de doorontwikkeling van DigiD maar ook enkele pilots met bestaande private inlogmiddelen. Bovendien is in 2018 de Europese **eIDAS**-verordening ingegaan. Die bepaalt dat overheidsdiensten EU-burgers en organisaties die zich identificeren met hun eigen nationale inlogmiddel moet erkennen. Denk aan een Duitse student die aan de TU Delft wil studeren en een vergunning nodig heeft, of een Spaanse toerist die schade wil claimen. Maar ook een Nederlander in Nederland die Belastingaangifte doet met een Ests authenticatiemiddel. Het gaat dus om een ingrijpende 'opening' van het Europese identificatieveld.[9]

Van de initiatieven in de markt is **iDIN** in Nederland de voornaamste. iDIN is een dienst opgezet door Betaalvereniging Nederland en diverse banken waarmee consumenten zich bij andere organisaties kunnen identificeren met de inlogmiddelen van hun eigen bank. Vergelijkbaar met de betalingsintermediair iDeal biedt dit een schakelpunt voor diverse (web)omgevingen om uiteindelijk naar het inlogmiddel van de eigen bank te worden doorgesluisd – maar nu niet om te betalen, maar slechts om te identificeren. Het wordt inmiddels gebruikt bij ruim 100 websites van bedrijven en instanties zoals ASR, BKR en MediaMarkt. Een nadeel is van iDIN dat het niet voor buitenstaanders (experts maar ook burgers) controleerbaar is: er is alleen indirecte democratische controle mogelijk. En net als bij DigiD is het een gecentraliseerde oplossing waarbij de onveiligheid groeit naarmate het werkingsgebied breder wordt.

Decentrale applicaties

Naast de door de markt geboden middelen zijn er diverse apps die in niet-commerciële contexten worden ontwikkeld. Bijvoorbeeld **IRMA**, ontwikkeld aan de Radboud Universiteit Nijmegen. IRMA (een afkorting van '*I Reveal My Attributes*') gedraagt zich als een *wallet*, portemonnee, van persoonlijke gegevens. Deze attributen bevinden zich (goed beveiligd) op je telefoon. Je hebt de volledige controle over met wie je ze deelt en je ziet ook bewust wat je deelt: niet een vaag begrip ('je inkomensgegevens' of 'je leeftijd') maar een specifiek en beperkt attribuut, ondertekend door de passende autoriteit. Omdat de

software die deze app gebruikt open-source is, is de werking en beveiliging voor onafhankelijke experts inzichtelijk. De gemeente Nijmegen, maar ook Haarlem, Almere, Leiden en Amsterdam, experimenteren met het verstrekken van attributen via de IRMA-app. Alle persoonsgegevens uit de BRP en andere basisregistraties kunnen worden upgeload in de digitale identificatie-app.

Ook de TU Delft werkt aan een digitaal identificatiemiddel, mede in opdracht van het ministerie van Binnenlandse Zaken. Net als IRMA wordt het een *wallet* die allerlei gegevens en attributen kan bevatten, waarbij de burger zelf controle heeft wat er in de portemonnee verschijnt en wanneer het wordt gedeeld. Projectleider Johan Pouwelse zegt in het FD dat de ambitie voor wat betreft functionaliteit hoog is. 'Je moet het zien als portemonnee, waarvoor je alleen maar een smartphone nodig hebt,' aldus Pouwelse.[10] Het Delftse project berust op blockchain-technologie.

Schluss. Net als IRMA is Schluss een app die je de controle over je persoonlijke gegevens wil teruggeven. De ontwikkelaars omschrijven het als 'een digitale kluis waar je al je gegevens in kwijt kunt en waar jij bepaalt wie wat van jou mag weten'.[11] Gebruikers kunnen de app straks downloaden en gebruiken voor een paar euro per jaar. Schluss richt zich op een gedecentraliseerde opslag van data, wat een veiliger opslagmethode is dan centrale opslag in één grote database. Waar IRMA zich richt op het beheren van een beperkte set persoonsgegevens, is de bedoeling van Schluss dat al je gegevens in de Schluss-kluis terecht komen: van hele simpele adresgegevens tot hele complexe medische en financiële gegevens.

Solid, een afkorting van 'Social linked data', is een (enigszins vergelijkbaar) project geïnitieerd door Tim Berners-Lee, de 'uitvinder' van het World Wide Web. Het beoogt de data-architectuur van het internet te veranderen met het idee van een 'datakluis' ofwel 'data pod' als vertrekpunt.[12] Toepassingen die zijn geverifieerd door Solid mogen gegevens opvragen als de gebruiker de toepassing toestemming verleent. Een gebruiker kan persoonlijke informatie over verschillende pods verspreiden, bijvoorbeeld pods voor persoonlijke profielgegevens, contactgegevens, financiële informatie, gezondheid, reisplannen of andere informatie bevatten.

Oplossingen zoals de bovengenoemde die de

gegevensopslag loskoppelen en decentraliseren, zijn vaak nog in een vroege ontwikkelfase. Steeds meer ontwikkelaars zijn er echter van overtuigd dat dit de richting is die digitale identiteit, en het internet in het algemeen, op moet. Een goed digitaal ID vormt één van de belangrijkste fundamenten onder een betrouwbare en veilige gedigitaliseerde samenleving. Het spreidt, en beperkt, zowel de verantwoordelijkheid als het risico door digitale identiteit technisch, juridisch en bestuurlijk decentraal te organiseren. Het is daarbij van belang dat een gekozen oplossing het mogelijk maakt dat veel verschillende (publieke en private) organisaties kunnen samenwerken terwijl zij hun eigen verantwoordelijkheden kunnen organiseren en risico's kunnen beheersen. Dat gaat niet wanneer ze afhankelijk zijn van één centraal *single point of failure* waar de gehele veiligheid van de digitale samenleving vanaf hangt.

Conclusie

Van wijkverpleging 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 doel-

groep werkbaar, betrouwbaar en veilig is, blijft het bij plannen, kleinschalige pilots en—maar al te vaak—frustraties. Intussen wordt de overheid verweten verkokerd te opereren en elke poging tot een holistische aanpak in de kiem te smoren.

Met de groeiende mate van complexiteit van de dienstverlening groeien ook de risico's van systeemfalen. Een betrouwbaar en veilig digitaal identificatiemiddel is niet alleen wenselijk binnen het overheidsapparaat, maar ook meer algemeen voor burgers en organisaties om zich te manoeuvreren in een digitaliserende samenleving. Het invoeren en beschikbaar stellen van attribuut-gebaseerde identificatie kan een belangrijke bijdrage leveren om risico's binnen het overheidsapparaat in te perken, maar ook een veilige en betrouwbare digitale identiteit te faciliteren voor andere dienstverleners.

Een 'contextueel identificerende identiteit' biedt uitkomst. Mensen delen niet hun hele identiteit, maar alleen de strikt noodzakelijke onderdelen van die identiteit: een identiteit op maat, die past bij de context. Gemeenten kunnen hieraan bijdragen door hun dienstverlening klaar te maken voor de *wallets* en andere identificatiemiddelen die recent het daglicht hebben gezien. Door samen te werken met andere gemeenten en te experimenteren in het kader van eID, kunnen gemeenten bijdragen aan het leerproces dat nodig is om in de nabije toekomst digitaal veilig en toegankelijk te blijven.

Stelling

Gemeenten moeten een rol spelen in het beschermen van de digitale identiteit van hun inwoners door actief samen te werken met innovatieve, open source identificatieoplossingen.

Noten

1 Voor organisaties en rechtspersonen wordt eHerkenning, een vergelijkbaar middel, gebruikt.

2 Frits de Jong, 'Vernieuwing in zicht voor DigiD Machtigen', iBestuur.nl, 20 februari 2019: https://ibestuur.nl/praktijk/vernieuwing-in-zicht-voor-digid-machtigen

3 Stephan Ockhuisen, 'Meer dan 5000 databases met persoonsgegevens bij overheid', Sargasso.nl, 10 mei 2012: http://sargasso.nl/meer-dan-5000-databases-met-persoonsgegevens-bij-overheid/

4 Onderzoeksbureau Objectief in opdracht van de gemeente Utrecht, september 2016: https://leeftijdscontrole.nl/wp-content/uploads/2016/09/NALEVINGSONDERZOEK_GEMEENTE_UTRECHT_OBJECTIEF_2016_LR-1.pdf

5 Voor informatie over het vereiste betrouwbaarheidsniveau zie de Handreiking Betrouwbaarheidsniveaus van het Forum Standaardisatie: https://www.forumstandaardisatie.nl/thema/handreiking-betrouwbaarheidsniveaus

6 Als het werkingsgebied wordt uitgebreid (op basis van de huidige DigiD-technologie), dan wordt DigiD onveiliger, omdat een grotere groep use cases op één centraal punt beveiligd moet worden.

7 Enkele relevante onderzoeken: DDMA Privacy Monitor (tweedelig), mei en december 2018: https://ddma.nl/privacy-monitor/; 'Online privacy baart veel Nederlanders zorgen', Emerce.nl, 6 maart 2018: https://www.emerce.nl/wire/online-privacy-baart-veel-nederlanders-zorgen.

8 Zie 'Kamerbrief over andere toelatingssystematiek inlogmiddelen voor burgers', 5 juli 2019: https://www.rijksoverheid.nl/documenten/kamerstukken/2019/07/05/kamerbrief-over-andere-toelatingssystematiek-inlogmiddelen-voor-burgers

9 De verordening eIDAS (Electronic IDentification Authentication and trust Services) regelt de Europese acceptatie van nationale elektronische identificatiemiddelen. Het gaat naast landen ook om andere (semi)publieke dienstverleners. In totaal zijn er ongeveer 500 dienstverleners geïdentificeerd die op eIDAS moeten worden aangesloten. Zie https://www.digitaleoverheid.nl/dossiers/eidas/dossier-berichten/zes-maanden-na-de-ingangsdatum-van-eidas/.

10 'Overheid lanceert paspoort op het mobieltje', Financieele Dagblad, 1 juli 2019:

https://fd.nl/ondernemen/1306756/overheid-lanceert-paspoort-op-het-mobieltje.

11 Bron: website Schluss, https://www.schluss.org.

12 In Solid blijven de gegevens bij de bron staan en krijgt de gebruiker via linked data-technologie de controle hebt over wie er inzage in die gegevens heeft. Schluss daarentegen ambieert om de opslag van persoonsgegevens bij de verwerker weg te halen.

Smart Society Cases

Digitale technologie is tot in de vezels van de samenleving doorgedrongen en roept vraagstukken op in diverse beleidsdomeinen. Digitalisering brengt kansen met zich mee voor doelmatiger en efficiënter bestuur, maar de praktijk is ook weerbarstig. Zoveel succesvolle oplossingen als er zijn ontwikkeld, zoveel projecten zijn er ook de mist in gegaan — met alle kostbare gevolgen van dien. Bovendien dienen zich nieuwe vragen aan: onder welke omstandigheden is een sterk gedigitaliseerde samenleving bijvoorbeeld nog democratisch en veilig? Waag en de VNG geven in deze reeks een overzicht van actuele cases rondom digitalisering. De reeks presenteert feiten en dilemma's en biedt handreikingen voor een betrouwbare en weerbare informatiesamenleving.

Auteurs
Socrates Schouten, Teuntje Bril

Illustraties en foto's
Waag, tenzij anders vermeld

Opmaak
Waag

Bij voorkeur citeren als:
S. Schouten en T.J. Bril (2019). 'Digitale identiteit: verdeel en beheers'. Smart Society Case nr. 2, November 2019. Amsterdam: Waag; Den Haag: Vereniging van Nederlandse Gemeenten.

VNG

waag technology & society