CASE

Beheer van digitale identiteit kan veiliger en handiger

Koppeling publieke en private systemen belofte voor de toekomst

Het beheer van onze digitale identiteiten kan veiliger en handiger. Wat kunnen we leren van de ervaringen in het publieke en het private domein? Een geïntegreerde aanpak die gebruik maakt van expertise uit het betalingsverkeer biedt uitkomst.

Onze digitale identiteit is niet meer te vertrouwen. We gaan steeds meer naar digitaal, maar de manier waarop we onze digitale identiteit tegenwoordig beheren is grotendeels gebaseerd op oude technologie: wachtwoorden, complexe authenticatieprocedures, veiligheidsvragen zoals het vermelden van de meisjesnaam van je moeder of het versturen van een afbeelding van je paspoort via e-mail.

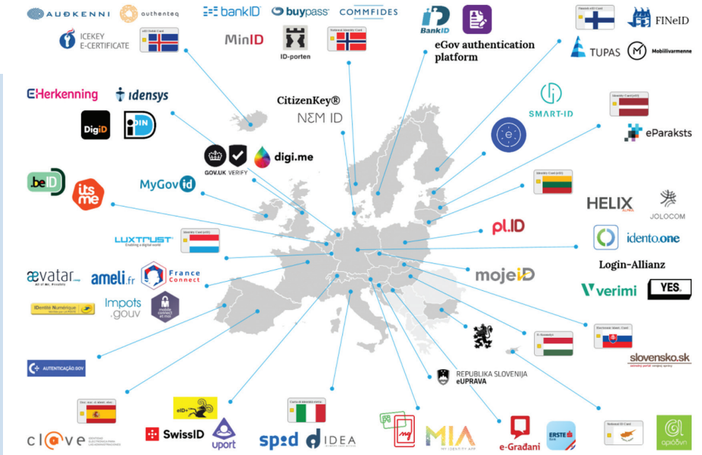
Het is geen verrassing dat hackers de tijd van hun leven hebben, want veel van deze verouderde veiligheidsmaatregelen blijken steeds kwetsbaarder te worden en leiden dagelijks tot grote datalekken. Daarnaast worden gebruikers gefrustreerd door eindeloze lijsten met pincodes en wachtwoorden, zien de online winkeliers dat volle, virtuele winkelwagens in de steek gelaten worden vanwege klantonvriendelijke betaalpagina's en worden overheden gefrustreerd door het slechte gebruik van hun digitale identiteitsmiddelen. Het is dus duidelijk dat we de manier waarop we ons digitale leven beveiligen dringend moeten veranderen: het beheer van onze digitale identiteiten moet veiliger en handiger worden.

Publieke sector

Veel regeringen over de hele wereld hebben geprobeerd het identiteitsprobleem voor hun burgers en bedrijven op te lossen. eIDAS, de Europese verordening voor de digitale uitwisseling van identiteiten, helpt ook om dit probleem aan te pakken. Het succes van initiatieven van overheden en regelgevers is echter zeer verschillend. De enorme inspanningen om in het Verenigd Koninkrijk een identiteitskaart te creëren stuitten op verzet van het publiek en moesten worden ingetrokken. En een andere grote inspanning om één enkele digitale aanmelding te creëren voor alle overheidsdiensten (gov.uk verify) werd geïntroduceerd met veel vertoon, maar er wordt vooralsnog weinig gebruik van gemaakt.
De digitale ID-dienst in Duitsland op basis van de persoonlijke identiteitskaart wordt nog nauwelijks toegepast en heeft weinig gebruikers.
De Nederlandse overheid gaf DigiD uit, maar heeft moeite met het upgraden van de technologie uit de jaren zeventig (gebruikersnaam en wachtwoord); het implementeren van een eIDAS-compatibele oplossing ter vervanging van de oudere, maar veelgebruikte DigiD, is een moeilijke en zeven jaar durende politieke discussie gebleken en kostte bijna 1 miljard euro. De lijst van mislukte overheidsinitiatieven op het gebied van digitale identiteit is lang en er lijkt nog geen eind aan te komen.
Men is het er nog steeds niet over eens of de grootschalige uitrol van digitale identiteitsmiddelen vanuit overheden in Europa (eIDAS) en India (Aadhaar) de juiste antwoorden zijn aan de behoeften in de markt. Sommige landen hebben echter duidelijk succes geboekt in het verstrekken van een publieke digitale identiteit. Estland levert alle e-overheidsdiensten digitaal, gebaseerd op een door de overheid verstrekte identiteit. Maar ook deze middelen zijn al gehackt en ook zij hebben al te maken gehad met grote problemen op het gebied van digitale beveiliging. Oostenrijk heeft een kleine maar nuttige oplossing op basis van mobiele identiteit ('Handysignatur') en Italië heeft ook een werkende oplossing. Maar de lijst met succesvolle digitale identiteitsoplossingen vanuit de overheid is kort. Te kort.

Private sector

Particuliere identiteitsverstrekkers daarentegen zijn talrijk - misschien wel te talrijk - en velen hebben veel succes, een groot bereik en worden regelmatig gebruikt. Banken bieden hun klanten, net als veel andere sectoren, zeer veilige identiteitsdiensten aan. Uit enquêtes blijkt dat klanten doorgaans de voorkeur geven aan de producten uit deze sector – in plaats van producten van de overheid – om hun identiteitsoplossing in te richten.
Het probleem is hier meer dat de private sector te veel concurrerende oplossingen opzet, waarbij de gebruiker ook nog eens met eindeloos veel gegevens wordt overspoeld die alleen in een bepaalde silo gebruikt kunnen worden. Het is dus duidelijk dat we de inrichting van onze digitale identiteit beter moeten organiseren. In plaats van nog meer en aparte oplossingen te creëren om de identiteit van een gebruiker te verifiëren - tegenwoordig heeft elke organisatie of website zijn eigen identiteitsmethoden - is een gezamenlijke aanpak in een ecosysteem met publiek-private middelen zeker beter.



De waanzinnige wereld van silo's die we nu aan het opbouwen zijn. Bron: asquared 2018

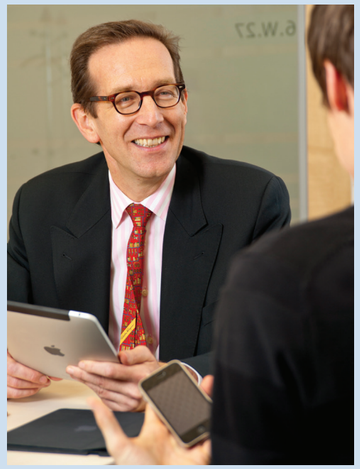
Multi-middelen als Europese standaard

Het naast elkaar bestaan van publieke- en private identiteiten is nu de facto de nationale, Europese en wereldwijde norm. In een publiek-private samenwerking worden de digitale identiteit en de daarmee samenhangende attributen over meerdere bronnen en identiteitsbeheersystemen samengesteld, die vervolgens aan elkaar kunnen worden gekoppeld om bepaalde aspecten van zowel mensen als dingen te verifiëren. Dit principe van verbinden is precies wat er in de betaalsector ook is gebeurd. Het is immers gemeengoed geworden om met een betaal- of creditkaart in elke winkel, overal ter wereld, te betalen. Dankzij eIDAS en door verdere Europese samenwerking van de verschillende digitale identiteitsinitiatiefnemers, publiek en privaat, zullen we daarmee in de toekomst binnen Europa precies dezelfde ervaring op het gebied van digitale identificatie en authenticatie krijgen zoals we die nu gewend zijn bij het betalen.
Als men de beste oplossingen van de overheid en het bedrijfsleven met elkaar weet te verbinden, waarbij de gebruiker controle heeft over zijn eigen gegevens, dan wordt zeker een stap in deze goede richting gezet. De naam, geboortedatum en -plaats van een persoon worden door de overheid verstrekt en zijn daarmee betrouwbaar. De kredietwaardigheid (als de gebruiker dit toestaat) getoetst door een bank en of de betrokkene verzekerd is, vastgelegd door zijn verzekeringsmaatschappij en hoe fit hij is bevonden door zijn arts. Het zijn alle attributen waarmee een gebruiker – met zijn uitdrukkelijke toestemming – zich wenst te identificeren of die hij wenst te delen, zijn beschikbaar uit verschillende publieke- en private bronnen. Een gebruiker moet deze attributen kunnen laten verifiëren door de bevoegde instantie, in een ecosysteem waar publieke- en private systemen door centrale routeringvoorzieningen met elkaar zijn verbonden.

Publiek-private oplossingen ecosystemen

Dergelijke ecosystemen beginnen te ontstaan: de Scandinavische landen hebben veel industrieën met elkaar verbonden rond een op banken gebaseerd identiteitsmodel, de Australische regering heeft een multi-industriële regeling genaamd myGov ingevoerd en in de Verenigde Staten is de 'National Strategy for Trusted Identities in Cyberspace' (NSTIC) eigenlijk een open identiteitsmarkt zonder nationale regeling, opgebouwd rond open identiteitsprotocollen. In dezelfde lijn wordt het pan-Canadese 'Trust Framework' als een veelbelovend open publiek-private samenwerking gezien. Dergelijke publiek-private ecosystemen zijn er dus al, verspreiden zich snel en blijken zeer succesvol. Door ook gebruik te maken van de expertise op het gebied van betalingsverkeer en door het hergebruik van de zeer vertrouwde betaalinfrastructuur van bedrijven zoals equensWorldline, de pan-Europese leider in betalingen en transactiediensten, zal de invoering van deze oplossingen verder kunnen worden versneld.

Laten we duidelijk zijn: geen enkele publieke- of private partij zal alle identiteitsattributen voor iedereen kunnen gaan leveren - zelfs niet als daar door een overheid zwaar op wordt geïnvesteerd, noch als een krachtig consortium van grote industriële spelers samenkomt en daarop inzet. Laten we dus stoppen met het bouwen van nog meer eilanden en in plaats daarvan de bestaande oplossingen met elkaar verbinden. De attributen van elke speler kunnen naar behoefte worden gecombineerd en beschermd onder strikte gebruikerscontrole. Op die manier bereiken we een Europese dekking, tevreden gebruikers en bedrijven en hebben we een veilige basis voor de Europese Digitale Interne Markt van de toekomst.



Michael Salmony is executive advisor bij equensWorldline en internationaal vermaard om zijn bedrijfsinnovaties in de digitale en financiële dienstverlening. Salmony adviseert grote Europese banken, brancheorganisaties en Europese financiële instellingen op het gebied van digitale strategie.

Voor meer informatie:
michael.salmony@equensworldline.com