Stichting Privacy By Design
privacybydesign.foundation
irma.app

Nijmegen, 28 januari 2020

WDO verbeterpunten voor een goed-ID

De Tweede Kamer is van plan om eind januari 2020 de discussie over het wetsvoorstel Digitale Overheid (WDO) voort te zetten. Deze notitie is bedoeld als input voor die discussie en geeft concrete voorstellen (met name aan Kamerleden) voor verbetering van het wetsvoorstel. Het uitgangspunt is dat de identiteit van burgers geen handelswaar is. Vertrouwen van burgers vereist dat hun persoonsgegevens goed beschermd worden en niet door de overheid in handen gegeven worden van (buitenlandse) ICT-monopolisten voor een surveillance economie.

De afgelopen weken is er grote onrust ontstaan over de verplichting voor *bedrijven* om exclusief via het dure en omslachtige eHerkenning-systeem in te loggen bij de overheid (i.h.b. bij de belastingdienst). Inloggen met eHerkenning kan alleen via toegelaten private partijen, waarbij een inlogmiddel minimaal ongeveer 50€ per jaar kost en door kleine ondernemingen maar één of enkele keren per jaar gebruikt wordt: de prijs per login is daarmee extreem hoog. Er zijn enkel commerciële leveranciers van inlogmiddelen als gevolg van de bewuste keuze van de overheid om dit aan de markt over te laten. Het inloggen bij de overheid door individuele *burgers* ligt nog veel gevoeliger vanwege de additionale privacy-verwachtingen en -eisen. De maatschappelijke onrust daarover is nu reeds voelbaar, zie bijvoorbeeld de website goed-ID.org.

De WDO schept een wettelijk kader voor inloggen bij de overheid. Maar het wetsvoorstel beoogt niet om inloggen buiten de overheid (bijvoorbeeld bij webwinkels) te reguleren — ondanks grote maatschappelijke behoefte daaraan (zie punt 6 hieronder). Voor inloggen buiten de overheid zijn Nederlandse

burgers dus afhankelijk van ofwel commerciële ofwel non-profit oplossingen. De recente onrust rond eHerkenning toont aan dat een commerciële benadering van inloggen duur en omstreden is. In de kern draait het om de volgende drie samenhangende vragen.

1. Moet inloggen beheerd worden door een *bedrijf*, door de *overheid* zelf, of door een *non-profit* organisatie?

2. Hoe transparant moet een inlog-middel zijn voor gebruikers? Heel concreet, moet zo'n middel met *open source* software werken, zie punt 3?

3. Moeten inlog-attributen van gebruikers *centraal* of *decentraal* opgeslagen worden? Punt 2 geeft hieronder meer informatie over dit onderscheid.

Commerciële partijen kiezen typisch voor centrale opslag en intransparante werking via gesloten (*proprietary*) software. Het enige beschikbare non-profit eID-middel (IRMA) gebruikt daarentegen decentrale opslag en open source.

Er is dus sprake van een echte en betekenisvolle keuzemogelijkheid met een politieke lading: wordt de aanpak van eHerkenning herhaald, of wordt een nieuwe weg gekozen met grotere nadruk op publieke belangen?

Hieronder worden deze punten nader uitgewerkt, waarbij begonnen wordt met een korte uiteenzetting over attributen en identiteiten.

1 Attributen voor natuurlijke personen

We kunnen constateren dat er de laatste jaren maatschappelijke en wetenschappelijke consensus is ontstaan dat een modern eID-stelsel gebaseerd moet zijn op attributen d.w.z. op persoonlijke kenmerken, zoals naam, e-mail, 06, BSN, leeftijdsgrenzen, BIG/AGB registratie, etc. Burgers kunnen dan in verschillende situaties, op privacy-vriendelijke wijze, met alleen relevante gegevens, zichzelf online bekend maken. Met zulke attributen kun je bijvoorbeeld bewijzen dat je ouder dan 16 bent, om online een film te spelen, zonder dat je andere dingen van jezelf hoeft te onthullen. Volledige anonimiteit online kan makkelijk leiden tot misdragingen en volledige identificatie kan leiden tot privacy-schending en ongewenste profilering. Attributen bieden een tussenweg waarmee op het gepaste nivo zekerheid geboden wordt, in lijn met de Algemene Verordening Gegevensbescherming (AVG).

Het bestaande inlogmiddel DigiD is gebaseerd op het burger servicenummer (BSN) en kan (daarom) alleen in de publieke sector gebruikt worden. Door inloggen met meer attributen dan alleen het BSN mogelijk te maken kan zo'n nieuw eID-middel zowel in de publieke als in de private sector gebruikt worden. Daar is grote maatschappelijke behoefte aan, zie later bij punt 6.

Maar ook binnen de overheid — zowel locaal als nationaal — bestaat behoefte aan meer attributen dan alleen het BSN. Zo zal een gemeente bij de online melding van een kapotte lantaarnpaal van de melder willen weten of die in de betreffende buurt/gemeente woont (bijvoorbeeld via het postcode attribuut) en wat diens e-mail adres is (bijvoorbeeld om een bevestiging te sturen); verder is eigenlijk niks nodig[1]. Ook kan het voor het UWV belangrijk zijn om een BIG registratie als attribuut te ontvangen, bijvoorbeeld om na te kunnen gaan dat een ziekmelding van een echte arts komt (en geen fraudegeval is). Kortom, het BSN is een belangrijk attribuut in het publieke domein, maar in een breder verband zijn veel meer attributen vereist voor een vertrouwde digitale wereld.

Verbeterpunt: Het wetsvoorstel digitale overheid erkent niet het belang van attributen van natuurlijke personen in een identiteitsinfrastructuur. In art. 12.2 krijgt de Minister weliswaar de mogelijkheid om attributen aan te wijzen, maar slechts voor identificatie van ondernemingen en rechtspersonen. Hier dienen natuurlijke personen toegevoegd te worden. Ook de doelstelling "voor identificatie" is te smal omdat attributen ook voor digitale handtekeningen en voor versleuteling gebruikt kunnen worden[2]. De wet moet daarom in het algemeen attribuut-gebaseerde elektronische diensten voor ondernemingen, rechtspersonen, en natuurlijke personen mogelijk maken.

2 Opslag van attributen: centraal of decentraal

Er is dus consensus over het belang van attributen. Er is echter vooralsnog geen consensus over waar die persoonlijke attributen opgeslagen moeten wor-

[1] Gebruik van het BSN attribuut via DigiD is feitelijk onwettig voor zulke meldingen omdat daarbij geen sprake is van data minimalisatie, zoals vereist door de AVG.

[2] Voor een uitgebreidere uiteenzetting, zie het IRMA manifest.

den: *decentraal*, bij de burger zelf, of *centraal*, bij een eID-beheerder. Dit belangrijke verschil kan concreet gemaakt worden in het volgende gedachtenexperiment.

1. Stel dat **Apple** in Nederland een eID gaat aanbieden. Het verdienmodel van Apple is vooral gebaseerd op de eigen (dure) hardware, en minder op het verhandelen van persoonsgegevens. Apple staat er om bekend dat het gegevens goed beschermt en in handen van gebruikers houdt. Een Apple eID zal attributen daarom zeer waarschijnlijk decentraal opslaan, in een (beveiligde hardware) wallet op de iPhone van de gebruiker. Als een gebruiker in wil loggen op website A, dan zal diens iPhone de relevante attributen rechtstreeks vanuit de wallet aan website A laten zien, zonder tussenkomst van Apple of andere partijen. Het bedrijf Apple registreert zulke logins in principe niet, net zoals Apple ook iPay-betalingen niet zegt te zien.

2. Stel nu dat ook **Facebook** in Nederland een eID gaat aanbieden. Dan is het redelijk om er van uit te gaan dat dit net zo zal gebeuren als bij de bestaande *Facebook Login*. Daarbij zullen alle persoonlijke attributen centraal bij Facebook opgeslagen worden. Wanneer een gebruiker dan bij website A in wil loggen, zal die gebruiker eerst doorgestuurd worden naar Facebook om daar in te loggen; Facebook zal vervolgens de relevante attributen vanuit de eigen systemen aan website A verschaffen.

De *decentrale* variant van Apple past goed in het huidige wettelijke kader, i.h.b. in de AVG, omdat deze aanpak inherent privacy-vriendelijk is en de gegevensverwerking minimaliseert. De *centrale* aanpak van Facebook is echter inherent niet privacy-vriendelijk, omdat een derde partij (namelijk Facebook zelf) kan bijhouden welke Nederlander wanneer en waar inlogt; daarmee kunnen gedetailleerde profielen opgebouwd worden, gebaseerd bijvoorbeeld op hoe vaak iemand online bij een slijter inlogt, of bij een psychiatrische kliniek, of bij een islamitisch of homo tijdschrift[3]. Dit centrale model past haarfijn in de surveillance economie van (machtige) commerciële organisaties. De centrale attributen-beheerder is een extreem gevoelige privacy-hotspot. Dat centrale model staat op gespannen voet met AVG art. 25.1, waar vereist

[3]Zie ook het artikel Inloggen bij de overheid met Google. Een goed idee? in Trouw van 18 jan. 2020.

wordt dat een (redelijke) privacy-vriendelijke oplossing gekozen moet worden indien beschikbaar.

Met art. 16.2 van het wetsvoorstel Digitale Overheid (WDO) wil het kabinet de mogelijkheid scheppen om ook het centrale eID-model juridisch mogelijk te maken. Expliciet wordt daar ruimte geschapen voor de opslag en verwerking van persoonlijke attributen (inclusief BSN) bij een partij als Facebook, of Huawei, of Itsme, of Baidu. Deze mogelijkheid staat niet alleen op gespannen voet met de AVG — waarmee een gang naar de rechter mogelijk is, zoals by SyRI — maar onderwerpt Nederlandse burgers ook aan onnodige surveillance door (machtige, buitenlandse) data-giganten. Dit ondermijnt de Nederlandse soevereiniteit (zie ook punt 5).

Verbeterpunt: De verwerking van persoonsgegevens als het BSN door toegelaten aanbieders van eID middelen is in art. 16 van het wetsvoorstel Digitale Overheid veel te ruim gesteld. Deze verwerking moet alleen toegestaan worden aan aanbieders van een *decentraal* eID-middel.

3 Transpartantie en open source

Software (programmatuur) vertelt een computer wat te doen. Wanneer die software openlijk gepubliceerd wordt — dat wil zeggen, 'open source' is — kan iedereen in principe controleren dat die software doet wat ze moet doen en geen verborgen achterdeurtjes bevat. Die openheid is in het bijzonder belangrijk voor software die gebruikt wordt voor taken die van algemeen (publiek) belang zijn. Deze transparantie van software wordt steeds breder, ook binnen de overheid, erkend en leidt tot een beleid van "open, tenzij". Digitale identiteit is het onderwerp bij uitstek voor het verplicht stellen van open source software, juist om via transparantie het vertrouwen van burgers te winnen.

Het gebruik van open source software heeft daarnaast ook grote economische voordelen, omdat verschillende partijen van elkaars werk gebruik kunnen maken en er op voort kunnen bouwen, bij eigen software productie — in Nederland zelf en niet elders. Dit voorkomt een *lock in*, waarbij men vast komt te zitten aan één leverancier, die de prijzen naar willekeur op kan drijven. Inderdaad, geloten (niet-open) software leidt vaak tot hoge kosten, zoals bij

eHerkenning, waar sprake is van zes verschillende leveranciers[4] die allemaal zelf in essentie dezelfde software ontwikkeld hebben en daar nu ieder de kosten voor terug willen verdienen. Er bestaat een groot maatschappelijk belang om voor taken van algemeen belang — zoals inloggen — te kiezen voor open source software.

Verbeterpunt: Een van de toelatingseisen voor aanbieders van eID-middelen in het wetsvoorstel Digitale Overheid moet zijn: gebruik van open source voor alle applicatie-software die met persoonsgegevens omgaat. Die eis moet worden uitgewerkt in de bijbehorende Algemene Maatregel van Bestuur (AMvB).

4 Markt of non-profit

Bij inloggen door bedrijven is er door de overheid expliciet voor gekozen om eHerkenning aan de markt over te laten. Dat paste in de tijdsgeest van dat moment. De tijd is nu rijp voor een andere aanpak die het algemene belang vooropstelt, uitgaande van het idee dat digitale identiteit geen handelswaar is[5].

Cruciale onderdelen van de ICT-infrastructuur kunnen uitstekend in een non-profit model georganiseerd worden. Een sterk voorbeeld daarvan is SIDN, de *stichting* internet domeinregistratie Nederland, die domeinnamen als irma.nl uitgeeft. SIDN vervult deze taak al jarenlang, naar volle tevredenheid, tegen relatief lage kosten. SIDN heeft een monopolie onder een convenant met het ministerie van Economische Zaken en Klimaat. Een ander voorbeeld is het pensioenregister dat als stichting, met een wettelijke basis, burgers inzicht geeft in de opgebouwde pensioenaanspraken.

Bij inloggen door bedrijven via eHerkenning is expliciet gekozen om inlogmiddelen aan de markt over te laten. Dit leidt nu tot groot verzet vanwege gedwongen winkelnering bij dure partijen. Voor inloggen door burgers moeten niet dezelfde fouten gemaakt worden. De stichting Privacy by Design en SIDN werken intensief samen bij het aanbieden van het open source eID-middel IRMA. Tientallen gemeenten hebben of ontwikkelen plannen voor het

[4] zie: eherkenning.nl/leveranciersoverzicht

[5] Zie ook de campagne goed-ID.org

gebruik van IRMA[6]. De gemeente Amsterdam ontwikkelt zelfs een nieuwe gebruikersinterface voor online identiteiten die binnenkort in de IRMA app geïntegreerd gaat worden. Zo onstaat een ecosysteem vanuit de eigen gemeenschap waarin meerdere partijen met open source software samenwerken. Ook verschillende partijen in de zorg dragen bij aan dit ecosysteem: daar wordt IRMA nu gebruikt[7], onder andere door Nedap, Ivido, Chipsoft en VGZ. Een wet Digitale Overheid zou juist voor zulke samenwerking een wettelijk kader moeten bieden.

Verbeterpunt: Laat het marktmodel voor digitale identiteiten los en organiseer een non-profit model, zoals met succes wordt toegepast op andere gebieden.

5 Digitale soevereiniteit en IRMA

Hierboven in punt 2 is een hypothische schets gegeven van eID-betrokkenheid van de grote Amerikaanse bedrijven Apple en Facebook. Het afgelopen jaar wordt in de Nederlandse politiek, terecht, groeiend belang gehecht aan digitale soevereiniteit. Juist daarin past geen dominante rol van commerciële ICT-giganten (big-IT). Wat wel goed past is het Nederlandse IRMA initiatief dat via een stichting, zonder winstoogmerk, een privacy-vriendelijk decentraal eID heeft ontwikkeld. IRMA is up-and-running, werkt gratis of tegen minimale kosten, en wordt door een snel groeiend aantal partijen in de praktijk gebruikt, met name bij gemeenten, in de zorg en bij verzekeraars[8].

Omdat IRMA in een stichting is ondergebracht kan IRMA niet zomaar opgekocht (en om zeep geholpen) worden door big-IT. IRMA is een werkend en levensvatbaar Nederlands initiatief dat erop gericht is gevoelige persoonsgegevens in Nederland te houden, onder controle van burgers zelf[9]. Gegeven het bestaan van dit succesvolle eID-middel IRMA, dat uit de samenleving

[6]Zie ook de logo's van de ondersteunende gemeenten op de IRMA-BRP attribuut uitgifte pagina.

[7]In het antwoord op recente kamervragen (zie i.h.b. vraag 7) stelt minister Knops duidelijk dat DigiD niet het verplichte eID-middel in de zorg is.

[8]Zie bijvoorbeeld de onafhankelijke beoordeling van IRMA voor de verzekeringssector op de website sivi.org.

[9]Zie ook de beoordeling van IRMA in het recente Handvest voor de Slimme Stad van het wetenschappelijke bureau van GroenLinks.

zelf voortgekomen is en daardoor omarmt wordt, is het moeilijk te begrijpen dat het kabinet met het wetsvoorstel Digitale Overheid er voor kiest om wettelijke ruimte te scheppen om persoonsgegevens elders bij centrale partijen onder te brengen. Eigen beheer over digitale identiteit is niet alleen van belang voor de Nederlandse soevereiniteit, maar ook voor de nationale veiligheid.

Verbeterpunt: Het wetsartikel 16.2 biedt de basis voor onwenselijke digitale surveillance van het online gedrag Nederlandse burgers en voor ondermijning van de Nederlandse digitale soevereiniteit. De in punt 2 reeds voorgestelde beperking tot *decentrale* eID-middelen in art. 16 is ook omwille van national soevereiniteit van groot belang.

6 Maatschappelijke behoefte

Het wetsvoorstel Digitale Overheid stelt regels aan het inloggen bij de overheid zelf. Het heeft daarmee geen oog voor wat er maatschappelijk, buiten de overheid, hard nodig is om de Nederlandse digitale economie te ondersteunen. Onder andere thuiswinkel.org en de Cyber Security Raad hebben er recentelijk op aangedrongen dat de Rijksoverheid het betrouwbaar inloggen niet alleen voor zichzelf regelt, maar ook breder kijkt naar wat maatschappelijk (dringend) nodig is. Daarbij heeft de Rijksoverheid een cruciale rol, als verschaffer van een bron-identiteit. Tevens speelt de Rijksoverheid een cruciale rol bij het verschaffen van belangrijke attributen aan burgers — vanuit relevante registers zoals BRP, BIG, KvK etc. Juist daar moet het wetsvoorstel Digitale Overheid de wettelijke ruimte voor geven[10]. Het bestaande eID-middel IRMA biedt nu reeds de mogelijkheid voor zowel publiek als privaat gebruik. Verdere uitrol van IRMA voorziet daarmee in een grote maatschappelijke behoefte, niet alleen voor burgers maar ook voor (vertegenwoordigers van) bedrijven.

Verbeterpunt: Het wetsvoorstel Digitale Overheid biedt onvoldoende ruimte voor de rol van de overheid die attributen verschaft aan burgers (in een

[10]IRMA is nu onder andere gekoppeld aan de Basisregistratie Personen (BRP). Indien IRMA ook aan de KvK gekoppeld wordt, zouden bedrijven en andere organisaties zonder kosten bij de overheid in kunnen loggen. Zo'n koppeling vormt de basis voor een (snelle en eenvoudige) oplossing van de huidige problemen met eHerkenning.

decentraal eID-model), waarmee burgers binnen, maar vooral ook buiten de overheid, veel zaken digitaal kunnen regelen.

7 Het amendement Online Identiteit

De Tweede Kamerleden Middendorp en Verhoeven pleiten voor een "online identiteit" voor alle burgers. Deze naam "online identiteit" leidt tot een zekere mate van verwarring en leidt af van de kern. De Kamerleden beogen de inrichting van informatiestromen rondom persoonsgegevens binnen de overheid zelf te veranderen en burgers daarin (terecht) meer transparantie en invloed te geven; zij doen dat vanuit een één-bron-gedachte. Zij willen dat alle uitwisseling van gegevens van burgers binnen de overheid verloopt via één "knooppunt". Burgers moeten zelf toegang tot dat knooppunt kunnen krijgen en moeten daar kunnen zien wie welke gegevens heeft verwerkt binnen de overheid (en daar ook invloed op kunnen uitoefenen). Dit vergt een substantiële aanpassing van de gegevenshuishouding van de overheid, die veel gevolgen heeft voor overheidsorganisaties zoals de Belastingdienst, UWV, DUO, etc. die nu hun eigen administraties met persoonsgegevens voeren, waardoor burgers geen eenduidig overzicht hebben.

Deze bron/knooppunt-systematiek hangt enigzins samen met de eID discussie maar gaat in essentie over iets anders, namelijk over de gegevenshuishouding binnen de overheid en niet over inloggen en authenticatie.

Verbeterpunt: Het wetsvoorstel Digitale Overheid en het amendement Middendorp-Verhoeven vermengen zaken die verschillend van aard zijn. Deze onderwerpen dienen gescheiden te worden omdat vermenging niet bijdraagt aan een heldere discussie.

Prof. B. Jacobs,
Voorzitter stichting Privacy by Design.

Email: voorzitter@privacybydesign.foundation