SIDN
Bob Kronenburg
Meander 501
6825 MD Arnhem

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

Bezoekadres
Meander 501
6825 MD Arnhem

Postadres
Postbus 5022
6802 EA Arnhem

KvK
Arnhem 41 21 57 24

Bankgegevens
Rabobank
NL09RABO014.51.16.646
BIC
RABONL2U
Incassant ID
NL04ZZZ412157240000

Btw-nummer
NL8048 02 671 B01

Betreft	Datum	Blad
Reactie SIDN op de 'Regeling nadere eisen toelating identificatiemiddelen WDO'	05 december 2022	1/3

Behandeld door
Bob Kronenburg

E-mail contactpersoon
bob.kronenburg@sidn.nl

Classificatie
Publiek

Beste lezer,

Graag maak ik van de gelegenheid gebruik om namens SIDN en haar privacyvriendelijke identificatiedienst feedback te geven op de voorgestelde regeling.

Middelen in relatie tot wallets

Wat ons opvalt is dat de regeling 'middelen' in klassieke zin beschrijft. Daardoor voorziet de regeling niet in situaties waarin 'middelen' via een Self Sovereign Identity Wallet (SSI) worden gebruikt om gebruikers toegang te geven tot overheidsdiensten. Neem als voorbeeld met IRMA. Dit is een volledig decentraal systeem waarbij een gebruiker gegevens uit betrouwbare bronnen zelf beheert en kan gebruiken.

- Om 2 redenen is het noodzakelijk om goed vast te leggen hoe we moeten omgaan met een 'middel' dat veilig opgeslagen is op de telefoon van een burger in een 'drager/wallet' (als credential set, attribuut of attestatie):
    1. In Europa zijn er veel ontwikkelingen op het gebied van de EU-identiteitwallets;
    2. In Nederland zijn steeds meer partijen die SSI-diensten leveren die toelatingsaspiraties hebben.
- Het is zeer nuttig om voor deze regeling een goed onderscheid te maken tussen 'centrale middelen' en 'wallet-oplossingen'. Omdat ook andere variabelen, aandachtspunten en voorwaarden ten aanzien van opslag, beveiliging en gebruikersregistratie noodzakelijk zijn. En toezicht en handhaving hiervan ook andere vraagstukken en aandachtspunten met zich meebrengen.
- SSI-wallets, waaronder IRMA, verwerken gegevens in een directe verbinding tussen bron (Issuer) en gebruiker, of gebruiker en vragende partij (Verifier) zonder tussenkomst van een centrale infrastructuur. De gegevens van de gebruiker staan versleuteld opgeslagen op de telefoon van de gebruiker. SIDN stelt gebruikers in staat IRMA te gebruiken, maar wij kunnen niet zien wie de gebruiker is of welke

gegevens hij/zij ontvangt en toont. Ook zien wij niet van en aan wie de gebruiker deze gegevens ontvangt en/of toont. Hier is dus géén sprake van centrale opslag van gebruikersgegevens, het gedrag van een gebruiker kan niet worden gevolgd Dit past helemaal in de geest van de voorgestelde Wet Digitale Overheid (WDO) en de EU-ambities voor digitale identiteitswallets. Er moet ruimte komen in de regeling voor dergelijke decentrale oplossingen.

Openbare broncode

Wij zien de verplichtte publicatie van de broncode van toegelaten middelen/wallets als waardevol. Het is een extra bewijs dat de makers van software instaan voor de kwaliteit ervan. Waar in veel van de discussies geschermd wordt met “closed source is veiliger” of “open source betekent dat er een paar vrijwilligers werken aan de oplossing” is de realiteit heel anders:

- Closed source: afnemers en gebruikers hebben geen keus de beloftes van de aanbieder rondom privacy en security te geloven. Men heeft geen inzicht in hoe het product werkt en wat er in de praktijk gebeurt.
- Open source: veiligheid en privacy zijn geen belofte, maar door iedereen te toetsen. De source code is inzichtelijk en daardoor kan iedereen het bewijs toetsen.
- In beide gevallen zullen professionele partijen werken aan een oplossing voor het eID vraagstuk. Maar in de praktijk zal de betrouwbaarheid en veiligheid van Open Source groter zijn. Het argument dat closed source veiliger is doordat kwaadwillenden geen toegang hebben tot de broncode gaat niet op. “Security through obscurity” is een begrip dat al jarenlang achterhaald is binnen softwareontwikkeling.

Het is nog onduidelijk hoe de overgang van closed source naar open source geregeld wordt. Als de uiteindelijke doelstelling is om alle toegelaten middelen onder open-source verplichting te publiceren, is het belangrijk om deze overgangsperiode zo kort mogelijk te houden. Wij adviseren dan een maximale periode te hanteren van 1 jaar.

Wij juichen de belofte van de staatssecretaris toe om zelf bij te dragen aan het ontstaan van een ontwikkelcommunity. Een goed instrument hiervoor is het beschikbaar stellen van “bounty incentives”. Dit kan fungeren als aanjager om alle toegelaten middelen te blijven beproeven door hackers en de community.

Ten slotte wijzen wij op het feit dat de EU in haar plannen open source prefereert. De referentiewallet van de EU is al op basis van open source-publicatieplicht via een tender vergund.

Logging van gebruik van middelen

Het voorkomen van centrale databases lijkt ons wenselijk. Daarvoor dient er een verbijzondering van de regeling te komen die ruimte laat voor privacybeschermende logging. Een SSI-wallet, zoals IRMA, houdt in de wallet zelf het loggen bij van het gebruik van middelen en attributen. In tegenstelling tot andere wallets die op een centrale database deze

gegevens vastleggen waar ook logs van meerdere gebruikers worden vastgelegd. Zo'n omvangrijke centrale database brengt extra veiligheidsrisico's met zich mee.

- Registratieplicht van gebruikersgegevens van een toegelaten middel
  In art 2.7 wordt nadrukkelijk om gegevens van de gebruiker gevraagd in een registratieproces, waarbij een gebruiker zichzelf moet identificeren om gebruik van een middel/oplossing te kunnen maken. Maar dit is in principe niet nodig als er gebruik wordt gemaakt van decentrale SSI-oplossingen.
- Op basis van privacy by design-principes kan de IRMA-wallet volledig anoniem gebruikt worden. Alleen als een gebruiker dat zelf wenst kan deze via een mailadresregistratie een herstelfunctie aanvragen. Daardoor hoeft SIDN helemaal niets van haar IRMA-gebruikers te weten bij registratie, dit is privacy by design in de meeste pure vorm. Als de gebruiker de telefoon verliest of deze stuk gaat kan deze de herstelfunctie gebruiken om de oude installatie onbruikbaar te maken. En vervolgens een nieuwe app installeren en de gegevens die de gebruiker in bezit had opnieuw bij de bron(nen) op te halen.

Onze vraag met betrekking tot de registratieplicht is: Waarom wordt in deze regeling geen rekening gehouden met, en onderscheid gemaakt tussen, een centraal gefaciliteerd middel en decentrale wallet-oplossingen die middelen in beheer van de gebruiker brengen?

Tot besluit

Wij adviseren om meer onderscheid te maken tussen centraal verwerkte middelen (vanuit een centrale database) ten opzichte van identiteitswallets, waarbij de opgeslagen middelen op basis van decentrale dataopslag moeten functioneren en waarop de privacy by design-principes van toepassing zijn.

Wij verzoeken de staatssecretaris deze regeling te verbijzonderen. Ook zou bij toezicht en handhaving zowel de centrale als decentrale oplossingsvarianten moeten worden meegenomen.

Wij vertrouwen op een spoedige vaststelling van de Wet Digitale Overheid met een duidelijk toelatingskader voor private middelen.

Met vriendelijke groet,
SIDN

Bob (B.) Kronenburg
SIDN