# Memo

Reactie Besluit identificatiemiddelen voor burgers i.v.m.

Datum
11 mei 2020

Inzenders
SIDN (Stichting Internet Domeinregistratie Nederland) en Stichting Privacy by Design (PbD).

Blad
1/4

**Contact**
T 026 352 55 00
support@sidn.nl
www.sidn.nl

**Bezoekadres**
Meander 501
6825 MD Arnhem

**Postadres**
Postbus 5022
6802 EA Arnhem

Aan & Onderwerp
Ministerie van Binnenlandse Zaken
Reactie op de internet consultatie “Besluit identificatiemiddelen voor burgers ivm WDO” op MijnOverheid.nl

Auteur
Bob (B.) Kronenburg SIDN
bob.kronenburg@sidn.nl

## Indieners

SIDN (Stichting Internet Domeinregistratie Nederland) en Stichting Privacy by Design (PbD). Contactpersoon: Bob Kronenburg <bob.kronenburg@sidn.nl>

## Betrokkenheid

SIDN en Privacy by Design werken samen, onder contractuele overeenkomst, aan de ontwikkeling van IRMA, een privacyvriendelijk decentraal identiteits-ecosysteem, zie http://www.irma.app). SIDN beheert binnen deze samenwerking de centrale infrastructurele componenten die zorgen voor een veilig, betrouwbaar en solide functioneren van het IRMA-ecosysteem. Stichting Privacy by Design ontwikkelt en onderhoudt de software voor de IRMA-app. Beide partijen hebben doelstellingen gericht op een veilig en privacyvriendelijk internet en hebben geen winstoogmerk.

## Wat is IRMA?

IRMA staat voor *I Reveal my Attributes*. IRMA-gebruikers kunnen allerhande kenmerken (attributen) over zichzelf verzamelen in "kaartjes" in hun app. Met behulp van de IRMA-app kunnen gebruikers relevante gegevens tonen aan en delen met partijen om zichzelf te authentiseren. Met IRMA beheert een burger dus zelf wat hij deelt en met wie. Ook kunnen IRMA-gebruikers toestemmingen verlenen aan derden en deze ondertekenen met hun attributen.

Het IRMA-stelsel is decentraal: alle persoonsgegevens (op kaartjes) staan alleen in de app van de gebruiker en nergens anders (ook niet in de cloud). Er is geen centrale database waar alle attributen van alle gebruikers opgeslagen worden. Ook is er geen centrale log van wie op welk moment waar inlogt.

Kortom, IRMA is gebaseerd op het privacy-by-design principe en heeft geen privacy-hotspot, zoals in een centrale organisatie van eID-middelen. Zo'n privacy-hotspot is mogelijk in strijd met de AVG.

# 1 Belangrijkste kritiekpunten over het conceptbesluit 'Identificatiemiddelen voor burgers'

Hieronder worden de drie belangrijkste kritiekpunten uiteengezet: het conceptbesluit bevat belangrijke hiaten op het gebied van architectuur, attributen, en transparantie. De nadruk moet juist liggen op eID-middelen die decentraal, attribuut-gebaseerd en open source zijn.

## 1.1 Eenzijdige centrale benadering

Het conceptbesluit lijkt vooral opgesteld vanuit het gedachtengoed van centraal verwerkende identificatiemiddelen. Decentrale oplossingen, zoals IRMA of andere *self-souvereign*-oplossingen, zijn in het conceptbesluit onvoldoende in scope, terwijl het minimaliseren van data-hotspots juist in het belang is van een veilige en privacyvriendelijke publieke digitale infrastructuur.

Centrale middelen, zoals bijvoorbeeld DigiD en iDIN, zijn verwerkers en beheerders van de attributen en gebruiksgegevens van hun gebruikers. Zij slaan identiteitsinformatie van veel gebruikers op en zijn verantwoordelijk voor het deugdelijk beheer van deze informatie. Zoals minister Knops in het kamerdebat over de WDO aangaf, is het onwenselijk dat de data die deze centrale verwerkers in beheer hebben, voor andere doeleinden gebruikt worden dan authenticatie/inloggen bij de overheid. Het volstaat dan niet om "commerciële doeleinden" uit te sluiten om te voorkomen dat identiteits- en gedragsinformatie van individuele gebruikers voor andere doeleinden gebruikt worden. Ieder ander gebruik dient uitgesloten te worden, commercieel of niet.

Bovendien beperkt een centrale aanpak de functionaliteit van een eID-stelsel. Zo'n stelsel is gebaat bij een grote hoeveelheid attributen die voor allerlei doeleinden door burgers gebruikt kunnen worden. Om zichzelf in allerlei situaties op de gepaste (proportionele) wijze bekend te maken. Wanneer de architectuur zodanig is ingericht (of afgedwongen wordt) dat dit soort attributen centraal opgeslagen moeten worden, zijn minder burgers en beheerders van registers bereid om mee te werken; vanwege de privacy- en securityrisico's van een dergelijke centrale concentratie van gevoelige persoonsgegevens. Zoals met IRMA nu in de praktijk blijkt zijn beheerders van registers wel degelijk bereid om attributen rechtstreeks aan burgers over te dragen. Sterker nog, de AVG verplicht ze daartoe.

## 1.2 Attributen ontbreken

In het conceptbesluit wordt niet gesproken over attributen, terwijl deze de basis vormen voor modern privacyvriendelijk identitymanagement. Impliciet lijkt de aanname te zijn dat de overheid slechts het BSN als attribuut nodig heeft. Dit is echter onjuist, bijvoorbeeld omdat een burger ook bij de overheid proportioneel moet kunnen inloggen, volgens principes van dataminimalisatie uit de AVG. Voor het melden van een losliggende stoeptegel hoeft (feitelijk: mag) een burger niet met BSN in te loggen bij de eigen

gemeente. En voor bijvoorbeeld het bevestigen van een ziekmelding bij het UWV, heeft een arts geen BSN-attribuut nodig, maar een BIG- (of AGB-) attribuut.

Een attribuut-gebaseerde benadering gaat bij uitstek goed samen met een decentrale architectuur, waarbij (kopieën van) attributen rechtstreeks vanuit registers aan de burger overgedragen worden in een eigen kluis/app. Zo kunnen burgers zichzelf met die attributen, op gepaste proportionele wijze, bekendmaken.

Het conceptbesluit maakt daarmee samenhangend onvoldoende onderscheid tussen een eID-middel als kluis (container van attributen) en tussen de daarin opgeslagen attributen. Dit is zeer relevant voor de betrouwbaarheid van de eID-middelen (in eIDAS-kader). De kluis zelf moet een hoge mate van betrouwbaarheid hebben. Maar de betrouwbaarheid van attributen kan sterk variëren. Een BSN- of BIG-attribuut moet op niveau substantieel of hoog zitten, terwijl voor e-mail of voor het lidmaatschap van de lokale duivenclub het niveau laag kan volstaan. Deze hele differentiatie tussen drager en inhoud ontbreekt in het conceptbesluit.

### 1.3 Open source is geen vereiste in het conceptbesluit

Onlangs heeft staatssecretaris Knops een “Open tenzij en aanpak open source 2020-2021” gepubliceerd[1]. In het conceptbesluit wordt hieraan niet gerefereerd. Deze richtlijn gaat primair over software die zelf ontwikkeld wordt door de overheid en over software die door de overheid ingekocht wordt. In het toelatingskader voor middelen die inloggen bij de overheid mogelijk maken, koopt of maakt de overheid zelf geen software maar laat deze wel toe, door eID-middelen te erkennen. In het kader van transparantie, controleerbaarheid en consistentie is het maatschappelijk zeer wenselijk hierin ook een opensource-eis op te nemen. Bij de recente discussie over traceer-apps in het kader van corona was de maatschappelijke druk zeer groot om exclusief opensourcesoftware te gebruiken voor systemen die met gevoelige gegevens van burgers omgaan. Daaraan is door de overheid, terecht, gehoor gegeven. Eenzelfde maatschappelijk druk en beweging is op dit onderwerp te verwachten: het is eenvoudigweg ondenkbaar dat een overheid vandaag de dag geen harde opensource-eis stelt aan eID-middelen die op een zeer directe manier omgaan met zeer persoonlijke gegevens (attributen) van burgers.

Overigens is door staatssecretaris Knops in het kamerdebat van 5 februari 2020[2] zelf op de relevantie gewezen van zijn “open tenzij”-beleid in het kader van eID-middelen. Na vragen over een opensourceverplichting voor eID-middelen antwoordt de minister:

*“Met betrekking tot open source merk ik op dat door mij een brief wordt voorbereid, waarin de mogelijkheden van open source in kaart worden gebracht. Ik verwacht deze brief in maart te kunnen aanbieden aan uw Kamer.” (p. 50-3-11)*

En:

*“Het opensourceverhaal waar we het eerder over hadden, is ook belangrijk, om te voorkomen dat je dadelijk klem komt te zitten in systemen waar je niet meer uit kunt en waar je wel voor moet betalen.” (pagina 50-3-19)*

Ten overvloede wordt er hierop gewezen dat de Tweede Kamer de WDO-motie van mevrouw Özütok (GroenLinks) aangenomen heeft, waarin de regering verzocht wordt te waarborgen dat zo veel mogelijk opensourcesoftware gebruikt wordt in applicaties die persoonsgegevens verwerken.

## 2 Aanvullende opmerkingen

1. Het conceptbesluit vereist bij artikel 2.3 lid c dat de gebruiker inzicht moet hebben in authenticatiehandelingen die zijn verricht met het middel. Deze formulering laat ruimte voor interpretatie en vereist daarom nadere specificatie. Is het bijvoorbeeld genoeg dat de burger ziet wanneer zijn middel gebruikt is? Of moet ook zichtbaar zijn waar het gebruikt is? En ook welke gegevens daar onthuld zijn? Vanzelfsprekend draagt een afgedwongen centrale opslag van zulke gegevens sterk bij aan het privacy-onvriendelijke karakter van een centralistische benadering en geeft zulke opslag ruimte voor verder ondeugdelijk gebruik van deze gegevens. Omdat juist op dit punt het verschil tussen een centrale en decentrale architectuur zichtbaar wordt is hier een nadere uitwerking wenselijk.

2. In de beraadslagingen rondom de Wet Digitale Overheid in de Tweede Kamer is met nadruk gewezen op de positieve ervaringen die gemeenten hebben met IRMA en is staatssecretaris Knops verzocht gebruik te maken van deze ervaringen. In diezelfde beraadslagingen zijn de voordelen van een non-profit benadering benoemd door woordvoerders van meerdere politieke partijen. Dit zou moeten leiden tot een non-profit voorkeur in het conceptbesluit.

[1] Zie: https://www.rijksoverheid.nl/documenten/publicaties/2020/04/17/overwegingen-bij-open-tenzij-en-aanpak-open-source

[2] Zie het verslag op: https://www.tweedekamer.nl/downloads/document?id=c0016d1a-f884-4dff-a78f-00253a303e74&title=Wet%20digitale%20overheid.pdf