Open brief aan: dhr. R.W. Knops
Staatssecretaris van Binnenlandse
Zaken en Koninkrijksrelaties

Stichting Privacy By Design
privacybydesign.foundation

Nijmegen, 12 augustus 2019

Geachte Heer Knops,

Deze open brief schrijf ik u in mijn hoedanigheid van voorzitter van de stichting *Privacy by Design*, de non-profit organisatie achter het open source identiteitsplatform IRMA. Ik schrijf een *open* brief vanuit de gedachte dat de materie ook anderen aangaat.

De aanleiding voor mijn schrijven is uw brief van 13 juni 2019 aan de Tweede Kamer (kenmerk 2019-0000362393) over een andere toelatingssystematiek voor inlogmiddelen voor burgers. U kondigt daarin een belangrijke, positieve beleidswijziging aan, namelijk om private inlogmiddelen via een open systeem van toelating te gaan verwerven.

Tegelijkertijd bevat deze brief van 13 juni een omineuze voorlaatste alinea. U spreekt daarin over de nieuwe toe te laten private partijen en schrijft: "Gelet op de verwerking van persoonsgegevens (waaronder mogelijk het BSN) die deze partijen mogelijk verwerken moet grondslag voor verwerking (art 16, bescherming van persoonsgegevens) aangepast worden."

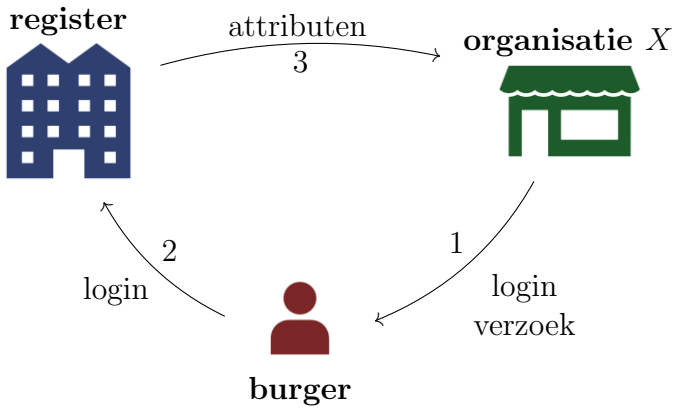
Achter deze aankondiging gaat een *centralistisch* paradigma schuil dat nadere aandacht en discussie verdient, vooral ook omdat er een alternatief *decentraal* paradigma bestaat dat privacy-vriendelijk is, nu al toegepast wordt, en geen verdere privacy-onvriendelijke wetswijziging vereist.

De onderbouwing van deze laatste beweringen vereist enige achtergrond. Ik veroorloof mij om die hieronder eerst uiteen te zetten.

Begin intermezzo

Met betrekking tot elektronische identiteiten (eID's) zijn twee paradigma's (of architecturen) te onderscheiden, namelijk een 'centrale' en 'decentrale'. Ik zal deze via plaatjes illustreren. De *centrale* architectuur is dominant en wordt gebruikt door partijen als Facebook, iDIN, Itsme en ook DigiD. Hierbij wordt een burger die bij (de webpagina van) organisatie X wil inloggen doorgestuurd naar een centrale 'register' partij met identiteitsgegevens (attributen), waar de daadwerkelijke login plaatsvindt. Deze centrale partij geeft vervolgens aan organisatie X de benodigde identiteitsgegevens (attributen) door.

Schematisch ziet dat er als volgt uit.



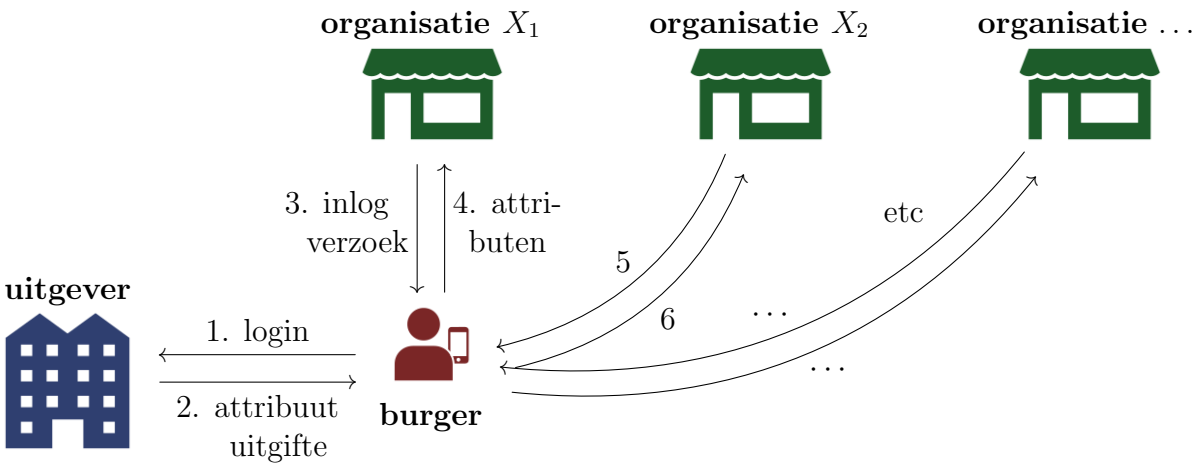
Deze cyclus wordt continu doorlopen, bij iedere organisatie $X_1, X_2, X_3, \ldots$ waar de burger in wil loggen. Het cruciale kenmerk van deze centrale architectuur is dat alle logins via de register partij verlopen, waardoor deze tussenliggende partij voor iedere login:

- een bedrag kan vragen aan organisatie X;
- kan bijhouden bij welke organisatie de betreffende burger op welk moment met welke persoonlijke attributen inlogt. Hierdoor is de register partij een *privacy hotspot*. Regelmatige logins bij een psychiatrische kliniek, bij een slijter, of gewoon bij een bepaalde krant, vakbond of kerkgenootschap vertellen veel over het privé leven van een burger.

De Nederlandse banken vragen via hun iDIN systeem op zo'n manier enkele dubbeltjes per login; voor hen is het bovenstaande eerste punt van groot belang. Facebook biedt *Facebook login* gratis aan, maar doet dat omdat Facebook vooral geïnteresseerd is in de gegevens, om gedetailleerde login profielen van gebruikers op te bouwen, om deze te koppelen aan andere gegevens, en om deze verzamelde gegevens vervolgens te verkopen en/of zelf te gebruiken om mensen commercieel (of politiek) te manipuleren.

De *decentrale* architectuur werkt anders. Daarin heeft een burger in principe eenmalig contact met de register partij om daar zelf (een kopie van) de eigen attributen op te halen, voor opslag in een speciale app op de eigen telefoon. Vervolgens kan de burger (een selectie van) deze attributen voor login zelf tonen, zonder tussenkomst van anderen. Zulke logins kunnen herhaald worden, bij verschillende organisaties, zonder verdere tussenkomst van

de register partij. In een plaatje:



Kenmerkend voor deze decentrale aanpak is dat de (gekopieerde) persoonsgegevens/attributen bij de burger zelf opgeslagen worden. Hierdoor kan de register partij niet bijhouden waar de burger de eigen attributen gebruikt om in te loggen. Deze architectuur is privacy-vriendelijk, *by design*.

In voordrachten spreek ik regelmatig over het grote verschil tussen de centrale en de decentrale architectuur, vooral om het impliciete verschil in machtsverhoudingen expliciet te maken. Daarbij stel ik het publiek vaak de vraag: wat denkt u, aan welke architectuur zou de Chinese overheid de voorkeur geven?

Inderdaad, machtige ICT-bedrijven en dictatoriale regimes zullen altijd aansturen op de centrale architectuur. Er zijn echter alternatieven. De keuze tussen de ene of de andere architectuur dwingt ons tot de vraag: in wat voor samenleving willen wij leven?

Natuurlijk kan men zeggen: wij stellen ons 'neutraal' op en laten deze keuze over aan de markt. Dat is echter geen neutrale opstelling want daarmee is de keuze feitelijk al gemaakt. Dit is bij uitstek een gebied waar de politiek een doorslaggevende rol kan — en misschien ook moet — spelen, in het verdedigen van publieke waarden, ook in de digitale wereld. Juist op dit gebied kan een eigen Europese, op waarden gebaseerde opstelling, zich manifesteren.

Eind intermezzo

Los van de zojuist genoemde gewichtige maatschappelijke/politieke vragen biedt de decentrale architectuur unieke gebruiksmogelijkheden. De burger heeft hierbij 'regie op gegevens' en kan uit verschillende bronnen zelf attributen verzamelen en in de eigen app opslaan. Voorbeelden van zulke attributen zijn persoonsgegevens uit de BRP, maar ook contactgegevens (e-mail, 06), beroepsgegevens (bijv. uit het BIG register, of uit het KvK register), inkomensgrenzen, diplomagegevens, klantgegevens (bijv. kortingskaarten), enz, enz. In het centrale model zouden al die persoonsgegevens bij de centrale register partij (denk: Facebook) opgeslagen moeten worden. Niet alleen wettelijke beperkingen, maar ook voorspelbare reserves van burgers, staan dat in de weg.

Het opvallende aan de voorlaatste alinea van uw brief van 13 juni is dat u daarin aankondigt te willen onderzoeken of u het centrale model verder kunt faciliteren, en private

centrale register partijen (iDIN, Itsme, Facebook, wie weet ook Huawei) via een wetswijziging de wettelijke ruimte wil bieden om meer persoonsgegevens (i.h.b. het BSN) in hun eigen, private systemen op te slaan. U kiest hierbij nadrukkelijk voor een privacy-onvriendelijke aanpak die machtige ICT-partijen alleen maar machtiger maakt. In het licht van het bovenstaande is dit voor mij onbegrijpelijk.

Ik snap goed dat dit persoonlijke onbegrip mijnerzijds voor u, beleidsmatig, geen enkele rol speelt. Een grotere rol is mogelijk weggelegd voor het algemene (juridische en beleidsmatige) principe van subsidiariteit: wanneer een doel met minder ingrijpende maatregelen (i.c. zonder privacy-onvriendelijke wetswijziging) bereikt kan worden heeft dat altijd de voorkeur. Ook de eis van data-minimalisatie (uit de AVG) is hierbij van toepassing: zonder de tussenliggende partijen in het centrale model worden immers minder persoonsgegevens verwerkt.

Aan het begin van mijn brief heb ik direct mijn betrokkenheid bij het identiteitsplatform IRMA expliciet gemaakt. Ik heb daarbij geen financiële belangen: ik ben onbezolgdigd voorzitter van een stichting zonder winstoogmerk die beoogt het gebruik van privacy-vriendelijke en goed-beveiligde open source ICT te bevorderen. En inderdaad, IRMA is gebaseerd op het decentrale model en laat via een groeiend aantal toepassingen zien dat dit model goed functioneert en levensvatbaar is, tegen minimale kosten. Daarbij wordt ook nu al het BSN in de eigen IRMA app van burgers opgeslagen — en nergens anders — via een IRMA-BRP koppeling die al bijna een jaar via gemeenten bestaat. Deze koppeling heeft een juridische toets van de landsadvocaat Pels-Rijcken doorstaan, en vereist (daarmee) geen wijziging van de wet. De onderwerpen die ik hier aansnijd overstijgen hun realisatie in IRMA. Er verschijnen meer en meer identiteitsoplossingen (zoals Sovrin) die gebaseerd zijn op de hierboven geschetste decentrale architectuur.

Mijn doel met deze brief is om u er toe uit te nodigen om de *politieke* keuze te maken voor een *decentrale* architectuur, en niet, zoals u aangekondigd heeft, via onnodige wetswijzigingen verdere ruimte te scheppen voor de *centrale* architectuur. Het nieuwe door u aangekondigde, op toelating gebaseerde, eID-stelsel geeft u de mogelijkheid daartoe strekkende eisen te stellen. Zelfs kunt u nu eisen dat toegelaten systemen met open source software werken, omwille van transparantie, om aansluiting te vergemakkelijken, en om dure *vendor lock-ins* te vermijden.

Mocht het bovenstaande de behoefte oproepen tot nadere onderlinge uiteenzettingen, dan ben ik daartoe gaarne bereid.

Met vriendelijke groet,

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

Email: voorzitter@privacybydesign.foundation

Cc: Vaste Kamercommissie voor Binnenlandse Zaken.