

51



> Retouradres

ministerie van BZK

Postbus 20011  
2500 EA Den Haag

Bestuurskern  
Dir. Ruimtelijke Ontwikkeling  
Afdeling Geoinformatie  
Plesmanweg 1-6  
Den Haag



IENM/BSK-2017/89099

Datum **- 7 APR. 2017**  
Betreft **Reactie IenM wet GDI en Uniforme Set van Eisen  
(consultatieversie)**

Geachte heer Prinsen,

**Inleiding**

Hierbij ontvangt u de reactie van IenM op de wet GDI. In deze brief meld ik u een aantal hoofdpunten dat voor ons ministerie als geheel van belang is.

Een aantal IenM-organisaties heeft ook separaat een reactie aan u toegezonden via het aangegeven emailadres. Als bijlagen bij deze brief vindt u de integrale reacties aan van deze uitvoeringsorganisaties.

Voor eID op het rijbewijs gaat het Ministerie van IenM ervan uit dat zaken omtrent regelgeving, financiering en dergelijke in de daarvoor gebruikelijke gremia worden besproken. Punten die hierbij voor IenM nog aandacht behoeven zijn derhalve niet in deze reactie opgenomen.

Gelet op het nog ontbreken van uitvoeringsregels kan deze reactie niet anders dan op hoofdlijnen zijn en een voorlopig karakter hebben.

**Reikwijdte**

In zijn algemeenheid wil IenM zoveel mogelijk gebruik maken van GDI-bouwstenen, met name voor de implementatie van de Omgevingswet in het Digitaal Stelsel Omgevingswet (DSO) dat thans in ontwikkeling is en bestaande ICT-voorzieningen, zoals het Omgevingsloket Online (OLO), Ruimtelijkeplannen.nl (RP) en Activiteitenbesluit Internet Module (AIM) zal gaan vervangen. IenM ondersteunt de wet GDI, omdat deze wet een basis kan bieden voor een betere rechtspositie van de burger en het bedrijf voor hun relatie met de overheid. De voorbereiding van de wet GDI valt samen met de Omgevingswet. De Omgevingswet zal naar verwachting op 1 juli 2019 in werking treden. Gelet op uitfasering van de bestaande voorzieningen is het niet gewenst de wet GDI hierop van toepassing te doen zijn. IenM vraagt daar aandacht voor.

In vergelijking met de brief van BZK van 4 december 2015 aan de TK valt op dat de reikwijdte van het onderhavige wetsontwerp aanzienlijk is versmald. Mede omdat IenM zoveel mogelijk gebruik wil maken van GDI-bouwstenen voor het DSO heeft IenM grote belangstelling voor de verdere ontwikkeling van de wet GDI op middellange en lange termijn.

Om te bepalen voor welke organisaties IenM een verantwoordelijkheid heeft voor voorliggend wetsvoorstel zij verwezen naar bijlage 4.1 van de Rijksbegroting<sup>1</sup>. Deze bijlage geeft hierin principe een goed inzicht in. Voor de overige vragen van het format Uitvoerbaarheids- en handhaafbaarheidstoets Wet GDI zij verwezen naar de antwoorden van de verschillende uitvoeringsorganisaties, omdat deze antwoorden per organisatie verschillend zijn.

**Bestuurskern**  
Dir. Ruimtelijke Ontwikkeling  
Afdeling Geo informatie

**Datum**  
3 april 2017

### **Wetsontwerp**

Door de RDW is uitvoerig ingegaan op praktische gevolgen van de wet GDI alsook van de USvE. Verwezen zij dan ook vooral naar deze reactie.

*Doorgifteplicht in plaats van acceptatieplicht.* Het wetsontwerp, zoals in consultatie is gebracht, gaat in artikel 5 van de wet uit van een acceptatieplicht van de Bestuursorganen en aangewezen organisaties. Gepleit wordt voor het omgekeerde model waarbij de ontsluitende diensten de verplichting krijgen tot het ontsluiten van alle erkende middelen, zoals ook in een eerdere versie van het wetsontwerp was opgenomen.

*Multimiddelenaanpak en level playing field.* In de wet is nu geregeld dat private middelen wel in het publieke domein gebruikt kunnen en mogen worden, maar dat publieke middelen niet in het private domein mogen worden gebruikt. Dit belemmert het gebruik van het publieke middel als 'moederkaart'.

*Ketenafhankelijkheid.* Door RDW is de vraag opgeworpen of de wet ook dient te gelden voor zakelijke diensten aan vaste ketenpartners volgende eIDAS-verordening. De RDW staat op het standpunt dat zakelijke diensten aan vaste ketenpartners volgens de eIDAS-verordening vallen onder "verlening van diensten die uitsluitend binnen gesloten systemen gebruikt worden tussen een welbepaalde groep deelnemers" en dus geen openbare diensten zijn "die aan het publiek verleend worden" (o.a. overweging 21 uit EU nr 910/2014). De RDW leest het wetsvoorstel GDI, hoewel dat hierin nog niet scherp is afgebakend, in dat licht. Uitgaande van dat standpunt blijft de RDW voor dergelijke sectorale diensten het RDW-eigen middel ondersteunen.

Veel bedrijven hebben daarbij te maken met geïntegreerde RDW-diensten binnen hun eigen bedrijfsvoering.

Naar verwachting zullen bij andere uitvoeringsorganisaties analoge ketensituaties optreden.

RDW geeft voorts aan dat indien de wet GDI toch van toepassing zal worden verklaard op dergelijke gevallen, dan in ieder geval een overgangstermijn van 5 jaar dient te worden gehanteerd.

IenM sluit zich voorshands aan bij het standpunt van RDW.

*Identificatie en Authenticatie.* IenM heeft behoefte aan het kunnen machtigen van bedrijven door burgers en omgekeerd. Een voorbeeld is het - in het Digitaal Stelsel Omgevingswet - kunnen machtigen door een burger van, bijvoorbeeld, een aannemer om een omgevingsvergunning voor een verbouwing aan te vragen. Machtigen gaat nu nog alleen om de machtiging die burgers elkaar kunnen geven t.b.v. het afnemen van diensten van de overheid. Voor diverse diensten van IenM (onder andere in het kader van de Omgevingswet en de basisregistraties) geldt dat overheidsdiensten (bronhouders), bedrijven en burgers andere organisaties/bedrijven willen kunnen machtigen om namens hen op te treden of informatie aan te leveren aan de overheid. IenM verzoekt BZK om voor de tweede versie van de Uniforme Set van Eisen t.b.v. de Wet GDI prioriteit te geven aan het machtigen van bedrijven.

<sup>1</sup> [http://www.rijksbegroting.nl/2016/voorbereiding/begroting,kst212297\\_10.html](http://www.rijksbegroting.nl/2016/voorbereiding/begroting,kst212297_10.html)

*Berichtenboxen.* IenM heeft behoefte aan het kunnen inzetten van de berichtenboxen voor de communicatie vanuit het Bevoegd Gezag naar burgers en bedrijven. Met name voor de uitvoering van de Omgevingswet. Voorbeelden zijn ontvangstbevestigingen van aanvragen, verzoeken om aanvullingen en de vergunningen. Hiermee wordt ook tegemoet gekomen aan de ambities van Digitale Overheid 2017. Bij voorkeur zijn deze berichtenboxen ook te integreren in voorzieningen zoals het Digitaal Stelsel Omgevingswet (DSO) zodat de gebruiker verzonden berichten vanuit het DSO en ontvangen berichten van het bevoegd gezag in samenhang kan raadplegen.

**Bestuurskern**  
Dir. Ruimtelijke Ontwikkeling  
Afdeling Geo informatie

**Datum**  
3 april 2017

*Digimelding.* Binnen het geo-informatiedomein zijn verschillende voorzieningen in gebruik (zoals het geoknooppunt PDOK, maar ook 'terugmelden op de kaart') die officieel geen GDI-voorzieningen zijn, maar wel op deze wijze functioneren. IenM wil graag in gesprek om de positie van deze voorzieningen in relatie tot de GDI te verkennen.

*Lopende zaken.* IenM vindt het wenselijk dat voorzieningen zoals het Digitale Stelsel Omgevingswet berichten in het onderdeel 'Lopende zaken' van MijnOverheid.nl kunnen plaatsen. Denk aan het bericht dat een aanvraag is verzonden naar het Bevoegd Gezag.

*Kosten.* Door meerdere uitvoeringsorganisaties wordt opgemerkt dat verwacht wordt dat de kosten, zowel voor die organisaties zelf, alsook voor hun afnemers, aanzienlijk zullen stijgen. Daarbij geldt hoe groter het bedrijf des te minder bevoegdheden bij dezelfde persoon zullen liggen. Hierdoor dienen extra kosten te worden gemaakt. IenM vraagt de aandacht voor het tijdig in beeld brengen van de met het wetsontwerp gemoeide kosten

*Uniforme set van eisen.* Van belang is dat verkrijgers van erkende middelen de garantie krijgen dat hun middel tot de vervaldatum erkend en ondersteund zullen blijven. Bij voorgenomen wijzigingen van de uniforme set van eisen dienen uitvoeringsorganisaties in een vroeg stadium te worden betrokken in verband met allerlei impacteisen voor hun organisaties.

*Uitzondering voor organisaties die geen BSN-gegevens gebruiken.* Door het NIWO wordt de vraag gesteld of de wet ook zou moeten gelden voor publieke dienstverleners die geen BSN-gegevens verwerken. Dit dient nader in de wet GDI te worden uitgewerkt.

*Anonieme melder.* Zowel de ILT als de NIWO geven aan dat het in sommige gevallen mogelijk moet zijn dat een anonieme melding moet kunnen worden gedaan, mede gelet op de klokkenluidersregelingen.

*Redelijke termijn van aansluiting nieuw koppelvlak.* Het wetsvoorstel geeft geen termijn voor aansluiting door de ontvangende dienst. Gelet op de beperkte beschikbare capaciteit in Nederland waar alle uitvoeringsorganisaties op zijn aangewezen is het noodzakelijk dat een goede planning wordt gemaakt samen met de betreffende uitvoeringsdiensten. In lagere regelgeving dienen hier garanties voor te worden opgenomen.

*Relatie eIDAS en wet GDI.* In de MvT wordt aandacht gemist voor de relatie tussen eIDAS en wet GDI. IenM gaat ervan uit dat BZK de conformiteit bewaakt tussen beide regels.

*Uitzonderingsbepaling WCAG standaarden (artikel 2).* De standaarden voor visueel beperkten zijn niet in alle gevallen goed toepasbaar voor geo-informatie. Het is noodzakelijk om bij het vaststellen van het functionele en organisatorische toepassingsbereik hiermee rekening te houden en de benodigde expertise vanuit

de geo-informatie hierbij te betrekken. Ten aanzien van de informatiebeveiligingstandaarden zou er via explains in concrete situaties de mogelijkheid moeten bestaan af te wijken van open standaarden, omdat deze in specifieke situaties niet altijd de beste oplossing bieden.

**Bestuurskern**  
Dir. Ruimtelijke Ontwikkeling  
Afdeling Geo Informatie

**Datum**  
3 april 2017

*Ontsluitende dienst.* Bij IenM is een Standaard Platform (SP)<sup>2</sup> ontwikkeld als een generieke voorziening voor de dienstverlening van diensten van het ministerie van Infrastructuur en Milieu. Het SP zal standaard worden ingezet voor hoogwaardige digitale dienstverlening aan overheidsorganisaties, burgers en bedrijven. Component op het Standaard Platform is het Centraal Aansluitpunt als koppelpunt voor berichtenverkeer. Voor het centraal aansluitpunt geldt dat er ook sprake is van authenticatie door aanbieders van diensten en authenticatie van afnemers van gegevens die via het Centraal Aansluitpunt worden ontsloten.

In de tekst van het wetvoorstel GDI wordt er nu vanuit gegaan dat private<sup>3</sup> organisaties de rol van ontsluitende dienst op zich nemen. Verder wordt aangegeven dat de ontsluitende dienst erkend moet worden door de minister van Binnenlandse Zaken, dit op basis van accreditatie.

Op basis van de uitleg over wat een ontsluitende dienst is en doet concludeert IenM dat het SP de functie van een dergelijk dienst vervult.

Ziet BZK het Standaard Platform ook als ontsluitende dienst (dan wel toegangsdienst) in het kader van de Wet GDI? Indien het SP kan worden gezien als ontsluitende dienst in het kader van de Wet GDI verzoeken wij BZK om de tekst van de wet en Memorie van Toelichting aan te passen opdat ook publieke partijen deze rol op zich kunnen nemen. Daarbij stelt IenM ook de vraag of het strikt noodzakelijk is om als ontsluitende dienst ook daadwerkelijk erkend te worden door de minister van BZK.

*Https.* In het AO van 18 januari 2017<sup>4</sup> heeft minister Plasterk aan de TK aangegeven dat alle websites aan de https-standaard moeten voldoen, ook als het gaat om websites die geen persoonsbeveiligde informatie bevatten. Doelstelling is te voorkomen dat sites worden gehackt en info wordt geplaatst die niet waar is. Deze regel wordt via een AMvB vastgesteld op grond van de Wet GDI. Met BZK is IenM van mening dat beveiliging van overheidssites belangrijk is om de digitale informatieverstrekking en het zaken doen tussen burger en bedrijf enerzijds en de overheid anderzijds veilig te kunnen laten plaatsvinden. Daarbij dient wel overwogen te worden of de te nemen maatregelen opwegen tegen het belang dat ermee wordt gediend en of het belang van informatiebeveiliging niet al op een andere wijze adequaat is geborgd. Het via de wet GDI verplicht stellen van een https-verbinding voor alle overheidswebsites is naar de mening van IenM een zwaar middel. De informatieveiligheid kan ook op andere wijze, zoals via het PKI-overheidscertificaat, doeltreffend en efficiënt gegarandeerd zijn. In de bijlagen bij deze brief heeft het Kadaster, op verzoek van IenM, nader aangegeven op welke wijze de informatiebeveiliging nu bij de Landelijke Voorziening Ruimtelijkeplannen.nl is vormgegeven. Het is voor IenM de vraag of uit overwegingen van informatiebeveiliging altijd volgens https-standaard, via de wet GDI, verplicht zou moeten zijn, of dat ook informatiebeveiliging op andere wijze ook volstaat. De vraag is daarbij of het

<sup>2</sup> Het SP is een Cloud gebaseerd platform dat wordt gehost in een overheidsdatacentrum en wordt beheerd door het Programma Alliantie Standaard Platform.

<sup>3</sup> In de Memorie van toelichting staat op pagina 63, verwijzend naar artikel 6 lid 1-3 het volgende: "Het betreft een, in opdracht van een bestuursorgaan of aangewezen organisatie werkende, private partij die zorgt voor de ontsluiting van erkende middelen teneinde de toegang tot elektronische dienstverlening te faciliteren. Hierdoor kan een bestuursorgaan of aangewezen organisatie eenvoudiger aan zijn acceptatieplicht (artikel 5) voldoen."

<sup>4</sup> Tweede Kamer, vergaderjaar 2016–2017, 26 643, nr. 443, blz. 11/12.

verplicht stellen van de https-standaarden via de wet GDI voor dit soort overheidswebsites wel voldoende meerwaarde heeft, aangezien deze hoge kosten met zich brengt, zowel voor de ongeveer 400 bronhouders, als ook voor het beheer van deze landelijke voorziening.

**Bestuurskern**  
Dir. Ruimtelijke Ontwikkeling  
Afdeling Geo informatie

**Datum**  
3 april 2017

*Toezicht.* In artikel 14 is het toezicht op bestuursorganen en aangewezen organisaties op Rijksniveau geregeld. Op grond van deze bepaling kan de betrokken minister toezichthouders aanwijzen voor de naleving van de bij of krachtens deze wet gestelde regels door bestuursorganen op het niveau van de Rijksoverheid (ministeries en zelfstandige bestuursorganen) en door andere aangewezen organisaties. Het gaat hierbij om de in artikel 5 neergelegde verplichting om alle erkende middelen te accepteren bij dienstverlening op het betrouwbaarheidsniveau substantieel of hoog en om de krachtens artikel 8 gestelde regels met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang tot de elektronische dienstverlening.

Conform eerdere ambtelijke afstemming over het wetsontwerp ben ik voornemens om voor de onder mijn ministeriële verantwoordelijkheid opererende Zelfstandige Bestuursorganen het toezicht in te bedden in de plan en verantwoordingscyclus van de ZBO's. Zoals ook voor de huidige toezichtactiviteiten het geval is zal het voortouw voor de verantwoording bij de betreffende ZBO's zelf worden gelegd. Voorts zou het logisch zijn om in het betreffende artikel 14 ook het toezicht op de standaarden (artikel 2) op te nemen.

Tenslotte ziet IenM graag bij artikel 15 de toevoeging dat BZK deze bevoegdheid uitoefent na raadpleging van het betreffende bestuursorgaan en in overeenstemming met de betrokken toezichthoudende Minister.

De minister van Infrastructuur en Milieu,



51



ILT  
Handhavingsbeleid  
Beleidsadvies  
Koningsskade 4  
Den Haag  
Postbus 90653  
2509 LR Den Haag



# memo

Consultatie Wet GDI

Datum  
20 maart 2017

## Aanleiding

De Wet Generieke Digitale Infrastructuur (Wet GDI) bevindt zich momenteel in de fase van internetconsultatie. Alle betrokken partijen hebben hierbij de mogelijkheid om richting BZK aan te geven wat de mogelijkheden, knelpunten en onduidelijkheden in de concept wet zijn en daarmee of de wet in de huidige vorm is na te leven. Vanuit IenM wordt er gewerkt aan een centrale reactie (zal ook worden voorgelegd), de reactie specifiek vanuit ILT staat in deze memo verwoord.

## Gevraagd:

- Wordt ingestemd met de reactie vanuit ILT tbv reactie vanuit IenM? Deze reactie heeft niet de intentie volledig te zijn, mede omdat het niet mogelijk is om alle consequenties op dit moment in kaart te brengen. De Wet GDI is een kaderwet waarbij nadere uitwerkingen in onderliggende regelgeving moet worden vastgelegd.
- Is het gewenst de reactie van ILT naast de centrale IenM reactie ook zelfstandig in te dienen bij BZK?  
Advies: geen losse ILT reactie verzenden op de consultatie. Op het moment dat de ILT punten onvoldoende in de centrale reactie tot uiting komen kan eventueel alsnog een eigen reactie worden verstuurd richting BZK.

## Toelichting

### Verplichting

De Wet GDI treedt per 1 januari 2019 in werking. Het betreft de eerste tranche van de wet en deze richt zich specifiek op digitale dienstverlening door middel van authenticatie en identificatie via BSN. Door de wet ontstaat er een acceptatieplicht voor dienstverleners van erkende authenticatie en identificatie middelen bij digitale dienstverlening. De ILT is verplicht de wet na te leven. De ILT is geen toezichthouder op grond van de Wet GDI. Onder de reikwijdte van de Wet GDI vallen ook organisaties die zaken in mandaat doen, waaronder KIWA. ILT is binnen IenM accounthouder voor KIWA. KIWA is door ILT geattendeerd op de wet GDI.

Onder de Wet DGI, waar ILT geen accounthouder is binnen IenM, vallen waarschijnlijk ook klassenbureau en keuringsinstanties.



#### *Algemene opmerkingen op de Wet GDI*

- De wet GDI is een kaderwet met als doel de mogelijkheid te scheppen in een later stadium bij AMvB keuzes voor voorzieningen tot standaard te verhieven. Hoewel de werkingskracht zich daarmee uitstrekt tot de verhouding tussen overheid enerzijds en bedrijven en burgers anderzijds is het toch primair de overheid die door deze wet gecommiteerd wordt. Een uitgebreidere Impact assessment vanuit ILT is noodzakelijk. Specifiek om de consequenties voor ICT architectuur en processen te bepalen en te (her) prioriteren waar nodig.
- De ILT is, in tegenstelling tot een aantal andere onderdelen van het ministerie van IenM (bijvoorbeeld de RDW), niet zozeer een uitvoerende dienst als wel een toezichthouder. Dat zou kunnen betekenen dat dienstverlening in het geval van de ILT een net iets andere invulling krijgt. Dat laat onverlet dat de ILT zich vanzelfsprekend wel aan de overheidsstandaarden conformeert.
- De Wet GDI stelt op welke wijze een authenticatie en identificatie dienst erkend wordt en binnen welke termijn. Hiermee zijn de rechten en plichten voor de aanbieders duidelijk. Indien een nieuwe erkende aanbieder niet via een bestaand koppelvlak gaat, deze betreffen Idensys, eherkenning of DIGID, moet een ontvangende dienst zoals ILT een nieuw koppelvlak maken voor de aansluiting op haar systeem. De wet geeft hierbij geen termijn voor aansluiting door de ontvangende dienst. Binnen welke redelijke termijn dient dit te gebeuren? Ook al wordt gewerkt met standaarden vraagt het creëren van een nieuw koppelvlak tussen systemen enige tijd en brengt aanvullende eenmalige en structurele kosten met zich mee. Het realiseren van een nieuwe koppelvlak kost (eerste inschatting) rond de 100.000 euro. Hierbij wordt opgemerkt dat ook voor de bestaande providers nog een koppelvlak gemaakt moet worden binnen ILT.
- Vanuit de ILT is het van belang dat het mogelijk blijft om (digitaal) contact te hebben met de overheid zonder verplicht gebruik van authenticatie en identificatie middelen, denk bijvoorbeeld aan anonieme meldingen. Dit vraagt een specifieke duiding in de toelichting dan wel in de wet zelf.
- De verplichting uit de Wet GDI is helder. Voor een goede invulling moet tijdig, voor 1 januari, duidelijk zijn welke erkende diensten via welke koppeling vanaf 2019 gaan gelden.

ILT  
Handreiking/beleed  
Beleidsadvies

Datum  
20 maart 2017

#### *Kan de ILT voldoen aan de wet?*

ILT biedt momenteel al digitale dienstverlening aan, maar maakt hierbij nog geen gebruik van een authenticatie of identificatie dienst. Voor zaken die BSN gerelateerd zijn, zoals energielabels voor burgers moet dit per 2019 zijn ingeregeld. Op dit moment worden aanvragen en meldingen afgehandeld via het insturen van een formulier. Dit formulier staat op de internetpagina van ILT. Aanvragen en meldingen kunnen niet digitaal worden gevolgd door de indiener door in te loggen bij de ILT.

De achterliggende ICT architectuur van ILT moet worden aangepast om te voldoen aan de verplichting die volgt uit de Wet GDI. Door ILT wordt momenteel gewerkt aan één centraal systeem (zogenaamde digitale snelweg) waar de verschillende bestaande systemen op aansluiten. Dit systeem is gebaseerd op de NORA principes van het Rijk. Dit centrale systeem kan op termijn worden



gekoppeld aan de authenticatie en identificatiesystemen. Hiermee is het mogelijk om bijvoorbeeld het melden en indienen van een aanvraag met behulp van authenticatie en identificatie te doen. Hiermee is nog niet direct zo dat een aanvrager de voortgang kan volgen in het digitale dossier. Welke informatie door een aanvrager is in te zien, wordt niet door de kaderwet GDI geregeld en wordt daarmee als vrij in te vullen door ILT gezien.

ILT  
Handhavingsbeleid  
Beleidsadvies

Datum  
29 maart 2017

De architectuur van ILT is in lijn met de Wet GDI rekening indien de nadere uitwerking rekening houdt met de architectuurnormen IMEA en NORA. Of ILT per 1 januari 2019 wordt voldaan aan de Wet GDI hangt voor een deel samen met de prioritering van de projecten binnen ILT. Momenteel is ILT bezig om het ILT IV landschap te vernieuwen.

Sinds eind vorig jaar heeft ILT een tijdelijke voorziening draaien bij de DICTU (TVS), waarbij de verschillende meldprocessen zoals vuurwerkmeldingen gebruik kunnen maken van authenticatie. In geval van vuurwerkmeldingen wordt eHerkenning gebruikt, maar TVS ondersteund ook DiGID en voor buitenlanders de authenticatie op basis van naam wachtwoord herkenning.

#### *Energielabels*

De eerste tranche richt zich specifiek op contacten via BSN met de overheid. Veel klanten van de ILT zijn bedrijven en zullen geen BSN gebruiken, maar bijvoorbeeld voor energielabels heeft ILT te maken met burgers. Voor energielabels bestaat een algemene website beheerd door Milieu Centraal in opdracht van BZK. Het doen van meldingen en aanvragen van een label verloopt niet via ILT. Wel kan ILT worden benaderd met vragen.

*Producten van de ILT onder de Wet GDI, met een globale inschatting van de omvang.*

- Vragen, 50.000
- Meldingen, 550.000
- Bestuurlijke boete rapporten, 21.000
- Bestuurlijke interventies niet zijnde boete, pm. Energielabels hebben wat betreft Last onder Dwangsom voor een tijdelijk sterke toename gezorgd in verband met de 100% toezicht die hier verplicht is.
- Vergunningen/ aanvragen, 17.000
- Klachten, 60
- WOB verzoeken, 500
- Kennisgevingen EVOA, 3000
- Handhavingverzoeken, pm.

#### *Kosten*

##### Eenmalige kosten

Gemiddeld kost een koppeling tussen systemen ICT technisch 100.000 euro. Voor de ILT zijn er in ieder geval drie koppelingen (Idensys, DIGID, eHerkenning), mogelijk vier (buitenland) koppelingen noodzakelijk. Dit brengt een eenmalige kostenpost van 400.000 euro met zich mee. Exacte kosten kunnen pas worden berekend op het moment dat de nadere invulling van de kaderwet GDI bekend is. ILT is zich bewust van de noodzaak van de vernieuwing en maakt op dit moment kosten voor de vernieuwing van het ILT IV landschap. Dit proces draagt bij aan de naleving van de Wet GDI.





### Structurele kosten

N naast eenmalige kosten zijn er ook structurele kosten. Deze kosten hangen voor een groot deel af van de kosten die de erkende diensten in rekening gaan brengen per transactie. Geen inschatting mogelijk op dit moment, het tarief wordt nog nader uitgewerkt onder artikel 21 Wet GDI.

ILT  
Handhavingsoebelod  
Beleidsadvies

**Datum**  
20 maart 2017

### *Personeel*

Het inhuren of structureel uitbreiden van capaciteit hangt samen met de prioritering van projecten. De taak kan centraal worden uitgevoerd. Naast technische aspecten kan ook gedacht worden aan inzet communicatie over de nieuwe werkwijze binnen ILT richting de klant.

### *Tot slot*

De nieuwe Wet GDI heeft gevolgen voor de procesinrichting binnen de ILT. Er zijn geen bestaande uniforme kaders beschikbaar. Processen en werkinstructies moeten worden opgesteld. Het kwaliteitsmanagementsysteem moet worden aangepast. Het Meld- en Informatiecentrum krijgt in elk geval te maken met deze nieuwe processen en bij het opstarten van een nieuw digitaal proces voor klantcontact ontstaat er mogelijk een tijdelijke toename van vragen per telefoon.

Met vriendelijke groet,



## Bijlage

De wet stelt:

- Bestuursorganen en aangewezen organisaties verlenen uitsluitend toegang tot hun elektronische dienstverlening waarvoor het betrouwbaarheidsniveau substantieel of hoog als bedoeld in Verordening (EU) nr. 910/2014 vereist is, onder de voorwaarde dat gebruik wordt gemaakt van een erkend middel dat door een erkende ontsluitende dienst wordt ontsloten, gebruik makend van, voor zover van toepassing, een erkende machtigingsdienst of erkende attributendienst.
- Bestuursorganen en aangewezen organisaties accepteren bij de toegang tot hun elektronische dienstverlening alle erkende middelen en erkende machtigingsdiensten, mits dat middel en die dienst ten minste van het voor de betreffende dienstverlening vereiste betrouwbaarheidsniveau is.
- Met een erkend middel wordt gelijkgesteld een middel dat behoort tot een door een ander lidstaat van de Europese Unie ingevolge Verordening (EU) nr. 910/2014 bij de Europese Commissie aangemeld stelsel.

ILT  
Handhaving/beleid  
Beleidsadvies

Datum  
20 maart 2017

## Reactie op wetsvoorstel Wet GDI

d.d. 17 maart 2017

Algemene opmerkingen t.a.v. het Wetsvoorstel GDI

- Definitie erkende middelen mist;
- Onderdeel standaarden (artikel 2); Aangegeven wordt dat bij algemene maatregel van bestuur een standaard kan worden aangewezen. Bij deze aanwijzing wordt het functionele en organisatorische toepassingsbereik van de standaard omschreven. Voor wat betreft de aanwijzing voor de standaard WCAG voor toegankelijkheid van websites (als vervanger van Webrichtlijnen 2) willen we opmerken dat er in de tekst van het wetsvoorstel en in de memorie van toelichting op de wet, onderdeel 3.5, nu nog niet wordt genoemd dat er ook uitzonderingsbepalingen worden gegeven t.a.v. de toepassing van de standaard WCAG. Onze vragen: Waarom is in de MvT niet aangegeven dat er uitzonderingsbepalingen mogelijk zijn op deze standaard. Hoe komen de uitzonderingsbepalingen tot stand en in welke regelgeving worden deze opgenomen?
- Ten aanzien van de informatiebeveiligingsstandaarden willen we opmerken dat er wellicht ook de mogelijkheid moet worden opengelaten om af te wijken van de toepassing van een specifieke open standaard, omdat deze in specifieke gevallen wellicht niet de beste oplossing biedt. Is het mogelijk om in de toekomst nog met explains te werken voor de afwijking in toepassing van de standaard? En is BZK voornemens om een register met mogelijke explains op te richten t.b.v. een eenduidige uitleg, wanneer het gerechtvaardigd is af te wijken van het gebruik van een specifieke standaard (in het geval de toepassing valt onder het functionele en organisatorische toepassingsbereik van de open standaard).

Opmerking specifiek op de onderdelen Machtiging en Ontsluitende dienst (dan wel toegangsdienst)

### 1. Machtiging

Machtigen gaat nu nog alleen om de machtiging die burgers elkaar kunnen geven t.b.v. het afnemen van diensten van de overheid. Voor diverse diensten van IenM (i.h.k.v. bijvoorbeeld de Omgevingswet en de basisregistraties) geldt dat overheidsdiensten (bronhouders), bedrijven en burgers andere organisaties/bedrijven willen kunnen machtigen om namens hen op te treden of informatie aan te leveren aan de overheid. IenM verzoekt BZK om voor de tweede versie van de Uniforme Set van Eisen t.b.v. de Wet GDI prioriteit te geven aan het machtigen van bedrijven.

#### Onze Vragen:

- Wanneer is deze tweede versie van de Uniforme Set van Eisen gereed?
- Hoe worden we geïnformeerd over het proces van schrijven van de tweede versie en hoe kunnen we daarbij betrokken worden?

### 2. Ontsluitende dienst (dan wel toegangsdienst)

Bij het ministerie van IenM is een Standaard Platform (SP)<sup>1</sup> ontwikkeld als een generieke voorziening voor de dienstverlening van diensten van het ministerie van Infrastructuur en Milieu. Het SP zal standaard worden ingezet voor hoogwaardige digitale dienstverlening aan overheidsorganisaties, burgers en bedrijven.

Component op het Standaard Platform is het Centraal Aansluitpunt en is een koppelpunt voor berichtenverkeer. Voor het centraal aansluitpunt geldt dat er ook sprake is van authenticatie door aanbieders van diensten en authenticatie van afnemers van gegevens die via het Centraal Aansluitpunt worden ontsloten.

---

<sup>1</sup> Het SP is een Cloud gebaseerd platform dat wordt gehost in een overheidsdatacentrum en wordt beheerd door het Programma Alliantie Standaard Platform.

In de tekst van het wetsvoorstel GDI wordt er nu vanuit gegaan dat private<sup>2</sup> organisaties de rol van ontsluitende dienst op zich nemen. Verder wordt aangegeven dat de ontsluitende dienst erkend moet worden door de minister van Binnenlandse Zaken, dit op basis van accreditatie.

Op basis van de uitleg over wat een ontsluitende dienst is en doet concluderen wij dat het SP de functie van een dergelijk dienst vervult.

Onze vraag: Ziet BZK het Standaard Platform ook als ontsluitende dienst (dan wel toegangsdienst) in het kader van de Wet GDI?

Indien het SP moet worden gezien als ontsluitende dienst in het kader van de Wet GDI verzoeken wij BZK om de tekst van de wet en Memorie van Toelichting aan te passen opdat ook niet private partijen deze rol op zich kunnen nemen. Daarbij stellen we ook de vraag of het strikt noodzakelijk is om als ontsluitende dienst ook daadwerkelijk erkend te worden door de minister van BZK.

---

<sup>2</sup> In de Memorie van toelichting staat op pagina 63, verwijzend naar artikel 6 lid 1-3 het volgende: "Het betreft een, in opdracht van een bestuursorgaan of aangewezen organisatie werkende, private partij die zorgt voor de ontsluiting van erkende middelen teneinde de toegang tot elektronische dienstverlening te faciliteren. Hierdoor kan een bestuursorgaan of aangewezen organisatie eenvoudiger aan zijn acceptatieplicht (artikel 5) voldoen."

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties  
Directie Informatiesamenleving en Overheid

[REDACTED]

Tevens per email: [SupportOfficeEid@minbzk.nl](mailto:SupportOfficeEid@minbzk.nl)

[REDACTED]

[REDACTED]

Dank voor uw brief van 23 december 2016 waarin u ons de gelegenheid biedt te reageren op de concept tekst van de Wet generieke digitale infrastructuur (hierna: Wet GDI). De concept tekst hebben we bestudeerd en bij een aantal wetsartikelen hebben we suggesties en/of vragen die hierna worden benoemd. Tevens gaan we in op de vragen die zijn gesteld in het format Uitvoerbaarheid- en handhaafbaarheidstoets Wet GDI. Onze reactie op de vragen is in de bijlage verwerkt.

#### *Opmerkingen wetsartikelen*

##### Artikel 2 Standaarden

In het tweede lid van artikel 2 staat dat bij Algemene maatregel van bestuur een standaard (dwingend) kan worden aangewezen. In de toelichting staat dat bij het gebruik van deze bevoegdheid een zorgvuldig en transparant proces wordt doorlopen en wordt verwezen naar de reeds ingerichte en beproefde procedure voor plaatsing op de 'pas-toe-of-leg-uit' lijst. Het Kadaster zou ervoor willen pleiten dat de genoemde, reeds ingerichte, procedure meer waarborgen gaat bieden zodat het proces van vaststellen van een standaard volledig transparant gaat plaatsvinden waarbij ook voor de bestuursorganen die het aangaan voldoende inspraakmogelijkheden zijn ingebouwd alvorens een advies aan de minister wordt gegeven. In het bijzonder wil het Kadaster aandacht vragen voor standaarden in relatie tot geo-informatie aangezien huidige standaarden op de 'pas-toe-of-leg-uit' lijst niet altijd toepasbaar zijn op geo-informatie. Het is noodzakelijk om bij het vaststellen van het functionele en organisatorische toepassingsbereik hiermee rekening te houden en de benodigde expertise vanuit de geo-informatie sector te betrekken.

##### Artikel 5 Acceptatieplicht

In het vijfde lid van artikel 5 staat dat bestuursorganen met inachtneming van bij ministeriele regeling te stellen regels dienen te bepalen voor welke elektronische diensten tenminste het betrouwbaarheidsniveau substantieel of hoog heeft te gelden. Aangezien de regels die hierover gesteld gaan worden nog niet bekend zijn, is het voor het Kadaster lastig inschatten wat de impact hiervan zal zijn cq welke dienstverlening van het Kadaster straks ook onder de werking van de Wet GDI gaat vallen. Daarnaast is niet duidelijk in de concepttekst, noch in de toelichting in hoeverre een bestuursorgaan of aangewezen organisatie nog de vrijheid heeft om af te wijken van de te stellen regels. Volgens het Kadaster dient duidelijk(er) te worden toegelicht hoe dwingend de te stellen regels zullen gaan gelden, dan wel in hoeverre bestuursorganen en aangewezen organisaties keuzevrijheid behouden.

##### Artikel 6 Erkenning

In het derde lid van artikel 6 staat dat er ontsluitende diensten zullen worden erkend. Het is voorsnog niet de verwachting dat de ontsluitende diensten *ieder erkend* middel van iedere erkende

authenticatiedienst zullen ontsluiten. Dit betekent dat het Kadaster met meer dan één ontsluitende dienst zal moeten contracteren cq in technische zin met meer dan een koppelvlak rekening zal moeten houden, hetgeen hogere kosten met zich mee zal brengen. Het Kadaster zou graag ervoor willen pleiten dat in de komende tijd door BZK de nodige stimuleringsmaatregelen worden getroffen zodat op het moment van inwerkingtreding van de Wet GDI er door de minister erkende ontsluitende diensten zijn die ieder voor zich alle erkende middelen van iedere erkende authenticatiedienst ontsluiten.

#### Artikel 15 en 16 Meldplicht en informatieverstrekking

Het tweede lid van artikel 15 introduceert een meldplicht voor inbreuken op de beveiliging of de integriteit van een elektronische dienst of van misbruik of oneigenlijk gebruik van de toegang tot de elektronische dienstverlening. In de toelichting wordt aangegeven dat deze (nieuwe) meldplicht moet worden onderscheiden van de meldplicht inzake art. 34a Wet bescherming persoonsgegevens, maar ook van de meldplicht inzake art. 18.15a van de Telecommunicatiewet en de meldplicht op grond van de (komende) Wet gegevensverwerking en meldplicht cybersecurity. Het Kadaster pleit ervoor dat de diverse meldplichten zoveel als mogelijk worden geharmoniseerd, althans dat, waar mogelijk, de verschillende meldprocedures/protocollen op elkaar worden afgestemd, aangezien bestuursorganen al snel met twee of meer van de genoemde meldplichten te maken zullen of kunnen krijgen.

Daarnaast volgt uit de toelichting van het tweede lid van artikel 15, niet duidelijk *welke informatie* door bestuursorganen en aangewezen organisaties moeten worden verstrekt aan de minister ingeval sprake is van een inbreuk op de beveiliging of de integriteit van zijn elektronische dienstverlening of van misbruik of oneigenlijk gebruik van de toegang tot elektronische dienstverlening. De toelichting spreekt over 'alle benodigde' informatie. Kan dit per situatie verschillend zijn of zou op dit punt niet nog uitvoeringsregels moeten worden opgesteld over welke informatie dan verstrekt moet worden? Een verduidelijking op dit punt is wenselijk. Dit geldt in zekere zin ook voor artikel 16, eerste lid waarin bestuursorganen en aangewezen organisaties ook een verplichting opgelegd krijgen om desgevraagd 'de gegevens en inlichtingen' te verstrekken aan de minister die nodig zijn om compromittering van de veilige en betrouwbare toegang tot elektronische dienstverlening te voorkomen of te beëindigen. Ook bij deze verplichting rijst de vraag om welke gegevens en inlichtingen het gaat/kan gaan, of dit per situatie verschillend kan zijn en of ook voor deze informatieplicht niet nog nadere uitvoeringsregels zouden moeten worden opgesteld.

Mochten er nog vragen zijn naar aanleiding van bovenstaande toelichting of de reactie op de Uitvoerbaarheid- en handhaafbaarheidstoets, dan vernemen we dat uiteraard graag.

Met vriendelijke groet,

Raad van Bestuur  
Namens deze,

[ ]

## Bijlage vragen Uitvoerbaarheid en Handhaafbaarheid

### Dienst voor het Kadaster en de openbare registers

#### 1. Uitvoerbaarheid

a. Wat is uw voornemen met de Wet GDI? Welke organisatie wordt hiervoor verantwoordelijk gesteld? (naam)

Kan het eruit zien dat uw documenten voldoende uitvoeringsvormules de Wet GDI aan voldoen (a bestuursorganen)?

Geef aan welke andere (aansluitende) wetgeving zal de uitvoering van de Wet GDI kunnen vallen (zie art. 3 lid 2 Wet GDI).

ib. Is het de organisatie(s) helder wat de opgedragen taak is?

Ja, in hoofdzaak: het accepteren van alle erkende middelen.

- Geef daarbij ook aan of er taken of verplichtingen zijn die voor een correcte uitvoering c.q. naleving verduidelijking behoeven.

Zie opmerkingen hiervoor inzake de gewenste verduidelijking van een aantal artikelen van de wet.

c. Zijn/ is de uitvoerende organisatie(s) voldoende toegerust voor een doeltreffende uitvoering?

Ja, er van uitgaande dat de regels die in lagere regelgeving zullen worden vastgelegd aansluiten bij de huidige processen cq gangbare standaarden/protocollen. Zie bijv. ihkv art. 8, eerste lid mbt aanvullende regels over beveiliging. Het beveiligingsbeleid van het Kadaster is gebaseerd op de Baseline Informatiebeveiliging Rijk (BIR) en als in de lagere regels hierop wordt aangesloten dan zal het Kadaster voldoende toegerust zijn om hieraan doeltreffend uitvoering te geven. Dit geldt bijv. ook voor de regels mbt de onafhankelijke audit (dit gebeurt nu voor de DigiD aansluiting door een onafhankelijke EDP auditor).

- Geef aan of er voldoende capaciteit is, of dat de uitvoering verschuiving van prioriteiten of andere maatregelen vergt.

Dit is een aandachtspunt voor het Kadaster. Implementatie van de Wet GDI zal het nodige vragen.

- Geef aan of uw organisatie op het gebied van de ICT voldoende is toegerust. Geef ook aan of voldoende helder is wat de uitvoering van de automatisering vraagt.

Projecten zijn in wording om al deels gerealiseerd te worden. Nb: Webrichtlijnen worden hierin meegenomen. Zorgpunt hierbij is wel of straks sprake zal/kan zijn van één koppelvlak.

- Geef aan in hoeverre de voor de uitvoering benodigde werkprocessen voorhanden zijn.

d. Wat zijn de verwachte effecten van de ontwerpwet voor uw organisatie of departement?

- Geef aan wat de effecten van de ontwerpwet zijn op de digitale dienstverlening aan de burger en ondernemer.

De Wet GDI zal nagenoeg alle digitale dienstverlening van het Kadaster ri. burgers en bedrijven (kunnen) raken.

- Geef aan welke producten of processen door de Wet GDI geraakt worden en wat de voordelen en nadelen van de ontwerpwet zijn.

- Het portaal Mijn Kadaster (toegang tot diverse digitale producten en diensten van het Kadaster) werkt nu nog met een username en password en zal mede naar aanleiding van de onderhavige wet worden aangepast.

- Wanneer PKI-overheid certificaten de status van erkend middel krijgen dan zouden de Landelijke Voorziening (hierna: LV) Ruimtelijke plannen en de LV WVKPB daar door geraakt kunnen worden. **Tevens zullen deze diensten (ingrijpend) geraakt worden indien het gebruik van HTTPS verplicht wordt gesteld.**

- Voor digitale inzage op de Basisregistratie kadaster cq afname diverse producten uit de Basisregistratie kadaster; en tevens van toepassing op digitale indiening klachten en bezwaren en de scheepsboekhouding.

- Aanleveren gegevens Basisregistratie grootschalige topografie door bronhouders zal geraakt gaan worden. Wanneer PKI-overheid certificaten de status van erkend middel krijgen dan zou de distributie van beeldmateriaal onder de werking van de wet GDI kunnen vallen;

- Voor het berichtenverkeer met bronhouders in het kader van de Basisregistratie adressen en gebouwen (BAG) en de Basisregistratie WOZ, voor bevragingen door afnemers van BAG en WOZ en afname van producten BAG, worden PKI-overheid certificaten gebruikt en zouden mogelijk onder de Wet GDI kunnen vallen;

- Aanmelden voor de KLIC-dienstverlening zal onder de werking van de wet GDI komen te vallen (voor ca. 95% van de professionele gebruikers in Nederland). Voor ca. 5% van de incidentele gebruikers zal de e-IDAS Verordening van toepassing zijn.

- Geef aan of er ook mogelijke neven- en onvoorziene of onbedoelde effecten zijn.

#### e. Wat zijn de gevolgen van de acceptatieplicht van de erkende middelen?

- Geef aan wat de gevolgen van de acceptatieplicht zijn, mede in relatie tot interoperabiliteit, tarifiering, de uitfasering van DigiD-laag/basis en de ambitie om bestuursorganen en aangewezen organisaties zo eenvoudig mogelijk aan te kunnen laten sluiten op de diverse erkende authenticatiemiddelen.

Het gebruik van de erkende middelen cq deze toepassen op de digitale dienstverlening kan in sommige gevallen drempelverhogend werken. Dit zal op termijn wel overgaan omdat e.e.a. gewenning wordt, maar het zou in beginsel belemmerend kunnen werken om met zwaardere inlogmiddelen te moeten werken (waar nu bijv. password en username al voldoende is).

#### f. Wat zijn de ingeschatte kosten die nodig zijn voor uitvoering van de wet voor uw organisaties of departement?

Dit zijn IT kosten (grote schatting: >1 miljoen euro).

- Geef aan om welke type kosten (directe/indirecte kosten?) het gaat en of het eenmalige of structurele kosten zijn.

Dit betreffen eenmalige kosten die zien op met name systeemtoegangswijzigingen.

- Geef aan waarop de inschatting is gebaseerd en of de kosten als proportioneel kunnen worden beschouwd.

**Opmerking [101]:** Moet dit nog elders in onze reactie worden aangesipt of is dit op deze plek voldoende?



## 2. Handhaafbaarheid

a. Vraag voor departementen: "Welke organisaties of organisatieonderdelen zullen nodig zijn om aan te zien tot een correcte uitvoering van de wet?"

Geef voor uw departement aan welke organisatie of organisatieonderdeel hiervoor verantwoordelijk is op de naleving van de Wet SDI (inb) de art. 5 en 18).

b. Wat is het oordeel van de toezichthoudende organisaties (of organisatieonderdelen) over de uitvoerbaarheid en handhaafbaarheid?

- Geef daarbij ook aan of er taken of verplichtingen zijn die voor een correcte uitvoering c.q. naleving verduidelijking behoeven.

Zie hiervoor de opmerkingen inzake art. 15 van de concept wettekst.

- Geef aan of de toezichthoudende organisatie of organisatieonderdeel over voldoende kennis en/of capaciteit beschikt.



Ministerie van Binnenlandse Zaken en Koninkrijksrelaties



Uw kenmerk  
2016-0000798041

Datum  
22 maart 2017

Onderwerp: Consultatie Wet generieke digitale infrastructuur (WGD1)



Per brief van 23 december 2016 verzocht de minister van Binnenlandse Zaken en Koninkrijksrelaties het CBR om te reageren op het meegezonden wetsvoorstel voor de Wet generieke digitale infrastructuur. Conform dit verzoek is het wetsvoorstel bezien op werkbaarheid en uitvoerbaarheid.

Voor het weergeven van onze reactie maken wij hieronder gebruik van het daarvoor beschikbaar gestelde format.

**1. Uitvoerbaarheid**

a. Vraag voor departementen: Welke organisaties op uw beleidsdomeinen dienen de wet na te leven?

- Geef aan welke onder uw departement ressorterende uitvoeringsorganisaties de Wet GDI gaan uitvoeren (a-bestuursorganen).
- Geef aan welke andere (categorieën van) organisaties onder de reikwijdte van de Wet GDI moeten vallen (zie art. 3 lid 2 Wgdi).

Niet van toepassing voor het CBR

b. Is het de organisatie(s) helder wat de opgedragen taak is?

- Geef daarbij ook aan of er taken of verplichtingen zijn die voor een correcte uitvoering c.q. naleving verduidelijking behoeven.

Specifiek voor het onderwerp open standaarden is eerder al verduidelijking gevraagd voor een eenduidige overzichtelijke lijst van welke elementen wanneer verplicht zijn, zodat hier in de interne portfolio planning rekening mee kan worden gehouden. Helderheid is ook gevraagd voor de verwachte tranches, zodat hier in de planning rekening mee gehouden kan worden.

De verplichte aansluiting tot elektronische dienstverlening is duidelijk. Wat hiervoor het beste implementatie traject is (planning, keuze broker, kosten etc) is op dit moment met de huidige informatie niet goed in beeld te brengen.



Het ontbreken van concrete invulling in de lagere regelgeving maakt het ingewikkeld om met zekerheid aan te kunnen geven dat het CBR kan voldoen aan alle taken en verplichtingen die verwacht worden voor een correcte uitvoering.

c. Zijn/ is de uitvoerende organisatie(s) voldoende toegerust voor een doeltreffende uitvoering?

- Geef aan of er voldoende capaciteit is, of dat de uitvoering verschuiving van prioriteiten of andere maatregelen vergt.
- Geef aan of uw organisatie op het gebied van de ICT voldoende is toegerust. Geef ook aan of voldoende helder is wat de uitvoering van de automatisering vraagt.
- Geef aan in hoeverre de voor de uitvoering benodigde werkprocessen voorhanden zijn.

Voor het CBR geldt dat er een verschuiving in prioriteiten moet worden aangebracht in het huidige portfolio dat vol is met bedrijfskritische en wettelijke opgaves. Een overgangperiode van 1 jaar is nodig om adequaat invulling te kunnen geven aan de wet. Op dit moment is er nog veel onduidelijk over de termijnen en de toekomstige verplichte standaarden wat met zich meebrengt dat e.e.a. lastig is in te plannen en door te voeren in alle systemen.

Door het verplicht stellen van enkele standaarden zal er binnen het CBR een toetsing plaats vinden om deze elementen onderdeel te maken van de architectuur principes; de huidige Webrichtlijnen zullen hierop moeten worden aangepast. Capaciteit voor de implementatie is onvoldoende i.v.m. de huidige portfolio en programma's.

Met het voorstel is nog niet duidelijk welke technische koppelvlakken worden geraakt en wat hiervoor moet worden aangepast in onze huidige systemen.

d. Wat zijn de verwachten effecten van de ontwerpwet voor uw organisatie of departement?

- Geef aan wat de effecten van de ontwerpwet zijn op de digitale dienstverlening aan de burger en ondernemer.
- Geef aan welke producten of processen door de Wet GDI geraakt worden en wat de voordelen en nadelen van de ontwerpwet zijn.
- Geef aan of er ook mogelijke neven- en onvoorziene of onbedoelde effecten zijn.

Onderscheid kunnen maken naar een hoger inscriptie niveau geeft voordelen voor de producten en diensten die nu niet via DigiD basis aangeboden kunnen worden. De digitale dienstverlening van het CBR kan hiermee uitgebreid worden. De erkenning van authenticatie Hoog en Substantieel geeft bijvoorbeeld de mogelijkheid om medische producten digitaal aan te bieden aan de burger. Voor het maken van een afspraak is een verhoogd beveiligingsniveau echter weinig klantvriendelijk.

Meerdere manieren van authenticatie betekent ook dat onze klanten zich op verschillende manieren kunnen identificeren, afhankelijk van de dienstverlening die zij vragen. Wij verwachten een toename aan vragen bij onze klantenservice over welke authenticatiemethode gebruikt moet worden.

Wij missen nog wel de relatie met de verplichtingen van eIDAS en de Wet GDI. De verwachte effecten kunnen een cumulatief effect hebben op onze organisatie voor wat betreft het moeten voldoen aan de verschillende authenticatie eisen.

De uniforme set van eisen bevat eisen waaraan de aanbieders van erkende elektronische authenticatiemiddelen moeten voldoen. Het CBR zal via de aanbieder indirect met deze eisen te



maken hebben. In het bijzonder de inloghistorie genereert een verzameling profilerende gegevens van de gebruiker bij de authenticatie dienst. Met betrekking tot privacyvraagstuk in het kader van de WBP en specifiek het recht om vergeten te worden ofwel vergeetrecht is een recht voor burgers van de Europese Unie om bepaalde verouderde of onjuiste privacygevoelige informatie te laten verwijderen van internet data bij de bron. Onduidelijk is hoe om te gaan met inloghistorie van onze klanten als ook hun data bij een andere partij worden opgeslagen.

e. Wat zijn de gevolgen van de acceptatieplicht van de erkende middelen?

*- Geef aan wat de gevolgen van de acceptatieplicht zijn, mede in relatie tot interoperabiliteit, tarifiering, de uitfasering van DigiD-laag/basis en de ambitie om bestuursorganen en aangewezen organisaties zo eenvoudig mogelijk aan te kunnen laten sluiten op de diverse erkende authenticatiemiddelen.*

Het gevolg van de acceptatieplicht van de erkende middelen heeft als gevolg dat het CBR moet aansluiten op een authenticatie makelaar. Op dit moment wordt gebruikt gemaakt van DigiD, dit zal met het gebruik van een authenticatiemakelaar worden afgebouwd en uit gefaseerd. Voor het CBR betekent dit dat de koppeling zal moeten worden omgebouwd.

In het huidige wetsontwerp is aangegeven dat ontsluitende diensten niet de verplichting krijgen tot het ontsluiten van alle erkende middelen. Voor de dienstverlener bestaat echter wel de acceptatieplicht voor alle erkende middelen. Dit betekent dus een onwenselijke situatie wanneer onze organisatie met meerdere contractpartijen te maken gaat krijgen. Op dit moment is niet inzichtelijk welke partijen welke middelen aanbieden en voor welke prijs. Een goede analyse om tot een keuze te komen is nu niet te maken.

Tevens is door gebrek aan capaciteit, ervaring en kennis op dit vlak het moeilijk om te beoordelen wat de huidige kwaliteit van een makelaar is en dit wordt nog bemoeilijkt als meerdere makelaars zich op de markt aanbieden.

f. Wat zijn de ingeschatte kosten die nodig zijn voor uitvoering van de wet voor uw organisaties of departement?

*- Geef aan om welke type kosten (directe/indirecte kosten?) het gaat en of het eenmalige of structurele kosten zijn.  
- Geef aan waarop de inschatting is gebaseerd en of de kosten als proportioneel kunnen worden beschouwd.*

De kosten van aansluiting op de verplichte elementen vanuit de wet GDI zijn sterk afhankelijk van het tijdstip van implementatie van de aansluiting op de voorziening. Dat geldt met name voor de aansluiting op de authenticatie makelaar aangezien er op dit moment gebruikt wordt gemaakt van DigiD.

Omdat de overheid een level-playing field tussen de erkende authenticatiemiddelen wil en een acceptatieplicht instelt, is de onderhandelingsvrijheid voor het maken van prijsafspraken met dienstverleners beperkt. Op dit moment is het niet inzichtelijk wat het beprijzingsmodel zal zijn waardoor een realistische kosten inschatting niet te maken valt.

Kosten van de instandhouding van de generieke voorziening, het BSN-K, en van de publiekrechtelijke verankerde stelsel van toezicht op erkende partijen worden door het Rijk gedragen, maar kunnen door het Rijk doorberekend worden. Uit het voorstel is niet inzichtelijk welke kosten in welke mate worden doorbelast, en welke gevolgen dat voor de tarieven van het CBR – en derhalve ook voor de klanten van het CBR- zal hebben.



Ik vertrouw u hiermee voldoende te hebben geïnformeerd.

Met vriendelijke groet,



## Reactie NIWO op Internetconsultatie Wet GDI: Digitale toegang tot dienstverlening van de overheid

### NIWO (Nationale en Internationale Wegvervoer Organisatie)

De NIWO is sinds jaar en dag de vergunningverlener voor het wegtransport. Op grond van de Wet wegvervoer goederen verleent de NIWO Eurovergunningen aan de ruim 13.000 transportondernemingen die zich in Nederland bezig houden met het goederenvervoer over de weg. Ook verstrekt de NIWO bestuurdersattesten voor niet EU-chauffeurs, ritmachtigingen en CEMT-vergunningen en geeft de NIWO TIR-carnets af. Daarnaast beheert de NIWO de VIHB-lijst van afvalinzamelaars, -vervoerders, -handelaren en -bemiddelaars.

De NIWO is geen (inlog)middelenuitgever. Sinds januari 2017 kunnen aanvragen voor de producten van de NIWO via het digitaal ondernemersloket worden gedaan. Zowel Nederlandse als buitenlandse ondernemingen kunnen producten aanvragen bij de NIWO. De inlog van Nederlandse onderneming geschiedt momenteel via e-herkenning (niveau laag). Buitenlandse onderneming loggen in via een zelf ontworpen inlog.

Met belangstelling hebben wij kennisgenomen van het voorstel om te komen tot de Wet generieke digitale infrastructuur. Wij delen de opvatting dat veiligheid, betrouwbaarheid en bescherming voorop moeten staan wanneer het gaat om de uitwisseling van persoonsgegevens.

Naar aanleiding van de consultatie hebben wij enige vragen en opmerkingen die wij hierbij in overweging willen geven.

### Toepassingsbereik Wet GDI

Uit het toepassingskader van de Wet GDI, artikelen 2 en 3, komt expliciet naar voren dat a-organen onder de werking van de wet vallen. Uit die artikelen komt steeds expliciet naar voren dat het verwerken van BSN-gegevens leidend is voor het bepalen van het toepassingskader van de Wet GDI. Met betrekking tot de acceptatieplicht van minimale betrouwbaarheidsniveaus 'substantieel' en 'hoog' neergelegd in artikel 5 van de Wet GDI, lijkt ook impliciet dat het gaat om het betrouwbaar maken van de verwerking van BSN-gegevens. Ook artikel 9 spreekt van "(...) persoonsgegevens, waaronder het BSN(...)". In artikel 1 Wet GDI, de lijst van definities, is niet opgenomen wat in het kader van de Wet GDI wordt verstaan onder persoonsgegevens en dus of dat minimaal het BSN betreft.

Publieke dienstverleners (hierna: uitvoeringsinstanties) die geen BSN-gegevens verwerken maken geen gebruik van de authenticatiedienst. De Wet GDI is onduidelijk en voorziet ons inziens onvoldoende in een voorgeschreven handelwijze in deze gevallen. Dit dient nader in de Wet GDI te worden uitgewerkt.

Gelet op het voorgaande rijst de vraag in hoeverre de Wet GDI uitvoeringsinstanties die geen BSN-gegevens verwerken beoogt te includeren? Is het mogelijk om een uitzonderingspositie te creëren voor deze uitvoeringsinstanties, zodat zij niet onder de reikwijdte van artikel 3 van de Wet GDI vallen?

### Betrouwbaarheidsniveau

Indien elke uitvoeringsinstantie (toch) onder de Wet GDI komt te vallen of zij nu wel of geen BSN-gegevens verwerkt, doen wij de suggestie dat een uitzonderingspositie wordt gecreëerd voor het gebruik van bijv. e-herkenning op niveau 'laag' (of andere diensten die aansluiten op de verplicht te accepteren koppelvlakken) wanneer de uitvoeringsinstantie geen BSN-gegevens verwerkt.

In de Memorie van Toelichting (MvT, blz. 54) wordt gesteld dat de verwachting is dat het aantal diensten waarbij met een betrouwbaarheidsniveau 'laag' kan worden volstaan zal afnemen. Vanwege dit veronderstelde afnemende gebruik zullen de kosten van instandhouding van een publiek middel op niveau 'laag' niet meer verdedigbaar zijn, aldus de MvT. Het hebben van de hiervoor bepleite uitzonderingspositie zal in de praktijk dan geen betekenis meer hebben.

Daarom is het noodzakelijk in kaart te brengen hoe klein of groot de groep zal zijn die eventueel een uitzonderingspositie zou kunnen krijgen omdat zij geen BSN-gegevens verwerkt.

Indien geen uitzonderingspositie wordt gecreëerd voor het blijven werken met betrouwbaarheidsniveau 'laag' zal dit niveau op den duur worden uitgefaseerd. De impact voor de NIWO om over te stappen naar een hoger niveau van e-herkenning is niet heel groot. De impact voor de gebruiker (de vervoerder) is groter. De aanvraag van e-herkenning wordt ingewikkelder en vooral ook kostbaarder. In de MvT wordt voorbij gegaan aan deze administratieve lasten- en kostenverzwaring.

### Standaarden

Artikel 2 van de Wet GDI ziet op standaarden. Indien op basis van de Wet GDI eenmaal een aanwijzing is gedaan voor het verplicht toepassen van een open standaard is daar niet meer van af te wijken en worden op de open standaardisatie geen uitzonderingen toegelaten. Een aangewezen open standaard kan dus niet op de 'pas toe of leg uit' lijst staan. In de MvT (blz. 56) staat vermeld dat de procedure voor plaatsing op de 'pas toe of leg uit' lijst parallel kan lopen naast die van de aanwijzing. Omdat deze procedures parallel naast elkaar kunnen lopen bestaat het gevaar dat de uitkomst van één van die procedures beïnvloedt kan worden. De wetenschap dat een open standaard in procedure is om aangewezen te worden zou er namelijk toe kunnen leiden dat deze niet meer op de 'pas toe of leg uit' lijst terecht kan komen, zodat de uitkomst van deze laatste procedure (in dit voorbeeld) negatief beïnvloedt wordt.

TLS (beveiligde omgevingen/https-verbindingen) is een vereiste voor websites zodra er data wordt achtergelaten. Is er enkel sprake van raadpleging dan is TLS niet vereist. Voor wat betreft het digitaal ondernemersloket van de NIWO voldoen wij al aan voornoemde TLS-verplichting. Op de algemene website van de NIWO wordt geen data achtergelaten, zodat hiervoor geen TLS verplicht is.

We hebben op onze website echter wel een webformulier voor het doen van een anonieme melding. Soms wenst de anonieme melder een terugkoppeling van de melding. Hij laat hierbij zijn gegevens achter (een woonadres, e-mailadres of telefoonnummer). De NIWO zal het webformulier in een beveiligde omgeving toegankelijk moeten maken. De melder is dan niet meer anoniem. De Wet GDI lijkt voorbij te gaan aan de wenselijkheid van het doen van anonieme meldingen. Dit is in deze tijd met klokkenluidersregelingen niet geheel logisch.

### Nationale en internationale koppelvlakken

Nederland kent en maakt momenteel gebruik van 3 koppelvlakken: IDIN (betaalsystemen/banken maken hier gebruik van), Idensys (e-herkenning) en DIGID. De eIDAS-verordening treedt in werking op 18 september 2018. Op basis van de eIDAS-verordening komt er ook één internationaal uniform koppelvlak. De eIDAS-verordening ziet niet alleen op het BSN-domein, maar op alle 'openbare instanties'. De NIWO is per 18 september 2017 dus verplicht dit eIDAS-koppelvlak te accepteren en te kunnen faciliteren. Voor het zaakstelsel 'Inproces' dat de NIWO gebruikt, wordt momenteel een zelfgebouwde log-in voor buitenlandse accounts gebruikt. Deze zal straks moeten aansluiten op het koppelvlak dat op basis van eIDAS ontwikkeld wordt en het ministerie van Economische Zaken gaat aanbieden (als een soort e-herkenning).

Via de grondslag van artikel 6 van de Wet GDI, en inhoudelijk op basis van de eIDAS-verordening, zal de minister van Binnenlandse Zaken en Koninkrijksrelaties (aanbieders van) inlogmiddelen erkennen. Op basis van de eIDAS-verordening is een (voorlopige) Uniforme Set van Eisen tot stand gekomen. Hieraan toegevoegd zijn enkele eisen i.v.m. de verwerking van BSN-gegevens. Deze set van eisen geeft aan waar alle te erkennen middelen op het niveau 'substantieel' of 'hoog' aan moet voldoen. De inlogmiddelen dienen aan te (kunnen) sluiten op een koppelvlak. Met de komst van de Wet GDI worden uitvoeringsinstanties verplicht om alle koppelvlakken te kunnen faciliteren en accepteren. Zij heeft daarbij nog wel de keuze tussen alle(en) erkende aanbieders van een inlogmiddel te accepteren/contracteren die op één van deze koppelvlakken gebruikt kan worden.

De impact voor de NIWO, een uitvoeringsinstantie met een bestand van 13.000 Nederlandse klanten en bijna 7.000 buitenlandse klanten, om alle nationale en internationale koppelvakken te moeten accepteren is groot. Het is wenselijk om een maximum te bepalen voor het aantal koppelvakken dat er mogen zijn. De Wet GDI voorziet in het huidige ontwerp niet in een maximum aantal koppelvakken. Als aandachtspunt bij het ontwerp van de Wet GDI willen wij de suggestie doen dat via de Uniforme Set van Eisen de aanvullende eis wordt gesteld dat er een maximum komt voor het aantal koppelvakken dat door een uitvoeringsinstantie moet worden geaccepteerd, bijvoorbeeld door de eis te stellen aan de te erkennen inlogmiddelen om compatibel te zijn voor een limitatief aantal in de Uniforme Set van Eisen specifiek benoemde koppelvakken.

## Kosten

Het profijtbeginsel zal ook bij de invoering van de Wet GDI gelden, zodat de kosten voor de acceptatie en het gebruik van de koppelvakken straks worden verdeeld onder uitvoeringsinstanties die er (verplicht) gebruik van maken. Wij willen een duidelijker beeld hebben van de hoogte/bandbreedte van de kosten die wij als uitvoeringsorganisatie zullen hebben voor het naleven van de acceptatieplicht.

Het grootste bezwaar dat wij hebben op dit onderwerp is dat bij het bepalen dat doorberekening (via de betrokken partijen uiteindelijk) aan de uitvoeringsinstanties (de dienstverleners) zal plaatsvinden, geen rekening is gehouden met het feit dat niet alle uitvoeringsinstanties (inlog)middelen uitgeven zodat zij deze kosten dus niet kunnen doorberekenen aan burgers/bedrijven. Wij zouden graag zien dat de Wet GDI hier rekening mee houdt.

Uit de MvT (blz. 44) blijkt dat kosten van toezicht in beginsel niet doorberekend worden aan uitvoeringsinstanties. Vervolgens wordt niet duidelijk gemaakt wat specifiek onder 'de kosten van toezicht' valt. Een voorbeeld is de plicht voor een bestuursorgaan jaarlijks een onafhankelijke audit uit te laten voeren.<sup>1</sup> Voornoemde plicht heeft alles te maken met het toezicht houden op de Wet GDI, toch wordt in de MvT niet vermeld dat de kosten van de onafhankelijke auditor uit de algemene middelen worden voldaan, maar wel dat zij voor rekening komt van de uitvoeringsinstantie. Daarbij stelt de MvT dat de kosten van de audit vergelijkbaar zullen zijn met de kosten voor de huidige jaarlijkse DigiD-assessments. De NIWO heeft nooit te maken gehad met DigiD-assessments, zodat deze kosten voor de NIWO nieuwe bijkomende kosten zijn. Hier lijkt de MvT geen rekening mee te hebben gehouden.

Een en ander klemt te meer nu in de MvT (blz. 46) wordt gesproken over financiële baten voor de uitvoeringsinstanties (de publieke dienstverleners) terwijl volstrekt in het midden wordt gelaten om welke financiële baten het hier gaat.

In de MvT moet veel duidelijker worden aangegeven wat de bestuurslasten zijn en hoe die worden gefinancierd. Daarmee komt ook de administratieve lasterverzwarening beter in beeld. Op dit moment is dit onduidelijk en kan, ook door de wetgever, geen goede belangenafweging worden gemaakt.

<sup>1</sup> Overigens is ook niet duidelijk wie de audits mogen uitvoeren. Zullen dit specifiek aangewezen organisaties zijn?







Ministerie van Binnenlandse Zaken en Koninkrijksrelaties  
t.a.v. dhr. M.N. Prinsen  
Postbus 20011  
2500 EA Den Haag

<b>Uw kenmerk</b> 2016-0000798041	<b>Ons kenmerk</b> DIR2017/1403	<b>Datum</b> 31 maart 2017	<b>Bijlage(n)</b> 1
--------------------------------------	------------------------------------	-------------------------------	------------------------

[Redacted]

**Onderwerp**  
Consultatie Wet generieke digitale infrastructuur (WGDI)

Geachte [Redacted]

Dank u voor het ter consultatie voorleggen van het conceptvoorstel van de Wet generieke digitale infrastructuur (Wet GDI). En bijbehorende Uniforme Set van Eisen versie 1.0. Bijgaand onze bevindingen.

Voor rechtstreekse dienstverlening aan het publiek, waarbij burgers en bedrijven moeten inloggen op rdw.nl, is de wet GDI in grote lijn uitvoerbaar. De RDW staat op het standpunt dat er geen verplichting is de erkende middelen te moeten accepteren voor diensten die uitsluitend binnen gesloten systemen gebruikt worden ten behoeve van erkenningen die de RDW krachtens de Wegen Verkeerswet aan (rechts-)personen verleent. Daarnaast hebben we enkele andere aandachtspunten.

Mocht u naar aanleiding van onze bevindingen inhoudelijke vragen hebben, kunt u contact opnemen [Redacted]

Met vriendelijke groet,

[Redacted signature block]

Postbus 777  
2700 AT Zoetermeer  
Europaweg 225  
2700AR Zoetermeer

[Redacted]



RDW

## Consultatie Wet generieke digitale infrastructuur (WGDI)

### *Reactie van de RDW op het conceptvoorstel WGDI*

Doel en inhoud wetsvoorstel (uit de aanbiedingsbrief van het ministerie van BZK):

“Dit wetsvoorstel geeft invulling aan het kabinetsvoornemen tot een volledig digitaal werkende overheid. Om digitale dienstverlening in het publieke domein te intensiveren, is veilige en betrouwbare toegang daartoe door burgers en bedrijven nodig. Dit zal geschieden via door mij erkende publieke en private authenticatiemiddelen op betrouwbaarheidsniveau substantieel en hoog.”

Opdrachtgever	[REDACTED]
Auteur	[REDACTED]
Versie	1.0
Versiedatum	31-03-2017



## Inhoudsopgave

<b>Managementsamenvatting .....</b>	<b>4</b>
0 Inleiding.....	7
1 Gevolgen voor dienstverlening aan burgers .....	8
1.1 De burger online	8
1.2 De burger aan de balie	8
2 Gevolgen voor dienstverlening aan bedrijven .....	10
2.1 Willekeurig bedrijf	10
2.2 Vaste klanten (ketenpartners)	11
2.3 Vaste klanten met in systemen geïntegreerde RDW-diensten	12
3 Gevolgen voor RDW zelf.....	14
3.1 Wettelijke taken RDW	14
3.2 RDW als leverancier van een authenticatiemiddel voor bedrijven	15
3.3 RDW als leverancier van een authenticatiemiddel voor burgers	15
<b>Bijlagen .....</b>	<b>16</b>
A. Antwoorden per door BZK in de consultatie gestelde vraag	16
B. Artikelsgewijze opmerkingen WGDI	19
C. Opmerkingen per eis uit de USvE 1.0	24
D. Voorbeelden van zakelijke portaaldiensten op <a href="http://rdw.nl">rdw.nl</a>	30



## Managementsamenvatting

De minister van Binnenlandse Zaken en Koninkrijksrelaties heeft op 23 december 2016 het conceptvoorstel van de Wet generieke digitale infrastructuur (Wet GDI) ter consultatie aan de RDW voorgelegd. Onder kenmerk 2016-798041. De RDW juicht het Kabinetsvoornemen toe om burgers en bedrijven, als ze dat willen, volledig digitaal zaken te laten doen met de overheid. De RDW is daar groot voorstander van. Wij steunen dan ook de realisatie van generieke infrastructuur om overheidsdienstverlening uniform en betrouwbaar te ontsluiten.

Voor rechtstreekse, publiekelijke, dienstverlening, waarbij burgers en bedrijven moeten inloggen op rdw.nl is de wet GDI in grote lijn uitvoerbaar. De RDW kan deze dienstverlening ontsluiten voor bij wet GDI te erkennen middelen.

Het wetsvoorstel dat ter consultatie voorligt is een krachtige katalysator voor die brede, uniforme, digitale ontsluiting. Wij zien drie hoofdpunten voor bijstelling:

1. Scope definitie 'elektronische dienstverlening' en invoeringsstrategie:
  - a. De RDW staat op het standpunt dat de onder § 2.2 en 2.3 genoemde zakelijke diensten aan vaste ketenpartners volgens de eIDAS-verordening vallen onder "verlening van diensten die uitsluitend binnen gesloten systemen gebruikt worden tussen een welbepaalde groep deelnemers" en dus geen openbare diensten zijn "die aan het publiek verleend worden" (o.a. overweging 21 uit EU nr 910/2014). De RDW leest het wetsvoorstel GDI, hoewel dat hierin nog niet scherp is afgebakend, in dat licht. Uitgaande van dat standpunt blijft de RDW voor dergelijke sectorale diensten het RDW-eigen middel ondersteunen. Daarbij gebruik makend van mogelijkheden die in de Telecommunicatiewet zijn gegeven om het berichtenverkeer middels certificaten te beveiligen. Bij gebleken toegevoegde waarde, behoefte en realiseerbaarheid wordt aanvullend tevens eHerkenning gefaciliteerd.
  - b. Mocht de wet GDI door de wetgever ook van toepassing worden verklaard op de gesloten zakelijke systemen uit § 2.2 en 2.3, adviseren we met klem voor het exclusief gebruik van erkende middelen bij deze diensten een overgangstermijn van 5 jaar te hanteren. Ketenpartners hebben ons aangegeven dat het ontbreken van zo'n overgangstermijn een ontwrichtende uitwerking zal hebben op hun bedrijfsvoering. Wat ook *direct* de baliedienstverlening aan het publiek raakt (zie § 1.2). En de tijdigheid, juistheid en volledigheid van meldingen van bijvoorbeeld import, aankoop, APK-goedkeuring, export, sloop of verzekering via een stelsel aan RDW-erkenningen. Waardoor er problemen in de bedrijfsvoering zullen ontstaan bij organisaties als Belastingdienst, gemeenten, verzekeraars en politie.
2. Kosten publieke dienstverleners: we zien voornamelijk geen incentive voor lage doorbelastingkosten aan de publieke dienstverleners. Bij stijging van de doorbelastingkosten per authenticatie ten opzichte van bestaande authenticaties, zullen de leges van RDW-diensten die nu al digitaal beschikbaar zijn, mee stijgen. Er zijn jaarlijks tientallen miljoenen authenticaties voor RDW-diensten nodig. Tot welke meerkosten dit leidt hangt af van scope (zie 1) en tarief per authenticatie.
3. Verandering van uniforme set van eisen: eisen die aan de middelen worden gesteld om te worden erkend, kunnen in de loop der tijd veranderen. Personen die middelen aanschaffen verdienen een zekere mate van garantie dat hun middel tot de vervaldatum erkend en ondersteund blijft. De impact van wijziging van de uniforme set van eisen op middelen-



leveranciers en hun klanten dient voorafgaande aan een voorgenomen wijziging inzichtelijk te worden gemaakt door middel van impactanalyses en uitvoeringstoetsen.

De RDW vraagt bevestiging van de toezegging tijdens de voorlichtingsbijeenkomsten voor overheidsdiensten dat bij uitwerking van de wet in AMvB wederom wordt geconsulteerd.

De RDW heeft van buiten naar binnen geredeneerd wat de gevolgen zijn van de wet op RDW-dienstverlening. De gevolgen voor de RDW-eigen bedrijfsvoering hebben we uiteraard ook bekeken, om te bepalen in hoeverre het gevraagde doenbaar is. Maar, centraal staat veilige en betrouwbare online toegang tot RDW-diensten. Hierna een samenvatting van onze bevindingen.

#### Gevolgen voor dienstverlening aan burgers

Voor burgers zien we veel voordelen. Als er middelen beschikbaar komen met een hoger betrouwbaarheidsniveau, gaan we voor baliediensten ook online varianten maken. Bij onze eigen pilot 'online voertuigen overschrijven' merken we dat daar behoefte aan is. Een deel van de burgers heeft moeite met ingewikkelde(re) inlogmethoden. Burgers die minder digivaardig zijn of het niet prettig vinden online hun aanvraag bij de RDW in te moeten dienen, blijven bij de RDW de keus houden om naar een balie te gaan. Echter, onbedoeld kan nu juist die baliefunctie door de wet GDI in gevaar komen, zoals onder punt 1b op de vorige pagina aangegeven. Bestaande dienstverlening die nu achter DigiD zit ook door andere erkende middelen laten ontsluiten lijkt de RDW goed doenbaar.

#### Gevolgen voor zakelijke dienstverlening

##### *Willekeurig bedrijf*

Hier geldt onverkort het onder 'burgers' vermelde verhaal. Complicaties bij bedrijven:

1. Hoe groter het bedrijf, hoe specifiekere de functie en hoe minder voordeel dat je met 1 en hetzelfde middel overal inlogt. Bij veel bedrijven zal een medewerker vanuit zijn functie bij slechts 1 of een enkele overheidsdienst(soort) in mogen loggen. Het voordeel is dus met name voor de eenpitters.
2. Het heeft geen zin een Substantieel middel aan te schaffen als er soms met een Hoog middel moet worden ingelogd. Dan zal men toch al een Hoog middel moeten aanschaffen en voor de eenvoud altijd met Hoog inloggen. Op dit moment leveren alle eHerkenningmiddelenleveranciers, op eentje na, het Hoog-middel echter enkel via smartcard icm cardreader. Tijdens een pilot bij onze klanten kregen we smartcardreaders regelmatig niet werkend: geen (werkende) USB-poort (tablets, geen systeem-rechten, afgesloten poort) of geen ondersteuning (besturingssysteem, webbrowser, driver).

##### *Vaste klanten*

Ruim 30 duizend vaste klanten van de RDW (veelal door de RDW erkend) maken op dit moment gebruik van een door de RDW zelf uitgegeven certificaat. Deze bedrijven en met deze bedrijven de RDW, zijn afhankelijk van ongestoorde en betrouwbare processen. Waar garanties nodig zijn dat de erkende middelen onder bestaande condities en configuraties blijven werken. Het huidige certificaat is bedrijfsgebonden. Een bedrijf bepaalt zelf welke medewerker hij gebruik van het certificaat toe staat. Deze bedrijven zullen veelal nadelen ervaren van de overstap naar erkende middelen:

1. Het huidige middel kost € 19 per jaar. Ongeacht de grootte van het bedrijf.
2. Het nieuwe middel kost tussen de € 36 en € 55 (voor een EH3-middel). Per medewerker. Er zijn klanten die zeggen meer dan 100 gebruikers te hebben.
3. En voorts: machtigingslogistiek eHerkenning, niet inzetbare medewerker als hij zijn middel kwijt of vergeten is, zorg dat middelen met pin/wachtwoord voor de grijp liggen



(denk aan autoshowrooms), lastenverzwaring door extra transactiehandelingen en de niet-inpasbaarheid in de huidige in gebruik zijnde ICT-infrastructuur.

*Vaste klanten  
met in systemen  
geïntegreerde  
RDW-diensten*

Een belangrijk deel van het volume aan RDW-dienstverlening wordt geleverd vanuit systemen van derden waar RDW-functionaliteit in is geïntegreerd. Waaronder dealermanagement-, werkplaats, lease- en verzekeringssystemen. Tussen die systemen en de RDW zitten vaak nog speciale intermediairs die toegevoegde waarde aan hun klanten leveren. Het hele stelsel staat onder in wet- en regelgeving en besluiten gereguleerd toezicht. Onduidelijk is nog welke verandering de wet vereist in deze constellatie. De RDW denkt op dit moment aan het overschakelen naar een andere eIDAS figuur voor de RDW-dienstverlening: het gebruik van geavanceerde zegels op basis van de bestaande RDW-certificaten. De figuur van zegels valt echter onder de Telecommunicatiewet en niet onder de wet GDI.

Gevolgen voor RDW zelf

Hiervoor gaand is al een en ander geraakt. De RDW krijgt te maken met hogere kosten om diensten initieel en structureel te ontsluiten voor erkende middelen. De RDW heeft een eerste dienst, die al via een RDW-eigen authenticatiemiddel online was, nu ook via eHerkenning ontsloten (het schorsen van voertuigen). Dat vergde 1.000 uur. De RDW heeft op rdw.nl meer zakelijke diensten die via eHerkenning ontsloten zouden kunnen worden. De hoop en verwachting is dat het overzetten van volgende diensten sneller verloopt. Niettemin blijft het een majeure operatie die herprioritering vergt.

Indien de wet GDI ook van toepassing wordt verklaard op zogenaamde gesloten systemen uit § 2.2 en 2.3 lopen de uitvoering van wettelijke taken en de zuiverheid van het Kentekenregister gevaar als er geen betere overgangsregeling komt.

Als middelenuitgever van het eID op rijbewijs voor burgers constateren wij een paar punten in de Uniforme Set van Eisen die afwijken van de projectstartarchitectuur van publieke middelen. Waardoor de publieke middelen straks mogelijk niet aan de uniforme set van eisen zullen voldoen. De RDW ziet dit als risico. Bij voorgenomen wijziging van de uniforme set van eisen verzoekt de RDW voorafgaand geconsulteerd te worden inzake de impact op reeds in roulatie zijnde middelen, noodzakelijke aanpassingen en burgers. Voor het overige worden bevindingen via de reguliere projectgovernance met Logius afgestemd. Als authenticatiedienst die DigiD Hoog heeft te laten erkennen. De RDW constateert dat er geen sprake is van een level playing field qua gebruik tussen private en publieke middelen: Private middelen kunnen wel worden gebruikt in het publieke domein, maar publieke middelen niet in het private domein. Daarmee kunnen de publieke middelen bijvoorbeeld niet gebruikt worden in het aanvraag- en/of activatieproces van private middelen (het publieke middel als 'moederkaart'). De toelichting op pagina 132 van de USvE "Het uitgeven van een middel op basis van een bestaand middel mag niet een volledig geautomatiseerd proces zijn." roept vragen op over wat onder 'volledig geautomatiseerd' moet worden begrepen. Er wordt een onlinedienst voorbereid waarmee burgers via internet een nieuw rijbewijs kunnen aanvragen. Op basis van een bestaand middel. De uitreiking blijft op basis van een face-to-face identiteitsvaststelling. Er staan meer aspecten bij deze eis op pagina 132 van de USvE die vragen oproepen (zie p 15 van deze reactie).

Het altijd voor de volle 100% voldoen aan de webrichtlijnen is een goed streven, doch in de praktijk blijkt het noodzakelijk soms hiervan af te moeten wijken. Zo krijgen wij van onze leverancier terug dat er geen videospeler in de markt beschikbaar is die kan voldoen aan de webrichtlijnen. Voor documenten vormt het gebruik van PDF-jes een probleem. De RDW hoopt dat hier enige eigen invullingsruimte blijft op basis van gezond verstand.



## 0 Inleiding

De minister van Binnenlandse Zaken en Koninkrijksrelaties heeft, mede namens de minister van Economische Zaken, op 23 december 2016 ter consultatie het conceptvoorstel van de Wet generieke digitale infrastructuur (Wet GDI) aan ons voorgelegd. Onder kenmerk 2016-798041. Met deze consultatie wil de minister ons enerzijds over het wetsvoorstel informeren en anderzijds de mogelijkheid bieden om op de inhoud te reageren.

### Doel en inhoud wetsvoorstel

Dit wetsvoorstel geeft invulling aan het kabinetsvoornemen tot een volledig digitaal werkende overheid. Om digitale dienstverlening in het publieke domein te intensiveren, is veilige en betrouwbare toegang daartoe door burgers en bedrijven nodig. Dit zal geschieden via door de minister erkende publieke en private authenticatiemiddelen op betrouwbaarheidsniveau substantieel en hoog.

Het wetsvoorstel bevat de volgende onderdelen:

- a. Aanspraak van houders van erkende authenticatiemiddelen op het gebruik daarvan bij de (semi)overheid. Spiegelbeeldig hieraan krijgen bestuursorganen en aangewezen organisaties de plicht om alle erkende middelen te accepteren;
- b. Een toezichtsregime dat uitgaat van vertrouwen en aansluit bij regulier interbestuurlijk toezicht. Op partijen in het authenticatieproces zal sprake zijn van een externe toezichthouder;
- c. Grondslagen voor financiering door bij authenticatie betrokken publieke en private partijen en voor leges;
- d. Overgangsrecht ter zake van het gebruik van DigiD laag/basis en voor partijen die de voorgenomen eisen aan werking, veiligheid en betrouwbaarheid hebben beproefd.
- e. De verplichting om de bij amvb aangewezen standaarden voor elektronisch verkeer met de publieke sector toe te passen.

### Wat is ons gevraagd

Het wetsvoorstel te bezien op werkbaarheid en uitvoerbaarheid, en daarbij de volgende aspecten te betrekken:

- Welke (categorieën van) BSN-gerechtigde organisaties zouden, gelet op de aard van hun dienstverlening, moeten worden aangewezen, opdat ze - evenals bestuursorganen in de zin van art. 1:1, eerste lid, onder a, Awb - binnen de werkingssfeer van het wetsvoorstel komen te vallen?
- De betekenis en gevolgen van de acceptatieplicht, mede in relatie tot interoperabiliteit, tarifiering en de uitfasering van DigiD-laag/basis en de ambitie om bestuursorganen zo eenvoudig mogelijk aan te kunnen laten sluiten op de verschillende erkende authenticatiemiddelen.
- De onderwerpen die in de uitvoeringsregelgeving zullen worden geregeld en de daarbij te betrekken overwegingen.

### Aanpak

Wij hebben een aanpak gehanteerd waarbij we via bijeenkomsten de veranderingen hebben bekeken vanuit de dienstverlening aan onze klanten en onze wettelijke taken. Artikel voor artikel, eis voor eis en vraag voor vraag (zie de 3 bijlagen voor de details). Waarbij we de hoofduitkomsten collegiaal hebben getoetst bij andere bestuursorganen. Via de Manifestgroep en het ministerie van IenM.



# 1 Gevolgen voor dienstverlening aan burgers

## 1.1 De burger online

Voor burgers is het gemakkelijk als ze met een en hetzelfde middel bij alle publieke diensten kunnen inloggen. Zodra er middelen beschikbaar komen met een hoger betrouwbaarheidsniveau, kunnen er voor baliediensten waar de identiteit moet worden vastgesteld, ook online varianten komen.

Om hier ervaring mee op te doen heeft de RDW 1,5 jaar geleden de dienst 'online voertuigen overschrijven' online gezet. Omdat het een proef met DigiD betreft, wordt geen ruchtbaarheid aan deze dienst gegeven. Meer dan 6.000 burgers hebben spontaan aan de proef meegedaan en succesvol een of meer keer een voertuig digitaal via de website van de RDW op hun naam gezet. Sommige burgers die deze dienst wilden gebruiken haakten af omdat ze de inlogmethode niet voor elkaar kregen of te ingewikkeld vonden. Feedback van burgers krijgen we via recensies in de 'RDA Lezer'-app in de Google Playstore. Bij een multimiddelenstrategie kunnen burgers kiezen voor een inlogmethode die het best bij hen past. Bestaande dienstverlening die nu achter DigiD zit ook door andere erkende middelen laten ontsluiten lijkt de RDW goed doenbaar. De kosten zullen afhangen van de mate van uniformiteit die ontsluitende diensten bieden. In koppelvlak, aansluitvoorwaarden en zaken als testinfrastructuur.

RDW Particulier

Inloggen zakelijk Over RDW Pers Contact Information in English Onderhoud en storingen Online loket

Particulier Zakelijk

Auto

Kopen

- Kentekenbewijs op naam zetten
- Tellerstand in bij het kopen van een (bedrijfs)auto
- Voorkom aankoop van een gestolen voertuig
- Zuinig en milieuvriendelijk voertuig kopen
- 1 dag timmeren bij aankoop van een voertuig
- Ongeluk of gekleurd voertuig
- Rijden als u de kentekencard nog niet heeft ontvangen
- Met spoed kenteken aanvragen
- Online voertuig overschrijven

Particulier > Auto > Kopen > Online voertuig overschrijven

### Online voertuig overschrijven

Als u een voertuig heeft gekocht dan moet u als nieuwe eigenaar het kentekenbewijs op uw naam laten zetten (overschrijven). Dit kan ook online. Hiervoor heeft u een identiteitsbewijs nodig en een kaartlezer. Deze kunt u downloaden op uw telefoon (klik voor meer informatie onder het kopje 'Voorwaarden').

**Voertuig overschrijven**

#### Hoe kan ik een voertuig online overschrijven?

- U gaat naar de dienst via de knop 'Voertuig overschrijven'. Daarmee komt u in het DigiD-scherm terecht waar u kunt inloggen.
- Kies voor de optie 'Ik wil inloggen met: alleen gebruikersnaam en wachtwoord'

**DigiD** Inloggen bij RDW

Inloggen met:

- Inloggen met mijn DigiD-identiteitsbewijs
- Inloggen met een ander DigiD-identiteitsbewijs
- Inloggen met een ander DigiD-identiteitsbewijs (voor gebruikers van andere gemeenten)

- Nadat u bent ingelogd bij DigiD wordt een extra controle gevraagd. Hiervoor legt u uw identiteitsbewijs op de kaartlezer. Als uit de controle blijkt dat het identiteitsbewijs ge-dig is en dat het van u is, komt u in de RDW-dienst om

## 1.2 De burger aan de balie

Dit lijkt een vreemde paragraaf in een wet die primair gaat over online dienstverlening. Echter, zoals hierna wordt uitgelegd, brengt de wet de continuïteit van bestaande baliekanalen voor RDW-dienstverlening ernstig in gevaar als de wet ook betrekking heeft op de dienstverlening uit § 2.2 en 2.3 die de RDW beschouwt als onderdeel van gesloten systemen.

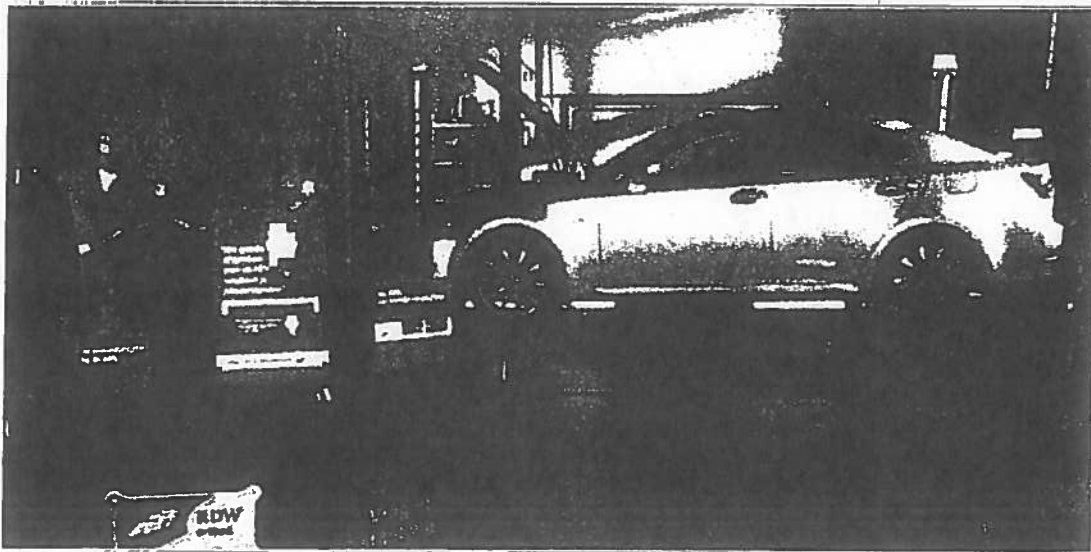
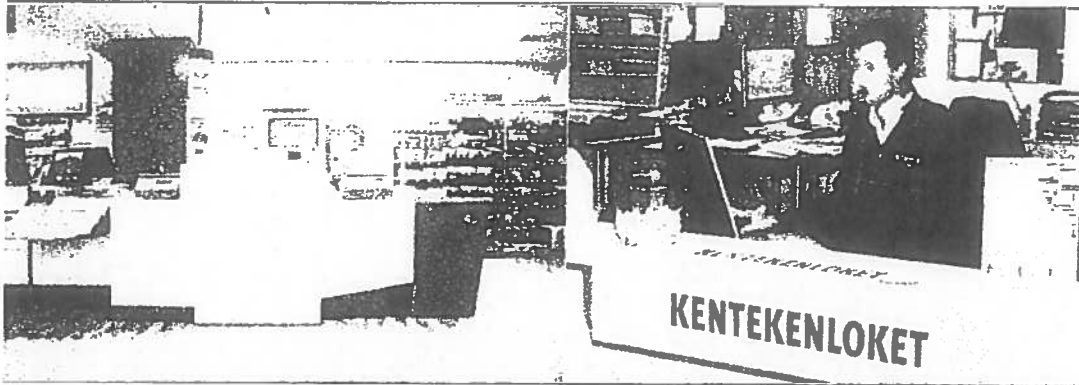
RDW-baliediensten worden vrijwel geheel geleverd door private partijen. Zo kunnen voertuigbezitters hun voertuig tenaamstellen of schorsen bij balies van PostNL (met volledig geïntegreerde balieterminals) of stichting Kentekenloket (een netwerk van hiertoe samenwer-





kende bedrijven uit de voertuigbranche). En gebeurtenissen omtrent hun voertuig doorgeven via ongeveer 33.000 RDW-erkenninghouders. Zoals aan- of verkoop van een voertuig, de APK-goedkeuring, export of sloop.

Als de wet GDI ook op dergelijke gesloten systemen van toepassing wordt verklaard en de voorgenomen veranderingen weten de ketenpartners niet tijdig doorgevoerd te krijgen, kunnen voertuigen bijvoorbeeld niet meer worden overgeschreven, APK-goedgekeurd, geëxporteerd, gesloopt, etc. De handel in voertuigen valt stil. Een ander gevolg kan zijn dat burgers onterecht boetes krijgen wegens verlopen APK's, het onverzekerd rondrijden, etc.





## 2 Gevolgen voor dienstverlening aan bedrijven

### 2.1 Willekeurig bedrijf

Elk bedrijf dat straks een van de publieke online diensten van de RDW wil gebruiken, zal straks te maken krijgen met de gevolgen van de WGDI. Bedrijven die eigenaar/houder zijn van voertuigen gebruiken bijvoorbeeld diensten om een voertuig op naam te zetten, te schorsen of een ontheffing aan te vragen. Voor diensten aan zakelijke eigenaar/houders van voertuigen geldt in grote lijn hetgeen onder het vorige hoofdstuk (burgers) is beschreven. Zowel voor de groep die ad hoc gebruikt maakt van zakelijke RDW-diensten als vaste klanten (zie volgende paragrafen) zal de wet GDI in het algemeen minder voordelen brengen dan voor de burger:

1. Hoe groter het bedrijf, hoe specifiekere de functie en hoe minder voordeel dat met een en hetzelfde middel overal kan worden ingelogd. Bij veel bedrijven zal een medewerker vanuit zijn functie bij slechts een of een enkele overheidsdienst(soort) in mogen loggen. Het voordeel van een middel is dus met name voor de eenpitters.
2. Het heeft geen zin een Substantieel middel aan te schaffen als er soms met een Hoog middel moet worden ingelogd. Dan zal men toch al een Hoog middel moeten aanschaffen en voor de eenvoud altijd met Hoog inloggen. Op dit moment leveren alle eHerkenningmiddelenleveranciers, op eentje na, het Hoog-middel echter enkel via smartcard icm cardreader. Tijdens een pilot bij onze klanten kregen we smartcardreaders regelmatig niet werkend: geen (werkende) USB-poort (tablets, geen systeemrechten, afgesloten poort) of geen ondersteuning (besturingssysteem, webbrowser, driver).

De vaste klanten uit § 2.2 en 2.3 buiten beschouwing latend, is het voor alle overige, reguliere, bedrijven een vooruitgang als ze met een erkend middel straks bij de RDW kunnen inloggen om van de publieke onlinedienstverlening gebruik te maken. Voor bedrijven die geen gebruik willen of kunnen maken van deze mogelijkheid, blijven de bestaande baliekanalen beschikbaar.

The screenshot shows the RDW website interface. At the top, there is a navigation bar with links for 'Inloggen zakelijk', 'Over RDW', 'Pers', 'Contact', 'Information in English', 'Onderhoud en storingen', and 'Onze site'. Below this is the RDW logo and the text 'Zakelijk'. A search bar is visible on the right. The main content area is titled 'Zakelijk - Een voertuig van de zaak schorsen' and 'Voertuig van de zaak schorsen of verlengen met eHerkenning'. The page content includes a list of links on the left, a main text block explaining the process of suspending or extending a vehicle with eHerkenning, and a section titled 'Heeft u een eHerkenningmiddel?' with further instructions. A small inset image shows a close-up of a document titled 'Voertuig van de zaak schorsen of verlengen met eHerkenning'.

## 2.2 Vaste klanten (ketenpartners)

In bijlage D is een overzicht van de zakelijke portaaldiensten opgenomen. Vrijwel alle op dit moment bestaande diensten waarop moet worden ingelogd zijn niet publiekelijk. Ze mogen enkel worden gebruikt door een gesloten groep vaste klanten (ketenpartners). Onder (erkenings-) voorwaarden die grotendeels in wet- en regelgeving zijn vastgelegd.

De RDW staat op het standpunt dat de zakelijke diensten aan deze vaste ketenpartners volgens de eIDAS-verordening vallen onder “verlening van diensten die uitsluitend binnen gesloten systemen gebruikt worden tussen een welbepaalde groep deelnemers” en dus geen openbare diensten zijn “die aan het publiek verleend worden” (o.a. overweging 21 uit EU nr 910/2014). De RDW heeft het wetsvoorstel GDI in dat licht gelezen. Uitgaande van dat standpunt blijft de RDW sectoraal eigen middelen ondersteunen. Om de continuïteit van uitvoering van taken voortkomend uit de WegenVerkeersWet en hiervan afhankelijke overige wetgeving voor dergelijke diensten te garanderen. Bij gebleken toegevoegde waarde, behoefte en realiseerbaarheid wordt aanvullend tevens eHerkenning gefaciliteerd.

Hiermee mitigeert de RDW de volgende risico's:

1. Onzekerheden over wanneer en in welke vorm de Kamer de wet GDI aanneemt. Mocht op enige moment toch nog worden besloten tot uitstel of afstel van (onderdelen van) de wet GDI, garandeert het RDW-middel de continuïteit die overige wetgeving vereist. Betrokkenen kunnen investeringsbeslissingen beter afwegen en bijsturen.
2. Door ketenpartners als onwerkbaar geschetste situaties van eHerkenningssystemen of eHerkenningssystemen binnen bestaande infrastructuur en context. Het RDW-eigen middel garandeert de bedrijfscontinuïteit voor die ketenpartners.
3. Ketenpartners kunnen in tegenstelling tot burgers of ‘reguliere’ zakelijke klanten uit § 2.1 niet uitwijken naar baliekanalen. Want die bestaan niet voor dit type zakelijke diensten.

Mocht de wet GDI door de wetgever (op termijn) ook van toepassing worden verklaard op de gesloten zakelijke systemen, adviseren we met klem voor het exclusief gebruik van erkende middelen bij deze diensten een overgangstermijn van 5 jaar te hanteren. Het ontbreken van zo'n overgangstermijn kan een ontwrichtende uitwerking hebben op de bedrijfsvoering van ketenpartners. Waardoor o.a. baliedienstverlening aan het publiek in gevaar komt. Zie daartoe § 1.2.

Vaste klanten van de RDW maken op dit moment gebruik van een certificaat dat de RDW in eigen beheer aanmaakt en verstrekt. De meeste klanten staan onder direct (via eigen bedrijvencontroleurs en -inspecteurs) of indirect (via goedkeurende accountantsverklaringen) onder toezicht van de RDW.

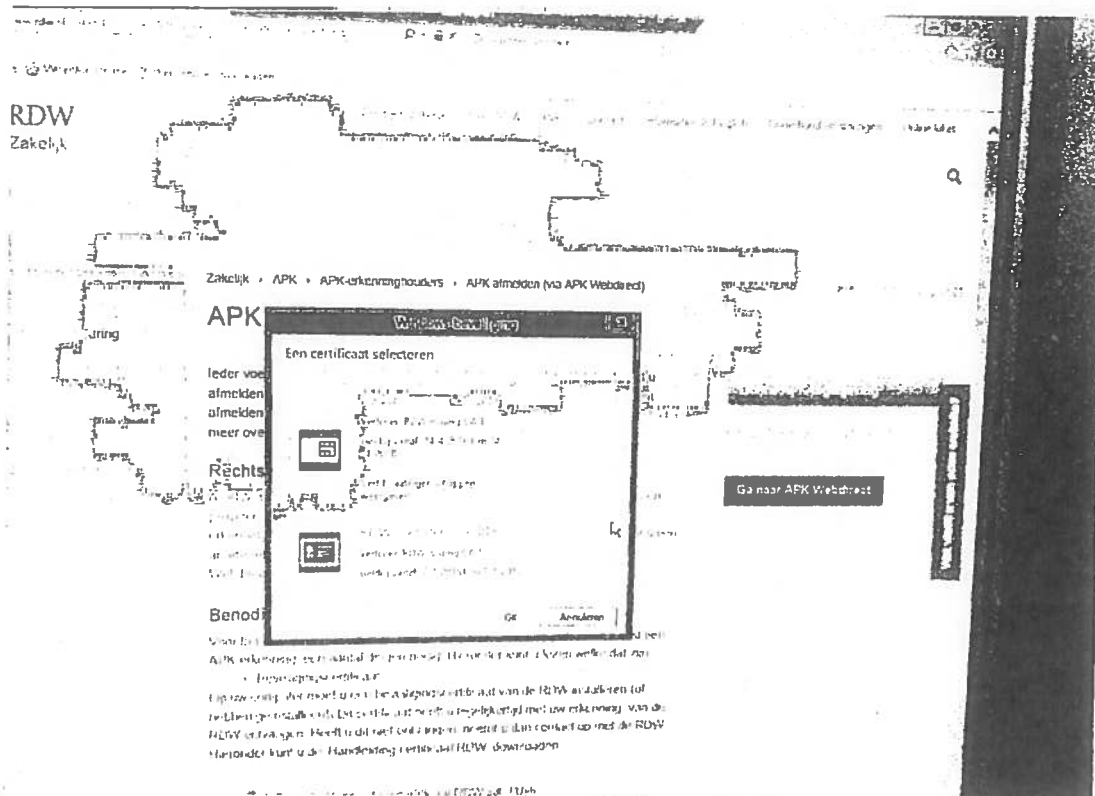
Het RDW-certificaat is bedrijfsgebonden. Een bedrijf bepaalt zelf welke medewerker gebruik van het certificaat wordt toegestaan. Deze bedrijven zullen met name nadelen ervaren van de overstap naar erkende middelen:

1. Het huidige middel kost € 19 per jaar. Ongeacht de grootte van het bedrijf.
2. Het nieuwe middel kost tussen de € 36 en € 55 (niveau EH3). Per medewerker.
3. Bij sommige klanten gaat het om meer dan 100 medewerkers die een middel zouden moeten gaan aanschaffen voor RDW-dienstverlening. Bij enkele (zoals PostNL) om meer dan 1.000 medewerkers.

Daarnaast kent de RDW ook vaste zakelijke klanten van buiten de EU. Denk aan voertuigfabrikanten uit bijvoorbeeld Azië of VS die m.b.v. een RDW-certificaat digitaal de voertuiggegevens

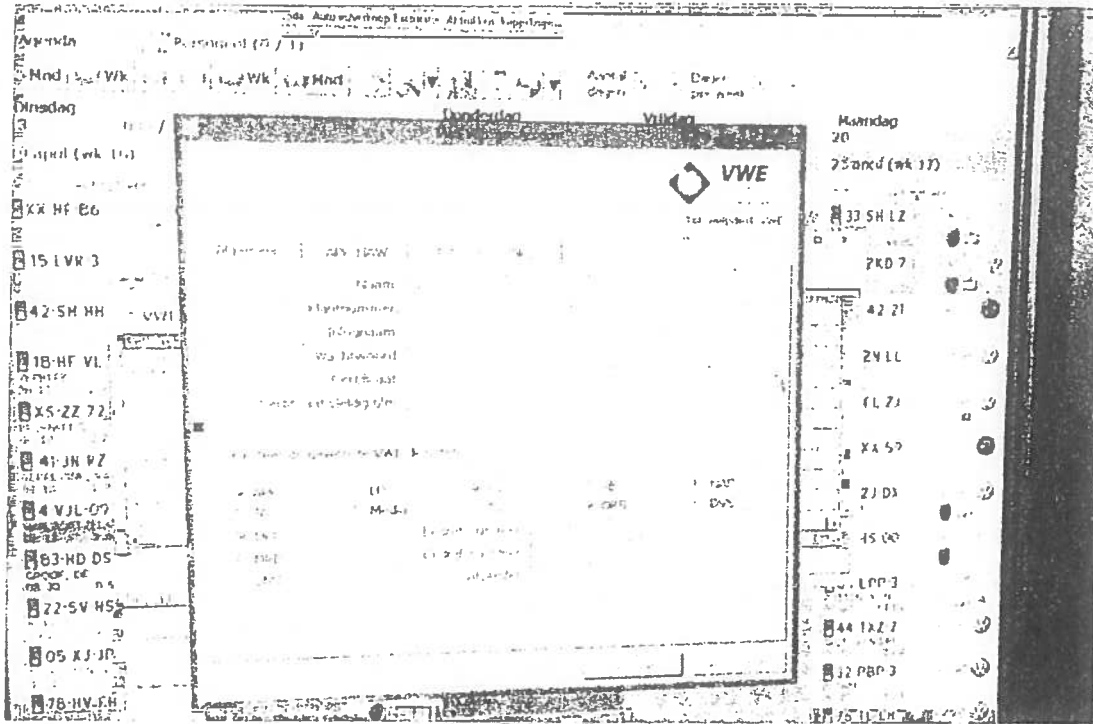
aanleveren. Die kunnen niet aan een eHerkenningmiddel, noch aan een eIDAS-middel komen als ze geen vestiging in Europa hebben.

De logistiek om via eHerkenning machtigingen te registreren zal, met name bij grotere bedrijven, tot extra overhead en kosten leiden. Daarnaast hebben onze vaste klanten aangegeven productiviteitsverlies te voorzien wegens medewerkers die hun middel kwijt of vergeten zijn en lastenverzwaring door extra inloghandelingen. Tot slot hebben branchevertegenwoordigers aangegeven dat de extra betrouwbaarheid die wordt beoogd relatief is omdat de kans groot is dat medewerkers hun EH4-smartcard in de reader laten zitten (mede vanwege het voorgaande) met pin/wachtwoord onder handbereik. Met name daar waar ook veel vreemden over de vloer komen, zoals in autoshowrooms, zitten daar keerzijden aan ten opzichte van de huidige situatie, waar het RDW-certificaat in de PC zit.



### 2.3 Vaste klanten met in systemen geïntegreerde RDW-diensten

Een belangrijk deel van het volume aan RDW-dienstverlening wordt geleverd vanuit systemen van derden waar RDW-functionaliteit in is geïntegreerd. Waaronder dealermanagement-, werkplaats, lease- en verzekeringssystemen. Tussen die systemen en de RDW zitten vaak ook nog intermediairs (providers genoemd) die toegevoegde waarde leveren. Hier geldt hetzelfde als onder § 2.2 beschreven dat de RDW op het standpunt staat dat dit type sectorale dienstverlening deel uitmaakt van een gesloten systeem voor een welbepaalde groep deelnemers. Niet voor een breder publiek en dus buiten de scope van de wet GDI vallend wat betreft het verplicht gebruik van uitsluitend erkende middelen.



De RDW denkt op dit moment aan het overschakelen naar zegels, door de hele keten heen. Zegels zijn een andere figuur uit de eIDAS verordening, in nationale wetgeving vallend onder de Telecommunicatiewet. Eenvoudig gezegd:

- Een authenticatiemiddel kan worden gebruikt om te bepalen of je iemand toegang verleent tot een (eigen) systeem.
- Een digitale handtekening of zegel kan worden gebruikt om vast te stellen van wie een bericht afkomstig is. En of het bericht authentiek is.

De gedachte is deze zegels aan te laten brengen op basis van de bestaande RDW-certificaten. RDW gaat met haar ketenpartners onderzoeken welke inspanning het vraagt om al het berichtenverkeer om te bouwen tot berichtenverkeer op basis van zegels. Er moet rekening mee worden gehouden dat deze bedrijven, in tegenstelling tot burgers, niet meer kunnen terugvallen op andere kanalen, omdat de diensten enkel nog volledig geautomatiseerd worden aangeboden.

Onze eHerkenningmakelaar kon ons nog niet vertellen, of, hoe en op welke termijn eHerkenning hierbij zou kunnen faciliteren. Onze eHerkenningmakelaar vertelde ons dat de nieuwe functionaliteit 'Dienstbemiddeling' uit eHerkenningrelease 1.10 hiertoe in elk geval *niet* de geschikte oplossing wordt.

Een 'big bang' om *uitsluitend* nog het gebruik van erkende bedrijfsmiddelen toe te staan per inwerkingtredingsdatum is niet verantwoord. Mocht de wet GDI (al dan niet op termijn) ook betrekking krijgen op dit type dienstverlening, zouden bedrijven een overgangstermijn van 5 jaar moeten krijgen waarin ze er nog voor kunnen kiezen bestaande authenticatiemiddelen te blijven gebruiken. Dat geeft ze de tijd om in overleg met hun ICT-leveranciers, beheerste stappen te zetten. Realistischer, maar niettemin nog steeds ambitieus en strenger dan eIDAS vereist.



## 3 Gevolgen voor RDW zelf

### 3.1 Wettelijke taken RDW

De RDW krijgt te maken met hogere kosten om diensten initieel en structureel te ontsluiten voor erkende middelen. De RDW heeft een eerste dienst, die al via een RDW-eigen authenticatiemiddel online was, nu ook via eHerkenning ontsloten (het schorsen van voertuigen). Dat vergde 1.000 uur. De hoop en verwachting is dat het overzetten van volgende diensten sneller verloopt. Er wordt nog onderzocht welke diensten als 'publiek' kunnen worden beschouwd. Dat wil zeggen: niet vallend onder de diensten die de RDW via gesloten systemen aan een welbepaalde groep deelnemers (RDW-erkenninghouders) levert. Bij het webportaal voor burgers valt het aantal diensten die nu nog enkel achter DigiD zitten mee (circa 10 diensten). De initiële kosten hier zullen met name afhangen van het aantal koppelvlakken waarop moet worden aangesloten.

De initiële kosten zitten met name in ICT-uren. Om enerzijds de architectuur van het webportaal aan te passen op multimiddelen-inlog. En anderzijds om bij de diensten die verlopen via berichtenverkeer te kunnen gaan werken met zegels (een vorm van bedrijfshandtekeningen). Beide aanpassingen kennen nog onzekerheden die nader worden onderzocht. Op dit moment lijkt een project met een totale omvang van tienduizenden uren realistischer dan duizenden uren. De RDW verwacht in dat geval andere projecten 'on hold' te moeten gaan zetten.

Op dit moment heeft de RDW geen danwel nauwelijks kosten per authenticatie. Straks krijgt de RDW kosten per authenticatie doorbelast. De memorie van toelichting op het wetsvoorstel zegt daar verder niets concreets over, waardoor het absolute effect niet valt door te berekenen. Soms horen we een bandbreedte van € 0,08 tot € 0,80 per transactie. Daarvoor is, indien een balieproces wordt vervangen door een online proces, een goede business case op te zetten. Als het bovenop de leges komt voor reeds bestaande onlinediensten als "Opvragen tellerstandenrapport t.b.v. erkenning bedrijfsvoorraad" (€ 0,10) is de tariefstijging procentueel fors. Er zijn jaarlijks tientallen miljoenen authenticaties voor RDW-diensten nodig. Tot welke meerkosten dit leidt hangt af van de preciezere afbakening van het begrip 'elektronische dienstverlening' in de wet GDI en tarief per authenticatie.

Mocht de wet GDI door de wetgever ook van toepassing worden verklaard op de gesloten zakelijke systemen uit § 2.2 en 2.3 lopen de uitvoering van wettelijke taken en de zuiverheid van het Kentekenregister gevaar als er geen betere overgangsregeling komt. Het Kentekenregister is dé informatiebron voor voertuiginformatie. Voor o.a. Belastingdienst, gemeenten (parkeerbelastingen en ontheffingen), politie (handhaving) en verzekeraars.

Het altijd voor de volle 100% voldoen aan de webrichtlijnen is een goed streven, doch in de praktijk blijkt het noodzakelijk soms hiervan af te moeten wijken. Zo krijgen wij van onze leverancier terug dat er geen videospeler in de markt beschikbaar is die kan voldoen aan de webrichtlijnen. Voor documenten kan (aanvullend) gebruik van PDF-jes, zeker waar het gaat om bijvoorbeeld (projectmatig) voorlichtingsmateriaal als factsheets of het beschikbaar stellen van instructies, handleidingen, handboeken of formele brieven, erg waardevol zijn. De RDW hoopt dat hier eigen invullingsruimte blijft op basis van gezond verstand.



### 3.2 RDW als leverancier van een authenticatiemiddel voor bedrijven

Uitgaande van dat de RDW de bestaande RDW-certificaten blijft gebruiken voor het zetten van zegels op het berichtenverkeer, zal nauwelijks sprake zijn van besparing door het wegvallen van de aanmaak en uitgifte van deze RDW-certificaten. De precieze effecten hoeveel personen uitsluitend nog gebruik zullen gaan maken van erkende middelen en dus zullen bedanken voor een RDW-certificaat, zijn nu nog lastig in te schatten. Tegenover lagere kosten voor de RDW wegens minder uitgereikte certificaten, staan evenredig lagere opbrengsten vanuit de leges "Instandhouding datacommunicatie met de RDW via een beveiligde aansluiting (certificaat)".

### 3.3 RDW als leverancier van een authenticatiemiddel voor burgers

Als middelenuitgever van het eID op rijbewijs voor burgers zijn er een paar puntjes in de Uniforme Set van Eisen die afwijken van de projectstartarchitectuur van publieke middelen. Waardoor de publieke middelen straks mogelijk niet aan de uniforme set van eisen zullen voldoen. De RDW ziet dit als risico. De RDW ziet de in de Uniforme set van Eisen onderkende rol van middelenuitgever niet expliciet onderkend in de wet GDI.

De RDW constateert voorts dat er geen sprake is van een level playing field qua gebruik tussen private en publieke middelen: Private middelen kunnen wel worden gebruikt in het publieke domein, maar publieke middelen niet in het private domein. Daarmee kunnen de publieke middelen bijvoorbeeld niet gebruikt gaan worden in het aanvraag- en/of activeringsproces van private middelen (het publieke middel als 'moederkaart'). Waardoor het middelenuitgifteproces van private aanbieders een mogelijke kostenbesparing wordt onthouden.

Op pagina 132 van de USvE staat "De Middelenuitgever MOET bij uitgifte van een middel op basis van een bestaand middel naast de eisen voor niveau Substantieel in punt 5 ook de volgende eis toepassen: De validatie van het bezit van het middel en actuele juistheid van de attributen MOET onder de supervisie van een medewerker van de uitgever van het middel staan en het resultaat MOET door een medewerker worden bevestigd." Met als toelichting: "Het uitgeven van een middel op basis van een bestaand middel mag niet een volledig geautomatiseerd proces zijn." Wij voorzien discussies tussen beoordelende instanties en authenticatiediensten over wat onder 'actuele juistheid van de attributen', 'supervisie van een medewerker van de uitgever van het middel', 'resultaat door een medewerker bevestigd' en 'volledig geautomatiseerd' moet worden verstaan. We denken het doel van de nadere invulling te begrijpen, maar zouden graag een smartere omschrijving zien. En voor alle duidelijkheid: IenM en RDW bereiden in afstemming met BZK en gemeenten een onlinedienst voor waarmee burgers via internet een nieuw rijbewijs kunnen aanvragen. Op basis van een bestaand middel. De uitreiking blijft op basis van een face-to-face identiteitsvaststelling. Dit kan een gemeenteambtenaar zijn, maar kan ook worden uitbesteed aan een in identiteitsvaststelling gespecialiseerd koeriersbedrijf.

Onduidelijk is of het de bedoeling is operationele beheerkosten die de RDW maakt inzake instandhouding, ondersteuning en gebruik van het eID-middel op rijbewijs te laten doorbelasten in de kosten per authenticatie of te laten omslaan naar de leges voor verstrekking van het publieke middel.



## Bijlagen

### A. Antwoorden per door BZK in de consultatie gestelde vraag

#### Format Uitvoerbaarheids- en handhaafbaarheidstoets Wet GDI

Let op! De vragen vult u per departement of organisatie in. De vragen zijn bedoeld voor zowel de departementen als de (overige) bestuursorganen, behalve vraag 1a en 2a. Deze zijn alleen bedoeld voor de departementen.

#### Contactgegevens

Naam organisatie: RDW - Dienst Wegverkeer

#### 1. Uitvoerbaarheid

a. Vraag voor departementen: Welke organisaties op uw beleidsdomeinen dienen de wet na te leven?

nvt

b. Is het de organisatie(s) helder wat de opgedragen taak is?

- Geef daarbij ook aan of er taken of verplichtingen zijn die voor een correcte uitvoering c.q. naleving verduidelijking behoeven.

**Nee**, de opgedragen taak is voor de RDW onvoldoende helder.

De RDW stelt voor duidelijker te zijn: Dat het verplicht gebruik van (uitsluitend) erkende middelen niet van toepassing is op de "verlening van diensten die uitsluitend binnen gesloten systemen gebruikt worden tussen een welbepaalde groep deelnemers" en die geen openbare diensten zijn "die aan het publiek verleend worden" (naar o.a. overweging 21 uit de eIDAS verordening EU nr 910/2014). Voor meer informatie: zie § 2.2 en 2.3.

Daarnaast graag meer duidelijkheid over de normen die gelden tav classificatie van het betrouwbaarheidsniveau van overheidsdiensten.

c. Zijn/ is de uitvoerende organisatie(s) voldoende toegerust voor een doeltreffende uitvoering?

- Geef aan of er voldoende capaciteit is, of dat de uitvoering verschuiving van prioriteiten of andere maatregelen vergt.
- Geef aan of uw organisatie op het gebied van de ICT voldoende is toegerust. Geef ook aan of voldoende helder is wat de uitvoering van de automatisering vraagt.
- Geef aan in hoeverre de voor de uitvoering benodigde werkprocessen voorhanden zijn.

**Nee**, de RDW en vaste zakelijke ketenpartners zijn, bij ontbreken van de onder 1b gevraagde duidelijkheid, onvoldoende toegerust voor een doeltreffende uitvoering.

Afhankelijk van de ruimte die wordt geboden t.a.v. met name zakelijke dienstverlening vraagt invoering veel capaciteit en herprioritering van geplande ICT-veranderingen in de projectenportefeuille; We verwachten voor de ICT-divisie van de RDW een inspanning die mogelijk in de tienduizenden uren loopt.

Verder zijn er nog vragen aan welke normenkaders de audit(s?) moeten voldoen: is dat ISO27001 en BIR? Of iets anders?





d. Wat zijn de verwachte effecten van de ontwerpwet voor uw organisatie of departement?

- Geef aan wat de effecten van de ontwerpwet zijn op de digitale dienstverlening aan de burger en ondernemer.
- Geef aan welke producten of processen door de Wet GDI geraakt worden en wat de voordelen en nadelen van de ontwerpwet zijn.
- Geef aan of er ook mogelijke neven- en onvoorziene of onbedoelde effecten zijn.

Zonder de gevraagde verduidelijking van 1b: Grote kans op en hoge impact wegens uitval van bestaande digitale dienstverlening en uitval zo niet sluiting van baliedienstverlening.

Met de gevraagde verduidelijking van 1b zullen er meer digitale diensten voor burgers en ondernemers beschikbaar komen. En gaat het serviceniveau omhoog.

Alle RDW-taken worden door de wet GDI geraakt, tenzij taken die via vaste ketenpartners worden uitgevoerd buiten scope 'verplicht gebruik van uitsluitend erkende middelen' worden geplaatst (zie onder vraag 1b).

Voor rechtstreekse dienstverlening, waarbij het publiek (zowel burgers als rechtspersonen) moeten inloggen op rdw.nl is de wet GDI in grote lijn uitvoerbaar en zal de wet het positieve effect hebben dat we nog meer dienstverlening, waar voertuigbezitters nu nog voor naar een balie moeten, online kunnen brengen.

Wat betreft neveneffecten:

Het ontbreken van de gevraagde scope-afbakening, het uitsluiten van het gebruik van het huidige RDW-certificaat als authenticatiemiddel binnen de gesloten systeemcontext van de RDW, en het ontbreken van een overgangstermijn van 5 jaar, kan een ontwrichtende uitwerking hebben op de bedrijfsvoering van ketenpartners. Waardoor o.a. baliedienstverlening aan het publiek in gevaar komt. Via baliedienstverlening wordt het Kentekenregister bijgewerkt. Als ketenpartners het Kentekenregister niet kunnen bijwerken, komen o.a. Belastingdienst en gemeenten in problemen met de inning van belastingen, de politie met handhaving en burgers met APK en aan- en verkoop van hun voertuig.

We zien voornamelijk geen incentive voor lage doorbelastingkosten aan de publieke dienstverleners. Bij stijging van de doorbelastingkosten per authenticatie ten opzichte van bestaande authenticaties, zullen de leges van RDW-diensten die nu al digitaal beschikbaar zijn, mee stijgen. Er zijn jaarlijks tientallen miljoenen authenticaties voor RDW-diensten nodig. Tot welke meerkosten dit leidt hangt af van scope en tarief per authenticatie.

Voorts:

- noodzakelijke wijzigingen bij marktpartijen (providers/softwarehuizen/erkende bedrijven), met doorlooptijd en kosten voor deze marktpartijen voor digitale dienstverlening;
- kosten eHerkenningmiddel kunnen fors gaan oplopen voor bedrijven: per medewerker een middel aanvragen, eventuele machtigingskosten, eventuele ICT-wijzigingen en extra handeling(en) per authenticatie.
- Voordeel: met name zeer kleine bedrijven zullen met hun middel ook andere overheidsdienstverlening kunnen afnemen.
- Mogelijk raakt de positie van RDW-applicatieproviders in de knel.
- De RDW verstrekt de RDW-certificaten ook aan vaste zakelijke klanten buiten de EU. Zoals voertuigfabrikanten in Azië en VS om digitaal specificaties van voertuigen aan te leveren. Deze klanten moeten wel bediend kunnen blijven worden. Wij zien op dit moment niet hoe die aan een middel kunnen komen.
- Effecten hangen ook af van het tempo c.q. de fasering / tranches waarin uitvoering wordt gegeven aan de wet c.q. de te onderscheiden tranches in werking treden. Opname van een globale planning in de MvT helpt betrokkenen hun investeringsbeslissingen af te stemmen op deze planning.



e. Wat zijn de gevolgen van de acceptatieplicht van de erkende middelen?

- Geef aan wat de gevolgen van de acceptatieplicht zijn, mede in relatie tot interoperabiliteit, tarifiering, de uitfasering van DigiD-laag/basis en de ambitie om bestuursorganen en aangewezen organisaties zo eenvoudig mogelijk aan te kunnen laten sluiten op de diverse erkende authenticatiemiddelen.

Acceptatieplicht is doenbaar voor publieke dienstverlening op rdw.nl. Leges voor diensten die nu achter DigiD of het RDW eigen middel zitten, zullen stijgen met de meerkosten die per authenticatie door de ontsluitende dienst gaan worden doorbelast. Verder is hier bij andere vragen al antwoord op gegeven. In feite is er niet enkel een acceptatieplicht voor de dienstverlener, maar ook een gebruiksplicht voor de bedrijven (wat enigszins eufemistisch een 'recht' wordt genoemd in de wet). Niet alleen voor de RDW, maar ook haar zakelijke klanten nemen de kosten daarmee flink toe. Een van de grootste RDW-providers (het RDC) heeft, zien wij, inmiddels zelf gereageerd op de internetconsultatie.

f. Wat zijn de ingeschatte kosten die nodig zijn voor uitvoering van de wet voor uw organisaties of departement?

- Geef aan om welke type kosten (directe/indirecte kosten?) het gaat en of het eenmalige of structurele kosten zijn. Beide: eenmalig en structureel.
- Geef aan waarop de inschatting is gebaseerd en of de kosten als proportioneel kunnen worden beschouwd.

Het kostte bijna 1.000 uur om 1 dienst, de dienst 'zakelijk schorsen online' op rdw.nl achter eHerkenning te ontsluiten. De dienst zelf bestond al voor klanten met een RDW-certificaat. Er wordt nog onderzocht welke diensten als 'publiek' kunnen worden beschouwd. Dat wil zeggen: niet vallend onder de diensten die de RDW via gesloten systemen aan een welbepaalde groep deelnemers (RDW-erkenninghouders) levert. Er wordt een inleereffect verwacht en dat er een vereenvoudiging in de architectuur valt te maken waardoor de oplossing meer generiek kan worden gemaakt. Bij het webportaal voor burgers valt het aantal diensten die nu nog enkel achter DigiD zitten mee (circa 10 diensten). De initiële kosten hier zullen met name afhangen van het aantal koppelvlakken waarop moet worden aangesloten.

Er zijn rond de 35.000 vaste zakelijke klanten, met elk enkele, tot meer dan duizend medewerkers die transacties uitvoeren die tot een mutatie in het Kentekenregister leiden. Overheden als politie, Belastingdienst en gemeenten niet meegerekend. Samen goed voor tientallen miljoenen transacties per jaar, afhankelijk van de scope van de wet GDI. Die gemiddeld op betrouwbaarheidsniveau Substantieel moeten worden afgehandeld. Als per transactie een authenticatie plaats vindt en er per authenticatie moet worden afgerekend, kan het bedrag dat de RDW heeft te betalen aan de ontsluitende diensten flink oplopen als de scope van de wet GDI niet wordt beperkt tot diensten aan het publiek.

## 2. Handhaafbaarheid

a. Vraag voor departementen: Welke organisaties of organisatieonderdelen zullen toezicht houden op een correcte uitvoering van de wet?

- Geef voor uw departement aan welke organisatie of organisatieonderdeel toezicht houdt op de naleving van de Wet GDI (ihbz de artt. 5,8 en 16). nvt

b. Wat is het oordeel van de toezichthoudende organisaties (of organisatieonderdelen) over de uitvoerbaarheid en handhaafbaarheid?

- Geef daarbij ook aan of er taken of verplichtingen zijn die voor een correcte uitvoering c.q. naleving verduidelijking behoeven.
- Geef aan of de toezichthoudende organisatie of organisatieonderdeel over voldoende kennis en/of capaciteit beschikt.
- Geef aan wat de kosten van toezicht en handhaving zijn. Geef verder aan waarop deze inschatting is gebaseerd en of de kosten als proportioneel kunnen worden beschouwd.

?

## B. Artikelsgewijze opmerkingen WGDI

### Artikel 1. Definities

- Elektronische dienstverlening: is dit beperkt tot rechtstreeks elektronisch verkeer met bestuursorganen, of wordt hieronder ook dienstverlening verstaan waarbij toegang wordt verkregen tot elektronisch verkeer met bestuursorganen via derden?
- In dit kader graag ook de passage over PKI-overheid-certificaten in de MvT op p17 bezien: Hier lijkt te worden gesteld dat erkenning van een dergelijk certificaat als authenticatiemiddel enkel van belang is bij authenticatie door personen. Niet bij informatie-uitwisseling tussen systemen of zetten van elektronische handtekeningen. Dit wordt geïnterpreteerd als dat een niet erkend authenticatiemiddel volstaat indien een persoon via een (software-)systeem met een systeem van een bestuursorgaan communiceert. Of daarmee nu een digitale handtekening wordt gezet of niet doet er dan niet toe. Als het anders is bedoeld: hoe dan?
- Hoe verhoudt zich 'dat de standaard openbaar toegankelijk en kosteloos bruikbaar is, met het profijtbeginsel waar GDI voorzieningen nu onder gaan vallen (met name bij Diginetwerk).
- De rol en definitie van middelenuitgever ontbreekt. Is het voldoende dat samenhang met en afbakening van de authenticatiedienst slechts blijkt uit de Uniforme Set van Eisen?

### Artikel 2. Standaarden

- Effect hiervan hangt af wat de (aanscherping) van deze standaarden in lagere regelgeving met zich mee brengt.
- Lid 3, "Bij de aanwijzing wordt het functionele en organisatorische toepassingsbereik van de standaard omschreven": Het zou voor voldoende flexibiliteit bij de uitvoering van deze wet de voorkeur hebben om een grondslag voor uitzondering te creëren. Op basis van dat een uitvoeringsorganisatie in afstemming met het verantwoordelijke departement (al dan niet voor een bepaalde periode) kan worden vrijgesteld van een standaardplicht. Bijvoorbeeld als de benodigde inspanning zijn doel voorbij schiet, of er andere zwaarwegende redenen zijn om van de standaardplicht af te wijken.
- De 'explain' is er uit. Geen ruimte voor eigen afweging op basis van business case.
- Besluitvorming voor nieuwe standaard komt verder van bestuursorganen af te staan.
- Webrichtlijnen (ETSI EN 301 549) zet alle websites en bestaande dienstverlening onder druk. Er is geen videospeler in de markt die kan voldoen aan de gestelde eisen. Ook het soms onvermijdelijke gebruik van PDF-jes vormt een probleem.

### Artikel 3. Reikwijdte

[Geen opmerkingen]

### Artikel 4. Taken en verantwoordelijkheden

- Check: is I&M het eens met de passage in de MvT op p 58?
- In de USvE is de middelenuitgever (RDW) expliciet verantwoordelijk gesteld voor de uitgifte van eID op rijbewijs.
- In de rol van beheerder BSNk (dus niet AD) speelt Logius wel een rol bij de uitgifte, door het uitreiken van de bijbehorende pseudoniemen voor personalisering en aanmaak eID op het rijbewijs.
- Voor eID op rijbewijs is uitgangspunt dat eID de rijbewijsproductie en -afgifteprocessen volgt. Dit vereist afstemming van regelgeving,



- De aangekondigde extra taken en grondslagen gegevensverwerking in Wvw, moeten nog worden verwerkt in art 25.

#### Artikel 5. Acceptatieplicht

- Stel er wordt een nieuw middel erkend. Die buiten de bestaande ontsluitende dienst om werkt: hoeveel tijd krijgen de bestuursorganen die te accepteren?
- In hoeverre geldt de acceptatieplicht ook in de situaties die de RDW heeft beschreven in paragrafen 2.2 en 2.3.? Wanneer vallen situaties onder 'interne', 'gesloten', en/of 'RDW-eigen'-netwerken waarop een eigen authenticatieregime van toepassing is?
- Moeten bestuursorganen qua betrouwbaarheidsclassificering van diensten er van uitgaan dat de richtlijnen van het Forum Standaardisatie worden overgenomen?

#### Artikel 6. Erkenning

- Lid 9: noem een termijn waarbinnen een besluit wordt genomen of een middel wordt erkend (komt in MR, maar geen indicatie in MvT).
- P. 53, par 14 3e al. Je kunt niet zeggen vanaf inwerkingtreding WGDI. Hoe gaat het bijv als er na die tijd een nieuw middel op de markt komt. Dit zal binnen redelijke termijn moeten worden aangesloten. Geen "verantwoord" tijdspad.
- Idem voor laatste alinea par 14. Ook dan een redelijke aansluitperiode nodig. MvT, p3: 'Ook de publieke en private organisatie die een middel uitgeeft (authenticatiedienst) dient door de minister te worden erkend.' Hier zit een tweeslachtigheid in. Staat Logius als AD aan de lat om publieke middelen te laten erkennen, of moet de RDW als middelenuitgever (dus geen AD) ook zelfstandig een aanvraag indienen? Laatste lijkt ons niet.

#### Artikel 7. Eisen aan erkende diensten, erkende middelen en publieke voorziening

- Wijziging in de UsvE in de loop van de tijd. Afspraken maken over uitvoeringstoets om gevolgen van wijziging in eisen in beeld te brengen. En om het benodigde overgangsregime vast te stellen. Upgrade UsvE kan niet leiden tot niet-ondersteuning van eerdere versies en dus verplichte omwisseling van 10-jarige WIDs'.
- MvT p20: Tevens wordt bij de verstrekking vastgelegd voor welke zaken de houder van dit middel bevoegd is namens de onderneming: is dit een realistische voorstelling van zaken? Hoe ziet de overheid dit voor zich zodra toegang verkregen kan worden tot tientallen zo niet honderden (bestuurs-)organen met elk tientallen diensten? Enerzijds is dit niet op een (aanvraag-)formulier aan te kruizen (zou dan enkel elektronisch kunnen), anderzijds stelt dit hoge eisen aan overzichtelijke beheerfunctionaliteiten voor ondernemingen.
- Degene die het middel aanvraagt voor een medewerker moet bevoegd zijn: dat betekent dus o.a. dat beoordeeld moet worden of toe te kennen bevoegdheden binnen de portefeuille/zelfstandige bevoegdheid van een bestuurder vallen.
- MvT op p18: Bij het publieke middel wordt al voor aanmaak van het publieke middel bij het BSNk polymorfe identiteit en pseudoniemen gegenereerd en op het middel (rijbewijs) geplaatst. Dat is dus precies andersom dan in de MvT staat.
- MvT p18: "De polymorfe pseudoniem is daarom bedoeld voor toepassingen waar het BSN niet nodig is": als het gebruik van het publieke middel beperkt is tot het publieke domein, zou het gebruik van die polymorfe pseudoniemen voor publieke middelen strikt genomen niet noodzakelijk zijn. Want binnen dat stelsel is immers al de afspraak dat burgers worden geïdentificeerd aan de hand van hun BSN.
- Art 7.2 en p 66 onder kopje "werking". Zie ook eerdere opmerking over "uitgifte... middel". Voorbehoud proces rijbewijs.

**Artikel 8. Eisen aan bestuursorganen en aangewezen organisaties**

- Dit is zoets als het huidige DigiD assessment? Maar dan met als scope alle dienstverlening waarvoor authenticatieniveau substantieel of hoger is vereist, dus bijna alle zakelijke RDW dienstverlening? Dat brengt extra kosten met zich mee + natuurlijk meer inspanning auditpunten te voorkomen en eventueel op te lossen. Worden de daadwerkelijke eisen in lagere regelgeving verwerkt? Om te kunnen kijken wat de impact van deze wet is, is nodig te weten welke regels worden bedoeld.
- Lastendruk wordt onderschat.

**Artikel 9. Verwerking van persoonsgegevens**

- Lid 3 inhoud AMVB is nog niet bekend, maar levert vermoedelijk geen probleem.

**Artikel 10. Toezicht op publieke en private diensten**

- Krijgt de RDW ook te maken met dit toezicht? Hoe ziet dit er uit, wat gaat dit kosten en welke gevolgen heeft dit verder?
- P 73, tweede alinea. 'afgewogen toezicht- en handhavingssysteem'. Hoe kan dit worden gesteld terwijl de uitwerking nog ontbreekt?

**Artikel 11. Bestuursdwang en dwangsom**

*[Geen opmerkingen]*

**Artikel 12. Bestuurlijke boete**

*[Geen opmerkingen]*

**Artikel 13. Schorsen of intrekken erkenning**

*[Geen opmerkingen]*

**Artikel 14. Toezicht op bestuursorganen Rijk en aangewezen organisaties**

*[Geen opmerkingen]*

**Artikel 15. Bijzondere bevoegdheden**

- Betrokkenheid uitvoeringsorganisatie en verantwoordelijk departement verankeren: "Onze Minister kan .... " toevoegen: " gehoord hebbende het bestuursorgaan of de aangewezen organisatie, en in overeenstemming met Onze Minister wie het aangaat ..."
- Min BZK kan dan feitelijk de dienstverlening van de uitvoerders van IenM stil leggen?
- De RDW wordt als middelenuitgever geïnformeerd over eventuele onderbreking van de dienstverlening van een of meer door de RDW uitgegeven middelen.

**Artikel 16. Informatieverstrekking**

*[Geen opmerkingen]*

**Artikel 17. Leges voor erkenning diensten en middelen**

*[Geen opmerkingen]*

**Artikel 18. Leges voor verstrekking publiek middel**

- IenM en BZK moeten overleg hebben over de formulering van deze bepaling vwb eID op het rijbewijs. Bij de RDW gaat het namelijk om de kosten die de RDW maakt en die de RDW bij de gemeenten (rijkskostencomponent) of bij de burger (straks bij online aanvraagmogelijkheid) in rekening brengt.
- In verband brengen met wijziging WVV achterin het wetsvoorstel.
- Kosten samenhangend met het gebruik van het eID op het rijbewijs. Opslag per tik?



- Wat is de financiële positie van de middelenuitgever?
- Financiering instandhoudingskosten middel zelfstandig of via Logius?

#### Artikel 19. Leges voor publieke authenticatiedienst en publieke machtigingsdienst

- Hoe vindt de verrekening plaats en wat wordt er verrekend? Het aantal inlogpogingen? Het aantal succesvolle authenticaties? Is er een vast tarief en daarnaast nog per 'tik'?

#### Artikel 20. Doorberekening kosten publieke voorziening en toezicht

*[Weinig zinnigs over te zeggen zolang dit niet concreter is]*

#### Artikel 21. Tarifiering

- Hier blijft het risico dat publieke dienstverleners opdraaien voor de rekening van het gebruik van door burgers gekozen (extra) dure oplossingen. Immers: die moeten alle erkende middelen accepteren. Ongeacht welk tarief wordt doorbelast. De dienstverleners zullen dit op hun beurt in hun tarieven doorberekenen. RDW is tariefgefinancierd: hogere kosten per authenticatie betekent tariefsverhoging voor onze klanten. T.o.v. huidige online dienstverlening wordt die geconfronteerd met een hoger tarief per dienst.
- MvT p45: Een private partij hoeft niets te rekenen voor de aanschaf van het middel. Hij zal bij 'gratis' verstrekking veel burgers verleiden tot aanschaf. De kosten die die private partij dan maakt zullen linksom of rechtsom in het gebruik worden doorbelast. De rekening komt dan bij een ander te liggen. Hoe wordt de marktwerking wel geprikkeld?
- MvT p51: gevolgen voor ondernemers: door functiescheiding zal een door een onderneming voor een medewerker aangeschaft (persoonsgebonden!) authenticatiemiddel niet snel verder bruikbaar zijn in de onderneming voor toegang tot andere overheidsdiensten.
- Wat betreft regeldruk (we weten niet waar we dat anders kwijt kunnen): onderschat niet de inspanning benodigd om over te schakelen op eHerkenning. Risico voor bedrijven dat het (duur) aangeschafte eHerkenningmiddel het nieuwe single point of failure wordt. Om dat te voorkomen moeten ze mogelijk bij kritieke processen van meerdere leveranciers middelen gaan aanschaffen. Tot slot: sommige branches hadden al privaat een 'eigen' standaard. Zal daar niet als lastenverlichting maar als lastenverzwaring door branche worden ontvangen.

#### Artikel 22. Evaluatie

- De evaluatietermijn (5 jaar) zou ook kunnen worden gehanteerd als overgangstermijn om definitief te besluiten bestaande authenticatiemiddelen voor bedrijven niet meer naast erkende middelen te accepteren.

#### Artikel 23. Overgangsrecht

- Ad 4: Hierin lijkt een impliciete aanname te zitten dat DigiD Basis en Midden voldoen aan de betrouwbaarheidseisen van eIDAS Laag. Zolang en indien DigiD Basis en Midden (nog) niet getoetst zijn aan en/of blijken te voldoen aan die eisen, kan het dan zo zijn dat die middelen niet mogen worden geaccepteerd? Of wordt bedoeld dat DigiD Basis en Midden nog 3 jaar mogen worden geaccepteerd, ongeacht of ze (volledig) aan 'Laag' voldoen en/of als 'Laag' middelen worden erkend?
- Ons voorstel is bestaande zakelijke authenticatiemiddelen voor bedrijven, gedurende een overgangstermijn van 5 jaar te mogen blijven accepteren. Naast erkende middelen (van eHerkenning).
- Overweeg ingroeipad voor eHerkenning: bijvoorbeeld eerst verplichte acceptatie bij rechtstreekse dienstverlening (zoals overheidseigen websites/-portals). En meer tijd te geven al naar gelang de dienstverlening via meer partijen en infrastructuren loopt.



- Ook zou de eerste tranche zich kunnen beperken tot rechtstreekse dienstverlening (inloggen op websites / -portaldiensten). Dienstverlening o.b.v. ander berichtenverkeer zou eerst dmv facultatieve richtlijnen kunnen starten en na de evaluatie over 5 jaar alsnog een verplichtend karakter kunnen krijgen.
- Het huidige voorgestelde tijdpad brengt de continuïteit van de RDW-dienstverlening, de uitvoering van wettelijke taken, de uitvoering van daarvan afhankelijke taken van andere overheden, de dienstverlening van bedrijven en het kunnen voldoen van voertuigbezitters aan wettelijke verplichtingen in gevaar.
- Lid 4 ziet niet op EH1, EH2, EH2+ en iDIN Laag. Voor alle duidelijkheid: ingevolge artikel 5 mogen die dus m.i.v. inwerkingtreding wet GDI niet meer worden geaccepteerd door publieke dienstverleners(?)

Artikel 24. Wijziging van de Wet Elektronisch berichtenverkeer Belastingdienst  
*[Geen opmerkingen]*

Artikel 25. Wijziging van de Wegenverkeerswet 1994

- Het is noodzakelijk dat BZK en IenM voordat de WGDI verder de procedure in gaat met elkaar afstemmen welke wijziging van de Wegenverkeerswet en WGDI nodig is om de taken van de RDW en de financiering van de kosten die de RDW maakt voor eID afdoende te verankeren
- Beheer in en instandhouding van artikel RBW-register valt onder rijkskostencomponent (huidig art 121 WvW.WvW).
- Zie toelichting bij art 4: nog opnemen taak en grondslag voor gegevensverwerking/extra data. Of wil IenM de taak het liefst in de WGDI zien?

Artikel 26. Omhangen  
*[Geen opmerkingen]*

Artikel 27. Inwerkingtreding

- Bij verschillende tijdlijnen: Wat moet er klaar zijn per datum-X?
- Gezien de impact van sommige punten moet hier vroegtijdig zicht op zijn.

Artikel 28. Citeertitel  
*[Geen opmerkingen]*



## C. Opmerkingen per eis uit de USvE 1.0

Nr.	Bijz.	Onderwerp	Wat zegt de USvE	Reactie RDW
1.	-	KV's	De koppelvlakken voldoen niet aan de overheidsstandaarden die in de GDI wet verankerd worden	Het is jammer dat de Digikoppelingen patronen (WUS BE-S) niet als uitgangspunten voor de koppelvlakken zijn genomen. Dit bespaart een hoop documentatie omdat DK de gehele logistieke laag (envelop) beschrijft. Daarnaast heeft DK diverse voorzieningen voor het testen en zijn we daarmee als overheidspartijen compliant aan de overheidsstandaarden (GDI). Als MV willen we natuurlijk diginetwerk als transport netwerk gebruiken. DK is gebaseerd op open standaarden dus het zou voor de private partijen weinig uitmaken.
2.	-	Onderscheid publieke en private middelenuitgevers	In de USvE wordt geen onderscheid gemaakt tussen publieke en private MU's.	Onder gelijke omstandigheden moeten Participanten aan gelijke eisen voldoen. Daar waar er door (overige) wetgeving echter verschil is, verdient het de voorkeur om het verschil ook te benoemen, om de eisen concreet te houden. In onze reactie geven wij dergelijke verschillen aan.
3.	10	Geen USvE voor authenticatiemiddelen bedrijven?	De Uniforme Set van Eisen beschrijft eisen aan partijen in de Authenticatieketen die burger-authenticatie in het Publieke domein verzorgen. Het betreft hier een afbakening naar doelgroep (Natuurlijke personen die over een BSN beschikken, zie Gebruiker) en niet naar partijen. Voor alle partijen die een rol spelen in de Authenticatieketen geldt, dat zij slechts deze functionaliteit mogen aanbieden indien zij aan de Uniforme Set van Eisen voldoen.	De Uniforme Set van Eisen beschrijft geen eisen aan partijen in de Authenticatieketen die authenticatie van bedrijven in het Publieke domein verzorgen. Aangezien daar geen aparte set voor in consultatie is: wie erkent op grond waarvan deze middelen?
4.	11	Begrippenlijst USvE wijkt af van de wet GDI	Bijvoorbeeld: "Authenticatiemiddel. Een <i>middel</i> op grond waarvan Authenticatie van een Gebruiker kan plaatsvinden."	In wet GDI: "authenticatiemiddel. <i>methode</i> voor de verificatie en bevestiging van de identiteit van een natuurlijke persoon of rechtspersoon die deze toegang biedt tot elektronische dienstverlening"



Nr	Biz	Onderwerp	Wat zegt de USvE	Reactie RDW
5.	15 16 17 35	Rol van <i>middelenuitgever</i>	<p>De Middelenuitgever (MU) is een rol van een Participant die een elektronisch Authenticatiemiddel verstrekt aan de Gebruiker en het middel bij het BSNk activeert voor gebruik in het Publieke domein. De Middelenuitgever biedt de Gebruiker de mogelijkheid om zijn Authenticatiemiddel(en) te beheren en zorgt ervoor dat het BSNk Inzageregister een actuele status van de Authenticatiemiddelen (of de relatie) heeft.</p> <p>P35. Het activeren van een relatie van een Gebruiker met een Authenticatiedienst naar aanleiding van een weloverwogen verzoek van de Gebruiker.</p>	<p>Graag nog goed naar formulering kijken dat die straks niet onnodig beperkend wordt:</p> <ul style="list-style-type: none"> <li>De MU mag de Gebruiker de mogelijkheid tot beheer ook enkel <i>via de AD</i> geven.</li> <li>'activeert' wekt onjuiste verwachting. Suggesties voor alternatieven: 'geschikt maakt' of 'aanmeldt'.</li> </ul> <p>BZK heeft besloten dat de eID functionaliteit op alle nieuw uitgegeven middelen wordt geplaatst. Er komt geen verzoek van de gebruiker aan te pas. De gebruiker heeft uitsluitend een opt-out: hij kan een revocatie aanvragen (via DigiD bij de AD). Voldoet dat aan deze formulering? Zo niet, dan moet de formulering worden aangepast of er komt een (kostbare) aanpassing van de aanvraag procedure voor Rijbewijs en NIK.</p> <p>Bij IDIN wordt het middel expliciet gekoppeld aan BSN via BSNk. Dit zullen we met publieke middelen nooit doen (veel impact).</p>
6.	19	Beschikbaarheid statussen	De actuele status van een middel is voor de Gebruiker altijd bij de Middelenuitgever beschikbaar.	<p>Mag er sprake zijn van het gebruik van een subset aan statussen?</p> <p>Expired is op dit moment geen status die RDW doorgeeft. Als we dit moeten doen dan zal een batchverwerking gedefinieerd moeten worden die bv elke dag de expired rijbewijzen scant in het CRB en dan de statussen doorgeeft</p>
7.	23	Plan voor het beëindigen van de dienstverlening	Participanten MOETEN over een plan beschikken voor het beëindigen van de dienstverlening ongeacht de intentie of oorzaak van de beëindiging. Het plan voorziet in elk geval in: [...]	Publiek middel hiervan uitzonderen: een dergelijk plan is niet zinvol omdat er wegens de wettelijke taak geen sprake kan zijn van beëindiging dienstverlening
8.	25	Inrichting fysiek inzageproces	Indien een persoon claimt niet meer over een geldig Authenticatiemiddel te beschikken of claimt dat een middel ten onrechte aan zijn identiteit is gekoppeld en online inzage niet mogelijk is, MOET fysiek inzicht gegeven worden in de gegevens	T.a.v. welke rol geldt deze eis? Indien MU: graag dit dusdanig formuleren dat de voorziening anaaloog aan voorstel bij punt 5 ook via de AD mag lopen.
9.	32	Inzageregister	Inzageregister lijkt zoals nu in de figuur weergegeven te worden gevoed door de AD.	Kan verwarring wekken omdat in teksten deze rol belegd is bij MU.

18-04-2017 10:44:53

Nr	Biz	Onderwerp	Wat zegt de USvE	Reactie RDW
10.	35	De rol van de authenticatiedienst	Indien de Authenticatiedienst en de Middelenuitgever twee verschillende partijen zijn, dan ook: Het activeren (en de-activeren) van de relatie met de Gebruiker bij de betreffende Middelenuitgever Het zorgvuldig verkrijgen van de Polymorfe identiteit/pseudoniem van deze Gebruiker aan deze Authenticatiedienst (volgens eisen aan Informatiebeveiliging en Privacy).	In het geval van RDW (en ook RViG) als zijnde MU wordt de polymorfe identiteit/pseudoniem aangevraagd door de MU om deze op het middel te kunnen zetten. Als de authenticatiedienst een andere partij is dan de middelenuitgever (RDW/RViG) is het verkrijgen van deze PI/PP dus geen rol van de authenticatiedienst
11.	38	Meesturen controlegegevens met het BSN naar BSNk	Hiervoor stuurt de Middelenuitgever het BSN en controlegegevens naar het BSNk.	In het BSN-domein worden ivm dataminimalisatie en privacy geen controlegegevens meegestuurd. Binnen overheden wordt enkel o.b.v. BSN informatie over burgers uitgewisseld.
12.	38	Activeren BSN	Tenslotte registreert het BSNk deze activering bij zijn eigen Inzageregister.	Dit is hoogstens een activering in de betekenis van het koppelen van een PI/PP aan de BSN van de burger. Het middel is niet actief aangezien de RDW het middel uitgeeft aan de burger met het eID middel status "inactief" De burger moet dan zelf via de "self service"
13.	38	Misbruikbestrijdingsregister	Een Authenticatiedienst of Middelenuitgever registreert een Opmerkelijke gebeurtenis van een Gebruiker bij het Misbruikbestrijdingsregister.	Opmerkelijke gebeurtenissen hebben te maken met gebruik en vallen daarom onder de rol AD. Niet MU. De MU bestrijdt misbruik via de actuele status v/h middel.
14.	38	Transformeren	Een Authenticatiedienst heeft hiernaast de keuze om deze transformatie zelf uit te voeren. Hiertoe kan de Authenticatiedienst een speciaal beveiligd computer systeem (HSM) aanschaffen en speciaal Sleutelmateriaal verkrijgen van de Sleutelbeheer-functie.	De USvE spreekt hier alleen over een eigen HSM voor de functie "Tranformereren" (VP en VI) maar niet voor de functie "Activatie" (Genereren PI en PP) Voor een middelenuitgever zou een HSM voor het verkrijgen van de PI/PP ook mogelijk moeten zijn omdat de interface-naar BSNk een risico vormt voor het aanmaak proces van het middel (rijbewijs)
15.	40	Registratiefase en de rol van de AD	In de registratiefase heeft de Authenticatiedienst de Gebruiker en zijn BSN geregistreerd. De Authenticatiedienst registreert de Gebruiker daarna in de infrastructuur door het verzenden van dit BSN naar de BSN activeringsfunctie (AUC1 Activeren BSN) BSNk. Met het BSN worden enkele andere gegevens meegestuurd waarop het BSNk enkele plausibiliteit checks uitvoert. Als deze checks succesvol afgerond worden, krijgt de Authenticatiedienst een Polymorfe Identiteit en Pseudoniem terug geleverd van het BSNk. Zie onderstaande figuur	Net als bij punt 9 wordt ook hier beschreven dat de AD de pseudoniemen opvraagt bij BSNk. Dit terwijl op andere plaatsen staat dat dit is belegd bij MU.

Nr.	Biz.	Onderwerp	Wat zegt de USvE	Reactie RDW
16.	59	Nader uit te werken functionaliteiten	In opvolgende versies van de Uniforme Set van Eisen komen hier de volgende functionaliteiten en diensten bij:	Het ontbreken van machine-to-machine in deze versie is jammer en verwarrend omdat binnen de overheid al diverse standaarden gebruikt worden voor dergelijke functionaliteit. Het advies is om duidelijkheid te creëren mbt de huidige standaarden voor machine-to-machine functionaliteit tussen overheden.  Kortom ligt deze paragraaf beter toe zodat partijen beter kunnen inschatten waar ze aan toe zijn m.b.t. deze functionaliteit.
17.	45 92	statusdienst	Er wordt een statusdienst ingericht die werkt op basis van pseudoniemen en waar de Authenticatiedienst (of Middelenuitgever) de status van de PPCA middelen kan registreren, i.e. of een middel 'Uitgegeven', 'Geactiveerd', 'Ingetrokken' etc. (zie Status (van het Authenticatiemiddel)) is.	Het gebruik van statusbenamingen is in het document niet consequent. (soms engels en soms nederlands; verschillende types.etc. Graag 1 set van statussen afspreken waarvan de MU een subset kan gebruiken.
18.	86  87	Request  N.B.	An identical <ProvidePP_PPCAOptimizedRequest> request exists for Middelenuitgevers that implement optimized versions of PPCA.  N.B. Only providing the BSN is not deemed to identify a subject with sufficient assurance, additional information must be provided for verification. In general: the more information is provided in the request, the more chance of a unique match with sufficient assurance.	In dit request bericht zal RDW alleen het BSN meegeven en niet andere "controle" gegevens zoals Document ID e.d. ivm dataminimalisatie en privacy. RDW controleert de BSN al op geldigheid tegen het BRP register. Daarmee is het uniek zijn en de validiteit al gegarandeerd.  De extra controle elementen in het request zijn overigens optioneel volgens de definitie.
19.	87	Response tekst	An identical <ProvidePP_PPCAOptimizedResponse> is provided that will return a PIP (and PP) for PPCA optimized implementations.	Dit is de enige aanwijzing dat er naast de PIP ook een PP in het response bericht zit. Of deze aan elkaar gelinkt zijn is niet gedefinieerd. (De EC points in de PP moeten hetzelfde zijn als de PP EC points in de PIP)
20.	87	Response definitie	One or more (signed) Polymorphic Pseudonymization structure(s) for the User. At least one structure MUST be provided.	RDW verwacht hier minimaal twee Pseudonymen. Een PIP en een PP. (waarbij de PP gekoppeld is aan de PIP zoals ook beschreven bij het review-commentaar bij Response tekst.
21.	93	Request definitie	IDP	Alle statusverzoeken, wijzigingen die bij de RDW binnenkomen (wijzigingsverzoeken door DigiD zelf of door de burger) zullen worden doorgegeven met in dit element de OIN van DigiD. Als de status door RDW zelf wordt aangepast zal dit element niet gevuld/meegegeven worden.

Nr	Biz	Onderwerp	Wat zegt de USvE	Reactie RDW
22.	93	ReadableCardID	This element is required for every new registration and optional for any existing registration (any new will overwrite the old text).	Dit element is verplicht bij nieuwe aanvragen maar vanuit privacy en traceability redenen wil RDW hier geen info in meegeven. Het is bij RDW nog niet bekend wat er dan wel in komt.
23.	93	Response definitie	The current status, after processing the optional status change in the request.	Het statusverzoek vanuit de MU is geen optionele status wijziging. Het inzageregister moet verplicht de statuswijziging vanuit de MU overnemen. Dit omdat is afgesproken dat het MU register (b.v. het CRB eID register bij de RDW) het bronregister is.
24.	128	Natuurlijk personen die rechtspersonen vertegenwoordigen	De eisen betreffen hier de Authenticatiemiddelen die aan natuurlijke personen worden verstrekt. De vereisten voor uitgifte van Authenticatiemiddelen aan natuurlijke personen die rechtspersonen vertegenwoordigen worden in de volgende fase ingevuld.	Vanaf welke versie bevat de USvE eisen t.a.v. gebruik van authenticatiemiddelen om rechtspersonen te vertegenwoordigen?
25.	129	Actieve voorlichtingsrol MU	De Middelenuitgever MOET de Gebruiker aantoonbaar bekend maken met de voorwaarden voor het gebruik van het Authenticatiemiddel.	Zie ook opmerking bij punt 5 en 8: mag de voorlichting ook via de AD worden georganiseerd? Anders kan de burger in verwarring geraken bij wie hij terecht moet.
26.	132	Vereisten voor de verificatie van aangeleverde ID	Bij uitgifte 'Hoog': Het uitgeven van een middel op basis van een bestaand middel mag niet een volledig geautomatiseerd proces zijn. De validatie van het bezit van het middel MOET door een medewerker van de uitgever van het middel worden bevestigd, etc	De validatie van het bezit van een (privaat) middel uitgeven op 'Hoog' enkel obv een (publiek) middel 'Hoog' is dus niet toegestaan? Voor meer details: zie pagina 15 van de RDW-reactie op de consultatie.
27.	134	Initiële pincode beperkt geldig?	Als een activatiecode wordt verstrekt MOET de bruikbaarheid daarvan beperkt zijn in tijd.	Wordt met een activatiecode gelijkgesteld een initiële pincode?
28.	134	Activatiemoment bij AD mag later in de tijd liggen dan uitreiking middel.	In het geval de rollen van Middelenuitgever en Authenticatiedienst door afzonderlijke Participanten worden vervuld kan het proces van uitgifte van het middel gescheiden zijn van het proces activatie bij de Authenticatiedienst.	Niettemin moet een burger gezien punt 27 mogelijk toch direct activeren als hij een nieuw WID krijgt uitgereikt, wil zijn ten tijde van uitreiking tevens toegezonden initiële PIN niet al 'verlopen' zijn op het moment dat hij behoefte heeft aan gebruik.
29.	134	Eisen t.a.v. uitgifte van beide authenticatiefactoren bij 'Hoog'	De Middelenuitgever MOET de authenticatiefactoren afzonderlijk verstrekken via gescheiden kanalen of gescheiden in tijd. De verstrekking aan de Gebruiker MOET plaatsvinden met eenzelfde betrouwbaarheid als het identificatieproces voor Betrouwbaarheidsniveau Hoog.	Wat wordt met de 2° zin bedoeld in relatie tot de 1° zin? Moeten beide factoren, naast de vereisten in de 1° zin, ook persoonlijk, met ID-vaststelling, worden verstrekt? M.a.w.: een pinbrief mag niet per post?
30.	136	Verificatie minimaal eens per 5 jaar	De Middelenuitgever MOET minimaal 1 maal per 5 jaar de juistheid verifiëren van de geregistreerde Persoonsidentificatiegegevens van de gebruiker.	Wat houdt die verificatie op juistheid in? Is met een dagelijkse synchronisatie met de persoonsgegevens in BPR hieraan voldaan of wordt op iets anders gedoeld?



Nnr	Blz	Onderwerp	Wat zegt de USVe	Reactie RDW
31.	138	Benaderen middel via hetzelfde device als via welke het middel wordt benaderd	Het authenticatiemechanisme MOET een betrouwbaar kanaal bevatten voor notificatie van de inlogpoging van de gebruiker en de bevestiging van het authenticatieverzoek door de Gebruiker. Deze notificatie geeft de Gebruiker aan dat deze op het punt staat in te loggen op een specifieke Dienstverlener en, indien van toepassing, een specifieke door de Dienstverlener geregistreerde Dienst. De Gebruiker MOET in staat gesteld worden om met deze informatie het inloggen af te breken. Het kanaal MOET ook betrouwbaar zijn als applicatie waarvoor de authenticatie bestemd is of het platform waarop deze applicatie actief is, gecorrumpereerd is.	Hoe moet dit worden gelezen. Graag meer toelichting. Denk aan de voorziene werking publiek eID-middel via kanalen smartphone en (usb-)kaartlezer: Voldoet dit straks aan deze vereisten? Zowel in de situatie dat een Gebruiker een Dienstverlener met zijn computer benadert als met zijn smartphone?

4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28  
29  
30  
31  
32  
33  
34  
35  
36  
37  
38  
39  
40  
41  
42  
43  
44  
45  
46  
47  
48  
49  
50



## D. Voorbeelden van zakelijke portaaldiensten op rdw.nl

RDW Zakelijk

Loggen zakelijk Over RDW Pers Contact Informatie in English Onderhoud en storingen Online lijst

Zakelijke diensten

Print deze pagina

### Producten en diensten

#### Meest geraadpleegde diensten

<p><b>APK afmelden (via APK Webdirect)</b> Gebruik deze dienst om voertuigen af te melden voor de APK. <a href="#">Meer informatie</a></p>	<p><b>Digitaal vrijwaringsbewijs</b> Gebruik deze dienst om een digitaal vrijwaringsbewijs te downloaden. <a href="#">Meer informatie</a></p>	<p><b>Tijdelijk documentnummer en tennaamstellingscode aanvragen</b> Gebruik deze dienst om een tijdelijk documentnummer met tennaamstellingscode aan te vragen. <a href="#">Meer informatie</a></p>
--	---	--

<p><b>Op naam zetten/vrijwaren</b></p> <p><b><u>Demontagecode aanvragen door overheidsinstantie of demontagebedrijf</u></b> Gebruik deze dienst om een demontagecode aan te vragen als u een voertuig wilt slopen maar het kentekenbewijs is niet compleet. <a href="#">Meer informatie</a></p> <p><b><u>Demontagecode aanvragen met RDW-certificaat</u></b> Gebruik deze dienst om een demontagecode aan te vragen als u een voertuig wilt laten slopen en u heeft het kentekenbewijs niet meer. <a href="#">Meer informatie</a></p> <p><b><u>Digitaal machtigen</u></b> Gebruik deze dienst om een digitale machtiging aan te vragen. <a href="#">Meer informatie</a></p> <p><b><u>Eenmalig machtigen</u></b> Gebruik deze dienst om een eenmalige machtiging in te vullen en af te drukken. <a href="#">Meer informatie</a></p> <p><b><u>Online registratie bedrijfsvoorraad</u></b> Gebruik deze dienst om voertuigen in uw bedrijfsvoorraad te zetten of om over te schrijven tussen verschillende bedrijfsvoorraden. <a href="#">Meer informatie</a></p> <p><b><u>Tennaamstelling Voertuigen</u></b> Gebruik deze dienst om voertuigen uit uw bedrijfsvoorraad op naam van een particulier of rechtspersoon te zetten. <a href="#">Meer informatie</a></p> <p><b><u>Tijdelijk documentnummer en tennaamstellingscode aanvragen</u></b> Gebruik deze dienst om een tijdelijk documentnummer met tennaamstellingscode aan te vragen. <a href="#">Meer informatie</a></p>	<p><b>Controleren</b></p> <p><b><u>Documentnummer controleren</u></b> Gebruik deze dienst om aan de hand van het documentnummer te kijken of het kentekenbewijs geldig is. <a href="#">Meer informatie</a></p> <p><b><u>Documentnummer en tennaamstellingscode controleren</u></b> Gebruik deze dienst als u twijfelt of u het juiste kentekenbewijs bij de juiste tennaamstellingscode heeft of andersom. <a href="#">Meer informatie</a></p> <p><b><u>Online leermodule legitimatiemiddelen controleren</u></b> Gebruik deze module om te leren hoe u de echtheid en geldigheid van legitimatiebewijzen kunt controleren. <a href="#">Meer informatie</a></p> <p><b><u>Rijbewijscontrole</u></b> Gebruik deze dienst om te controleren of een rijbewijs een geldig identificatiemiddel is. <a href="#">Meer informatie</a></p>	<p><b>Raadplegen</b></p> <p><b><u>Bedrijfsgegevens wijzigen</u></b> Gebruik deze dienst om uw bedrijfsgegevens te controleren en/of te wijzigen. <a href="#">Meer informatie</a></p> <p><b><u>Bedrijfsvoorraad opvragen</u></b> Gebruik deze dienst om een overzicht van de voertuigen in uw bedrijfsvoorraad op te vragen. <a href="#">Meer informatie</a></p> <p><b><u>Informatie verzekeringsregister voor verzekeringsmaatschappijen</u></b> Gebruik als verzekeringsmaatschappij deze dienst om online wijzigingen door te geven aan de RDW. <a href="#">Meer informatie</a></p> <p><b><u>Tellerrapport uitgebreid - erkenninghouder</u></b> Gebruik deze dienst om als erkenninghouder Tellerrapporten uitgebreid aan te vragen van de voertuigen in uw bedrijfsvoorraad. <a href="#">Meer informatie</a></p> <p><b><u>Tellerrapport uitgebreid - zakelijke eigenaar van een voertuig</u></b> Gebruik deze dienst om een uitgebreid overzicht op te vragen van de geregistreerde gegevens van een voertuig, inclusief tellerstanden. <a href="#">Meer informatie</a></p> <p><b><u>Voertuiggegevens raadplegen</u></b> Gebruik deze dienst om grote hoeveelheden gegevens tegen betaling op te vragen. <a href="#">Meer informatie</a></p>
--	--	---



B rdw.nl

**Diensten voor  
leasemaatschappijen****Opdracht tot tenaamstelling  
opvoeren**

Gebruik deze dienst om als leasemaatschappij een opdracht tot tenaamstelling op te voeren.

[Meer informatie](#)

**Opdracht tot tenaamstelling  
wijzigen**

Gebruik deze dienst om als leasemaatschappij een opdracht tot tenaamstelling te wijzigen.

[Meer informatie](#)

**RTL**

Gebruik deze dienst om gegevens t.a.v. lease of financiering door te geven aan de RDW.

[Meer informatie](#)

**Tenaamstellingscode aanvragen**

Gebruik deze dienst om als leasemaatschappij een tenaamstellingscode aan te vragen voor voertuigen waar u verantwoordelijk voor bent.

[Meer informatie](#)

**Verstrekkingsvoorbehoud  
opvoeren**

Gebruik deze dienst om als leasemaatschappij een verstrekkingsvoorbehoud op te voeren bij een kenteken.

[Meer informatie](#)

**Verstrekkingsvoorbehoud  
verwijderen**

Gebruik deze dienst om als leasemaatschappij een verstrekkingsvoorbehoud bij een kenteken te verwijderen.

[Meer informatie](#)

**Tellerstanden****Eerdere tellerstanden corrigeren**

Is de tellerstand onjuist, maar is dit niet de laatste geregistreerde stand? Dan kunt u hierna de RDW een correctieverzoek indienen.

[Meer informatie](#)

**Laatste tellerstand corrigeren**

Gebruik deze dienst om de laatste geregistreerde tellerstand die u zelf heeft ingevoerd, te corrigeren.

[Meer informatie](#)

**Tellerrapport aanvragen**

Gebruik deze dienst als u een (nieuw) tellerrapport wilt aanvragen (en uw provider is niet A2SP, RDC of VWE).

[Meer informatie](#)

**Tellerstand controleren**

Gebruik deze dienst om het oordeel over de reeks tellerstanden te bekijken.

[Meer informatie](#)

**Tellerstand corrigeren**

U kunt op deze pagina uw verkeerd geregistreerde tellerstanden (laten) corrigeren.

[Meer informatie](#)

**Tellerstand registreren**

Gebruik deze dienst om de tellerstand van personenauto's en lichte bedrijfsauto's op te voeren.

**Een auto van de zaak schorsen,  
verlengen of beëindigen****Schorsing beëindigen met uw  
eHerkenning**

Gebruik deze dienst als u de schorsing van uw voertuig wilt opheffen met eHerkenning.

[Meer informatie](#)

**Schorsing beëindigen met uw  
RDW-certificaat**

Gebruik deze dienst als u de schorsing van uw voertuig wilt opheffen.

[Meer informatie](#)

**Voertuig van de zaak schorsen of  
schorsing verlengen met  
certificaat**

Gebruik deze dienst om uw voertuig van de zaak tijdelijk te schorsen met uw RDW-certificaat.

[Meer informatie](#)

**Voertuig van de zaak schorsen of  
verlengen met eHerkenning**

Gebruik deze dienst om uw voertuig van de zaak tijdelijk te schorsen met eHerkenning.

[Meer informatie](#)

**Voertuig keuren bij de RDW****Eendagskentekenbewijs aanvragen**

Als u een voertuig laat keuren bij de RDW, dan heeft u mogelijk een eendagskentekenbewijs nodig.

[Meer informatie](#)

**Keuringsafpraak aan huis maken**

Gebruik deze dienst om een keuringsafpraak 'aan huis te maken'.

[Meer informatie](#)

**Keuringsafpraak maken**

Gebruik deze dienst om voor een of meerdere voertuigen een afspraak te maken voor een keuring of een combinatie van keuringsproducten bij de RDW.

[Meer informatie](#)

**Machtigen bij tenaamstelling op  
keuringsstation**

Gebruik deze machtigingsformulieren bij tenaamstelling op het keuringsstation.

[Meer informatie](#)

**Diensten rond het kentekenbewijs****Nieuw kentekenbewijs aanvragen  
voor voertuigen op naam van uw  
bedrijf**

Gebruik deze dienst om een nieuw kentekenbewijs en/of tenaamstellingscode aan te vragen als u dit/deze kwijt bent.

[Meer informatie](#)

**Kentekenbewijs voor voertuig in  
bedrijfsvoorraad aanvragen**

Gebruik deze dienst om een kentekencard aan te vragen als u een voertuig in uw bedrijfsvoorraad heeft staan waar geen kentekenbewijs (meer) bij zit.

[Meer informatie](#)

**Aanvragen kentekenbewijzen deel  
II**

Gebruik deze dienst om kentekenbewijzen deel II te bestellen bij de RDW.

[Meer informatie](#)

**Eendagskentekenbewijs aanvragen**

Als u een voertuig laat keuren bij de RDW, dan heeft u mogelijk een eendagskentekenbewijs nodig.

[Meer informatie](#)

**WebVKR**

Een inschrijving aanvragen voor een nieuw en ongebruikt voertuig op basis van een CvO (Certificaat van Overeenstemming).

[Meer informatie](#)

10-11-16 10:52:14  
Raad van Bestuur



Datum  
28 maart 2017

Orderwerp  
Consultatie Wet GDI

Behandeld door  
[Redacted]

Contactgegevens  
[Redacted]

Uw kenmerk  
2016-0000798041

Blad  
1 van 6

Postretouradres  
Postbus 9046, 7300 GH Apeldoorn

Ministerie van Binnenlandse Zaken en  
Koninkrijksrelaties  
Directie Informatiesamenleving en Overheid  
[Redacted]

Postbus 20011  
2500 EA DEN HAAG

Tevens per mail: [SupportOfficeEid@minbzk.nl](mailto:SupportOfficeEid@minbzk.nl)

Geachte heer Prinsen,

Dank voor uw brief van 23 december 2016 waarin u ons de gelegenheid biedt te reageren op de concept tekst van de Wet generieke digitale infrastructuur (hierna: Wet GDI). De concept tekst hebben we bestudeerd en bij een aantal wetsartikelen hebben we suggesties en/of vragen die hierna worden benoemd. Tevens gaan we in op de vragen die zijn gesteld in het format Uitvoerbaarheid- en handhaafbaarheidstoets Wet GDI. Onze reactie op de vragen is in de bijlage verwerkt.

#### Opmerkingen wetsartikelen

##### Artikel 2 Standaarden

In het tweede lid van artikel 2 staat dat bij Algemene maatregel van bestuur een standaard (dwingend) kan worden aangewezen. In de toelichting staat dat bij het gebruik van deze bevoegdheid een zorgvuldig en transparant proces wordt doorlopen en wordt verwezen naar de reeds ingerichte en beproefde procedure voor plaatsing op de 'pas-toe-of-leg-uit' lijst. Het Kadaster zou ervoor willen pleiten dat de genoemde, reeds ingerichte, procedure meer waarborgen gaat bieden zodat het proces van vaststellen van een standaard volledig transparant gaat plaatsvinden waarbij ook voor de bestuursorganen die het aangaan voldoende inspraakmogelijkheden zijn ingebouwd alvorens een advies aan de minister wordt gegeven. In het bijzonder wil het Kadaster aandacht vragen voor standaarden in relatie tot geo-informatie aangezien huidige standaarden op de 'pas-toe-of-leg-uit' lijst niet altijd toepasbaar zijn op geo-informatie<sup>1</sup> Het is noodzakelijk om bij het vaststellen van het functionele en organisatorische toepassingsbereik hiermee rekening te houden en de benodigde expertise vanuit de geo-informatie sector te betrekken.

<sup>1</sup> Bijv. de Webrichtlijnen die voor een belangrijk deel niet toepasbaar zijn op kaartviewers. Dit is bekend, maar moet in het proces ook goed vastgelegd worden. Hetzelfde geldt voor het leveren van geodata, waar het Kadaster OGC webservices gebruikt in plaats van de overheidsstandaard webservices.

Bezoekadres  
Hofstraat 110,  
7311 KZ Apeldoorn

kadaster



Daarnaast wil het Kadaster aandacht vragen voor het feit dat de (dwingende) aanwijzing bij Algemene maatregel van bestuur slechts het overheidsdomein betreft. Veel van de afnemers van het Kadaster komen uit het private domein en herkennen zich niet in die standaarden en vinden deze al snel verouderd. Dit dwingt het Kadaster tot het investeren in dubbele oplossingen: marktconform<sup>2</sup> (meestal open standaarden, soms proprietary) en overheidsstandaarden. Voor wat betreft deze overheidsstandaarden zou het Kadaster ervoor willen pleiten dat deze zich zoveel als mogelijk conformeren aan open (wereld)standaarden en marktstandaarden.

#### Artikel 5 Acceptatieplicht

Het Kadaster wil in het kader van de acceptatieplicht nadrukkelijk wijzen op het volgende. In het proces van het (digitaal) aanleveren van akten (stukken) ter inschrijving in de openbare registers voor registergoederen wordt thans gewerkt met een elektronische handtekening die is gebaseerd op een gekwalificeerd certificaat, genoemd in artikel 15a, tweede lid, onderdelen a tot en met f, van Boek 3 van het Burgerlijk Wetboek. Dit is vastgelegd in artikel 7e van de Kadasterwet. Voor dit hoge betrouwbaarheidsniveau in het vastgoedverkeer is gekozen zodat de elektronische handtekening eenzelfde bewijskracht heeft als de handgeschreven handtekening aangezien de inschrijving van bepaalde stukken in de openbare registers een constitutioneel vereiste is voor het intreden van het rechtsgevolg. Het Kadaster wil ervoor pleiten dat de bestaande elektronische handtekening die reeds gebruikt wordt in het proces van elektronisch aanleveren van akten, gehandhaafd blijft cq na inwerkingtreding van de Wet GDI gebruikt mag blijven worden, een en ander zoals verwoord in artikel 7e van de Kadasterwet. Reden hiervoor is dat volledige aanpassing van dit elektronische proces van aanleveren hoge kosten met zich mee zal brengen die voor een groot deel voor rekening zal komen van private partijen. Het Kadaster onderkent wel dat op termijn andere authenticatiemiddelen, dan de nu gehanteerde elektronisch handtekening, geïntroduceerd zouden moeten kunnen worden voor inschrijving van stukken in de openbare registers. Het Kadaster pleit er dan ook voor dat het genoemde artikel 7e van de Kadasterwet wordt aangepast, in de zin dat per categorie stukken kan worden bepaald (bijv. middels een ministeriele regeling) welk authenticatiemiddel met een substantieel of hoog betrouwbaarheidsniveau noodzakelijk is ter inschrijving in de openbare registers. Hierdoor zal op termijn, in ieder geval ook voor een deel van de stukken die ingeschreven dient te worden in de openbare registers, een overeenkomstig de Wet GDI erkend authenticatiemiddel gebruikt kunnen gaan worden.

In het verlengde van het voorgaande wil het Kadaster opmerken dat in het vijfde lid van artikel 5 staat dat bestuursorganen met inachtneming van bij ministeriele regeling te stellen regels dienen te bepalen voor welke elektronische diensten tenminste het betrouwbaarheidsniveau substantieel of hoog heeft te gelden. Aangezien de regels die hierover gesteld gaan worden nog niet bekend zijn, is het voor het Kadaster lastig inschatten wat de impact hiervan zal zijn cq welke dienstverlening van het Kadaster straks ook onder de werking van de Wet GDI gaat vallen. Daarnaast is niet duidelijk in de concepttekst, noch in de toelichting in hoeverre een bestuursorgaan of aangewezen organisatie nog de vrijheid heeft om af te wijken van de te stellen regels. Volgens het Kadaster dient duidelijk(er) te worden toegelicht hoe dwingend de te stellen regels zullen gaan gelden, dan wel in hoeverre bestuursorganen en aangewezen organisaties keuzevrijheid behouden.

<sup>2</sup> Private partijen vragen en gebruiken bijv. al lang REST services in plaats van SOAP/WUS.

Datum  
28 maart 2017

Onderwerp  
Consultatie Wet GDI

Blad  
3 van 6

#### Artikel 6 Erkenning

In het derde lid van artikel 6 staat dat er ontsluitende diensten zullen worden erkend. Het is vooralsnog niet de verwachting dat de ontsluitende diensten ieder erkend middel van iedere erkende authenticatiedienst zullen ontsluiten. Dit betekent dat het Kadaster met meer dan één ontsluitende dienst zal moeten contracteren en in technische zin met meer dan een koppelvlak rekening zal moeten houden, hetgeen hogere kosten met zich mee zal brengen. Het Kadaster zou graag ervoor willen pleiten dat in de komende tijd door BZK de nodige stimuleringsmaatregelen worden getroffen zodat op het moment van inwerkingtreding van de Wet GDI er door de minister erkende ontsluitende diensten zijn die ieder voor zich alle erkende middelen van iedere erkende authenticatiedienst ontsluiten.

#### Artikel 15 en 16 Meldplicht en informatieverstrekking

Het tweede lid van artikel 15 introduceert een meldplicht voor inbreuken op de beveiliging of de integriteit van een elektronische dienst of van misbruik of oneigenlijk gebruik van de toegang tot de elektronische dienstverlening. In de toelichting wordt aangegeven dat deze (nieuwe) meldplicht moet worden onderscheiden van de meldplicht inzake art. 34a Wet bescherming persoonsgegevens, maar ook van de meldplicht inzake art. 18.15a van de Telecommunicatiewet en de meldplicht op grond van de (komende) Wet gegevensverwerking en meldplicht cybersecurity. Het Kadaster pleit ervoor dat de diverse meldplichten zoveel als mogelijk worden geharmoniseerd, althans dat, waar mogelijk, de verschillende meldprocedures/protocollen op elkaar worden afgestemd, aangezien bestuursorganen al snel met twee of meer van de genoemde meldplichten te maken zullen of kunnen krijgen.

Daarnaast volgt uit de toelichting van het tweede lid van artikel 15, niet duidelijk welke informatie door bestuursorganen en aangewezen organisaties moeten worden verstrekt aan de minister ingeval sprake is van een inbreuk op de beveiliging of de integriteit van zijn elektronische dienstverlening of van misbruik of oneigenlijk gebruik van de toegang tot elektronische dienstverlening. De toelichting spreekt over 'alle benodigde' informatie. Kan dit per situatie verschillend zijn of zou op dit punt niet nog uitvoeringsregels moeten worden opgesteld over welke informatie dan verstrekt moet worden? Een verduidelijking op dit punt is wenselijk. Dit geldt in zekere zin ook voor artikel 16, eerste lid waarin bestuursorganen en aangewezen organisaties ook een verplichting opgelegd krijgen om desgevraagd 'de gegevens en inlichtingen' te verstrekken aan de minister die nodig zijn om compromittering van de veilige en betrouwbare toegang tot elektronische dienstverlening te voorkomen of te beëindigen. Ook bij deze verplichting rijst de vraag om welke gegevens en inlichtingen het gaat/kan gaan, of dit per situatie verschillend kan zijn en of ook voor deze informatieplicht niet nog nadere uitvoeringsregels zouden moeten worden opgesteld.

Mochten er nog vragen zijn naar aanleiding van bovenstaande toelichting of de reactie op de Uitvoerbaarheid- en handhaafbaarheidstoets, dan vernemen we die uiteraard graag.

Met vriendelijke groet,



kadaster

## Bijlage vragen Uitvoerbaarheid en Handhaafbaarheid

### Dienst voor het kadaster en de openbare registers

#### 1. Uitvoerbaarheid

a. Vraag voor departementen: Welke organisaties op uw beleidsdomeinen dienen de wet na te leven?

- Geef aan welke onder uw departement ressorterende uitvoeringsorganisaties de Wet GDI gaan uitvoeren (a-bestuursorganen).

- Geef aan welke andere (categorieën van) organisaties onder de reikwijdte van de Wet GDI moeten vallen (zie art. 3 lid 2 Wgdi).

b. Is het de organisatie(s) helder wat de opgedragen taak is?

*Ja, in hoofdzaak: het accepteren van alle erkende middelen.*

- Geef daarbij ook aan of er taken of verplichtingen zijn die voor een correcte uitvoering c.q. naleving verduidelijking behoeven.

*Zie opmerkingen hiervoor inzake de gewenste verduidelijking van een aantal artikelen van de wet.*

c. Zijn/ is de uitvoerende organisatie(s) voldoende toegerust voor een doeltreffende uitvoering?

*Ja, er van uitgaande dat de regels die in lagere regelgeving zullen worden vastgelegd aansluiten bij de huidige processen cq gangbare standaarden/protocollen. Zie bijv. in het kader van art. 8, eerste lid met betrekking tot aanvullende regels over beveiliging. Het beveiligingsbeleid van het Kadaster is gebaseerd op de Baseline Informatiebeveiliging Rijk (BIR) en als in de lagere regels hierop wordt aangesloten dan zal het Kadaster voldoende toegerust zijn om hiaraan doeltreffend uitvoering te geven. Dit geldt bijv. ook voor de regels met betrekking tot de onafhankelijke audit (dit gebeurt nu voor de DigiD aansluiting door een onafhankelijke EDP auditor).*

- Geef aan of er voldoende capaciteit is, of dat de uitvoering verschuiving van prioriteiten of andere maatregelen vergt.

*Dit is een aandachtspunt voor het Kadaster. Implementatie van de Wet GDI zal het nodige vragen.*

- Geef aan of uw organisatie op het gebied van de ICT voldoende is toegerust. Geef ook aan of voldoende helder is wat de uitvoering van de automatisering vraagt.

*Projecten zijn in wording om al deels gerealiseerd te worden. Nb: Webrichtlijnen worden hierin meegenomen. Zorgpunt hierbij is wel of straks sprake zal/kan zijn van één koppelvak.*

- Geef aan in hoeverre de voor de uitvoering benodigde werkprocessen voorhanden zijn.

d. Wat zijn de verwachte effecten van de ontwerpwet voor uw organisatie of departement?

- Geef aan wat de effecten van de ontwerpwet zijn op de digitale dienstverlening aan de burger en ondernemer.

*De Wet GDI zal nagenoeg alle digitale dienstverlening van het Kadaster richting burgers en bedrijven (kunnen) raken. Tevens als digitale dienstverlening richting overheden. Probleem daarbij is dat eisen aan ontsluiting naar overheden afwijken aan de vraag van private partijen. Private partijen hebben ook geen toegang tot kanalen die wij voor overheid moeten gebruiken, waardoor organisaties als Kadaster, die in het publieke en private domein opereren, voor dubbele investeringen komen te staan.*

- Geef aan welke producten of processen door de Wet GDI geraakt worden en wat de voordelen en nadelen van de ontwerpwet zijn.
- Het portaal *Mijn Kadaster* (toegang tot diverse digitale producten en diensten van het Kadaster) werkt nu nog met een usemame en password en zal mede naar aanleiding van de onderhavige wet worden aangepast;
- *Ruimtelijkeplannen.nl* wordt geraakt indien het gebruik van *https* verplicht wordt gesteld; deze dienst wordt hierdoor met name geraakt doordat alle bronhouders van *Ruimtelijkeplannen* eveneens van *https* gebruik moeten maken. Deze bronhouders moeten hierdoor hun gehele planvoorraad herzien, zowel bij hen zelf als op *Ruimtelijkeplannen*. De reden hiervan is dat alle bronhouders conform Wro verplicht gebruik moeten maken van documenten waarin de exacte bronlocaties vermeld staan, inclusief *http* of *https*. Hierdoor moet ca. 90% van de huidige planvoorraad (resultierend in ca. 55.000 plannen van ca. 380 bronhouders) opnieuw verwerkt worden;
- Voor digitale inzage op de Basisregistratie kadaster cq toegang en afname diverse producten uit de Basisregistratie kadaster; en tevens van toepassing op digitale indiening klachten en bezwaren en de scheepsboekhouding;
- Aanleveren gegevens Basisregistratie grootschalige topografie door bronhouders zal geraakt gaan worden. Wanneer PKI-overheid certificaten de status van erkend middel krijgen dan zou de distributie van beeldmateriaal onder de werking van de wet GDI kunnen vallen;
- Voor het berichtenverkeer met bronhouders in het kader van de Basisregistratie adressen en gebouwen (BAG) en de Basisregistratie WOZ, voor bevragingen door afnemers van BAG en WOZ en afname van producten BAG, worden PKI-overheid certificaten gebruikt en zouden mogelijk onder de Wet GDI kunnen vallen;
- Aanmelden voor de KLIC-dienstverlening zal onder de werking van de wet GDI komen te vallen (voor ca. 95% van de professionele gebruikers in Nederland). Voor ca. 5% van de incidentele gebruikers zal de e-IDAS Verordening van toepassing zijn.
- Geef aan of er ook mogelijke neven- en onvoorziene of onbedoelde effecten zijn.

Zie bovenstaand bij *Ruimtelijkeplannen.nl*, namelijk dat alle bronhouders hun planvoorraden moeten herzien met alle gevolgen van dien.

e. Wat zijn de gevolgen van de acceptatieplicht van de erkende middelen?

- Geef aan wat de gevolgen van de acceptatieplicht zijn, mede in relatie tot interoperabiliteit, tarifiering, de uitfasering van DigiD-laag/basis en de ambitie om bestuursorganen en aangewezen organisaties zo eenvoudig mogelijk aan te kunnen laten sluiten op de diverse erkende authenticatiemiddelen.

*Het gebruik van de erkende middelen cq deze toepassen op de digitale dienstverlening kan in sommige gevallen drempelverhogend werken. Dit zal op termijn wel overgaan omdat e.o.a. gewenning wordt, maar het zou in beginsel belemmerend kunnen werken om met zwaardere inlogmiddelen te moeten werken (waar nu bijv. password en usemame al voldoende is).*

f. Wat zijn de ingeschatte kosten die nodig zijn voor uitvoering van de wet voor uw organisaties of departement?

*Op dit moment is hiervoor nog geen bedrag te noemen. De kosten zullen in ieder geval zien op IT-kosten, maar ook kosten voor communicatie en support. Daarnaast zullen maatschappelijke kosten ontstaan aangezien tienduizenden (private) klanten gebruik maken van onze diensten, online, via webservices of via download. Zij moeten hun processen en vaak ook hun systemen aanpassen.*

Datum  
28 maart 2017

Orderaap  
Consultatie Wet GDI

Blad  
6 van 6

- Geef aan om welke type kosten (directe/indirecte kosten?) het gaat en of het eenmalige of structurele kosten zijn.

*Dit betreffen eenmalige IT-kosten die zien op met name systeemtoegangs wijzigingen aan de zijde van het Kadaster. Daarnaast zullen de maatschappelijke kosten aanzienlijk zijn (zowel eenmalige als jaarlijks beheer).*

- Geef aan waarop de inschatting is gebaseerd en of de kosten als proportioneel kunnen worden beschouwd.

*De vraag is of de voorziene maatschappelijke kosten proportioneel zullen zijn. NB: Ons inziens zouden deze kosten aanzienlijk verminderd kunnen worden wanneer private partijen naar eigen keuze voor eenvoudige raadplegingen van onze openbare registraties ook gebruik mogen blijven maken van bestaande authenticatie (user-id wachtwoord).*

## 2. Handhaafbaarheid

a. Vraag voor departementen: Welke organisaties of organisatieonderdelen zullen toezicht houden op een correcte uitvoering van de wet?

- Geef voor uw departement aan welke organisatie of organisatieonderdeel toezicht houdt op de naleving van de Wet GDI (inz. de artt. 5,8 en 16).

b. Wat is het oordeel van de toezichthoudende organisaties (of organisatieonderdelen) over de uitvoerbaarheid en handhaafbaarheid?

- Geef daarbij ook aan of er taken of verplichtingen zijn die voor een correcte uitvoering c.q. naleving verduidelijking behoeven.

*Zie hiervoor de opmerkingen inzake artikel 15 van de concept wettekst.*

- Geef aan of de toezichthoudende organisatie of organisatieonderdeel over voldoende kennis en/of capaciteit beschikt.

### **Inleiding**

De versie van de Wet GDI die momenteel ter (internet) consultatie voorligt, heeft nog veel kenmerken van een wet in wording. Dat komt doordat het een eerste tranche is en omdat veel lagere regelgeving en AMVB's nog moeten worden opgesteld. In diverse voorlichtingsbijeenkomsten die zijn geweest, geeft BZK ons ook de indruk dat de huidige versie van de wet een "openingsbod" is en dat de resultaten uit de consultatie de tekst nog ingrijpend kan wijzigen. Dit alles heeft gevolgen voor het inschatten van de impact van de Wet GDI op de uitvoering.

In deze notitie komen schetsen wij op hoofdlijnen de impact van deze eerste tranche, de belangrijkste issues die wij zien en doen wij een aanbeveling hoe deze op te lossen.

### **Impact**

Het bepalen van de impact van de Wet GDI is niet goed mogelijk omdat de volgende aspecten nog onzeker zijn.

- De invoering van eID-middelen. Het is, afgezien van de verplichting na toelating tot het stelsel, niet duidelijk hoeveel middelen straks moeten worden geaccepteerd.
- Realisatie invoering. Er zijn zorgen over voldoende expertise binnen organisaties en in de markt om de invoering te begeleiden.
- De kosten van het accepteren van eID-middelen. Het is niet duidelijk hoe de 'beprijzing' van de middelen eruit zal zien. Daardoor is ook onzeker op welke wijze organisaties kunnen sturen op de kosten.
- De lagere regelgeving. Naar verwachting zal juist die regelgeving (waaronder algemene maatregelen van bestuur) het meeste effect hebben op de uitvoering. Een complete bepaling van de impact, is dan ook pas mogelijk als al deze regels bekend zijn.
- Dekkingsgraad van de middelen. DigiD substantieel is bijvoorbeeld alleen beschikbaar voor Android, DigiD machtigen is voorlopig niet beschikbaar, er zijn geen middelen voor buitenlanders.
- Invoeringsmoment. Risico's als vele organisaties volgens eenzelfde tijdpad moeten invoeren, onduidelijkheid over de precieze relatie met eIDAS.

### **Belangrijke issues**

De volgende punten wegen op dit moment het zwaarst.

#### Scope / afbakening van de wet GDI:

- a. *Wat is ons gebleken:* De Wet GDI wordt opgesteld als een kaderwet. De 1<sup>e</sup> tranche is pas het begin. Deze tranche is nog niet tot het gaatje uitgewerkt, veel moet nog geregeld worden in lagere regelgeving en AMVB's.
- b. *Waarom is dit een issue:* De impact op de uitvoering kan nu alleen op hoofdlijnen worden geschetst. Juist die lagere regels gaan bepalen wat de uitvoeringsconsequenties precies zijn.

#### Scope / afbakening van de wet GDI:

- a. *Wat is ons gebleken:* De scope is nog niet helder. In de Q&A is aangegeven "de Wet GDI gaat ook over de online relatie organisatie-vertegenwoordiger (gemachtigde) richting overheid. Dus niet verkeer tussen machines sec. Er moet een bevoegde persoon achter de machine zitten". Echter, dit biedt nog geen duidelijkheid op het punt waar een eindgebruiker achter een computer zit en het dienstverlening betreft via ICT-systemen van derden waarin overheidsdiensten zijn geïntegreerd. En waarbij ook nog intermediairs zijn betrokken die een overeenkomst hebben met de overheid om in opdracht van eindgebruikers met de overheid te mogen communiceren. Dit is relevant voor bijvoorbeeld de Belastingdienst en de RDW.

- b. *Waarom is dit een issue:* Uitvoeringstoets/impactbepaling over de gehele keten is niet mogelijk zolang onduidelijk is of de verplichting dat enkel erkende authenticatiemiddelen mogen worden gebruikt, ook wordt opgelegd indien personen via derden van overheidsdiensten gebruikmaken. Onduidelijkheid, zowel bij overheden als intermediairs, als softwarehuizen als eindgebruikers. Bijvoorbeeld: een belangrijk deel van het volume aan RDW-dienstverlening wordt geleverd vanuit systemen van derden waar RDW-functionaliteit in is geïntegreerd. Waaronder dealermanagement-, werkplaats, lease- en verzekeringssystemen. Tussen die systemen en de RDW zitten vaak nog speciale intermediairs die toegevoegde waarde aan hun klanten leveren. Het hele stelsel staat onder in wet- en regelgeving en besluiten gereguleerd toezicht. Onduidelijk is nog welke verandering de wet vereist in deze constellatie. De RDW denkt op dit moment aan het overschakelen naar een andere eIDAS figuur voor de RDW-dienstverlening: het gebruik van geavanceerde zegels op basis van de bestaande RDW-certificaten. De figuur van zegels valt echter onder de Telecommunicatiewet en niet onder de wet GDI. Indien deze aannahme onjuist blijkt te zijn, is overgangstermijn van 5 jaar nodig.

#### Impact wet GDI op zakelijke dienstverleningsketens:

- a. *Wat is ons gebleken:* De impact op ketens is groot (zie hierboven). Implementatie is daardoor een majeure operatie: mogelijk moet het berichtenverkeer van zo'n eindgebruiker met een digitale, geavanceerde, handtekening of zegel worden ondertekend voordat het via software van derden naar de overheid wordt gestuurd.
- b. *Waarom is dit een issue:* Dit betekent voor zowel overheidspartijen als bedrijfsleven: verminderd draagvlak, hoge initiële investeringskosten door aanpassing van systemen, aanschaf meerdere middelen (daar waar nu via 1 authenticatiemiddel op naam van en bedrijf door tientallen medewerkers van een bedrijf wordt gecommuniceerd met een overheidsdienst, moet straks voor elke medewerker afzonderlijk een middel worden aangeschaft), machtigingslogistiek, beveiligingsvraagstukken e.d. Dat levert vraagtekens op voor de continuïteit van overheidsdienstverlening: Een 'big bang' per 1/1/2019 is niet verantwoord. Daarnaast is voor het eH4-niveau het middelenaanbod dusdanig eenzijdig (PKI-overheidscertificaat op smartcard) dat problemen kunnen worden verwacht voor omgevingen waar niet gewerkt kan worden met usb-smartcard readers. Er is nog maar 1 aanbieder die een alternatief biedt.

#### Effecten op uitvoering van wet GDI:

- a. *Wat is ons gebleken:* De verplichting om tot het stelsel toegelaten middelen te accepteren betekent dat met meerdere leveranciers en wellicht met nieuwe 'makelaars' contracten moeten worden afgesloten.
- b. *Waarom is dit een issue:* De (nog vast te stellen) bandbreedte voor tikprijzen en het ontbreken van de verplichting aan middenleveranciers/makelaars om ontsluiting van nieuw toegelaten middelen (ook) te regelen via bestaande makelaars, betekent dat dienstaanbieders:
- ter beperking van exploitatielasten noch kunnen sturen op volumes per middel, noch op de 'prijs per tik',
  - met hoge implementatiekosten geconfronteerd kunnen worden indien toelating van een nieuw middel betekent dat een nieuw koppelvlak moet worden geïmplementeerd.
- De facto spelen dienstaanbieders daardoor geen rol van betekenis in deze 'markt'.

#### Invoering wetGDI irt eIDAS verordening

- a. *Wat is ons gebleken:* De relatie tussen de wet GDI en eIDAS verordening is onduidelijk.
- b. *Waarom is dit een issue:* Het is onduidelijk wat precies wanneer wordt verwacht van uitvoeringsorganisaties.

### Invoering wetGDI irt eIDAS verordening

- a. *Wat is ons gebleken:* Organisaties moeten makelaars contracteren om het elektronisch verkeer tussen organisaties en erkende authenticatiediensten, machtigingsdiensten en attributiediensten te routeren. Een makelaar is niet verplicht om alle erkende diensten te faciliteren
- b. *Waarom is dit een issue:* Dit roept allerlei vragen op over of en hoe aanbestedingstrajecten georganiseerd moeten worden en aan welke eisen deze moeten voldoen. Het zou kunnen gaan om Europese aanbestedingen die over het algemeen intensief zijn en een lange doorlooptijd kennen. Vraag is ook of het beperkte aantal potentiële makelaars het te verwachte grote aantal aanbestedingen kan managen. Daarnaast leidt het inschakelen van dienstenaanbieders tot vraagstukken omtrent aansprakelijkheidsrisico's en de verwerking van persoonsgegevens (ook in relatie tot de AVG).

### **Onze aanbeveling**

Er moet een werkwijze worden gevonden waarmee bij het opstellen van lagere regelgeving rekening wordt gehouden met de uitvoerbaarheid. Dus: vooraf en tijdens dit proces werken beleid (opsteller van regelgeving) en vertegenwoordigers van de uitvoering samen. Op die manier vindt er continu een toets op uitvoerbaarheid plaats. De eerste stap in dit proces betreft het maken van afspraken over hoe deze samenwerking vorm kan krijgen. Het initiatief hiervoor ligt bij BZK.