Reactie iDIN B.V. op Consultatie Besluit identificatiemiddelen voor burgers i.v.m. Wdo

Aan

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Datum
12-05-2020

Van
iDIN B.V.
iDIN@Currence.nl

Betreft
Reactie iDIN B.V. op Internetconsultatie Besluit identificatiemiddelen voor burgers

Inhoud

Reactie op Internetconsultatie Besluit identificatiemiddelen voor burgers

iDIN B.V. (hierna iDIN) is verheugd dat met het voorgenomen Besluit (hierna Besluit) een aantal regels voor de aanwijzing en erkenning van publieke en private identificatiemiddelen wordt verduidelijkt. iDIN onderschrijft de doelen en basisuitgangspunten uit het Besluit. Hieronder vallen de uitgangspunten van veiligheid, betrouwbaarheid, gebruikersvriendelijkheid (en privacy) van de eID-middelen, maar ook de multi-middelen strategie, level playing field, meerdere technologische oplossingen en het niet stellen van eisen die elders zijn vastgelegd in andere wet- en regelgeving. Onderstaand treft u onze reactie aan op de internetconsultatie. De belangrijkste in het oog springende punten zijn hieronder samengevat. In de bijlage vindt u onze meer gedetailleerde reacties met opmerkingen en vragen tot verduidelijking.

1. Transparantie nog onvoldoende: het Besluit bevat veel open einden

Het is moeilijk om een concrete reactie te geven op het voorgenomen Besluit (verder Besluit) zonder dat de Ministeriele Regelingen (MR) en technische eisen beschikbaar zijn. In het Besluit wordt gerefereerd (11 keer) aan nog op te stellen MR. Wij vragen ons af of die veelvoud van nadere regels voor de uitvoering van een Europese Verordening noodzakelijk is en/of het toelaten van (private) identificatiemiddelen niet eenvoudiger kan. Bijvoorbeeld op de wijze waarop leveranciers van overige eIDAS-vertrouwensdiensten in Nederland worden toegelaten. Er zal sprake zijn van een omvangrijk pakket van gestapelde Europese, Nederlandse wet- en regelgeving. Zonder duidelijke afstemming tussen het Besluit, de MR en bijhorende technische eisen en verplichtingen kunnen eID-middelen bovendien niet de juiste voorbereidingen treffen en kunnen zij geen goede impact- en kostenanalyse maken. Zonder bijvoorbeeld nadere duidelijkheid over punten genoemd in artikel 2.4 en artikel 2.20 van het Besluit, als ook paragraaf 4.1.3 en 6.1 van de Nota van Toelichting (NvT) en de beprijzing, inclusief contractmodaliteiten (in artikel 2.18), is een goede inschatting van de business case nagenoeg onmogelijk. iDIN vindt het niet wenselijk dat er zoveel belangrijke nadere eisen bij een MR bepaald worden. Het bemoeilijkt de operationele en technische voorbereiding voor connectie van middelen op de Generieke Digitale Infrastructuur (GDI) en verhoogt daarmee onnodig de voorbereidingskosten. Wij gaan er dan ook vanuit dat zowel de MR als de bijbehorende technische eisen rond de inrichting van de GDI spoedig in concept beschikbaar zijn en in consultatie zullen worden voorgelegd aan de belanghebbenden en dat deze niet zonder enige vorm van afstemming opgelegd worden.

2. Ontbreken van level playing field tussen de verschillende middelen

Het besluit maakt het mogelijk dat drie categorieën middelen erkend kunnen worden; een genotificeerd eIDAS-middel, een publiek middel en een privaat middel. Dit vergroot het bereik en keuzevrijheid voor de gebruiker. In paragraaf 4.1 in de NvT wordt gesteld dat eisen aan publieke middelen gelijk zijn aan de eisen die worden gesteld aan private middelen. Tegelijkertijd wordt in dezelfde paragraaf beargumenteerd dat het publieke middel op een aantal punten wezenlijk anders is dan een privaat middel (relatie met gebruikers waarmee geen overeenkomst kan worden gesloten), waardoor het mogelijk wordt via het Besluit en de MR recht te doen aan verschillen (zoals benoemd bij de eisen met betrekking tot de aanvraag voor erkenning (artikel 2.5 t/m 2.12) en artikel 2.15 (rapportage), artikel 2.16 (accepteren van gebruikers), artikel 2.17 (meldingsplicht) en 2.18 (beprijzing) die blijkbaar niet gelden voor het publieke middel. Ook is ons niet duidelijk waarom voor het publieke middel de eisen zoals geformuleerd in artikel 2.4 lid 1 en 2 niet van toepassing zijn. Wat betreft het gestelde in paragraaf 4.2 dat met gebruikers van het publieke middel geen overeenkomst kan worden afgesloten, wordt opgemerkt dat ook gebruikers van het publieke middel gehouden zijn aan een aantal zorgvuldigheidseisen om onder meer misbruik en fraude te voorkomen. Dat zou in elk geval een overeenkomst rechtvaardigen.

Wij zijn van mening dat de verschillen in toetsingseisen voor erkenning/toelating tussen deze categorieën van middelen principieel onjuist zijn. Wij pleiten dan ook voor een gelijk speelveld voor alle categorieën middelen in lijn met de regels die de ACM hierover heeft opgesteld.

3. Erkenning afsprakenstelsel en vermijden van dubbel toezicht

iDIN B.V. zal als scheme owner van iDIN (afsprakenstelsel) de aanvraag voor erkenning indienen en wenst ook als scheme geaccrediteerd te worden. Het scheme ziet toe op naleving van de (eIDAS-compliant) iDIN-regelgeving door de vergunninghoudende iDIN-banken/middelenverschaffers (licentiehouders). iDIN zal dan de onder toezicht staande partij zijn die op haar beurt dient aan te tonen dat de iDIN-banken voldoen aan alle gestelde eisen. Wat wij met deze gelaagde opzet van toezicht willen voorkomen is dat elke individuele iDIN-bank een dubbele toezichtlast ondergaat. Enerzijds vanuit het iDIN scheme en het bestaande ICT-toezicht van DNB op middelen/mechanisme en anderzijds vanuit de overheid (BZK/AT). Onnodige lastenverzwaringen - en daarmee een verhoging van kosten in de keten van digitale transacties - dienen zoveel mogelijk beperkt te worden. Wij vragen dan ook in het Besluit duidelijker aan te geven dat ook schemes die private middelen in licentie uitgeven kunnen worden erkend (enigszins vergelijkbaar met het ETD-stelsel) en het bewijs van naleving levert.

4. Hergebruik van gegevens vergt verduidelijking

Wij begrijpen dat de gegevens over het gebruik (bijvoorbeeld hoe vaak een gebruiker ingelogd heeft) niet hergebruikt mogen worden. Wij gaan ervan uit dat de identiteitsgegevens van de gebruiker (bijvoorbeeld de naam) die worden verkregen/geverifieerd vanuit de BRP wel hergebruikt mogen worden in het scheme in het kader van beheersing van datakwaliteit en one-version-of-the-truth. In dit kader is het van belang om nog voor het treffen van de voorbereidingen duidelijkheid te krijgen hoe deze ID-controle zal worden ingevuld en dus zo snel mogelijk duidelijkheid te krijgen over de invulling van de technische eisen.

5. Rol ontsluitende diensten belangrijk voor soepele samenwerking

Het Besluit maakt niet duidelijk welke eisen worden gesteld aan de routeringsvoorziening en de ontsluitende dienst in het kader van aansluiting van het middel bij de GDI (zie artikel 2.3 en artikel 2.4 tweede lid). In onze opvatting vervullen deze een cruciale rol voor een snelle implementatie en het reduceren van kosten in de keten en borgen zij een robuust en soepel werkend systeem. Wij missen hier een architectuurplaat die het fundament vormt voor de verdere invulling hiervan. Voor een soepel verlopende samenwerking tussen alle betrokken ketenpartijen is een gedegen inzicht in de eisen/voorwaarden rondom de routeringsvoorziening en de ontsluitende dienst onontbeerlijk. Tenslotte missen wij in het Besluit een duidelijke bepaling dat de ontsluitende dienst/machtigingsdienst ook door private partijen onder gelijke voorwaarden als publieke partijen kan worden ingevuld. En voorts, aan welke eisen deze partijen dienen te voldoen.

6. Technologie neutraliteit moet echt neutraal blijven

Wij juichen het gehanteerde principe in het Besluit over technologieneutraliteit zeer toe. Echter, in de NvT paragraaf 4.1.2 (met referentie naar artikel 4.2 lid l) wordt diverse malen gesproken over het verplichten van open standaarden en (privacy)technologieën. Dit lijkt ons niet in overeenstemming met elkaar. Het opstellen van richtlijnen ten aanzien van mogelijk te gebruiken standaarden of technologieën biedt meer flexibiliteit en is meer in overeenstemming met het neutraliteitsprincipe en komt daarmee meer tegemoet aan de doorlopende innovaties rondom eIDs.

7. Onnodige regeldruk en administratieve lasten zoveel mogelijk beperken

Aanvullende voorschriften boven op eIDAS- en AVG-eisen werken ongelijke concurrentieverhoudingen in de hand ten opzichte van andere Europese middelenaanbieders en belemmeren daarmee ook

innovaties, bijvoorbeeld op het gebied van biometrische identificatietechnieken en remote document authentication. Daarnaast bestaat de kans dat nadere nationale regels on-top-of Europese Verordeningen zullen leiden tot botsingen tussen de diverse wetgevingen. Deze zullen aanvragers met interpretatie-issues opzadelen als ook verwarring veroorzaken over welke regel het primaat heeft. Dit heeft juridische consequenties en een kostenverhogend effect welke impact hebben op de hele keten, dus ook voor publieke dienstverleners.

Verder worden er in de NvT in paragraaf 5.2 enkele standaarden voorgeschreven. Zo is de ISO-27001 als leidende norm voorgeschreven met betrekking tot de toetsing van informatiebeveiliging. Wij willen u erop wijzen dat er meerdere breed geaccepteerde internationale standaarden bestaan die hetzelfde doel dienen, die gelijkwaardig zijn en vaak in combinatie worden ingezet. Om middelenaanbieders niet onnodig op kosten te jagen, pleiten wij ervoor om niet één standaard voor te schrijven, maar ruimte te bieden aan alternatieve standaarden mits het gebruik van dergelijke alternatieven goed wordt gemotiveerd door de middelenaanbieder. Dit punt geldt natuurlijk ook voor de overige standaarden die in de NvT zijn voorgeschreven.

8. Duidelijkheid procedures certificering en toezicht is noodzakelijk met accent op beperking van kosten

In de NvT en het Besluit wordt op verschillende plaatsen ingegaan op certificering en toezicht. Een verwijzing naar een nog op te stellen certificeringsprocedure en toezichtkader ontbreekt. Op voorhand is het gewenst duidelijkheid te hebben over hoe de certificering in zijn werk gaat (en de afspraken die daarop van toepassing zijn) en hoe het toezicht in de praktijk wordt vormgegeven. Wel wordt in een aantal paragrafen (met name 5.2 en 8) ingegaan op een aantal eisen rond deze thema's. De insteek van zorgvuldigheid is begrijpelijk, maar beseft dient te worden dat de kosten hiervan uiteindelijk in de keten van digitale transacties neerslaan. Gegeven de randvoorwaarden waaraan minimaal voldaan moet zijn, dient kostenbeperking het uitgangspunt te zijn.

9. Duidelijkheid over beprijzing noodzakelijk

In paragraaf 6.5 van de NvT en art 2.8 van het Besluit wordt ingegaan op de beprijzing. Het gaat hier om de tarifering aan de burger (gebruiker). Informatie over de beprijzing van de afnemers (bestuursorganen) voor het gebruik van het middel (om gebruikers te kunnen identificeren) alsmede over hoe de voorgenomen contractuele relaties met de middelenaanbieders vorm zullen worden gegeven, ontbreekt. Deze informatie is cruciaal voor het bepalen van de business case voor de private middelen, die op zijn minst sluitend moet zijn. Er is sprake van een gemeenschappelijk belang. De beprijzing bepaalt de financiële situatie en uiteindelijk de financiële continuïteit (zie ook art. 2.8) van de erkende middelenaanbieders. Dit is cruciaal voor continuïteit van de dienstverlening en voortgaande (en gewenste) innovatie. Daarnaast is er een gemeenschappelijk belang voor zo laag mogelijke transactiekosten in de keten teneinde het beslag op publieke (financiële) middelen zoveel mogelijk te beperken. Met als randvoorwaarden veiligheid, betrouwbaarheid en gebruikersvriendelijkheid geldt ook hier dat het uitgangspunt moet zijn de kosten zo beperkt mogelijk te houden door slim organiseren en efficiënt werkende procedures. Dat is ook vanuit het oogpunt van innovatie van belang.

Bijlage 1
Reactie op Nota van Toelichting Besluit identificatiemiddelen voor burgers Wdo

2. Juridische context

2.3. Verhouding tot eIDAS verordening

Reactie iDIN
Een eIDAS genotificeerd middel hoeft niet het Nederlandse toelatingstraject te doorlopen. Uiteraard geldt dit voor middelen en burgers uit andere lidstaten, maar geldt ook dat dit middel automatisch als burgermiddel erkend is op grond van notificatie van een andere lidstaat indien dit middel wordt uitgegeven in Nederland aan een Nederlander? Zo ja, dan is het van belang dat de burgers een helder gepresenteerd overzicht krijgen van de nationale NL en de EU middelen, mede om dreigingen als phishing en social engineering voldoende het hoofd te kunnen bieden. Hierbij is het ook van belang de presentatie zo vorm te geven dat er geen ongelijke promotie ontstaat tussen NL- en EU-middelen als ook binnen de NL middelen. Bijvoorbeeld kan gedacht worden aan nationale middelen onder één knop en een separate eIDAS-knop. Het is ook van belang op welke wijze de lijst wordt geordend om geen onnodige indicatie van voorkeur te geven (immers, op de lijst komen alleen erkende middelen).
Houdt de minister een actuele lijst bij van accrediterende instanties die bevoegd zijn inzake de WDO? Zal er op de lijst ook onderscheid worden gemaakt tussen de fasen erkenning in opzet en in werking (na 6 maanden)?

3. Toelating van identificatiemiddelen

3.1 Beleidsmatige achtergrond
Private partijen kunnen een rol spelen bij identificatie van natuurlijke personen zonder dat gegevens van die gebruikers handelswaar worden in het verdienmodel van die partijen.

Reactie iDIN
Dit punt is gekoppeld aan het AVG-principe van doelbinding en aan de bepaling uit dit Besluit dat ook bij expliciet consent van de gebruiker dit niet is toegestaan. Het lijkt ons van groot belang dat deze interpretatie wordt getoetst door de AP (zie verder ook commentaar bij art 2.19 en par.6.1).

3.2 Doelvoorschriften gebaseerd op eIDAS en AVG

Reactie iDIN
Extra Nederlandse doelvoorschriften (principles) boven op eIDAS en AVG-overheidseisen werken ongelijke concurrentieverhoudingen in de hand ten opzichte van andere Europese middelenaanbieders en belemmeren daarmee ook innovaties bijvoorbeeld op het gebied van biometrische identificatietechnieken en remote document authentication. Daarnaast bestaat het risico dat nadere regels on-top-of zullen leiden tot botsingen tussen de diverse wetgevingen. Hierdoor worden aanvragers opgezadeld met interpretatie issues onder andere over de vraag welke wetgeving het primaat heeft. Dit heeft allemaal een kostenverhogend effect.

3.3. Aanvulling en invulling ter bescherming van Nederlandse eindgebruikers
- Aanvalspotentieel

Reactie iDIN
De eIDAS-eisen rondom het authenticatiemechanisme als ook het aanvraag- en registratieproces zijn duidelijk genoeg en toereikend. Uit de fraudepraktijken blijkt dat aanvallers zich met name richten op menselijke kwetsbaarheden door gebruik te maken van bijv. phishing en social engineering technieken om zodoende ongeoorloofd toegang te krijgen tot andermans identiteit en deze over te nemen. Als eIDAS-normen effectief zijn geïmplementeerd dan blijken de in de eIDAS genoemde dreigingen niet schaalbaar te zijn en daarmee minder of niet interessant voor aanvallen.

Met andere woorden, aanvullende regels zijn niet nodig, maar misschien wel richtlijnen (guidance) voor een mogelijke invulling van de bestaande eIDAS-regels en -normen. Dit is flexibeler en sneller aanpasbaar dan een Ministeriële Regeling. Deze richtlijnen zouden omwille van een gelijk speelveld ook van toepassing moeten zijn op het publieksmiddel. De gebruiker heeft daarnaast ook een eigen verantwoordelijkheid (te borgen bijvoorbeeld in de gebruikersovereenkomst).

- Gescheiden opslag van gebruikersgegevens en gebruiksgegevens

Reactie iDIN
Wat wordt verstaan onder verwerking en gegevens. Wordt hier alleen de back-end verwerking en opslag bedoeld? Om welke gebruiksgegevens gaat het in de regelgeving? Verduidelijking is hier gewenst.
De regel van gescheiden opslag is één van de maatregelen uit een scala aan mogelijke alternatieve maatregelen zoals anonimiseren, pseudonimiseren en versleutelen. Er zijn dus meer maatregelen die, al dan niet in combinatie, getroffen kunnen worden om risico's van bijvoorbeeld een datalek te mitigeren. Verder lijkt het ons meer juist te spreken over "logisch gescheiden opslag".

- Omleiding gebruikers naar andere website dan waar zij denken in te loggen

Reactie iDIN
Dit is zeker een goed aandachtspunt gezien ook de gesofisticeerde, al maar wijzigende vormen van aanvallen als phishing en social engineering. Een combinatie van maatregelen om awareness te verhogen en technische maatregelen kan inderdaad helpen om dit tegen te gaan zonder de privacy van de gebruiker onevenredig aan te tasten.

- Doelbinding

Reactie iDIN
Het is niet toegestaan gebruiksgegevens uit identificatieactiviteiten te gebruiken voor andere doeleinden. Dit is reeds geregeld in de AVG en behoeft niet opnieuw in dit besluit geregeld te worden. Dit geldt ook voor gebruiksgegevens "die met nadere handelingen(?) herleidbaar zijn tot de desbetreffende gebruikers" (zie ook commentaar bij art 2.19). Graag ontvangen wij een verduidelijking van de term "nadere handelingen".
In de NvT wordt een onderscheid gemaakt tussen middelen die in een andere EU-lidstaat zijn toegelaten en middelen die door BZK zijn erkend. Aan de laatste groep middelen kunnen aanvullende eisen worden gesteld. Los van het eerder genoemde ongelijk speelveld dat hierdoor ontstaat, is het in het kader van de noodzakelijke transparantie en consumentenvoorlichting raadzaam voor het publiek inzichtelijk te maken welke verschillen er zijn tussen de diverse middelen.

3.4 Werking binnen digitale overheidsinfrastructuur

Reactie iDIN
Om tijdig voorbereid te zijn op de aansluiting van het middel op de routeringsvoorziening is vereist dat aanvragers zo spoedig mogelijk de architectuurplaat ontvangen van de overheid, inclusief de noodzakelijke koppelvlakken en de bijbehorende specificaties.
In dit kader willen wij graag ook duidelijkheid over de status (publiek of privaat) van de ontsluitende dienst en welke eisen aan deze dienst worden gesteld Dit achten wij essentieel voor de aanvraag, erkenning en uiteindelijk de technische implementatie. Wij gaan ervan uit dat deze partijen gecertificeerd worden door het Scheme zoals binnen de huidige opzet om dubbel toezicht en werk te voorkomen.
Daarnaast is het van belang dat er geen standaarden opgelegd worden aan de middelenaanbieders, maar dat juist de ontsluitende diensten (specialisten) zorg dragen voor de interoperabiliteit van de verschillende eID middelen zoals in de huidige situatie. Op deze manier worden er geen grote externe afhankelijkheden gecreëerd bij bestaande partijen die tevens buiten de overheid functioneren. Het change management blijft dan bij de middelenaanbieders/scheme zelf wat zorgt voor meer efficiëntie en kostenbesparing en houdt de impact beperkt.

4 Eisen aan een identificatiemiddel (publiek en privaat)

Reactie iDIN

In het Besluit (art.3.2.) wordt gesteld dat eisen tussen publiek en privaat in principe gelijk zijn om vervolgens in te gaan op de (unlevel) verschillen. Het publieksmiddel wordt ambtshalve aangewezen, waardoor de procedure aanzienlijk eenvoudiger is met ook gevolgen voor de toetsing van de gestelde eisen.

Voor een eerlijk en gelijk speelveld dienen private en publieke middelen op gelijke wijze te worden getoetst aan de veiligheids- en betrouwbaarheidseisen bij toetreding. iDIN heeft zich als privaat middel in de praktijk reeds bewezen wat betreft veiligheid en betrouwbaarheid, zowel bij de overheid (succesvolle pilot met de Belastingdienst) als binnen de financiële sector en daarbuiten. De ACM heeft in dit kader richtlijnen opgesteld. Wij zijn dan ook benieuwd naar de overwegingen voor de ambtshalve toewijzing en of deze in lijn zijn met de uitgangspunten van de ACM terzake. Zie hiervoor: https://www.acm.nl/nl/onderwerpen/concurrentie-en-marktwerking/concurrentie-door-overheden/ondernemers-en-de-wet-markt-en-overheid
Wij tekenen hierbij wellicht ten overvloede aan dat ook publieke middelen vatbaar zijn voor de (cyber)dreigingen.

Reactie iDIN

Er bestaat onduidelijkheid rondom het toezicht. Hoe gaat dat in zijn werk?

4.1. Erkenning Private identificatiemiddelen

4.1.1 Eisen aanvrager

Aanvraag door Rechtspersoon (iDIN B.V.) met voldoende financiële continuïteitswaarborgen en die geen gevaar vormt voor cyber- of staatsveiligheid.

Reactie iDIN

Wij gaan ervan uit dat een privaat middel afkomstig van een afsprakenstelsel (scheme) ook kan worden erkend. Bij de beoordeling van een scheme-aanvraag wordt in eerste instantie gekeken naar de beheersing door het scheme van de individuele middelenaanbieders en dat de laatsten in principe niet opnieuw afzonderlijk getoetst worden door de overheid.
Wanneer kan de aanvraag worden gestart (planning) en is er reeds een concept aanvraagformulier beschikbaar?

4.1.2 Eisen aan het Middel: eIDAS- en AVG gerelateerde eisen

- eIDAS eisen

De Overheid vindt het noodzakelijk om boven op de eIDAS (1502) eisen op basis van art 2.4 van het Besluit, nadere regels uit te vaardigen via de ministeriele regeling. De aanvullende regels zien o.a. op verplicht uit te voeren identiteitscontroles in de Basis Registratie Personen (BRP) aanvullend op de controles die de aanbieder zelf uitvoert (onderdeel a uit art 2.4.).

Reactie iDIN

Betekent dit dat private aanvragers of houders van een erkenning met deze bepaling de bevoegdheid krijgen te beschikken over het BSN en deze in kunnen zetten in het publieke domein?
De identiteit verificatie in het BRP vindt iDIN een goede zaak, omdat dit het idee van één gezaghebbende bron van "waarheid" perfect ondersteunt en omdat hierdoor tegelijk mogelijke discussies over de datakwaliteit worden opgelost en daarmee uitval in de GDI wordt gereduceerd. De technische connectiviteit en juridische voorwaarden moeten zo snel mogelijk worden gedeeld om tijdig de juiste voorbereidingen te kunnen treffen. Wij veronderstellen dat het noodzakelijk is dat versleuteling van lijn en data voldoende is voor de bescherming van met name het BSN.
Waarom hoeft het publieke middel niet aan art 2.4 lid 1 en 2 te voldoen?

4.1.3 Verplicht scheiden gebruiker gegevens en gebruiksgegevens

- AVG

Gegevens over gebruikers moeten zodanig worden bewaard dat deze niet herleidbaar zijn tot gegevens over het gebruik van het middel bij publieke dienstverleners.

Reactie iDIN

De vraag is of dit niet reeds wordt gedekt door de AVG-uitgangspunten privacy by design en privacy by default en dataminimalisatie. Ook het hier genoemde mogelijk commercieel verhandelen van de gebruiksgegevens wordt reeds ingeperkt door het AVG-principe van doelbinding. Wat is de noodzaak om dit weer apart in dit Besluit te regelen?
Ten aanzien van de wijze van invulling worden gescheiden databases voorgeschreven. Wij zijn van mening dat alternatieve effectieve opties voor het aanbrengen van (logische)scheiding en of protectie in het Besluit ook ruimte dienen te krijgen.

4.1.4. Eisen aan werking van middel

Dit Besluit bevat in artikel 2.4, tweede lid, een grondslag voor het stellen van nadere technische eisen bij MR. Deze eisen kunnen nodig zijn als de specifieke inrichting van de Nederlandse GDI daartoe noopt. Afhankelijk van de keuzes die worden gemaakt met betrekking tot het toelaten van private ontsluitende diensten kan het nodig zijn het gebruik van specifieke protocollen of standaarden voor te schrijven die beide private partijen in hun onderlinge processen moeten gebruiken.

Reactie iDIN

In dit kader willen wij graag ook tijdig duidelijkheid over de status (publiek en privaat) van de ontsluitende dienst en welke specifieke eisen aan deze dienst worden gesteld? Deze is namelijk essentieel voor de aanvraag, erkenning en uiteindelijk de technische implementatie als ook voor het maken van de business case.

4.2. Eisen aan een publiek identificatiemiddel

Deze eisen zijn gelijk aan de eisen die gelden voor private middelen, met dien verstande dat

- de eisen met betrekking tot de financiële positie van de aanbieder van het middel niet van toepassing zijn.
- de eis met betrekking tot het scheiden van gegevens over de gebruiker van gegevens over het gebruik van een middel door die gebruiker van toepassing is.

Op een aantal punten is het publieke middel wezenlijk anders dan een privaat middel.

- Een voorbeeld is de relatie met de gebruikers, waarmee geen overeenkomst wordt gesloten.
- Voor een publiek middel geldt verder dat deze niet wordt erkend op basis van een aanvraag, maar dat daarvoor een ambtshalve aanwijzing plaatsvindt als het middel aan de eisen voldoet.

Reactie iDIN

Het uitgangspunt hoort te zijn dat het publieke middel in wezen gelijk is aan het private middel. Dit geldt niet alleen voor de veiligheids-technische en juridische voorwaarden, maar ook voor de financiële voorwaarden (zonder additionele begrotingsfinanciering). Dit betekent onzes inziens dat ook voor het publieke middel een overeenkomst met de gebruiker nodig is. Een ambtshalve toewijzing, zonder een vergelijkbaar toetsingstraject zoals bij private middelen, neemt bestaande cyberdreigingen en ICT-risico's niet weg. Publieke middelen lopen immers dezelfde risico's als private middelen. Wij zien dan ook graag dat publieke middelen zoveel mogelijk tegen dezelfde voorwaarden worden getoetst en toegelaten.

5.2 Verklaring van geaccrediteerde certificerende instelling
Een certificaat of conformiteitsverklaring is in het algemeen een zelfstandig document met eigen rechtsgevolg (keurmerk of toelating). In dit geval geeft de certificerende instelling een verklaring af, die echter niet meer is dan een vermoeden dat aan de geldende normen en eisen is voldaan. Het is in feite een advies aan de minister, die zelf op de aanvraag en continuering moet beslissen. Daarom toetst hij, zo volgt uit het zorgvuldigheidsbeginsel, of de (geaccrediteerde) certificerende instelling zorgvuldig onderzoek heeft verricht. De Minister van BZK is voornemens om het Agentschap Telecom in te schakelen voor deze toets, gelet op deskundigheid inzake (technisch-) inhoudelijke, procesmatige en juridische kennis en ervaring van die organisatie.

Reactie iDIN
Zijn er specifieke eisen van toepassing ten aanzien van de inhoud (structuur) en format van de conformiteitverklaring?
Op welke wijze gaat de beoogde toezichthouder (AT) haar toetsingsmandaat invullen, zowel inhoudelijk (uit te voeren verificaties) en in tijd (wanneer en hoe vaak) en wordt er ook rekening gehouden met het bestaande toezicht (door DNB) op middelenaanbieders (iDIN banken), en zo ja, op welke wijze? Het voorkomen van dubbel toezicht is belangrijk om kosten in de keten te beperken.

Leidende norm bij de verklaring is de standaard ISO 27001 Informatiebeveiliging. Deze standaard is de leidende norm bij zowel:
a. Bij aanvragers die private middelen uitgeven voor particulier gebruik bij toegang tot overheidsdiensten en
b. Bij aanvragers die private middelen uitgeven voor bedrijf/organisatie gebruik (eHerkenning) bij toegang tot de overheidsdiensten
Bij (a) is de gangbare norm waartegen de certificerende instelling dient te worden geaccrediteerd de ISO-norm 27006. ISO 27006 heeft betrekking op Information Security Management System (ISMS). D.i. een proces om informatiebeveiliging langs een gecontroleerd proces continu te verbeteren.
Bij (b) is de gangbare norm waartegen de certificerende instelling dient te worden geaccrediteerd ide ISO-norm 17065. ISO 17065 heeft betrekking op Conformiteit assessments. Omdat er voor ISO 17065 geen specifiek certificeringschema beschikbaar is, heeft BZK hiervoor een schema opgesteld dat gevolgd moet worden om aan de eisen te voldoen. Beoogd toezichthouder is Agentschap Telecom.

Reactie iDIN
In het Besluit wordt slechts één standaard voorgeschreven, terwijl er meerdere alternatieve, breed geaccepteerde standaarden bestaan die gelijkwaardig zijn. Het besluit dient ook ruimte te bieden aan de inzet van dergelijke standaarden.

6.1. Vertrouwelijk omgaan met gegevens
Hier wordt gewezen op privacy- en informatiebeveiligingsprincipes zoals Privacy by Design/Default, Dataminimalisatie, Doelbinding en Need to know/have.

Reactie iDIN
Opmerkelijk is dat doelbinding blijkbaar van toepassing blijft als de gebruiker uitdrukkelijk toestemming geeft voor gebruik voor andere doeleinden, zoals bijvoorbeeld voor een commercieel doel omdat het gebruiksgegevens zijn over inlog bij overheidsinstanties. De vraag of dit niet indruist tegen het AVG-uitgangspunt van expliciete toestemming?

6.3. Acceptatieplicht
Eenmaal erkend mag de houder van de erkenning geen potentiële gebruikers weigeren, behalve wanneer acceptatie van die gebruiker redelijkerwijs niet kan worden verwacht. Als voorbeeld wordt genoemd als de gebruiker een openstaande schuld heeft bij de houder van de erkenning.

Reactie iDIN
De middelenaanbieders van iDIN zijn als bank ook gehouden aan bijv. de WWFT en kunnen uit hoofde van anti-witwas- en sanctieregelgeving gronden hebben om bepaalde rekeninghouders te weren. Dit zou in strijd kunnen zijn met dit artikel.

6.4. Meldingsplicht
De erkenninghouder dient materiële wijzigingen in of rondom het authenticatiemiddel met mogelijke substantiële impact op veiligheid, betrouwbaarheid en gebruiksvriendelijkheid op eindgebruikers tijdig en actief te melden aan BZK. Dit geldt ook voor majeure incidenten en wijzigingen in de organisatie van de erkenninghouder of zeggenschap binnen de organisatie.

Reactie iDIN
Graag meer duiding over de aard en omvang van een meldingswaardig event. Dit dient beperkt te blijven tot relatief grote wijzigingen van het eID middel zelf.

6.5. Regels met betrekking tot het tarief
De overheid streeft naar laagdrempelig gebruik van middelen bij de overheid en heeft besloten dat de gebruikerskosten voor het gebruik betaald worden door de overheid voor zover het gebruik plaatsvindt in het publieke domein. Alleen de vaste aanschafkosten van het middel mogen in rekening worden gebracht bij de gebruiker. De overheid denkt bij de variabele gebruikerskosten aan enkele eurocenten(?) per authenticatie.

Omdat het niet efficiënt is burgergebruikers subsidies te verstrekken voor authenticatie bij de overheid heeft overheid besloten het gebruik te betalen. Twee opties worden onderzocht:
- Rechtstreekse subsidie
- Op basis van een overeenkomst

Nadere regels volgen over tarifering door een erkenninghouder aan gebruikers voor de vaste en variabele kosten van gebruik.

Reactie iDIN
Voor het maken van een business case van een privaat middel zal private partijen snel duidelijkheid moeten worden geboden over tarifering, omdat dat leidend is bij het maken van allerlei keuzes in de opmaat naar erkenning. iDIN adviseert om hiervoor ook naar het business model in andere Europese landen te kijken (4-corner model). Zie ook artikel 2.18.

6.6. Nadere regels bij ministeriele regeling
Op grond van art 2.20 eerste lid kunnen aan de erkenninghouder aanvullende eisen worden gesteld inzake hun leveringsplichten en leveringszekerheid:
1. Bereikbaarheid voor de gebruiker als het middel niet werkt: loket/website voor vragen, problem solving en melden security incidenten e.d. (onderdeel a)
2. Bescherming en vertrouwelijke behandeling van gegevens door organisatorische en security technische maatregelen (onderdeel b)
3. Bewaren van gegevens voor traceerbaarheid en herstelvermogen en inzage mogelijkheid in bepaalde gegevens voor geschilbeslechting en inzicht in eigen gebruik van het middel, (onderdeel c)
4. Periodieke controle van juistheid van de gebruikte gegevens (onderdeel d)
5. Notificatie gebruikers bij geplande onbeschikbaarheid (onderdeel e)
6. Bereikbaarheid voor dienstverleners of beheerders van GDI (onderdeel f)
7. Naleving van gestelde beschikbaarheid normen. Normen komen in MR (onderdeel g)
8. Herkenning van misbruik of fraude of het herstellen of beperken van de gevolgen daarvan (onderdeel h)

Reactie iDIN
Voor zover bekend, dekt de vereiste verklaring initieel en daarna jaarlijks (afgegeven of op basis van standaard ISO 27001) alle voornoemde punten rond leveringszekerheid. Dit lijkt op een onnodige doublure. De jaarlijkse hertoetsing borgt de continuïteit van leveringszekerheid.

8. Regeldruk en administratieve lasten:
De Kosten voor het indienen van een aanvraag en voor houders van een erkenning bestaan uit:

- Kosten voor certificering (= kosten voorbereiding audit + kosten uitvoering audit)
- Kosten van de technische beveiligingstest die driejaarlijkse dient te worden uitgevoerd als bewijs van juiste veilige werking van het middel.
- Kosten certificering conform ISO/IEC 27001 (Eisen Informatiebeveiliging) en ETSI 319-411-2 (eisen certificaat uitgifte Trust Service Providers)

Reactie iDIN
Deze kosten kunnen flink oplopen. Dit is erg ondoorzichtig. Kosten die door wet- en regelgeving ontstaan moeten in rekening kunnen worden gebracht. Graag meer duidelijkheid hierover, ook om de business case te kunnen maken.
Hoe zit het met de kosten van het reguliere toezicht?

Bijlage 2
Reactie op Besluit identificatiemiddelen voor burgers Wdo

Art.2.2. Eisen aanvrager
Lid f: zodanige scheiding van gegevens van gebruikers- en gebruiksgegevens dat aantoonbaar te maken is dat gegevens van de gebruiker niet herleidbaar zijn tot gegevens over het gebruik door de gebruiker.

Reactie iDIN
Graag nadere guidance (voorbeelden) over de verschillende alternatieven voor wat de overheid een toereikende scheiding maatregel acht. Nu is alleen scheiding van databases genoemd.
Volgens art. 2.2 lid 1 onder f moet een aanvrager gegevens over een gebruiker van een middel verwerken op een wijze die is afgescheiden van gegevens over het gebruik van het middel. Paragraaf 4.1.3 suggereert dat indien beide soorten gegevens tegelijkertijd zouden worden gecompromitteerd, zij niet aan elkaar gerelateerd zouden moeten kunnen worden. Wij vatten dit op dat er een logische scheiding dient te zijn en geen technische scheiding. Een technische scheiding heeft namelijk een enorme impact en is daardoor kostenverhogend.

Wat wordt bedoeld met "een vestiging in Nederland " (lid 1 sub g). Als een BigTech uit VS of China een vestiging opent in Nederland, kan deze dan een aanvraag indienen? Of gaat het om een in Nederland gevestigde rechtspersoon (die bijvoorbeeld al onder toezicht van DNB/AFM valt).

Art 2.3 Eisen middel
Sub b: stelt eisen aan functionering van het middel. Art 5b Besluit DO specificeert de eisen

Reactie iDIN
Van belang is om zo snel mogelijk te weten te komen op welke wijze het private middel toegang kan krijgen tot deze BRP-voorziening om voornoemde data te ontsluiten. Welke technische en juridische voorwaarden zijn van toepassing?
Is het mogelijk dat bij erkenning van een scheme, met daaronder meerdere individuele middelenaanbieders, deze aanbieders individueel gebruik kunnen maken van de BRP-connectie? Hoe ziet men dit precies voor zich? Is daar aanvullende wet- of regelgeving voor nodig?

De machtigingsvoorziening dient ook een onderdeel van de Generieke Digitale Infrastructuur te zijn. Dit zou een algemene dienst moeten zijn, die kan werken met alle eID middelen (zoals iDIN) om een gelijk speelveld te creëren. Graag zouden wij de werking van de machtigingsvoorziening in de architectuurplaat opgenomen zien.

Artikel 5b Besluit DO geeft aan:
Door invoering van artikel 5b wordt de persoonsgegevensverwerking geregeld die plaatsvindt door de aanbieder van een toegelaten (erkend) privaat identificatiemiddel als bedoeld in artikel 9, tweede lid, van de wet, of door de erkende ontsluitende dienst als bedoeld in artikel 9, derde lid van de wet.
Onderdelen d en e geven een opsomming:
d. de gebruiksgegevens, waaronder het IP-adres en de kenmerken van de gebruikte software en hardware van het apparaat waarmee de gebruiker van het middel is ingelogd, handelingen van de gebruiker, het door de gebruiker gekozen authenticatieniveau, de website van de instelling waar de gebruiker een toegelaten privaat authenticatiemiddel aanvraagt of vanuit welke de gebruiker van het toegelaten private identificatiemiddel met het middel inlogt, sessiegegevens, waaronder cookies, en overige gegevens met betrekking tot het soort en tijdstip, kenmerken van het gebruik waaronder gegevens over de gezondheid waar mogelijk in versleutelde vorm;
e. gegevens die relevant zijn voor de adequate werking van het middel, waaronder in ieder geval de kenmerken van de door de gebruiker gebruikte software en hardware;

Reactie iDIN
Moet deze persoons identificerende informatie en eventuele wijzigingen hierin worden geleverd aan de overheid door de aanbieder van het private middel? Indien dit het geval is, lijkt dit ons disproportioneel en niet in lijn met het principe van dataminimalisatie. Graag meer duidelijkheid over de noodzaak van de overheid om deze informatie te verkrijgen.

Art.2.4. Nadere eisen bij Ministeriele Regeling (MR)
Reactie iDIN
*De invulling van de nadere eisen ten aanzien van de **onderdelen a tot en met i** (eIDAS focus), zoals uitgeschreven in de NvT (4.1.2), lijken redundant. Pas bij de publicatie van MR kan goed worden beoordeeld of e.e.a. niet onevenredig unlevel wordt gemaakt voor NL-instellingen (tegenover hun EU counterparts).*
Ook de eisen voor interoperabiliteit (koppelvlakken) met onderdelen binnen GDI dienen op korte termijn gedeeld te worden, omdat zij ook impact hebben op ontsluitende diensten (zie 4.1.4. van NvL).

Art.2.8. Eisen aan verklaring van certificering
De verklaring door de certificerende instelling op grond van ISO 27006 dient conformiteit aan te tonen met aan de eisen bedoeld in art.2.2, 2.3, 2.4: dat zijn o.a. de volgende aspecten:
- Scheiding van gegevens van gebruikers- en gebruiksgegevens;
- Interoperabiliteit binnen GDI;
- Koppeling BRP en veilige verwerking BRP-data;
- Gebruiker inzicht geven in authenticatiehandelingen;
- Zie verder Eisen uit par 4.1.2 en 4.1.3 NvT.

Reactie iDIN
iDIN BV zal als scheme owner van iDIN (afsprakenstelsel) de aanvraag voor erkenning indienen en wenst ook als scheme geaccrediteerd te worden. Het scheme ziet toe op naleving van de (eIDAS-compliant) iDIN-regelgeving van de vergunninghoudende iDIN-banken/middelenverschaffers (licentiehouders). Wij vragen dan ook dat in het Besluit duidelijker wordt aangegeven dat ook schemes die private middelen in licentie uitgeven kunnen worden erkend (enigszins vergelijkbaar met het ETD-stelsel) en het bewijs van naleving levert.

Art.2.18 Beprijzing
Reactie iDIN
Zie ook par 6.5 van NvT
De overheid denkt bij de variabele gebruikerskosten aan enkele eurocenten(?) per authenticatie in rekening te brengen door rechtstreekse Subsidie of op basis van een Overeenkomst. Dit betreft de tarifering van de gebruiker. Onduidelijk is hoe de tarifering van de afnemer (de bestuursorganen) plaatsvindt en op welke wijze de contractuele relatie met de middelenaanbieder zal plaatsvinden.

Art.2.19 Omgaan met gegevens
Ziet toe op vertrouwelijke en veilige omgang met gegevens (i.c. privacy by design, privacy by default, dataminimalisatie, need to know/have, functiescheiding, 4-ogenprincipe) en doelbinding d.w.z. alleen te gebruiken voor authenticatiedienstverlening. Verder past hier ook een gebruiker ondersteunende dienst voor zowel gebruiker als dienstverlener (bijv. voor security meldingen). Zie ook art 20.lid a en b.

Reactie iDIN
De overheid is van mening dat art.6 lid 1 onderdeel a van de AVG (expliciet consent) niet kan worden toegepast om de gegevens toch voor andere doeleinden te gebruiken.
Belangrijk is eerst goed duidelijk te krijgen op welke gegevensset deze regel precies van toepassing is, d.w.z. gaat het om de gegevens over de gebruiker of de gegevens over het gebruik. Is het juist te veronderstellen dat het om het laatste gaat?

Art. 3.1 Betrouwbaarheidsniveaus
Reactie iDIN
Hoe ziet de ministeriële regeling eruit? Op basis waarvan wordt dat besluit genomen?