Deloitte.

In samenwerking met **Grabowsky**

Digitale identiteit en de noodzaak van een actieve overheidsrol

Waar een klein land groot in kan én moet zijn

Auteurs

Anouk Mulder
mulder@grabowsky.com

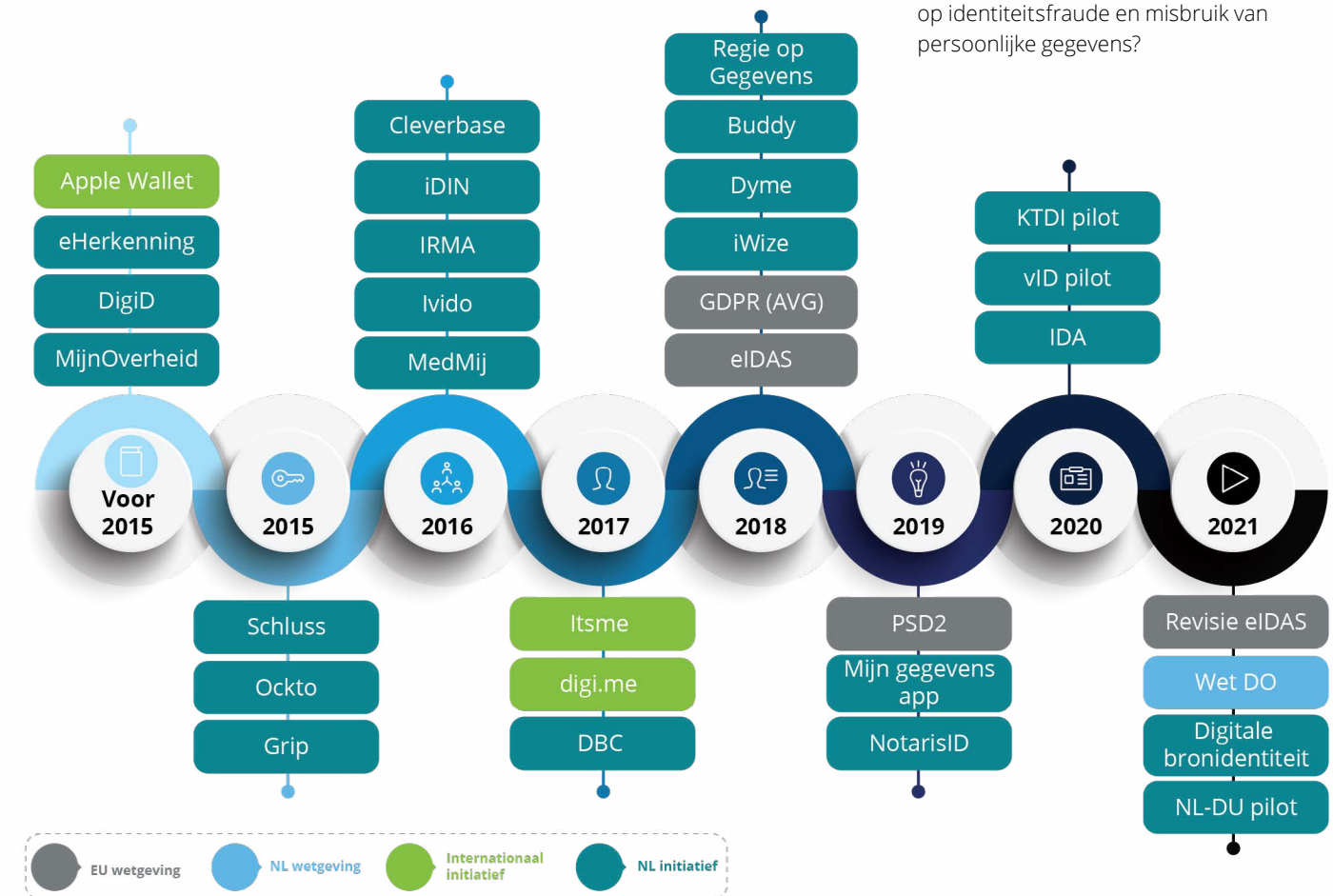
Suzanne van Oosterum
van.oosterum@grabowsky.com

Mathijs Brouwer
mabrouwer@deloitte.nl

Een identiteitsbewijs, zoals een paspoort of een rijbewijs, of een attribuut, zoals een Burgerservicenummer (BSN), zijn belangrijke representaties en bewijsstukken van iemands identiteit. In de fysieke wereld wordt een identiteitsbewijs vooral gebruikt om aan te tonen wie je bent bij gelegenheden als het kopen of het huren van een huis, het openen van een bankrekening of het afsluiten van een verzekering. Een identiteitsbewijs is daarmee van grote waarde, maar daardoor ook een groot doelwit voor identiteitsfraude en misbruik door kwaadwillenden.

In de digitale wereld is dit niet anders. Overheidsorganisaties, bedrijven, maar ook burgers willen zekerheid hebben dat de persoon of het bedrijf waarmee zij digitaal zakendoen ook daadwerkelijk diegene is en/of de benodigde bevoegdheden heeft. In de fysieke wereld zijn er goede manieren om dit te controleren en te verifiëren door gebruik te maken van echtheidskenmerken en waarneembare kenmerken op het identiteitsbewijs. Online is dit moeilijker te bewijzen en te controleren. Om zekerheid te verkrijgen, wordt er nu nog vaak teruggevallen op een "kopietje paspoort", met alle risico's van dien.

Een betrouwbare digitale identiteit, waaraan een aantal geverifieerde attributen of claims gekoppeld is, zoals een naam, BSN of een bewijs dat je ouder dan 18 bent, biedt grote meerwaarde en gebruiksgemak in het digitaal zakendoen met elkaar. Het is dan ook geen verrassing dat er inmiddels verschillende publieke en private initiatieven ontstaan die gebruikmaken van verschillende technologieën, zoals te zien in ***Figuur 1.*** Toch zijn er al jaren grote discussiepunten over het nut en de noodzaak van een digitale identiteit. Want wegen de voordelen, zoals gebruiksgemak, wel op tegen de nadelen, zoals risico's op identiteitsfraude en misbruik van persoonlijke gegevens?



Figuur 1 Overzicht van initiatieven en wet- en regelgeving (niet uitputtend)

Het vraagstuk is nu, mede door de coronacrisis, in een stroomversnelling geraakt en heeft tot structurele veranderingen geleid. We moesten opeens massaal vanuit huis werken, hierdoor werden activiteiten die normaal fysiek plaats zouden vinden, zoals aandeelhoudersvergaderingen, digitaal georganiseerd. Bij dit soort activiteiten is het essentieel dat diegene die aan de andere kant van het scherm zit ook daadwerkelijk diegene is en/of de benodigde bevoegdheden heeft.

De Kamerbrief over een visie digitale identiteit en het voorstel voor een Europese verordening voor een Raamwerk voor een Europese digitale identiteit zijn belangrijke facilitators om een geverifieerde digitale identiteit mogelijk te maken. Met name de plannen van de Europese Unie (EU) zijn ambitieus: in 2023 moet het raamwerk voor een Europese digitale identiteit staan. Om deze ambities vanuit de EU waar te kunnen maken, dienen de globale plannen, zoals beschreven in de Kamerbrief, geconcretiseerd te worden. Maar, wat is er nodig van de Nederlandse overheid om dit tot een succes te maken en wat zijn hierin de uitdagingen?

Om de plannen te realiseren, zal de Nederlandse overheid de huidige koers om moeten gooien. De ontwikkelingen in de markt en op Europees niveau vragen een actievere overheidsrol bij het creëren van vertrouwen in een digitale identiteit, waarmee zorgvuldige identificatie, betrouwbare authenticatie en gecontroleerde autorisatie in een samenwerkend stelsel mogelijk gemaakt worden.

Een eerste stap hierin is de samenwerking die Nederland is aangegaan met Duitsland.[3] Hierbij zullen de twee landen een grensoverschrijdende pilot starten en voorbeelden en werkwijzen delen bij het ontwikkelen van middelen om een digitale identiteit te gebruiken. De uitkomsten van de pilot zullen dienen als input voor het raamwerk voor een Europese identiteit.

---

[1] Kamerstukken II 2020/21, 26643, nr. 743. https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z02985&did=2021D06488

[2] https://ec.europa.eu/commission/presscorner/detail/en/IP_21_2663

[3] https://www.rijksoverheid.nl/actueel/nieuws/2021/09/23/nederland-gaat-met-duitsland-werken-aan-digitale-identiteit

Rond het onderwerp digitale identiteit spelen een aantal belangrijke uitdagingen. Denk hierbij aan de wettelijke basis, maatschappelijke acceptatie, digitale inclusie en het borgen van een correcte informatievoorziening. In dit artikel focussen wij ons op de meest fundamentele uitdagingen welke moeten worden beheerst om het gebruik van een digitale identiteit betrouwbaar en breed toepasbaar te maken - zowel binnen als buiten de overheid. Deze uitdagingen worden aan de hand van drie dilemma's uitgewerkt.

Digitale Identiteit – Wat verstaan we er onder?
Als aan tien verschillende personen gevraagd wordt wat 'digitale identiteit' precies inhoudt, worden er waarschijnlijk tien verschillende antwoorden gegeven. Dit komt onder andere door de vele initiatieven die zijn vormgegeven rondom de digitale identiteit. Alleen al binnen overheidsorganisaties zijn er pilots met virtual digital identity (vdI), Known Traveller Digital Identity (KTDI), Self Sovereign Identity (SSI), DigiD, MedMij en het programma Regie op Gegevens. In dit artikel wordt als definitie een combinatie van de definities van de Nederlandse overheid[4] en de Europese Unie[5] aangehouden:

Een digitale identiteit is een verzameling van betrouwbare gegevens waarmee een entiteit (persoon, organisatie, object of apparaat) zich digitaal kan identificeren en identiteitsgegevens en officiële documenten in elektronisch formaat kan opslaan en beheren.

Voorbeelden van gegevens zijn:
- Naam, geboortedatum, adres;
- Statische identificerende gegevens, identifiers (bijv. Burgerservicenummer (BSN), rekeningnummer, Rechtspersonen en Samenwerkingsverbanden Informatienummer (RSIN) of telefoonnummer);
- Biometrie (bijv. gezicht, vingerafdruk);
- Certificaten (bijv. diploma's of rijvaardigheid);
- Dynamische attributen of claims, zoals digitale transacties (bijv. financieel).

[4] Kamerstukken II 2020/21, 26643, nr. 743. https://www.tweedekamer.nl/kamerstukken/brieven_regering/detail?id=2021Z02985&did=2021D06488
[5] Q&A: Commission proposes trusted and secure Digital Identity (europa.eu)

Digitale veiligheid vs. Gebruiksgemak

De initiatieven genoemd in ***Figuur 1,*** maken gebruik van verschillende technologieën, variërend van een decentrale tot een centrale architectuur en van open source tot closed source software[6]. Aan al deze technologieën kleven voor- en nadelen. Dit zorgt voor grote discussiepunten.

Ook omdat het vaak een afweging is tussen gebruiksgemak en digitale veiligheid. Mensen willen op een gemakkelijke manier en met één druk op de knop digitaal zakendoen, maar dit mag niet ten koste gaan van de digitale veiligheid.

Decentrale vs. Centrale architectuur

Het centraal beheren van de identiteit creëert het risico dat identiteitsgegevens gekoppeld kunnen worden aan gebruiksgegevens. Dit is een angst die veelvuldig naar voren is gekomen in het debat in de Eerste- en Tweede Kamer over de eerste tranche van de Wet Digitale Overheid. In deze Wet wordt de toelating van identificatiemiddelen in het BSN-domein geregeld. Zo leeft bijvoorbeeld de angst dat een bank, als leverancier van een digitale identiteit, een aanbieding doet voor een verzekering of deze juist voor een hoger tarief aanbiedt op basis van gebruiksgegevens. Het is dan ook geen wonder dat er een grote voorkeur is voor een digitale identiteit die decentraal geregeld is.

Centrale initiatieven, zoals DigiD, maken gebruik van één centraal register, waardoor de integriteit van een identiteit gecontroleerd kan worden. Bij mogelijk misbruik of identiteitsfraude kunnen gebruikers daardoor gewaarschuwd worden en kan de digitale identiteit 'geblokkeerd' worden. Aan de andere kant kan het hacken van zo'n centraal systeem interessant zijn voor kwaadwillenden omdat alle gegevens zich op één systeem bevinden. Kwaadwillenden kunnen daardoor in theorie alle (identiteits) gegevens in dat systeem benaderen en/ of aanpassen. Als resultaat kan de gehele dienstverlening verstoord worden. Dit kan leiden tot grote maatschappelijke gevolgen, zoals ook het geval was bij de aanval op DigiNotar. Aanvullende maatregelen zijn dus nodig om een centraal systeem hiertegen te beschermen.

[6] Bij open source wordt in tegenstelling tot closed source de broncode openbaar gemaakt waardoor in principe iedereen kan controleren hoe de software in elkaar zit. Deze transparantie kan tot hogere veiligheid en vertrouwen leiden maar dit is geen garantie.

Vanuit privacy-oogpunt is het niet wenselijk dat de overheid of een andere partij alles weet wat je als burger of consument doet. Om de koppeling van gebruiks- en identiteitsgegevens tegen te gaan, is er daarom nu al in de AVG[8] en straks ook in de Wet Digitale Overheid[9] een verplichting opgenomen tot gescheiden opslag van gebruiks- en identiteitsgegevens waardoor koppeling van loggegevens aan personen niet mogelijk is. Toegelaten middelen, zoals DigiD, mogen deze gegevens alleen delen als het in overeenstemming is met het nationaal recht en er mogen niet meer gegevens worden gedeeld dan voor het gebruik van de dienst noodzakelijk is.

In tegensteling tot centrale initiatieven, slaan decentrale initiatieven attributen decentraal op, bijvoorbeeld op de telefoon van de gebruiker. Daarmee is het een privacy vriendelijker initiatief, maar het is geen garantie dat het ook veiliger is. Gegevens op een telefoon of de app zelf kunnen nog steeds gehackt worden. Wanneer de digitale identiteit van een gebruiker gestolen of gehackt wordt of een gebruiker de telefoon kwijtraakt, is er een aanvullend centraal element nodig. Op deze manier kan een correlatie tussen de (afgeleide) identiteit gelegd worden, waardoor de aanbieder van de digitale identiteit de digitale identiteit kan 'blokkeren'. Op dit moment kunnen echter (nog) niet alle decentrale diensten daaraan voldoen.

Een digitale identiteit kan dus zowel centraal als decentraal gerealiseerd worden, maar zal altijd een centraal element moeten bevatten, zoals ook het geval is bij het fysieke paspoort (de Basisregistratie Personen en het Register Paspoortsignaleringen voor documenten die niet meer gebruikt mogen worden).

DigiNotar[7]

In juli 2011 werd DigiNotar, het bedrijf dat onder andere PKIoverheid-certificaten voor overheidswebsites verzorgde, door Iraanse hackers gehackt. Door de hack konden kwaadwillenden zich voordoen als een legitieme server en zo valse beveiligingscertificaten in omloop brengen, waardoor websites nagemaakt konden worden. Als resultaat kon niet meer met zekerheid geverifieerd worden met welke organisatie je online interactie had.

De veiligheid van overheidswebsites en -diensten, als DigiD en de Belastingdienst, waren langere tijd niet te garanderen. Een volledige "black out" van de overheidsdienstverlening werd nog net voorkomen doordat Microsoft na overleg met de Nederlandse overheid besloot een beveiligingsupdate voor Windows een week uit te stellen. De Nederlandse overheid kreeg daardoor meer tijd om de DigiNotar certificaten te vervangen. De hack was een "wake-up call" voor de Nederlandse overheid: niet langer mocht de overheid zo afhankelijk zijn van één partij. Natuurlijk is dit geen garantie dat hacks niet meer voorkomen. Ook als er gebruikgemaakt wordt van verschillende initatieven zijn hacks niet uit te sluiten, maar de (maatschappelijke) impact zal minder groot zijn als er bruikbare alternatieven zijn.

---

[7] Rapport Fox-IT Black Tulip, Bijlage bij Kamerstukken II 26 643, nr. 256 en Kamerstuk 26643, nr. 256

[8] https://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32016R0679&from=NL

[9] Besluit houdende vaststelling van regels inzake de aanwijzing en erkenning van publieke en private identificatiemiddelen (Besluit identificatiemiddelen voor natuurlijke personen Wdo), artikel 3, lid 1f.

Onafhankelijke principes en open standaarden

Om de veiligheid, inclusiviteit en gebruiksvriendelijkheid van een digitale identiteit - net als bij ons fysieke identiteitsbewijs – zoveel mogelijk te waarborgen, moet het Europese raamwerk voor de digitale identiteit gerealiseerd worden op basis van technologie onafhankelijke principes en open standaarden. Daarmee kan tegengegaan worden dat diensten gelimiteerd worden tot bijvoorbeeld Apple- of Android-gebruikers, maar juist voor iedereen inzetbaar, toepasbaar en bruikbaar zijn.

Op deze manier wordt er ook enige vorm van keuzevrijheid voor burgers gerealiseerd, omdat verschillende partijen de dienst aan kunnen bieden. Een bijkomend voordeel is dat een ***"single point of failure"*** voorkomen wordt. Onlangs bleek bijvoorbeeld dat DigiD, het enige middel voor burgers dat momenteel toegelaten is in het BSN-domein, meerdere keren per week onder vuur ligt van DDoS-aanvallen.[10] Een gedeelte van deze aanvallen kan gemitigeerd worden, maar het gebeurt toch ook regelmatig dat DigiD niet beschikbaar is.[11] Als dit gebeurt, kunnen burgers op geen enkele manier onlinediensten afnemen van de overheid.

Het nadeel is een versnipperd aanbod van diensten die (enigszins) vergelijkbare functionaliteit bieden. Door actiever de kaders te scheppen, hier richting aan te geven en daarop toe te zien, kan de overheid zorgdragen dat enkel diensten aangeboden mogen worden die aan deze betrouwbare principes en standaarden voldoen.

Een paspoort is immers ook meer een concept dan een "object": op EU-niveau zijn de hoofdlijnen geschetst, maar landen blijven zelf verantwoordelijk voor de invulling. Sommige landen produceren hun paspoort zelf en andere landen, zoals Nederland, besteden de uitvoering uit aan een marktpartij. Zo zal het ook bij een digitale identiteit zijn: ***met het European Digital Identity framework worden de*** hoofdlijnen en kaders op EU-niveau geschetst. Deze kunnen vervolgens op verschillende manieren met gebruik van onafhankelijke principes en open standaarden (publiek of privaat, maar ook met meerdere technologieën) ingevuld worden. Een randvoorwaarde hierbij is dat de interoperabiliteit tussen de lidstaten en verschillende diensten geborgd is.

[10] https://www.computable.nl/artikel/nieuws/security/7260274/250449/digid-steeds-vaker-onder-ddos-vuur-via-booter-site.html?utm_source=computable.nl&utm_medium=email&utm_campaign=dagelijkse_update&utm_content=topartikele
[11] https://www.hartvannederland.nl/nieuws/nog-steeds-meldingen-digid-door-ddos-aanvallen

Privacy vs. Zorgplicht

Een terugkomend vraagstuk rondom een digitale identiteit is of de burger in staat is om zelf controle over zijn gegevens te hebben of dat de overheid een zorgplicht heeft om de burger te beschermen tegen misbruik door organisaties. De burger moet in principe zelf kunnen bepalen welke gegevens hij of zij in welke context deelt. Immers, iemand die zich authentiseert bij een bank doet dit in de rol van rekeninghouder bij diezelfde bank, maar iemand die zich authentiseert bij een gemeente doet dit in de rol van inwoner van die gemeente. Hierbij hoort een andere privacy afweging en bovendien andere gegevens.

Het waarborgen van het grondrecht op privacy lijkt een uitdaging, maar ook een kans, bij het ontwikkelen van oplossingen voor een digitale identiteit. Door het ***"privacy by design"*** principe krijgt de eigenaar van de digitale identiteit de controle over zijn of haar gegevens. Dit betekent dat de gebruiker heel gericht en bewust kiest welke attributen of claims hij/zij met een ander deelt, in welke omstandigheden en onder welke voorwaarden.

"94% van de Nederlanders maakt zich zorgen over de bescherming van persoonsgegevens"

Autoriteit Persoonsgegevens

Dit klinkt als een mooie kans: het zijn immers de eigen gegevens, waarover de persoon zelf regie kan en mag voeren. De keerzijde is echter dat organisaties buitenproportioneel gegevens kunnen opvragen als voorwaarde om gebruik te maken van hun dienstverlening. Dit wordt bijvoorbeeld al gedaan bij het huren van een woning[12] . Door de overspannen woningmarkt voelen potentiële huurders zich gedwongen om meer gegevens te verstrekken dan zij eigenlijk willen. Het risico is dat verhuurders en makelaars beschikken over veel meer gegevens en data dan benodigd. Dit brengt risico's met zich mee, zoals het misbruik van deze gegevens of een verhoogde kans op datalekken.

Het is daardoor geen verrassing dat uit een onderzoek van de Autoriteit Persoonsgegevens in het voorjaar van 2019[13] blijkt dat 94 procent van de Nederlanders zich zorgen maakt over de bescherming van persoonsgegevens. Bovendien was tijdens de week van Centrum voor Informatiebeveiliging en Privacybescherming (CIP)[14] maar liefst 66% van de respondenten van mening dat de zorgplicht van de overheid zwaarder weegt dan de autonomie van de burger (34%).

De overheid heeft dus een zorgplicht om burgers te beschermen tegen mogelijk misbruik door organisaties. Dit kan de overheid doen door controles uit te voeren, burgers voorlichting en informatie te geven, maar ook door eisen te stellen aan toegelaten diensten. Er zijn namelijk verschillende (technische) varianten denkbaar waarin burgers in meer of mindere mate regie kunnen voeren over hun gegevens.[15]

Bij burgers roept de versnippering van de oplossingen en het 'waarom' van een digitale identiteit veel vragen op.[16] Door als overheid 'checks and balances' in te bouwen, kunnen burgers geïnformeerd toestemming geven voor het delen van hun persoonlijke gegevens. Informatie die gedeeld wordt, dient hierbij - in overeenstemming met de AVG - proportioneel te zijn in relatie tot de diensten die hier tegenover staan.

[12] https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2019D13616&did=2019D13616
[13] Autoriteit Persoonsgegevens, Nederland maakt zich zorgen over privacy – flitspeiling privacyrechten.
[14] https://www.youtube.com/watch?v=8vKvQ_YsWmQ
[15] https://rog.pleio.nl/file/download/feac7dc7-1774-49ac-b1ee-59f36dcd36ff/1553009641ictu%20rog%20rapport%20kader%20voor%20rog.pdf
[16] BMH 13, Een betere overheid voor burgers en bedrijven, https://www.rijksfinancien.nl/bmh/bmh-13-een-betere-overheid-richting-burgers-en-bedrijven.pdf

Rol van de overheid: Leverancier vs. Afnemer

De rol van de overheid in het opzetten van een digitale identiteit is niet eenduidig. De overheid is bijvoorbeeld registerhouder (BRP), maar tegelijkertijd ook een afnemer (o.a. Belastingdienst, UWV, SVB). Daarnaast is de overheid een leverancier (DigiD), maar ook wetgever (Wet Digitale Overheid) en toezichthouder (Autoriteit Persoonsgegevens, Agentschap Telecom).

De verschillende taken en verantwoordelijkheden van overheidsorganisaties brengen ook andere belangen mee rondom het vraagstuk van digitale identiteit. Doordat er – in tegenstelling tot bij ons fysieke identiteitsbewijs – geen duidelijke verantwoordelijkheid bij één overheidsorganisatie belegd is, kunnen de verdeelde belangen elkaar bijten. Dit vergemakkelijkt het gezamenlijk maken van fundamentele keuzes niet. Als resultaat zien wij alleen al binnen de overheid een gefragmenteerd landschap met veel initiatieven.

Doordat de overheid niet altijd met "één stem" spreekt, blijven die initiatieven veelal hangen in de pilotfase. Mede daardoor lijkt het onderwerp digitale identiteit in Nederland onvoldoende van de grond te komen. Dit terwijl er initiatieven in de (Europese) markt zijn, die inmiddels een hoog volwassenheidsniveau hebben. Denk bijvoorbeeld aan Irma, Itsme, maar ook aan initiatieven van Apple, Facebook en Microsoft. Deze partijen ontwikkelen in een snel tempo nieuwe middelen waarmee de burger zich kan identificeren en authentiseren en regie kan voeren over zijn/haar gegevens. Het zijn deze grote technologische partijen die het heft in handen hebben genomen en inspelen op de toenemende vraag.

Het snel ontwikkelende landschap met vele initiatieven vraagt om een nieuwe, eenduidige overheidsaanpak. Dit is niet alleen nodig om interoperabiliteit tussen de verschillende diensten te realiseren, maar ook om als Nederland koers te bepalen bij het opstellen van het Europees raamwerk. Daarmee kan Nederland zorgen voor duidelijke regulering en onze Europese koploperspositie in digitalisering behouden.

Als Nederland deze koploperspositie verliest en achterblijft in de ontwikkelingen rondom een digitale identiteit, ontstaat het risico dat de wildgroei aan initiatieven, die niet optimaal aansluiten op de Nederlandse (overheids)dienstverlening en die niet interoperabel zijn, alleen maar groter wordt. Dit is niet alleen onduidelijk en onhandig voor burgers en bedrijven, maar bemoeilijkt ook het uitoefenen van de rol en de zorgplicht van de Nederlandse overheid.

Het behouden van de koploperspositie kan de Nederlandse overheid niet alleen. Om bij te blijven met ontwikkelingen in andere Europese landen en ontwikkelingen buiten het overheidsdomein, is samenwerking met publieke en private partners onvermijdelijk. Afhankelijkheid van private partners en platformen is al jaren een gevoelig onderwerp binnen de overheid, maar zij moet deelnemen aan dit ecosysteem om ontwikkeling mogelijk te maken. Dit begint bij het uitzetten van concrete stappen om de kaders van het Europees raamwerk te scheppen. Vervolgens moet duidelijke toekenning van taken en verantwoordelijkheden zorgen voor een actieve samenwerking, om het raamwerk en de daarop aansluitende middelen vorm te geven.

De weg naar een digitale identiteit

De weg naar een digitale identiteit vraagt niet alleen een integrale visie, regievoering en daadkracht van de overheid. Omdat we steeds vaker digitaal zakendoen met elkaar, vereist het ook een andere aanpak van publieke en commerciële organisaties.

Digitale identiteiten zijn de sleutel om burgers en organisaties maximaal te faciliteren, hun interacties zo vertrouwd mogelijk te doen, klanten en diensten een optimale digitale ervaring te geven en tegelijkertijd informatie te beschermen.

Door de waarde van digitale identiteiten goed te benutten, kunnen organisaties meer efficiëntie, controle en inkomsten behalen. Daardoor wordt niet alleen een verbeterde gebruikerservaring gerealiseerd, maar ook veiligheid en privacybescherming. De digitale identiteit is daarmee een strategische component in de bedrijfsvoering van organisaties.

Deloitte en Grabowsky adviseren en ondersteunen publieke en commerciële organisaties vanaf het vormgeven van een visie en strategie rondom digitale identiteiten tot aan de implementatie van de gewenste oplossing.

Contact

Guus van Es
Partner Risk Advisory
guvanes@deloitte.nl

Steven Daniels
Managing Director Grabowsky
daniels@grabowsky.com
+31 (0)70 3131 020

Deloitte.

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited ("DTTL"), its global network of member firms, and their related entities. DTTL (also referred to as "Deloitte Global") and each of its member firms are legally separate and independent entities. DTTL does not provide services to clients. Please see www.deloitte.nl/about to learn more.

Deloitte is a leading global provider of audit and assurance, consulting, financial advisory, risk advisory, tax and related services. Our network of member firms in more than 150 countries serves four out of five Fortune Global 500® companies. Learn how Deloitte's approximately 264,000 people make an impact that matters at www.deloitte.nl.

This communication contains general information only, and none of Deloitte Touche Tohmatsu Limited, its member firms, or their related entities (collectively, the "Deloitte network") is, by means of this communication, rendering professional advice or services. Before making any decision or taking any action that may affect your finances or your business, you should consult a qualified professional adviser. No entity in the Deloitte network shall be responsible for any loss whatsoever sustained by any person who relies on this communication.

© 2021 Deloitte The Netherlands