Empowering people through digital trust

Reactie Digie B.V. op Internetconsultatie
‘Besluit identificatiemiddelen voor burgers i.v.m. Wdo’

Keten-ID: 10752

Inleiding

Voorafgaand aan onze inhoudelijke reactie willen wij onze waardering uitspreken richting minister Knops voor het toelaten van private middelen in het beoogde stelsel en het omarmen, hoewel verplicht, van de Europese verordeningen zoals eIDAS en de AVG. De Wet digitale overheid (Wdo) is, mede gebaseerd op de 'lessons learned' zoals voortgekomen uit Idensys, een grote stap voorwaarts voor Nederland. Dit in navolging van andere landen die een dergelijk stelsel succesvol hebben gelanceerd in de publieke sector. Overigens is de succesfactor van landen als België en Estland terug te brengen naar het feit dat de publieke en private sector het daar gekozen digitale middel in beide sectoren inzet. Dit middel is, vertalende naar de Nederlandse context, gebaseerd op het Burgerservicenummer (BSN). De zogenaamde 'core identity'. De 'single source of truth' op het gebied van identiteitsgegevens.

Het gebruik van een dergelijk middel zorgt voor de reductie van administratieve lasten, de gewenste interoperabiliteit, een versnelling van de digitalisering van (overheids)dienstverlening, voorkomt identiteitsfraude en reduceert cyber security risico's aanzienlijk. Burgers krijgen op deze wijze een gebruiksvriendelijk, veilig en privacy vriendelijk middel tot hun beschikking en kunnen dit zowel in de publieke als private sector inzetten.

Anders dan in andere landen stelt de Nederlandse overheid extra eisen aan de aanbieder van en het een private middel. Eisen die worden vastgelegd in lagere wetgeving. In die context zijn wij vooral benieuwd op welk detailniveau de Rijksoverheid, en in het bijzonder het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, deze verdere verdieping invulling wil geven zonder dat het innovatie of de naleving van Europese kaders in de weg staat.

In die context onderschrijven wij dat het van belang is om waarborgen in te bouwen in plaats van technische eisen te stellen, want deze kunnen door de snelheid van innovatie en andere ontwikkelingen belemmerend werken. In die zin gaat de Wet digitale overheid niet enkel over de situatie in Nederland, maar raakt het de Europese realiteit en is het van belang om dit Europese perspectief mee te wegen in de keuzes die de Nederlandse overheid maakt. Daarbij is het leren van de successen en foutieve inschattingen door andere Europese landen in het voordeel van Nederland.

Naast deze inzichten constateren wij dat minister Knops bewust kiest voor het creëren van vertrouwen in onze digitale samenleving en ook op deze wijze communiceert. Dit doet hij samen met zijn politieke collegae, ambtenaren, private organisaties en de betrokken burgers. Hiermee neemt hij duidelijk afstand van de zogenaamde 'privacy' schrikbeelden die door sommige organisaties naar voren worden gebracht zonder dat deze gestaafd worden door wetgevende kaders in Nederland of Europa of concrete voorbeelden in de praktijk. Andere landen laten zien dat het beschikbaar stellen en het gebruik van een betrouwbare digitale identiteit juist het vertrouwen, in de overheid en het 'systeem', doet toenemen. Wij ondersteunen de inclusieve attitude van de minister, net als het centraal stellen van technologieneutraliteit, van harte.

Kijkende naar het '**Concept Besluit identificatiemiddelen voor burgers Wdo'** en de **'Concept Nota van Toelichting Concept Besluit identificatiemiddelen voor burgers Wdo'** constateren wij dat de Rijksoverheid in deze de intentie heeft om te komen tot een constructieve samenwerking met private partijen en hiervoor, op hoofdlijnen, veelvuldig de juiste conclusies trekt en eisen opstelt. Cruciaal is echter de verdere verdieping in lagere wetgeving en de randvoorwaarden die daarin worden opgenomen. Om de transparantie van het gehele proces te bevorderen is het wenselijk dat een dergelijke ministeriële regeling ook ter consultatie zal worden aangeboden.

Zoals aangegeven is de minister voorstander van een publiek-private samenwerking op het gebied van de Nederlandse digitale identiteit. Dit is in de praktijk zeer goed mogelijk zolang het wetgevend kader innovatie, digitalisering en veiligheid ondersteunt en in overeenstemming is met de Europese en internationaal vastgestelde kaders.

Verder dient opgemerkt te worden dat de Wdo vooral ingaat om de identificatie van burgers en niet zo zeer op andere diensten die digitaal beschikbaar zijn zoals het digital ondertekenen van bijvoorbeeld contracten en het digitaal bevestigen van handelingen. Diensten die de volledige digitalisering van diverse (overheids)processen mogelijk maken. Als deze diensten en mogelijkheden wel in scope worden genomen is het van belang om de geldende wetgeving op die exacte terreinen te relateren aan de Wdo of de onderliggende ministeriële regeling.

Reactie 'Concept Besluit identificatiemiddelen voor burgers Wdo'

Vanzelfsprekend zal de aanvrager moeten voldoen aan de eisen zoals gesteld in dit concept. Ervaring leert dat er naast het stellen van eisen aan het private middel het net zo belangrijk is om eisen te stellen aan de aanvrager. Het is in deze van belang om te kunnen garanderen dat de aanvrager, naast de genoemde voorwaarden, voldoet aan de volgende eisen:

1. Het private middel aangeboden door de aanvrager is gebaseerd op bewezen technologie en voldoet aan internationale open standaarden zoals bijvoorbeeld OpenID Connect. Daarnaast voldoet de aanvrager aan de Europese kaders (controle kan plaatsvinden op basis van audits door eIDAS en AVG gecertificeerde auditoren);
2. De aanvrager is in staat om continuïteit te garanderen in zowel de dienstverlening als het hebben van voldoende financiële middelen om het bestaansrecht te verzekeren;
3. De aanvrager is in staat om grote volumes transacties te verwerken en garandeert een minimale uptime van 99%;
4. De aanvrager respecteert dat de gebruiker, in deze context de burger, in 'full control' is en moet in staat worden gesteld om eenvoudig handelingen te verrichten met het private middel. Denk hierbij aan het updaten van de identiteitsgegevens, het blokkeren van een account en het verwijderen van een account (in AVG termen 'right to be forgotten'). Daarnaast moet ieder middel voldoen aan de vereisten zoals opgenomen in de AVG en is het middel, en de daar bijbehorende handelingen, gebaseerd op het 'consent' van de burger;
5. De aanvrager dient, te allen tijde, te voldoen aan de wetgeving en auditeerbaar te zijn net als het private middel dat de aanvrager ter beschikking stelt. Dit kan per industrie verschillen. Zo zijn financiële instellingen wettelijk verplicht om haar transacties met klanten 10 jaar ter beschikking te houden voor een audit of, wanneer noodzakelijk, gerechtelijk onderzoek. Daarnaast hebben zij ook de verplichting om de transacties na 10 jaar te vernietigen;
6. De aanvrager zal de eindgebruiker, in deze context de burger, ieder moment de mogelijkheid geven om zijn of haar data te vernietigen. Echter dit ontneemt het private middel niet de wettelijke verplichting, zoals aangegeven in punt 5, om de audit trails te vernietigen aangezien deze opvraagbaar moeten blijven voor wettelijk bevoegde instanties.

GDI en het private middel

Het private middel dient compatibel te zijn met de generieke digitale infrastructuur (GDI). Hetgeen logisch is, maar wij vragen ons af in hoeverre alle onderdelen van diezelfde infrastructuur voldoen aan de huidige, technologische vereisten/mogelijkheden. Als het gaat om het aansluiten van moderne private middelen is het relevant om te weten of er sprake is van bepaalde 'legacy' of dat er al open standaarden zoals OpenID Connect worden toegepast binnen de genoemde infrastructuur. Dit is wat ons betreft een punt van aandacht omdat wij geloven in interoperabiliteit, werkbaarheid, schaalbaarheid en een snelle integratie en implementatie van private oplossingen. Hierdoor kan de overheid afstappen van ingewikkelde koppelvlakken en de doorlooptijd van integraties en implementaties drastische verkorten. Om een dergelijke integratie en implementatie te bevorderen is het noodzakelijk om tijdig een architectuurplaat te ontvangen van de overheid, inclusief de bijbehorende technische specificaties.

Aanvullende eisen, een zegen of beperking?

De nadere eisen die gesteld worden bij ministeriële regeling lijken te wijzen op gedetailleerde organisatorische, technische en functionele eisen en/of voorwaarden. Deze komen terug in artikel 2.4. Zoals eerder geschetst zijn wij ervan overtuigd dat het van belang is om waarborgen in te bouwen, maar niet de innovatie in de markt te belemmeren door op detailniveau te beschrijven wat noodzakelijk is. Eerder is binnen de Nederlandse overheid gebleken dat dergelijke detaillistische beschrijvingen niet aangepast kunnen worden in een bepaalde contractperiode met een leverancier en daardoor gewacht moet worden om een innovatie in de praktijk te brengen.

Europese verordeningen en certificering. Wie toetst met welke bevoegdheid?

Gelet op de Europese realiteit zien wij dat er de komende jaren veel zal gebeuren op het gebied een digitale identiteit. Dit overziende kun je constateren dat de snelheid van ontwikkelingen toeneemt en overheden in staat gesteld moeten worden om mee te bewegen. Zeker als diezelfde overheid de gebruiksvriendelijkheid, veiligheid en privacybescherming wil blijven garanderen richting haar burgers. Daarom is het naast het voldoen aan eIDAS en de AVG evident dat een aanvrager over de juiste ISO-certificering beschikt en dit feitelijk is vastgesteld door een geaccrediteerde instelling. Als het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties extra certificeringseisen wil stellen, via de eerdere genoemde ministeriële regeling, dan zal het ook een geaccrediteerde instelling (op basis van nationale of Europese wetgeving) moeten benoemen die toezicht kan houden op deze nadere eisen. Daarnaast zal deze instantie de certificering en bijbehorende jaarlijkse audit moeten verzorgen. De kaders en vereisten voor een dergelijke certificerende instantie ontbreken echter in dit geheel. Hier zal specifieke aandacht voor moeten zijn in het verdere vervolg.

Onderweg naar een schaalbaar en betaalbaar stelsel?

Als het gaat om het beprijzen (van het gebruik) van het private middel is het leggen van de relatie tussen het huidige DigiD businessmodel en die van het nieuwe stelsel relevant. Om kosten per transactie, bij identificatie en authenticatie, te voorkomen adviseren wij toe te groeien naar een prijsmodel per gebruiker per jaar. Daarnaast is het de vraag of, om te voldoen aan de vereisten bij eIDAS Hoog, het noodzakelijk is om bij iedere transactie realtime verbinding te leggen met de BRP en of deze 'check' iedere keer bekostigd moet worden. Naast dit mogelijke onevenredige prijsmodel creëert de Nederlandse overheid dan wederom een 'single point of failure', terwijl juist de Wdo is geïnitieerd om dergelijke risico's te voorkomen. Het lijkt ons zinvoller om een asynchroon model te ontwikkelen waarbij de Nederlandse overheid elke X-uur een update met wijzigingen naar de erkende aanvrager stuurt voor enkel de burgers die verbonden zijn aan deze wijzigingen.

Voor het delen van identiteitsgegevens en het digitaal ondertekenen via het private middel zijn kosten per transactie bijna onvermijdelijk. Net als het gebruik van de persoonlijke gegevens zou het prijsmodel gebaseerd moeten zijn op doelbinding en in redelijke mate moeten passen bij de bewuste context. Een transactiemodel is vaak de belemmerede factor voor de acceptatie en adoptie van een oplossing. Terwijl een intelligent 'user based' model juist stimulerend werkt

Bouwen aan vertrouwen

Als het gaat om het opslaan, gebruiken en herstellen van gegevens zijn er enkele vanzelfsprekendheden. Zo moet vertrouwelijk omgegaan worden met de gegevens, heeft de gebruiker inzicht in zijn/haar gegevens en de gedane transacties en bestaat de mogelijkheid om gegevens te herstellen of in te trekken. Dit gaat verder dan enkel het hebben van een digitale identiteit. Hier gaat het om een vorm van dataportabiliteit die altijd in het voordeel van de gebruiker, zijnde de burger, moet werken en zijn of haar grondrechten beschermd. Daarnaast ervaart de burger een behoorlijke mate van bescherming doordat de overheid, in samenwerking met een erkende aanvrager, misbruik of fraude voorkomt. In dit kader vragen wij ons af of de niveaus behorende bij eIDAS (laag, substantieel en hoog) allen toegepast moeten worden in de Nederlandse context.

In Europese context mag niveau Laag niet gebruikt worden, maar wel op nationaal niveau en dan volledig op eigen risico. Er zijn voldoende middelen op de markt beschikbaar die zonder enige moeite voldoen aan eIDAS Hoog zonder dat dit gevolgen heeft voor de gebruiksvriendelijkheid. Waarom zou een overheid dan het risico nemen om alsnog eIDAS laag en substantieel te accepteren in haar eigen digitale omgeving? Hierdoor bestaat er nog immer de kans op misbruik, fraude en cyber security risico's. Ervaring leert en studies tonen aan dat burgers, wanneer eIDAS Hoog middelen gebruiksvriendelijk zijn, liever voor deze variant kiezen dan de andere niveaus. Dit komt mede door de geboden transparantie en het gebruiksgemak doordat burgers meerdere 'klantreizen' kunnen afdekken met een, vertrouwde en veilige oplossing.

Technologieneutraliteit, Europese verordeningen en certificering als de sleutels tot succes

Alles overziende laat het ‘Concept Besluit identificatiemiddelen voor burgers Wdo’ voldoende ruimte voor innovatie, een effectieve publiek-private samenwerking en worden de relevante Europese kaders en ISO-certificering gerespecteerd. Verder constateren wij dat minister Knops uitgaat van vertrouwen in een privaat middel mits de aanvrager en het private middel voldoen aan specifieke eisen zonder dat technische specificaties worden opgelegd. Deze houding en handreiking tonen dat de Nederlandse overheid kaders stelt en tegelijkertijd uitgaat van de volwassenheid en professionaliteit van de aanvrager en het in te zetten private middel. Immers zijn er voldoende waarborgen ingebouwd door de verplichtende kaders als eIDAS, de AVG en de genoemde ISO-certificering af te dwingen. Dergelijke kaders tonen aan dat het introduceren en gebruik van een privaat middel, dat voldoet aan de gestelde eisen, uitstekend gereguleerd is op zowel nationaal als Europees vlak. Verder is het van belang om te onderkennen dat internationale organisaties, zowel publiek als privaat, problemen kunnen ervaren als de extra Nederlandse eisen niet aansluiten op de Europese of internationale kaders. Terwijl zij, in de meeste gevallen, juist zorgen voor een bredere uitrol van een erkend middel.

Reactie ‘Concept Nota van Toelichting Concept Besluit identificatiemiddelen voor burgers Wdo’

Zoals de titel doet vermoeden richt het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties zich op burgers gedurende het creëren van een betrouwbaar stelsel van identificatiemiddelen. Echter kan een burger ook een vertegenwoordiger zijn van een organisatie/onderneming/bedrijf. Op dit moment is minister Knops zowel verantwoordelijk voor deze ontwikkeling als voor de ontwikkeling van eHerkenning. Wij adviseren dan ook om beide trajecten te bekijken en te zorgen voor een sluitende aanpak voor burgers en bedrijven om de complexiteit en administratieve lasten voor deze doelgroepen tot een minimum te beperken. Er zijn diverse verwijzingen naar de ministeriële regeling zonder hier een concrete tijdlijn voor te benoemen en aan te geven hoe een dergelijke regeling tot stand komt. Wij gaan ervan uit dat onder andere de resultaten van de pilot ‘Sesam-ID’ en ook andere onderzoeken de input vormen voor de genoemde regeling. Hier willen wij benadrukken dat het feitelijk vaststellen van de resultaten en het toetsen van de uitkomsten van deze pilots/onderzoeken en onderzoeken gedaan moeten worden door geaccrediteerde instellingen/organisaties. Zeker op het gebied van eIDAS en de AVG.

Van knooppunt naar beslispunt

Europa telt enkele spelers die genotificeerd zijn volgens, in overeenstemming met de eIDAS-verordening. Deze private partijen hoeven het nationale toelatingstraject niet te doorlopen om geaccepteerd te worden in een andere lidstaat, in dit geval Nederland. Echter wordt het eIDAS-knooppunt als voorziening genoemd als brug tussen het private middel en het Nederlandse stelsel. De vraag is echter of dit enkel via het eIDAS-knooppunt moet als de genotificeerde partij voldoet aan alle Europese eisen zoals genoemd in de eIDAS en AVG-verordeningen. Wellicht is deze erkenning voldoende om private middelen die voldoen aan de vereisten direct toegang te bieden tot de Basisregistratie Personen en het BSN-nummer. Het doel van de Europese notificatie is altijd geweest om publieke en private middelen over de grenzen in te zetten zonder dat een middel in iedere lidstaat door een nationaal kwalificatieproces moet.

Een gezamenlijke verantwoordelijkheid

Dat private partijen zorgvuldig om moeten gaan met de gegevens van gebruikers, zijnde burgers, is evident. Echter zou het voorgestelde stelsel en middel ook moeten zorgen voor de reductie van schaduw registraties binnen de overheid en het voorkomen van datalekken door onzorgvuldige en, vaak onnodige en dubbele, opslag van identiteitsgegevens.
Het zogenaamde 'once only' principe en dataminimalisatie horen niet enkel ten grondslag te liggen aan het private middel, maar vooral ook aan het gehele stelsel en de publieke organisaties die er gebruik van maken. Hergebruik van gegevens, regie op gegevens door de burger zelf, het recht om (gegevens of gegevensgebruik) door de burger in te zien en om gegevens of acties/interacties te herstellen, bijvoorbeeld in het geval van misbruik of fraude, zijn fundamentele voorwaarden.

De aanvulling en invulling te bescherming van de Nederlandse eindgebruikers doet vermoeden dat de Europese verordeningen en de succesvolle voorbeelden in Estland en België dergelijke aspecten niet hebben afgedekt. De genoemde overwegingen zijn allen, bewijsbaar, in te regelen. Zo kan de inzet van een goed privaat middel al de genoemde aanvullingen en zorgen wegnemen. Dat data van burgers niet doorverkocht mag worden is volgens ons een van de eisen die je extra kunt stellen aan een aanvrager. Dergelijke organisaties hebben veelal een reputatie op dit gebied en of zij dit wel of niet doorverkopen is zeer goed te controleren. Wij gaan er dan ook vanuit dat dergelijke bedrijven niet door de 'keuring' heenkomen. In onze ogen zijn dit echter geen aanvullingen, maar maakt dit onderdeel uit van de integriteit van een aanvrager en op die grond kan men wel of niet toegelaten worden tot het stelsel. Een goedwerkend en transparant privaat middel zal, in principe, al vanuit digitale hygiëne voldoen aan deze aanvullingen. Daarnaast is de scheiding van de gegevens van de gebruiker en de gegevens over het gebruik van het private middel vanzelfsprekend. Net als dat de gebruiker, zijn de burger, de 'controle' heeft en zelf kan bepalen welke persoonsgegevens met wie gedeeld worden (doelbinding).

Een privaat middel en digitale ankerpunten als extra bouwstenen

Gelet op de huidige generieke digitale infrastructuur (GDI) kun je stellen dat het te accepteren private middel gemakkelijk inpasbaar moet zijn. Het biedt echter ook kansen om de huidige GDI te 'upgraden' aangezien een goed privaat middel meer te bieden heeft dan enkel identificatie en authenticatie. Een betrouwbare digitale identiteit is de versneller van de digitale (overheids)dienstverlening, dus ook van alle bijbehorende producten, voorzieningen en standaarden. Zeker ook als burger in staat zijn om zelf de onboarding te organiseren door middel van het inbouwen van zogenaamde digital ankerpunten naast de reguliere onboarding. Denk hierbij aan bijvoorbeeld het uitlezen van de NFC-chip van identiteitsdocumenten of het maken van een actuele foto die te vergelijken is met de foto op bijvoorbeeld de chip van het paspoort. Wij durven dan ook te stellen dat een goed privaat middel, ten opzichte van de huidige situatie in Nederland, zorgt voor meer gebruiksgemak, betere beveiliging en toename in de bescherming van de privacy.

Van erkenning naar gebruik in de praktijk

Toetsing in de praktijk zal bewijzen of een privaat middel wel of niet inpasbaar is in de huidige context. Feitelijk kunnen in het proces van toelating van een privaat middel drie fasen worden onderscheiden. De eerste is de aanvraag van en erkenning van het middel en de besluitvorming daarover, de tweede fase gaat over de toetsing in de praktijk en de derde fase is het toezicht op basis van conformiteit van het middel. Eerder is gesteld dat de minister niet langer dan 12 weken zal nemen om de erkenning toe- of af te wijzen. Aangezien de Wet digitale overheid op 1 juli 2020 ingaat is de vraag of aanvragers direct een verzoek in kunnen dienen of dat de ministeriële regeling volledig afgerond moet zijn. Als dit het geval is dan kan Nederland pas profiteren van de voordelen van een nieuwe digitale identiteit in, op zijn vroegst, het 2e kwartaal van 2021. Hetgeen betekent dat er bijna een jaar zit tussen de inwerkingtreding van de Wdo en de daadwerkelijke erkenning en het gebruik van een privaat middel in de praktijk. Dit is qua doorlooptijd erg lang gezien de trajecten die andere Europese lidstaten hebben doorlopen. Wij adviseren dan ook om dit proces te versnellen.

Van certificering naar algemene waardering

Als het gaat om toezicht en het voldoen aan internationale normen zijn wij zeer verheugd om te zien dat minister Knops voornemens is om het Agentschap Telecom in te schakelen voor het toezicht en dat de ISO-27001 norm leidend is en als eis gesteld zal worden aan aanvragers. Dit is volledig in lijn met internationale en Europese voorbeelden en richtlijnen. In die zin is het veilig en integer omgaan met informatie van burgers geregeld indien een aanvrager als Trust Service Provider is aangewezen op basis van ISO-27001.

In navolging van een dergelijke certificering ondersteunen wij zowel de acceptatie- en meldingsplicht. Het gebruik van een digitale identiteit in de publieke sector is gebaseerd op het vertrouwen dat burgers in het middel hebben. Zowel de Nederlandse overheid als de aanvragers zijn niet gebaat bij incidenten die het vertrouwen van de burgers ondermijnen. Daarnaast zal het vertrouwen in een dergelijk middel verder toenemen als burgers het ook in de private sector kunnen gebruiken. Door een middel dagelijks te gebruiken weet men wat de voordelen zijn, wat men kan verwachten en hoe te handelen in geval van misbruik en fraude.

Eén stelsel, één voorwaardenkader

Waar de nadruk in deze documenten ligt op het zorgen voor de bescherming van persoonsgegevens door de aanvragers van een privaat middel is er (te) weinig aandacht voor dezelfde eis voor de overheid. In hoeverre zal en kan de overheid de gegevens verkregen of gebruikt via het digitale middel inzetten om haar taken uit te voeren, zowel vanuit de dienstverlening als de handhaving geredeneerd? Een privaat middel kan uitstekend werken, volledig betrouwbaar en veilig zijn, maar enige vorm van oneigenlijke toegang of het gebruik van gegevens door de overheid doet al het gecreëerde vertrouwen teniet. De Nationale Ombudsman heeft dit punt de laatste jaren meerdere malen op de agenda gezet. Een privaat middel dient dus niet enkel als achtervang van een publiek middel, de burger moeten ook het vertrouwen hebben dat beide middelen op een soortgelijke manier ingezet en gebruikt zullen worden. Dus de eisen die men aan het private middel stelt dienen ook te gelden voor het publieke middel. Uiteindelijk werkt de minister toe naar een integraal stelsel waarin publieke en private partijen elkaar ondersteunen en zorgen voor vertrouwen door gebruiksvriendelijke, veilige en privacybeschermende middelen te bieden die gebaseerd zijn op bepaalde maatschappelijke waarborgen. Onzes inziens werkt dit alleen als zowel de publieke als private sector gebruik kunnen maken van de Nederlandse ‘core identity’, zijnde het BSN-nummer, op een acceptabele, gereguleerde en veilige manier.

Het concept besluit dat voorligt lijkt te voldoen aan de eisen van een modern kader voor een digitale samenleving in de 21e eeuw. Echter kijken wij uit naar de ministeriële regeling aangezien deze, wanneer te stringent, de toon en intentie van de Wdo teniet kan doen en daarmee de kans om aan te sluiten bij de Europese koplopers voorbijgaat.

Als laatste adviseren wij de minister kennis te nemen van internationale kaders die mede tot stand zijn gekomen door de inzet van onze Digie experts. We verwijzen graag naar de volgende documenten:

1. **The Financial Action Task Force (FATF)** - Guidance on Digital ID.
   Zie: https://www.fatf-gafi.org/publications/fatfrecommendations/documents/digital-identity-guidance.html
2. **World Economic Forum** - Reimagining Digital Identity: A Strategic Imperative.
   Zie: https://www.weforum.org/whitepapers/reimagining-digital-identity-a-strategic-imperative

Wij danken minister Knops en de betrokken ambtenaren voor de geleverde inspanningen en kijken uit naar het vervolg.

Arthur Dallau
+31647100048
arthur@digie.expert

digie