iDIN B.V.
Gustav Mahlerplein 33-35
1082 MS Amsterdam
Postbus 83073
1080 AB Amsterdam

Telefoon 020 888 85 90
www.idin.nl

De Staatssecretaris voor Digitalisering en
Koninkrijksrelaties
Mevrouw drs. A. C. Van Huffelen
Ministerie van BZK
Postbus 20011
2500 EA DEN HAAG

Datum
05-12-2022

Contact
iDIN@currence.nl

Betreft
Reactie Regeling nadere eisen toelating identificatiemiddelen WDO

Geachte mevrouw Van Huffelen,

Graag maakt Currence gebruik van de mogelijkheid om te reageren op de Regeling nadere eisen toelating identificatiemiddelen WDO. Wij doen dit mede namens onze aandeelhouders: ABN AMRO, ING, Rabobank en de Volksbank (SNS, ASN Bank en RegioBank). Genoemde banken hebben te samen en onder regie van Currence de identificatiedienst iDIN ontwikkeld en deze in 2016 op de markt geïntroduceerd met een succesvolle pilot van de Belastingdienst met meerdere online identificatie- en inlogmiddelen. Met deze online identificatiedienst kunnen natuurlijke personen zich eenvoudig bij organisaties kenbaar maken door de toegangsmiddelen van hun eigen bank te gebruiken op het eIDAS betrouwbaarheidsniveau Substantieel.

Currence en de banken onderschrijven van harte het doel van de WDO: het aanbieden van laagdrempelige en gebruiksvriendelijke inlogmiddelen om personen op een veilige en betrouwbare manier toegang te verlenen tot online dienstverlening van de overheid. Na het stopzetten van de pilot bij de Belastingdienst heeft Currence aan ditzelfde doel in het private domein gewerkt. Wij kijken uit naar de inwerkingtreding van de WDO waarmee het private en (semi-) publieke domein voor inlogmiddelen kan worden samengetrokken. Helaas zien wij in de voorliggende regeling voor ons te weinig aanknopingspunten om deze samensmelting van domeinen te realiseren.

Wij zien het belang in van de eisen die gesteld worden om de veiligheid en privacy te borgen. Tegelijkertijd merken wij op dat ons inziens de huidige Regeling doorschiet in het voorschrijven van de extra eisen die gesteld worden bovenop eIDAS. De Regeling is in huidige vorm niet bevorderlijk voor een Europees gelijk speelveld en legt een disproportionele administratieve druk op aanvragende authenticatiediensten, zelfs als deze al beschikken over een eIDAS-Substantieel verklaring, uitgegeven door een erkende, onafhankelijke en deskundige partij (auditor).

Verder onderkennen wij de voordelen van het gebruik van open source; ook componenten van iDIN zijn openbaar gepubliceerd. Echter, het volledig openstellen van alle betrokken ICT-componenten schiet naar onze mening voorbij aan het doel van transparantie en ondermijnt juist de veiligheid van authenticatiediensten. Daarbij komt dat iDIN gebruik maakt van componenten die integraal onderdeel vormen van, onder toezicht staande, financiële diensten. De verplichtingen die toezichthouder DNB in het kader van veiligheid oplegt aan financiële dienstverleners, verhinderen juist het publiceren van de broncode van componenten die onder deze Regeling aangewezen zijn.

Deze factoren leiden ertoe dat wij in sterke mate betwijfelen of het juridisch mogelijk en financieel rendabel is om voor iDIN een aanvraag tot een erkenning in te dienen, mede omdat wij op basis van de Regeling nog geen business case kunnen opstellen. Currence en de banken leveren graag een maatschappelijke bijdrage middels het beschikbaar stellen van iDIN als authenticatiedienst voor overheidsdienstverlening. De Regeling in huidige vorm weerhoudt ons vooralsnog daarvan.

Bijgaand treft u een nadere toelichting op bovenstaande en gespecificeerde reactie op de Regeling. Deze zal ook per post naar uw ministerie worden opgestuurd. Wij zijn u erkentelijk voor de geboden mogelijkheid tot reactie en gaan graag met u in gesprek om te komen tot voor iDIN werkbare eisen voor erkenning.

Met vriendelijke groet,

iDIN B.V.
(Currence Holding B.V. is Product- en merkeigenaar van het iDIN Scheme)

Reactie Consultatie

Consultatie: Regeling nadere eisen toelating identificatiemiddelen WDO

Reactie Consultatie: iDIN B.V.

5 december 2022 | Version 1.0

Auteurs
iDIN B.V. | iDIN@currence.nl

Index

Belangrijkste bevindingen 5

De eIDAS-verordening als duidelijker fundament voor de eisen 5

Open Source 6

Techniek 6

Biometrie 7

Toetreden als Scheme 7

Artikelsgewijze bevindingen 8

Hoofdstuk 2 – Aanvullende erkenningseisen 8

Hoofdstuk 3 – Regels over de aanvraag voor erkenning 9

Hoofdstuk 4 – Verplichtingen voor houders van een erkenning 9

Belangrijkste bevindingen

Belangrijk is om te constateren dat de banken en Currence de doelen en basisuitgangspunten zoals onder meer verwoord in de voorgenomen wet onderschrijven. Hieronder vallen de uitgangspunten van betrouwbaarheid, privacy-vriendelijkheid en gebruikersvriendelijkheid, maar ook het level playing field, ruimte voor meerdere technologische oplossingen en het voorkomen van redundante eisen (die elders al zijn vastgelegd in wet- en regelgeving).

Tegelijkertijd constateren we dat bij de uitwerking van de Regeling op veel aspecten niet voldaan wordt aan deze doelen en uitgangspunten. Zo worden er bijvoorbeeld extra eisen gesteld boven op eIDAS en bestaande wetgeving en zijn de eisen en compliance voor financiële instellingen inzake het identificeren van klanten al in bestaande wetgeving (Wft/Wwft/AVG) geregeld. Ook worden er voor het publieksmiddel uitzonderingen gemaakt op de erkenningseisen, waarbij de noodzaak hiervoor onduidelijk is. Belangrijk is dus om de uitwerking in overeenstemming te brengen met de uitgangspunten en doelen.

De eIDAS-verordening als duidelijker fundament voor de eisen

iDIN levert reeds identiteitsvaststelling en authenticatie op het betrouwbaarheidsniveau eIDAS Substantieel. Niet alleen zijn de iDIN normen en regels conform eIDAS Substantieel opgezet, ook zijn de iDIN-normen gedetailleerder en specifieker dan de eIDAS-norm en bieden aanvullende informatie (guidance) opdat voldoende kan worden aangetoond dat ook daadwerkelijk aan eIDAS wordt voldaan. Daarnaast laat Currence iDIN ten aanzien van eIDAS Substantieel regelmatig adviseren door (onafhankelijke) externe partijen en worden waar nodig maatregelen genomen voor een verdere verbetering van de huidige certificerings- en toetsingsprocedure. Een erkende onafhankelijke auditor heeft een verklaring afgegeven dat het iDIN Scheme voldoet aan de eisen voor eIDAS Substantieel.

De Staatssecretaris heeft aangegeven de richtlijnen te volgen die worden gegeven in de eIDAS-uitvoeringsverordening 2015/1502. Hoewel een aantal eisen die zijn opgenomen in de Regeling inderdaad overeenkomen met deze richtlijnen, moeten aanvragers alle benodigde documentatie voor een eIDAS-verklaring nogmaals aanleveren. Mogelijk kan verduidelijkt worden welke stukken niet meer aangeleverd hoeven worden, als partijen al in bezit zijn van een eIDAS-verklaring welke is uitgegeven door een erkende, onafhankelijke en deskundige partij.

Een mogelijke aanpassing kan zijn om alleen de aanvullende vereisten te specificeren in de Regeling, en verder door te verwijzen naar de eisen onder de Uitvoeringsverordening 2015/1502. Dit is geen nieuwe praktijk in Nederlandse wetgeving: in de Uitvoeringsregeling Wet ter voorkoming van witwassen en financieren van terrorisme stelt voor eisen voor betrouwbare identificatiemiddelen in de financiële sector slechts het volgende: *“Een voldoende betrouwbaar identificatiemiddel is een identificatiemiddel dat voldoet aan het betrouwbaarheidsniveau ‘substantieel’ of ‘hoog’ als bedoeld in de eIDAS-verordening”.*

Wij vragen ook aandacht voor specifiek de aanvullende eisen die de Regeling introduceert bovenop de al uitgebreide Uitvoeringsverordening 2015/1502. Extra eisen bovenop eIDAS zijn niet bevorderlijk voor een Europees gelijk speelveld en leggen Nederlandse aanbieders extra eisen op terwijl buitenlandse Europese eIDAS compliant aanbieders via notificatie in een andere lidstaat zonder meer de Nederlandse markt kunnen betreden zonder aan de extra Nederlandse eisen te hoeven voldoen. De mate waarin (private) Nederlandse eID oplossingen hierdoor in Europa concurrerend kunnen zijn in het **private** domein lijkt daardoor vrijwel nihil. Ook zullen andere oplossingen vanuit het buitenland de Nederlandse markt betreden, terwijl die niet voldoen aan de nu geformuleerde Nederlandse eisen, maar aan een veel lichter regime. Deze ongelijkheid ondermijnt de principes van een Europees gelijk speelveld in de markt.

Open Source

Wij maken graag gebruik van de mogelijkheid om te reageren op de open source vereisten in relatie tot het verzekeren van een breed beschikbaar aanbod van inlogmiddelen. Wij onderkennen de voordelen van het gebruik van opensource; ook componenten van de broncode van iDIN zijn openbaar gepubliceerd. Echter, het volledig openstellen van alle betrokken ICT-componenten schiet naar onze mening voorbij aan het doel van transparantie en ondermijnt juist de veiligheid van authenticatiediensten.

Het opstellen van een lijst met componenten die op termijn allemaal volledig gepubliceerd moeten worden, gaat voorbij aan de hoog geautomatiseerde verwerkingen bij financiële instellingen. (Elektronische) identificatiediensten vormen integraal onderdeel vormen van onder toezicht staande financiële diensten die gevoelige gegevens verwerken, zoals persoonsgegevens en betalingsgegevens. De toegangsmiddelen van financiële instellingen, die de basis vormen van het iDIN Scheme, vallen daarom onder streng toezicht van de De Nederlandse Bank en worden door de instellingen zelf continu gemonitord en frequent getest op weerbaarheid tegen cyberdreigingen.

Juist dit strenge toezicht vanuit een andere overheidsinstelling maakt het voor iDIN onmogelijk om de volledige lijst van componenten openbaar te publiceren. Wij erkennen de rol die open source kan spelen op het gebied van transparantie: ook bepaalde componenten van iDIN, zoals de technische en functionele schemeregels, zijn openbaar gepubliceerd. Wij missen echter een balans in openheid en veiligheid rondom dit vraagstuk. Naar onze mening ontbreekt ook de rol van het Agentschap Telecom als toezichthouder in deze context. Wij nemen aan dat waar het openbaar publiceren van broncode veiligheidshalve niet gewenst is, het Agentschap Telecom in voldoende mate controle op het functioneren van de broncode kan uitvoeren.

Business Case

Voor Currence en de banken bestaat nog veel onduidelijkheid over de business case voor private inlogmiddelen. De Regeling specificeert niet op welke wijze private inlogmiddelen vergoed worden voor het aanbieden van de authenticatiedienst. Inzicht in kosten en onkostenvergoedingen is essentieel om de afweging te maken voor het indienen van een aanvraag tot erkenning. Zonder tegengeluid gaan wij ervan uit dat de onkostenvergoeding gelijk staat aan de kostprijs van DigiD (In 2023 begroot op €0,11 per succesvolle authenticatie), in lijn met de gedragsregels voor de overheid onder de Wet Markt en Overheid.

Techniek

Het uitgangspunt van eIDAS is dat vereisten technologieneutraal worden gedefinieerd. Hiermee worden meerdere invullingen van inlogmiddelen ondersteund die wel moeten resulteren in hetzelfde vereiste betrouwbaarheidsniveau. Wij adviseren de architectuur meer high level te beschrijven en terughoudend te zijn in het voorschrijven van specifieke technische invullingen, waarbij ook rekening gehouden moet worden met bewezen, veilige implementaties binnen bestaande oplossingen. In de voorgestelde technische opzet wordt het principe van technologieneutraliteit feitelijk al ondergraven door o.a. het voorschrijven van een systematiek van stelselcodes en authenticatiecodes. Voorschrijven van een systematiek zonder dat hierover een duidelijk beeld wordt geschetst sluit defacto alternatieve nieuwe en veilige oplossingen uit.

Onze aanbeveling, als het gaat om techniek, is om veel terughoudender te zijn in het voorschrijven van techniek, de private en publieke oplossingen niet onder te brengen in één technisch stelsel, en de mogelijkheden die vanuit oplossingen, zoals iDIN, geboden kunnen worden een plek te geven in de mogelijke toepassingen bij dienstverleners, zodat er meer differentiatie mogelijk is om aan te sluiten bij de specifieke wensen en situatie van die dienstverlener.

Biometrie

Het is onduidelijk waarom het gebruik van biometrie als authenticatie-factor expliciet wordt uitgesloten (art. 2.13). Genotificeerde eIDAS-middelen die door Nederlandse dienstverleners geaccepteerd moeten worden mogen wel gebruik maken van biometrie als authenticatiefactor. Waar multi-authenticatie veelal de keuze biedt tussen 3 factoren (kennis, bezit en persoonlijke kenmerken) wordt hier feitelijk een combinatie van kennis en bezit voorgeschreven.

Biometrie is tegenwoordig de ‘gebruikersstandaard’ op toestellen, dat verbieden geeft een minder goede gebruikerservaring. Gezien het breed gebruik is deze eis achterhaald, waarbij ook geldt dat de AVG voldoende waarborgen bevat waar alle eID aanbieders zich aan dienen te houden. Hoe verhoudt zich dit tot het verwerken van biometrische gegevens uit de AVG? In de financiële sector wordt dit reeds toegepast en is dit toegestaan door de Toezichthouders.

Toetreden als Scheme

Graag zien wij verduidelijkt dat private middelen die samenwerken binnen een formeel stelsel van eID afspraken en veiligheidseisen (Scheme) ook als Scheme kunnen worden toegelaten/erkend als eID dienstverlener in plaats van de afzonderlijke deelnemende instellingen. Als het gaat over het publiceren van broncode, gaan wij ervan uit dat als een Scheme optreedt als authenticatiedienst, de schemeregels (technische en functioneel) voldoende inzicht geven in de werking van de middelen.

Wij raden aan om de Regeling tot alleen het noodzakelijke te beperken: voorwaarden voor het gebruik van BSN voor authenticatie in het overheidsdomein. Laat stelsels vrij in het hanteren van het eigen rollenmodel en erken oplossingen op stelsel-niveau in plaats van de individuele rollen en partijen daarbinnen. Afhankelijkheden tussen rollen moeten vermeden worden.

Artikelsgewijze bevindingen

Naast de beschreven belangrijkste bevindingen geeft dit hoofdstuk artikelsgewijs feedback.

Hoofdstuk 2 – Aanvullende erkenningseisen

Artikel 2.2 en 3.1.1.d: ISO 27001 certificering
Wij adviseren het mogelijk te maken om andere vergelijkbare internationale marktconforme standaarden te mogen gebruiken.

Artikel 2.3: Verplichtingen bij het beëindigen van een erkenning
Bij dit artikel moet ons inziens onderscheid gemaakt worden tussen verschillende databases: stamgegevens en gebruiksgegevens. Van het verwijderen van persoonsgegevens kan in het iDIN-scheme geen sprake zijn. De persoonsgegevens die bij het bancaire KYC-proces zijn vastgelegd worden namelijk, met toestemming van de persoon, hergebruikt. Verplichtingen onder de Wft en Wwft maken het onmogelijk om persoonsgegevens te verwijderen.

Artikel 2.5 en 2.6: Gebruik van software met openbare broncode
Naast bovenstaande opmerkingen gaan wij ervan uit dat als een Scheme optreedt als authenticatiedienst, de schemeregels (technisch en functioneel) voldoende inzicht in de werking van de middelen verschaft

Artikel 2.7: Registratieproces
Wij gaan ervan uit dat bij andere wettelijke verplichtingen dit artikel vervalt, bijvoorbeeld Algemene Wet inzake Rijksbelastingen. *Artikel 26a, eerste lid van het Besluit prudentiële regels stelt dat "een bank … beschikt over procedures en maatregelen die waarborgen dat de voor de uitvoering van de vangnetregelingen noodzakelijke gegevens voortdurend actueel worden bijgehouden en adequaat zijn vastgelegd." Het tweede lid regelt dat "de financiële onderneming de gegevens, bedoeld in het eerste lid, verstrekt op verzoek van DNB binnen een door DNB te bepalen termijn en op een door DNB te bepalen wijze." Artikel 26a geeft hiermee uitvoering aan artikel 3:17, tweede lid, aanhef en onderdeel d van de wet op het financieel toezicht (Wft). Artikel 3:17, zesde lid van de Wft regelt het gebruik van het BSN bij de uitvoering van het DGS en biedt de juridische grondslag voor banken en DNB om het BSN van (vertegenwoordigers van) depositohouders te verzamelen, vast te leggen, te verwerken en aan te leveren. Afspraken over het gebruik en de verwerking persoonsgegevens zijn opgenomen in dit Handboek en de GLO.*

Artikel 2.10 en 4.10: Authenticatie en gebruik
Wij zien graag verduidelijking over de werking van stelsel- en authenticatiecodes. Bijvoorbeeld:

- Moet er per publieke dienstverlener een aparte stelselcode gebruikt worden? I.e. één voor de Belastingdienst, één voor het UWV?
- Of wordt er één persoonlijke code gebruikt voor alle aangesloten publieke dienstverleners?
- Wie maakt de persoonlijke stelselcodes aan?
- Het authenticatieproces staat ook nog niet volledig beschreven in de MR.
- Is de werking gelijk aan de pilot bij de Belastingdienst met meerdere online identificatie- en inlogmiddelen

Artikel 2.13: Gebruik van biometrie bij authenticatie uitgesloten
Biometrie is tegenwoordig de ‘gebruikersstandaard’ op toestellen. Dat verbieden geeft een minder goede gebruikerservaring. Gezien het breed gebruik is deze eis achterhaald, waarbij ook geldt dat de AVG voldoende waarborgen bevat waar alle eID aanbieders zich aan dienen te houden. Hoe verhoudt zich dit tot het verwerken van biometrische gegevens uit de AVG? In de financiële sector wordt dit reeds toegepast en is dit toegestaan door de Toezichthouder.

Voorbeeld: *The European Banking Authority (EBA) has published guidelines outlining the steps credit and financial institutions need to take to ensure safe and effective remote customer onboarding practices in line with applicable AML/CFT legislation, and the EU’s data protection framework. Any credit and financial institutions that fall within the scope of the Anti-Money Laundering Directive (AMLD) are subject to these guidelines. This final set of guidelines sets out the steps financial institutions must take when selecting customer onboarding tools and when assessing the adequacy and reliability of these tools. They have been developed in response to the European Commission’s request in the context of its Digital Finance Strategy, published in 2020.*

Artikel 2.22 en 4.4: Continuïteitsbeheer
In de markt wordt onderscheid gemaakt tussen “prime-time” en non “prime-time” (tussen 00:00 en 06:00), waarbij tijdens non-“prime-time” de beschikbaarheidsnorm lager ligt. Zie bijvoorbeeld ook de verplichtingen onder de Wet op het financieel toezicht, artikel 3.17. Wordt dit hier ook toegepast?

Artikel 2.26: Interoperabiliteit
Wij zien graag de standaarden gespecificeerd in de Regeling. Het duidelijk hebben van de verplichte standaarden voor erkende authenticatiediensten is van belang voor de afweging om eventueel toe te treden als privaat middel.

Artikel 2.28
Graag zien wij een specifieke toelichting hoe afwijkende eisen voor een publiek middel geen ondermijning van het level playing field oplevert.

Hoofdstuk 3 – Regels over de aanvraag voor erkenning

Artikel 3.1.1.s: Inhoud van de aanvraag
Wat wordt bedoeld met “overige gegevens”? Specificatie is hier nodig.

Artikel 3.4: Aanvraag per identificatiemiddel
Wij gaan ervan uit dat een Scheme als authenticatiedienst erkend kan worden.

Hoofdstuk 4 – Verplichtingen voor houders van een erkenning

Artikel 4.14:
Het is voor ons onduidelijk welke gegevens precies moeten worden verstrekt op welk moment. Wij zien graag “andere informatie” (artikel 4.14.1.a.ii) gespecificeerd. Ook is ons inziens een centraal register voor inzage door de gebruiker niet wenselijk: inzage kan decentraal binnen de structuur van het middel zelf geboden worden. Zo is het voor iDIN-gebruikers mogelijk om in de eigen internetbankieren-app terug te zien welke gegevens via iDIN met wie zijn gedeeld.

Artikel 4.18
Voor private uitgevers is er geen garantie dat de overheid na de erkenning het stelsel gaat notificeren. Volgens dit artikel moet de private uitgever verplicht meewerken aan een notificatie. Wij zien graag duidelijk gemaakt waarom er geen verplichting is voor de overheid om het stelsel te notificeren.