Geachte Mevrouw Van Huffelen,

Wij wensen U, de Staatssecretaris voor Koninkrijksrelaties en Digitalisering, te bedanken voor het delen van het concept Ministriële Regeling betreffende de nadere eisen toelating identificatiemiddelen Wet Digital Overheid (WDO).

Als eIDAS erkende speler verwelkomen wij een dergelijke openbare consultatie. Aangezien deze nieuwe wetgeving een kader dient te creëren waarbinnen burgers zich op een veilige doch makkelijke manier digitaal kunnen identificeren, is het niet meer dan logisch dat strikte vereisten worden opgelegd.

Desalniettemin zijn er aantal aandachtspunten waarop we graag constructieve feedback geven, teneinde een werkbaar ecosysteem uit te bouwen waarbinnen alle EU-burgers in de nabije toekomst over een veilige en gebruiksvriendelijke digitale identiteit beschikken, die ten allen tijde hun privacy respecteert. In onze opinie wensen wij daarom dieper in te gaan op de volgende aspecten:

- Verplichting van het plaatsen van de gebruikte software in openbroncode
- Contractuele verplichtingen
- Gebruik van biometrie
- Machtigen
- Verdienmodel
- Inconsistenties met bestaande normen, kaders en standaarden

1. Verplichting van het plaatsen van de gebruikte software in openbroncode

a. Security

Het plaatsen van software in open source is geen garantie op verhoogde veiligheid. Recente wereldwijde incidenten (Log4J, Solarwinds, …) hebben laten zien dat dit mogelijks risico's met zich meebrengt op verschillende vlakken. Supply chain attacks worden hierdoor mogelijk gemaakt. Tevens geeft het inzicht aan criminele actoren op de interne architectuur waarbij ze een nog groter voordeel krijgen dan ze vandaag al hebben bij het ontwikkelen en plannen van hun aanvallen. Als de software bijkomstig dan ook volledig via een open source community wordt onderhouden dan is er geen enkele borging op het vlak van tijdige incident response processen. eIDAS heeft om de veiligheid te borgen reeds gezorgd voor een certificatie kader via erkende Conformity Assessment Bodies voor vertrouwensdiensten en peer reviews via het EU Cooperation Network betreffende de implementatie van de CIR voor e-identification means. Deze CAB's krijgen tijdens de jaarlijkse audits volledige inzage in de architectuur en processen onder NDA. Deze CAB's staan in Europa onder toezicht van de National Accreditation Bodies die erop toezien dat deze auditeurs met kennis van zaken deze audits correct uitvoeren.

b. Intellectuele Rechten van private spelers

Alle geaccrediteerde oplossingen binnen het eIDAS kader maken vandaag gebruik van gecertificeerde componenten. Het is onmogelijk voor 1 partij om alle ontwikkelingen op het vlak van software, hardware, hosting, cryptografie, etc.. onder 1 dak te huisvesten. Daarvoor wordt beroep gedaan op gespecialiseerde deeloplossingen (bv HSM's, RQSCD's, SDK's voor het uitlezen van ID documenten, biometrische oplossingen, …) die elkeen eigen deelcertificaties ondergaan tegen de geldende standaarden. Het is ondenkbaar dat al deze partijen, die dikwijls ook patenten hebben op hun software, deze in open source zullen vrijgeven. Daarbovenop zullen private spelers die niet binnen het eIDAS kader werken een concurrentieel voordeel krijgen door inzicht in de oplossingen van partijen die wel onder het eIDAS kader moeten werken. Dit zal leiden tot een geforceerde concurrentievervalsing.

c. Business Continuity

Er wordt gesteld dat de broncode zo moet zijn dat deze op een workstation kan geinstalleerd en getest worden. Veiligheidsoplossingen vereisen echter veel meer dan een workstation (bv cloud componenten en infrastructuur, HSM's in datacenters, …). Een oplossing die standalone op een workstation kan draaien zal onmogelijk aan alle security vereisten kunnen voldoen.

2. Contractuele verplichtingen

Er wordt gesteld dat een geselecteerde oplossing binnen de 3 maand de nodige integraties (inclusief specifieke integraties die alleen voor de NL overheid zijn) moet kunnen realiseren. Deze timing lijkt ons weinig realistisch.

Bovendien lijkt het ons niet wenselijk om land-specifieke implementaties op te leggen gezien dit de Europese schaalbaarheid bemoeilijkt. In een versnipperd Europees landschap zou het voor wereldspelers uit bijvoorbeeld de VS steeds meer tijd geven om voet aan grond te krijgen in de Europese authenticatiemarkt buiten het eIDAS-kader om.

Tevens wordt er gevraagd om een verzekering van 10 miljoen af te sluiten, wat significant hoger is dan de huidige 2,5 miljoen. Dit vraagt enorme investeringen die zelfs voor grote partijen moeilijk te verantwoorden zullen zijn.

3. Gebruik van biometrie

Het is verrassend dat biometrie verboden wordt in het kader van transactioneel gebruik. Enerzijds kan dit in specifieke gevallen de veiligheid van de oplossing verhogen, bijvoorbeeld bij events waarbij er een risico op fraude zou zijn (bv gebruiker installeert zijn digitale identiteit op een nieuw toestel en wil meteen een grote banktransactie uitvoeren naar een crypto wallet).

Anderzijds zien wij in het kader van NIS2 verplichtingen voor het gebruik van Multi Factor Authenticatie waarbij biometrie een verplichtte factor is wanneer er toegang wordt verleend tot high security zones. Hiermee wordt het dus potentieel onmogelijk om aan beide wetgevende kaders te voldoen.

4. Machtigen

De beschrijving van het machtigen is in dit wetsvoorstel op een klasssieke manier beschreven en zou enkel toepasbaar zijn in het kader van legale entiteiten. Deze zeer specifieke implementatie is niet meer in lijn met de recente ontwikkelingen binnen eIDAS V2 waarbij consent/mandaten/machtigingen binnen verschillende sectoren plaatsvinden en als (Verifiable) Credentials zouden geimplementeerd worden verbonden aan een natuurlijke persoon.
Hierbij gaat het bijvoorbeeld over de ouder-kind relatie, dokter-patient relatie, financiële machtigingen,… Elk van deze voorbeelden doet zich voor binnen een specifiek eigen ecosysteem, waar heel vaak specifieke regelgeving in voege is.

Het voorstel binnen eIDAS V2 is om het beheer hiervan in de desbetreffende ecosystemen te laten (inclusief het intrekken van credentials/consent/machtigingen) wat zorgt voor een generiek beheer van verschillende types machtigingen in zowel de publieke als private sector en voor een systeem dat internationaal schaalbaar en compatibel is.

5. Verdienmodel

Het voorstel doet uitschijnen dat een erkend middel geen verdienmodel mag naar voor schuiven en/of dat er geen vergoedingsmodel vanuit de overheid zal voorzien worden. Gezien eIDAS identificatie middelen op de NIS2 lijst als klasse 1 kritieke infrastructuur worden geklassificeerd dienen deze spelers echter substantiële investeringen te maken in schaalbaarheid, security, operationele taken, klanten support, … Zonder verdienmodel is dit niet mogelijk en dreigen private spelers zich te onthouden van deelname aan dit nieuwe kader.

Daarnaast moet men erkennen dat ongeveer 50% van de identificatie- en authenticatie-markt via broker platformen verloopt (voorbeelden hiervan zijn Signicat, OKTA, …). Hetzelfde geldt voor Signing diensten. Deze brokers leveren niet enkel diensten aan overheden maar aan tal van private sectoren. Indien een verdienmodel uitgesloten wordt riskeert men dat de private sector zal afkoppelen van eIDASV2/de publieke sector en zich uitsluitend zal focussen op de private sector.

Indien echter bedoeld wordt dat de data buiten de daarvoor bestemde identificatie- en authenticatie-diensten niet mag vermarkt worden voor bijvoorbeeld marketing doeleinden dan staan wij daar zeker achter.

6. Inconsistenties met bestaande normen, kaders en standaarden

Het gebruik van middelen met betrekking tot het intrekken en schorsen wordt gelinkt aan een veiligheids niveau enhanced-basic. Dit zou tot gevolg kunnen hebben dat het voor de gebruiker moeilijk wordt gemaakt om zijn account te schorsen terwijl criminelen misbruik kunnen blijven maken van de account. Vanuit veiligheidsperspectief is het erger dat een legitieme gebruiker zijn gecompromiteerd identificatiemiddel niet kan schorsen dan dat iemand anders het middel ongeoorloofd schorst. Hier moet volgens ons de juiste balans gevonden worden.

Een van de vereisten (artikel 4.1, lid 5) verplicht de gebruiker te informeren dat het middel geschorst is. Dit is volgens de geldende OWASP normen een praktijk die ten stelligste wordt afgeraken omdat dit actieve enumeratie toelaat. Vermits de OWASP standaarden deel uitmaken van de security vereisten onder eIDAS zorgt dit voor een tegenstelling want binnen dat kader zou dat zelfs tot non-compliancy kunnen leiden.

Artikel 4.1, lid 6 laat toe om een geschorst middel te heractiveren door een identificatie die bestand is tegen een aanval op niveau Enhanced-Basic. Het opheffen van een schorsing mag echter nooit gebeuren met een identificatie die een lager veiligheidsniveau heeft dan de initiële identificatie waarmee het middel geactiveerd is. Dit zou een aanvaller in staat stellen het middel ongeoorloofd te schorsen en daarna via bijvoorbeeld phishing technieken ter kwader trouw terug te heractiveren en over te nemen indien het middel hier niet tegen bestand is (refererend naar het stuk over biometrie zou dat bijvoorbeeld een veilige oplossing zijn om te bevestigen dat het hier nog steeds over dezelfde burger gaat). Dit artikel is niet in lijn met de geldende ETSI normen die integraal deel uitmaken van het eIDAS framework.

Artikel 4.16 sluit automatische processen voor het registreren en uitgeven van identificatiemiddelen uit. Nochtans bestaan er gecertifieerde oplossingen die op vele vlakken beter scoren dan manuele processen op vlak van identificatie (wij refereren hier ook graag naar het Europese dossier van de Chaos Computer Club over de zwaktes van video identificatie, o.a. door de zwakte van de menselijke schakel waar biometrische algoritmes look-a-likes wel kunnen identificeren).

Het kader vermeldt het gebruik van stelselcodes die door de Nederlandse overheid worden uitgegeven. Het implementatiemodel is hier echter niet duidelijk. Huidige standaarden streven ernaar om vanuit de identificatiemiddelen pair-wise identifiers uit te geven en te beheren zodat afnemers geen data van de burgers met elkaar kunnen consolideren en profileren. Indien wordt opgelegd om een unieke “stelselcode” te gebruiken in het hele eco-systeem is er een groot risico op de-anonimisatie. Standaarden zoals W3C DiD/VC hebben dit reeds een tijd onderkend en de standaard hierop aangepast.

7. Conclusies

Samenvattend kunnen we stellen dat er in het Nederlandse voorstel een aantal verrassende en soms contradictorische elementen zitten die de schaalbaarheid binnen Europa en de publiek/private samenwerking zullen bemoeilijken.

Het is cruciaal voor het succes van het kader dat de burgers middelen aangereikt krijgen waarmee ze op een veilige en eenvoudige manier digitale interacties kunnen aangaan in zowel de publieke als private sectoren. Een aantal van de elementen die we hier aangehaald hebben zullen volgens onze mening potentieel leiden tot een splitsing tussen de overheid en de private sector op vlak van identificatie middelen. Dit zou de Nederlandse overheid kunnen isoleren, niet alleen nationaal, maar tevens Europees inzake cross-border interoperability.

Wij raden aan deze elementen grondig te evalueren en waar nodig aan te passen zodoende een kader te hebben dat zowel de Nederlandse overheid, de leveranciers van de middelen als de burgers ten goede komt en dat in lijn is met de Europese kaders en normen zodoende internationale interoperabiliteit en schaalbaarheid te kunnen garanderen.