



Identity



Beste lezer,

De toekomst van de digitale identiteit; wat is hiervan op dit moment de status? Hoe waarborgen we de privacy en veiligheid van consumenten en bedrijven? Met dit onderwerpen hielden wij ons 5 jaar geleden al bezig. Daarom besloten we om op 28 januari 2016 de eerste editie van het congres 'Toekomst van de Digitale Identiteit' (nu bekend als: e-Identity Congres) te organiseren.

Na een succesvolle eerste editie bleek dat het Identity landschap ook de jaren erop nog volop in beweging zou zijn. Waar het congres de eerste jaren vooral een 360-graden overzicht gaf van alle zakelijke en technologische ontwikkelingen in de telecom en financiële sector, is het inmiddels een thema dat in alle sectoren top-of-mind is.

De afgelopen jaren hebben we allerlei Identity experts vanuit de wetenschap, overheid en bedrijfsleven een podium gegeven. **In dit e-book blikken we terug op 5 jaar kennis en ervaring van digitale identiteit.** We legden onze experts onder meer de volgende vragen voor:

- Welke ontwikkelingen zijn er op het gebied van identificatie & authenticatie van klanten?
- Welke initiatieven zijn er om identificatie en authenticatie van personen (burgers, consumenten) en bedrijven op de digitale toekomst in te kunnen richten?
- Wat is er nodig om de volgende stap in digitale identiteit te maken?
- Hoe is het gesteld met de privacy en bescherming van de klant, nu en in de toekomst?

Lees in dit eBook hoe onze experts de afgelopen jaren hebben gekeken naar de toekomst van digitale identiteit en maak een vergelijking met de huidige ontwikkelingen.

Veel leesplezier en op naar de volgende 5 jaar aan vooruitstrevende ideeën en innovatieve ontwikkelingen!

Liz Boeren

Programmamanager e-Identity congres

Inhoud

De kloof tussen gebruikers en aanbieders van e-Identity oplossingen	3
Congresverslag e-Identity 2019	7
Dagvoorzitter e-Identity Congres blikst vooruit	9
Identity management: 'Convenience en privacy bijten elkaar niet'	11
e-Identity congres: 'We hebben stappen gemaakt'	13
Zorg dat de gebruiker van een e-Identity altijd aan het roer staat	17
Inloggen met je rijbewijs of met een selfie? De burger mag het zeggen!	19
We gaan onvoldoende zorgvuldig om met privacygevoelige informatie	21
e-Identity: Het borgen van de privacy van de klant is essentieel	23
Belangrijk is om onderscheid te maken tussen verschillende vormen van identificatie en authenticatie	26
Idensys moet de opvolger van Digid/eHerkenning worden	28

De kloof tussen gebruikers en aanbieders van e-Identity oplossingen

29 oktober 2019

'Jij bent jij en ik ben ik!'

Een blog over e-Identity, digitale identiteit. Je denkt vast: daar gaan we de diepte in over blockchain, SSI of biometrie? Ja, uiteindelijk gaat het daar zeker over. Maar in deze blog ga ik allereerst in op de context van e-Identity. Een onderwerp dat elke consument en ondernemer raakt. Want we hebben het over de oplossing hoe jij als eindgebruiker in de digitale wereld op een eenvoudige, veilige manier kan bewijzen dat jij, jij bent! Dat is belangrijker dan ooit doordat we steeds meer online, wereldwijd actief zijn en daar helaas misbruik van kan worden gemaakt.

Op 12 februari 2020 vindt het [e-Identity congres](#) hierover plaats en Euroforum vroeg mij hiervoor als dagvoorzitter. Vanaf dat moment heb ik bewuster dan ooit de situaties beleefd waarbij online een identiteitscheck werd gevraagd. Een greep uit de afgelopen twee weken:

- Mijn vakantie in Spanje. Volgens onze Airbnb host moesten we wegens lokale regelgeving een foto van onze paspoorten naar hem appen, anders kwamen we het huis niet in?!? Dit hoefde uiteindelijk in de praktijk niet, maar sommigen hadden al foto's geappt naar ene Igor. Hmmm.
- Inzage in de stand van zaken van de orthodontistenverzekering voor mijn zoon van 15. Hij moest eerst een DigiD aanvragen en mij vervolgens machtigen?!? Schijnt vanaf 12 jaar een regel te zijn. Gaat hij dan ook betalen, vroeg ik me af? Deze regel zal vast zijn nut hebben in situaties waarbij de relatie van ouder-kind slecht is, maar dat is gelukkig bij ons niet het geval. Afijn, mijn zoon weet nu wat een DigiD is en hoeveel zijn beugel kost.
- Een geraffineerde ransom mail binnengekregen op mijn werk-mailadres: 'Bitcoins betalen, anders sturen we compromitterende beelden naar al jouw contacten'. Uiteraard schrik ik hier niet van en heb ik die mail gewoon weggegooid. Maar ik dacht wel: die camera moet ik eens afplakken...

Nu is de vraag niet zozeer hoe ik hierop heb gereageerd, maar hoe een gemiddelde burger hiermee omgaat. Begrijpt hij wat hem gevraagd wordt? En waardoor? Doorziet hij pogingen tot fraude? En welke rol nemen bedrijven en overheden hierin? Dit soort vragen ga ik ook meenemen tijdens het congres.

E-Identity oplossingen aanbieden

Ik ben geen ras-specialist op dit onderwerp, maar nieuw is het niet voor me. Tijdens mijn werk bij ABN AMRO's Innovation Centre hadden we in 2013 een samenwerking met Qiy Foundation. 'Iedereen eigenaar van zijn persoonlijke data en de internetversie 3.0 die dit ondersteunt', hoor ik Marcel van Galen vol passie verkondigen in 2013. Early birds? Waren we er allemaal (te) vroeg bij?

De afgelopen jaren heb ik bij Moneyou een nieuwe 'mobiele money management'-propositie mogen ontwikkelen en lanceren. Toeters en bellen verzinnen is makkelijk. Lastig is het om de dienst zo intuïtief te maken dat hij daadwerkelijk in de praktijk gebruikt wordt. Hier hebben we rekening mee te houden met de onboarding (degelijke KYC-toetsing), het functionele gebruik van de app, maar ook bij toepassingen als multi-banking, waar we nu mee bezig zijn (het koppelen van accounts van andere financiële instellingen). Zo vraagt PSD2 veel inlevingsvermogen bij gebruikers en aanbieders. Mooi thema voor het congres?

E-Identity congres over tech & gebruiksgemak

De centrale thema's van het [e-Identity congres 2020](#) gaan niet alleen over de technische kant, maar ook over de veilige, betrouwbare en gebruiksvriendelijke toepassing van e-Identity. Een belangrijke randvoorwaarde voor massa-adoptie lijkt me. Het onderwerp e-Identity is inmiddels een stuk actueler dan toen ik er 6 jaar geleden mee mocht experimenteren. Opgewarmd door de Marcellen van deze wereld, de volwassenheid van technologieën, de toename van toepassingen en voeding door privacyschandalen á la Cambridge Analytica. Zou dat niet de belangrijkste factor zijn: de noodzaak van een veilige, betrouwbare e-Identity-oplossing wordt steeds meer gezien door de eindgebruiker, de burger?

Ik dacht: laat ik deze aanname eens toetsen tijdens een interview met de moderator van 2019 en tevens keynote speaker in 2020.

Onze keynote speaker Michiel van der Veen

Michiel heeft een rijke achtergrond, bij een multinational (Philips), en als ondernemer (spin-out Priv-ID). Hij bekleedt een nevenfunctie bij de Wereldbank en is sinds kort directeur Innovatie & Ontwikkeling bij de Rijksdienst voor Identiteitsgegevens (RvIG). Hier is hij verantwoordelijk voor alle ontwikkelingen en vernieuwingen rondom de Basisregistratie Personen (BRP), reisdocumenten en digitale identiteit.

De vooravond van grote veranderingen

Ik vroeg hem wat hem is bijgebleven van het congres van vorig jaar: e-Identity in 2019.

Michiel: 'In 2019 staan we aan de vooravond van grote veranderingen. Iedere week kan je wel naar een congres of hackathon over dit thema. Dit toont aan dat de behoefte aan e-identity-oplossingen groot is, mede gevoed door de digitalisering, de globalisatie en het toenemend aantal reisbewegingen dat wij maken. Veel partijen weten dat ze 'iets' met identiteit moeten; een betrouwbare, vertrouwde, KYC-oplossing wordt gevraagd waarbij de papieren weg niet volstaat. **Wat mij opviel aan het congres is dat het aanbod van oplossingen nog erg gefragmenteerd is en dat een consolidatie nog moet plaatsvinden.**'

Dat is een mooie uitdaging voor ons congres in 2020: Wat zou die eenduidige richting moeten zijn?

Verwachtingen voor 2020

Als sneak preview voor het congres, vroeg ik Michiel alvast iets te delen van zijn verwachtingen voor 2020.

Michiel herkent de themasetting van het congres: de zoektocht naar betrouwbare, veilige en gebruiksvriendelijke oplossingen. **De eindgebruiker een vrije keus geven moet het streven zijn. Maar dan wel voor alle gebruikers**, licht Michiel toe. Als grote thema's voor 2020 ziet hij privacy, cybersecurity en inclusiviteit. 'Voorkoming van misbruik van gegevens, en ervoor zorgen dat alle groepen mee kunnen in de geboden oplossingen, is een typische overheidszorg. Soms past een fysiek loket juist goed bij een online overheidsdienst. Bijvoorbeeld: bij het UWV blijft het mogelijk om naar een Werkplein te gaan om daar gebruik te maken van de aangeboden diensten. Die 'rol' past de overheid vooral in het maatschappelijk kader, een inclusieve benadering'. Ongetwijfeld gaan we hier nog meer van vernemen op 12 februari.

Ten slotte vroeg ik Michiel naar zijn vergezicht: wanneer krijgen wij die consolidatie van oplossingen en ontstaat er een massaal eenduidig, wereldwijd gebruik?

Volwassenheid van governance

Michiel voorziet dat de komende jaren standaardisering een grote rol gaat spelen in het gebruik van e-identity. 'Dit vraagt wel nog volwassenheid in technologie maar ook in wetgeving en governance die rekening houdt met alle belangen. Hoe we daar komen is vooral door aan tafel te zitten en te experimenteren', zo sprak Michiel als ervaren en realistische innovator. 'Laten we eerst in Nederland en Europa slagen maken, standaarden op wereldschaal liggen nog een eind weg.'

De kloof?

Mijn praktijkvoorbeeld van Spanje, over de zogenaamd verplichte foto van je paspoort, illustreert het vraagstuk van internationale standaardisatie. Bij navraag schijnt dit voor Airbnb in Spanje niet wettelijk verplicht te zijn, maar dient dit voornamelijk om verhuurders meer grip te geven op huurders, als er kosten verhaald moeten worden. Deze oplossing staat in contrast met wat in Nederland kan: daar is het verboden om identiteitsbewijzen op deze manier op te vragen. Hier zit nog wel een kloof qua wetgeving. En hoe moet een gemiddelde Europeaan zich van deze spelregels bewust zijn?

Misschien is de digitale generatie beter opgewassen tegen dit soort vraagstukken. Zij zijn opgegroeid in het mobiele tijdperk vol 'fake news' en dataschandalen. Afgaande op mijn zoon denk ik van wel. Ik ging met hem in gesprek over het belang van een DigiD en waarschuwde hem met mijn genoemde praktijkvoorbeelden. 'Pa, daar trap je toch niet in?!? Kijk, jij bent jij en ik ben ik. Ik deel echt niet alles online, ik mess mijn profiel zodat Facebook echt geen clue heeft wie ik ben en mijn cam is afgeschermd natuurlijk. Ik kijk wel uit!'

Kloof gedicht.

Congresverslag e-Identity 2019

6 maart 2019

Op woensdag 13 februari vond de 4^e editie van het [e-Identity congres](#) plaats. Met meer dan 140 bezoekers was het een dag vol kennisuitwisseling en inspiratie. In deze blog lichten wij 5 thema's uit die gedurende de dag regelmatig ter discussie stonden. De thema's zijn bij de deelnemers van het congres getoetst doordat zij live konden meestemmen op een aantal stellingen.

Identiteitsfraude

Het congres werd geopend door Michiel van der Veen, CEO, European Association for Biometrics en dagvoorzitter van het e-Identity congres. Michiel begon met de vraag hoeveel van de aanwezigen de recente [uitzending van Rambam](#) over identiteitsfraude heeft gezien. Deze uitzending is volgens Michiel een must see voor iedereen die zich bezig houdt met digitale identiteit management. In de uitzending laten de makers namelijk zien hoe eenvoudig het is om iemand zijn identiteit te 'stelen' en hier o.a. rekeningen mee te openen, een huurwoning op naam zetten en online aankopen doen.

In de live enquête is 26% het met de dagvoorzitter eens; zij vinden het waarborgen van privacy & veiligheid een van de belangrijkste zaken als het gaat om digitale identiteit.

Customer Experience

Gedurende de dag blijkt al snel dat beveiliging niet het enige thema is dat deelnemers belangrijk vinden. 24% van de aanwezigen vindt Customer Experience en gemak het belangrijkste als het gaat om digitale identiteit management. Dit beaamt ook KLM, voor hen zijn er 2 pilaren erg belangrijk vanuit Identity & Access Management: Brand en Klant. Zij zijn bezig met een splitsing van Customer Data en Customer Identity en hiermee verwachten ze de komende jaren grote sprongen te kunnen maken. Klanten kunnen dan op voor hen eenvoudige wijze herkend worden en zij kunnen hen de ultieme persoonlijke ervaring bieden.

Verantwoordelijkheid

"Wie is er verantwoordelijk voor onze digitale identiteit?" is een van de vragen die vaak aan bod is gekomen gedurende de dag. Van de deelnemers vindt 55% dat de burger hiervoor zelf verantwoordelijk is. 37% vindt dat de verantwoordelijkheid bij de overheid belegd is. Slechts 9% is van mening dat de publieke sector hiervoor verantwoordelijk is. De discussie over dit thema kwam duidelijk naar voren in de presentatie van Wouter Welling, Coördinerend beleidsmedewerker digitale overheid, Ministerie van Binnenlandse Zaken en Koninkrijksrelaties en Allard Keuter, Business Development e-Identity, Currence.

Betrouwbaarheid



73% van de deelnemers geeft aan dat zij online ID verificatie alleen willen inzetten als deze 100% betrouwbaar is. 27% is het daar niet mee eens omdat zij van mening zijn dat betrouwbaarheid nooit voor de volle 100% te garanderen is.

De use case sessie van Peter Stroetenga ging bijvoorbeeld dieper in op hoe u ervoor kunt

zorgen dat u compliant kunt zijn in het Zorgdomein. VECOZO moet namens de aangesloten zorgpartijen in de keten een bepaalde mate van betrouwbaarheid hebben over de identiteit van de gebruikers, zodat overige ketenpartijen erop mogen vertrouwen dat gegevens worden gedeeld met de juiste gebruiker/ partij. Dit doen zij door een (soft)certificaat te verstrekken om een gebruiker van een zorgaanbieder te **authenticiseren** en vervolgens te **autoriseren**. Hiermee was VECOZO een voorloper in de zorg.

Privacy

De zaal is erg verdeeld als het gaat om privacy en het leveren van service. 49% vindt dat privacy belangrijker is dan dienstverlening, tegen 51% die het hiermee niet eens is. *“Wanneer je een persoon vraagt iets te vertellen over zijn of haar identiteit, zijn er vrij weinig mensen die zullen beginnen over de gegevens die ergens in databases staan. Mensen beginnen over hun cultuur, hun liefdes, hun hobby’s en waar ze vandaan komen. Gek genoeg is je digitale identiteit in het maatschappelijk verkeer misschien wel belangrijker dan je andere identiteiten.”* Aldus Joseph Kakisina, Product Manager Identity & Privacy, KPN in zijn ronde tafel sessie.

Dagvoorzitter e-Identity Congres blikt vooruit

9 januari 2018



Voor de [Toekomst van de Digitale Identiteit \(eID\)](#) citeer ik graag William Gibson: *“The future is already here — it’s just not very evenly distributed”*, de eID van de toekomst is er al, alleen ongelijk verdeeld.

Volgens mij is dat een goede reden om naar het congres te komen, namelijk kijken bij de burens hoe zij het doen. Als de toekomst er bij de burens al is dan wilt

u weten hoe u daarvan kunnen profiteren of dat u nog wat uitstel voor vernieuwing hebt. Hak het eID vraagstuk maar op in partjes en kijk welk partje voor uw organisatie te verbeteren is. eID partjes zijn o.a. bronregistratie, aanvraagproces, productie, uitgifte, activering en monitoring van eID gebruik, privacy.

e-Identity highlights

Ik noem een aantal highlights in het programma. De presentatie van Jacoba Sieders ABN-AMRO vanwege haar scherpe visie. Voorlichting over iDIN is belangrijk vanwege de potentie tot snelle groei en massa.

Heel praktisch is de uitleg over digitale handtekeningen. Er kan zoveel veel meer dan bedrijven denken. Een krabbel zetten met een muis of je vinger op een mobieltje kan gewoon. Rechtszaken die digitale handtekeningen betwisten worden niet genoemd. En let op het is veelzeggend dat de banken digitale handtekeningen met iDIN ondersteunen.

Voor de liefhebber spreekt Prof. dr. Didier Muewly over biometrische informatie, een interessante bijdrage van zijn hand valt te lezen in een whitepaper.

Nog even over de toekomst

Nieuw is niet altijd fijn of mooi. Zachtjes aan raakt eHerkenning ingevoerd. Is dat nu mooi? eHerkenning is net zo mooi als een vaatwasmachine in een restaurant. Je hebt het gewoon nodig, het kost geld en je moet de vaatwasser nog steeds in- en uitruimen. Maar niemand gaat daar nog met de hand afwassen. Liever eHerkenning dan papieren rompslomp, trouwens voor sommige zaken moet je eHerkenning gebruiken.

Nieuw, voor Nederland is Digi.me een beetje nieuw. Digi.me gaat over de “consent economy” veilig data delen, bescherming van klant privacy. Privacy komt ruim aan bod op het congres. Wat dat betreft zijn we in goed gezelschap van Professor Internetrecht Gerrit-Jan Zwenne.

Lastige keuze...

Het lastige van het congres is dat ik moet kiezen tussen twee In-Depth sessies: e-Identity in de Financiële sector en het verhaal over de gezondheidszorg de grootste sector die vraagt om een sterk beveiligde eID. Dat gaat goed komen.

Emma Lindley, een zeer ervaren eID specialist, vertelt over haar blik in de toekomst dat lijkt mij een waardige afsluiting van het congres.

Waarom is dit congres waardevol? De onderwerpen, de sprekers en het netwerk van deelnemers bieden de mogelijkheid om snel up to date te raken, wat u met een dag achter uw bureau studeren nooit realiseert. Daar komt bij dat dit congres nationaal is, het weet wat belangrijk is hier in onze Nederlandse setting en cultuur.

Als dagvoorzitter wil ik u een garantie bieden: **voor elke e-Identity vraag brengen wij u in contact met eID deskundigen, ter plekke of in twee handshakes na afloop.** Uw eID toekomst wordt weer een stukje voorspelbaarder.

Geschreven door: Jaap Kuipers, *Initiatiefnemer Platform Identity Management Nederland (PIMN)*

Identity management: 'Convenience en privacy bijten elkaar niet'

7 november 2018



Aldus Michiel van der Veen. Michiel van der Veen is thought leader op het gebied van digital ID en biometrie én spreker op het [e-Identity Congres](#). Identity management speelt een steeds belangrijkere rol in bedrijven. Met welke trends moet je rekening houden op het gebied van identity management de komende tijd?

Biometrie wordt steeds belangrijker in identity management volgens Michiel van der Veen: "Enerzijds om de veiligheid te verhogen, want biometrie is op een unieke manier gekoppeld aan mensen. Maar ook om het gemak te bevorderen; een selfie als 'wachtwoord' is nou eenmaal handiger dan wanneer je een code moet gebruiken. Het toenemende gebruik van mobiele authenticatie is belangrijk. Niet alleen voor zo'n 'selfie-wachtwoord', maar ook het gebruik van je toestel als token.

Ook wordt identity management een steeds grotere differentiator voor bedrijven. In de bankensector is die strijd al volop bezig: hoe gemakkelijk kunnen ze het hun klanten maken om te onboarden? Is mijn systeem gebruiksvriendelijker dan dat van de concurrent?

Overall blijft privacy een heel bepalende rol spelen, en die rol wordt alleen maar groter. Het is geen kwestie meer van achteraf kijken hoe we als bedrijf of instelling omgaan met privacy, maar van onszelf afvragen: hoe bouwen we privacy in? *Privacy by design* dus. Daarnaast heb je de ethische en juridische kant. Waar mag je verzamelde data voor gebruiken? Mag je ze gebruiken om geld mee te verdienen? Kijk bijvoorbeeld naar de Kamer van Koophandel, die onlangs in het nieuws was omdat er steeds meer klachten kwamen over het doorverkopen van gegevens uit hun database."

De (eind)klant heeft hoge eisen als het gaat om customer experience en dienstverlening van een bedrijf. Hoe kun je daaraan voldoen, maar ook juridisch en technisch je identity management op orde hebben?

"Ten eerste: die twee bijten elkaar niet; convenience en privacy zijn geen *zero* maar een *positive sum game*. Het is belangrijk om de goede technologieën te gebruiken en de goede architectuur voor je systemen. Maar ik realiseer me dat dat lastig op dit moment, omdat de markt, ook op het gebied van advies, heel gefragmenteerd is. Je moet bijna een specialist zijn om de juiste keuze te kunnen maken. Daarnaast moet je als bedrijf ook goed kijken naar de overheid: hoe ver gaat die in het waken over de privacy van burgers?"

In welke branches zijn op dit moment interessante initiatieven te vinden op het gebied van e-identity?

“De financiële sector speelt daarin een leidende rol, gedreven door wet- en regelgeving. Ze moeten hun klanten kunnen identificeren. Met dat doel wordt bijvoorbeeld iDIN ontwikkeld.

Daarnaast zijn er heel veel startups met interessante initiatieven, bijvoorbeeld op het gebied van behavioral biometrics, waarbij inschattingen worden gemaakt van bijvoorbeeld iemands geloofwaardigheid en kredietwaardigheid op basis van zijn bestaande gedrag en transacties.

Verder zijn er interessante startups op het gebied van self-sovereign identity en ondernemingen in de blockchain-hoek, wat daarmee samenhangt. Hoewel blockchain volgens mij nog steeds een beetje een modewoord is; ik beschouw het als een technologie op zoek naar een oplossing. Hoe dan ook is het ID-landschap heel divers.”

Waar ga je het over hebben tijdens je presentatie?

Het congres is gericht op ondernemingen, met als kernvraag: welke manieren zijn er voor het verwerken van identiteit in de businessprocessen? Mensen werken daar vaak aan in een cocon; ze kijken binnen hun eigen organisatie wat er allemaal bij komt kijken. Terwijl digitale identiteit juist een overstijgend begrip is, met als kernvraag: wie ben je in de online wereld?

Daar wil ik in ieder geval bewustwording over creëren. Wat gebeurt er als in de app van jouw specifieke bedrijf de identiteit van een individu wordt gecompromitteerd? En wat gebeurt er dan met die identiteit buiten de app, juist in die andere sectoren, waar dezelfde persoon dezelfde identiteit gebruikt?

Verder is mijn boodschap tijdens e-Identity: **ga weg van het centraliseren van allerlei systemen en kijk hoe identity management decentraal te regelen is**. Platforms waar ID-data centraal verzameld worden, daar komen we van terug te laatste tijd. Kijk naar het Facebook- en Cambridge Analytica-verhaal bijvoorbeeld. Maar is iDIN dan bijvoorbeeld de juiste oplossing voor jouw onderneming? Dat soort vragen komen tijdens het congres aan bod, en als het goed is komen deelnemers op dat gebied wijzer naar buiten.”

e-Identity congres: 'We hebben stappen gemaakt'

9 februari 2017

Op dinsdag 31 januari 2017 vond in Amsterdam het tweede e-Identity congres plaats. Het algehele gevoel na afloop: we hebben stappen gemaakt. Vorig jaar was het nog vooral aftasten. Nu worden de ontwikkelingen steeds beter zichtbaar. Hieronder in vogelvlucht wat resultaten en bevindingen van bezoekers.

Martijn Kaag is directeur van Connectis, een bedrijf dat naar eigen zeggen pionier is op het gebied van federatief identiteitsbeheer in de zorg. Connectis ontsluit informatie op een veilige manier, onder andere met DigiD. Connectis is onlangs overgenomen door SIDN, wat Connectis volgens Kaag heel veel mogelijkheden biedt, bijvoorbeeld goede beveiliging tegen bij DDoS-aanvallen. Dit geeft vertrouwen. Ze zijn op zoek gegaan naar een grotere partij en hebben deze gevonden in SIDN. Nu de BV is overgenomen door een stichting, heeft de aandeelhouder dus geen winstoogmerk meer, maar maken ze een gezonde marge om de continuïteit te waarborgen. 'Maar wel een bedrijf met (ook) een hoog maatschappelijk rendement, omdat we de overheid en het bedrijfsleven beschermen en daarmee de maatschappij veel geld besparen.'

Dagvoorzitter Jaap Kuipers vraagt Kaag om de toekomst te voorspellen. 'Dat is heel lastig, zo leert de geschiedenis. De markt zat er al vaker naast.' Stap voor stap schetst Kaag de historie van het fenomeen elektronische identiteit vanaf Microsoft Passport (1999) tot iDIN en eIDAS nu. Dat diverse partijen met hun eigen oplossing op de proppen kwamen, vindt Kaag niet zo vreemd. Echter, 'de markt zit niet te wachten op één oplossing.' Kaag herinnert het publiek eraan dat sommigen bij de lancering van DigiD in 2003 dachten dat het de potentie had een internationale standaard te worden. 'Maar dat pakte anders uit. Er werd, net zoals bij Diginotar, leergeld betaald. De overheid wil terecht niet meer afhankelijk wil zijn van één leverancier.'

Prikkelende stellingen

Kaag houdt zijn gehoor drie prikkelende stellingen voor:

- In 2025 zullen gebruikers van een digitale identiteit daar wél voor betalen, wat hen tot kritische gebruikers zal maken.
- In 2025 is minder dan 50% van hier aanwezige identiteitsverstrekkers nog als actief als leverancier van online identiteiten.
- In 2025 is er een internationale standaard voor veilig federatief inloggen. Ook is dan de daartoe benodigde technologie beschikbaar.

Volgens Kaag is de hamvraag: hoe bereid je je voor op je rol als ofwel aanbieder ofwel afnemer van digitale identiteit? 'Zorg dat je goed bent in je rol en focus je daarop. En: omarm diversiteit. Je kunt het je niet veroorloven stelsels uit te sluiten.'

- Rondetafelsessies -

Alternatieven naast Idensys en iDIN

Het middagprogramma staat voor een deel in het teken van rondetafelsessies. Tafel 1 wordt geleid Peter Vogelsang (Verbond van Verzekeraars). Thema: alternatieven naast Idensys en iDIN voor de private markt. Peter Vogelsang, beleidsadviseur bij Verbond van Verzekeraars, alternatieven voor Idensys en iDIN. Hij vertelt dat het Verbond van Verzekeraars bezig is een systeem te maken dat consumenten inzicht geeft in al hun verzekeringen. Alles overzichtelijk bij elkaar. Volgens Vogelsang zijn verzekeraars voorstander van diversiteit in middelen en zullen ze het toejuichen als Idensys een succes wordt. Hij vreest alleen dat iDIN en Idensys zich op een te kleine markt richten, namelijk uitsluitend de publieke sector. Wat ook niet meehelpt, is de onduidelijkheid over prijzen en attributen.

Aan de tafel wordt gespeculeerd over een Facebook-account als betrouwbare inlog. 'Als je al tien jaar een account hebt en tweehonderd vrienden hebt, dan biedt dat redelijk wat zekerheid over iemands identiteit. Zo'n ID maak je niet zomaar na.' Consumenten zijn veeleisend. Ze willen gemak maar ook veiligheid. Die lijken haaks op elkaar te staan. 'Tickets bij KLM reserveren via je Facebook-account, dat zien we wel zitten. Maar via Facebook een hypotheek afsluiten? Daar zijn we huiverig voor. De consument moet nu op allerlei plekken data achterlaten. Dat geeft een ongemakkelijk gevoel. Je zou het op één plek willen hebben en ook weer willen kunnen terughalen van organisaties als je dat wilt of nodig vindt.' Lang niet iedereen vertrouwt op eerlijke intenties bij bedrijven. 'Waarom wil TomTom toegang tot mijn foto's en mijn contacten? En ik kan het niet eens uitzetten!'

Wat kan Idensys voor u betekenen?

Aan Tafel 2 leidt Marije Jurriëns, business consultant eHerkenning/Idensys bij Logius, het gesprek. Het thema: wat kan Idensys voor u betekenen? Ze wordt bijgestaan door Jasper Jansen (Pazio) en Gideon Kreytz (Pharmeon). Recent zijn ruim twintig pilots gedraaid, onder meer bij overheden en gemeente, en bij Pazio en Pharmeon, vertegenwoordigd aan deze tafel. Jurriëns meldt dat Idensys ook buiten de overheid zal kunnen worden gebruikt.

De pilot bij Pazio had als doel een portal te bouwen voor ziekenhuizen en huisartsen. Alles bereikbaar vanaf één plek (website). Je logt gewoon bij je oude site in – de schil blijft vertrouwd – maar op de achtergrond draait een ander systeem.

Het aantal inloggen was volgens Pazio lager dan gehoopt. Dat kwam waarschijnlijk omdat mensen ook nog steeds met DidiD konden inloggen. Dat was bekend en vertrouwd en kreeg daarom vaak de voorkeur. Opvallend was dat nogal wat mensen zich opgaven voor de pilot, maar uiteindelijk toch afhaakten. Advies is daarom deelname lonend te maken en zorgaanbieders zover te krijgen dat ze deelname aan de pilot stevig promoten.

Zo'n duizend klanten van Pharmeon hebben een portaal. Pharmeon nam deel aan de pilot omdat ze een van de eersten waren die toegang gaven tot medische gegevens. Daarvoor hadden ze aanvankelijk een eigen authenticatiemethode ontwikkeld. Die werkte goed, maar de functionaliteit was beperkt. DigiD bleek voor veel eindgebruikers lastig, waardoor deelname aan het portaal afnam. Kreytz: 'Mijn ervaring is dat zaken heel simpel moeten zijn. Als je iets moet uitleggen, sta je al met 1-0 achter.'

e-Identity 2017 in vogelvlucht:

- Toekomstvisie biedt legio opties voor new business
- Focus op B2C, maar hoe met zakelijke klanten (B2B)?
- iDIN leidt nu wel. Logius/Idensys was wel open.
- We zijn stappen verder dan vorig jaar. We hebben meters gemaakt in de implementatie.
- Verzekeraars: 'Al je verzekeringen op een rij met Ideal, iDin, Idensys. Makkelijk!'
- Log in met één middel
- DNB mist presentatie over fraude en misbruik. Risico ligt nu bij de burger.
- Wat moet er nog gebeuren? Welke stap moeten we zetten? ABN Amro: awareness bij burger en consument moet verhoogd worden.
- Er moeten meer partijen aansluiten.

Reacties van bezoekers

- 'Focus op wat de consument eraan heeft'

'Betalen wordt steeds meer onderdeel van een proces, met allerlei services eromheen. Denk aan loyalty en dynamische check-out. Dan is ID wel heel belangrijk', aldus Michel van Westen (Buckaroo). 'Ik was er vorig jaar ook bij. Dit jaar is het niveau hoger. Er gebeurt meer. Wel vind ik dat sommige initiatieven langzaam gaan en dat de focus voor op Nederland is. Niet internationaal.' Tips voor de volgende editie? 'Ja, neem de big techs mee. Facebook, Google, dat soort clubs. Verder: minder focus op wat er technisch mogelijk is en meer op wat het oplost en wat de consument eraan heeft.'

- ‘Even babbelen met architectuur’

Aegon is bezig met een flinke digitalisatie om de klanten snel en goed van dienst te kunnen zijn’, aldus Irene Visser, product owner identity and access management. ‘Ik ben hier om te kijken wat de stand van zaken is en welke ontwikkelingen door de markt worden omarmd. Wat me vandaag verraste is dat er partijen zijn die zich opwerpen om voor organisaties zoals Aegon de toegang te verzorgen via verschillende vormen van E-identity, dus iDIN, DigiD enzovoorts. Identity brokers dus. Daar ga ik eens over praten met onze mensen van architectuur.

Volgend jaar meer B2B?

Inzicht opdoen in de verschillende identiteitschema’s, hun mogelijkheden en beperkingen en kijken hoe die identiteitschema’s kunnen aansluiten op het eigen platform van TransFollow. Dat was de reden voor software-ontwikkelaar Victor van der Wolf om e-Identity te bezoeken.

‘Wat ik sterk vond aan de opzet, was de aanwezigheid van de vele experts in combinatie met vertegenwoordigers van grote gebruikersgroepen zoals banken, de overheid en verzekeringsmaatschappijen en de discussies over de toekomst en de voor- en nadelen van de verschillende vormen van E-Identity. Wel lag de focus wat mij betreft te veel op B2C, terwijl wij meer op in het B2B-segment actief zijn. Iets voor volgend jaar?’

Zorg dat de gebruiker van een e-Identity altijd aan het roer staat

2 januari 2017



De technologische ontwikkelingen rond e-Identity gaan steeds sneller. Maar niet alle vernieuwingen moeten we per se gebruiken, stelt Allard Keuter, senior-adviseur bij de Betaalvereniging Nederland. Belangrijkste is dat de gebruiker altijd weet wat hij aan het doen is.

Hoe ziet het e-identity landschap eruit?

‘Online identity bestaat al heel lang. Kijk maar naar internetbankieren en bijvoorbeeld DigiD. Daarnaast bestaan er talloze andere e-identity’s. Zoals toegangspasjes voor bedrijven of UZI-passen voor het veilig uitwisselen van medische gegevens. Al deze oplossingen zijn stand-alone-systemen. Wat er nu ontstaat, is consolidatie naar een dynamische e-identity die overal toepasbaar is. Zoals iDIN.

Het interessante is dat we lang dachten dat iedereen uiteindelijk één online identiteit zou hebben. Maar nu weten we dat dat ons heel afhankelijk zou maken. Stel dat er een cyberattack komt of een storing, dan zitten we echt met de gebakken peren. Ook de overheid zegt nu: we hebben tien jaar DigiD, misschien zijn we daar wel te afhankelijk van geworden. Daarom ontstaan er nu meerdere systemen voor online identificatie.’

Wat is er nu al mogelijk met e-identity?

‘Het hang ervan af wat je onder e-identity verstaat. Als dat is: breder gebruikmaken van je inlogmiddelen, dan is er al veel mogelijk. Zoals toegang tot zorgdeclaraties, of je via je cookies laten herkennen door bol.com. Veel bedrijven zijn echter nog terughoudend met het aanbieden van online diensten, omdat ze niet goed in staat zijn iemands identiteit vast te stellen.

Want wat heeft een klant nodig? Een gebruikersnaam of e-mailadres en een wachtwoord. Een e-mailadres is snel te achterhalen en een wachtwoord is vaak iets als 12345. Dat is heel makkelijk te ontfutselen, dus beperkt betrouwbaar.

Daarom zijn de banken en de Betaalvereniging met iDIN begonnen, een dienst waarmee bedrijven kunnen gebruikmaken van de bancaire inlogmiddelen. Wanneer iDIN breed beschikbaar wordt, verwacht ik dat het aantal zaken dat via internet geregeld kan worden, snel zal groeien.’

Hoe staat het met de vervanging van DigiD voor consumenten?

‘Wat ik ervan weet, is dat DigiD meerdere verschijningsvormen krijgt en dat het systeem betrouwbaarder wordt. Paspoorten en rijbewijzen krijgen een NFC-chip en een pincode. Die chip kan worden uitgelezen op een DigiD-app op een telefoon met NFC of met een losse NFC-kaartlezer.

Ik denk dat er flink wat aandacht aan de communicatie met burgers besteed moet worden. Want je krijgt natuurlijk vragen als: welke gegevens kunnen instanties van mij inzien? Dat merken wij ook bij de ontwikkelingen van iDIN.

We kunnen vragen verwachten als: kan het bedrijf waarbij ik inlog ook mijn belastinggegevens zien, of mijn bankrekening? Dat is natuurlijk niet het geval, maar we moeten het wel duidelijk maken.

En áls er gehackt wordt met een identiteit die op meer plaatsen bruikbaar is, kan het goed misgaan. Daarom zijn er nu allerlei fraudedetectorsystemen bijgekomen. De controle bij inloggen is verscherpt.’

Wat zijn de 3 belangrijkste ontwikkelingen op het gebied van identity dit moment?

Mijn inziens zijn de volgende ontwikkelingen belangrijk:

‘Wat ik persoonlijk erg interessant vind, is biometrie. Er wordt continu gezocht naar betrouwbare lichaamskenmerken om iemands identiteit vast te stellen. De vingerafdruk, de gezichtsscan, of de vorm van hand en vingers. Maar een gezichtsscan zal niet altijd herkend worden, waardoor het niet goed werkt. Er is bijvoorbeeld een andere belichting, of iemand heeft net zijn bril af. Andere vormen zoals een vingerafdruk of de vorm van de vingers is dan een betrouwbaarder middel.

Waar ik verder aandacht voor wil vragen is geen technologische ontwikkeling, maar een blikrichting. De technologische ontwikkeling gaat maar door. Onder water kun je van alles voor gebruikers regelen, zonder dat de gebruiker het ziet. De vraag is of dat wenselijk is. Wij vinden van niet. Ongeacht de mogelijkheden van de techniek, moet steeds de gebruiker aan het roer staan, bewust zijn van wat hij doet. We moeten de gebruiker te allen tijde in het centrum zetten. Wanneer dat niet gebeurt, geeft dat mensen een ongemakkelijk gevoel. Voorbeelden daarvan zijn Facebook en Apple die van alles ontwikkelen om dingen “nog gemakkelijker” te maken en waarbij de gebruiker niet meer weet waar hij aan toe is.

Ten slotte vind ik het belangrijk dat de overheid niet alles in regels vat. Het gevaar van regels voor technologie is dat de huidige situatie bevriest, terwijl er over drie maanden misschien iets beters is uitgevonden wat dan niet mag. Dan is er weer aanpassing van de regels nodig, en we weten hoeveel tijd en geld dat kost. Dus laten we regels stellen waar het nodig is, vooral op wat we willen bereiken en verder de technologie de kans geven om dingen uit te proberen.’

Inloggen met je rijbewijs of met een selfie? De burger mag het zeggen!

22 december 2016



Binnenkort moeten burgers zelf kunnen kiezen hoe ze zich identificeren bij online contact met de overheid. Aan de techniek wordt nog hard gewerkt. Winfried de Valk, hoofd Toegangsdiensden van Logius, Ministerie van BZK, vertelt over het spanningsveld tussen politiek, techniek en de burger. ‘Het gebruikersperspectief is bepalend. Als mensen niet meedoen, dan houdt het op.’

Hoe ziet het identity landschap eruit?

‘Laat ik vooraf aangeven dat ik me beperk tot het overheidsdeel van het digital identity landschap, en dan dat deel waarvoor het burgerservicenummer (BSN) nodig is. In dat deel van het landschap hebben we DigiD. En dat vinden we niet genoeg. We willen méér en beter.

Waarom? Het is niet meer van deze tijd om afhankelijk te zijn van één manier van inloggen. Er wordt dit jaar 250 miljoen keer ingelogd met DigiD. Als DigiD zou uitvallen, ligt een groot deel van de online overheidsdienstverlening plat. Bovendien willen organisaties ook diensten digitaliseren die nu alleen met een face-to-face identiteitscheck kunnen worden afgenomen. Daar is het huidige DigiD niet voor bedoeld. Daarom zijn we bezig andere, sterkere inlogmethoden te ontwikkelen, ook in samenwerking met private partijen. Al deze inlogmethoden moeten aan de strenge eisen van de overheid voldoen. Straks kunnen burgers zelf kiezen hoe zij zich online identificeren en wordt het voor de overheid mogelijk om meer diensten digitaal aan te bieden.’

Wat is er nu al mogelijk met e-identity?

‘De helft van alle interacties tussen overheid en burger gaat nu al digitaal. Bij een groot deel daarvan is het nodig om in te loggen. Daarvoor gebruiken mensen dus hun e-identity. Iets vergelijkbaars gebeurt al tussen bedrijven en overheid, zoals met de belastingaangifte. De overheid moet zorgen dat dit zo blijft, en die structuur versterken.’

Hoe staat het met de vervanging van DigiD voor consumenten?

‘Dat is een hardnekkig misverstand: DigiD wordt niet vervangen maar versterkt, naar een hoger plan gebracht. Het merk blijft, maar de techniek wordt anders. Kortweg komt het erop neer dat je straks met een DigiD-app op je mobiele telefoon de chip op je rijbewijs of identiteitskaart uitleest om te kunnen inloggen. Zo komen er meer inlogmethoden: Idensys gaat met verschillende inlogmanieren werken, zoals gezichtsherkenning via een selfie.

Met alle innovaties wordt nog druk geëxperimenteerd. De eerste verbeterde versie van DigiD – DigiD Substantieel – wordt de eerste helft van 2017 beschikbaar. De andere variant, DigiD Hoog, volgt later. Inloggen via Idensys is nu al mogelijk en levert een betrouwbare identiteitscheck tot op het hoogste betrouwbaarheidsniveau. Verder kunnen burgers straks ook inloggen met hun persoonlijke bankmiddel. Ingewikkeld? Ja, het zal straks inderdaad een hele opgave worden om al deze varianten op een simpele manier aan de burger duidelijk te maken.’

Wat zijn de 3 belangrijkste ontwikkelingen op het gebied van identity dit moment?

‘Allereerst de techniek zelf. De ontwikkelingen gaan zeer snel en zijn onvoorspelbaar. Weet je hoe lang wij smartphones hebben? Nog geen tien jaar. En bijna alles wat we nu technologisch neerzetten, maakt gebruik van smartphonetechnologie. Het kan dus zomaar zijn dat over twee jaar alles ineens weer anders is.

Dan is er de eIDAS-verordening. Deze Europese verordening wordt in september 2018 van kracht en komt erop neer dat Europese burgers met hun eigen inlogmiddel kunnen inloggen bij overheidsdienstverleners in een andere EU-staat. Je kunt je voorstellen dat dit voor de techniek geen sinecure is. Met de Europese maatregel wordt het makkelijker en veiliger om binnen Europa online zaken met elkaar te doen. Bijvoorbeeld binnen het hoger onderwijs. Buitenlandse studenten die meedoen aan een uitwisseling, kunnen dit dan al vanuit hun eigen land regelen. DigiD en Idensys willen aan de eIDAS-normen voldoen zodat ze over de grens kunnen worden gebruikt.

De derde ontwikkeling die ik heel belangrijk vind: ongeveer twee à drie miljoen Nederlanders zijn niet digitaal vaardig. Allereerst is dat de groep functioneel analfabeten. Daarnaast bestaat een groep mensen die wel kunnen lezen, maar die de aansluiting met de digitalisering hebben gemist. Wanneer wij als overheid digitaal zaken willen doen met de burger, moeten we die mensen niet uitsluiten. Juist omdat we zulke hoge ambities hebben, wordt die groep steeds belangrijker. Er is nog geen oplossing voor. Mensen geven nu bij wijze van spreken een geeltje met hun codes aan de buurman met de vraag of die even iets voor ze wil regelen.

Bij Logius hebben we veel contact met de burgers. En we beseffen dat het gebruikersperspectief bepalend is. Als mensen niet meedoen, dan houdt het op.’

We gaan onvoldoende zorgvuldig om met privacygevoelige informatie

5 januari 2016

Voorafgaand aan het [e-Identity congres](#) geeft Haydar Cimen, Director Strategic Development KPN, zijn visie op het gebied van de toekomst van de e-Identity. Verder bespreekt hij welke ontwikkelingen er gaande zijn en wat er nodig is om die volgende stap in de digitale identiteit te maken is.

Welke ontwikkelingen zijn er op het gebied van identificatie & authenticatie van klanten?

Veel van onze klanten staan aan de vooravond van verdere verdigitalisering van haar dienstverlening. Deze dienstverleners dienen op korte termijn sterkere authenticatie voorzieningen te realiseren dan voorheen. Waar nu nog gebruikersnamen/wachtwoorden worden gebruikt (Stork niveau 1 en 2) moeten er alternatieven worden ingezet waarbij er hogere mate van zekerheden (Stork 3+) noodzakelijk zijn voor nieuwe generatie toepassingen zoals bijvoorbeeld privacy gevoelige patientendossiers en rechtsgeldige transacties.

“De technologie is gereed om de volgende stappen te zetten in verdere verdigitalisering van de bedrijfsprocessen van onze klanten en de samenleving.”

Welke initiatieven zijn er om identificatie en authenticatie van personen (burgers, consumenten) en bedrijven op de digitale toekomst in te kunnen richten?

KPN biedt al vele jaren identity- en crypto infrastructures voor stelsels zoals eHerkenning/Idensys. Daarnaast ontwikkelen wij momenteel veel mobiele applicaties die als identiteitsmiddel functioneren en geschikt zijn voor verschillende doelgroepen. Het valideren van gebruikers en het koppelen van de natuurlijke / rechtspersoon aan hoogwaardige identiteitsmiddelen vindt momenteel veelal plaats door middel van face-2-face validatie aan de deur. Wij ontwikkelen daarnaast in samenwerking met verschillende partners (privaat/wetenschap) nieuwe generatie identificatie-op-afstand processen om op grote schaal gebruikers/burgers/consumenten uit te rusten met een nieuwe generatie digitale identiteit.

Wat is er nodig om de volgende stap in digitale identiteit te maken?

De technologie is gereed om de volgende stappen te zetten in verdere ver-digitalisering van de bedrijfsprocessen van onze klanten en de samenleving. Hiervoor is het noodzakelijk dat er afsprakenstelsels ontstaan zoals Idensys die eenduidigheid creëren in de te gebruiken identiteitsmiddelen. Zonder dergelijke afspraken en standaarden kunnen dienstverleners via haar digitale portalen niet eenduidig een gebruiker identificeren.

De publieke- en private- identiteitsmiddelen dienen op grote schaal beschikbaar te zijn voor de consument en burgers in Nederland. Dienstverleners kunnen hierdoor hoogwaardige en privacy-gevoelige processen die eerder op papier dienden plaats te vinden verdigitaliseren.

Hoe zit het met de opvolger van DigID/eHerkenning?

Het nieuwe Idensys stelsel biedt een multimiddelen strategie waarbij consumenten/burgers zelf kunnen kiezen met welke id's men inlogt bij een dienstverlener of webshop. Dit Idensys stelsel zal per dec 2015 in productie gaan en er zullen in 2016 ca. 20 pilots starten met overheidsdienstverleners en portalen in de private-sector. De verwachting is dat huidige "stelsels" zoals PKIOverheid, BAPI, SBR, Digid, eHerkenning zullen opgaan in dit nieuwe Idensys stelsel. Ook zal het Idensys stelsel de interoperabiliteit met Europe mogelijk maken waardoor ingezetenen vanuit andere lidstaten in de nabije toekomst kunnen interacteren met andere overheden en private ondernemingen.

Hoe is het gesteld met de privacy en bescherming van de klant, nu en in de toekomst?

Privacy is essentieel in deze identiteitsvraagstukken en staat voorop in de KPN-strategie op dit punt. Momenteel is het slecht gesteld met de privacy van de burger en zeker van de consument. Er wordt door veel partijen onvoldoende zorgvuldig omgegaan met privacygevoelige informatie. Ook wordt er veel afgeleide informatie gecollecteerd en verwerkt door advertentie/profiling bedrijven. Deze informatie zwerft wereldwijd rond en gebruikers zijn niet meer in staat om te achterhalen wie/welke data van de gebruikers heeft ontvangen en verwerkt. KPN biedt oplossingen waarbij de gebruikers-anonimiteit wordt gewaarborgd door middel van privacy protectie- en privacy-enhancing technologieën.

In dit kader werkt KPN samen met de wetenschap en andere kennispartners om zoveel mogelijk zekerheden te creëren voor de consument en de keuze om informatie te verstrekken aan portalen over te laten aan de gebruiker (user consent). Voorbeeld: het is niet noodzakelijk om een geboortedatum op te geven wanneer een ja/nee voldoende is om te bepalen of een gebruiker volwassen is. Nieuwe ontwikkelingen zoals Attribute Based Credentials bieden momenteel de mogelijkheid om gedoseerd en per attribuut (bv kledingmaat, BSN nummer, woonplaats,...) authenticatie mogelijk te maken. De gebruiker bepaalt welke informatie hij wil/mag aanbieden aan de partij die hier om vragen bij authenticatie of autorisatie.

e-Identity: Het borgen van de privacy van de klant is essentieel

11 november 2015



Voorafgaand aan het [e-Identity congres](#) interviewde wij **Maarten Wegdam**, managing partner InnoValor. In het interview geeft hij zijn visie op de ontwikkelingen van identificatie & authenticatie van klanten en wat er nodig is om de volgende stap in digitale identiteit te maken.

“Onze smartphone is het ultieme persoonlijke apparaat, die dragen we altijd bij ons. En we zijn er zuiniger op dan op onze portemonnee.” - Maarten Wegdam, managing partner, [InnoValor](#)

Welke ontwikkelingen zijn er op het gebied van identificatie & authenticatie van klanten?

Steeds meer realiseren organisaties zich dat identificatie & authenticatie van klanten niet hun core business is. Dit zelf doen is niet alleen duur, maar in veel gevallen ook minder veilig en minder gebruikersvriendelijke dan dit aan gespecialiseerde derden over te laten, zogenaamde identiteitsproviders of authenticatiediensten. In het overheidsdomein kent iedereen dit al met DigiD, die als een soort derde partij burgers authenticiseert voor allerlei overheidsdiensten en anders diensten die BSN mogen gebruiken (zorg en pensioen).

Dat dit soort herbruikbare identiteiten een goed idee is heeft, uitzonderingen daargelaten zoals in het hoger onderwijs, nog niet echt geleid tot een grootschalige introductie van herbruikbare identiteiten. Redenen hiervoor zijn dat het erg veel vertrouwen eist van de afnemende partij (bv een online retailer) in de identiteitsprovider, onduidelijkheid over businessmodellen, market entry uitdagingen (kip-ei probleem) en privacy uitdagingen.

Welke initiatieven zijn er om identificatie en authenticatie van personen (burgers, consumenten) en bedrijven op de digitale toekomst in te kunnen richten?

Er zijn vele initiatieven, misschien is dat wel één van de problemen. Als dit geen dagelijkse kost is, is het lastig bij te houden. Ik noem wat belangrijke initiatieven. In Nederlands zijn het met name Idensys, BankID, een nieuw publiek middel en versterkingen van DigiD. Idensys is de nieuwe naam van het eID Stelsel, een afsprakenstelsel beheert door de Nederlandse overheid waarin private identiteitsproviders gebruikers authenticiseren voor publieke en private partijen. Idensys kan gezien worden als een doorontwikkeling van eHerkenning, een vergelijkbaar afsprakenstelsel gericht op business-2-government diensten. BankID is een gezamenlijk initiatief van de Nederlandse banken, die van plan zijn hun bancaire identiteiten te gaan hergebruiken vergelijkbaar het Idensys.

Er is ook een initiatief van de Nederlandse overheid tot een veilig publiek middel voor toegang tot publieke diensten, door rijbewijs en identiteitskaart hiervoor geschikt te maken. In de tussentijd werkt de Nederlandse overheid ook aan DigiD versterking door een DigiD app te introduceren en het mogelijk te maken een rijbewijs, paspoort of identiteitskaart te gebruiken als authenticatiemiddel bovenop DigiD basis, door de contactloze chip uit te lezen met een NFC reader of smartphone.

Kortom, een bult ontwikkelingen die hopelijk elkaar versterkend allemaal samenkomen in één afsprakenstelsel. Maar of en wanneer dit gebeurt is nog erg spannend.

Vanuit Europe wil ik met name eIDAS noemen, dit is een EU-verordening waarbinnen landen elkaars digitale identiteitsoplossingen moeten gaan accepteren. Als laatste wil ik FIDO noemen, dit is een veelbelovende nieuwe standaard waarmee het makkelijk wordt allerlei verschillende authenticatiemiddelen te koppelen, zodat een Bring-Your-Own-Authentication haalbaar wordt: mensen kunnen zelf kiezen welk authenticatiemiddel ze willen gebruiken.

Wat is er nodig om de volgende stap in digitale identiteit te maken?

Ik ga het nu even niet over de diverse initiatieven hebben, of het gebrek aan besluitvaardigheid en tempo. In plaats daarvan richt ik me op twee meer inhoudelijk stappen: online identiteitsverificatie en mobile-first identity. Van oudsher is het nodig om bij het uitreiken van betrouwbare digitale identiteiten, in betrouwbaarheidsniveaus STORK 3 en 4, om een face-2-face identiteitscontrole uit te voeren. Maar dit is duur en gebruikersonvriendelijk, en de technologie is inmiddels verder. We kunnen mijns inziens nu ook serieus werk gaan maken van online identiteitsverificatie processen, die gebruik maken van eerder wel fysiek uitgereikte identiteiten, bijvoorbeeld het op afstand uitlezen van de chip van een paspoort met een smartphone, in combinatie met een videochat. In Duitsland is men hier al verder mee, maar ook in Nederland zie ik dat de tijd rijp is om dit te gaan doen.

Een andere, parallel, stap is wat ik noem mobile-first identity. Onze smartphone is het ultieme persoonlijke apparaat, die dragen we altijd bij ons, en we zijn er zuiniger op dan op onze portemonnee. Identiteitsoplossing zouden ook meer de mobiel centraal moeten stellen, in plaats van smartcards of hardware tokens. Voor betalingen hebben we binnenkort met mobile payments als geen pasjes meer nodig, maar ik denk dat voor digitale identiteiten we snel daarna ook geen portemonnee meer nodig hebben.

Hoe is het gesteld met de privacy en bescherming van de klant, nu en in de toekomst?

Het is essentieel dat we dit goed borgen, niet alleen omdat de wet dit eist, niet alleen omdat dit ethisch vereist is, maar omdat dit de basis is van vertrouwen van de gebruiker in digitale identiteiten, en onlinedienstverlening in het algemeen. We moeten hier goed gebruik maken van de laatste ontwikkelingen in privacy-enhancing technologieën, en waar deze er (nog) niet zijn, of te onvolwassen, is een goede maatschappelijke dialoog nodig om keuzes te maken. En, mijns inziens, ook deskundige en goede toezichthouders hierop.

Het is geen simpele materie, ook niet voor volksvertegenwoordigers en de rechtelijke macht. Een zinvolle maatschappelijk dialoog en effectief toezicht vereisen allereerst transparantie, over welke informatie er nu over wie met wie wordt gedeeld, en met welk doel. Dat ontbreekt nog weleens. En hoewel er experts zijn die hier minder vertrouwen in hebben, blijf ik geloven in informed consent, dus controle houden bij de gebruiker over zijn data. De nieuwe privacy verordening van de EU, wanneer deze eindelijk in werking treedt, zou ook moeten helpen.

Belangrijk is om onderscheid te maken tussen verschillende vormen van identificatie en authenticatie

4 december 2015



Voorafgaand aan het e-Identity congres geeft Arnold Roosendaal, auteur De Informatievuik en werkzaam bij TNO, zijn visie op het gebied van de toekomst van de e-Identity. Verder bespreekt hij welke ontwikkelingen er gaande zijn en wat er nodig is om die volgende stap in de digitale identiteit te maken is.

“Er wordt hard gewerkt aan de opvolger van DigID/e-Herkenning, maar de echte uitkomst is nog steeds onduidelijk”

Welke ontwikkelingen zijn er op het gebied van identificatie & authenticatie van klanten?

Er zijn veel ontwikkelingen gaande. Belangrijk is om onderscheid te maken tussen verschillende vormen van identificatie en authenticatie, met name in het licht van wat nodig is. Voor verschillende diensten kunnen immers verschillende gewenste niveaus van zekerheid over een identiteit bestaan. Flexibel daarmee omgaan kan helpen voorkomen dat meer geïnvesteerd wordt dan nodig. Waar mogelijk kan daarom goed aangesloten worden op bestaande infrastructuur en middelen.

Welke initiatieven zijn er om identificatie en authenticatie van personen (burgers, consumenten) en bedrijven op de digitale toekomst in te kunnen richten?

Er zijn vele initiatieven. De mooiste zijn naar mijn idee diensten die bijdragen aan vertrouwen en veiligheid in communicatie en dienstverlening. Als dienstverlener wil je immers vaak precies weten met wie je te maken hebt. Maar vaak is dat ook niet relevant, als maar vaststaat dat je betrouwbaar bent en aan bepaalde vereisten voldoet. Voorbeelden van initiatieven die hierbij kunnen helpen zijn de IRMA card en TrustTester. Een interessant verschil tussen die twee is nog dat de IRMA card uitgaat van het gecontroleerd verstrekken van attributen, terwijl TrustTester uitgaat van het verstrekken van informatie over de juistheid van een claim, zonder de attributen zelf te verstrekken.

Wat is er nodig om de volgende stap in digitale identiteit te maken?

Het belangrijkste wat nodig is is duidelijkheid. Nu is er nog veel verwarring omdat alle typen diensten en middelen worden gekoppeld aan Idensys. Daardoor is er veel verwarring over wat nu eigenlijk eID middelen zijn, wat aanvullende diensten zijn, wat ze met elkaar te maken hebben,

en vooral welke toegevoegde waarde er waar te behalen valt. Het gevolg is dat er veel geconcentreerd wordt tussen aanbieders, maar voorlopig nog zonder 'winnaar'.

Ook is het gevolg dat de overheid die beslissingen moet nemen over het eID stelsel het overzicht kwijt is geraakt en hoofdzakelijk gekleurde verhalen hoort. Het geheel proces wordt daardoor vertraagd en leidt zeker niet logischerwijs tot een betere toekomst voor digitale identiteiten.

Hoe zit het met de opvolger van DigID/eHerkenning?

Daar wordt hard aan gewerkt, maar de echte uitkomst is nog steeds onduidelijk.

Hoe is het gesteld met de privacy en bescherming van de klant, nu en in de toekomst?

Je ziet dat er op het gebied van privacy en bescherming van de klant veel te winnen valt. Het is mooi om te zien dat er verschillende partijen zijn die hier gericht naar kijken en ook mooie oplossingen bedenken. Een kanttekening is dat vaak vanuit een technologisch perspectief gedacht wordt, terwijl straks de gebruiksvriendelijkheid bepalend zal zijn voor het slagen van die oplossingen.

Als een oplossing niet gebruiksvriendelijk is zal er immers weinig gebruik van gemaakt worden. En dat is wel cruciaal vanuit het idee dat het gebruik van digitale identiteiten en online transacties in een veelheid aan vormen alleen nog maar zal toenemen.

Idensys moet de opvolger van Digid/eHerkenning worden

11 november 2015

De toekomst van de digitale identiteit, hoe staat het daarmee? En hoe waarborgen we de privacy en veiligheid van consumenten en bedrijven? Belangrijke vraagstukken! **Robert Garskamp**, oprichter IDnextplatform, gaat in onderstaand interview in op de noodzaak en behoefte van een betrouwbaar systeem, privacy en de opvolger van Digid.

“Digid is (op dit moment) een single point of failure en het gebruik van idensys moet dit oplossen: Het is duidelijk dat de organisatorische en financiële gevolgen voor de dienstverlening bij uitval van DigiD erg groot kunnen zijn”

Welke ontwikkelingen zijn er op het gebied van identificatie & authenticatie van klanten?

Identificatie en authenticatie gaat steeds meer een significante en zichtbare rol spelen in de digitale dienstverlening en dus ook in de maatschappij. Convergentie van authenticatie middelen lijkt hierin nog niet een belangrijke rol te spelen. Momenteel worden er verschillende soorten authenticatie middelen door dienstverleners aangeboden waardoor er een (grote) keuze is voor de consument maar dat ook een significante groei aan de digitale sleutelbos. Door het gebruik van twee factor authenticatie wordt de betrouwbaarheid in het gebruik van de dienstverlening wel verhoogd. Ook is er een significante toename in mobiele toepassingen waardoor het mogelijk is om voor consumenten op een laagdrempelige manier zaken te kunnen doen met commerciële dienstverleners.

Standaardisatie is daarbij een belangrijk component in de vervolwassenwording van de mogelijkheden op het gebied van authenticatie. Zonder standaarden is het gewoonweg niet mogelijk om een betrouwbare, consistente en ook veilige dienstverlening te kunnen aanbieden. Ook binnen de Europese Commissie wordt elektronisch identificatie en authenticatie gezien als een van de belangrijkste voorwaarden voor interoperabiliteit binnen de Europese Landen. Een van de pijlers is de ‘Digital single market’ dat zich ten doel stelt om de digitale mogelijkheden voor mensen en bedrijfsleven binnen Europa te verbeteren en interoperabel te maken.

Welke initiatieven zijn er om identificatie en authenticatie van personen (burgers, consumenten) en bedrijven op de digitale toekomst in te kunnen richten?

Er zijn verschillende initiatieven gaande op het gebied van identificatie en authenticatie. Een initiatief is het programma Digitaal 2017. De overheid heeft dit programma gestart dat het mogelijk maakt voor de burger om (vanaf 2017) zaken met de overheid op digitale wijze kunnen afhandelen. Onderdeel hiervan is idensys – de opvolger van digid genaamd idensys. Dit platform (voortbordurend op het eHerkenning netwerk) moet de nieuwe standaard worden dat burgers en bedrijven veilige en betrouwbare toegang verleent tot online dienstverlening van overheid en bedrijfsleven.

Daarnaast werken de banken (gezamenlijk) aan een pilot i.s.m. de Belastingdienst waarbij het mogelijk is om met een bankmiddel in te loggen op digitale diensten van de belastingdienst. Een soortgelijk pilot is er ook met een verzekeringsmaatschappij. Last but not least is de overheid ook nog een pilot gestart voor gebruik van een publiek middel waarbij het mogelijk moet zijn om een rijbewijs/identiteitskaart in te loggen bij publieke dienstverleners.

Wat is er nodig om de volgende stap in digitale identiteit te maken?

De convergentie van de fysieke (offline) en online wereld gaat met rasse schreden voort. Steeds meer consumenten en burgers begeven zich op het internet voor (digitale) zaken. De bescherming van de digitale identiteit is essentieel ter preventie van o.a. identiteitsfraude. Een (gestolen) digitale identiteit is geld waard voor de dienstverleners. De 'digitale identiteit' van internetgebruikers vertegenwoordigt in Europa momenteel een economische waarde van zo'n €450 miljard. Tot 2020 groeit de marktwaarde van digitale identiteit met 14% per jaar. De economische waarde van digitale identiteit heeft (minimaal) twee onderdelen. De directe inkomsten van het bedrijfsleven (zo'n €100 miljard) en de indirecte waarde voor consumenten door de meerwaarde en gemak die digitale diensten opleveren (€250 miljard). Digitale identiteit en de data wordt ook wel als de brandstof van de digitale economie beschouwd.

Hoe zit het met de opvolger van DigiD/eHerkenning?

Idensys moet de opvolger van Digid/eHerkenning worden. De standaard voor identificatie en authenticatie vanuit de burger naar de overheid. Vanuit de overheid is de duidelijk gesteld dat er een noodzaak en behoefte is aan een middel met een hoog betrouwbaarheidsniveau voor burgers. Dit is essentieel om de digitale dienstverlening te kunnen uitbreiden, veiliger maken en verbeteren. Dit is alleen mogelijk wanneer er adequate authenticatiemiddelen beschikbaar zijn.

Digid is (op dit moment) een single point of failure en het gebruik van idensys moet dit oplossen: Het is duidelijk dat de organisatorische en financiële gevolgen voor de dienstverlening bij uitval van DigiD erg groot kunnen zijn. Aangezien er naar verwachting meer dan 200 miljoen authenticaties in 2015 zijn via Digid. Daarom is de keuze voor een multimiddelenstrategie een belangrijke vereiste voor een robuuste toekomst. Vanuit burgerperspectief betekent dit keuzevrijheid. Alleen laat de realisatie van idensys nog even op zich wachten. Belangrijke oorzaken hierin zijn dat het thans zeer complex en onoverzichtelijk is en het ontbreekt aan daadkracht op politiek niveau. Gebrekkige communicatie is ook een belangrijke oorzaak. En het lijkt erop dat niemand het geheel overziet en ook niet de besluiten neemt. De aansluiting tussen private en publiek domein lijkt niet de synergie op te leveren die gewenst is. Besluitvorming vanuit de politiek is gewenst en noodzakelijk om een volgende stap te maken.

Hoe is het gesteld met de privacy en bescherming van de klant, nu en in de toekomst?

Privacy betekent dat iemand dingen kan doen zonder dat de *buitenwereld* daar inbreuk op maakt of weet van heeft. Privacy is dan ook een belangrijk maatschappelijke kwestie in de digitale wereld. Net als in de fysieke wereld heeft een mens recht op privacy in de digitale wereld.

Maar in de digitale wereld is het vaak onduidelijk wat er met je gegevens nu gebeurt, waar het wordt opgeslagen en hoe ze worden gebruikt. Controle dan wel zeggenschap hebben over je eigen gegevens en de preventie voor de distributie van de gegevens lijkt een heikele kwestie.

Privacy is in de wet wel verankerd maar dat is erg gericht op de bescherming van privacy in de fysieke wereld. De bescherming van de burger op dit vlak krijgt daardoor meer en meer onaangename trekken. De Snowden affaire spreekt hierover boekdelen. Er wordt geroepen om het centrale belang van burgerrechten in het digitale tijdperk te erkennen. Maar het zal nog even duren voordat dit het geval is.