Retouradres Postbus 96810 2509 JE Den Haag

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
T.a.v. De staatssecretaris van Koninkrijksrelaties en Digitalisering
Mevr. A. Van Huffelen
Turfmarkt 147
2511DP Den Haag

eHerkenning
Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 96810
2509 JE Den Haag

www.eherkenning.nl
info@eherkenning.nl

Kenmerk
01/2022-1

Classificatie
Openbaar

Datum 2 december 2022
Betreft Reactie MR nadere eisen toelating identificatiemiddelen WDO

Geachte mevrouw Van Huffelen,

Allereerst willen wij u, de staatssecretaris voor Koninkrijksrelaties en Digitalisering bedanken voor de mogelijkheid om onze visie met u te delen op de concept Ministeriële Regeling (MR) nadere eisen toelating identificatiemiddelen WDO (Wet digitale overheid). Als onderdeel van de governance voor eHerkenning, voor het stelsel Elektronische Toegangsdiensten (ETD), maken wij hier graag gebruik van.

Het is niet meer dan logisch dat er onder de WDO goede, strenge eisen aan de toelating van digitale identificatiemiddelen worden gesteld, net zoals in het Afsprakenstelsel ETD al gebeurt. Op dit moment zijn ca 1500 diensten van de overheid (belastingdienst, RVO, KvK, VNG, etc.) aangesloten op het stelsel herkenning en hebben ruim 1 miljoen ondernemers een eHerkenning inlogniddel en bijbehoren de machtigingen om in te loggen op deze diensten. Wij willen u via deze internetconsultatie van constructief commentaar voorzien, met het oog op behoud van continuïteit voor diensten aanbieders en andere gebruikers van het eH stelsel, zodat u tot een passende en realistische regeling kunt komen, die erin voorziet dat de dienstverlening met eHerkenning ongestoord verder kan gaan onder de WDO.

Er zijn zoals vermeld ruim een miljoen gebruikers van eHerkenning, die dagelijks hiermee inloggen om efficiënt, veilig en betrouwbaar digitaal hun zaken te kunnen doen. Niet alleen ondernemers, maar ook kerkgenootschappen, verenigingen, stichtingen en binnenkort ook ambassades, maken daar gebruik van. Daarnaast zijn er meer dan 600 dienstverleners, publieke én private, met hun elektronische diensten aangesloten om inloggen met eHerkenning aan te kunnen bieden. Kortom, de BV Nederland is inmiddels zeer afhankelijk van eHerkenning. Voor eHerkenning is een soepele overgang naar de WDO in 2023, daarom van het grootste belang. Wij gaan ervanuit dat dit ook voor u als huidige eigenaar van het ETD-stelsel geldt.

Namens de Vereniging van eHerkenning aanbieders

F. Jonker (Reconi), voorzitter
L. van Lent (Unified Post), secretaris
M. Wendt (Digidentity), penningmeester
M. Valk (KPN)
A. Keuter (Signicat/We-ID)
A. Jonkers (Quo Vadis)
M. Stultjens (OneWelcome)

1. Algemeen

Voordat we specifiek ingaan op een aantal belangrijke onderwerpen in de MR, willen we eerst wat algemene opmerkingen en kanttekeningen plaatsen.

Ten eerste wordt een uitputtende reactie op deze conceptregeling bemoeilijkt door het feit dat deze samenhangt met verschillende AMvB's en Ministeriële Regelingen die al een tijd geleden in consultatie zijn geweest, van commentaar voorzien zijn, maar waarvan in de tussentijd geen nieuwe, definitieve, versies verschenen zijn. Zo is het o.a. onduidelijk wat gedaan is en wordt met het commentaar op het Besluit digitale overheid van ruim 4 jaar geleden. Dit geldt bijvoorbeeld ook voor het Besluit bedrijfs- en organisatie middel Wdo en Besluit identificatiemiddelen voor natuurlijke personen Wdo. Alle AMvB's en regelingen moeten aansluiten op elkaar en de WDO, en consistent zijn met elkaar. Wijzigingen in één hiervan heeft consequenties voor de ander en de beoordeling daarvan. Ook zijn inmiddels bepaalde veronderstellingen niet meer juist. Zo is de HM (de ontsluitende dienst) geen erkende rol meer omdat daarmee de administratieve lasten zouden verminderen. Met de kennis die we nu hebben weten we dat dit geen juiste veronderstelling is.

Ten tweede merken wij op dat het gebruik van authenticatie en machtigingen in het Business to Business (B2B) domein geen onderdeel is van de MR. Wij benadrukken dat dit een omissie is en onzekerheid bij private dienstverleners en hun gebruikers veroorzaakt. In tegenstelling tot DigiD worden private digitale identificatiemiddelen, zoals eHerkenning, nu al voor zowel transacties met de overheid (voor publieke diensten), als voor puur zakelijke transacties gebruikt (private diensten).

Ten derde worden ketenmachtigingen, oftewel horizontale machtigingen, niet beschreven. Dit zijn machtigingen tussen bedrijven. Denk bijvoorbeeld aan intermediairs, zoals accountantskantoren, die door bedrijf x gemachtigd worden om digitaal belastingaangifte te doen. Er zijn duizenden intermediairs actief, die ondernemers veel werk uit handen nemen. De processen van intermediairs zijn ingericht op het gebruiken van eHerkenning en ketenmachtigingen. EHerkenning leveranciers hebben dan ook inmiddels vele tienduizenden ketenmachtigingen uitgegeven. Continuïteit van deze dienstverlening is van groot belang en grote waarde voor ondernemend Nederland. Onduidelijk is hoe hierin voorzien wordt met deze beoogde regelgeving.

Het vierde opvallende punt in deze MR is dat er geen eisen gesteld worden aan de erkenning van "ontsluitende diensten", zoals genoemd in de WDO, artikel 11, lid 3. In combinatie met de eisen in artikel 2.18 om bij een bedrijfs- en organisatiemiddel de authenticatiecode door de machtigingsdienst te laten verzenden, bevestigt dit het beeld dat voor een andere inrichting, een andere architectuur van het hele stelsel voor identificatiemiddelen gekozen wordt. Het nieuwe ontwerp hiervoor, de IT-architectuur, is echter nog niet afgerond, en zorgt voor een niet te onderschatten wijziging ten opzichte van de huidige situatie. De huidige "ontsluitende dienst" binnen het stelsel voor eHerkenning, de HM (eHerkenningsmakelaar), is een cruciaal onderdeel van het stelsel, en ontzorgt de dienstverleners in hun aansluiting erop. Wij hebben de volgende zorgen over deze nieuwe architectuur:

- Het nieuwe ontwerp heeft zich nog niet bewezen in de praktijk en de tijd dringt. De huidige architectuur van eHerkenning heeft zich al ruim 12 jaar bewezen en werkt zonder problemen. De nieuwe architectuur lijkt zich vooral op nieuwe techniek te richten in plaats van hergebruik van bestaande bewezen voorzieningen. Het is niet wenselijk dat hierdoor continuïteitsrisico's voor gebruikers in het bedrijvendomein ontstaan.

- Voor de meer dan 600 aangesloten dienstverleners, waaronder de Belastingdienst, RVO, UWV, gemeenten, worden verschillende inlog en machtiging scenario's ondersteund. Alle scenario's zullen als separaat document worden toegevoegd. Er is nog onvoldoende zekerheid dat al deze scenario's ook in de nieuwe situatie worden ondersteund. Dit moet geborgd zijn om grote problemen in de praktijk te voorkomen. Wij zijn samen met de belangrijkste dienstverleners gestart met een inventarisatie van alle inlog en machtiging scenario's die momenteel door eHerkenning worden ondersteund. Zodra deze inventarisatie gereed is zullen wij deze aan uw medewerkers beschikbaar stellen, zodat in de volgende versie van MR hier rekening mee gehouden kan worden. Ons grootste angst scenario is dat we geen goede continuïteit en een soepele migratie kunnen bieden aan de huidige gebruikers van eHerkenning in en naar de nieuwe situatie. In bijlage 1 hebben we het resultaat van de inventarisatie tot nu opgenomen. In het reguliere periodieke overleg dat ons Intaketeam heeft met de architecten van BZK zal uiteindelijk tot een definitieve (en dus volledige) lijst moeten worden gekomen.
- De migratie van de oude situatie naar de nieuwe architectuur. Er is geen zekerheid of er voldoende borging is dat de huidige dienstverlening binnen het bestaande ETD-stelsel in de overgangssituatie ondersteund blijft worden, en dat er ook ruimte blijft voor gewenste doorontwikkelingen. Wij pleiten ervoor dat hier voldoende budgetten en organisatorische capaciteit beschikbaar voor worden gesteld. De overgangssituatie voor dienstverleners is immers 3 jaar. Voor eHerkenning leveranciers 18 maanden.
- Het is niet mogelijk nu een impactbepaling te maken op haalbaarheid en tijdigheid door de onduidelijkheden die er nog zijn, bijvoorbeeld ten aanzien van de nieuwe architectuur en/of de wijze van aansluiten op centrale voorzieningen. De overgangstermijn van 18 maanden is mogelijk niet haalbaar.
- Het kan leiden tot problemen en kostenverhogingen voor publieke dienstverleners, waaronder dure tijdrovende IT (migratie) projecten.
- Of de huidige ondersteunde bijzondere groepen gebruikers, die niet onder een standaard KVK-inschrijving vallen, zoals kerkgenootschappen, ambassades en buitenlandse organisaties, ook in de nieuwe situatie nog optimaal gebruik kunnen maken van eHerkenning is onduidelijk. Ook zijn er gebruikers zonder BSN die met behulp van eHerkenning nu kunnen inloggen en zo direct niet meer. eIDAS kan daar een oplossing zijn, maar niet ieder land heeft een erkend eID en gebruikers buiten Europa hebben niets aan eIDAS.

Wij stellen voor dat de nieuwe architectuur eerst bewijst dat het alle bestaande situaties, alle bestaande usecases van eHerkenning, probleemloos ondersteunt en dan pas gefaseerd wordt ingevoerd. Bovendien mogen huidige gebruikers, die middelen kunnen hebben met een looptijd van 5 jaar, geen problemen ondervinden. Een overgangstermijn van 5 jaar is dan ook noodzakelijk.
Wij gaan graag het gesprek met u aan over de nog ontbrekende usecases.

Overigens adviseren wij u om een herbezinning te doen op de architectuur. Wij zijn er stellig van overtuigd dat het veel voordelen biedt om op basis van de eHerkenning architectuur verder te gaan. Graag willen wij met u in gesprek over de voordelen die dat zou opleveren.

We zullen verder per onderwerp of artikel opmerkingen en kanttekeningen bij de MR plaatsen, en waar mogelijk suggesties geven.

2. Veiligheid: open source en publicatie broncode

De erkende aanbieders moeten het middel laten toetsen tegen een aanvalspotentieel (art 2.4 regeling). Wij betwijfelen of open source dan nog iets toevoegt aan de veiligheid van het middel. Daarnaast kunnen inzake open source (art. 2.5 e.v.) de volgende kanttekeningen worden geplaatst:

- Buitenlandse aanbieders die voldoen aan eIDAS mogen in Nederland actief zijn en hun inlogmiddelen aanbieden. Zij mogen wel van biometrische technieken gebruik maken en kunnen geen Open Source eis opgelegd worden. Dit zorgt voor oneerlijke concurrentie ten opzichte van Nederlandse aanbieders. Wij bepleiten een level playing field.
- Wij vragen ons af hoe de minister de uitzonderingen op de eis wil gaan beoordelen. Wij stellen voor dat een toetsingskader wordt ontwikkeld en een toezichthouder hiervoor wordt aangewezen.
- Onduidelijk is welke onderdelen van de identificatiemiddelen aangewezen gaan worden als open source en per wanneer, de tabel (bijlage 1) hiervoor is namelijk niet ingevuld. Als de gehele lijst van onderdelen uiteindelijk open source moet worden, zetten wij onze vraagtekens bij de haalbaarheid hiervan. De huidige aanbieders van eHerkenning maken veelal gebruik van standaard softwarepakketten. Deze software kan niet altijd vervangen worden door open source varianten. Deze broncode zal nooit vrijgegeven kunnen worden.
- Onduidelijk is of de bepalingen inzake open source ook voor software van onderaannemers geldt. Erkende partijen kunnen dit niet afdwingen.
- Onzeker is of de open source verplichting geldt voor (aangewezen) publieke identificatiemiddelen en machtigingen, en voor centrale voorzieningen zoals het centraal inzageregister, BSNk.
- Het publiceren van broncode is slechts bij een gedegen bug bounty programma (vanuit de overheid) een oplossing. Het gaat er niet om dat de broncode gepubliceerd wordt, maar dat deze beoordeeld wordt door betrouwbare ethische hackers. Dit kan alleen met een bug bounty programma. Het publiceren van broncode zal slechts kwaadwillenden (denk aan hackers vanuit GEO-politieke achtergrond) een voorsprong geven, wat voor een identiteitsoplossing zeer ongewenst is.
- Marktpartijen hebben veel geïnvesteerd in hun software. Zij hebben het intellectueel eigendom (IP) van de software (de broncode). Die broncode wordt nu goed beschermd. Het mag niet zo zijn dat deze broncode door andere partijen wordt gebruikt. Wij pleiten ervoor dat dit IP beschermd wordt en voorkomen wordt dat buitenlandse kapers Nederlandse eToegangsdiensten stelen.

3. Biometrie

Het is onduidelijk waarom het gebruik van biometrie als authenticatie-factor expliciet wordt uitgesloten (art. 2.13). Wij zien dit als een gemiste kans als deze keuze overeind blijft. Het level playing field wordt hierdoor scheef getrokken. Elders in de EU mag dit namelijk wel. Genotificeerde eIDAS-middelen die door Nederlandse dienstverleners geaccepteerd móeten worden mogen wél 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. Wij stellen voor om dit expliciete verbod te schrappen en dit aan te erkennen partijen zelf te laten. Gebruikers kunnen zelf een keuze maken uit middelen die dit wel of niet gebruiken.

4. Overeenkomsten

Onduidelijk is wat precies de overeenkomst tussen gebruiker of rechtspersoon en authenticatiedienst of machtigingsdienst (art. 2.9 en 2.21) moet inhouden. Het lijkt erop dat vereist wordt dat er per gebruiker en dienstafnemer (rechtspersoon of onderneming) een overeenkomst/contract afgesloten dient te worden. Dit is een extra administratieve last. In de huidige situatie kan volstaan worden met een handtekening en een akkoord op gebruikersvoorwaarden. Als álle huidige gebruikers en/of dienstafnemers alsnog een contract af moeten sluiten, betekent dit een enorme administratieve lastenverzwaring en flinke uitdaging in de uitvoering voor de huidige eHerkenningsleveranciers. Wij bepleiten een ruime interpretatie van het begrip “overeenkomst” zodat een grote administratieve lastenverzwaring voorkomen wordt.

Tevens lijkt het erop dat vereist wordt dat elke dienstverlener een overeenkomst moet sluiten met alle erkende Machtigingsdiensten (MD’s). Dit zou een verzwaring van de regeldruk bij dienstverleners veroorzaken die niet gewenst is.

5. Verzekering

De eis dat erkende aanvragers (leveranciers) een verzekering (art. 2.1) voor direct en indirecte schade van 10 miljoen euro moeten afsluiten leidt tot hoge(re) kosten voor de erkende leveranciers en staat niet in verhouding met de 2,5 miljoen die nu wordt gevraagd. De onderbouwing mist waarom dit bedrag zo hoog moet zijn. Kan deze niet gegeven worden, dan stellen wij voor het verplichte bedrag van het ETD-stelsel aan te houden. Hogere kosten moeten immers terug verdiend worden.

6. BSN

Het BSN verplicht stellen in álle situaties leidt tot problemen. In het business to government (B2G) domein is het niet nodig en ook niet altijd mogelijk om aan acterende persoon een BSN te koppelen. Restgroepen en met name buitenlandse restgroepen die relevant zijn voor de Belastingdienst hebben ook geen BSN. Een direct gevolg van deze keuze is dat in de toekomst niet alle inlog- en machtiging scenario's zoals deze nu in het ETD-stelsel worden ondersteund, gehandhaafd kunnen worden. Daarnaast zal het alsnog opvragen en verifiëren van het BSN van alle bestaande gebruikers, kostenverhogend werken. Het leidt ook tot een onduidelijke situatie als gebruikers niet binnen 18 maanden hun BSN registreren.

7. Klantreis

Aan de Machtigingsdienst wordt de eis gesteld om de authenticatiecode te versturen naar publieke dienstverleners (art. 2.18 en paragraaf 2.2.5 in de toelichting) i.p.v. dat de ontsluitende dienst, de eHerkenningsmakelaar dit doet. Dit leidt tot een geheel andere klantreis voor bedrijfs- en organisatiemiddelen dan nu het geval is. Wij hebben zorgen dat dit tot een langere en minder positieve klantreis leidt. Zo moet een gebruiker elke keer extra handelingen doen, bij het inloggen bij een andere Dienstverlener. Dit heeft effect op het gebruik en adoptie van de nieuwe voorzieningen door de gebruiker. In de voorlopige architectuur zijn optimalisaties van de klantreis, zoals het onthouden van gemaakte keuzes, ook niet mogelijk (op een manier die voor de gebruiker echt werkt en onderhoudbaar is). Bij de architectuur die voor eHerkenning gebruikt wordt is onthouden wel mogelijk en kan het aantal keuzes beperkt worden tot één (simpelweg: "Inloggen"). Wij stellen voor de klantreis zo eenvoudig, begrijpelijk en efficiënt mogelijk te laten zijn.

8. Interoperabiliteit

Samenwerking tussen de verschillende aanbieders (houders van erkenning) én de aangewezen publieke voorzieningen is essentieel voor een goede werking van het gehele stelsel voor Toegang. Naast de eHerkenning leveranciers, kunnen ook geheel nieuwe inlogmiddelen zich laten erkennen als bedrijfs- en organisatiemiddel. De gebruiker zal dus nog meer keuze krijgen. Het is alleen onduidelijk hoe de samenwerking tussen al deze verschillende aanbieders gaat worden geregeld en hoe de overheid hierin faciliteert met ingang van de Wdo. Wij roepen u op om voor verduidelijking te zorgen.

9. Publiek identificatiemiddel

In Artikel 1.1 staat 'Persoonlijke stelselcode'. In het beoogde cryptografische polymorfe pseudonimisering schema komt deze term echter niet voor. Het is niet duidelijk wat wordt bedoeld met 'Persoonlijke stelselcode'. Wij stellen voor dit te verduidelijken.

10. Beschikbaarheid, beveiliging en incidenten

Het is niet duidelijk hoe men gekomen is tot de (vrij specifieke) eisen aan beschikbaarheid in art 4.4 en ook is er onduidelijkheid omtrent de wijze van meten. Daarnaast moet volgens de MR de helpdesk van erkende partijen ten minste 60 uur per week telefonisch bereikbaar zijn (art. 4.8). Wij hebben begrepen dat deze eis gebaseerd is op de wens dat het voor iedereen mogelijk moet zijn om gedurende een groot deel van de dag in contact te kunnen komen met een erkende leverancier. Als dit op deze manier gevuld moet worden, dan leidt dit onnodig tot hoge kosten voor de leverancier en dus gebruiker en/of dienstverlener aangezien nu 40 uur de norm is. Daarnaast gaat deze invulling voorbij aan die situaties dat een gebruiker de Nederlandse taal niet machtig is, of dat de persoon op een andere manier wenst te communiceren. Wij stellen voor deze eis andere te formuleren, zodat deze meer aansluit op de wijze waarop personen in deze moderne tijd 24/7 wensen te communiceren en dat diegene die het wil overdag contact kan opnemen per telefoon. Daarnaast is een specificering wat onder 'telefonisch bereikbaar zijn' verstaan wordt ook wenselijk om verschillende interpretaties te voorkomen.
De voorgestelde incidentafhandeling (art. 4.6 e.v. en toelichting paragraaf 5.3.6) is ten opzichte van het huidige ETD-stelsel veel minder uitgewerkt met minder voorschriften. Dit leidt tot een mindere service aan gebruikers en dienstverleners. Ook is het niet duidelijk hoe er invulling aan gegeven wordt als er ergens in de keten een storing plaatsvindt. En hoe verloopt bij een incident de samenwerking tussen publieke dienstverleners en erkende aanbieders?

11. Fraude

In een stelsel van meerdere aanbieders van identificatiemiddelen, centrale voorzieningen, grote groepen dienstverleners en grote aantallen gebruikers is een zorgvuldige en gedegen coördinatie bij onderzoek naar (mogelijke) fraude van zeer groot belang. Het is in de MR niet duidelijk hoe deze coördinatie ingevuld zal gaan worden. Wenselijk is dat dit verder uitgewerkt wordt in de MR.

12. eIDAS

Buitenlandse aanbieders van identificatiemiddelen welke zijn genotificeerd onder eIDAS mogen en kunnen in Nederland actief zijn en hun toegangsdiensten/identificatiemiddelen aanbieden. Het is daarom van belang dat de MR op eIDAS aansluit en hier niet verzwarend werkt. Dit zodat er een level playing field is en blijft. Geconstateerd is echter dat de MR in diverse artikelen zwaardere eisen stelt dan de eIDAS uitvoeringsverordening 2015/1502.

Concreet brengen we hier graag Artikel 2.4 onder MR onder de aandacht. In lijn met eIDAS schrijft de MR voor dat identificatiemiddelen weerstand moeten bieden tegen aanvallen. Echter constateren wij dat de eisen die onder de MR worden gesteld aanzienlijk zwaarder en breder zijn dan de eisen die gesteld worden onder de eIDAS uitvoeringsverordening 2015/1502.

Het is onduidelijk waarom, en ongewenst dat, er onder de MR zwaardere eisen worden gesteld ten opzichte van de eIDAS uitvoeringsverordening (2015/1502). We bepleiten daarom een level playing field.

13. Vergoeding burgermiddel

Om actief te worden in het burgerdomein is voor private partijen een (transactie)vergoeding voor het leveren van authenticatiediensten in het burgerdomein noodzakelijk. Voor het inloggen met DigiD hebben Dienstverleners ook jarenlang moeten betalen aan BZK/Logius. Zo'n (transactie)vergoeding voor het leveren van authenticatiediensten in het burgerdomein ontbreekt momenteel. Zonder vergoeding verwachten wij dat private partijen hun rol als fall back ingeval van uitvallen van DigiD niet kunnen en dus niet zullen gaan invullen.

14. Expertgroep normenkader eHerkenning

De expertgroep normenkader eHerkenning – specialisten op het gebied van uitleg van regelgeving- hebben gezamenlijk een verschillen analyse op artikel niveau uitgevoerd. Wij denken dat dit een waardevolle inbreng is voor uw medewerkers om te bepalen waar de MR schuurt of volledig strijdig is met eIDAS en/ of eHerkenning. Deze inventarisatie is nog niet volledig afgerond. In overleg met ambtenaren van BZK is afgesproken dat de definitieve verschillenanalyse op een later moment zal ingediend en worden besproken met uw specialisten. Alles met het oog op continuïteit van dienstverlening en soepele migratie van eHerkenning nu naar de nieuwe situatie

Bijlage 1 Voorlopige lijst met Inlog en machtiging scenario's eHerkenning