Naar een veilig eID-stelsel

Advies inzake een veilig, universeel en open digitaal eID-stelsel voor een open, veilige en welvarende samenleving

CSR
Cyber Security Council
Cyber Security Raad

Naar een veilig eID-stelsel

Advies inzake een veilig, universeel en open digitaal eID-stelsel voor een open, veilige en welvarende samenleving

Gericht aan:

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties
De minister van Justitie en Veiligheid
De staatssecretaris van Economische Zaken en Klimaat

CSR
Cyber Security Council
Cyber Security Raad

7 november 2019

CSR-advies 2019, nr. 1

Inleiding

De ontwikkelingen in het digitale domein bieden veel economische en maatschappelijke kansen die alleen kunnen worden verzilverd als Nederland digitaal veilig is. De in 2018 verschenen Agenda Digitale Overheid[1] geeft aan dat de Grondwet en de daaruit voorvloeiende publieke waarden, zoals privacy, zelfbeschikking en gelijkheid, juist bij de voortschrijdende digitalisering essentieel zijn om te borgen. De agenda gaat over het benutten van kansen en borgen van rechten. Vorig jaar verscheen ook de Nederlandse Digitaliseringsstrategie[2] waarmee het kabinet onder andere het verdienvermogen van Nederland verder wil versterken en zorgen voor betere digitale vaardigheden en cyberveiligheid in de maatschappij. Het is belangrijk dat de randvoorwaarden voor economisch succes goed worden geborgd: veiligheid, vertrouwen en betrouwbaarheid van de digitale infrastructuur. Elektronische identiteiten (eID's) vormen daarvoor een noodzakelijke pijler.

Er is brede consensus dat burgers en (medewerkers van) bedrijven veilig moeten kunnen inloggen bij overheidsorganisaties, dienstverleners, zorginstellingen, webwinkels, leveranciers enz. Stapsgewijs wordt door veel verschillende partijen (publiek, privaat, non-profit) gewerkt aan het verhogen van het betrouwbaarheidsniveau van de beschikbare inlogmiddelen en aan het waarborgen van de continuïteit, opdat burgers en bedrijven meer zaken kunnen regelen via internet. De inspanningen van de Rijksoverheid hierbij richten zich op het inloggen van burgers en bedrijven in het publieke domein, maar niet op het inloggen in het private domein. Deze eenzijdige concentratie leidt niet alleen tot versnippering en verwarring, maar zou er ook toe kunnen leiden dat privacy en veiligheid onvoldoende zijn gegarandeerd bij het inloggen bij bedrijven en organisaties in de private en non-profit sectoren, waardoor fraude en misbruik zouden kunnen toenemen en cruciale digitaliseringsprojecten zouden kunnen stagneren.

De digitale economie biedt grote kansen en mogelijkheden om online diensten en producten af te nemen. Voor het bedrijfsleven in Nederland zijn digitale identificatie, het faciliteren van economische transacties en (juridische) duidelijkheid over het gebruik van data essentieel; zij vormen de pijlers voor economische groei in het (steeds dominantere) digitale domein. In de fysieke wereld kunnen we ons nauwelijks economische transacties voorstellen zonder zekerheden over identiteiten, bezit en over wie is gemachtigd om wat te doen. Daarvoor bestaan middelen en organisaties, zoals paspoorten en identiteitskaarten, kadaster en kamer van koophandel, notarissen en gemeentebalies. Voor deze structuren bestaan wettelijke kaders en garanties en heeft de overheid een zware verantwoordelijkheid.

In de digitale wereld ontbreekt vooralsnog een dergelijke brede infrastructuur en zijn benodigde zekerheden veel minder vanzelfsprekend. De digitalisering van transactieprocessen verloopt moeizaam, met name door het ontbreken van een flexibele eID-infrastructuur voor zowel het publieke (BSN) domein als voor het private domein. De overheid laat niet alleen de authenticatie van (medewerkers van) bedrijven over aan de markt, maar ook de authenticatie van burgers in het private domein. Daardoor beschikken burgers vooralsnog niet over een (veilig en privacy-vriendelijk) eID dat in het maatschappelijk verkeer en in de e-commerce gebruikt kan worden. De vraag is of we in Nederland voldoende aankoersen op het neerzetten van een solide digitale infrastructuur, die burgers en bedrijven beschermt in het digitale tijdperk en de economische groei faciliteert in de volgende fase van de digitale interne Europese markt.

[1] NL DIGIbeter: Agenda Digitale Overheid, Overheidsbrede Beleidsoverleg Digitale Overheid, 2018
[2] Nederlandse Digitaliseringsstrategie: Nederland digitaal - Hier kan het. Hier gebeurt het, Ministerie van Economische Zaken en Klimaat, 2018

De raad is van mening dat Nederland grote stappen kan en moet zetten voor het creëren van een brede veilige en privacy-vriendelijke eID infrastructuur. Hier komen economische belangen samen met nationale veiligheid en met bescherming van (de gegevens van) de eigen burgers en bedrijven. Gezien de rol van de overheid als traditionele verankeraar en leverancier van de `bron' identiteit van burgers en bedrijven, kan de overheid op dit gebied een voortrekkersrol worden verwacht. Uiteraard ligt hier ook een taak van de verschillende maatschappelijke organisaties die beschikken over relevante (identiteits)informatie.

HUIDIGE SITUATIE: TWEE GESCHEIDEN DOMEINEN

In de digitale wereld is alles met elkaar verbonden. Dit uitgangspunt zal de aanpak voor het creëren van een digitaal veilige infrastructuur moeten bepalen. Echter, onze huidige identiteitsinfrastructuur is nog verdeeld in twee domeinen, namelijk het publieke (BSN) domein (van burgers en overheden) en het private domein (van burgers, bedrijven en niet-publieke organisaties). Deze scheiding is in Nederland gebaseerd op de regelgeving voor het gebruik van het BSN. Het is niet de bedoeling van de raad om die scheiding ter discussie te stellen. Wel wil de raad benadrukken dat deze scheiding een flexibele eID-infrastructuur vereist, die het burgers mogelijk maakt om onder verschillende omstandigheden verschillende kenmerken van zichzelf te laten zien bij authenticatie: het BSN in het publieke domein en andere relevante kenmerken in het private domein. Dit is in lijn met de eIDAS-verordening, die de lidstaten aanmoedigt om hun vertrouwensdiensten en -infrastructuur zodanig op (en in) te zetten dat die ook kunnen worden gebruikt voor het maatschappelijk verkeer en voor de 'markt'. Zie overweging 17 van eIDAS:

> *De lidstaten dienen de private sector aan te moedigen vrijwillig gebruik te maken van elektronische identificatiemiddelen die onder een aangemeld stelsel vallen, indien identificatie bij online diensten of elektronische transacties nodig is.*

Het huidige eID-programma van de Rijksoverheid heeft nog niet de ambitie om veilige, privacy-vriendelijke digitale authenticaties en transacties in het maatschappelijke (private) domein te faciliteren. De overheid richt zich hoofdzakelijk op het verhogen van het betrouwbaarheidsniveau van de eigen bestaande inlogmiddelen en op het waarborgen van de continuïteit daarvan, opdat burgers en bedrijven veilig online zaken kunnen doen met overheidsorganisaties en zorginstellingen binnen het publieke domein. Dat zijn belangrijke zaken die de raad van harte ondersteunt. Er is echter alle aanleiding om onze digitale samenleving van een breed eID-stelsel te voorzien dat de gebruikers overal dezelfde voorzieningen en bescherming biedt.

De raad ziet twee ontwikkelingen die de urgentie van een breed eID-stelsel benadrukken:

Onze digitale veiligheid staat onder druk

Het onderwerp digitale identiteit is van strategisch belang voor Nederland en Europa. Recente publicaties als het Cybersecurity Beeld 2019[3] en het WRR-rapport 'Voorbereiden op digitale ontwrichting'[4] laten zien dat de omvang van de dreiging die uitgaat van statelijke actoren blijft

[3] Cyber Security Beeld Nederland 2019, Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), Den Haag, 2019

[4] Adviesrapport 'Voorbereiden op digitale ontwrichting', Wetenschappelijke Raad voor het Regeringsbeleid (WRR), 2019

groeien. Landen als China, Iran en Rusland hebben offensieve cyberprogramma's gericht tegen Nederland. Dit betekent dat deze landen digitale middelen inzetten om geopolitieke en economische doelstellingen te bereiken ten koste van Nederlandse belangen. Statelijke actoren zijn uit op gedetailleerde informatie van onze bedrijven en burgers en verkrijgen die typisch door onder een valse identiteit binnen te dringen. Daarnaast willen sommige statelijke actoren de publieke opinie of democratische processen beïnvloeden, vitale systemen verstoren of zelfs saboteren. Staten bespioneren ook burgers. Hierbij wordt onderscheid gemaakt tussen een algemene interesse van staten in persoonsgegevens en het gericht bespioneren van personen of (dissidente) groeperingen, bijvoorbeeld met als doel deze personen of groeperingen te beïnvloeden of zelfs te intimideren. Een eerste verdedigingslinie tegen dergelijke activiteiten is een solide eID-infrastructuur, die niet alleen de publieke sector, maar ook de private sector, afschermt tegen ongeautoriseerde toegang.

Onze privacy en digitale soevereiniteit staat onder druk

Nederland bevindt zich in de Europese top 5 van online shoppen[5]. De Nederlandse digitale infrastructuur is daarbij sterk afhankelijk van een beperkt aantal buitenlandse organisaties met eigen belangen wat betreft het verzamelen en gebruiken van gebruikersgegevens. Dit maakt Nederland potentieel kwetsbaar. Nationale initiatieven in de private en non-profit sector op het terrein van eID zijn tot op heden kleinschalig en niet breed aangeslagen; voor gebruikers is het daardoor niet duidelijk welke toepassingen ze kunnen gebruiken en of deze aan veiligheids- en privacy-eisen voldoen. Het gevolg hiervan is dat burgers op dit moment voor bijna iedere dienst nog steeds met het kwetsbare systeem van gebruikersnaam gecombineerd met wachtwoord moeten inloggen en daarbij handmatig (steeds dezelfde) persoonsgegevens moeten invoeren en prijsgeven. Om inloggen te versimpelen bieden veel websites burgers de optie om zich te authentiseren via hun account bij een van de grote buitenlandse platformen, zoals Facebook, Apple, Amazon, Google, of straks mogelijk Alibaba of Tencent. Hierdoor ontstaan bij deze platformen grote concentraties van zowel Nederlandse bedrijfs- als persoonsgegevens, hetgeen direct gevolgen heeft voor onze privacy en digitale soevereiniteit.

[5] CBS, Eurostat 2018, https://www.cbs.nl/nl-nl/nieuws/2018/38/nederland-in-europese-top-5-online-winkelen

ADVIES

Nederland moet een veilige, open en welvarende samenleving zijn en blijven. Vertrouwen in de samenleving en haar structuren is van cruciaal maatschappelijk en economisch belang. Het veilig identificeren en authentificeren, veilig inloggen, veilig delen van gegevens alsook het veilig (digitaal) ondertekenen en adequaat afschermen (versleutelen) van gegevens behoort tot de noodzakelijke basisinfrastructuur van een digitale wereld.

In de fysieke wereld beschikken we over voldoende mogelijkheden en middelen en zijn de verantwoordelijkheden van markt en de overheid op dit gebied wettelijk geregeld, via talrijke regelingen en instanties. Of we in staat zullen zijn om de voordelen van een digitaliserende samenleving te kunnen realiseren zal afhankelijk zijn van de borging van drie kernthema's: veiligheid, privacy en vertrouwen. Deze drie pijlers zijn onlosmakelijk verbonden met de rol van de overheid. Nederland moet vaart maken met het neerzetten van een digitale eID-infrastructuur die zowel publiek als privaat bruikbaar is. De overheid dient haar beperking tot het publieke eID-domein te heroverwegen; een krachtige, brede regie- en toezichtsrol van de overheid is dringend gewenst voor gecombineerd publiek en privaat gebruik van eID-middelen. Het uitgangspunt van de raad is dat er zo snel mogelijk, zoveel mogelijk gebruikers moeten kunnen beschikken over inlogmiddelen op het in EU-verband vastgestelde niveau *substantieel of hoog*[6].

De raad adviseert de volgende handelingsperspectieven:

1. Coördineer en faciliteer de ontwikkeling van een universeel stelsel voor digitale authenticatie, ondertekening en versleuteling dat burgers en bedrijven zowel in het publieke als maatschappelijke domein beschermt (eID-stelsel), waarbij wordt voortgebouwd op de in Nederland aanwezige expertise.

2. Kies voor een slagvaardige publiek en private aanpak onder toezicht van de overheid, die gericht is op een open infrastructuur (voorkom gedwongen winkelnering en lock-in).

3. Stimuleer het gebruik van veilige inlogmiddelen in het maatschappelijke domein door burgers en bedrijven.

[6] Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, https://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX%3A32014R0910

Ad 1. Coördineer en faciliteer de ontwikkeling van een universeel stelsel voor digital authenticatie, ondertekening en versleuteling dat burgers en bedrijven zowel in het publieke als maatschappelijke domein beschermt (eID-stelsel), waarbij wordt voortgebouwd op de in Nederland aanwezige expertise.

Ons land is gediend met een integrale, breed-gedeelde visie en aanpak vanuit de overheid. Het veilig inloggen, veilig delen van gegevens en veilig (digitaal) ondertekenen zou in onze digitale wereld net zo vanzelfsprekend moeten zijn als in de fysieke wereld. De raad roept het kabinet daarom op om in aanvulling op het bestaande beleid actief en vanuit een coördinerende en faciliterende rol bij te dragen aan de ontwikkeling van een universeel stelsel voor digitale identificatie en authenticatie (eID-stelsel). Hierbij dringt de raad erop aan goed aan te sluiten op recente eID-ontwikkelingen in Nederland (bij bedrijven, gemeenten, in de zorg, etc.) en de Europese Unie. De ontwikkeling van het universele stelsel moet passen binnen de door de EU vastgestelde kaders. De (juridische) obstakels die dit verhinderen moeten zo snel mogelijk worden opgelost. De focus van de overheid moet hier nadrukkelijker op liggen. Dit sluit goed aan op de onlangs verschenen *'Nederlandse Digitaliseringsstrategie: Nederland digitaal - Hier kan het. Hier gebeurt het'*[7]. Voor de pijlers onder de economische groei zijn digitale identificatie, het faciliteren van economische transacties en het gebruiksrecht van data essentieel en onlosmakelijk aan deze strategie verbonden. Deze strategie moet het verdienvermogen van Nederland verder versterken, zorgen voor betere digitale vaardigheden van burgers en cyberveiligheid van de maatschappij. Een veilig eID is noodzakelijk als basis voor betrouwbare digitale (economische) transacties en voor het adequaat afschermen van persoonsgegevens.

Ad 2 **Kies voor een slagvaardige publiek en private aanpak onder toezicht van de overheid, die gericht is op een open infrastructuur (voorkom gedwongen winkelnering en lock-in).**

In de fysieke wereld is de rol van de overheid duidelijk en zijn de (beleids)ambities ingericht aan de hand van een abstract kader als het sociaal contract. In de digitale wereld wordt een dergelijk raamwerk gemist. Hierdoor is de rolverdeling tussen burgers, bedrijven en overheid onduidelijk en ontbreekt, in tegenstelling tot de fysieke wereld, de overheidsregie in het maatschappelijke domein. Nederland bevindt zich wereldwijd gezien in de kopgroep als het om cybersecurity gaat. Het behouden van onze vooraanstaande positie blijft prioriteit en dit vraagt structurele aandacht voor onze digitale infrastructuur van regering, politici, beleidsmakers, bestuurders, toezichthouders, bedrijven en burgers. Iedereen heeft een verantwoordelijkheid in het gezamenlijk beschermen van onze economie, welvaart en maatschappij. Een betrouwbaar eID-stelsel is daarvan een hoeksteen. De overheid heeft hierin een belangrijke (voorbeeld)rol; burgers en bedrijven moeten zaken met de overheid veilig online kunnen doen. Er bestaat volgens de raad brede maatschappelijke behoefte dat de overheid deze rol uitstrekt tot het private domein.

De overheid dient een zorgvuldige regie- en toezichtrol te vervullen ter bescherming van publieke belangen, ter verankering van Europese waarden en ter voorkoming van scheve (digitale) machtsmonopolies. Er is behoefte aan veilige en praktische bruikbare identificatie- en authenticatiemiddelen die Europese waarden, zoals autonomie, transparantie, zelfbeschikking en privacy, reflecteren en die niet de afhankelijkheden van buitenlandse ICT-leveranciers vergroten.

[7] 'Nederlandse Digitaliseringsstrategie: Nederland digitaal - Hier kan het. Hier gebeurt het', ministerie van Economische Zaken en Klimaat, Den Haag, juni 2018

De drie ministeries die ieder verantwoordelijk zijn voor een deel van de digitale samenleving, te weten de ministeries van Binnenlandse Zaken en Koninkrijksrelaties (BZK), van Economische Zaken en Klimaat (EZK) en van Justitie en Veiligheid (JenV) zouden gezamenlijk en in samenwerking met de private en de non-profit sector spoedig tot de realisatie van een universeel eID-stelsel moeten komen.

Ad 3 Stimuleer het gebruik van veilige inlogmiddelen in het maatschappelijke domein door burgers en bedrijven.

De Algemene Verordening Gegevensbescherming en eIDAS vereisen security en privacy by design. Om aan dergelijke verplichtingen te kunnen voldoen moeten er passende voorzieningen worden getroffen De raad benadrukt ook in deze de (juridische) zorgplichten die bedrijven hebben op het gebied van cybersecurity en gegevensverwerking[8].

Pas sinds kort voorziet het ministerie van BZK een toelatingsstelsel voor private inlogmiddelen voor burgers in het overheidsdomein. Dit kan een positieve weerslag hebben op de inzet van dergelijke middelen in het maatschappelijke private domein. Een brede inzet van deze middelen zal zeker niet vanzelf gaan; daar is de medewerking van de (inter)nationale e-commerce sector voor nodig. Het is ook van belang dat we ons op buitenlandse sites veilig kunnen identificeren. Deze sector moet in staat worden gesteld om de eigen dienstverlening op veilige, privacy-vriendelijke en betaalbare wijze toegankelijk te maken, zodat gebruikers niet (de facto) gedwongen zijn met bijvoorbeeld hun Facebook-account in te loggen. Deze inlogmiddelen moeten gebruiksvriendelijk en wellicht zelfs gratis zijn, willen ze kunnen concurreren met de authenticatiemiddelen van de grote platformen. Dit is een strategisch Nederlands belang. Dit betekent dat ook commerciële partijen die online diensten en producten aanbieden moeten worden betrokken in de beoogde samenwerking. Zij moeten in staat worden gesteld, de veilige eID-middelen aan hun gebruikers aan te bieden. De spelregels, waardoor burgers controle hebben over hun gegevens, zoals beschreven in het BZK-document ‘Visie Regie op gegevens’, zouden ook moeten gelden in het private domein.

[8] Ieder bedrijf heeft digitale zorgplichten; een handreiking voor bedrijven, Cyber Security Raad, 2017

GERICHTE ADVIEZEN

De adviezen zijn gericht aan:
de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
de minister van Justitie en Veiligheid en
de staatssecretaris van Economische Zaken en Klimaat.

De raad adviseert:

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties:

1. Voer regie en houd toezicht op de (verdere) ontwikkeling van een universeel open eID-stelsel dat ook burgers en bedrijven in het maatschappelijke domein beschermt.
2. Coördineer en faciliteer dat op korte termijn betrouwbare eID-middelen kunnen worden ingezet in het maatschappelijke digitale domein zodat veilig authenticeren, ondertekenen en versleutelen ook in dit domein mogelijk is.
3. Faciliteer de ontwikkeling van betrouwbare eID-middelen op zodanige wijze dat het recht op privacy, autonomie en zelfbeschikking centraal staan.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
De minister van Justitie en Veiligheid en de staatssecretaris van Economische Zaken en Klimaat:

4 Investeer en werk samen aan een veilig universeel en open digitaal eID-stelsel voor een open, veilige en welvarende samenleving.

De staatssecretaris van Economische Zaken en Klimaat:

5. Stimuleer het gebruik van veilige identificatiemiddelen door burgers en bedrijven.

’s-Gravenhage,

Namens de Cyber Security Raad,

Hans de Jong
Covoorzitter CSR

Pieter-Jaap Aalbersberg
Covoorzitter CSR