MEMORIE VAN TOELICHTING

I Algemeen

1. Inleiding

1.1. Aanleiding

Nederland digitaliseert. Steeds meer diensten worden via online transacties geleverd. Ook de overheid moet moderniseren en gaat mee in deze ontwikkeling. Hiervoor is de ontwikkeling van generieke digitale voorzieningen in een gemeenschappelijke infrastructuur van de overheid noodzakelijk. Maar zolang afzonderlijke overheidsonderdelen bij de inzet van ICT in relatief isolement hun eigen weg gaan, blijft de overheid op achterstand. Duidelijk is geworden dat het vrijwel onmogelijk is om alleen op basis van bestuursakkoorden tot de gewenste modernisering te komen.
Er is vooruitgang geboekt, maar er wordt nog niet voldoende tempo gemaakt. Dit wetsvoorstel biedt op twee punten steviger sturing. Ten eerste bevat het de mogelijkheid tot het verplicht stellen van open standaarden[1] en ten tweede bevat het generieke regels over elektronische authenticatie door burgers en ondernemers bij hun transacties met de overheid.

1.2. Verplichten van open standaarden

Het wetsvoorstel bevat een grondslag om bij algemene maatregel van bestuur open standaarden aan te wijzen die overheden dienen te hanteren in het elektronisch verkeer met andere overheden, met burgers en met bedrijven. Deze aanwijzing zal plaatsvinden indien dit noodzakelijk en proportioneel is gelet op de goede werking, veiligheid, betrouwbaarheid of de doelmatigheid van het elektronisch verkeer, of dit voortvloeit uit verdragen of besluiten van volkenrechtelijke organisaties. Alhoewel in de praktijk in dit verkeer reeds veelvuldig van deze open standaarden gebruik wordt gemaakt en hierover ook instructies en afspraken bestaan, acht de regering het, nu thans de mogelijkheid bestaat om van deze standaarden af te wijken gewenst dat de overheden in bepaalde gevallen verplicht kunnen worden om deze standaarden te gebruiken.

1.3. Verplichte aansluiting op eID

Voor de verdere ontwikkeling van het digitale verkeer met bestuursorganen is het noodzakelijk om betrouwbare en veilige elektronische identificatie (eID) te hebben waarmee veilige en betrouwbare toegang tot alle digitale diensten van bestuursorganen mogelijk is. Dit wetsvoorstel bevat de wettelijke randvoorwaarden waarmee deze digitale toegang tot alle bestuursorganen, dus generiek, wordt ingericht. Een stelsel waarop bestuursorganen verplicht dienen aan te sluiten en waarin door zowel burgers als ondernemers in het verkeer met bestuursorganen verschillende publieke en private middelen voor authenticatie[2] op een voldoende hoog betrouwbaarheidsniveau naast elkaar kunnen worden gebruikt.[3] De verplichte aansluiting geldt niet alleen voor bestuursorganen, maar ook voor daartoe aangewezen[4] private organisaties die elektronische diensten verlenen aan burgers of ondernemers waarvoor een veilige en betrouwbare authenticatie essentieel is, zoals bij zorgverzekeraars en pensioenuitvoerders. De bestuursorganen en aangewezen organisaties zullen in het vervolg van deze memorie van toelichting gezamenlijk worden aangeduid als publieke dienstverleners, en het domein waar zij hun diensten aanbieden als het publieke domein.

---

[1] Onder 'open standaard' wordt verstaan: Een afspraak die is vastgelegd in een specificatiedocument dat vrij te verkrijgen (open) is. Om gegevens uit te kunnen wisselen moeten ICT-systemen dezelfde standaard hebben geïmplementeerd.
[2] Onder 'authenticatie' wordt in deze wet verstaan: elektronisch proces voor de verificatie en bevestiging van de identiteit van een natuurlijke persoon of rechtspersoon.
[3] Zie visiebrief digitale overheid 2017 van 23 mei 2013, Kamerstukken II 2012/13, 26 643, nr. 280.
[4] De aanwijzing vindt plaats door middel van opname in de bijlage bij het wetsvoorstel of door middel van aanwijzing bij besluit van de minister van Binnenlandse Zaken en Koninkrijksrelaties en de betrokken vakminister.

Bij brief van 14 december 2015 heb ik de Tweede Kamer toegezegd de regelgeving voor de authenticatiemiddelen die gebruikt kunnen worden in het publieke domein onder één stelsel te brengen: wettelijke eisen waaraan alle publieke en private authenticatiemiddelen moeten voldoen, alsook waaraan alle betrokken partijen moeten voldoen.[5] De wettelijke eisen zullen, volgens de brief, onderdeel uitmaken van de Wet generieke digitale infrastructuur (Wet GDI). In de brief heb ik de Tweede Kamer ook meegedeeld dat – in overleg met de minister van Economische Zaken (EZ) en de Staatssecretaris van Financiën – is vastgesteld dat de verantwoordelijkheid voor dit publieke stelsel bij de minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) ligt.

1.4. Elektronische authenticatie

Bij veel digitale contacten met publieke dienstverleners wordt vertrouwelijke informatie (waaronder persoonsgegevens) uitgewisseld tussen deze dienstverlener en de burger of het bedrijf. Voordat de dienstverlener dergelijke informatie kan vrijgeven, moet met voldoende mate van zekerheid worden vastgesteld aan wie die informatie wordt verstrekt. Hetzelfde geldt voor het door de dienstverlener verwerken van aangeleverde informatie: niet iedereen mag informatie betreffende een burger of bedrijf aanleveren. Dit vereist dus adequate identificatie en authenticatie voor het verlenen van toegang tot gepersonaliseerde informatie.

Met het toenemen van de digitale dienstverlening van de publieke dienstverleners wordt het noodzakelijk om de methode van authenticatie ook in de toekomst goed geborgd te hebben. De authenticatievoorziening DigiD heeft op dit moment een adequate mate van veiligheid door onder meer eisen aan de wachtwoorden en de beschikbaarheid van een bijzonder veilige infrastructuur. Het betrouwbaarheidsniveau van het huidige DigiD [6] is echter niet toereikend voor alle diensten die de publieke dienstverleners aanbieden aan burgers, bijvoorbeeld voor diensten waarbij zeer vertrouwelijke informatie (zoals medische gegevens) wordt uitgewisseld. Dit is het gevolg van het feit dat degene aan wie een DigiD wordt verstrekt thans niet in persoon (face to face) wordt geïdentificeerd.

Naast DigiD zijn er nu geen andere authenticatievoorzieningen voor burgers in het publieke domein.[7] In het verleden is het voorgekomen dat het systeem DigiD stilgelegd moest worden omdat er kwetsbaarheden aan het licht kwamen in de voor DigiD gebruikte software. Op zo'n moment ligt alle digitale dienstverlening van de overheid aan burgers stil. Doordat er thans maar één authenticatiemiddel is voor burgers, is dit een zogenoemde *Single point of failure*.

Dit wetsvoorstel strekt er toe dat burgers op een veilige en betrouwbare manier met meerdere authenticatiemiddelen (op een hoger betrouwbaarheidsniveau dan het huidige DigiD) toegang hebben tot digitale diensten van de publieke dienstverleners. Er wordt onder meer geregeld dat zowel door de rijksoverheid als door private aanbieders uitgegeven authenticatiemiddelen kunnen worden gebruikt voor toegang tot digitale dienstverlening van de overheid. Dit wordt wel aangeduid als de multimiddelenaanpak.[8] Hiermee wordt een *Single point of failure* voorkomen.

Om de veiligheid en betrouwbaarheid van de toegang tot overheidsdienstverlening te borgen voorziet het wetsvoorstel ook in bijzondere bevoegdheden om te kunnen ingrijpen in geval van ernstige storing van de elektronische dienstverlening of bij misbruik of oneigenlijk gebruik van de toegang tot de elektronische dienstverlening.

Zowel een door de rijksoverheid uitgegeven middel (een publiek middel) als een de door een private organisatie uitgegeven middel (een privaat middel) dient op grond van dit wetsvoorstel te zijn erkend door de minister van BZK, alvorens deze mag worden gebruikt in het publieke domein.

---

[5] Zie brief van brief van 14 december 2015, Kamerstukken II, 2015/16, 26 643, nr. 379.
[6] DigiD Basis bestaat uit een gebruikersnaam en wachtwoord; bij DigiD Midden wordt daarnaast ook een code ingevoerd, die de gebruiker via een sms heeft ontvangen. In dit verband wordt, aansluitend bij Europese kaders ter zake, gesproken over middelen met een laag betrouwbaarheidsniveau.
[7] Onder het begrip 'publieke domein' vallen alle bestuursorganen en organisaties die gerechtigd zijn het burgerservicenummer (BSN) te gebruiken, zoals zorgverzekeraars en pensioenfondsen die bij of krachtens deze wet zijn aangewezen. In plaats van 'publieke domein' wordt daarom ook wel gesproken over: BSN-domein.
[8] Zie onder meer de brief van de minister van BZK aan de Tweede Kamer van 25 augustus 2016, Kamerstukken II 2015/16, 26 643, nr. 419.

Ook de publieke en private organisatie die een middel uitgeeft (authenticatiedienst) dient door de minister te worden erkend. In de op dit wetsvoorstel gebaseerde uitvoeringsregelgeving worden gelijkluidende (uniforme) eisen gesteld waaraan de authenticatiediensten en de door hen aangeboden authenticatiemiddelen dienen te voldoen.

Burgers en ondernemers kunnen dus straks met authenticatiemiddelen van verschillende authenticatiediensten toegang krijgen tot digitale dienstverlening in het publieke domein. Deze authenticatiediensten moeten daarvoor aansluiten op een zogeheten ontsluitende dienst. Deze ontsluitende dienst zorgt er voor dat degene die toegang tot digitale publieke dienstverlening wil krijgen, doorgeleid wordt naar de authenticatiedienst die de gebruiker kan authenticeren. Ook de andere partijen in de authenticatieketen zoals de ontsluitende dienst en de machtigingsdienst moeten worden erkend. Ook zij dienen te voldoen aan eisen die in uitvoeringsregelgeving worden opgenomen. Ook is voorzien in toezicht en de mogelijkheid om sancties op te leggen indien niet aan de gestelde eisen wordt voldaan.

Een essentieel onderdeel van het wetsvoorstel is de verplichting voor bestuursorganen en aangewezen organisaties om alle erkende authenticatiemiddelen te accepteren. De andere kant van de medaille is dat deze publieke dienstverleners alleen erkende middelen mogen accepteren.

Op grond van de op grond van dit wetsvoorstel vast te stellen uitvoeringsregelgeving worden aan publieke dienstverleners eisen gesteld met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang van hun elektronische dienstverlening. Het is in eerste instantie aan de publieke dienstverleners zelf om te zorgen dat aan deze eisen wordt voldaan, hetgeen jaarlijks getoetst dient te worden door een onafhankelijk auditor.

1.5. Doelstellingen van het wetsvoorstel

De doelstelling van het wetsvoorstel zijn:
- Het overheidsbreed kunnen verplichten tot de toepassing van open standaarden.
- Het versterken van de veiligheid, betrouwbaarheid en goede werking van de digitale dienstverlening van publieke dienstverleners.
- Het verhogen van het vertrouwen in de digitale dienstverlening van publieke dienstverleners bij burgers en ondernemers.
- Het realiseren van eenvoudige, veilige en betrouwbare toegang van burgers en ondernemers tot elektronische dienstverlening van publieke dienstverleners.
- Het creëren van een terugvaloptie bij calamiteiten bij de toegang tot digitale dienstverlening van publieke dienstverleners .
- Het beperken van de kosten voor publieke dienstverleners voor de beveiliging van gegevens.

1.6. Wetgeving in tranches

Dit wetsvoorstel is de eerste tranche van de Wet GDI. De regels inzake standaarden en eID vormen een onderdeel van de generieke digitale infrastructuur (GDI). Het is de bedoeling dat op termijn ook andere onderdelen van de GDI in deze wet worden geregeld. De GDI bestaat uit generieke digitale basisvoorzieningen waarmee overheidsorganisaties hun digitale processen kunnen inrichten.[9] De GDI is naar zijn aard niet organisatie, sector- of domeinspecifiek. Een breed gebruik van deze basisvoorzieningen door overheidsorganisaties bevordert eenduidige, veilige en eenvoudige dienstverlening aan burgers en ondernemers. De GDI vormt een dynamisch geheel dat in de toekomst – op basis van technologische ontwikkelingen of nieuwe inzichten – gewijzigd kan worden door het toevoegen van nieuwe generieke voorzieningen (of functionaliteiten van een voorziening) of door het uitfaseren van bestaande generieke voorzieningen.
Dit betekent dat ook de wetgeving voor de GDI een dynamisch proces is. De regering kiest er daarom voor de wetgeving voor de GDI in tranches tot stand te brengen.

[9] *Voor een overzicht van de GDI voorzieningen zie https://www.digicommissaris.nl/*

In overleg met de decentrale overheden heeft de regering er voor gekozen om de eerste tranche van de Wet GDI te beperken tot de regeling van de toegang tot elektronische dienstverlening en standaarden voor elektronisch verkeer. De bevoegdheid om standaarden te verplichten is op korte termijn noodzakelijk in verband met de uitvoering van de Richtlijn 2016/2102/EU betreffende de toegankelijkheid van de websites en mobiele applicaties van overheidsinstanties.[10]

In volgende tranche(s) zullen naar verwachting de andere in de uitgangspuntenbrief genoemde GDI-voorzieningen worden geregeld. Dit betreft de voorzieningen voor burgers en ondernemers waarmee een ieder toegang wordt geboden tot informatie over producten en diensten van bestuursorganen (thans: Overheid.nl en Ondernemersplein.nl) en de voorzieningen waarmee burgers of ondernemers toegang wordt geboden tot persoonsgebonden respectievelijk ondernemingsgebonden informatie (thans: MijnOverheid, Berichtenbox voor bedrijven en het Ondernemingsdossier; de twee laatstgenoemde voorzieningen zullen naar verwachting worden doorontwikkeld tot de voorziening MijnOverheid voor Ondernemers).

Daarnaast worden in volgende tranche(s) mogelijk nog andere voorzieningen van de GDI geregeld, zoals Digipoort, Diginetwerk, Digilevering en Digimelding.[11] Deze voorzieningen zijn werkenderwijs ontwikkeld en stoelen op een in de praktijk meegegroeide juridische grondslag: een breed scala aan onderlinge (privaatrechtelijke) afspraken. Op dit moment zijn deze onderlinge afspraken nog werkbaar. In de toekomst is wettelijke regeling voor deze voorzieningen wellicht wenselijk zodat de privaatrechtelijke afspraken kunnen worden omgezet in publiekrechtelijke voorschriften.

2. De generieke digitale infrastructuur

2.1 Voorgeschiedenis

In de notitie *Op weg naar de elektronische overheid*[12] uit 2004 wordt het risico benoemd dat zolang afzonderlijke overheidsonderdelen bij de inzet van ICT in relatief isolement hun eigen weg gaan, de voor burgers en bedrijven én voor de overheid zinvolle ontwikkelingen buiten bereik blijven. Daarnaast wordt in de notitie beschreven welke voorzieningen en maatregelen op het vlak van informatievoorziening en ICT nodig zijn om de overheid beter te laten functioneren en dienstverlening aan burgers en bedrijven te verbeteren, zoals portals voor het verstrekken van informatie en verlenen van diensten, een overheidstoegangsvoorziening (nu bekend als DigiD) en een gezamenlijke infrastructuur voor registratie en uitwisseling van basisgegevens (het stelsel van basisregistraties).

Met het *Nationaal Actieprogramma Elektronische Overheid (ELO)*[13] was al duidelijk geworden dat voor het ondersteunen van de voornoemde basisfuncties zoveel mogelijk generieke voorzieningen gebruikt moeten worden. Voornamelijk aan de voorkant, maar ook voor de achterliggende processen. Daarom moet ingezet worden op ontwikkeling van gezamenlijke basisvoorzieningen om deze functies te ondersteunen. Hiermee wordt eenduidige dienstverlening voor burgers en bedrijven gerealiseerd, worden de administratieve lasten voor burgers en bedrijven verminderd en wordt de efficiency van de overheidsorganisaties verhoogd. Desondanks constateerde de commissie Wallage/Postma in haar rapport *Het uur van de waarheid*[14] dat er in 2007 nog steeds een gebrek is aan regie en samenhang, waardoor de gezamenlijke overheidsbrede elektronische infrastructuur nog te weinig werd gebruikt. De commissie stelt een Nationaal Urgentieprogramma voor, waarin zowel de noodzakelijke infrastructuur een plaats krijgt, als aansprekende voorbeeldprojecten, die gebruik (gaan) maken van die infrastructuur. Alle overheden moeten dan verplicht worden het urgentieprogramma uit te voeren.

---

[10] Richtlijn (EU) 2016/2102 van het Europees Parlement en de Raad van 26 oktober 2016 inzake de toegankelijkheid van de websites en mobiele applicaties van overheidsinstanties, Pb EU, L 327/1
[11] Voor een beschrijving van de werking van de voorzieningen zie: https://www.digicommissaris.nl/gdi
[12] Kamerstukken II 2003/04, 26 387, nr. 23.
[13] Kamerstukken II 1994/95, 23 900, nr. 20.
[14] Kamerstukken II 2008/09, 29 362, nr. 137-b2. https://www.digitaleoverheid.nl/images/stories/ Publicaties/eindrapport-e-overheid-postmawallage.pdf

Mede naar aanleiding van het rapport van de commissie Wallage/Postma zijn in 2008 de visie *Betere Dienstverlening Overheid*[15] en het bijbehorende actieprogramma *Dienstverlening en e-overheid* opgesteld. Deze nota beschrijft het geheel aan ambities en activiteiten van het kabinet om de dienstverlening door de overheid te verbeteren. Dit heeft geleid tot een aantal bestuursakkoorden. Het meest in het oog springende is het *Nationaal Uitvoeringsprogramma Dienstverlening en e-overheid "Burger en bedrijf centraal" (NUP)*[16], een gezamenlijk initiatief van het Rijk, het IPO, de VNG en de Unie van Waterschappen. Met het NUP spraken deze overheden op 1 december 2008 af dat uiterlijk op 1 januari 2011 een aantal voorzieningen geïmplementeerd zouden zijn. Het beoogd doel is dat overheden informatie snel en vlekkeloos kunnen uitwisselen, zodat de dienstverlening aan burgers en bedrijven beter wordt. De basisinfrastructuur van de elektronische overheid moet dan bestaan uit de elektronische toegang tot de overheid, elektronische authenticatie, informatienummers, basisregistraties en elektronische informatie-uitwisseling.

De implementatieagenda Nationaal UitvoeringsProgramma (i-NUP, april 2011 –januari 2015) bouwt voort op de door Wallage/Postma gedefinieerde basisinfrastructuur en heeft tot doel het afronden, opleveren en het in beheer brengen van de basisvoorzieningen en daarnaast een grootschalige implementatie van die basisvoorzieningen. Daarvoor is als onderdeel van de implementatieagenda een ondersteuningsprogramma voor gemeenten, Operatie NUP (o-NUP), ingericht. Operatie NUP was een programma van het Kwaliteitsinstituut Nederlandse Gemeenten (KING) – in opdracht van VNG – en ondersteunde gemeenten bij de implementatie van de ruim 20 NUP-bouwstenen en het nakomen van 19 resultaatafspraken. Deze vormen samen de basisinfrastructuur van de overheid en zijn onderdeel van de GDI. Operatie NUP liep tot 1 januari 2015.

In de Digitale Agenda.nl[17] die detoenmalige minister van EZ aan de Tweede Kamer zond is een breed recht op elektronisch zakendoen voor ondernemers aangekondigd. Daarmee wordt vastgelegd dat de overheidsdienstverlening aan ondernemers wordt gedigitaliseerd en onder welke voorwaarden dit gebeurt. Deze Digitale Agenda bouwt voort op de Europese Digitale Agenda, waarin de Europese Commissie een ambitieuze agenda neerzette voor 2010-2020. Als uitwerking van de Digitale Agenda is in december 2011 de brief Digitale Implementatie Agenda[18] uitgebracht. In deze Implementatie Agenda zijn voor de voorzieningen Digitaal Ondernemersplein, Ondernemingsdossier en eHerkenning concrete ambities opgenomen. Voor het Digitaal Ondernemersplein was die ambitie dat in 2015 ondernemers voor al hun zaken bij de overheid op deze ene plek terecht zouden kunnen. Voor eHerkenning was de ambitie dat in 2014 80% van de overheidsorganisaties die digitale diensten leveren aangesloten is. Voor het Ondernemingsdossier is vastgelegd dat in 2015 ondernemers in branches en sectoren met veel wet- en regelgeving gegevens, waar in het kader van toezicht, handhaving en vergunningverlening om gevraagd wordt, eenmalig en digitaal opslaan in het Ondernemingsdossier.

Uit de tussenbalans i-NUP[19] van medio 2013 bleek dat de grootschalige implementatie voor sommige onderdelen van de GDI goed verliep, maar voor andere onderdelen meer moeite kostte. Totaal bezien was met de grootschalige implementatie goede voortgang geboekt, al zou deze niet voor de volle honderd procent voor eind 2014 worden afgerond. Dit geeft aan dat er een goede basis is gelegd met het (i)NUP. Daarnaast maakt het duidelijk dat alleen op basis van bestuursakkoorden het vrijwel onmogelijk is om tot een volledige implementatie van de elektronische overheid te komen.

Dit sluit aan op de tussenrapportage van de Digitale Agenda[20] die in juli 2013 werd uitgebracht. Daarin werd aangegeven dat er vooruitgang geboekt is met betrekking tot de ambities voor de in de Digitale Agenda aangekondigde voorzieningen zoals Digitaal Ondernemersplein en Ondernemingsdossier, , maar nog niet voldoende tempo wordt gemaakt. De eindrapportage van i-

[15] *Kamerstukken II 2008/09, 29 362, nr. 137-b1.*
[16] *Kamerstukken II 2008/09, 29 362, nr. 148.*
[17] *Kamerstukken II 2010/11, 29 515, nr. 331.*
[18] *Kamerstukken II 2011/12, 26 643, nr. 217.*
[19] *https://www.digitaleoverheid.nl/images/stories/Publicaties/i-NUP-tussenbalans%20medio%202013.pdf*
[20] *Kamerstukken II 2012/13, 32 637, nr. 70.*

NUP[21] concludeert dat een goede basis gelegd is waarmee alle overheden nu zelf aan de slag kunnen in hun dienstverlening. De veranderende overheid met nieuwe werkprocessen zal de vraag naar nieuwe functionaliteiten van de infrastructuur oproepen, net zoals maatschappelijke en technologische ontwikkelingen dat ook zullen doen. Dit vraagt een samenhangende, meerjarige aanpak, waarbij de overheidsbrede samenwerking die in het programma i-NUP gestalte heeft gekregen wordt voortgezet en uitgebouwd.

In de visiebrief digitale overheid 2017 van 23 mei 2013 aan de Tweede Kamer heb ik, mede namens de minister voor Wonen en Rijksdienst, uiteengezet hoe deze doelstelling voor burgers wordt aangepakt.[22] Volgens de visiebrief is sprake van een forse ambitie voor alle bestuursorganen van de rijksoverheid, gemeenten, provincies en waterschappen, maar ook een kans om met een gezamenlijke en effectieve aanpak te komen tot:

a. een aantoonbare verbetering in kwaliteit van digitale overheidsinformatie en overheidsdienstverlening, met aandacht voor die mensen die (nog) minder digivaardig zijn;
b. aanzienlijk minder administratieve lasten voor burgers en bedrijven;
c. belangrijke efficiencywinsten waardoor onder meer departementale taakstellingen makkelijker gehaald kunnen worden.

Deze ambitie kan volgens de regering alleen worden gerealiseerd indien:

- Burgers en bedrijven een wettelijk (in de Algemene wet bestuursrecht) vastgelegd recht krijgen op elektronisch zakendoen met de overheid;
- De GDI wettelijk wordt verankerd, en,
- Het gebruik van (onderdelen van) de GDI door bestuursorganen wettelijk wordt verplicht.

Er is daarnaast een sterkere en meer centrale sturing nodig om te zorgen dat burgers en ondernemers het beoogde recht op elektronisch zakendoen daadwerkelijk geldend kunnen maken. Het kabinet heeft een stap daartoe gezet met de benoeming van de Nationale Commissaris Digitale Overheid.[23] De Digicommissaris heeft de opdracht "beleidsontwikkeling en vernieuwing aan te jagen, daarmee de totstandkoming van (voorzieningen voor) de digitale overheid - aangeduid als Generieke digitale infrastructuur (GDI) - te bevorderen, het beheer van essentiële voorzieningen te borgen en het gebruik van voorzieningen te stimuleren".

Bij brief van 25 april 2014 heeft de minister van EZ, mede namens de minister van BZK, de Tweede Kamer laten weten dat de in oktober 2013 door hem aangekondigde Wet Elektronisch Zakendoen[24], onderdeel wordt van een breder integraal wetgevingsprogramma.[25] Bij de voorbereiding van de internetconsultatie van het ontwerp van de Wet elektronisch Zakendoen was namelijk gebleken dat er behoefte is aan harmonisatie van beleid op het terrein van de elektronische overheid. Het brede integrale wetgevingsprogramma zal een overheidsbreed, wettelijk kader realiseren voor een aantal generieke, gestandaardiseerde voorzieningen, zodat burgers én bedrijven zaken met de overheid veilig, makkelijk, snel en lastenarm digitaal kunnen afhandelen.

De minister van BZK heeft mede namens de minister van EZ en de minister voor Wonen en Rijksdienst bij brief van 4 december 2015 de Tweede Kamer geïnformeerd over de uitgangspunten voor de Wet GDI.[26] Met de beoogde wet wordt – nadat de verschillende tranches van de wet zijn ingevoerd – een juridische basis gelegd onder voorzieningen en standaarden van de GDI. Deze wet zal het proces van voortschrijdende digitalisering dan ook ondersteunen en is nodig om waarborgen en rechtszekerheid aan burgers en bedrijven te bieden voor de digitaal optredende overheid. Daarnaast beoogt de wet een eenduidige wijze van informatieverschaffing door, en communicatie met de overheid te regelen voor burgers en bedrijven.

---

[21] Kamerstukken II 2014/15, 26 643, nr. 351.
[22] Kamerstukken II 2012/13, 26 643, nr. 280.
[23] Kamerstukken II 2013/14, 26 643, nr. 314.
[24] Kamerstukken II, 2013/14, 32 637, nr. 88, p. 10.
[25] Kamerstukken II, 2013/14, 32637, nr. 131.
[26] Kamerstukken II, 2015/16, 26643, nr. 373.

2.2 Belang

De regering ziet digitalisering als een belangrijk middel om betere dienstverlening aan burgers en ondernemers te kunnen leveren, zo mogelijk in combinatie met een hogere efficiëntie en aanzienlijk minder administratieve lasten voor burgers en ondernemers.

De afgelopen decennia is het gebruik van de elektronische weg in de contacten tussen burgers respectievelijk ondernemers en publieke dienstverleners toegenomen en breed geaccepteerd. In bijzondere wetten is soms al de elektronische weg met uitsluiting van de papieren weg voorgeschreven.[27] Hierbij zijn de manieren waarop de elektronische weg is opengesteld, sterk verschillend. Dit hangt samen met verschillen in tempo waarop bestuursorganen digitaliseren en de invloed van nieuwe technologische ontwikkelingen.

Van de overheid mag worden verwacht dat zij organisatieoverstijgend opereert; uitvoeringsprocessen zijn op elkaar afgestemd, informatie is makkelijk vindbaar en transacties zijn eenvoudig uitvoerbaar. Deze maatregelen leiden tot een eenduidig en samenhangende digitale overheidsdienstverlening.

Voor een goede dienstverlening is het noodzakelijk dat berichten en andere gegevensverkeer tussen de publieke dienstverleners en burgers en ondernemers op een veilige en betrouwbare wijze worden afgehandeld. Ook dient publieke overheidsinformatie betrouwbaar en eenvoudig digitaal raadpleegbaar te zijn. Voorts is het voor een goede digitale dienstverlening noodzakelijk dat de overheidsbrede digitale basisinfrastructuur (de GDI) robuust en toekomstbestendig is.[28]

Uit onderzoek blijkt dat burgers en ondernemers één overheidsportaal prettig vinden.[29] Tweederde van de respondenten is het eens met de stelling 'Het zou goed zijn als er één website is voor burgers en voor ondernemers, waar je *alle* overheidszaken kan regelen'. Uit hetzelfde onderzoek blijkt dat de helft van degenen die MijnOverheid.nl kennen, het portaal een verbetering vindt voor de overheidsdienstverlening en slechts 3% vindt het een verslechtering. Bijna negen op de tien respondenten (88%) die bekend zijn met MijnOverheid.nl vindt het belangrijk om de gegevens die de overheid van hen heeft, op één plaats in te zien.

Breed gebruik van de GDI-voorzieningen is een voorwaarde om versnippering in de publieke dienstverlening aan burgers en ondernemers tegen te gaan. Bovendien worden de voorzieningen kosteneffectiever en ontstaan er op macroniveau efficiencyvoordelen. Bij breed gebruik daalt de prijs per transactie. Ook hoeven alternatieve voorzieningen niet meer doorontwikkeld en beheerd te worden. Een goed voorbeeld is de GDI-voorziening DigiD, waarmee burgers bij publieke dienstverleners op eenzelfde manier kunnen inloggen.

2.3 Toekomstige ontwikkelingen

De GDI is door technologische ontwikkelingen dynamisch en veranderlijk. De intentie is dat de komende jaren diverse GDI-voorzieningen worden (door)ontwikkeld, gewijzigd of afgebouwd, en dat nieuwe GDI-functionaliteiten worden toegevoegd. Ook het vergroten van het gebruik van huidige GDI-voorzieningen door overheidsorganisaties is voor komende jaren een prioriteit.

Voor een uitgebreid overzicht van de ontwikkeling van de GDI(-voorzieningen) de komende jaren wordt verwezen naar het Digiprogramma 2016/2017, opgesteld door de Digicommissaris en vastgesteld in de ministerraad.[30]

---

[27] Bijvoorbeeld de Wet elektronisch berichtenverkeer Belastingdienst waarin enkele wijzigingen worden aangebracht in de formele belastingwetgeving om een wettelijk kader te scheppen voor het verplichten van elektronisch berichtenverkeer in het contact met de Belastingdienst (Stb. 2015, 378).

[28] Zie ook het advies 'Geen goede overheidsdienstverlening zonder een uitstekende generieke digitale infrastructuur', opgesteld door drs. R.IJ.M. Kuipers, ABD TopConsultants, d.d. 15 januari 2014. Raadpleegbaar via www.tweedekamer.nl

[29] Zie het rapport De kwaliteit van overheidsdienstverlening 2015, https://www.rijksoverheid.nl/documenten/rapporten/2016/05/02/de-kwaliteit-van-de-overheidsdienstverlening-2015

[30] https://www.digicommissaris.nl/page/893/digiprogramma-2016-2017

3. Standaarden

3.1. Inleiding

Standaardisering is randvoorwaardelijk om te kunnen communiceren.[31] In de fysieke wereld wordt bijvoorbeeld door middel van het Internationale Stelsel van Eenheden overal ter wereld hetzelfde verstaan onder bepaalde maten, waardoor een meter overal even lang is. Net zoals bij de fysieke infrastructuur is het essentieel om afspraken te maken waar de gebruikers van de digitale infrastructuur zich aan moeten houden. ICT-standaarden zijn afspraken vastgelegd in een specificatiedocument. Ze beschrijven hoe gegevens eruit zien, wat ze betekenen en hoe ze kunnen worden uitgewisseld. Door standaarden te gebruiken, begrijpen communicerende partijen hoe gegevens moeten worden geïnterpreteerd, zodat applicaties of andere softwarecomponenten elkaars gegevens volledig en correct kunnen verwerken. Zonder afspraken in de vorm van standaarden loopt het digitale verkeer vast, is het verkeer minder veilig en kost het deelnemen aan het verkeer onnodig veel geld.

Overheidsverkeer langs de elektronische weg moet veilig, betaalbaar en betrouwbaar zijn. Het elektronische verkeer kan zich van en naar burgers en ondernemers begeven of richting andere overheidsorganisaties. Voor elektronisch verkeer over de organisatiegrenzen heen is het noodzakelijk dat de ICT-systemen van samenwerkende overheidsorganisaties elkaar kunnen verstaan en probleemloos op elkaar aansluiten, ook al zijn de ICT-systemen afkomstig van verschillende leveranciers. Hiervoor zijn ICT-standaarden noodzakelijk.

Standaardiseren reduceert de kosten voor communicatie, doordat overheidsorganisaties in verschillende ketens met elkaar samen kunnen werken en elkaars gegevens kunnen hergebruiken, zonder burgers en bedrijven met uitvragen naar dezelfde informatie te belasten en daarmee verminderen de administratieve lasten. Door overheidsbreed dezelfde standaarden toe te passen, wordt het aantal koppelvlakken van ICT-systemen en daarmee de kosten voor communicatie beperkt. Het niet standaardiseren door slechts enkele overheidsorganisaties, jaagt andere organisaties onevenredig op kosten. Het kostenbesparend effect van standaardisering blijkt bijvoorbeeld uit het feit dat het bij de Kamer van Koophandel deponeren van de jaarrekening met *Standard Business Reporting* in documentformaat XBRL, een open standaard, op jaarbasis tientallen miljoenen euro's bespaart.[32]

3.2. Noodzaak van het gebruik van open standaarden

Standaardiseren zonder meer levert echter nieuwe problemen op, zoals leveranciersafhankelijkheid en het gebrek aan kostenbeheersing. Om de kosten te kunnen beheersen, moeten overheidsorganisaties bij het aanschaffen van nieuwe software of ICT-systemen over keuzevrijheid beschikken. Het gebruik van open standaarden draagt bij aan keuzevrijheid voor de ICT-gebruiker, doordat de implementatie van deze standaarden het eenvoudiger maakt om over te stappen op een andere producent met een ander softwareproduct als daar aanleiding toe is hetgeen de mededinging ten goede komt. De specificaties van open standaarden zijn vrij of eventueel tegen een redelijke vergoeding opvraagbaar. Deze standaarden worden ontwikkeld en beheerd op een open en toegankelijke manier en zijn vrij van licentierechten te gebruiken. Daarentegen kan de toepassing van gesloten standaarden – naast mogelijke kosten voor gebruik in verband met octrooien – met zich meebrengen dat de gebruiker min of meer gedwongen is om producten van dezelfde producent af te nemen, omdat alleen op die wijze opgeslagen data bruikbaar blijft of het uitwisselen van gegevens dan op de minste problemen stuit. Overstappen op een andere producent kan gepaard gaan met hoge kosten om deze problemen op te lossen voor zover dat mogelijk is, waardoor overstappen op een beter of goedkoper softwareproduct niet vanzelfsprekend is. Uit het rapport 'Meting Open Standaardenbeleid Onderwijs' blijkt bijvoorbeeld

[31] *Illustratief hiervoor zijn lucht- en ruimtevaartincidenten als gevolg van het door elkaar gebruiken van Britse en metrieke eenheden, zoals het communiceren van volume in gallons en het interpreteren in liters.*
[32] *Kamerstukken II 2014/15, 34 262, nr. 3.*

dat veel instellingen knelpunten ervaren met betrekking tot de afhankelijkheid van leveranciers en de gegevensuitwisseling.[33]

Het opslaan van overheidsinformatie in open standaarden maakt het waarschijnlijker dat de informatie in de toekomst nog beschikbaar zal zijn, omdat de ICT-gebruiker daardoor niet op een specifieke leverancier is aangewezen om de documenten na een softwarewijziging raadpleegbaar te houden. Applicaties worden namelijk slechts een beperkte tijd door de producent ondersteund en als de oude applicatie op een gesloten standaard is gebaseerd, hangt het van de ICT-leverancier af of de data, die bij deze applicatie horen, in de toekomst bruikbaar zal zijn. Het gebruik van gesloten standaarden door overheidsorganisaties draagt niet bij een doelmatige informatiehuishouding, waarin digitale documenten die ten behoeve van wettelijke eisen[34], administratieve eisen of maatschappelijke behoeften bewaard moeten worden, op een zodanige wijze worden vastgelegd, dat deze ook na verloop van tijd raadpleegbaar, authentiek zijn en gedeeld kunnen worden met overheidsorganisaties, burgers of bedrijven als dat vereist is. Naast duurzame toegankelijkheid[35] van overheidsinformatie biedt het overheidsbrede gebruik van open standaarden burgers, bedrijven en bestuursorganen de zekerheid dat communicatie slaagt zonder dat zij via de software van één of een beperkte groep softwareleveranciers moeten communiceren met de overheid. Het kabinet voert vanwege de bovengenoemde voordelen sinds 2007 een op open standaarden gericht beleid.[36]

Het kabinet stimuleert het overheidsbrede gebruik van open ICT-standaarden door middel van de plaatsing van bepaalde open standaarden op de zogeheten 'pas toe of leg uit'-lijst. Ter aanvulling op dit beleid voorziet dit wetsvoorstel in de bevoegdheid om bij algemene maatregel van bestuur een open standaard aan te wijzen die verplicht moet worden toegepast. Een standaard kan worden aangewezen indien dit noodzakelijk en proportioneel is voor de werking, de betrouwbaarheid of de doelmatigheid van het elektronische verkeer met of tussen bestuursorganen of indien dit voortvloeit uit internationale verplichtingen. Bij een dergelijke aanwijzing wordt per standaard bepaald welke bestuursorganen, rechtspersonen met een wettelijke taak en organen, personen en colleges als bedoeld in artikel 1:1, tweede lid, van de Algemene wet bestuursrecht (Awb) de standaard dienen toe te passen.

3.3. Het 'pas toe of leg uit'-beleid

De 'Instructie rijksdienst inzake de aanschaf van ICT-diensten en ICT-producten' schrijft voor dat overheidsorganisaties binnen het Rijk bij aanschaf of (ver)bouw van ICT-systemen de open standaarden, die op de zogeheten 'pas toe of leg uit'-lijst staan, hanteren ('pas toe').[37] Afwijken van deze verplichting mag alleen in geval van zwaarwegende redenen; verantwoording hierover moet worden afgelegd in het jaarverslag ('leg uit'). Deze rapportageverplichting is opgenomen in de Rijksbegrotingsvoorschriften. De Rijksbegrotingsvoorschriften bevatten de voorschriften voor de verantwoording over de begroting, de uitvoering van de begroting en de begroting. De verplichting om te vragen naar de open standaarden op de 'pas toe of leg uit'-lijst geldt alleen bij de inkoop van ICT-systemen en -diensten boven € 50.000,- (exclusief BTW).

De standaarden die op de 'pas toe of leg uit'-lijst staan, zijn open standaarden waarvoor breed draagvlak bestaat. De standaarden op deze lijst hebben een procedure doorlopen om te toetsen of aan de criteria voor openheid is voldaan. In deze procedure wordt onder andere getoetst of de standaard toepasbaar is voor elektronische gegevensuitwisseling tussen overheidsorganisaties en of er geen hindernissen zijn op het terrein van intellectueel eigendomsrecht. Het Forum Standaardisatie beheert de lijst met verplichte ('pas toe of leg uit') en aanbevolen open standaarden. In het kader van het programma i-NUP is in 2011 afgesproken dat het Rijk en de medeoverheden in 2015 de open standaarden, zoals vastgesteld door het College Standaardisatie,

---

[33] Kamerstukken II 2013/14, 26 643 nr. 295, blg-269959, p. 5.
[34] Zoals artikel 3 Archiefwet 1995.
[35] Duurzame toegankelijkheid houdt in dat informatie vindbaar, interpreteerbaar en uitwisselbaar is; dat wil zeggen dat informatie vanaf het moment van ontstaan beschikbaar en bruikbaar is voor iedereen die daar recht op heeft, voor zolang als noodzakelijk is.
[36] Kamerstukken II 2007/08, 26 643, nr. 98.
[37] Stcrt. 2008, nr. 227, bijlage, art. 3.

gebruiken en hierbij werken volgens het principe 'pas toe of leg uit'.[38] Gemeenten hebben zich aan deze resultaatverplichting gecommitteerd door middel van het Bestuursakkoord 2011-2015.[39] Op 18 mei 2015 is in het Nationaal Beraad Digitale Overheid, waarin alle overheden zijn vertegenwoordigd, de afspraak verlengd tot eind december 2017.

3.4. Noodzaak van wetgeving

Diverse instrumenten zijn ingezet om overheidsbreed gebruik van open standaarden te realiseren, zoals het actieplan Nederland Open in Verbinding[40], de Rijksbegrotingsvoorschriften, de Instructie rijksdienst inzake de aanschaf van ICT-diensten en ICT-producten, het i-NUP en het Bestuursakkoord 2011-2015. Het effect van deze instrumenten is beperkt. Het Forum Standaardisatie publiceert ieder jaar een Monitor Open Standaarden Beleid, die het uitvragen van open standaarden door de overheid meet en evalueert. Uit de 1-meting informatieveiligheidstandaarden en de Monitor Open Standaarden Beleid over de jaren 2012, 2013, 2014 en 2015, blijkt dat het adoptietempo van open standaarden laag is en dat er in de jaarverslagen zelden wordt uitgelegd waarom een open standaard niet wordt toegepast. Dit heeft nadelige gevolgen voor de interoperabiliteit, veiligheid en kosten(beheersing) van ICT-systemen.

In 2011 concludeerde de Algemene Rekenkamer in het rapport 'Open standaarden en opensourcesoftware bij de rijksoverheid'[41] dat het open standaardenbeleid te vrijblijvend is. Dat constateerde ook de Tijdelijke Commissie ICT (Commissie Elias) in oktober 2014 in haar eindrapportage. De Commissie Elias beveelt aan dat de overheid voortaan daadwerkelijk toeziet op naleving van haar 'pas toe of leg uit'-beleid rondom open standaarden.[42] De Commissie Elias sloot zich aan bij het rapport 'Geen goede overheidsdienstverlening zonder een uitstekende generieke digitale infrastructuur'[43] om een wettelijke basis te creëren waarmee het gebruik van standaarden kan worden verplicht. In de kabinetsreactie op het rapport van de Commissie Elias wordt ten aanzien van het gebruik van open standaarden verwezen naar dit wetsvoorstel.[44] In 2016 verzocht de Tweede Kamer het kabinet om het gebruik van open standaarden bij wet te verplichten. Daaraan lag de overweging ten grondslag dat het gebruik van open standaarden essentieel is in het actief beschikbaar stellen van informatie aan burgers en daarnaast zorgt voor meer keuzevrijheid in ICT-leveranciers, bevordering van de rechtszekerheid, administratieve lastenverlichting en het efficiënt en in ketens kunnen werken als één overheid.[45]

Een gemengde aanpak van wetgeving en voorlichtingsacties, die plaatsvinden in het kader van het 'pas toe of leg uit'-beleid, is nodig om de overheid doelmatiger en veiliger te laten functioneren met behulp van open standaarden. Het 'pas toe of leg uit'-principe blijft voor bepaalde open standaarden het meest proportionele instrument. Echter, voor sommige standaarden is het bevorderen van het gebruik onvoldoende en moeten overheidsorganisaties de standaard eenvoudigweg toepassen.

De gevolgen van het niet toepassen van een bepaalde standaard kunnen te ernstig zijn. Dit doet zich voor wanneer het gebrek aan tempo bij de invoering van bepaalde standaarden het publieke belang schaadt, bijvoorbeeld omdat de betrouwbaarheid en veiligheid van gegevens, de leveranciersonafhankelijkheid of de toegankelijkheid van overheidsinformatie in het geding is. Bij bepaalde open standaarden is geen rechtvaardiging voor uitzondering mogelijk of is het belang van de toepassing ervan zo groot dat het moment van een volgende ICT-aanschaf van € 50.000,- (exclusief BTW) of meer niet kan worden afgewacht.

---

[38] Kamerstukken II 2010/11, 26 643, nr. 182, blg-116878. De resultaatverplichtingen van het i-NUP werden gekoppeld aan de opzet van een ondersteuningsprogramma, dat deels door het Rijk is gefinancierd, voor gemeenten.
[39] Kamerstukken II 2010/11, 32 749, nr. 1, blg-110123, p. 52 en p. 53.
[40] Kamerstukken II 2007/08, 26 643, nr. 98.
[41] Kamerstukken II 2010/11, 32 679, nr. 2.
[42] Kamerstukken II 2014/15, 33 326, nr. 5, p. 21.
[43] Kamerstukken II 2013/14, 26 643, nr. 314.
[44] Kamerstukken II 2014/15, 33 326, nr. 13, p. 15.
[45] Kamerstukken II 2016/17, 32 802, nr. 31 (motie Oosenbrug).

Artikel 2, tweede lid, van dit wetsvoorstel biedt daarom een grondslag om bij algemene maatregel van bestuur een verplicht toe te passen open standaard aan te wijzen. Een bij algemene maatregel van bestuur verplichte standaard zal van de 'pas toe of leg uit'-lijst worden verwijderd. De minister van BZK zal het Forum Standaardisatie en het Nationaal Beraad Digitale Overheid (dat in 2014 de taak van het College Standaardisatie heeft overgenomen) betrekken in de voorbereiding van een algemene maatregel van bestuur. In het Nationaal Beraad zijn de decentrale overheden vertegenwoordigd. Voor zover er aanleiding is voor interbestuurlijk toezicht, wordt volstaan met de generieke toezichtinstrumenten in de Provinciewet en de Gemeentewet.

3.5. De toegankelijkheidstandaard

Het is van groot belang dat de diensten van de overheid toegankelijk zijn voor een ieder. Het internet is voor burgers en bedrijven een essentieel middel geworden om toegang te krijgen tot informatie en diensten van de overheid. Om de kwaliteit en de toegankelijkheid van websites te garanderen heeft het 'World Wide Web Consortium' (W3C) internationale standaarden ontwikkeld voor het ontwerpen, bouwen en beheren van websites. Een website die voldoet aan de Web Content Accessibility Guidelines (WCAG) werkt op alle apparaten, in alle internetbrowsers en besturingssystemen en kan door iedereen gebruikt worden, ook door personen met een visuele, auditieve of lichamelijke beperking of personen die taalkundig of digitaal minder vaardig zijn.

Op 14 juli 2016 is het Verdrag van de Verenigde Naties van 13 december 2006 inzake de rechten van personen met een handicap[46] (hierna: het verdrag) in werking getreden. Het doel van dit verdrag is onder meer dat personen met een handicap al bestaande mensenrechten effectief en op voet van gelijkheid met anderen kunnen uitoefenen. Het verdrag roept geen nieuwe rechten in het leven, maar geeft verdere uitwerking aan bestaande mensenrechten en verplichtingen uit andere verdragen. Op grond van het eerste lid van artikel 9 van het verdrag nemen Verdragstaten passende maatregelen om personen met een handicap op voet van gelijkheid met anderen de toegang te garanderen tot onder andere informatie en communicatie, met inbegrip van informatie- en communicatietechnologieën en -systemen, en tot andere voorzieningen en diensten die openstaan voor, of verleend worden aan het publiek. Op grond van het tweede lid van artikel 9 van het verdrag nemen Verdragsstaten passende maatregelen om de toegang voor personen met een handicap tot nieuwe informatie en communicatietechnologieën en -systemen, met inbegrip van het internet, te bevorderen.

De regering heeft de toegankelijkheid van websites in de publieke sector bevorderd door de nationale standaard die daarin voorziet, de Webrichtlijnen, op te nemen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie. De 'pas toe of leg uit'-verplichting geldt voor alle overheidsorganisaties. Tevens werd in de Overheidsbrede implementatieagenda voor dienstverlening en e-overheid (i-NUP) het toepassen van de Webrichtlijnen als resultaatverplichting opgenomen.

De regering is voornemens om bij algemene maatregel van bestuur krachtens artikel 2, tweede lid, van dit wetsvoorstel de Europese toegankelijkheidstandaard ETSI EN 301 549 aan te wijzen als een verplicht toe te passen standaard. Het voornemen om de toepassing van deze Europese standaard te verplichten, houdt verband met de Richtlijn 2016/2102/EU betreffende de toegankelijkheid van de websites en mobiele applicaties van overheidsinstanties. Deze richtlijn heeft tot doel te bereiken dat websites en mobiele applicaties van overheidsinstanties toegankelijker worden voor gebruikers, in het bijzonder voor personen met een beperking. Daartoe dienen lidstaten ervoor te zorgen dat websites en mobiele applicaties van overheidsinstanties voldoen aan de toegankelijkheidseisen van artikel 4 van de richtlijn. Daaraan kunnen websites en mobiele applicaties van overheidsinstanties voldoen, indien ze de in artikel 6 van de richtlijn aangewezen Europese standaard voor toegankelijkheid toepassen. Dit is de Europese norm ETSI EN 301 549. Deze Europese toegankelijkheidsstandaard voor websites is integraal en zonder aanpassing overgenomen van de wereldwijd toegepaste internationale standaard 'Web Content Accessibility Guidelines' (WCAG) versie 2.0, waarop ook Webrichtlijnen versie 2.0 is gebaseerd. Om eenduidigheid te realiseren is Webrichtlijnen versie 2.0 van de 'pas toe of leg uit'-lijst afgehaald en

[46] *Trb. 2007, 169.*

wordt ETSI EN 301 549 bij algemene maatregel van bestuur verplicht ter implementatie van Richtlijn 2016/2102/EU.

3.6. Informatieveiligheidstandaarden

De uitwisseling van informatie langs de elektronische weg door overheden dient zo veilig mogelijk te geschieden, te meer omdat aan de berichten rechtsgevolgen kunnen zijn verbonden. Het gebruik van verschillende standaarden zorgt dat meer koppelvlakken[47] nodig zijn, hetgeen leidt tot een verhoogd veiligheidsrisico. Elk koppelvlak dient gebouwd of gekocht te worden en dient vervolgens te worden beheerd. De kans op fouten, variërend van systemen die niet werken tot systemen die de verkeerde beslissingen nemen, neemt hiermee toe en de integriteit van gegevens en van systemen die ze gebruiken neemt af. Het overheidsbrede gebruik van dezelfde standaarden leidt tot minder koppelvlakken, wat de veiligheid van ICT-systemen ten goede komt.

Naast de bovengenoemde wijze om informatieveiligheid te vergroten, zijn er specifieke standaarden ten behoeve van informatieveiligheid. Het toepassen van bijvoorbeeld de standaard TLS 1.2 of de standaard DNSSEC, beveiligt de netwerkverbinding waarover gegevens worden uitgewisseld. De standaarden DKIM en SPF zorgen voor e-mailauthenticatie; hiermee wordt het mogelijk dat een internetprovider of een ontvanger de identiteit van de afzender deels controleert, waardoor fraude zoals 'phishing' wordt bestreden. Bij 'phishing' worden valse e-mails in naam van onder andere de overheid verstuurd en dan is het voor burgers en bedrijven niet eenvoudig om te ontdekken of een e-mail met een verwijzing naar een website daadwerkelijk afkomstig is van een bestuursorgaan.

Het niet toepassen van specifieke veiligheidstandaarden kan schade toebrengen aan de belangen van burgers, bedrijven of andere overheden. Indien inloggegevens in handen vallen van kwaadwillenden, kan dit burgers geld kosten of kunnen gegevens misbruikt worden voor identiteitsfraude. De overheidsbrede toepassing van bepaalde veiligheidstandaarden is noodzakelijk om veiligheidsrisico's te beperken, te meer omdat sommige standaarden pas functioneren als deze aan beide kanten van de communicerende partijen worden toegepast. Indien bijvoorbeeld één overheidsorganisatie besluit om een veiligheidsstandaard zoals SAML niet toe te passen, wordt het alle partijen die met deze organisatie communiceren onmogelijk gemaakt om deze veiligheidsstandaard toe te passen in de communicatie met die ene organisatie. Hierdoor is de informatieveiligheid van overheidsorganisaties, die wel hebben geïnvesteerd in het implementeren van de veiligheidsstandaard, evenmin geborgd.

Brede adoptie van de standaard Digikoppeling 2.0 is nodig vanuit veiligheidsoogpunt en omdat de financiële baten exponentieel afnemen naarmate er registraties afhaken. Op jaarbasis kan met de brede toepassing van Digikoppeling meer dan € 78 miljoen worden bespaard op kosten die overheidsorganisaties dienen te maken om te kunnen communiceren met andere overheidsorganisaties, zo blijkt uit de business case naar de potentiële besparingen van de voorzieningen voor het stelsel van basisregistraties.[48]

Gezien het belang van informatieveiligheid is het toepassen van bepaalde standaarden niet vrijblijvend voor de overheid. De veiligheidsstandaarden TLS 1.2, DNSSEC, DKIM, SPF en Digikoppeling 2.0, die reeds op de 'pas toe of leg uit'-lijst staan, komen daarom in aanmerking om bij algemene maatregel van bestuur, op grond van artikel 2, tweede lid, van dit wetsvoorstel, te worden verplicht. Daarmee vormt het voldoen aan de verplichte veiligheidsstandaarden een wettelijke ondergrens voor overheidsorganisaties om informatie met burgers, bedrijven en onderling veilig te kunnen uitwisselen en hergebruiken.

---

[47] Een koppelvlak is het geheel van afspraken (over het proces, de betekenis, de schrijfwijze en de techniek) die nodig zijn om twee partijen elektronisch te laten samenwerken.

[48] Daarnaast illustreert de business case dat het niet meedoen van enkele overheidsorganisaties de andere overheidsorganisaties onevenredig op kosten jaagt. Als bijvoorbeeld slechts 6 van de 13 basisregistraties standaardiseren op Digikoppeling, dalen de totale baten van 78 miljoen naar 11 miljoen euro. Bron: 'Verfijning en herijking kosten- batenanalyse voor investeringen in gemeenschappelijke voorzieningen in het stelsel van basisregistraties: Grip op centrale en decentrale investeringen en kosten maximaliseert de businesscase', PriceWaterhouseCoopers, 23 februari 2010 (gepubliceerd op www.rijksoverheid.nl/documenten).

4. Elektronische authenticatie

4.1. Inleiding

Bij digitale dienstverlening waarbij informatie wordt uitgewisseld die niet voor iedereen is bestemd, is het noodzakelijk dat de daarbij betrokken partijen weten met wie ze te maken hebben. Wanneer een publieke dienstverlener persoons- of bedrijfsgebonden informatie gaat uitwisselen met burgers of ondernemers, is het van belang dat de identiteit en bevoegdheid van de burger of ondernemer met voldoende zekerheid wordt vastgesteld. Het gaat daarbij om een betrouwbaar antwoord op de vragen 'Wie ben je?', 'Ben je wie je zegt dat je bent?' en 'Wat mag je?'. Alleen dan kan de publieke dienstverlener gegevens verstrekken aan of aanvaarden van de burger of de ondernemer. Om die benodigde zekerheid te verkrijgen, wordt gebruik gemaakt van elektronische authenticatiediensten, en in voorkomende gevallen ook van elektronische machtigings- of attributendiensten. Met de twee laatstgenoemde diensten wordt de bevoegdheid van degene die inlogt vastgesteld (Wat mag je?).

Voor burgers biedt de rijksoverheid al jaren elektronische authenticatie- en machtigingsdiensten aan, te weten het huidige DigiD en DigiD Machtigen. Voor ondernemers is eHerkenning ontwikkeld. eHerkenning is een publiek-private samenwerking, waarbij de middelen door private partijen worden uitgereikt. Tot op heden worden binnen het publieke domein geen attributendiensten aangeboden.

4.2. Het gebruik

Het aantal authenticaties via DigiD is in 2015 gestegen met 30% naar ruim 206 miljoen. In 2014 vonden 158 miljoen authenticaties plaats, in 2013 waren dit er 117 miljoen. In 2015 waren er ruim 12,5 miljoen actieve DigiD's. Het zwaartepunt van het gebruik van DigiD ligt op het basisniveau (gebruikersnaam en wachtwoord) dat zorgt voor 90% van alle authenticaties. Opvallend is dat 56% van de gebruikers – ruim 7 miljoen – een DigiD met een hoger beveiligingsniveau heeft (gebruikersnaam en wachtwoord en SMS-code), terwijl maar 10% van de authenticaties op dit niveau plaatsvindt.

Circa de helft van alle transacties met DigiD is te herleiden naar de dienstverlening van het UWV en de Belastingdienst. In totaal waren er eind 2015 551 organisaties aangesloten op DigiD. Dat waren er in 2014 nog 526. De gemeenten vertegenwoordigen de grootste groep van aangesloten organisaties; met eigen aansluitingen maar ook via samenwerkingsverbanden. Er zijn 42 grote landelijke overheidsorganisaties aangesloten op DigiD en ook pensioenfondsen maken er – met 44 aansluitingen – gebruik van. Elf kleinere pensioenfondsen zijn via twee centrale aansluitingen via DigiD bereikbaar. In het zorgdomein zijn 40 aansluitingen gerealiseerd op organisatieniveau, waarbij vaak het beveiligingsniveau DigiD met gebruikersnaam, wachtwoord en SMS-code wordt ingezet en via één aansluiting zijn 318 apotheken aangesloten.

In 2015 waren in de grensgemeenten 17.149 brieven opgehaald met de activatiecode voor DigiD-buitenland. Met DigiD-buitenland kunnen Nederlanders die in het buitenland wonen DigiD aanvragen. Uitgiftepunt Schiphol heeft het hoogste aantal aanvragen, in 2015 bijna 6.000. De uitgifte via de ambassades bedroeg 353, waarvan er 135 door de ambassade in Parijs zijn uitgegeven.

Bij eHerkenning, dat authenticatie door ondernemers betreft, is sprake van gestage groei in het aantal aangesloten overheidsorganisaties en het aantal transacties. Met name gemeenten sluiten steeds vaker aan op eHerkenning en ontsluiten een toenemend aantal van hun diensten ook voor ondernemers digitaal. Er is in 2015 sprake van een groei naar 185 publieke dienstverleners; gemeenten zijn hiervan de grootste groep. Er zijn 23 Rijkspartijen aangesloten met meerdere van hun diensten en producten.

Vanaf 1 januari 2015 is het verplicht om met eHerkenning in te loggen bij de Rijksdienst voor Ondernemend Nederland. Dit heeft in dat jaar geleid tot een toename van 200% in gebruik ten opzichte van het jaar daarvoor, resulterend in een aantal van ruim 5 miljoen authenticaties. In

2013 was dit aantal nog een miljoen. Het aantal uitgegeven eHerkenningsmiddelen steeg in 2015 met 46% tot ruim 242.000. In 2013 werden er 94.000 eHerkenningsmiddelen uitgegeven; in 2014 was dit aantal opgelopen naar 166.000. Van de eHerkenningsmiddelen wordt inmiddels de helft gebruikt voor meer dan één toepassing. Er zijn in 2015 184.000 ondernemers aangesloten op eHerkenning, tegen 134.000 in 2014 en 81.000 in 2013.

Op 31 december 2015 waren drie overheidsorganisaties rechtstreeks aangesloten op DigiD Machtigen: DUO, de Belastingdienst en de Belastingdienst Toeslagen. Via de voorziening MijnOverheid zijn verschillende andere overheidsorganisaties aangesloten. Het aantal geregistreerde actieve machtigingen was in 2015 ruim 1,6 miljoen. Ongeveer de helft daarvan, ruim 800.000, is in 2015 daadwerkelijk gebruikt bij het afnemen van publieke diensten.

4.3. Het eID-stelsel

Om doelstellingen van het eID beleid te bereiken, wordt met dit wetsvoorstel een publiekrechtelijk stelsel voorgesteld waarbinnen publieke en private partijen de benodigde diensten kunnen aanbieden.

Authenticatiedienst
Het eID-stelsel houdt in, dat authenticatiemiddelen door private en publieke partijen (authenticatiediensten) kunnen worden aangeboden. De rijksoverheid zal zelf voorzien in authenticatiemiddelen op betrouwbaarheidsniveau substantieel en hoog. Reden hiervoor is dat de regering wil dat uiteindelijk voor iedere burger een betrouwbaar en veilig authenticatiemiddel beschikbaar is en dat burgers niet afhankelijk zijn van de beschikbaarheid van private middelen voor de toegang tot digitale dienstverlening in het publieke domein.

Ontsluitende dienst
De ontsluitende dienst is een partij die werkt in opdracht van een publieke dienstverlener. De ontsluitende dienst verzorgt de aansluiting van de publieke dienstverlener op de erkende middelen. Een ontsluitende dienst vraagt aan degene die wil inloggen bij een dienstverlener van welk authenticatiemiddel hij of zij gebruik wil maken voor het afnemen van publieke diensten (bijvoorbeeld een vergunning) en verzamelt alle benodigde informatie (wie de persoon is, wat de persoon mag en eventueel andere attributen) voor een dienstverlener om een persoon toegang te kunnen verlenen tot het systeem van de dienstverlener. De rol van een ontsluitende dienst is te vergelijken met de rol van iDEAL bij online betaling. iDEAL vraagt met welke (bank) rekening de klant wil betalen.

Machtigingsdienst
Een machtigingsdienst registreert op een betrouwbare wijze dat een persoon een andere persoon heeft gemachtigd namens hem of haar diensten af te nemen bij een publieke dienstverlener. Een voorbeeld van een machtigingsdienst is de al bestaande publieke voorziening DigiD Machtigen. Deze voorziening is nu geregeld in op artikel X van de Wet elektronisch berichtenverkeer Belastingdienst gebaseerde uitvoeringsregelgeving. Op grond van voorliggend wetsvoorstel zullen onder meer gebruiksvoorschriften voor de publieke machtigingsdienst vastgesteld worden, waarbij bezien zal worden in hoeverre de huidige bepalingen wijziging behoeven.

Attributendienst
De attributendienst is een partij die ten behoeve van elektronische dienstverlening een verklaring afgeeft over bepaalde kenmerken of gegevens van een natuurlijke persoon (bijvoorbeeld leeftijd of beroep) of een rechtspersoon (bijvoorbeeld erkend bedrijf).

4.4. Noodzaak van wetgeving

Eisen, erkenning en toezicht
Het is essentieel dat burgers en ondernemers met een of enkele middelen al hun zaken met publieke dienstverleners digitaal op een betrouwbare en veilige wijze en met waarborgen voor de privacy kunnen afhandelen. Dat vereist dat er eisen worden gesteld aan de partijen die zijn

betrokken bij de authenticatie, te weten de authenticatiediensten, machtigingsdiensten, attributendiensten en ontsluitende diensten, en aan de authenticatiemiddelen. Tevens moeten de diensten en middelen die aan deze eisen voldoen, erkend worden alvorens ze in het publieke domein hun diensten kunnen aanbieden, respectievelijk gebruikt mogen worden. Om er op toe te zien dat de betrokken partijen ook na hun erkenning aan de gestelde eisen blijven voldoen, zijn onafhankelijk toezicht en een handhavingsinstrumentarium onontbeerlijk. Het stellen van afdwingbare eisen en het in het leven roepen van een systeem van erkenning, toezicht en handhaving maken een regeling bij of krachtens de wet noodzakelijk.

Acceptatieplicht
Zonder wettelijke regeling kunnen publieke dienstverleners zelf bepalen welke authenticatiemiddelen zij accepteren. Dit is onwenselijk, gelet op het (overheidsbrede) belang van een veilige en betrouwbare authenticatie bij publieke dienstverlening. Het is dus cruciaal om vast te leggen dat publieke dienstverleners uitsluitend middelen accepteren die erkend zijn, dat wil zeggen aan voorgeschreven eisen voldoen. Evenmin kan zonder wettelijke regeling worden geborgd dat burgers en ondernemers met een of enkele middelen bij alle publieke dienstverleners terecht kunnen, wat de groei van hun digitale sleutelbos tot gevolg kan hebben. Een wettelijke acceptatieplicht is derhalve aangewezen om deze aanspraak te waarborgen en burgers en ondernemers te 'ontzorgen'.

Eisen aan de elektronische dienstverlening van publieke dienstverleners
Naast een wettelijke acceptatieplicht voor erkende middelen, is het voor een veilige en betrouwbare authenticatie tevens noodzakelijk dat de publieke dienstverleners er zorg voor dragen dat de toegang als tot hun elektronische dienstverlening veilig en betrouwbaar is. Hun eigen ICT-systemen op het punt van elektronische dienstverlening dienen derhalve eveneens veilig en betrouwbaar te zijn en onafhankelijke audits hierop zijn onmisbaar. Voor het stellen van kortgezegd veiligheidseisen aan deze ICT-systemen en de verplichting tot onafhankelijke audtis is eveneens een regeling bij en krachtens de wet aangewezen.

Gebruik publiek middel uitsluitend in publieke domein
Het behoort niet tot de taak van de rijksoverheid om publieke middelen te ontwikkelen en uit te geven die ook voor commerciële transacties als het online kopen van kleding, boeken of meubelen gebruikt kunnen worden. Sterker nog, de regering acht het ook onwenselijk indien de rijksoverheid zich zou mengen in deze markt. Een wettelijk verbod voor het gebruik van publieke middelen buiten het publieke domein is daarom aangewezen. Een (positief) neveneffect van een dergelijke verbod is overigens dat de uitgifte van private middelen, die wel voor bedoelde commerciële transacties gebruikt kunnen worden, wordt gestimuleerd.

Publieke authenticatiemiddelen
De verantwoordelijkheden en bevoegdheden van de minister van BZK ten aanzienvan een publiek middel dienen publiekrechtelijk te worden geregeld. Zo dient bij wettelijk voorschrift te worden bepaald wie in aanmerking komt voor een publiek authenticatiemiddel, hoe het middel wordt uitgegeven, hoe daarbij gebruik moet worden gemaakt van wettelijke registraties, dat er voor het middel dient te worden betaald en wanneer het middel vervalt of wordt ingetrokken. Het wetsvoorstel bevat de grondslag voor deze wettelijke voorschriften. Een publiekrechtelijke grondslag is tevens nodig om BSN te kunnen verwerken.

Verwerking persoonsgegevens
Een wettelijke grondslag is tenslotte nodig vanwege het feit dat in het kader van authenticatie sprake is van de verwerking van persoonsgegevens, waaronder het BSN, door niet alleen publieke, maar ook private partijen. In het wetsvoorstel worden hiertoe bij authenticatie betrokken erkende diensten benoemd die werkzaamheden uitoefenen die verband houden met een veilige en betrouwbare authenticatie in het publieke domein. Met name de goede werking van de voorziening BSN-Koppelregister, waarvoor de minister van BZK verantwoordelijk is, is afhankelijk van de aanlevering van bepaalde persoonsgegevens over de gebruiker van een middel, die dit wil gebruiken voor de afname van elektronische diensten in het publieke domein (zie onder 4.6 de functiebeschrijving van deze voorziening). Bij de aanlevering van deze persoonsgegevens, waaronder het BSN, aan de minister van BZK als beheerder van de voorziening spelen met name

genoemde private diensten een essentiële rol. Wettelijke verankering terzake is daarom noodzakelijk.

4.5. Multimiddelenaanpak

De toegang tot digitale dienstverlening voor burgers in het publieke domein is thans kwetsbaar omdat deze afhankelijk is van slechts één authenticatievoorziening, namelijk DigiD.[49] Indien DigiD door een ernstige storing of inbraak in het informatiesysteem (tijdelijk) niet beschikbaar is of gebruikt kan worden, loopt de gehele digitale dienstverlening van de overheid aan burgers vast, met alle maatschappelijke gevolgen van dien. Daarom kiest de regering in dit wetsvoorstel voor een multimiddelenaanpak. Dit betekent dat ook burgers straks met verscheidene publieke en private authenticatiemiddelen kunnen inloggen bij de overheid. Meerdere middelen van meerdere leveranciers hebben bovendien als voordeel dat meerdere technologieën naast elkaar worden gebruikt. Dat betekent ook vanuit dat gezichtspunt een reductie van kwetsbaarheid. Het heeft ook als voordeel dat er meer ruimte ontstaat voor snelle introductie van nieuwe technologische innovaties.

De multimiddelenaanpak maakt niet alleen de publieke dienstverlening – met name het inlogproces – minder kwetsbaar, waardoor de continuïteit van deze dienstverlening wordt vergroot, maar geeft burgers ook de mogelijkheid zelf te kiezen voor de middelen die men makkelijk vindt en waar men vertrouwen in heeft.

4.6. Authenticatiemiddelen voor burgers

Burgers krijgen met dit wetsvoorstel de beschikking over hoger beveiligde authenticatiemiddelen dan het huidige DigiD. Na realisatie van de multimiddelenaanpak krijgen burgers ook de mogelijkheid om zelf uit diverse erkende, publiek of privaat uitgegeven, authenticatiemiddelen te kiezen voor het inloggen bij dienstverleners in het publieke domein.

De ontwikkeling en de uitgifte van publieke authenticatiemiddelen voor burgers geschieden onder de verantwoordelijkheid van de minister van BZK. Er worden twee publieke middelen op een hoog betrouwbaarheidsniveau ontwikkeld waarbij de Nederlandse identiteitskaart en het rijbewijs de drager zijn, te weten de zogenaamde e-NIK en het e-rijbewijs. De bestaande chips in deze dragers wordt uitgerust met de daarvoor noodzakelijke functionaliteit (een applet) om authenticatie mogelijk te maken. Naast deze twee genoemde publieke middelen op betrouwbaarheidsniveau hoog komt er ook een publiek middel op betrouwbaarheidsniveau substantieel beschikbaar voor burgers: DigiD substantieel.

Het is voor de werking van alle erkende middelen noodzakelijk dat de rechthebbende beschikt over een BSN. Iedereen die in de basisregistratie personen (BRP) is ingeschreven beschikt over een BSN, ongeacht of hij als ingezetene of als niet-ingezetene is ingeschreven.

Dit wetsvoorstel bevat geen regeling over de categorieën van personen die in aanmerking komen voor de middelen. Voor wat betreft de publieke middelen zal dit – analoog aan de wijze waarop dit reeds met betrekking tot het huidige DigiD is geregeld – worden bepaald in op grond van dit wetsvoorstel bij ministeriële regeling vast te stellen (gebruiks)voorschriften. Deze kunnen relatief eenvoudig worden aangepast aan de ontwikkelingen niet alleen met betrekking tot de middelen zelf, maar ook met betrekking tot het uitgifteproces en de in dat verband te verifiëren identiteitsdocumenten.

Inherent aan de keuze om de Nederlandse identiteitskaart en het rijbewijs als drager te nemen is dat de beschikbaarheid van de publieke middelen op het betrouwbaarheidsniveau hoog is beperkt tot de groep burgers die beschikt over een BSN en in het bezit is van dan wel recht heeft op een Nederlandse identiteitskaart (NIK) of een Nederlands rijbewijs. DigiD substantieel is een combinatie van het huidige DigiD met toevoeging van een controle aan de hand van (vooralsnog)

[49] *Voor ondernemers zijn al meerdere middelen van verscheidene leveranciers, onder de naam eHerkenning, beschikbaar.*

het Nederlands paspoort, de Nederlandse identiteitskaart of een Nederlands rijbewijs. Degene die inlogt met DigiD moet vervolgens voor de verstrekking van DigiDsubstantieel aantonen – via een kaartlezer of anderszins – dat hij of zij in het bezit is van één van de genoemde identiteitsdocumenten. Dit betekent dat (voorshands) uitsluitend houders van deze documenten in aanmerking kunnen komen voor DigiD substantieel.

Het streven is er op gericht om in een later stadium houders van andere wettelijke identiteitsdocumenten, zoals het identiteitsdocument voor vreemdelingen, aan de groep rechthebbenden op een publiek middel toe te voegen. Hierbij spelen beleidsmatige, juridische, technische en financiële overwegingen een rol. Dat aan bepaalde categorieën burgers op grond van het onderhavige wetsvoorstel geen publieke middelen wordt verstrekt, laat onverlet dat zij in aanmerking kunnen komen voor private middelen. Bovendien blijven bestuursorganen op grond van de Algemene wet bestuursrecht verplicht om bij hun dienstverlening de schriftelijke weg open te stellen. Dit is alleen anders indien bij of krachtens de wet de elektronische weg is voorgeschreven. Bezien zal worden welke oplossing voor die situatie aangewezen is, bijvoorbeeld in de vorm van machtigen.

De uitgifte van private authenticatiemiddelen voor burgers en de verstrekking ervan aan de gebruiker, vindt plaats door de door de minister van BZK erkende private authenticatiediensten. Zij bepalen in beginsel zelf de kring van rechthebbenden op 'hun' middel, waarbij het in ieder geval zal gaan om burgers die over een BSN en een wettig identiteitsdocument beschikken. Met in acht neming daarvan is het is aan de desbetreffende authenticatiedienst om te bepalen aan welke categorie burgers hij dit middel wil uitgeven.

Tot slot het volgende. Met behulp van zogeheten PKIoverheid-certificaten (*public key infrastructure*) kunnen websites worden geïdentificeerd en kan het verkeer met deze websites worden beveiligd. Ook kan met PKIoverheid informatie-uitwisseling van systeem naar systeem worden beveiligd en kunnen gekwalificeerde elektronische handtekeningen worden gezet. Daarnaast kunnen personen zich met een middel waarvoor het PKIoverheid-certificaat is afgegeven, authenticeren op systemen. Een dergelijke middel zou, indien wordt voldaan aan de in en krachtens dit wetsvoorstel gestelde eisen, de status van erkend middel kunnen verkrijgen.

Uitgifte van authenticatiemiddelen voor burgers
In op grond van dit wetsvoorstel vast te stellen uitvoeringsregelgeving zullen eisen worden gesteld aan de uitgifte van authenticatiemiddelen op de verschillende betrouwbaarheidsniveaus. Bij de formulering van deze eisen worden de relevante bepalingen uit de Europese eIDAS verordening[50] inzake de betrouwbaarheid en het uitgifteproces meegenomen. De in deze verordening opgenomen classificatie van authenticatiemiddelen naar betrouwbaarheidsniveau ('laag', 'substantieel' en 'hoog') wordt hierbij gevolgd, zij het dat dit wetsvoorstel alleen betrekking heeft op private en publieke middelen met betrouwbaarheidsniveau substantieel en hoog.

De verificatie van de identiteit van de aanvrager is voor deze betrouwbaarheidsniveaus van groot belang; authenticatiemiddelen worden niet verstrekt dan nadat de identiteit van de aanvrager is geverifieerd. Dit geldt zowel voor de publieke als de private middelen. Verificatie geschiedt in ieder geval door de opgegeven gegevens van de aanvrager te controleren aan de hand van in de BRP opgenomen gegevens, maar ook aan de hand van andere methodes om er zeker van te zijn dat de aanvrager ook daadwerkelijk is wie hij zegt te zijn, bijvoorbeeld een *face to face* controle.

BSN Koppelregister
Het BSN Koppelregister (BSN-K) is een voorziening in het kader van de GDI. De minister van BZK is verantwoordelijk voor de werking, betrouwbaarheid en veiligheid ervan. Het BSN-K stelt een authenticatiedienst in staat om een publieke dienstverlener op een veilige en betrouwbare manier het BSN te leveren van een gebruiker van een authenticatiemiddel. Daarnaast stelt het BSN-K de gebruiker in staat om met behulp van een inzagefunctie controle te houden over zijn authenticatiemiddelen.

---

[50] Verordening (EU) nr. 910/2014 van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt, PB L 257 van 28.8.2014, blz. 73.

Het BSN-K kent de volgende vier functionaliteiten.

Activeren van het middel voor het publieke domein
Wanneer een burger in de toekomst een privaat of publiek authenticatiemiddel aanschaft en hij dit middel wil gebruiken in het publieke domein, wordt voor zijn middel een zogeheten polymorfe identiteit en een polymorfe pseudoniem gegenereerd. Hiertoe stuurt de authenticatiedienst, die het middel heeft uitgegeven, het BSN van de burger samen met controlegegevens (die overgenomen worden van het identiteitsdocument van de gebruiker) naar het BSN-K. Na controle genereert het BSN-K een polymorfe identiteit en een polymorfe pseudoniem en verstrekt dit aan de authenticatiedienst. De polymorfe *identiteit* kan gebruikt worden ten behoeve van publieke dienstverleners die voor de desbetreffende dienst uiteindelijk het BSN moeten ontvangen. De polymorfe *pseudoniem* is weliswaar gebaseerd op het BSN van de betrokken burger, maar daar kan de dienstverlener niet meer het BSN uit halen. De polymorfe pseudoniem is daarom bedoeld voor toepassingen waar het BSN niet nodig is, maar de privacy wel van belang is. Tenslotte wordt het authenticatiemiddel geregistreerd in het inzageregister.

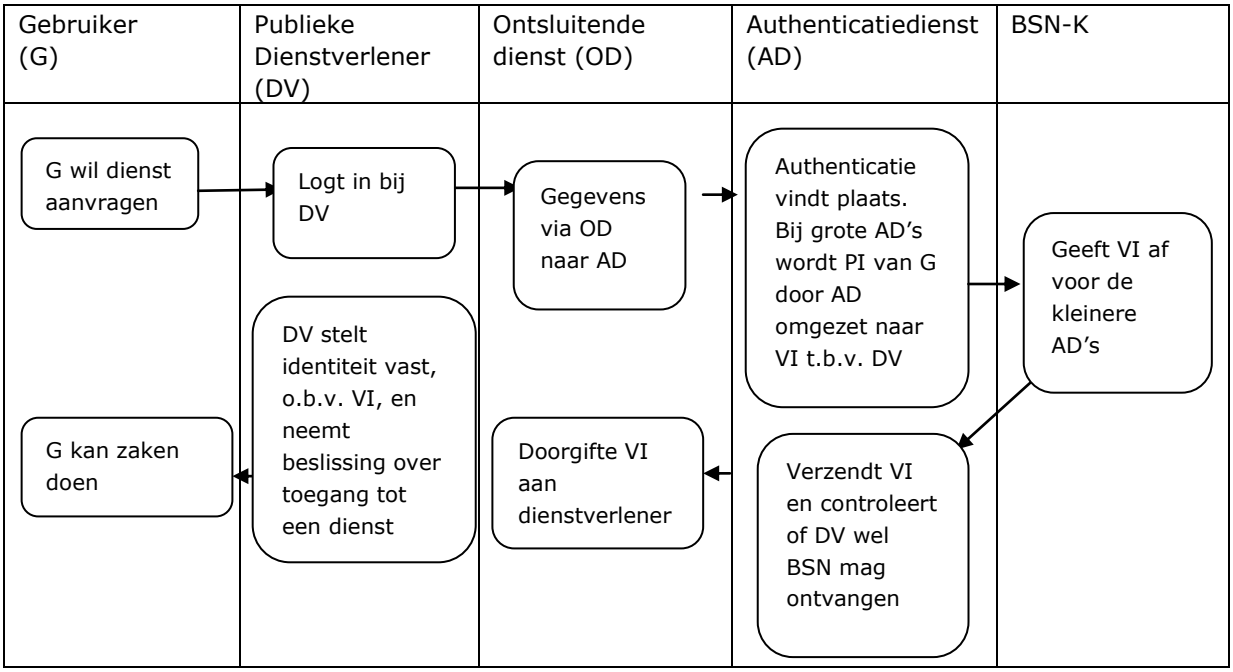
Gebruik middel
Het BSN-K speelt ook een rol in het authenticatieproces. Wanneer een gebruiker van een middel bij een publieke dienstverlener wil inloggen, ontvangt de authenticatiedienst een authenticatieverzoek. Een kleinere authenticatiedienst laat de polymorfe identiteit van de gebruiker, via het BSN-K, transformeren tot een voor de betreffende dienstverlener versleutelde identiteit, waarin het BSN van de gebruiker is versleuteld. Een grotere authenticatiedienst zal deze transformatie zelf doen.

Het gebruik van de polymorfe identiteit is een belangrijke maatregel om de privacy te beschermen. Door versleutelingstechnieken levert dit voor iedere dienstverlener waar men inlogt, een unieke versleutelde identiteit op. Hierdoor wordt het onmogelijk om de identiteit van de gebruiker te achterhalen of het inloggen bij verschillende dienstverleners aan elkaar te koppelen. Alleen de publieke dienstverlener kan het BSN uit de versleutelde identiteit destilleren. Indien de dienstverlener geen BSN nodig heeft, respectievelijk de dienstverlener het BSN niet mag gebruiken, zal de authenticatiedienst het polymorfe pseudoniem van de gebruiker transformeren naar een versleuteld pseudoniem.

Inzageregister
Een burger moet kunnen vaststellen of zijn authenticatiemiddel actief is of is geweest binnen het publieke domein. Dit kan hij doen in het inzageregister. Een authenticatiedienst is verplicht om de status van elk authenticatiemiddel (bijvoorbeeld: actief, inactief of ingetrokken) te registreren bij het inzageregister van het BSN-K. De registratie vindt plaats met een specifiek versleuteld pseudoniem voor het inzageregister (dus niet het BSN of de polymorfe identiteit of het polymorfe pseudoniem) en een identificatie en omschrijving van het betreffende authenticatiemiddel. Het inzageregister geeft geen inzicht in het gebruik dat van de middelen wordt gemaakt. Alleen de status wordt vermeld en alleen de desbetreffende burger heeft hier inzage in.

Sleutelbeheer en operationeel beheer
Om de veiligheid te waarborgen, wordt cryptografisch sleutelmateriaal verstrekt door het BSN-K. Het BSN-K beheert en verstrekt cryptografisch sleutelmateriaal aan authenticatiediensten om opgenomen te worden in hun speciaal beveiligd computer systeem zoals beschreven bij het vaststellen van het versleutelde BSN of pseudoniem. Hiermee kan een authenticatiedienst een polymorfe identiteit of een polymorfe pseudoniem van een gebruiker omzetten in een voor de betreffende publieke dienstverlener versleutelde identiteit, repectievelijk versleutelde pseudoniem. Daarnaast verstrekt het BSN-K cryptografisch sleutelmateriaal aan deze dienstverleners. De dienstverlener ontsleutelt hiermee het BSN of versleutelde pseudoniem van de gebruiker dat de authenticatiedienst verstrekt.

Werking van het authenticatieproces
Een publieke dienstverlener weet niet van te voren met welk middel een burgers zich meldt. Dit is vergelijkbaar met betalen via internet: de webwinkel weet ook niet van te voren via welke methode en via welke bank een klant zal betalen. Onder 'eID-stelsel', zijn de verschillende partijen, die bij authenticatie betrokken diensten aanbieden, benoemd en is hun functie kort beschreven.
In het onderstaande stroomschema wordt de werking van het eID-stelsel en met name het gebruik van een middel in het publieke domein geïllustreerd.



Overige afkortingen:
PI= polymorfe identiteit
VI= versleutelde identiteit.
NB. Dit schema is van toepassing indien voor de dienstverlening een BSN nodig is. Voor de situatie dat geen BSN nodig is, dient voor 'PI' te worden gelezen 'PP' (polymorfe pseudoniem) en voor 'VI' te worden gelezen 'VP' (versleutelde pseudoniem). In dat geval hoeft de AD niet te controleren of de DV het BSN mag ontvangen.

<u>Procesbeschrijving:</u>
Voor het gebruik van een authenticatiemiddel gaat de gebruiker online naar een publieke dienstverlener. Vervolgens leidt de ontsluitende dienst de gebruiker voor het authenticatieproces naar de authenticatiedienst. De authenticatiedienst authenticeert de gebruiker met behulp van diens middel. Vervolgens bepaalt de (grotere) authenticatiedienst op basis van de polymorfe identiteit (PI) van de gebruiker de voor de desbetreffende dienstverlener specifieke versleutelde identiteit (VI). Alleen de publieke dienstverlener kan de versleutelde identiteit omzetten in een BSN. Bij kleinere authenticatiediensten zal deze versleutelde identiteit worden afgegeven door het BSN-K. Grote authenticatiediensten hanteren een bepaalde techniek zodat zij zelf voor een transactie een polymorfe identiteit transformeren in een versleutelde identiteit. Hiermee wordt voorkomen dat het BSN-K overspoeld raakt met aanvragen.
Een publieke dienstverlener die geen BSN mag ontvangen krijgt in plaats van een versleutelde identiteit een versleuteld pseudoniem (VP). In dat geval transformeert de authenticatiedienst een polymorfe pseudoniem in een voor de desbetreffende dienstverlener versleutelde pseudoniem. De grote authenticatiedienst kan deze transformatie zelf doen, de kleinere doet dit met behulp van het BSN-K. Het voor de desbetreffende dienstverlener versleutelde pseudoniem gaat richting de dienstverlener via de ontsluitende dienst.

4.7. Authenticatiemiddelen voor ondernemers

Publieke dienstverlening richt zich zowel op burgers als op ondernemers. Wel zijn er enkele verschillen tussen de mogelijkheden voor authenticatie voor de dienstverlening aan burgers en aan ondernemers. Publieke middelen zijn bedoeld om als burger in contact te komen met bestuursorganen en aangewezen organisaties. Indien een KvK nummer[51] of RSIN nummer[52] vereist is voor authenticatie, kan niet uitsluitend met een publiek middel worden ingelogd. En daar waar burgers normaal gesproken volledig bevoegd zijn om namens zichzelf te handelen, is dat voor handelen door of namens een ondernemer (niet zijnde de eigenaar van een eenmanszaak) veelal niet het geval.

Voor het handelen als ondernemer is destijds het stelsel voor e-Herkenning ontwikkeld. De middelen die thans binnen dat stelsel worden gebruikt, zullen op grond van dit wetsvoorstel erkend moeten worden om ook in de toekomst in het publieke domein gebruikt te kunnen worden. In de op grond van dit wetsvoorstel vast te stellen uitvoeringsregelgeving zullen aan de middelen voor ondernemers dezelfde eisen worden gesteld als aan de middelen voor burgers. Ook zal sprake zijn van dezelfde betrouwbaarheidsniveaus als voor de middelen voor burgers. Maar daar waar een middel voor burgers wordt gekoppeld aan een BSN, wordt dit bij middelen voor ondernemers gekoppeld aan een KvK of RSIN nummer. En waar een burger in beginsel voor alles bevoegd is, zal, net als nu al het geval is, bij een middel voor een ondernemer vastgelegd worden waarvoor de betreffende medewerker bevoegd is. Die bevoegdheid kan volledig zijn, bijvoorbeeld wanneer het een middel voor een algemeen directeur of een eigenaar van een eenmanszaak betreft, maar het kan ook beperkt zijn tot een of enkele diensten. Zo kan de ene medewerker als bevoegdheid krijgen om digitaal rapporten aan een inspectiedienst aan te leveren, of om met die inspectiedienst te communiceren, terwijl een andere medewerker bevoegd wordt om de omzetbelasting aan te geven.

Uitgifte van authenticatiemiddelen voor ondernemers
Bij de uitgifte van middelen voor ondernemers zal een vergelijkbare procedure gehanteerd gaan worden als bij uitgifte van middelen voor burgers. Tevens wordt bij de verstrekking vastgelegd voor welke zaken de houder van dit middel bevoegd is namens de onderneming. Die bevoegdheid kan uiteenlopen van een enkele dienst tot volledig bevoegd. Deze bevoegdheid kan overigens later altijd gewijzigd worden. Op deze manier is er geen noodzaak een nieuw middel aan te schaffen als een medewerker andere taken krijgt. Men hoeft alleen de bevoegdheden van die medewerker te wijzigen.

Wanneer een middel voor ondernemers wordt uitgegeven, moet door de authenticatiedienst wel worden vastgesteld dat degene, die het middel aanvraagt namens een medewerker en laat koppelen aan het KvK- of RSIN-nummer, daartoe bevoegd is. Dat wordt gedaan op basis van de bevoegdheden die zijn vastgelegd in het Handelsregister.

Het staat private authenticatiediensten vrij om middelen voor ondernemers en burgers of alleen voor ondernemers of alleen voor burgers uit te geven. Publieke authenticatiediensten geven alleen middelen voor natuurlijke personen uit.

4.8. Erkenning van authenticatiemiddelen en partijen

Met dit wetsvoorstel wordt de erkenning van publieke en private middelen voor burgers en ondernemers onder één publiekrechtelijk stelsel gebracht. Er worden gelijkluidende eisen gesteld waaraan deze middelen voor gebruik in het publieke domein moeten voldoen, alsook waaraan betrokken (publieke en private) partijen moeten voldoen. Aldus wordt bewerkstelligd dat er een betrouwbare en veilige authenticatieketen ontstaat. Alleen middelen op een

[51] *Alle ondernemingen en organisaties die zich inschrijven in het Handelsregister krijgen een KvK-nummer. KvK staat voor Kamer van Koophandel.*
[52] *Alle rechtspersonen en samenwerkingsverbanden, zoals bv's, verenigingen, stichtingen, vof's en maatschappen (eenmanszaken niet) krijgen bij inschrijving bij de KvK naast een KvK-nummer ook een Rechtspersonen en Samenwerkingsverbanden Informatienummer (RSIN). Dit nummer wordt gebruikt om gegevens uit te wisselen met andere (overheids)organisaties, zoals de Belastingdienst.*

betrouwbaarheidsniveau 'substantieel' en 'hoog' zullen worden erkend. Middelen op een lager betrouwbaarheidsniveau, zoals het bestaande DigiD, zullen niet worden erkend. In het wetsvoorstel is bepaald dat deze middelen na een overgangsperiode van 3 jaar niet meer bruikbaar zijn. Tot die tijd kunnen ze nog bij een dienstverlening op het betrouwbaarheidsniveau laag worden gebruikt.

De minister van BZK besluit, in overeenstemming met de minister van EZ, op grond van dit wetsvoorstel over het erkennen van een publieke of private partij die een dienst binnen de authenticatieketen wil aanbieden en over het erkennen van door een publieke of private authenticatiedienst uitgegeven middelen. Dit is een besluit in de zin van artikel 1:3 van de Awb waartegen bezwaar en beroep open staat.

Rol van Agentschap Telecom bij de erkenning
Het voornemen bestaat om na de invoering van de wet Agentschap Telecom te betrekken bij het proces van erkenning van partijen die een dienst aanbieden binnen de authenticatieketen en van authenticatiemiddelen. Een partij die erkend wil worden moet hiertoe een aanvraag indienen bij de minister van BZK. Ditzelfde geldt voor een aanvraag tot erkenning van een authenticatiemiddel. De aanvraag dient te worden vergezeld van een verklaring van een geaccrediteerde certificerende instelling dat aan de ingevolge artikel 7 gestelde eisen wordt voldaan alsmede van het auditrapport waar deze verklaring op is gebaseerd.

De geaccrediteerde certificerende instelling die de verklaring van conformiteit aan de in artikel 7 gestelde eisen afgeeft, werkt in opdracht van en rapporteert aan de partij die erkenning vraagt. De instelling die de verklaring afgeeft, dient hiertoe geaccrediteerd te zijn door de Raad voor Accreditatie. Deze baseert de accreditatie op een hiertoe door de minister van BZK van toepassing verklaard conformiteitbeoordelingsschema. Dit schema is gebaseerd op de internationale standaard ISO/IEC 17065. De minister van BZK zal een beheerder van dit schema aanwijzen.

Nadat de minister van BZK een aanvraag tot erkenning heeft ontvangen, zal hij de minister van EZ hierbij betrekken. Deze zal het onder zijn verantwoordelijke ressorterende Agentschap Telecom inschakelen om te beoordelen of de aanvrager aan de eisen bij of krachtens dit wetsvoorstel voldoet. Bij zijn oordeelsvorming maakt Agentschap Telecom gebruik van de informatie die wordt aangeleverd door de partij die erkend wenst te worden. Daarbij kan aanvullend onderzoek worden uitgevoerd. Dit onderzoek kan onder andere bestaan uit inzage in de werking van processen.

De minister van BZK besluit, in samenspraak met de minister van EZ, op basis van het oordeel van Agentschap Telecom of een partij of authenticatiemiddel wordt erkend. De minister kan besluiten, ondanks een positieve conformiteitsbeoordeling en een positief oordeel van Agentschap Telecom, niet tot de gevraagde erkenning over te gaan indien zwaarwegende redenen zich tegen erkenning verzetten, zoals de staatsveiligheid die in het geding komt. Ook bij een negatief oordeel van Agentschap Telecom omdat de betreffende dienst of middel niet aan gestelde eisen voldoet, kan de minister van anders beslissen en een dienst of middel voorlopig erkennen indien anders essentiële dienstverlening in gevaar komt. In een dergelijk geval kan de minister voorwaarden verbinden aan die voorlopige erkenning. Ook los daarvan heeft de minister de bevoegdheid aan een erkenning voorschriften of beperkingen te verbinden. Wanneer bijvoorbeeld een aanvrager op ondergeschikte punten niet of niet geheel voldoet aan de voorwaarden, maar die punten betreffen niet de betrouwbare en veilige werking van de authenticatie, kan de minister besluiten deze partij voorlopig te erkennen, onder voorwaarde dat de gebreken binnen een aan te geven termijn worden opgelost. Nadat een partij of door hem uitgegeven middel is erkend, valt hij onder het toezicht van daartoe door de minister van BZK aangewezen ambtenaren.

4.9. Acceptatieplicht en veilige toegang tot elektronische dienstverlening

Burgers en ondernemers moeten er op kunnen vertrouwen dat zij met een erkend middel overal in het publieke domein terecht kunnen. Dat vereist dat bestuursorganen en aangewezen organisaties alle erkende middelen moeten accepteren, voor zover zij minimaal het voor de af te nemen dienst vereiste betrouwbaarheidsniveau hebben. Daarom is in dit wetsvoorstel voor de bestuursorganen en aangewezen organisaties de verplichting opgenomen om alle erkende middelen te accepteren.

Bestuursorganen en aangewezen organisaties zullen hun diensten, systemen en werkprocessen op de acceptatieplicht moeten aanpassen.

Om de veiligheid en betrouwbaarheid van het gehele authenticatieproces te kunnen waarborgen, mogen bestuursorganen en aangewezen organisaties ook alleen zaken doen met, dat wil zeggen gebruik maken van, erkende partijen, zoals authenticatiediensten en machtigingsdiensten. Ook mogen de publieke dienstverleners uitsluitend erkende middelen accepteren. Van deze middelen is aangetoond dat deze voldoen aan ingevolge dit wetsvoorstel te stellen eisen inzake werking, veiligheid en betrouwbaarheid. Hierop wordt bovendien toezicht gehouden.

Het gebruik van erkende middelen en erkende diensten is echter niet voldoende voor een veilige en betrouwbare authenticatie. De interne ICT-systemen van de publieke dienstverleners zelf dienen vanzelfsprekend ook veilig en betrouwbaar te zijn. Met het oog daarop worden op grond van dit wetsvoorstel ook ten aanzien van de publieke dienstverleners nadere eisen gesteld met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang tot hun elektronische dienstverlening.

4.10. Ondertekendienst en technische bewerker

Dit wetsvoorstel kent een viertal partijen (normadressaten) die een rol spelen in de authenticatieketen, waarop de regelgeving van toepassing is. Dat zijn de authenticatiedienst, de attributendienst, de ontsluitende dienst en de machtigingsdienst. Deze partijen moeten door de minister van BZK worden erkend om toegelaten te worden tot het publieke domein.

De keuze om de werking van het wetsvoorstel te beperken tot deze vier normadressaten is gebaseerd op de aard van hun rol in de authenticatieketen. Deze partijen zijn nodig om voor de burgers en ondernemers een goede toegang tot de elektronische dienstverlening van de bestuursorganen en aangewezen organisaties mogelijk te maken, en voor de bestuursorganen en aangewezen organisaties om betrouwbare partners te hebben die deze toegang mogelijk maken. Het is mogelijk dat er in de loop van de tijd andere partijen ontstaan die diensten verlenen die gebruikt worden bij de toegang tot de elektronische dienstverlening van bestuursorganen en aangewezen organisaties.

Voorbeelden van dergelijke andere partijen zijn de ondertekendienst en de technische bewerker. Een ondertekendienst is een partij die er voor zorgt dat documenten en formulieren op elektronische wijze rechtsgeldig kunnen worden ondertekend. Een ondertekendienst wordt in opdracht van een bestuursorgaan of aangewezen organisatie ingeschakeld om burgers en ondernemers formulieren en documenten elektronisch te laten ondertekenen. Een technische bewerker is een service provider die in opdracht van een bestuursorgaan of aangewezen organisatie onder meer ervoor zorgt dat een bestuursorgaan of aangewezen organisatie kan voldoen aan de acceptatieplicht. De technisch bewerker verzorgt dat alle koppelvlakken die door de ontsluitende diensten worden aangeboden, gebruikt kunnen worden door het bestuursorgaan of de aangewezen organisatie. Het is niet nodig aan deze andere partijen als de ondertekendienst en de technisch bewerker dezelfde ingrijpende verplichtingen op te leggen als aan de bovengenoemde vier partijen die een cruciale rol spelen in de authenticatieketen. De reden hiervoor is dat deze andere partijen niet een zelfstandige rol in de authenticatieketen vervullen, maar dat zij in opdracht van een bestuursorgaan of een aangewezen organisatie handelen. Dit bestuursorgaan of deze aangewezen organisatie is verantwoordelijk voor het handelen van deze partijen en moet er dus op toezien dat deze partijen hun werkzaamheden correct verrichten.

4.11. Authenticatie binnen de Europese Unie met Nederlandse middelen

Uit de eIDAS verordening[53] volgt dat een authenticatiemiddel dat is uitgegeven op grond van een stelsel voor elektronische identificatie, dat is opgenomen in een lijst die de Europese Commissie heeft bekendgemaakt, ook in andere lidstaten van de Europese Unie erkend moeten worden. Het

[53] Artikel 6 van de Verordening (EU) nr. 910/2014 van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt, PB L 257 van 28.8.2014.

voornemen bestaat om ook het Nederlandse stelsel bij de Europese Commissie te notificeren. De consequentie daarvan zal zijn dat de houders van de in Nederland erkende middelen gerechtigd zijn zich ook in andere lidstaten van de Europese Unie met deze middelen te authenticeren jegens publieke dienstverleners. Op grond van de eIDAS verordening geldt de acceptatieplicht voor publieke dienstverleners in alle lidstaten. Dit geldt voor de erkende publieke en private middelen.

5. Elektronische bevoegdheidsvaststelling

5.1. Inleiding

Digitalisering van de dienstverlening in het publieke domein mag er niet toe leiden dat mensen belemmeringen ondervinden bij het zaken doen met de overheid. Er zijn op hoofdlijnen drie situaties te onderscheiden waarin mensen niet zelf hun zaken met de overheid regelen: zij *willen* hun zaken niet zelf regelen (bijvoorbeeld uit gemaksoverwegingen), ze *kunnen* deze niet zelf regelen (zij hebben moeit met de complexiteit van overheidszaken, of zij missen digitale vaardigheden) of zij *mogen* hun zaken niet zelf regelen (bijvoorbeeld omdat hun handelingsbekwaamheid beperkt is).

De regering rekent het tot haar verantwoordelijkheid om ook kaders te stellen voor elektronische bevoegdheidsvaststelling. Bij het vaststellen van een bevoegdheid van een persoon kan het gaan om de beoordeling of hij bevoegd is om een dienst af te nemen voor zichzelf, ofwel voor een ander.

In het eerste geval (optreden namens zichzelf) kan gedacht worden aan het controleren van een leeftijd bij het afnemen van bepaalde diensten. Dit gebeurt bij een attributendienst. Aan attributendiensten worden in op basis van dit wetsvoorstel vast te stellen uitvoeringsregelgeving technische en organisatorische eisen gesteld en er wordt voorzien in een erkenningsstelsel, op gelijke wijze als bij authenticatiediensten. Op dit moment zijn er nog geen publieke en private attributendiensten operationeel, maar met uitbreiding van de digitale dienstverlening zal ook de behoefte aan elektronische ondersteuning van deze functie toenemen.

In het tweede geval (optreden namens een ander) gaat het om het controleren van een bevoegdheid op basis van een volmacht of een wettelijke bevoegdheid. Dit gebeurt bij een machtigingsdienst. Ook aan machtigingsdiensten worden in op grond van dit wetsvoorstel vast te stellen uitvoeringsregelgeving technische en organisatorische eisen gesteld en ook zij vallen onder het hierin geregelde erkenningsstelsel. Daarnaast maakt de zorg voor een publieke machtigingsdienst onderdeel uit van de verantwoordelijkheid van de minister van BZK voor veilige en betrouwbare toegang tot elektronische dienstverlening. De publieke machtigingsdienst is beschikbaar voor natuurlijke personen die zich willen of moeten laten vertegenwoordigen. Voor rechtspersonen zijn private voorzieningen beschikbaar om bijvoorbeeld de bevoegdheid te registeren en te beoordelen van medewerkers die elektronisch zaken met de overheid regelen namens het bedrijf.

In de volgende paragrafen wordt ingegaan op de functie en werking van de verschillende soorten bevoegdheidsdiensten.

5.2. Publieke machtigingsdienst

Op grond van artikel 2:1 van de Algemene wet bestuursrecht kan een ieder zich ter behartiging van zijn belangen in het verkeer met bestuursorganen laten bijstaan of door een gemachtigde laten vertegenwoordigen. Dat geldt ook bij elektronische dienstverlening in het publieke domein: diensten kunnen ook door een ander namens de belanghebbende digitaal worden afgenomen, bijvoorbeeld door een familielid, een vriend of een medewerker van een maatschappelijke of commerciële dienstverlener (vakbond, juridisch adviseur ed.). Aangezien een authenticatiemiddel persoonlijk is, kan een gebruiker dit niet aan een ander geven in geval hij niet in staat of in de gelegenheid is om zelf digitaal zaken te doen met de overheid. Op grond van het wetsvoorstel kunnen regels worden opgelegd aan de gebruiker van een erkend middel; die regels zullen ook de niet-overdraagbaarheid van middelen betreffen. Om redenen van toegankelijkheid van publieke

digitale dienstverlening wordt voorzien in een publieke machtigingsdienst, waarin elektronisch de toestemming wordt vastgelegd van een persoon dat een andere persoon (met zijn eigen authenticatiemiddel) de overheidszaken van de eerstgenoemde mag regelen. Aan deze registratie ligt een volmacht ten grondslag of in elk geval een afspraak tussen de betrokkene en zijn gemachtigde om zaken voor hem te regelen. De betrokkene bepaalt zelf waarvoor hij iemand machtigt en voor hoe lang.

Machtiging is ingevolge het Burgerlijk Wetboek en de Awb vormvrij. Registratie bij een machtigingsdienst is dus geen voorwaarde voor het *ontstaan* van een vertegenwoordigingsrelatie, maar wel een voorwaarde voor digitale machtiging. Een machtigingsdienst controleert niet of de volmacht die aan de registratie van de machtiging ten grondslag ligt, daadwerkelijk rechtsgeldig is,bijvoorbeeld of de volmachtgever handelingsbekwaam was op het moment van afgeven van de volmacht en registratie van de machtiging. Zonder de registratie van een machtiging is het niet mogelijk om namens een ander te handelen met een bestuursorgaan of aangewezen organisatie.

Op dit moment is DigiD Machtigen de publieke dienst voor het elektronisch registreren van machtigingen tussen burgers onderling. Daarnaast verlenen verschillende private leveranciers machtigingsdiensten in het verkeer tussen ondernemers en overheid, in het kader van het stelsel eHerkenning. De werking van DigiD Machtigen is beschreven in de nota van toelichting op het Besluit verwerking persoonsgegevens generieke digitale infrastructuur, dat gebaseerd is op artikel X van de Wet elektronisch berichtenverkeer Belastingdienst (Wet EBV). Dit besluit zal via artikel 26 van dit wetsvoorstel mede worden gebaseerd op de Wet GDI. Kortheidshalve wordt voor de werking van Digid Machtigen naar de beschrijving in de nota van toelichting bij het besluit verwezen.[54]

Het voornemen is om DigiD Machtigen uit te breiden met de registratie van machtigingen van degenen die namens de nabestaanden van een overledene toegang hebben tot diensten van publieke dienstverleners. Met behulp van zo'n nabestaandenmachtiging kunnen zaken van de overledene die nog afhandeling behoeven, worden afgewikkeld. Ook kan informatie worden geraadpleegd en afgehandeld (bijvoorbeeld het inzien en downloaden van resterende digitale post in de Berichtenbox van MijnOverheid). De beoogde werking van de nabestaandenmachtiging zal worden beproefd in een pilot bij de Belastingdienst. Op basis daarvan wordt besloten of en op welke wijze deze functionaliteit structureel wordt opgenomen in DigiD Machtigen. Een dergelijke functionaliteit zal vorm krijgen in de op grond van dit wetsvoorstel vast te stellen uitvoeringsregelgeving.

Een andere uitbreiding van de mogelijkheden in DigiD Machtigen betreft de mogelijkheid om een machtigingsrelatie tussen een natuurlijke persoon en een rechtspersoon te registeren, de zogenoemde burger-organisatiemachtiging. Ook hiervoor geldt dat dit in de op grond van dit wetsvoorstel vast te stellen uitvoeringsregelgeving zal worden geregeld.

5.3. Wettelijke vertegenwoordiging

Er zijn situaties waarin een natuurlijke persoon niet voor zichzelf rechtshandelingen kan verrichten, als gevolg van gehele of gedeeltelijke handelingsonbekwaamheid. Het ligt in de rede dat ook hun wettelijke vertegenwoordigers namens hen gebruik kunnen maken van elektronische diensten van publieke dienstverleners. Het recht op elektronisch zaken doen zoals neergelegd in de Algemene wet bestuursrecht geldt ook voor hen. Daarnaast is het wenselijk dat situaties waarin wettelijke vertegenwoordiging in het spel is, niet hoeven te worden uitgezonderd van elektronisch verkeer bij bestuursorganen die dat verplicht hebben gesteld, zoals het UWV en de Belastingdienst. Met het oog hierop zal aan DigiD Machtigen een functionaliteit worden toegevoegd voor de registratie van bevoegdheden van bewindvoerders en curatoren.

[54] *Zie Stb. 2016, 195, p. 15 e.v..*

5.4. Attributen

Het toetsen van de bevoegdheid om diensten af te nemen is niet alleen relevant in situaties waarin een ander voor de belanghebbende optreedt, maar ook in situaties waarin bepaalde eigenschappen of kenmerken van de belanghebbende zelf bepalend zijn voor zijn bevoegdheid om (rechts)handelingen te verrichten. Zo is het afnemen van bepaalde overheidsdiensten gekoppeld aan een leeftijdsgrens, of aan het hebben van bepaalde kwalificaties, blijkend uit een erkenning of registratie. Voorbeelden van dit laatste vormen de inschrijving van advocaten op grond van de Advocatenwet en die van medische beroepsbeoefenaren op grond van de Wet beroepen in de individuele gezondheidszorg. Bij het uitoefenen van bepaalde handelingen moet hun bevoegdheid op grond van deze inschrijving geverifieerd kunnen worden.

Bevoegdheidskenmerken van een persoon worden aangeduid als attributen. Zij kunnen bij het inloggen in een voorziening voor elektronische dienstverlening worden meegeleverd door het in het authenticatieproces aanroepen van een zogenoemde attributendienst waarin deze kenmerken zijn vastgelegd. Deze attributendiensten kunnen publiek of privaat zijn. Te denken valt bijvoorbeeld aan een generieke attributendienst die leeftijdsverificatie mogelijk maakt op basis van de basisregistratie personen. Tot nu toe verrichten publieke dienstverleners waar nodig zelf de leeftijdscontrole aan de hand van de eigen klantadministratie (die in de regel is afgeleid van de BRP).
Het wetsvoorstel bevat een basis voor het stellen van technische en organisatorische eisen aan publieke en private attributendiensten. Of in de toekomst behoefte bestaat aan een publieke attributendiensten is nog onderwerp van onderzoek.

6. Informatiebeveiliging

6.1. Inleiding

Door de vergaande digitalisering van processen in de samenleving, waaronder processen bij de rijksoverheid, medeoverheden en private partijen, is de beveiliging van (digitale) informatie en ICT-systemen van essentieel belang. Informatiestromen beperken zich daarbij niet tot de eigen organisaties. Dit geldt bij uitstek ook voor het BSN-K, de authenticatiediensten en de ontsluitende diensten, die niet alleen een eigen informatiestroom hebben naar andere organisaties, maar die ook een ketenfunctie vervullen in de toegang tot elektronische dienstverlening van deze organisaties.

Burgers, ondernemers en overheden zelf moeten er op kunnen vertrouwen dat partijen in de keten hun informatiebeveiliging goed op orde hebben en beschikbaarheid, integriteit en vertrouwelijkheid (klassieke informatiebeveiliging) alsmede authenticiteit, onweerlegbaarheid, transparantie en flexibiliteit borgen. De stand van zaken met betrekking tot de informatiebeveiliging moet daarnaast controleerbaar of auditbaar zijn, zodat zo nodig passende maatregelen kunnen worden getroffen of verantwoording kan worden afgelegd.

Voor de goede orde wordt opgemerkt dat informatiebeveiliging een veel breder aandachtsgebied omvat dan uitsluitend bescherming van persoonsgegevens, waartoe vaak de aandacht uitgaat. Het vormt binnen de overheidscontext een randvoorwaarde voor de algemene beginselen van behoorlijk ICT-gebruik en daarmee goed digitaal bestuur. Informatiebeveiliging is daarbij een absolute voorwaarde voor het garanderen van de betrouwbaarheid van de informatie binnen de voorzieningen voor toegang tot elektronische diensten van bestuursorganen en aangewezen organisaties. Uiteindelijk resulteert dat in het blijvend borgen van het vertrouwen van de burger in de toegang tot elektronische dienstverlening en betrouwbaarheid van authenticatiemiddelen.

6.2. Beveiliging van de toegang tot elektronische dienstverlening

Informatiebeveiliging staat bij de op grond van dit wetsvoorstel vast te stellen uitvoeringsregelgeving en bij het (functioneel) ontwerp van de toegang tot elektronische dienstverlening centraal. De publieke voorzieningen en erkende diensten dienen dan ook te voldoen aan de op grond van dit wetsvoorstel vast te stellen uitvoeringsregelgeving. Daaruit

volgen maatregelen die de voornaamste bijdrage zullen leveren aan een veilige toegang tot elektronische diensten. Daarnaast worden op grond van artikel 8 in het kader van reguliere informatiebeveiliging, verplichtingen opgelegd aan bestuursorganen en aangewezen organisaties voor toegang tot elektronische diensten voor de beveiliging van de eigen onderliggende systemen.

Bij informatiebeveiliging gaat het om het managen van risico's in geautomatiseerde en onderling afhankelijke processen en ketens. Informatiebeveiliging behelst een samenstel van strategische, tactische en operationele maatregelen om processen en ketens zodanig in te richten dat de goede werking, beschikbaarheid, veiligheid, vertrouwelijkheid en betrouwbaarheid zoveel mogelijk is gewaarborgd, alsmede het afleggen van verantwoording over de genomen maatregelen.

De genoemde maatregelen worden door de publieke dienstverleners getroffen en onderhouden op basis van een daartoe door hen vast te stellen informatiebeveiligingsbeleid en daaruit voortvloeiende informatiebeveiligingsplannen. De informatiebeveiligingsmaatregelen (zoals technische toegangsbeveiliging en scheiding van verantwoordelijkheden) worden opgenomen in de informatiebeveiligingsplannen en worden op basis van risicoanalyse geselecteerd en geïmplementeerd om de doelmatigheid en proportionaliteit van de maatregelen te borgen. Teneinde de veiligheid, betrouwbaarheid en continuïteit te borgen kunnen de maatregelen tussentijds worden aangepast indien daartoe aanleiding bestaat.

Beveiliging van publieke voorzieningen voor elektronische toegang
Uit artikel 7, eerste en tweede lid, van het wetsvoorstel volgt dat ook de erkende publieke diensten, middelen en voorzieningen waarvoor de minister van BZK ingevolge artikel 4 zorg draagt, moeten voldoen aan bij of krachtens algemene maatregel van bestuur te stellen technische en organisatorische eisen met betrekking tot werking, beveiliging en betrouwbaarheid van die diensten respectievelijk de middelen en de voorziening. Uit hoofde van dit artikel heeft de minister derhalve de verantwoordelijkheid voor informatieveiligheid met betrekking tot de publieke voorzieningen (publieke authenticatiedienst, publieke machtigingsdienst en het BSN-K) en de publieke middelen waarvoor hij verantwoordelijkheid draagt. Dit betekent dat de minister ter zake van 'zijn' voorzieningen voor toegang tot elektronische dienstverlening een beheersbaar risico moet realiseren en moet kunnen aantonen dat hij redelijkerwijs passende maatregelen heeft genomen om de risico's te beperken.

Informatiebeveiliging voor bestuursorganen en aangewezen organisaties
Om de veiligheid, betrouwbaarheid en beschikbaarheid van toegang tot elektronische diensten te waarborgen zullen bestuursorganen en aangewezen organisaties passende maatregelen dienen te treffen om inbreuken op en aantastingen van de (technische) beveiliging dan wel de processen ten behoeve van deze toegang te voorkomen.

Om dit te realiseren wordt voor wat betreft de bestuursorganen in de eerste plaats aansluiting gezocht bij geldende rijksbrede en relevante normen en open standaarden. Daaronder worden in ieder geval begrepen de normen en open standaarden die op grond van artikel 2, tweede lid, van het wetsvoorstel zijn aangewezen bij algemene maatregel van bestuur.

Zoals gezegd is er sprake van ketenafhankelijkheid, waarbij informatiebeveiligingsproblemen bij een schakel tevens problemen kunnen opleveren in andere schakels. Om deze reden dienen bestuursorganen en aangewezen organisaties op grond van dit wetsvoorstel te voldoen aan bij of krachtens algemene maatregel van bestuur vast te stellen regels met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang tot elektronische diensten die zij in stand houden. Daarbij zal het in de eerste plaats gaan om nadere regels gericht op de veilige interacties met erkende diensten. Om de veiligheid, betrouwbaarheid en beschikbaarheid van de toegang tot elektronische dienstverlening te waarborgen zullen daarnaast ook voor aansluitende systemen van bestuursorganen en aangewezen organisaties passende maatregelen getroffen dienen te worden om inbreuken op en aantastingen van de (technische) beveiliging dan wel de processen van de voorzieningen te voorkomen, waarbij aansluiting gezocht wordt bij geldende rijksbrede relevante normen en open standaarden, zoals opgenomen op de 'pas toe of leg uit'-lijst, dan wel de op grond van dit wetsvoorstel bij algemene maatregel van bestuur verplicht gestelde standaarden.

Beveiliging van erkende diensten
Erkende private authenticatiediensten, ontsluitende diensten, machtigingendiensten en attributendiensten moeten ingevolge het wetsvoorstel voldoen aan voor hen gestelde eisen inzake de werking, beveiliging en betrouwbaarheid. Deze verplichting zal nader worden uitgewerkt in uitvoeringsregelgeving op grond van artikel 7, eerste lid.

7. Privacy

7.1. Inleiding

Het wetsvoorstel bevat tevens regels om de bescherming van de persoonlijke levenssfeer bij het verlenen van toegang te waarborgen. De minister van BZK en erkende diensten verwerken ten behoeve van elektronische toegang persoonsgegevens en dienen derhalve zelf aan geldende privacy wet- en regelgeving te voldoen. Teneinde de persoonlijke levenssfeer te beschermen is daarom één van de doelstellingen van het wetsvoorstel om eisen te stellen inzake verwerking, beveiliging en betrouwbaarheid van persoonsgegevens. Deze eisen, waarin privacybeginselen zijn vervat, zullen in het functioneel ontwerp moeten worden verdisconteerd en door de minister van BZK en erkende diensten in het technisch ontwerp moeten worden meegenomen. Daardoor kan dan '*privacy by design'* worden gerealiseerd. De volgende privacybeginselen komen daarin nadrukkelijk naar voren:

I. Dataminimalisatie. Elke partij verwerkt voor het verlenen van toegang slechts die persoonsgegevens die nodig zijn voor de rol (en taken) die hij uitvoert.
II. Het vermijden van grote concentraties van persoonsgegevens (hotspots). De uitvoeringsregelgeving en het daaruit volgende functioneel ontwerp dient zodanig te worden ingericht dat het niet nodig of mogelijk is om identificatie en vertrouwelijke informatie bij één rol te beleggen.
III. Het gebruik van *privacy enhancing technologies.* De bescherming van persoonsgegevens wordt in de uitvoeringsregelgeving voorgeschreven en waar mogelijk systeemtechnisch afgedwongen. Het waar mogelijk feitelijk onherleidbaar maken van gegevens tot personen is een adequatere waarborg dan vertrouwen op procedurele afspraken.
IV. Incident impact beperking. Alhoewel met de uitvoeringsregelgeving en daaruit volgende maatregelen wordt gestreefd om beveiligingsincidenten en misbruik zoveel mogelijk te voorkomen, zijn deze niet geheel uit te sluiten. In de uitvoeringsregelgeving zal daarom een instrumentarium worden geregeld en maatregelen worden voorgeschreven waardoor de impact van een eventueel beveiligingsincident beperkt blijft en adequaat kan worden afgehandeld.

7.2. Wet- en regelgeving

Rond deze beginselen zullen vervolgens in de uitvoeringsregelgeving de benodigde gegevensverwerkingen verder worden gekaderd. Deze zullen in het functioneel ontwerp van de systemen (techniek en processen) hun beslag krijgen, conform het wettelijk kader inzake de bescherming van persoonsgegevens. Voor de regels voor toegang tot digitale dienstverlening speelt daarin op dit moment naast de Wet bescherming persoonsgegevens (hierna: Wbp) ook wetgeving over het BSN een rol. Binnen afzienbare tijd zal bovendien de in het kader van de Europese Unie vastgestelde Algemene verordening gegevensbescherming (hierna: AVG) het voornaamste kader vormen.[55]

De Algemene verordening gegevensbescherming (AVG)
Op 27 april 2016 is de AVG vastgesteld. De (materiële) bepalingen in deze verordening zullen op 25 mei 2018 directe werking krijgen in de Nederlandse rechtsorde. Met het in voorbereiding zijnde wetsvoorstel ter uitvoering van de AVG en ter implementatie van de hoofdstukken VI, VII en VIII van de richtlijn gegevensbescherming opsporing en vervolging, zal de Wet bescherming

[55] *Verordening (EU) 2016/679 van het Europees Parlement en de Raad, 27 april 2016, betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn95/46/EG (algemene verordening gegevensbescherming).*

persoonsgegevens worden ingetrokken. Gezien deze ontwikkeling wordt in de uitvoeringsregelgeving en in de onderhavige memorie reeds uitgegaan van de bepalingen zoals deze in de AVG zijn opgenomen, en niet meer over de bepalingen in de Wbp.

Privacybepalingen in de Wet GDI in relatie tot de AVG
Dit wetsvoorstel bevat bepalingen die een aanvulling zijn op de waarborgen van de AVG. In artikel 4 van het wetsvoorstel worden de taken en verantwoordelijkheden van de minister van BZK vastgelegd. De grondslag om persoonsgegevens te verwerken vloeit voort uit deze taakopdracht, in samenhang met artikel 6, eerste lid, onder e, van de AVG (op dit moment artikel 8, onder e, Wbp). In artikel 9 van het wetsvoorstel zijn grondslagen neergelegd voor de verwerking van persoonsgegevens door de minister van BZK en door private partijen voor zover dat noodzakelijk is voor de uitvoering en het verlenen van veilige toegang tot elektronische dienstverlening.

Krachtens het wetsvoorstel zullen nadere regels worden gesteld, waaronder regels over de verstrekking van persoonsgegevens en de bewaartermijnen die in acht moeten worden genomen. In deze nadere regelgeving wordt thans voorzien door het Besluit verwerking persoonsgegevens GDI, dat ingevolge artikel 26 van het wetsvoorstel mede komt te berusten op artikel 9, derde lid, en dat, als gevolg van dit wetsvoorstel, zal worden uitgebreid en gewijzigd. Voor alles wat dit wetsvoorstel en de daarop gebaseerde algemene maatregel van bestuur niet regelt over de verwerking van persoonsgegevens in het kader van de toegang tot elektronische dienstverlening, gelden de bepalingen van de AVG.

Toepassing materiële beginselen voor gegevensverwerking
De AVG introduceert ter bevordering van gegevensbescherming een aantal nieuwe instrumenten. De AVG bepaalt dat, ten behoeve van gegevensbescherming, daarmee rekening dient te worden gehouden in het ontwerp van gegevensverwerkingen en door standaardinstellingen (artikel 25 AVG, *privacy by design and by default*). Tevens bepaalt artikel 35 AVG, dat een gegevensbeschermingseffectbeoordeling (privacy impact assessment (PIA)) voorafgaand aan de verwerking dient te worden uitgevoerd. Hieronder wordt eerst nader ingegaan op de wijze waarop hiermee bij de toegang tot elektronische dienstverlening rekening is gehouden.

Privacy-by-design en uitvoering privacy impact assessment
In het kader van de totstandkoming van dit wetsvoorstel is een aantal maatregelen getroffen om een effectieve toepassing van de AVG te borgen. Belangrijke maatregelen zijn het gedurende het proces uitvoeren van PIA's[56], het meenemen van de uitkomsten en daaruit voortvloeiende eisen in op te stellen regelgeving en het verdisconteren van deze eisen bij de inrichting van het functioneel ontwerp. Daarnaast dient ervoor gezorgd te worden dat inrichting plaatsvindt volgens de (algemene) privacyeisen die voortvloeien uit de AVG, waaronder het vormgeven van een functionaliteit ten behoeve van het inzage- en correctierecht.

De belangrijkste aanpassingen als gevolg van de tijdens de voorbereiding van dit wetsvoorstel, in het kader van de pilots, uitgevoerde PIA's betreffen de inrichting van een functionaliteit voor inzage- en correctie voor gebruikers waarvan gegevens worden verwerkt. Door middel van dit zogeheten Inzageregister krijgt de gebruiker inzage in zijn aangemelde middelen en het gebruik ervan.[57] De registratie van de verschillende middelen gebeurt door middel van aanmelding via het BSN-K (zie par. 3.2.1.2.2).

Tevens wordt de gegevensverwerking zodanig ingericht dat geen enkele van de bij authenticatie betrokken partijen (inclusief publieke dienstverleners) kan zien welke andere websites door een gebruiker worden bezocht in het publieke domein. Dit is niet alleen een belangrijk punt voor de bescherming van persoonsgegevens als zodanig, maar doet tevens recht aan de wens en de

[56] Een Privacy Impact Assessment is een hulpmiddel bij de ontwikkeling van beleid, wetgeving en de bouw van ICT-systemen. Hiermee kunnen privacyrisico's op een gestructureerde en heldere wijze in kaart worden gebracht. Zo nodig kunnen richtinggevende aanbevelingen worden gedaan om privacy risico's te elimineren of te mitigeren. Aan de hand van de aanbevelingen kunnen maatregelen getroffen worden en optimalisaties worden gerealiseerd die verwerkt kunnen worden in (uitvoerings)regelgeving en architectuur.
[57] Mogelijk zal in de toekomst via Mijnoverheid.nl het inzageregister te raadplegen zijn.

verwachting dat de betrokken partijen geen inzicht in of bemoeienis moeten kunnen hebben met zaken die gebruikers in het publieke domein afwikkelen.

De uitgevoerde PIA's hebben ook input geleverd voor de uitvoeringsregelgeving, geleid tot aanpassingen op het (technisch) ontwerp en onderschrijving van verwerkingsgrondslagen in onderhavig wetsvoorstel voor het gebruik van het BSN door private partijen.

Ook bij de verdere inrichting en ontwikkeling van het stelsel zullen er PIA's worden uitgevoerd. De uitkomsten hiervan beogen doorlopende en blijvende expliciete aandacht voor privacybescherming, waaronder technische en procedurele maatregelen. Het zal sprake zijn van een voortdurend proces, waarbij continue PIA's uitgevoerd worden om de systemen, processen, wet- en regelgeving, maar ook beleid en uitvoering op elkaar aan te laten sluiten. Om de bescherming van persoonsgegevens van burgers, en daarmee ook de integriteit van de systemen voor toegang tot elektronische dienstverlening te waarborgen, zal regulier een PIA uitgevoerd worden. Dat zal ook gebeuren bij mogelijke toekomstige wijzigingen van onderhavig wetsvoorstel en de daarop gebaseerde regelgeving waarbij voorzien wordt dat deze waarschijnlijk impact op de verwerkingen van persoonsgegevens hebben.

Transparantie en rechten van betrokkenen
In hoofdstuk III van de AVG, waarin de rechten van betrokkenen worden geregeld, zijn de zogenaamde transparantievoorschriften opgenomen. Artikel 12 AVG stelt regels aan de begrijpelijkheid van informatie en communicatie over de verwerkingen van persoonsgegevens zodat betrokkenen daadwerkelijk in staat worden gesteld om hun toekomende rechten uit te oefenen.

Daarbij wordt een onderscheid gemaakt tussen het geval dat de verkrijging van de gegevens bij de betrokkene zelf plaatsvindt (artikel 13 AVG) en dat waarbij de gegevens niet bij de betrokkene zijn verkregen (artikel 14 AVG). Ingevolge dit wetsvoorstel en de bijbehorende uitvoeringsregelgeving vindt het verkrijging van de gegevens van de gebruikers van voorzieningen voor toegang tot elektronische dienstverlening op beide wijzen plaats. Bij aanvraag en registratie van middelen gaat het bijvoorbeeld om de gegevens die de burger zelf moet verstrekken op het moment dat hij een middel of registratie van een machtiging aanvraagt. Daarnaast is sprake van informatie die in het kader van de toegang tot elektronische dienstverlening buiten de betrokkene om wordt verkregen, bijvoorbeeld gegevens die nodig zijn om de juistheid van gegevens te controleren, zoals de controle van de identiteit door het BSN-K.

De minister van BZK en de andere verantwoordelijken voor de toegang tot elektronische dienstverlening zullen in het kader van de toegang tot elektronische dienstverlening uitvoering geven aan de transparantieverplichtingen door een privacyverklaring op de betreffende informatiewebsites. In deze verklaring staat onder andere wie de verantwoordelijke is voor de verwerking van persoonsgegevens en met welk doel de persoonsgegevens worden verwerkt. Ook zal op de websites van de betreffende voorzieningen een link worden opgenomen naar de bijbehorende wet- en regelgeving, waaronder, indien dit voorstel tot wet wordt verheven, de wet en deze toelichting, alsmede uitvoeringsregelgeving die op basis van deze wet is voorzien, en waarin nadere regels ten aanzien van de verwerkingen van persoonsgegevens worden gesteld.

Het recht van inzage en rectificatie (correctie)
Op grond van artikel 15 van de AVG heeft de betrokkene het recht om te weten welke persoonsgegevens door de verantwoordelijke worden verwerkt, onder meer voor welke doeleinden en aan welke personen of instanties deze gegevens zijn verstrekt. Op grond van de artikelen 16 tot en met 18 van de AVG heeft de betrokkene het recht de verantwoordelijke te verzoeken hem betreffende gegevens te rectificeren, gegevens te wissen ('recht op vergetelheid'), of de verwerking te beperken.

De wijze waarop partijen uitvoering geven aan deze rechten van de burger, zal worden vastgelegd in uitvoeringsregelgeving op basis van artikel 9 van dit wetsvoorstel en in de op te stellen privacyverklaringen van de dienstverleners en erkende diensten in het kader van toegang tot elektronische dienstverlening, die op de betreffende websites zullen worden geplaatst.

Ten behoeve van inzage in de gegevensverwerkingen ten behoeve van het verlenen van toegang tot elektronische dienstverlening wordt het eerdergenoemde inzageregister bij het BSN-K voorzien. Aldus kunnen betrokkenen op het moment dat zij dat zelf wensen, hun gegevens zoals deze worden verwerkt binnen de voorziening BSN-K inzien.

Beginselen en grondslagen voor verwerking van persoonsgegevens
Uit de AVG volgt, naast de hiervoor besproken transparantie, dat de verzameling en verwerking van persoonsgegevens plaatsvindt op een rechtmatige en behoorlijke wijze. Dit volgt uit artikel 5, eerste lid, onder a, van de AVG. Voorts dienen, op grond van artikel 5, lid 1, onder b, AVG, de doeleinden waarvoor verzameling en verwerking plaatsvindt gerechtvaardigd, welbepaald en uitdrukkelijk omschreven te zijn (doelbinding).

De verwerkingen worden ofwel uitgevoerd door de minister van BZK in het kader van de publiekrechtelijke taak ofwel door private partijen in het kader van een toegekende taak . Om deze redenen is in het wetsvoorstel voorzien in een grondslag, teneinde de doelen te verankeren voor verwerkingen die noodzakelijk zijn voor de toegang tot elektronische dienstverlening. Deze verwerkingsdoelen zijn opgenomen in artikel 4 (taken van de minister van BZK) en artikel 9 van het wetsvoorstel (verwerking van persoonsgegevens door private partijen). Hiermee wordt voorzien in een rechtsgrond, als bedoeld in artikel 6, lid 3, onder b, AVG, waardoor de rechtmatigheid van de verwerkingen kan worden gebaseerd op artikel 6, lid 1, onder e, (verwerking noodzakelijk voor de vervulling van een taak van algemeen belang). In artikel 9 wordt voorts de delegatiegrondslag gecreëerd voor uitvoeringsregelgeving. Daarin zullen nadere regels worden gesteld teneinde de naleving van de beginselen, zoals hieronder worden besproken, na te kunnen leven.

Verwerking BSN ten behoeve van toegang tot elektronische dienstverlening
Zoals eerder aangestipt kent de AVG enkele bepalingen in verband met specifieke situaties op het gebied van gegevensverwerking. Hierin zijn verschillende bijzondere situaties geregeld, waaronder de verwerking van het nationaal identificatienummer, dat in het kader van dit wetsvoorstel een belangrijk aspect vormt. Immers de verwerking van het BSN speelt bij de toegang tot elektronische dienstverlening een belangrijke rol. Artikel 87 AVG geeft een grondslag om bij nationaal recht specifieke voorwaarden op te stellen voor de verwerking van een nationaal identificatienummer. De in voorbereiding zijnde Uitvoeringswet AVG regelt het gebruik van wettelijk voorgeschreven nummers. Het artikel komt overeen met het huidige artikel 24 van de Wbp. Dit betekent dat voor de verwerking van het BSN dient te worden voorzien in een expliciete wettelijke grondslag. Om deze reden is in artikel 9 van het wetsvoorstel expliciet opgenomen dat het BSN mag worden verwerkt voor zover dat noodzakelijk is voor de goede werking van het BSN-K en voor de verlening van toegang tot elektronische dienstverlening. Overigens geldt daarbij hetgeen eerder is besproken, namelijk dat is getracht het gebruik van het BSN tot een minimum te beperken en te werken met pseudonimisering en versleuteling.

Dataminimalisatie
Tevens dienen de gegevens die voor de toegang tot elektronische dienstverlening worden verwerkt toereikend en ter zake dienend te zijn. Daarbij gaat om uitgangspunten als proportionaliteit en subsidiariteit, waardoor een minimum aan verwerking van persoonsgegevens wordt gerealiseerd (artikel 5, lid 1, onder c, AVG). In uitvoeringsregelgeving ingevolge artikel 9, derde lid, van het wetsvoorstel zal dit beginsel nader worden ingevuld.

Juistheid van persoonsgegevens
Tevens moet worden voorzien in maatregelen om te zorgen dat persoonsgegevens ten behoeve van de toegang tot elektronische dienstverlening op een juiste wijze worden verwerkt en dat maatregelen worden getroffen om te zorgen dat gegevens die niet (meer) juist worden verwerkt, gerectificeerd of verwijderd worden (artikel 5, lid 1, onder d, AVG). Bij nadere regelgeving zullen regels worden gesteld over de wijze waarop hieraan invulling wordt gegeven.

Opslagbeperking (bewaartermijnen)
Een belangrijk uitgangspunt is daarnaast dat persoonsgegevens niet langer worden verwerkt dan voor een termijn die voor de realisatie van het verlenen van toegang tot elektronische dienstverlening noodzakelijk (en daarmee te rechtvaardigen) is (artikel 5 lid 1 onder f). In uitvoeringsregelgeving zullen bewaartermijnen worden vastgelegd.

Beveiliging van persoonsgegevens
Tevens dienen bij de verwerking van persoonsgegevens voor toegang tot elektronische dienstverlening passende technische en organisatorische maatregelen te worden getroffen, zodanig dat een passende beveiliging gewaarborgd is (artikel 5, lid 1, onder f, AVG). Ten aanzien van de beveiliging van persoonsgegevens werkt artikel 32 van de AVG dit nader uit. Bepaald wordt dat, waar passend, pseudonimisering en versleuteling dient te worden ingezet. Ook wordt aangegeven dat maatregelen moeten worden genomen om te zorgen dat op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van de verwerkingssystemen kan worden gegarandeerd, en dat de beveiligingsmaatregelen op gezette tijden getest en geëvalueerd worden. Voorts volgt uit dit artikel dat dient te worden voorzien in maatregelen om, bij een fysiek of technisch incident, de beschikbaarheid van en de toegang tot persoonsgegevens tijdig te kunnen herstellen. Genoemde technische en organisatorische maatregelen worden doorgevoerd in de (ICT) systemen en processen die ingevolge dit wetsvoorstel noodzakelijk zijn. Ook wordt het BSN omgezet in pseudoniemen waardoor het BSN als zodanig niet verder wordt verwerkt.

De AVG bevat in artikel 33 de verplichting om melding te maken van een inbreuk in verband met persoonsgegevens. Deze regeling komt op hoofdlijnen overeen met meldplicht datalekken zoals deze thans in de Wbp is opgenomen.

Verantwoordingsplicht
De AVG legt in artikel 5, tweede lid, aan de verwerkingsverantwoordelijke een verplichting op om te zorgen dat de naleving van de hiervoor besproken beginselen kan worden aangetoond.

7.3. Grondwet en EVRM

Artikel 10, eerste lid, Grondwet
Ingevolge artikel 10, eerste lid, van de Grondwet heeft iedereen recht op eerbiediging van zijn persoonlijke levenssfeer. De verwerking van persoonsgegevens van een burger vormt een inbreuk op diens persoonlijke levenssfeer. Dit is bij de verwerking van persoonsgegevens in het kader van toegang tot elektronische dienstverlening aan de orde. Het recht op eerbiediging van de persoonlijke levenssfeer kan blijkens artikel 10, eerste lid, van de Grondwet evenwel bij of krachtens de wet worden beperkt. Aan de eis dat de beperking bij of krachtens de wet dient plaats te vinden, wordt met dit wetsvoorstel voldaan, gelet op de wettelijke grondslagen voor de gegevensverwerking in artikel 4 (taakomschrijving van de minister) en artikel 9 (private partijen) van het wetsvoorstel en het daarop gebaseerde Besluit verwerking persoonsgegevens generieke digitale infrastructuur.

Artikel 8 van het EVRM
Artikel 8 van het EVRM beschermt het recht op respect voor het privéleven. Dit recht is evenwel niet absoluut. Ingevolge artikel 8 van het EVRM is een inmenging in de uitoefening van dit recht gerechtvaardigd, wanneer deze bij de wet is voorzien, tegemoet komt aan een legitiem doel en in een democratische samenleving noodzakelijk is in verband met een of meer in het tweede lid genoemde belangen. De wet dient bovendien afdoende waarborgen te bevatten om willekeur en misbruik van de toegekende verwerkingsgrondslagen te vermijden. Volgens de jurisprudentie van het EHRM is een inmenging noodzakelijk in een democratische samenleving, wanneer er sprake is van een dringende maatschappelijke behoefte (*pressing social need*). Om de inbreuk op het recht op respect voor het privéleven gerechtvaardigd te doen zijn, dient blijkens de jurisprudentie voorts te zijn voldaan aan de voorwaarden van proportionaliteit (er dient een redelijke verhouding te bestaan tussen de ernst van de inbreuk en de zwaarte van het belang dat met de inbreuk wordt gediend) en subsidiariteit (er is geen alternatief, dat even effectief, maar minder ingrijpend is). Het wetsvoorstel en het hierop te baseren Besluit verwerking persoonsgegevens generieke digitale

infrastructuur beogen de verwerking van persoonsgegevens een wettelijke basis te verschaffen die voldoet aan de eisen van toegankelijkheid en voorzienbaarheid.

Voor wat betreft de voorzienbaarheid is daarbij relevant dat het (als gevolg van dit wetsvoorstel aan te passen) Besluit verwerking persoonsgegevens generieke digitale infrastructuur een heldere regeling zal bevatten met betrekking tot de persoonsgegevens die kunnen worden verwerkt, de instanties aan wie gegevens kunnen worden verstrekt, welke gegevens het daarbij betreft en de bewaartermijn van de gegevens. De rechten en plichten van de burger en het toezicht op de gegevensverwerking door een onafhankelijke instantie zijn bijvoorbeeld onderwerpen die onder de AVG en de als gevolg hiervan in voorbereiding zijnde uitvoeringsregelgeving vallen en die hierna wat betreft de rechten van de burger ook nog nader worden toegelicht.
Op het punt van de voorzienbaarheid bieden de artikelen 4 en 9 van dit wetsvoorstel bovendien een duidelijk richtinggevend kader voor de regeling bij algemene maatregel van bestuur. Zo bepaalt artikel 9, eerste en tweede lid, van het wetsvoorstel dat persoonsgegevens, waaronder het BSN, door private partijen worden verwerkt voor zover dit noodzakelijk is voor de goede werking van de voorziening BSN-K respectievelijk noodzakelijk is voor betrouwbare toegang tot elektronische dienstverlening door bestuursorganen en aangewezen organisaties. In het derde lid is vermeld dat bij algemene maatregel van bestuur nader wordt bepaald welke persoonsgegevens worden verwerkt, aan wie deze worden verstrekt en hoe lang deze worden bewaard.
De inmenging die de gegevensverwerking maakt op het recht in artikel 8 van het EVRM, dient noodzakelijk te zijn in een democratische samenleving in verband met een aantal nader genoemde belangen. In artikel 8, tweede lid, van het EVRM wordt in dat verband gesproken over het belang van de nationale veiligheid, de openbare veiligheid of het economisch welzijn van het land, het voorkomen van wanordelijkheden en strafbare feiten, de bescherming van de gezondheid of de goede zeden en de bescherming van de rechten en vrijheden van anderen. Deze opsomming omvat in feite voor het grootste deel de taken die een moderne overheid voor zijn burgers vervult.

Met dit wetsvoorstel wordt beoogd om betrouwbare en veilige toegang voor burgers en bedrijven tot elektronische dienstverlening in het publieke domein te regelen. Het gebruik van elektronische dienstverlening en de afhankelijkheid ervan zijn sterk toegenomen in de afgelopen jaren en zullen naar verwachting verder doorzetten. Het systeem van elektronische toegang beoogt toegang op een hoog betrouwbaarheidsniveau mogelijk te maken, waarbij burgers en bedrijven niet meer afhankelijk zijn van een enkel middel. Om dat mogelijk te maken is onder meer verwerking van persoonsgegevens noodzakelijk, hetgeen weer noodzaakt tot een wettelijke basis daarvoor. Het wetsvoorstel komt tegemoet aan een dringende maatschappelijke behoefte die meebrengt dat gegevensverwerking ten behoeve van veilige en betrouwbare authenticatie dient plaats te vinden, doch zodanig dat de inmenging in de persoonlijke levenssfeer niet groter is dan strikt noodzakelijk.

De uitvoeringsregelgeving op het onderhavige terrein zal het resultaat zijn van een zorgvuldige afweging tussen het publieke belang bij een doelmatige invulling van de zorgplicht van de minister die is neergelegd in artikel 4 en de taken die binnen het kader van de wet door private partijen worden uitgevoerd enerzijds en de bescherming van de persoonlijke levenssfeer van de gebruikers anderzijds. Dit uit zich in de eerste plaats in het feit dat de verwerking van persoonsgegevens beperkt is tot zo min mogelijk gegevens en alleen tot die gegevens van de burger die echt essentieel zijn om de toegang tot elektronische dienstverlening beschikbaar te kunnen stellen, in stand te kunnen houden, te laten werken en beveiligen en betrouwbaar te houden.

Het BSN speelt voor de herkenning van burgers in het publieke domein een cruciale rol. Echter een belangrijk ontwerpuitgangspunt van het systeem voor elektronische toegang is om het gebruik van het BSN te beperken (dataminimalisatie) en herleidbaarheid/terugleidbaarheid zoveel mogelijk onmogelijk te maken. Dit wordt gedaan door te werken met pseudoniemen en versleutelingstechnieken (PET-maatregelen), waardoor verwerking van het BSN tot een minimum beperkt wordt en geen van de partijen een totaalbeeld kan krijgen van het gebruik van een authenticatiemiddel. De voorzieningen voor elektronische toegang en bijbehorende grondslagen strekken er toe veilige toegang (authenticatie) te realiseren. Zij borgen een identiteitscontrole en veilige aflevering bij de publieke dienstverlener. Er worden geen andere gegevens van een gebruiker aan deze dienstverleners verstrekt. In het kader van veilige toegang tot elektronische

dienstverlening worden geen andere bijzondere persoonsgegevens verwerkt, zoals bijvoorbeeld gegevens over ras, politieke opvatting of geloof.

De proportionaliteit van de gegevensverwerking zal ook af te leiden zijn uit de bepalingen over de bewaartermijnen van de gegevens zoals deze in het hiervoor genoemde besluit zullen worden opgenomen, waarbij de bewaartermijn duidelijk is onderbouwd en beperkt tot het doel van de verwerking. Ook wordt vastgelegd aan wie welke gegevens mogen worden verstrekt. De desbetreffende bepalingen waarborgen dat gegevens niet langer worden bewaard en niet meer gegevens worden verstrekt dan noodzakelijk.

Ten slotte is er nog de vraag, of het doel dat met de voorzieningen wordt beoogd, ook op een andere, even effectieve, maar minder ingrijpende wijze zou kunnen worden bereikt (subsidiariteit). Op dit moment is het huidige publieke authenticatiemiddel – gezien de betrouwbaarheid die kan worden geboden – toe aan vernieuwing. Het middel kan in zijn huidige vorm niet voldoen aan de vraag naar hoogbetrouwbare authenticatie. Ook de afhankelijkheid van een enkel middel levert risico op. Dit kan alleen worden ondervangen door meerdere middelen aan te bieden. Deze multimiddelenaanpak kan alleen worden gerealiseerd als meerdere (private) partijen de mogelijkheid krijgen om middelen uit te geven om te gebruiken in het publieke domein. Hiertoe is verwerking van het BSN noodzakelijk, omdat dit op een persistente wijze uniciteit waarborgt.

8. Misbruik van de GDI

8.1. Inleiding

In een rapport van PricewaterhouseCoopers[58] uit 2013 wordt becijferd dat de omvang van de fraude bij de overheid in 2013 7,3 miljard euro bedroeg. Over identiteitsfraude waarbij overheidsgeld betrokken is, volgt uit de monitor Identiteit in cijfers dat het gaat om bijna dertig duizend zaken op jaarbasis. Zoals in het jaarverslag van het ministerie van BZK over 2015 is vermeld, zijn in dat jaar 15.000 DigiD's geblokkeerd, waarvan een groot aantal overigens preventief, waarmee misbruik lijkt te zijn voorkomen.[59] Ramingen zijn conservatief en vermoedelijk aan de lage kant.

Recentelijk is uit het Cybersecuritybeeld Nederland 2016 naar voren gekomen dat beroepscriminelen een steeds groter gevaar vormen voor digitale veiligheid in Nederland. Beroepscriminelen organiseren zich steeds beter en maken gebruik van geavanceerde digitale aanvalsmethoden. Het afgelopen jaar vonden verschillende grootschalige aanvallen plaats met een hoge organisatiegraad, gericht op diefstal van geld en kostbare informatie. Naast de overheid waren bedrijven en burgers hiervan in toenemende mate het slachtoffer.[60]

Echter niet alleen de financiële omvang van fraude is van belang. Minstens zo belangrijk zijn de maatschappelijke consequenties zoals ondermijning van het gevoel van betrouwbaarheid van en vertrouwen in de (digitale) overheid en in het algemeen het effect ervan op mensen en instituties. Fraude heeft bovendien een aanzuigende werking op personen die van de klaarblijkelijke gelegenheid om te frauderen, gebruik willen maken. Zo is fraude de laatste jaren een thema geworden dat met enige regelmaat politieke aandacht heeft gekregen.

8.2. Misbruik en identiteitsfraude

De erkende authenticatiemiddelen zullen voor een belangrijk deel gaan fungeren als toegangspoort tot digitale overheidsdienstverlening in Nederland. In het publieke domein zal er naar verwachting steeds meer gebruik van worden gemaakt, mede door verplichtstelling van de digitale weg in

---

[58] Naar een fraudebeeld Nederland; Inzicht in fraude draagt bij aan bewustwording en effectieve prioriteitstelling in de aanpak. Position paper van PricewaterhouseCoopers. http://www.pwc.nl/nl/assets/documents/pwc-naar-een-fraudebeeld-nederland.pdf

[59] Jaarverslag ministerie van BZK 2015 https://www.rijksoverheid.nl/actueel/nieuws/2016/05/18/jaarverslag-2015-binnenlandse-zaken-en-koninkrijksrelaties

[60] Cybersecuritybeeld Nederland, csbn 2016 van het Nationaal Cybersecurity Centrum. https://www.ncsc.nl/actueel/Cybersecuritybeeld+Nederland/cybersecuritybeeld-nederland-2016.html

sectorwetgeving. Burgers, ondernemers en overheden worden daardoor afhankelijker van de authenticatiemiddelen, en des te groter zijn voor hen de negatieve gevolgen als het onverhoopt toch een keer misgaat.

Bij het ontwerp, de inrichting en beveiliging van toegang tot elektronische dienstverlening is veel aandacht besteed aan maatregelen om misbruik tot een minimum te beperken. Een deel van de identiteitsfraude zoals die zich op dit moment manifesteert zal daardoor – onder meer door betrouwbaardere uitgifte van middelen en hoge betrouwbaarheidseisen bij authenticaties zelf – ook niet meer kunnen voorkomen.

Hoezeer ook gestreefd wordt naar 100% waterdichtheid van processen en veiligheid van authenticatiemiddelen en -systemen, risico op misbruik en beveiligingsinbreuken zal blijven bestaan. De praktijk wijst uit dat misbruikmakers, zolang er (financieel) gewin te behalen valt, actief en inventief zijn in manieren om systemen en processen voor toegang tot elektronische diensten te misbruiken inclusief de achterliggende diensten van dienstaanbieders waartoe toegang wordt verkregen. Door de voortschrijdende techniek, met nieuwe aanvalsvormen en methoden, zal het dreigingslandschap bovendien doorontwikkelen.

Het is verstandig om de realiteit te onderkennen en in aanvulling op de ontwerpmaatregelen van het stelsel om een zo betrouwbaar mogelijk systeem te leveren, als sluitstuk ook te voorzien in een instrumentarium om in de praktijk voorkomende en snel wijzigende dreigingen te herkennen en daartegen (nood)maatregelen te kunnen nemen.[61] Dit draagt net als maatregelen vooraf bij aan de betrouwbaarheid en weerbaarheid van de toegang tot elektronische dienstverlening. Het zorgt ervoor dat beveiliging en betrouwbaarheid kunnen meegroeien tegen nieuwe dreigingen.

Het begrip misbruik
Onder misbruik van toegang tot elektronische diensten wordt in dit wetsvoorstel en deze memorie begrepen zowel aantastingen van en inbreuken op de (technische) beveiliging (hacken, DDoS-aanvallen) als (bewuste) inbreuken op de processen van het stelsel ('fraude'), zoals het stelen van middelen. Gelet op de verschijningsvormen van misbruik is geen haarscherpe afbakening te maken tussen 'fraude' via digitale voorzieningen en kwetsbaarheden in elektronische voorzieningen en 'cybercrime'. De misbruikmaker zal pragmatisch zijn en niet schromen om het gehele palet aan mogelijkheden te gebruiken om zijn doel te bereiken.

Zo is het denkbaar dat bijvoorbeeld een voorziening eerst met een DDoS-aanval voor gebruikers ontoegankelijk wordt gemaakt, en vervolgens gehackt, waarna gegevens worden gestolen. Deze gegevens kunnen vervolgens in processen (van andere systemen of organisaties) voor frauduleuze doeleinden worden misbruikt. Het doel dat met het misbruik wordt beoogd kan verschillen, variërend van financieel gewin tot het veroorzaken van maatschappelijke ontwrichting door voor langere tijd eID systemen onbeschikbaar te maken. Misbruik kan ook de achterliggende dienstverlening van overheidsdienstverleners – en daarmee de maatschappij – raken. Gezien het voorgaande wordt daarom bewust een ruime invulling van misbruik gehanteerd.

Aanpak van misbruik
De op grond van dit wetsvoorstel tot stand te brengen uitvoeringsregelgeving is gericht op een betrouwbaar proces bij de inrichting van de toegang tot elektronische diensten. Daarbij gaat het om kaderstellende informatiebeveiliging, dat wil zeggen beveiliging gericht op het treffen van maatregelen vooraf. Misbruikbestrijding is in die relatie te beschouwen als 'actieve informatiebeveiliging'. Daarmee wordt bedoeld dat gedurende het gebruik van de systemen actief op zoek wordt gegaan naar bestaande en mogelijk nieuwe dreigingen, waarbij ook proactief maatregelen getroffen worden om negatieve gevolgen te voorkomen of te minimaliseren.

---

[61] Met het instrumentarium om te reageren op dreigingen en noodmaatregelen te kunnen nemen zoals dat is opgenomen, is ook invulling gegeven aan de opmerkingen van de Autoriteit Persoonsgegevens (AP) aangaande de mogelijkheden voor incidentbeheersing. Deze opmerkingen zijn gemaakt in brieven in reactie op de ontwikkeling van het eID-stelsel, te weten de brieven van 7 mei 2015 en 14 september 2016 (z2015-00357). https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_introductieplateau_eid.pdf https://autoriteitpersoonsgegevens.nl/sites/default/files/atoms/files/brief_eid_aan_bzk.pdf

Er zijn twee hoofdtaken bij misbruikbestrijding. In de eerste plaats moet misbruik worden ontdekt en herkend. Daaronder kan actieve monitoring, detectie, analyse en proactieve kennisopbouw worden verstaan. Ten tweede is er de taak om, indien het resultaat van de herkenning daartoe aanleiding geeft, herstel- en noodmaatregelen te treffen om snel en adequaat dreigingen weg te nemen en de veiligheid, de betrouwbaarheid en het imago van het eID-stelsel te borgen. Het nemen van maatregelen door de erkende diensten alsmede door de bestuursorganen en aangewezen organisaties om compromittering van de toegang tot elektronische diensten te voorkomen en te beëindigen, maakt onderdeel uit van de zorg voor de betrouwbaarheid en beveiliging, zoals nader uitgewerkt in de artikelen 7 en 8 van het wetsvoorstel. De door de minister te nemen (nood)maatregelen zelf zijn neergelegd in artikel 15 (bijzondere bevoegdheden). In het derde lid is opgenomen dat de minister de toegang tot elektronische dienstverlening via een welbepaald middel kan onderbreken bij het vermoeden van misbruik of oneigenlijk gebruik van het desbetreffende middel. In het eerste lid zijn de noodmaatregelen opgenomen die de minister kan treffen gericht op het onderbreken van dienstverlening van een bestuursorgaan of aangewezen organisatie, op het moment dat daar sprake is van een ernstige verstoring. Door te voorzien in deze maatregelen wordt beoogd om de betrouwbaarheid en de veiligheid van de toegang te kunnen blijven borgen dan wel vlot en gericht te kunnen herstellen en worden burgers, ondernemers en overheden beschermd.

8.3. Herkennen van misbruik

Een actieve aanpak van misbruik houdt in dat uitgevers van erkende authenticatiemiddelen en de minister, als onderdeel van de beheertaak, zelf (pro)actief onderzoek doen naar misbruik op basis van vroegtijdige signalen van (mogelijk) misbuik in de systemen zelf of op aangeven van ketenpartners (zoals achterliggende dienstverleners) en burgers en bedrijven die ervan gebruik maken. Dit is nodig om te begrijpen wat er gebeurt en om vast te stellen of misbruik plaatsvindt. Er dient onderzocht te worden op welke wijze het misbruik plaatsvindt, wie de slachtoffers zijn, of de gebeurtenis eerder is voorgekomen en wat adequaat is als nood- dan wel herstelmaatregel. Het herkennen en onderzoeken vormt de basis voor herstellend optreden (dat kan het blokkeren of intrekken van een erkend inlogmiddel of ontoegankelijkmaking van een systeem zijn), zodat het misbruik of aantasting ervan kan worden gestopt.

De activiteiten in het kader van de herkenning van misbruik kunnen worden onderverdeeld in (1) actieve herkenning door actieve monitoring en detectie van bekende misbruiksignalen (voorkomen van het opnieuw optreden van bekende misbruikvormen) en (2) proactief onderzoek naar nieuwe misbruiksignalen (‘doorleren op nieuwe misbruikvormen’).

Actieve herkenning van misbruik
Actieve herkenning van misbruik en onderzoek van gedetecteerde misbruiksignalen (analyse en duiding) betreft de vroegtijdige signalering van mogelijk misbruik. Dit kan door het monitoren van gegevensverkeer in de eigen voorziening of van signalen die worden aangereikt. Dit kan bijvoorbeeld ook een burger of ondernemer zelf zijn of een ketenpartner die misbruiksignalen opmerkt. Het doel van het monitoren is het detecteren van signalen of onregelmatigheden die kunnen wijzen op misbruik.

Ter illustratie van een signaal voor identiteitsfraude kan de situatie uit de praktijk van DigiD dienen waarin binnen een korte periode, vanaf één IP-adres in de nachtelijke uren zeer grote aantallen DigiD’s zijn aangevraagd. Dit is een signaal waarop in het vervolg wordt gecontroleerd om te voorkomen dat burgers in de toekomst slachtoffer worden.

Niet alle signalen van misbruik betekenen ook daadwerkelijk misbuik. Een signaal betekent wel dat verhoogde waakzaamheid nodig is en onderzoek naar wat er in de concrete situatie aan de hand is. Na het ontvangen en registreren van een misbruiksignaal wordt dat signaal onderzocht. De beheerder van de voorziening dient het signaal te onderzoeken, door te duiden wat het voor gebeurtenis is (contextbepaling) en wat de impact ervan kan zijn.

Proactieve herkenning van nieuwe misbruiksignalen
Naast de actieve herkenning van misbruik, dat gericht is op reeds bekende vormen van misbruik, is ook proactieve herkenning van misbruik nodig. Deze activiteiten zijn gericht op het vroegtijdig onderkennen, analyseren en mitigeren van situaties die kunnen duiden op nieuwe soorten misbruik of aanvalsmethodes, alsmede het achterhalen van nieuwe kwetsbaarheden. Uit de praktijk blijkt dat misbruikbestrijding ook een wedloop met de inventieve misbruikmaker is. Door zelf op zoek te gaan naar mogelijke signalen kan misbruikbestrijding inventief meegroeien en leert misbruikbestrijding zelf door. Analisten en (computer)beveiligingsexperts zullen daarvoor onderzoek moeten doen naar de technische en operationele data en de werking van voorzieningen om na te gaan waar bewuste aantastingen ontstaan of kunnen ontstaan als gevolg van kwetsbaarheden in de werking of opzet van de voorziening. Bij deze proactieve analyse worden de data van een of meer voorzieningen (gelet op het ketenkarakter) en de resultaten van eerdere onderzoeken en externe inbreng (signalen van ketenpartners) betrokken. Het doel van proactieve misbruikherkenning is steeds het verkleinen van het risico van (bekende of nieuwe) misbruikvormen en het onderkennen van nieuwe misbruikmethoden.

8.4. Herstel- en noodmaatregelen

In geval van herkend (geconstateerd) misbruik of waarschijnlijke mogelijkheid daartoe zal een erkende dienst of de minister als verantwoordelijke voor betrouwbare toegang in het publieke domein, herstellend op moeten treden om het misbruik dan wel het vastgestelde risico per direct weg te nemen. Dit betekent dat voor de misbruikmaker de mogelijkheid tot misbruik wordt weggenomen en de betrokken burgers of bedrijven in hun belang worden beschermd. Al naar gelang de situatie zullen herstel- en noodmaatregelen op maat moeten worden getroffen. Nadrukkelijk en voor de volledigheid wordt opgemerkt dat de hieronder beschreven maatregelen een reparerend en beschermend karakter hebben. Zij dienen geen punitief, d.w.z. geen bestraffend doel.

Onderstaand worden herstel- en noodmaatregelen besproken. Een maatregel kan een tijdelijk (preventief) of permanent effect beogen, afhankelijk van de situatie. Maatregelen kunnen zich richten tot gebruikers (burgers en ondernemers), overheidsorganisaties, erkende diensten dan wel de eID componenten en middelen zelf.

In het wetsvoorstel wordt er in voorzien dat de minister, om zijn taken en verantwoordelijkheden voor een veilige en betrouwbare elektronische authenticatie in het publieke domein waar te maken, beschikt over voldoende bevoegdheden om (bijzondere) maatregelen te (doen) nemen.

Maatregelen ten behoeve van en gericht tot gebruikers
In de techniek variëren de benamingen voor maatregelen nogal eens. Ten behoeve van stroomlijning wordt in de wet gesproken over ‘onderbreken’ om aan te geven dat het om een tijdelijke maatregel gaat die zich richt op tijdelijke onbruikbaarheid van een authenticatiemiddel of voorziening. Bij onderbreking is ‘deblokkering’ van een middel of dienst mogelijk, waardoor het gebruik kan worden voortgezet. Van ‘intrekking’ of ‘revocatie’ wordt gesproken om aan te geven dat een gebruik van een authenticatiemiddel of een dienst definitief onbruikbaar wordt gemaakt. Voor hernieuwd gebruik of toegang dient opnieuw een middel te worden aangevraagd.

Onderbreking van een authenticatiemiddel voor een gebruiker
Een herstelmaatregel gericht op burgers en ondernemers kan zijn het tijdelijk blokkeren van een bepaald authenticatiemiddel, zoals bedoeld in het derde lid van artikel 15. Een dergelijke maatregel kan gericht worden ingezet ten behoeve van een of meer gebruikers. Dit kan worden ingezet op het moment dat er aanwijzingen zijn dat bijvoorbeeld een authenticatiemiddel gecompromitteerd (gestolen) is en misbruikt wordt, maar dat dit nog niet onomstotelijk is vastgesteld. Op dat moment wordt het door blokkering van het middel onmogelijk gemaakt om het te gebruiken voor elektronische authenticatie. Indien na nader onderzoek blijkt dat geen sprake is van misbruik, kan het middel eenvoudig worden gedeblokkeerd, waarna het middel weer wordt vrijgegeven aan de gebruiker. Voor de gebruiker geeft blokkering binnen de context de minste hinder, omdat de maatregel een tijdelijk karakter heeft. Ook wordt de gebruiker preventief beschermd. Bij onterechte blokkering ondervindt de gebruiker weliswaar ongemak, maar deze

hoeft na vrijgave geen nieuw middel aan te vragen. Overigens is het ook mogelijk dat blokkering vooraf gaat aan een permanente maatregel, waarbij na gebleken misbruik een authenticatiemiddel uiteindelijk wordt ingetrokken.

Intrekken van middelen wegens misbruik[62]
Hierbij moet gedacht worden aan het intrekken van authenticatiemiddelen of het intrekken van elektronische registratie van machtigingen, op het moment dat misbruik wordt vermoed of gesignaleerd. Dit kan bijvoorbeeld nodig zijn als middelen worden gestolen, of wachtwoorden onderschept, waardoor de betrouwbaarheid van het middel niet meer kan worden gegarandeerd. Voorbeelden waarin dergelijke maatregelen in het verleden zijn getroffen zijn de identiteitsfraudes met DigiD in Amsterdam-Zuidoost en Groningen, waarbij DigiD codes van gebruikers uit brievenbussen zijn gehengeld en vervolgens misbruikt.[63]

(Tijdelijke) onderbreking van de gehele dienst
In het wetsvoorstel is de mogelijkheid voorzien om als tijdelijke maatregel een erkende dienst te onderbreken (uit de lucht te halen), op het moment dat er risico bestaat op misbruik als gevolg van een beveiligingsincident of een gebleken lacune in de beveiliging. Afhankelijk van de ernst en urgentie kan deze maatregel acuut door de beheerder worden genomen.

Een voorbeeld van een dergelijke situatie is het DigiD-incident geweest, waarbij een lek in de onderliggende software (*Ruby on Rails*) werd ontdekt, dat zodanig ernstig was dat daardoor per direct de veiligheid en betrouwbaarheid van DigiD niet meer kon worden gegarandeerd.[64] DigiD is daardoor uiteindelijk een dag offline geweest.
Een ander voorbeeld zijn de DDoS aanvallen 2013 geweest. In deze situatie is actief misbruik gemaakt van de systemen van DigiD (en overigens vele andere overheids- en banksystemen), waardoor de dienst verminderd of volledig onbeschikbaar is geworden. Om uiteindelijk dit misbruik het hoofd te kunnen bieden is de voorziening offline gehaald, om (tijdelijke) maatregelen te kunnen nemen. Ook is de dienst, als meer gerichte maatregel, tijdelijk geblokkeerd geweest voor gebruikers uit het buitenland (d.w.z. voor buitenlandse IP-adressen) omdat de aanval in het buitenland gelokaliseerd werd.[65]

(Tijdelijke) onderbreking van toegang tot eID-dienstverlening voor afnemers
Ten slotte is het voor de minister van BZK mogelijk om aan een of meer publieke dienstverleners de opdracht te geven zijn of hun toegang tot de dienstverlening te onderbreken als er bij de betreffende dienstverleners ernstige en acute beveiligingsgebreken blijken te zijn, die direct van invloed zijn op de beveiliging van de toegang tot elektronische dienstverlening.
Dit is bijvoorbeeld gebeurd naar aanleiding van de gebleken beveiligingsgebreken bij verscheidene afnemers van DigiD tijdens Lektober, waarbij Logius een groot aantal gemeenten acuut heeft afgesloten. Door het geconstateerde lek bleek het mogelijk om in de systemen van op DigiD aangesloten dienstverleners DigiD-gegevens van burgers te bemachtigen. Deze situatie heeft overigens de aanleiding gevormd voor het instellen van de DigiD-beveiligingsassessments, waarmee is beoogd om deze situaties zoveel mogelijk te voorkomen.

Noodprocedure
De hierboven beschreven maatregelen hebben het karakter van een noodmaatregel, bedoeld om acute risico's weg te nemen en burgers, ondernemers of dienstverleners en de toegang tot elektronische dienstverlening, zelf te beschermen tegen dreigingen. Zij dienen geen punitief karakter en beogen ook niet om toegang tot elektronische dienstverlening definitief uit te sluiten. Met het oog op bovenomschreven bijzondere bevoegdheden van de minister is in het tweede lid van artikel 15 bepaald dat bestuursorganen en aangewezen organisaties, op het moment dat zij zelf kennis hebben van situaties die kunnen leiden tot compromittering van de veilige of

---

[62] Intrekking van een middel kan ook om andere redenen plaatsvinden, zoals bij overlijden van een gebruiker. In deze paragraaf wordt revocatie voor misbruikbestrijding bedoeld.
[63] http://www.ad.nl/amsterdam/amsterdammers-slachtoffer-van-fraude-digid~aaebcb30/
[64] https://www.computable.nl/artikel/nieuws/security/4635155/250449/logius-haalt-digid-offline-na-lek-in-ruby-on-rails.html
[65] http://www.nu.nl/internet/3408271/digid-afgesloten-in-buitenland-cyberaanval-voorkomen.html

betrouwbare toegang tot elektronische dienstverlening, de minister daarover uit eigen beweging alle benodigde informatie verstrekken.

8.5. Ketensamenwerking en toezicht bij misbruikbestrijding

Voor bovenstaande activiteiten voor misbruikbestrijding is randvoorwaardelijk dat door de verschillende verantwoordelijken voor de toegang tot elektronische dienstverlening wordt samengewerkt. Immers misbruik van toegang tot elektronische dienstverlening zal zich kunnen manifesteren tussen en over losse componenten van de keten heen.

Elk onderdeel voor toegang tot elektronische dienstverlening (de erkende diensten alsmede de bestuursorganen en aangewezen organisaties) vervult een deel van een bovenliggend proces. Misbruik en de misbruikmaker kunnen in feite dezelfde route volgen, waarbij misbruik in een schakel, bijvoorbeeld een gecompromitteerd authenticatiemiddel, kan uitwaaieren naar misbruik bij diverse andere schakels en organisaties binnen – en buiten – de toegang tot elektronische dienstverlening.

Om misbruik effectief te kunnen aanpakken en 'uit de keten' te kunnen halen is daarom samenwerking en informatie uitwisseling noodzakelijk. Om te voorkomen dat door onduidelijkheid in verantwoordelijkheidsverdeling misbruik niet of slechts ten dele wordt opgepakt, is voorts regievoering daarop noodzakelijk.

In artikel 16, eerste lid, van het wetsvoorstel is voor de minister van BZK de mogelijkheid opgenomen om bij bestuursorganen en aangewezen organisaties en bij de erkende diensten informatie op te vragen om maatregelen te kunnen nemen om compromittering van de veilige en betrouwbare toegang tot elektronische dienstverlening te voorkomen of beëindigen. Daarmee wordt, naast de zorgplicht voor 'zijn' voorzieningen, ook een rol beoogd voor de minister voor integrale misbruikbestrijding binnen de toegang tot elektronische dienstverlening.

Om deze rol adequaat te kunnen invullen is het belangrijk dat informatie over beveiligings- en integriteitsinbreuken, misbruik of oneigenlijk gebruik, snel ter beschikking komt van de minister. Daarom is in artikel 15, tweede lid, van het wetsvoorstel de verplichting opgenomen voor bestuursorganen en aangewezen organisaties om de minister uit eigen beweging en onverwijld in kennis te stellen van een inbreuk op de beveiliging of de integriteit van een eigen voorziening voor elektronische dienstverlening, of als misbruik of oneigenlijk gebruik ervan wordt geconstateerd. Daarbij dient alle benodigde informatie te worden meegeleverd. Deze verplichting maakt het voor de minister mogelijk om snel en adequaat te reageren.

Voor het effectief tegengaan van misbruik, is het van belang dat de minister niet alleen informatie ontvangt en maatregelen kan nemen om een veilige en betrouwbare toegang te borgen of te herstellen, maar ook bestuursorganen, aangewezen organisaties en erkende diensten op de hoogte stelt van compromittering van de toegang tot elektronische dienstverlening, zodat zij voor zichzelf maatregelen kunnen nemen. De verplichting voor de minister om dergelijk informatie aan partijen te verstrekken is geregeld in het derde lid van artikel 16 van het wetsvoorstel.

Misbruikbestrijding wordt in het wetsvoorstel vormgegeven als een operationele beheertaak. Dit betekent dat herkenning van misbruik en het treffen van herstel- en noodmaatregelen de verantwoordelijkheid zijn van de verantwoordelijken voor de voorzieningen voor toegang tot elektronische dienstverlening, te weten de minister van BZK, en van de erkende diensten. De toezichtrol op de naleving van de wet bestaat er in dit verband uit dat de toezichthouder controleert of misbruikbestrijding als beheertaak is ingericht. De toezichthouder houdt zich nadrukkelijk zelf niet bezig met het herkennen van misbruik en het treffen van herstel of noodmaatregelen. De toezichthouder controleert derhalve of processen zijn ingericht en of de beheerorganisatie operationeel in staat is om misbruik te bestrijden. Dit houdt overigens in dat de beheerorganisatie informatie dient te kunnen verschaffen waaruit dit aantoonbaar blijkt.

Voorts dienen de erkende diensten en de minister van BZK als verantwoordelijke voor het BSN-K de toezichthouder onverwijld op de hoogte te stellen van een veiligheidsinbreuk of

integriteitsverlies met aanzienlijke gevolgen voor de veilige en betrouwbare toegang tot elektronische dienstverlening. Dat is voorzien in artikel 7, vijfde en zesde lid van het wetsvoorstel. In artikel 16, tweede lid is vervolgens vastgelegd dat de toezichthouder de minister van BZK op de hoogte stelt van dergelijke meldingen.

9. Toezicht en handhaving

9.1. Toezicht op bestuursorganen en aangewezen organisaties

Algemeen
Een goede taakuitvoering door publieke dienstverleners vergt naleving van de aan hen gestelde verplichtingen en normen. In dit wetsvoorstel gaat het om de acceptatieplicht, het voldoen aan de op grond van dit wetsvoorstel vast te stellen eisen met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang tot de elektronische dienstverlening en het jaarlijks overleggen aan de minister van BZK van een auditrapport betreffende de naleving van deze eisen. Voor bestuursorganen en andere overheden betreft dit voorts het gebruik van bij algemene maatregel van bestuur voorgeschreven standaarden.

Op de naleving van deze wet door bestuursorganen op decentraal niveau (en tevens decentrale overheden die geen bestuursorganen zijn waar het de open standaarden betreft) zijn de horizontale verantwoording en – controle, en het reguliere interbestuurlijke toezicht van toepassing. Voor bestuursorganen op niveau van het Rijk en de aangewezen organisaties wordt voor wat betreft de naleving van de acceptatieplicht en de bepalingen inzake informatieveiligheid in dit wetsvoorstel voorzien in het aanwijzen van toezichthouders. Los hiervan is in het wetsvoorstel voor alle publieke dienstverleners voorzien in verplichte audits inzake de naleving van de eisen met betrekking tot de toegang tot elektronische dienstverlening.

De decentrale overheden
In lijn met de Wet revitalisering generiek toezicht is het toezicht van de hogere overheid op de naleving van dit wetsvoorstel door de lagere overheid (interbestuurlijk toezicht) sober en terughoudend. Decentrale overheden zijn zelf verantwoordelijk voor de naleving van de wet en er wordt op vertrouwd dat de taken op het niveau waarop deze zijn belegd toereikend worden opgepakt. Het primaat voor de controle op de naleving ligt bij de horizontale verantwoording en controle binnen een bestuurslaag. In de tweede plaats komt het interbestuurlijk toezicht op de decentrale overheden, conform het beginsel dat slechts één bestuurslaag – de naast hoger gelegen bestuurslaag – toezicht houdt. De interventieladder van het interbestuurlijk toezicht voorziet onder meer in signaleren, informeren, overleg en afspraken over verbeteringen. Voorts biedt het interbestuurlijke toezicht de naast hoger gelegen bestuurslaag in uiterste gevallen de mogelijkheden tot repressief ingrijpen, te weten schorsing en vernietiging bij handelen in strijd met het recht of het algemeen belang (door de Kroon) en indeplaatsstelling (bij taakverwaarlozing).

De centrale overheid
Waar de ministeries zelf als publieke dienstverlener uitvoering geven aan het wetsvoorstel, is het ook aan de betrokken ministers er voor zorg te dragen dat de eigen (uitvoerings)organisaties, zoals de belastingdienst, dit wetsvoorstel naleven. Voor de zelfstandige bestuursorganen op het niveau van de centrale overheid, zoals het Uitvoeringsinstituut werknemersverzekeringen (UWV) en de Sociale Verzekeringsbank (SVB), geldt dat de naleving van het wetsvoorstel (eveneens) in eerste instantie een eigen verantwoordelijkheid van deze bestuursorganen zelf betreft. Voor wat betreft de acceptatieplicht en het naleving van de wettelijke veiligheidsvoorschriften door bestuursorganen op het niveau van het Rijk voorziet dit wetsvoorstel in de aanwijzing van toezichthoudende ambtenaren.

Aangewezen organisaties
Ook ten aanzien van de aangewezen organisaties is in dit wetsvoorstel voorzien in het aanwijzen van toezichthouders. Het streven is om het toezicht op deze aangewezen organisaties zo veel als mogelijk binnen de bestaande toezichtstructuren en met gebruik van bestaande instrumenten te laten plaatsvinden. Om dit te kunnen realiseren, kan de vakminister op grond van dit wetsvoorstel

ambtenaren aanwijzen die belast zijn met het toezicht op de naleving van de voorgestelde wet door deze aangewezen organisaties. De vakminister kan hier reeds bestaande toezichthouders dan wel nieuwe toezichthouders aanwijzen.

Onafhankelijke audits
Een kwetsbaarheid in de ICT-systemen die de toegang tot de elektronische diensten verzorgen, vormt niet alleen een risico voor het desbetreffende bestuursorgaan of aangewezen organisatie, maar vormt een risico voor de gehele authenticatieketen. Daarom voorziet het wetsvoorstel voor wat betreft de naleving van de eisen aan de werking, betrouwbaarheid en beveiliging van de toegang van de elektronische dienstverlening in een aanvullende verplichting: jaarlijks dient een verklaring van een onafhankelijk auditor aan de minister van BZK overlegd te worden. Deze auditor, die niet in dienstverband werkzaam mag zijn bij of anderszins verbonden mag zijn aan de betreffende publieke dienstverlener, toetst of de toegang tot de elektronische dienstverlening van deze dienstverlener daadwerkelijk aan de eisen voldoet.

De verklaring van de onafhankelijke auditor sluit aan bij de huidige systematiek die thans gehanteerd wordt bij de aansluiting op DigiD. Op grond van de DigiD-aansluitvoorwaarden dienen alle afnemers (deze groep komt naar verwachting goeddeels overeen met de bestuursorganen en aangewezen organisaties in de zin van dit wetsvoorstel) jaarlijks een audit te laten uitvoeren en de auditverklaring aan de minister van BZK te doen toekomen. In lijn met de huidige praktijk bieden de auditverklaringen allereerst een handvat voor gesprek en verdere afspraken over de benodigde verbeteringen.

Noodmaatregel als interventiemogelijkheid
Indien uit de te overleggen auditverklaringen zou blijken, dat de informatieveiligheid in het geding is ten gevolge van een ernstige storing of aantasting danwel misbruik of ongeoorloofd gebruik van de toegang tot elektronische dienstverlening en ook na herhaaldelijke aanmaningen de benodigde verbeteringen niet worden aangebracht, kan als uiterste middel de toegang tot de elektronische dienstverlening van de publieke dienstverlener afsluiten. Ook het stelselmatig niet overleggen van een auditverklaring of anderszins niet nakomen van bestuurlijke afspraken kan onder omstandigheden en als uiterste middel aanleiding vormen voor het afsluiten van deze toegang.

9.2. Toezicht op de erkende diensten

Het wetsvoorstel regelt dat de Minister van BZK ambtenaren kan aanwijzen die met het toezicht op erkende diensten zijn belast. Ambtenaren van Agentschap Telecom lijken thans een logische keuze voor deze taak, gezien de (technische) expertise en de ervaring op het gebied van elektronische communicatie en – netwerken. In het bijzonder in relatie tot de EU-verordening over het grensoverschrijdend gebruik van elektronische middelen en vertrouwensdiensten tussen lidstaten (eIDAS). De toezichthouder zal toezien op de naleving van de eisen die worden benoemd in artikel 7 en artikel 6 zevende lid, van dit wetsvoorstel. Het toezicht wordt gehouden op alle partijen die een rol spelen bij het goed functioneren van authenticatie en autorisatie in het publieke domein. De wettelijke voorschriften kunnen ook de samenwerking tussen verschillende partijen in de keten betreffen. Wanneer werkzaamheden die worden gereguleerd door het wetsvoorstel door een erkende partij worden uitbesteed aan onderaannemers, zijn deze onderaannemers net als de erkende partijen zelf verplicht aan de betrokken toezichthouder de benodigde medewerking te verlenen.

Hoe de toezichthouder invulling geeft aan zijn rol van toezichthouder, wordt afgestemd met de minister van BZK. Daarbij wordt conform de Aanwijzingen inzake Rijksinspecties[66] de onafhankelijke informatieverzameling en oordeelsvorming verzekerd. De toezichthouder zoekt bij de invulling van zijn taak afstemming met andere toezichthouders die op dit taakveld eigenstandige taken en bevoegdheden kennen. Ratio hierachter is onder andere de vermindering van de toezichtlast voor bedrijven. Hierbij valt de denken aan afstemming met De Nederlandsche Bank in het geval ook inlogmiddelen van banken een rol gaan vervullen bij authenticatie voor

[66] *https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/besluiten/2015/10/01/aanwijzingen-over-de-rijksinspecties/aanwijzingen-over-de-rijksinspecties.pdf*

elektronische dienstverlening van de overheid. De toezichthouder heeft op grond van de Algemene wet bestuursrecht de bevoegdheid om te allen tijde zelf een inspectie of audit uit te voeren. Wanneer de toezichthouder dit nodig acht, zal die van deze mogelijkheid gebruik maken. De toezichthouder stelt niet alleen vast of (management)processen bestaan, maar kent waar nodig een focus op de inhoud van processen en de werking van die processen in de praktijk. De ervaringen met het incident DigiNotar benadrukken de noodzaak hiervan. Zie het Onderzoeksrapport van de Raad voor de Veiligheid, het DigiNotarincident, Waarom digitale veiligheid de bestuurstafel te weinig bereikt, 2012.[67]

Conformiteitsbeoordeling van de erkende partij door een hiertoe geaccrediteerde instelling speelt niet alleen een rol in het kader van de procedure van aanvraag van een erkenning. Onderdeel van het conformiteitsbeoordelingsschema is een periodieke herbeoordeling van de normconformiteit, die in opdracht van de erkende partij wordt uitgevoerd door een hiertoe geaccrediteerde instelling. De toezichthouder kan bij de uitoefening van zijn toezicht gebruik maken van de rapportages die de erkende partij in dit verband laat vervaardigen. Deze rapportages en verklaringen die door conformiteit beoordelende instellingen op basis daarvan worden afgegeven, ontslaan de toezichthouder echter nooit van zijn eigenstandige verantwoordelijkheid om waar nodig op basis van eigen informatie en eigen onderzoek een oordeel te vormen over de mate van normconformiteit. Hiermee sluit dit wetsvoorstel aan bij het kabinetsstandpunt inzake certificering in relatie tot toezicht.[68]

Handhaving en bestuurlijke sancties
In het wetsvoorstel is instrumentarium opgenomen voor handhavend en sanctionerend optreden jegens de erkende diensten en middelen. De minister van BZK krijgt de bevoegdheid om conform de Algemene wet bestuursrecht[69] een bestuurlijke boete, een last onder dwangsom of een last onder bestuursdwang op te leggen. De bevoegdheden en sanctiemogelijkheden gelden onverkort voor alle erkende diensten en middelen.
De mogelijkheid bestaat dat de minister van BZK zijn handhavende bevoegdheden mandateert aan de toezichthouder. Het opleggen van bestuurlijke sancties is normaliter het sluitstuk van de escalatieladder bij toezicht. Wanneer de door de minister van BZK daartoe aangewezen ambtenaren vaststellen dat een of meer van de regels op grond van artikel 6, zevende lid en artikel 7 van dit wetsvoorstel niet of niet meer worden nageleefd, zullen zij in beginsel eerst met de betrokken partij in contact treden om deze alsnog binnen een bepaalde termijn in overeenstemming met de gestelde regels te laten handelen. Als het gewenste resultaat desondanks uitblijft of te lang op zich laat wachten, kunnen de daartoe aangewezen ambtenaren overgaan tot het initiëren van formele handhaving door de minister. Dit laat echter onverlet dat de toezichthouder, indien de aard en de ernst van de situatie dit vereist, zonder voorafgaand overleg met de betrokken partij tot het opleggen van maatregelen kan overgaan.

Schorsen en intrekking erkenning
Het intrekken of schorsen van de erkenning van een partij of middel op grond van artikel 13 van dit wetsvoorstel, is een bevoegdheid van de minister van BZK waarvan de aard zich tegen mandatering verzet. Indien de door de minister van BZK aangewezen toezichthoudende ambtenaren op basis van activiteiten die zij uitvoeren in relatie tot hun toezichttaak van oordeel zijn dat een partij de in dit wetsvoorstel gestelde eisen van de artikelen 6, zevende lid, en artikel 7 niet (langer) naleeft, kunnen zij de minister adviseren om tot schorsing of intrekking van de erkenning over te gaan. Uiteindelijk is het de minister van BZK die hierover beslist.

Toezicht bij veiligheidsinbreuken en integriteitsverliezen
Maatregelen die tot doel hebben de veiligheid van aangeboden diensten in de authenticatieketen op passende wijze te waarborgen, kunnen het risico op veiligheidsinbreuken of verlies van integriteit verminderen maar niet uitsluiten. Indien zich een incident met diensten in de authenticatieketen voordoet, dient vertrouwen zoveel mogelijk behouden te blijven of te worden hersteld. Diensten in de authenticatieketen zijn verplicht een veiligheidsinbreuk of

[67] *www.onderzoeksraad.nl/uploads/items-docs/1094/Rapport_Diginotar_NL_web_def_20062012.pdf*
[68] *Vergaderjaar 2015-2016, Kamerstuk 29304 nr. 6*
[69] *Hoofdstuk 5 van de Awb regelt de handhaving van wettelijke voorschriften door bestuursorganen.*

integriteitsverlies met aanzienlijke gevolgen voor de verleende dienst of voor de persoonsgegevens die daarmee worden beheerd, zo spoedig mogelijk, maar in ieder geval binnen vierentwintig uur na ontdekking te melden bij de toezichthouder. Als de veiligheidsinbreuk of het integriteitsverlies waarschijnlijk negatieve gevolgen heeft voor de gebruikers, moeten deze hierover door de aanbieder onmiddellijk worden geïnformeerd. Indien het algemeen belang daarmee wordt gediend, kan de toezichthouder bepalen dat het publiek wordt of moet worden geïnformeerd over een veiligheidsinbreuk of integriteitsverlies. Doel van deze verplichtingen is het bevestigen en waar nodig herstellen van het vertrouwen van het publiek, de klanten, de markt, de overheid en de toezichthouders in de desbetreffende instelling of het desbetreffende bedrijf en in elektronische identificatie en authenticatie bij de overheid in het algemeen. Ten algemene dient niet te snel te worden aangenomen dat een melding op grond van deze wetgeving achterwege kan blijven. Gelet op de ernst en omvang van de gevolgen die een incident met een dienst in de authenticatieketen kan veroorzaken, dient deze wetgeving hierin ruim opgevat te worden. Dat wil zeggen dat ook sprake is van aanzienlijke gevolgen als bedoeld in deze wetgeving indien een incident aanzienlijke gevolgen voor de verleende dienst kan hebben, ongeacht of het zeker is dat die zullen intreden. En in geval van gerede twijfel over de vraag hoe groot de gevolgen daadwerkelijk zouden kunnen zijn, dient eveneens tot melding te worden overgegaan. Indien daarentegen vaststaat dat een veiligheidsinbreuk of integriteitsverlies slechts beperkte impact heeft, kan een melding achterwege blijven. De verlener van een dienst in de authenticatieketen zal in dat geval in staat zijn de inbreuk snel en adequaat te herstellen.

Ook de eIDAS verordening (artikel 19 lid 2) kent een meldplicht. Deze geldt voor verleners van vertrouwensdiensten. Met dit wetsvoorstel wordt de meldplicht op grond van de eIDAS verordening uitgebreid naar erkende aanbieders van diensten in de authenticatieketen. In veel gevallen zijn dit dezelfde bedrijven die gelijksoortige veiligheidsnormen in acht dienen te nemen. De meldplicht uit de eIDAS verordening en uit dit wetsvoorstel zijn zo veel mogelijk gelijksoortig vormgegeven. Om die reden wordt in dit wetsvoorstel niet een nieuwe meldplicht met eigen procedures en meldindicatoren voorgeschreven. Veeleer wordt een bestaande praktijk uitgebreid die bij veel erkende diensten reeds geldt op basis van andere diensten die zij aanbieden, zoals elektronische handtekeningen. Het overgrote deel van de partijen die op basis van deze wet worden verplicht incidenten te melden, kent deze verplichting al ten aanzien van gelijksoortige incidenten. Op deze manier wordt de administratieve last die gepaard gaat met deze meldplicht geminimaliseerd.

10. Financiële bepalingen en -gevolgen

10.1 Inleiding

Voorop staat dat alle bij dit wetsvoorstel betrokken partijen financiële gevolgen zullen ondervinden van het wetsvoorstel. De ontwikkeling van deze gevolgen in de tijd is van vele variabelen afhankelijk, zoals het gebruik dat van de diverse middelen wordt gemaakt, de individuele inrichting van de interne ICT-voorzieningen, de mate waarin partijen de komende jaren, bij aanpassing van hun ICT-voorzieningen (kunnen) voorsorteren op de nieuwe situatie, de (nieuwe) eisen die aan de technologie worden gesteld, de hoogte van de kosten voor de generieke voorziening en het toezicht, en de mate waarin dit wordt doorbelast. Dit betekent dat de financiële gevolgen pas in de loop van de tijd duidelijker zullen worden.

De belangrijkste kostencomponenten van het eID stelsel zijn:
- De directe stelselkosten: dit zijn de kosten van instandhouding, beheer en exploitatie van de publieke voorziening BSN-K, en van het publiekrechtelijke verankerde stelsel voor toelating van en toezicht op publieke en private middelen en diensten,
- De kosten van ontwikkeling, instandhouding, beheer en exploitatie van de publieke authenticatiedienst en de publieke machtigingsdienst, en de uitgifte van publieke middelen,
- De kosten die publieke dienstverleners maken om aan te sluiten op het stelsel en de kosten die zij maken voor ontsluitende- en authenticatiediensten, en
- De kosten die private erkende partijen in rekening brengen in het kader van dienstverlening in het eID stelsel.

Voor de financiering van het voorgestelde eID-stelsel, zoals ook neergelegd in dit wetvoorstel, gelden de volgende uitgangspunten:

1) Publieke dienstverleners betalen voor:
   - de aanpassing van hun eigen, interne ICT-infrastructuur,
   - de diensten van de ontsluitende diensten (en daarmee ook voor de diensten van de overige erkende diensten, via deze ontsluitende diensten);
2) Gebruikers (burgers en bedrijven) kunnen kosten voor de aanschaf van een middel in rekening gebracht worden. Dat gebeurt in ieder geval voor de kosten van het e-rijbewijs en e-NIK;
3) De kosten van de instandhouding van de generieke voorziening, het BSN-K, en van het publiekrechtelijke verankerde stelsel van toezicht op erkende partijen worden door het Rijk gedragen, maar kunnen door het Rijk doorberekend worden. Voor de inwerkingtreding van de wet wordt (bij algemene maatregel van bestuur) bepaald of en in hoeverre (een gedeelte van) deze kosten ook daadwerkelijk doorberekend worden;
4) Van de rechtspersonen die een aanvraag tot erkenning doen zal in beginsel door het Rijk een vergoeding voor de kosten van de afwikkeling van de aanvraag gevraagd worden.

10.2. Financiële bepalingen

Kosten voor afwikkelen aanvraag erkenning
Authenticatiediensten, ontsluitende diensten, machtigingsdiensten en attributendiensten zullen om deel te nemen aan het eID stelsel erkend moeten worden door de minister van BZK. Ingevolge dit wetsvoorstel kan van deze diensten door het Rijk (lees: minister van BZK) een eenmalige vergoeding gevraagd worden voor het afwikkelen van een aanvraag tot erkenning. Dat deze kosten kunnen worden doorberekend aan de aanvrager is in lijn met het kabinetsbeleid.[70] Ook de Afdeling advisering van de Raad van State is van mening dat doorberekening gerechtvaardigd is vanuit het principe dat betaald moet worden voor de concreet aanwijsbare tegenprestatie van de overheid in de vorm van een erkenning.[71]

Ingevolge dit wetsvoorstel worden bij of krachtens algemene maatregel van bestuur regels gesteld over het doorberekenen van de kosten van het afwikkelen van de aanvraag. Er is in dit wetsvoorstel voor gekozen om de bevoegdheid van de minister van BZK om de kosten van erkenning door te belasten bij algemene maatregel van bestuur te reguleren, omdat het een nieuw stelsel is en daarmee kan worden ingespeeld op de actuele ontwikkelingen. Daarbij kan er ook voor gekozen worden om in de opstartfase geheel of ten dele geen of minder kosten voor de erkenning in rekening te brengen om daarmee de totstandkoming van het stelsel niet onnodig (financieel) te belemmeren. De vergoeding voor de afwikkeling van de aanvraag zal ten hoogste de kosten bedragen die in redelijk zijn toe te rekenen aan de activiteiten die de overheid in het kader van de erkenning verricht. De belangrijkste kostenpost is daarbij de post loonkosten. Deze kosten kunnen per categorie dienst verschillen. Met het beoordelen van een aanvraag tot erkenning als authenticatiedienst met betrekking tot een middel, kunnen bijvoorbeeld meer kosten voor het Rijk zijn gemoeid dan met een aanvraag tot erkenning van een attributendienst.

Grondslag doorberekening kosten aan erkende diensten
De regering acht het voorts gewenst dat de mogelijkheid bestaat om de kosten van de voorziening BSN-K, en het toezicht, door te berekenen aan de partijen die hier profijt van ondervinden, te weten de erkende diensten (authenticatiediensten, ontsluitende diensten, machtigingsdiensten en attributendiensten), die overigens op hun beurt deze kosten weer door kunnen/zullen belasten aan (uiteindelijk) de bestuursorganen en aangewezen organisaties. Daarom voorziet het wetsvoorstel in een bevoegdheid van de minister van BZK om deze kosten overeenkomstig bij of krachtens algemene maatregel van bestuur vast te stellen regels door te kunnen belasten aan de erkende diensten. Gekozen is hier voor een regeling bij algemene maatregel van bestuur omdat de kosten vooraf niet goed zijn in te schatten, kunnen variëren in de tijd, en de wenselijkheid van doorbelasting ook zal afhangen van de ontwikkelingen binnen het stelsel, onder meer het aantal

[70] *Maat houden 2014. Bekendmaking van het kader voor de doorberekening van toelatings- en handhavingskosten, ministerie van Veiligheid en Justitie, Stscrt. 2014, nr. 16734.*
[71] *Voorlichting over de doorberekening van kosten door het ministerie van EZ aan het bedrijfsleven, in het bijzonder ten aanzien van de huidige wijze van doorberekening van handhavings-, toezichts- en keuringskosten door de Nederlandse Voedsel- en Warenautoriteit (NVWA). Kamerstukken II 2015/2016, 33 835, nr. 46.*

partijen dat zal deelnemen en het aantal authenticaties dat zal plaatsvinden. Daarbij is tevens relevant dat regulering bij algemene maatregel van bestuur de mogelijkheid geeft om in te spelen op de actuele ontwikkelingen.

Voor wat betreft de doorberekening van de kosten van toezicht zijn het hiervoor reeds vermelde kabinetsstandpunt en de uitgebrachte voorlichting van de Afdeling advisering van de Raad van State van belang. Uitgangspunt hierin is dat de kosten van toezicht in beginsel uit de algemene middelen moeten worden voldaan, omdat het belang van het (doen) naleven van regels de gemeenschap in haar geheel dient. Bij de vaststelling van de algemene maatregel van bestuur zal belang worden gehecht aan het feit dat het voorzien in authenticatiemiddelen, of een ontsluitende dienst of machtigings- of attributendienst geen (klassieke) overheidstaak betreft, zodat doorberekening van toezichtskosten meer in de rede ligt. Voorts wordt er rekening mee gehouden dat de kosten die gemaakt zullen worden voor het toezicht substantieel zullen zijn, mede vanwege het grote belang van continuïteit van de authenticatiemogelijkheid en daarom van een intensief toezicht. Ten slotte gaat de regering er vanuit dat het aantal partijen waarop op grond van dit wetsvoorstel toezicht gehouden zal worden overzichtelijk zal zijn, zodat er geen pragmatische redenen zijn om deze kosten niet door te belasten.

De bijdrage in de kosten van de generieke voorziening en het toezicht zal per categorie dienst kunnen verschillen en bovendien zal de omvang van de dienst bepalend zijn voor de hoogte van de bijdrage. Ook kan de algemene maatregel van bestuur bepalen dat in de eerste jaren na inwerkingtreding van deze wet niet of slechts beperkt gebruik gemaakt wordt van de mogelijkheid om kosten aan de betrokken partijen door te belasten. Dit om te voorkomen dat als nog niet alle beoogde dienstverleners zijn aangesloten al deze kosten aan deze beperktere groep worden doorberekend. Ook kunnen in de algemene maatregel van bestuur bijzondere gevallen worden benoemd waarin niet de volledige kosten worden doorberekend.

De erkende diensten zullen als gezegd de bij hen in rekening gebrachte kosten weer door kunnen belasten in de tarieven die zij stellen voor hun dienstverlening aan (uiteindelijk) de dienstverleners. Overwogen is de kosten rechtstreeks in rekening te brengen bij de dienstverleners. Om de bestuurslasten respectievelijk administratieve lasten voor de dienstverleners te beperken, is hiervoor niet gekozen.

Regels inzake de tarieven en voorwaarden van de erkende diensten
De overeenkomsten inzake de diensten van private erkende partijen kunnen tot stand komen in onderhandelingen tussen de betrokken partijen. Om te borgen dat hierbij een afgewogen prijsstelling bereikt wordt cq. te voorkomen dat er ongewenste en/of onredelijke prijsstellingen ontstaan, kunnen op grond van dit wetsvoorstel bij of krachtens algemene maatregel van bestuur aanvullende regels over de gehanteerde tarieven en voorwaarden gesteld worden.

Met name bij de start van het nieuwe stelsel, doch ook in een latere fase, is er een aantal onzekerheden die kunnen leiden tot de noodzaak om tijdelijk dan wel duurzaam (centraal) in te grijpen op de tariefstelling:

- Er is op den duur een redelijke inschatting te maken van het totaal aantal verwachte authenticaties binnen het eID-stelsel. Voor individuele authenticatiediensten, zeker bij de start van het stelsel, is dit lastig. De burger bepaalt welk erkend middel hij gebruikt (binnen de eisen van het stelsel). Dit betekent dat in de aanvangsfase moeilijk is in te schatten hoe vaak een bepaald middel gebruikt gaat worden. De kosten voor authenticatie met een bepaald middel zijn sterk gerelateerd aan het totaal aantal authenticaties met dat middel. Bij hogere aantallen nemen de kosten significant af. Het is dus voor een authenticatiedienst, zeker in de beginperiode, lastig in te schatten tegen welke prijs een middel moet worden aangeboden.
- Een dienstverlener is verplicht alle erkende middelen die aan de betrouwbaarheidseisen van zijn diensten voldoen te accepteren. Dit betekent dat zijn onderhandelingsvrijheid bij het maken van prijsafspraken voor deze dienstverlening afwezig tot (zeer) beperkt is.
- Er is in economische termen geen *'level playing field'* voor de authenticatiediensten. Van mogelijke aanbieders als banken is de benodigde infrastructuur al voor een aanzienlijk deel bekostigd in het kader van de bancaire dienstverlening die zij nu reeds aanbieden. En ook bij

de publieke middelen op het hoogste niveau, het e-rijbewijs en e-NIK, wordt een gedeelte van de kosten al gedekt doordat bij het uitgifteproces gebruik gemaakt wordt van het uitgifteproces van de fysieke documenten en vindt er een verplichte doorberekening van de extra kosten voor de vervaardiging van deze documenten plaats aan de burger.

Bij de bij of krachtens algemene maatregel van bestuur te stellen regels kan gedacht worden aan het stellen van een maximumtarief, bandbreedtes voor tarieven, een tariefstructuur of zelfs het vaststellen van een vast tarief. Zodra dat nodig is om de multimiddelenaanpak te laten slagen, zal worden overgegaan tot het dwingend ingrijpen in de tarieven en voorwaarden.
Gekozen is voor een regeling bij of krachtens algemene maatregel van bestuur, omdat er sprake is van een nieuw stelsel waarbij vooraf de gedragingen van de betrokken partijen en overige ontwikkelingen niet (goed) te voorspellen vallen. Het voordeel van een regeling bij algemene maatregel van bestuur is bovendien dat het gewenst kan zijn snel in te spelen op de ontwikkelingen in de markt.

10.3. Financiële gevolgen

Voor de gebruiker (burgers en bedrijven)
In de nieuwe situatie zal de gebruiker bij verschillende authenticatiediensten middelen kunnen afnemen om zich bij de dienstverleners te kunnen authenticeren. Zoals hiervoor aangegeven, heeft het kabinet besloten om de aanschafkosten van de publieke middelen verbonden aan e-rijbewijs en e-NIK via het heffen van leges bij de gebruiker in rekening te brengen.[72] Het gebruik van de publieke middelen zal niet worden doorbelast aan de gebruiker, maar (uiteindelijk) aan de dienstverlener.

Voor het heffen van de leges voor de aanschaf bestaat reeds een wettelijke basis in de Paspoortwet voor wat betreft de eNIK. Dit wetsvoorstel bevat een voorstel tot wijziging van de Wegenverkeerswetgeving voor het creëren van een wettelijke grondslag voor het heffen van leges voor de chip op het e-Rijbewijs. Dit wetsvoorstel voorziet ten slotte in een grondslag voor het vaststellen van een tarief voor andere publieke middelen. Of hiervoor daadwerkelijk een tarief wordt gesteld is afhankelijk van de daadwerkelijke kosten van uitgifte van dit middel.

De private partijen zijn op grond van dit wetsvoorstel vrij om de gebruiker al dan niet te laten betalen voor de aanschaf of het gebruik van de middelen die zij leveren en voor welk tarief. Dit kan worden overgelaten aan de marktwerking zodat overheidsinterventie voor deze relatie ongewenst is. Indien de private partijen te hoge tarieven zullen stellen voor de gebruiker voor de aanschaf of het gebruik van het middel, zullen zij zichzelf vanzelf uit de eID-markt prijzen en zijn hun ontwikkelingskosten voor niets geweest.

Voor authenticatiediensten
Alvorens de authenticatiedienst zijn diensten kan aanbieden, zal hij door de minister van BZK erkend moeten worden met betrekking tot een door hem aangeboden middel. Naast de ontwikkelingskosten van de middelen, zal de authenticatiedienst te maken krijgen met de kosten van de inschakeling van een geaccrediteerde certificerende instelling die toetst of de authenticatiedienst en het middel aan de gestelde eisen voldoen. Gelet op het technische karakter, zullen deze kosten mogelijk aanzienlijk zijn. Voorts zal de authenticatiedienst op grond van dit wetsvoorstel verplicht kunnen worden per middel een bedrag te betalen aan het Rijk voor de kosten van de erkenning van deze dienst met betrekking tot dat middel. Daarnaast kan het zijn dat de authenticatiedienst een meer permanente vergoeding aan het Rijk moet betalen in verband met de instandhouding van het BSN-K en het toezicht.

Na zijn erkenning zal de authenticatiedienst inkomsten genereren. Bij het gebruik zal hij elke keer als een gebruiker bij een dienstverlener inlogt aan de ontsluitende dienst een authenticatieverklaring afgeven, die deze doorsluist naar de dienstverlener. Voor het afgeven van deze authenticatieverklaring zal de authenticatiedienst een tarief in rekening brengen bij de ontsluitende dienst.

[72] *Kamerstukken II, 2015/16, 26 643, nr. 419, blz. 5.*

Voor ontsluitende diensten
Net als de authenticatiediensten zullen ook de ontsluitende diensten voor hun diensten erkend moeten worden door de minister van BZK. Voor deze erkenning zal de ontsluitende dienst in de eerste plaats kosten hebben voor de inschakeling van een geaccrediteerde certificerende instelling die toetst of de ontsluitende dienst aan de uniforme set van eisen voldoet. De hoogte van deze kosten zijn nog niet bekend. Voorts kan de ontsluitende dienst net als de authenticatiedienst op grond van dit wetsvoorstel de kosten voor erkenning in rekening gebracht worden en bestaat de mogelijkheid dat kosten die het Rijk maakt in verband met de generieke voorziening of het toezicht aan de ontsluitende diensten worden doorberekend. Na zijn erkenning zal de ontsluitende dienst aan de authenticatiediensten moeten betalen voor het afgeven van de authenticatieverklaring en, indien aan de orde, aan de ingeschakelde machtigingsdienst of attributendienst voor de door hen geleverde werkzaamheden. Aan de andere kant zal de ontsluitende dienst voor zijn diensten een tarief in rekening brengen bij de bestuursorganen en aangewezen organisaties.

Voor publieke dienstverleners
Voor rekening van de publieke dienstverleners (belastingdienst, het Uitvoeringsinstituut werknemersverzekeringen, Sociale Verzekeringsbank, gemeenten, ziektekostenverzekeraars etc.) komen in de eerste plaats de kosten voor het aansluiten op de ontsluitende dienst. Ook zal de interne digitale infrastructuur geschikt gemaakt moeten worden om met de berichten van het eID-stelsel te kunnen werken en (zo nodig) om aan de bij of krachtens algemene maatregel van bestuur te stellen regels inzake de betrouwbaarheid en beveiliging van de toegang tot elektronische diensten te voldoen. Eventuele kosten zijn sterk afhankelijk van de specifieke, individuele, ICT-voorziening van die dienstverlener. Daarnaast zullen de dienstverleners ook (via de ontsluitende diensten) moeten betalen voor het gebruik van de middelen en, indien aan de orde, voor het inschakelen van de machtigingsdienst of attributendienst.
Jaarlijks zullen de dienstverleners bovendien op grond van het wetsvoorstel door een onafhankelijke auditor een audit moeten laten uitvoeren om te toetsen of hun digitale infrastructuur voor de toegang tot elektronische diensten voldoet aan de hiervoor bedoelde regels. Verwacht wordt dat de kosten van deze audit liggen in de orde van grootte van de huidige DigiD-assesments die reeds jaarlijks plaatsvinden.

Naast deze kosten, zullen de dienstverleners ook baten genereren door het gebruik van een generieke, betrouwbare infrastructuur voor het digitaal inloggen (meer diensten digitaal ontsluiten en door hogere betrouwbaarheid minder risico's). Het is niet goed mogelijk om de precieze kosten van aansluiting en het gebruik, en de baten hiervan vooraf in te schatten. Er wordt echter vanuit gegaan dat de baten opwegen tegen de lasten. Daarom zullen de publieke dienstverleners niet door het Rijk worden gecompenseerd voor het feit dat zij als gevolg van dit wetsvoorstel hun digitale infrastructuur moeten aanpassen.

<u>Standaarden</u>
Dit wetsvoorstel brengt voor bestuursorganen voorts de verplichting mee om bepaalde bij algemene maatregel van bestuur aan te wijzen open standaarden te hanteren voor het elektronisch verkeer. Voor wat betreft de financiële gevolgen van deze verplichting is relevant dat er vanuit wordt gegaan dat open standaarden worden aangewezen die doorgaans nu al door de bestuursorganen (moeten) worden gehanteerd. Dit betekent dat bestuursorganen in beginsel geen financiële gevolgen ondervinden van het verplicht stellen van een standaard. Voor het geval de bestuursorganen de standaarden nog niet hanteerden, zullen de implementatiekosten hiervan per te verplichten open standaard worden ingeschat. Dit zal plaatsvinden bij de voorbereiding van de algemene maatregel van bestuur waarbij de betreffende open standaard wordt aangewezen. Voor wat betreft een aantal informatieveiligheidstandaarden is reeds een indicatie gemaakt van de ordegrote van de implementatie, omdat het voornemen bestaat om deze standaarden bij algemene maatregel te verplichten. De indicatie is tot stand gekomen door consultatie van onder andere het Platform Internet Standaarden, en - voor wat betreft TLS en DNSSEC - de impactanalyse van VNG/KING. Hieruit blijkt dat voor een bestuursorgaan die de standaard nog niet toepast, de eenmalige implementatiekosten per standaard variëren van enkele honderden tot maximaal

tienduizend euro.[73] De jaarlijkse kosten variëren per standaard van ongeveer zevenhonderd tot vijfduizend euro.

Voor machtigingsdiensten en attributendiensten
De erkende machtigingsdiensten en erkende attributendiensten zullen naast de kosten van ontwikkeling van deze diensten, kosten hebben voor de erkenning en bovendien kunnen de kosten van het Rijk voor de generieke voorziening en het toezicht, aan hen worden doorbelast. Voor hun diensten zullen zij een tarief in rekening brengen bij de ontsluitende diensten.

Voor het Rijk
Het eID-stelsel brengt voor het Rijk uiteenlopende kosten met zich mee. Hiertegenover staan echter ook inkomsten. In totaal gaat het met name om de volgende kostenposten:

- De kosten van (door)ontwikkelingen en beheer van de middelen e-NIK, e-rijbewijs, DigiD substantieel en het nog tijdelijk in de lucht houden van de huidige versies van DigiD (inclusief de kosten voor de authenticatiedienst);
- De kosten van ontwikkeling, instandhouding, beheer en onderhoud van het BSN-K;
- De kosten van de inzagefunctie bij het BSN-K;
- De kosten gemoeid met het erkennen van de diverse diensten;
- De kosten voor instandhouding en gebruik van de publieke machtigingsdienst;
- De kosten van toezicht op de erkende diensten en middelen;
- De kosten van het gebruik van authenticatiemiddelen en de kosten van de ontsluitende diensten voor diensten die ten laste van de rijksbegroting komen (bijv. de belastingdienst).

Aan de inkomstenkant gaat het om de volgende inkomsten:

- Inkomsten als authenticatiedienst voor het uitgeven van het middel;
- Inkomsten als authenticatiedienst voor het gebruik van het middel;
- Inkomsten als erkenningsinstantie voor het erkennen van de diverse diensten;
- Inkomsten van de erkende diensten wegens het doorbelasten van kosten voor exploitatie en beheer van de algemene voorzieningen van het Rijk voor het eID stelsel.

11. Verhouding tot andere wetgeving en de eiDAS-verordening

11.1. Algemene wet bestuursrecht

Onderhavig wetsvoorstel heeft een directe relatie met een ander wetsvoorstel, te weten het voorstel van wet modernisering elektronisch bestuurlijk verkeer. Ingevolge dat wetsvoorstel tot wijziging van de Awb krijgen burgers en bedrijven het recht op elektronisch zakendoen met de overheid.

Op grond van de huidige Awb (afdeling 2.3) is het gebruik van de elektronische weg alleen toegestaan als zowel de burger of het bedrijf, als het bestuursorgaan met het gebruik hiervan hebben ingestemd. Op grond van genoemd wetsvoorstel kunnen burgers en bedrijven ook eenzijdig kiezen om hun berichten die onderdeel uitmaken van een procedure inzake een besluit, een voorgeschreven melding of een klacht, digitaal aan een bestuursorgaan te doen toekomen. De instemming van het bestuursorgaan is dus voor dit soort berichten niet langer vereist. Bestuursorganen kunnen echter indien het gaat om berichten die tot één of meer geadresseerden zijn gericht niet eenzijdig besluiten tot de elektronische weg.[74] In deze gevallen zal een bestuursorgaan (tevens) de schriftelijke weg moeten openstellen ten behoeve van burgers en bedrijven die hieraan de voorkeur geven. Dit is alleen anders indien burgers en bedrijven bij of

[73] Het implementeren van TLS en DNSSEC ter bestrijding van websitefraude kost eenmalig ongeveer € 400 en jaarlijks ongeveer € 700. Het implementeren van DKIM en SPF ter bestrijding van email-fraude kost eenmalig € 2.500 tot € 10.000, en kost jaarlijks € 1.250 tot € 5.000.
[74] Een bestuursorgaan kan op grond van het voorstel van wet modernisering elektronisch bestuurlijk verkeer wel eenzijdig besluiten tot de elektronische weg indien het gaat om berichten die niet zijn gericht aan één of meer geadresseerden. Aangezien dergelijke berichten buiten de werkingssfeer van dit wetsvoorstel vallen, blijft dit in deze memorie verder buiten beschouwing.

krachtens de wet, zoals de Wet EBV, verplicht zijn om bepaalde zaken op elektronische wijze met een bestuursorgaan af te wikkelen. Voor die zaken bevat het wetsvoorstel tot wijziging van de Awb echter de verplichting voor bestuursorganen om personen voor wie de voorgeschreven elektronische weg onredelijk bezwarend is, ondersteuning aan te bieden.

Indien een burger of een bedrijf er (in de toekomst) voor kiest om via elektronische weg met een bestuursorgaan zaken te doen, is het vervolgens de vraag op welke elektronische wijze hij dit kan doen. Het nieuwe artikel 2:15 Awb verplicht het bestuursorgaan een kanaal (specifiek webformulier, een algemeen contactformulier, een app of een e-mail) voor het type bericht aan te wijzen. Op grond van dit wetsvoorstel zal het bestuursorgaan, voor zover het gaat om dienstverlening waarvoor het betrouwbaarheidsniveau substantieel of hoog geldt, deze dienstverlening alleen kunnen aanbieden met gebruik van erkende authenticatiemiddelen. Het is op grond van dit wetsvoorstel aan het bestuursorgaan om volgens bij ministeriële regeling te stellen regels, te bepalen voor welke elektronische diensten ten minste dit betrouwbaarheidsniveau substantieel of hoog geldt. Verwacht mag worden dat bestuursorganen de aanwijzing van het kanaal en de bijbehorende betrouwbaarheidsniveaus in hetzelfde besluit vastleggen. Het aanwijzen van een betrouwbaarheidsniveau kan worden aangemerkt als een invulling van de bevoegdheid van artikel 2:15, tweede lid, Awb om aan het gebruik van een kanaal nadere eisen te stellen.

11.2. Paspoortwet

Voor de invoering van de e-NIK is een wijziging van de Paspoortwet nodig. In artikel 3 van de Paspoortwet is namelijk limitatief omschreven welke gegevens op een reisdocument zijn vermeld en waarvan een reisdocument is voorzien. Hieraan zal een chip voor authenticatie aan toegevoegd moeten worden. Aangezien de Paspoortwet een rijkswet is, kan deze wetswijziging niet worden meegenomen met dit wetsvoorstel, doch zal worden opgenomen in een ander wetsvoorstel tot wijziging van de Paspoortwet.

11.3. Wegenverkeerswet

In dit wetsvoorstel is een wijziging van de Wegenverkeerswet opgenomen die regelt dat de zogenoemde rijkskostencomponent van het rijbewijs ook het authenticatiemiddel omvat. Dit betekent dat gemeenten bij de uitgifte van het e-Rijbewijs aan het Rijk extra kosten zullen moeten afdragen in verband met de authenticatiefunctie van het rijbewijs. Dit extra bedrag zal door de gemeenten vervolgens worden doorberekend in de hoogte van de door de burger voor het rijbewijs te betalen leges.

De modellen voor het rijbewijs en de gegevens waarvan het rijbewijs wordt voorzien, worden geregeld in de Regeling vaststelling modellen rijbewijzen en daarmee verband houdende formulieren. Aan de introductie van het e-Rijbewijs zal derhalve tevens een wijziging van deze ministeriële regeling vooraf moeten gaan. Hierin zal geregeld worden welke chip op het rijbewijs zal worden opgenomen.

11.4. Wet op de identificatieplicht

In de Wet op de identificatieplicht (WID) zijn de documenten aangewezen waarmee in bij de wet aangewezen gevallen de identiteit van personen kan worden vastgesteld. De documenten die zijn aangewezen zijn onder meer het Nederlandse paspoort en het Nederlandse rijbewijs. De vraag is of in de WID ook erkende authenticatiemiddelen aangewezen moeten worden, voor de gevallen waarin de identiteit langs elektronische weg wordt vastgesteld. Deze vraag dient ontkennend beantwoord te worden. De documenten of te wel identiteitsbewijzen die in de WID zijn aangewezen zijn bedoeld voor de fysieke controle van de identiteit van een persoon. Een identiteitsbewijs als genoemd in de WID bevat in elk geval de naam, adres en woonplaats, een foto, het BSN indien dat is toegekend en verder de gegevens die nodig zijn voor het doel waarvoor het bewijs is uitgegeven. De aanwijzing van de documenten in de WID houdt primair verband met de algemene identificatieplicht, die ook in die wet is geregeld, van een ieder die de leeftijd van veertien jaar heeft bereikt om op de eerste vordering van bepaalde ambtenaren, militairen of toezichthouders, handelend in het kader van een redelijke taakuitoefening, een algemeen erkend

identiteitsbewijs te tonen. Naast de algemene identificatieplicht in de WID zijn in een groot aantal specifieke wetten bijzondere identificatie- en controleplichten opgenomen waarin – voor het voldoen aan die verplichting – verwezen wordt naar een of meer documenten genoemd in de WID. Bij de in de verschillende wetten geregelde identificatieplichten gaat het steeds om de fysieke controle van de identiteit van de betrokkene. Zo wordt in artikel 19e van Boek I van het Burgerlijk Wetboek bepaald dat de ambtenaar van de burgerlijke stand de identiteit van degene die aangifte van geboorte doet vaststelt aan de hand van een document als bedoeld in artikel 1 van de WID. In dit geval kunnen alle documenten genoemd in de WID (artikel 1) gebruikt worden ter identificatie.

Van deze identificatieplichten moeten worden onderscheiden de bepalingen in verschillende specifieke wetten die niet rechtstreeks een identificatieplicht jegens de overheid op de burger leggen, maar een andere burger of een particuliere instantie verplichten om de identiteit van de betrokkene te controleren. Ook bij deze verplichtingen wordt verwezen naar een of meer documenten genoemd in de WID. Een voorbeeld is artikel 15a van de Wet arbeid vreemdelingen. Op grond van deze bepaling is een werkgever verplicht in bepaalde situaties de identiteit vast te stellen van een persoon, aan de hand van een document als bedoeld in artikel 1, eerste lid, onder 1° tot en met 3°, van de WID en de toezichthouder te informeren door een afschrift van dit document te verstrekken. In dit geval is identificatie aan de hand van een rijbewijs (een document als bedoeld in artikel 1, eerste lid, onder 4°) niet toegestaan aangezien op een rijbewijs de nationaliteit niet is vermeld.

De WID en de verschillende wetten waarin identificatieplichten zijn opgenomen en waarin verwezen wordt naar een of meer documenten genoemd in de WID, gaan derhalve uit van identiteitsbewijzen ten behoeve van fysieke controle van de identiteit of waarvan een afschrift kan worden gemaakt. In deze systematiek past het niet om ook erkende authenticatiemiddelen in de WID aan te wijzen, voor de gevallen waarin de identiteit langs elektronische weg wordt vastgesteld. De regering kiest er daarom voor om niet de WID aan te passen maar te zijner tijd de verschillende wetten waarin identificatieplichten zijn opgenomen te wijzigen indien de dienstverlening op het desbetreffende terrein (volledig) wordt gedigitaliseerd. Dit biedt ook de mogelijkheid per dienst te bepalen welk betrouwbaarheidsniveau (substantieel of hoog) voor de dienst tenminste is vereist. Bovendien kan dan – voor zover nodig – bepaald worden dat naast de authenticatie aan de hand van een erkend middel ook bepaalde attributen (zoals de nationaliteit of leeftijd) aan de betrokken dienstverlener, via een bepaalde attributendienst, verstrekt moeten worden.

11.5 Wet elektronisch berichtenverkeer Belastingdienst

De Wet EBV heeft het wettelijk kader geschapen voor het verplichten van elektronisch berichtenverkeer in het contact met de Belastingdienst. Deze wet, waarvan de uitvoering onder de primaire verantwoordelijkheid van de staatssecretaris van Financiën valt, biedt een grondslag voor verplicht elektronisch berichtenverkeer met de Belastingdienst. In artikel X van deze wet is bovendien een grondslag opgenomen voor voorzieningen voor onder meer elektronisch berichtenverkeer (MijnOverheid, Berichtenbox), elektronische authenticatie (DigiD) en elektronische registratie van machtigingen en het raadplegen ervan (DigiD Machtigen), alsmede voor de in dat verband noodzakelijke verwerking van persoonsgegevens. De zorg voor deze voorzieningen wordt aan de minister van BZK opgedragen. Tevens is bepaald dat de minister persoonsgegevens verwerkt, waaronder het BSN, voor zover dit noodzakelijk is voor de goede vervulling van deze taak. Bij algemene maatregel van bestuur, op grond van genoemd artikel, wordt nader bepaald welke persoonsgegevens worden verwerkt, aan wie deze worden verstrekt en hoe lang deze worden bewaard. Tot slot worden op basis van de Wet EBV regels gesteld met betrekking tot de werking, beveiliging en betrouwbaarheid van de genoemde voorzieningen.

Met de Wet EBV, in werking getreden op 1 november 2015, is derhalve een eerste fundament gelegd onder de GDI, in het bijzonder met het oog op de reeds in de praktijk functionerende voorzieningen MijnOverheid, DigiD en DigiD Machtigen. Ook het BSN-K, een voorziening die essentieel is voor het kunnen functioneren van publieke en private authenticatiemiddelen in het publieke domein, is ingevolge de Wet EBV nader gereguleerd.

Conform hetgeen in de memorie van toelichting bij de Wet EBV wordt vermeld, zullen de betreffende bepalingen komen te vervallen wanneer een specifieke en onder de primaire verantwoordelijkheid van de minister van BZK tot stand te brengen wet in werking treedt: de Wet GDI. Aangezien de onderhavige tranche van de WGDI de grondslag zal bieden voor zaken rondom authenticatie en machtigen en dus niet voor voorzieningen voor elektronisch berichtenverkeer en informatieverschaffing, blijft artikel X van de Wet EBV voor dit laatste onderdeel gehandhaafd. Ingevolge artikel 26 van de Wet GDI zal het bepaalde inzake authenticatie en machtigen in artikel X van de Wet EBV komen te vervallen en wordt dit artikel beperkt tot de zorg voor voorzieningen voor elektronisch berichtenverkeer en informatieverschaffing.

Voor wat betreft de onder de Wet EBV tot stand gekomen uitvoeringsregelgeving geldt dat het Besluit verwerking persoonsgegevens GDI tevens zal worden gebaseerd op de Wet GDI. Het in de Regeling voorzieningen GDI ter zake van de voorziening voor elektronisch berichtenverkeer en informatieverschaffing bepaalde, blijft gehandhaafd. Voor wat betreft het publieke middel DigiD Basis blijven gedurende drie jaar na de inwerkingtreding van de wet de regels van toepassing die ter zake gelden op de dag voor inwerkingtreding van deze wet. Het gaat om (de desbetreffende regels in) het Besluit verwerking persoonsgegevens GDI en de Regeling voorzieningen GDI.

11.6. eIDAS en eIDAS Uitvoeringsverordening

In de eIDAS verordening worden eisen gesteld aan het grensoverschrijdend gebruik van elektronische identiteiten en vertrouwensdiensten, en worden de lidstaten van de EU verplicht om genotificeerde middelen uit andere lidstaten te accepteren. Die eisen betreffen onder andere de betrouwbaarheid van middelen en uitgifteprocessen. Deze verordening definieert drie niveaus van betrouwbaarheid voor elektronische identificatiemiddelen, te weten laag, substantieel en hoog. Bij het opstellen van de eisen die op grond van dit wetsvoorstel aan de middelen worden gesteld, wordt uitgegaan van deze drie betrouwbaarheidsniveaus. Ook dienstverleners hanteren deze betrouwbaarheidsniveaus voor toegang tot hun online diensten.
Voor de niveaus substantieel en hoog wordt in de eIDAS-verordening geregeld dat de lidstaten stelsels voor elektronische identificatie bij de Europese Commissie kunnen notificeren. Genotificeerde middelen moeten door publieke dienstverleners in andere lidstaten ook geaccepteerd worden, mits passend bij het betrouwbaarheidsniveau van hun dienstverlening.

Voor het kunnen accepteren van middelen uit andere lidstaten wordt een zogeheten eIDAS-knooppunt ingericht. Wanneer een persoon met een genotificeerd buitenlands middel een dienst in Nederland wil afnemen, wordt deze door de ontsluitende dienst doorverwezen naar het knooppunt, dat via het buitenlandse eIDAS-knooppunt het contact legt met de betreffende buitenlandse authenticatiedienst die de authenticatie verder verzorgt. In dat opzicht werkt het knooppunt dus als een authenticatiedienst, zij het dat het knooppunt zelf geen middelen uitgeeft. Het berichtenverkeer dat samenhangt met grensoverschrijdende authenticatie wordt dus via de ontsluitende dienst en het eIDAS-knooppunt afgehandeld.

Het ligt in de rede om de Nederlandse erkende middelen op niveau substantieel en hoog bij de Commissie te notificeren, zodat alle erkende Nederlandse middelen ook in andere lidstaten gebruikt kunnen worden.

De eIDAS verordening is vergezeld gegaan van een aantal aanvullende technische verordeningen. Een daarvan is de zogenaamde eIDAS Uitvoeringsverordening (2015/1502 inzake technische specificaties). Deze bevat bepalingen over de specificaties en procedures voor de authenticatiemiddelen. In de bijlage bij de Uitvoeringsverordeningen zijn deze specificaties en procedures nader uitgewerkt. Deze specificaties en procedures vormen een belangrijke aanleiding voor de uitvoeringsregelgeving bij dit wetsvoorstel. In deze uitvoeringsregelgeving is voorzien in nadere precisering en uitleg op basis van de Nederlandse situatie van de overigens rechtstreeks werkende bepalingen van de Uitvoeringsverordening.

12. Gevolgen voor burgers en ondernemers

12.1 Gevolgen voor burgers

Het belangrijkste gevolg van het wetsvoorstel is dat diensten op het betrouwbaarheidsniveau hoog of substantieel ook daadwerkelijk op een veilige en betrouwbare online van de overheid afgenomen kunnen worden waar dat nu nog niet mogelijk is. Voor burgers gaat het om 24/7 beschikbaarheid, locatie onafhankelijkheid en minder administratieve lasten. Vanwege het feit dat de burger met verschillende (publieke en private) middelen kan inloggen bij online publieke diensten is de beschikbaarheid en bereikbaarheid van publieke dienstverlening beter geborgd. Werkt het ene inlogmiddel niet, dan kan de burger ervoor kiezen in te loggen met een ander middel. De burger heeft bovendien keuzevrijheid met welk middel hij wil inloggen, waarbij hij kan kiezen uit middelen die hij al mogelijk in zijn bezit heeft. Burgers zullen in principe de aanschafkosten van de publieke middelen moeten betalen. Het is aan de private authenticatiedienst te beslissen of hij ook een aanschafprijs in rekening brengt bij de burger.

Zoals in de visiebrief digitale overheid 2017[75] reeds aangegeven, draagt dit wetsvoorstel ten slotte bij aan de verbetering van de kwaliteit van digitale overheidsinformatie en overheidsdienstverlening. De maatschappelijke baten van het gebruik van de infrastructuur worden geboekt in bestuurlijke processen; de overheid zal moeten inspelen op gebruikerswensen, kostenbesparing en innovatie.

Regeldruk en administratieve lasten voor burgers
Het wetsvoorstel beoogt een bijdrage te leveren aan vermindering van de regeldruk en administratieve lasten voor burgers, doordat de toegang tot elektronische overheidsdienstverlening wordt geüniformeerd. Het wetsvoorstel regelt het voor authenticatie relevante deel van de infrastructuur bij bestuursorganen, zodat burgers met één erkend middel van het juiste betrouwbaarheidsniveau toegang hebben tot de digitale dienstverlening van alle bestuursorganen en aangewezen organisaties waarop het voorstel ziet. Hierdoor verminderen voor burgers de (administratieve) lasten, doordat hij niet langer aan diverse overheidsorganen dezelfde gegevens hoeft te verschaffen.

Een merkbaar effect op de lasten voor burgers kan ontstaan als gevolg van het doorberekenen (in leges) van kosten voor het authenticatiemiddel op identiteitsdocumenten zoals het rijbewijs of de Nederlandse identiteitskaart.

12.2. Gevolgen voor ondernemers

Het wetsvoorstel heeft in beginsel vooral effect op bestuursorganen en aangewezen organisaties, oftewel publieke dienstverleners, omdat de reikwijdte van het wetsvoorstel zich uitstrekt tot toegang tot hun dienstverlening. Voor bedrijven ontstaan geen nieuwe verplichtingen, tenzij het private rechtspersonen betreft die in de bijlage bij het wetsvoorstel of in een aanwijzingsbesluit worden aangewezen. Hierna wordt ingegaan op het effect voor bedrijven die erkende diensten aanbieden in de zin van dit wetsvoorstel Deze bedrijven moeten een erkenning verkrijgen alvorens zij hun diensten mogen leveren in het publieke domein. Hierbij is geen sprake van een marktverstorend effect omdat het iedereen vrij staat de erkenning aan te vragen.

Regeldruk en administratieve lasten voor ondernemers
Het wetsvoorstel beoogt een bijdrage te leveren aan vermindering van de regeldruk en administratieve lasten voor bedrijven, doordat er verplichtingen voor publieke dienstverleners worden geïntroduceerd waarmee de toegang tot elektronische dienstverlening wordt geüniformeerd en gestandaardiseerd. Het wetsvoorstel bevat regels voor de voor authenticatie relevante infrastructuur bij bestuursorganen en aangewezen organisaties, zodat bedrijven met een erkend middel van het juiste betrouwbaarheidsniveau toegang hebben tot de digitale dienstverlening van de bestuursorganen en aangewezen organisaties waarop het wetsvoorstel ziet.

[75] *Kamerstukken II 2012/13, 26 643, nr. 280.*

Voor een specifieke categorie van bedrijven is er een regeldrukeffect. Authenticatiediensten, ontsluitende diensten, machtigingsdiensten of attributendiensten moeten worden erkend door de minister van BZK, alvorens zij hun diensten mogen leveren. Voor deze erkenning kunnen leges in rekening worden gebracht. Het gaat hier om maximaal enkele tientallen bedrijven. Daarnaast zal door de minister bij de ontsluitende diensten een bedrag in rekening worden gebracht voor het gebruik van de publieke authenticatiedienst en publieke machtigingsdienst. De kosten van toezicht en van het BSN-K kunnen worden doorberekend aan de erkende diensten.

Het wetsvoorstel verplicht, naast bestuursorganen, ook aangewezen organisaties om erkende authenticatiemiddelen te accepteren. Deze aangewezen organisaties kunnen privaatrechtelijke organisaties zoals pensioenfondsen of zorgverleners zijn, die een publiekrechtelijke taak hebben en dientengevolge BSN mogen verwerken. Met de acceptatieplicht ter zake van de erkende middelen zijn kosten gemoeid voor de aangewezen organisaties. Daarnaast ontstaat voor hen een administratieve last, omdat zij periodiek een verklaring van een onafhankelijke auditor moeten overleggen, waaruit blijkt of zij voldoen aan de ingevolge (artikel 8 van) deze wet gestelde bepalingen over de werking, de betrouwbaarheid en de beveiliging van de toegang tot de elektronische diensten die zij in stand houden. Na aanwijzing van deze organisaties alsmede na de vaststelling van de hen regarderende regels is het mogelijk een preciezere raming van het regeldrukeffect te geven.

13. Overgangsrecht

Dit wetsvoorstel ziet op het gebruik van erkende authenticatiemiddelen in het elektronisch verkeer met bestuursorganen en aangewezen organisaties. Alleen middelen op het betrouwbaarheidsniveau 'substantieel' of 'hoog' kunnen in aanmerking komen voor het verkrijgen van een erkenning. Bestuursorganen en aangewezen organisaties mogen slechts toegang tot hun elektronische diensten op betrouwbaarheidsniveau 'substantieel' of 'hoog' verlenen, indien de gebruiker met een erkend middel inlogt. Zij zijn verplicht vanaf de inwerkingtreding van dit wetsvoorstel erkende middelen te accepteren. Niet-erkende middelen mogen niet geaccepteerd worden voor elektronische diensten op betrouwbaarheidsniveau 'substantieel' of 'hoog'. Hiervoor geldt geen overgangsrecht. Middelen op een lager betrouwbaarheidsniveau dan substantieel of hoog, zoals het uit te faseren middel DigiD, zullen niet worden erkend ingevolge dit wetsvoorstel. Bij wijze van overgangsperiode mogen bestuursorganen en aangewezen organisaties deze middelen met betrouwbaarheidsniveau laag nog drie jaar na de inwerkingtreding van dit wetsvoorstel accepteren voor diensten waarvoor een laag betrouwbaarheidsniveau geldt. Hiervoor zal een tarief in rekening worden gebracht.

Ook voor partijen die in de maand voorafgaand aan inwerkingtreding van de wet deelnemen aan *pilots*[76] *of* vooruitlopend op deze wet op grotere schaal op vrijwillige basis zijn overgegaan tot het

[76] *Vanaf 2015 zijn pilots gedaan met publieke en private authenticatiemiddelen. De pilots hadden tot doel:*
- *de uniforme eisen te beproeven op hun werking in de praktijk en de opgedane ervaring te benutten bij het opstellen van uitvoeringsregelgeving bij deze wet;*
- *de werking van het BSN-K te beproeven;*
- *de werking van een publiek eID-middel met betrouwbaarheidsniveau hoog te beproeven;*
- *te komen tot een stapsgewijze en gecontroleerde uitrol van de multimiddelenaanpak.*

Er zijn gedurende dit traject meerdere PIA's uitgebracht. De bevindingen uit deze PIA's alsmede de met de pilots opgedane ervaringen zijn telkens verwerkt in nieuwe eisen voor de pilots (aansluitvoorwaarden).
In 2015 en 2016 zijn pilots gehouden met private middelen, waaronder bankmiddelen. Er zijn achttien organisaties (o.a. Belastingdienst, UWV, SVB, ziekenhuizen, gemeenten en zorgverzekeraars) die hebben meegedaan met de pilots in het publieke domein. Bij deze organisaties kon worden ingelogd met (een van de) middelen die door vier private middelenleveranciers zijn aangeboden. Bij de Belastingdienst kon daarnaast worden ingelogd met een bankpas van zeven banken, die aan de pilot deelnamen. Per eind 2016 waren ongeveer 2500 private middelen van Idensys geactiveerd en ongeveer 2100 bankmiddelen.
Er zijn tussen februari en mei 2016 ook pilots geweest met het publieke middel, DigiD Hoog. Hieraan hebben ongeveer 1500 burgers uit de gemeenten Den Haag, Eindhoven en Groningen deelgenomen. Vanaf najaar 2015 is een pilot uitgevoerd met DigiD Substantieel. Hieraan hebben tot en met mei 2016 (de evaluatieperiode) 455 burgers deelgenomen.De pilots zijn geëvalueerd door de commissie evaluatie pilots publieke en private authenticatiemiddelen (commissie-Kuipers), die in mei 2016 advies heeft uitgebracht (Kamerstukken II, 2015/16, 26643, nr. 419, blg-780657. De commissie concludeerde dat er, op basis van de uitgevoerde pilots, goede grond is om, met inachtneming van de bevindingen uit de pilots, te komen tot zo concreet mogelijke en

gebruik van middelen op het betrouwbaarheidsniveau 'substantieel' of 'hoog' (de zogenoemde eerste fase uitrol eID), geldt overgangsrecht. Deze partijen lopen op basis van een privaatrechtelijke overeenkomst vooruit op deze wet. Deze overeenkomsten treden voor de duur van de overgangsperiode in de plaats van de wettelijke eisen bedoeld in artikel 7, eerste lid. Genoemde partijen worden op grond van het overgangsrecht geacht over een erkenning te beschikken tot een jaar na inwerkingtreding van deze wet. Dat betekent dat een aanvraag voor erkenning ruim binnen een jaar na inwerkingtreding moet worden gedaan en dat uiterlijk een jaar na inwerkingtreding ten aanzien van de desbetreffende partij door de minister van BZK een besluit moet zijn genomen als bedoeld in artikel 6. Ter zake gelden de reguliere bepalingen en termijnen van de Algemene wet bestuursrecht. Zonder formele erkenning geldt de desbetreffende partij na een jaar niet langer als erkend. Gedurende de overgangsperiode gelden deze partijen als erkende diensten als bedoeld in artikel 6. Afgezien van de eisen in artikel 7, eerste lid, gelden voor hen gedurende de overgangstermijn wel de overige bepalingen die in dit wetsvoorstel en de uitvoeringsregels zijn gesteld. Van deze diensten en de voorwaarden wordt – analoog aan artikel 6, negende lid – door de minister van BZK mededeling gedaan in de Staatscourant.

Een overgangstermijn geldt eveneens met betrekking tot de in de maand voorafgaand aan inwerkingtreding van de wet beproefde private middelen alsmede met betrekking tot het publieke middel (DigiD) op betrouwbaarheidsniveau substantieel, dat beschikbaar komt in de periode van voorbereiding van deze wet. Uiterlijk een jaar na inwerkingtreding van de wet moet ter zake van deze middelen een besluit tot erkenning zijn genomen. Het karakter van een publiek middel doet niet af aan de noodzaak van een erkenning als bedoeld in artikel 6.

14. Inwerkingtreding en invoering

In mei 2016 is op verzoek van het ministerie van BZK en het ministerie van EZ door PBLQ / Ecorys een rapport uitgebracht ten behoeve van de invoering van de Wet GDI: Invoeringsplan Wet GDI. Een belangrijke aanbeveling daarin is een ruime generieke invoeringstermijn te hanteren bij de invoering van de verplichting voor bestuursorganen om aan te sluiten op de GDI. Door aan te sluiten op het gemiddelde afschrijvings- en investeringsritme voor digitale voorzieningen, worden additionele kosten voor aansluiting vermeden en kosten van desinvesteringen geminimaliseerd.

In aansluiting hierop moet worden benadrukt, dat al te veel vrijblijvendheid vanuit de doelstelling om te komen tot een uniforme, transparante en veilige dienstverlening aan burgers en bedrijven onwenselijk is. Tegelijkertijd moet worden vermeden dat bestuursorganen en aangewezen organisaties pas kort voor inwerkingtreding van de wet de overstap naar erkende diensten en middelen in gang zetten. Concreet betekent dit het volgende.

De eerste tranche van de Wet GDI betreft een specifiek onderdeel van de GDI, te weten authenticatie. Vanaf de inwerkingtreding van het wetsvoorstel geldt voor bestuursorganen en aangewezen organisaties de acceptatieplicht ter zake van authenticatiemiddelen op het niveau substantieel en hoog en moeten zij aan, goeddeels reeds in de praktijk gehanteerde, bepalingen inzake werking, beveiliging en betrouwbaarheid voldoen. Dit is een verantwoord tijdspad, ervan uitgaande dat met de start eind 2016 van de (internet)consultatie, bestuursorganen en aan te wijzen organisaties kunnen beginnen met een eerste oriëntatie op hetgeen deze wet voor hen meebrengt, en al hiermee rekening kunnen houden bij beslissingen over hun toekomstige investeringen voor digitale voorzieningen.

Voor middelen met een betrouwbaarheidsniveau laag geldt dat deze drie jaar na inwerkingtreding van het wetsvoorstel nog mogen worden geaccepteerd voor dienstverlening op betrouwbaarheidsniveau laag. Na die datum mogen bestuursorganen en de aangewezen

---

implementatiegerichte vervolgstappen in de multimiddelenaanpak. Gelet op de beperkte strekking van de pilots adviseerde de commissie tevens om bij de verdere realisatie het beproeven van de verschillende onderdelen van de multimiddelenaanpak voort te zetten. De pilots met private middelen zijn voortgezet in 2017. Hieraan is door xx organisaties en xx private middelenleveranciers deelgenomen. In het totaal zijn tot en met xx 2017 xx middelen geactiveerd. Vanaf xx 2017 is DigiD Substantieel beschikbaar gekomen. Hiermee zijn per xx 2017 xx authenticaties uitgevoerd.

organisaties nog slechts gebruik maken van erkende diensten en erkende middelen, die naar hun aard - anders komen ze namelijk niet voor erkenning in aanmerking - van voldoende hoog niveau zijn. Het publieke middel DigiD wordt om redenen van veiligheid en betrouwbaarheid uitgefaseerd en vervangen door middelen van een hoger betrouwbaarheidsniveau. Omdat, gegeven de technologische ontwikkelingen, verwacht wordt dat het aantal diensten waarbij met een betrouwbaarheidsniveau laag kan worden volstaan zal afnemen en dus sprake zal zijn van afnemend gebruik, zullen de kosten van instandhouding van een publiek middel op betrouwbaarheidsniveau laag niet meer verdedigbaar zijn.

In het kader van de invoering van dit wetsvoorstel is tevens de eIDAS verordening van belang. De verordening regelt onder andere de grensoverschrijdende wederzijdse erkenning van authenticatie- en identificatiemiddelen voor online publieke dienstverlening. Volgens de verordening moeten openbare instanties, waarvoor op grond van nationaal recht of gangbare bestuursrechtelijke praktijk elektronische identificatie met gebruikmaking van een elektronisch identificatiemiddel en authenticatie vereist is, met ingang van 18 september 2018, grensoverschrijdende authenticatiemiddelen accepteren, die zijn aangemeld bij de Europese Commissie. De eIDAS-verordening verplicht openbare instanties vanaf die datum tot erkenning van elektronische identificatiemiddelen van de niveaus ‘substantieel’ of ‘hoog’ uit andere lidstaten. Het wetsvoorstel bevat hiertoe een clausule van wederzijdse erkenning (artikel 5, derde lid). Bestuursorganen en aangewezen organisaties moeten in dit verband aansluiten op een nationaal eIDAS knooppunt, dat wordt ontsloten via de ontsluitende dienst.

15. Consultatie

PM

II Artikelsgewijs

Artikel 2

Lid 1
Artikel 2 heeft een ruime reikwijdte. Het verplicht bestuursorganen als bedoeld in artikel 1:1, eerste lid, van de Algemene wet bestuursrecht (zogeheten a en b- bestuursorganen, inclusief ZBO's), organen, personen en colleges als bedoeld in artikel 1:1, tweede lid, van de Algemene wet bestuursrecht (oa de Eerste en Tweede Kamer, de rechterlijke macht, de Raad van State en de Nationale ombudsman) en zogeheten rechtspersonen met een wettelijke taak (RWT[77]) tot de toepassing van de ingevolge het tweede lid aangewezen standaarden.

Standaarden zijn afspraken over elektronische gegevensuitwisseling, vastgelegd in zogeheten specificatiedocumenten, die beschrijven hoe gegevens er uit zien, wat ze betekenen en hoe ze kunnen worden uitgewisseld. Aldus wordt het mogelijk om op efficiënte, veilige en betrouwbare wijze (administratieve) processen geautomatiseerd af te wikkelen en onafhankelijkheid van ICT-systeemleveranciers te bewerkstelligen. Van de publieke en semi-publieke sector wordt sinds 2008 verwacht dat deze de standaarden, die op de zogeheten 'pas toe of leg uit' lijst staan, bij aanschaf of (ver)bouw van ICT-systemen hanteren en toepassen in het elektronisch verkeer. 'Pas toe of leg uit'-standaarden zijn open, dat wil zeggen algemeen beschikbare, onbeperkt (her)bruikbare en via een transparant proces ontwikkelde en beheerde, standaarden waarvoor breed draagvlak bestaat.[78] Afwijken mag alleen in geval van zwaarwegende redenen; verantwoording hierover moet worden afgelegd in het jaarverslag. In bepaalde gevallen kan echter de inherente afwijkingsmogelijkheid[79] tot onwenselijke situaties leiden en ligt het niet in de rede dat bijvoorbeeld een bestuursorgaan - hoe geldig ook op het individuele niveau – zich kan onttrekken aan toepassing. De 'pas toe of leg uit' lijst richt zich tot de publieke en semi-publieke sector, waaronder bijvoorbeeld onderwijsinstellingen en academische ziekenhuizen (veelal zijn dit RWT's die niet tevens ZBO zijn). Ook richt deze lijst zich op samenwerkingsverbanden, ingesteld bij een gemeenschappelijke regeling, bijvoorbeeld op belastinggebied, die gelet op hun taken en bevoegdheden bestuursorgaan zijn. De ruime werkingssfeer van dit artikel correspondeert hiermee. Zie evenwel de toelichting bij het derde lid.

Lid 2
Dit artikellid maakt het mogelijk om, bij algemene maatregel van bestuur op voordracht van de minister van Binnenlandse Zaken en Koninkrijksrelaties, een standaard dwingend voor te schrijven. Het voorziet in de bevoegdheid om indien dit noodzakelijk en proportioneel is voor de werking, de veiligheid, de betrouwbaarheid of de doelmatigheid van het elektronische verkeer of indien dit voortvloeit uit internationale verplichtingen (waaronder mede begrepen EU-regelgeving), een verplicht toe te passen standaard aan te wijzen. Van noodzakelijkheid is bijvoorbeeld sprake, wanneer er aantoonbaar een veiligheidsprobleem is in de informatie-uitwisseling met natuurlijke personen of rechtspersonen, tussen bestuursorganen of wanneer individuele bestuursorganen niet profiteren van standaardisatie maar de netwerkvoordelen neerslaan bij anderen of bij de samenleving als geheel (maatschappelijke baten). Verplichte toepassing moet proportioneel zijn; dat betekent dat voordien een afweging gemaakt wordt tussen het belang van interoperabiliteit en uitvoeringslasten.
Inherent aan de criteria, noodzakelijkheid en proportionaliteit in relatie tot werking, veiligheid, betrouwbaarheid en doelmatigheid van het elektronisch verkeer, is dat met de bevoegdheid tot aanwijzing terughoudend zal worden omgegaan en dat het niet de verwachting is dat de beschikbare lijst van open standaarden in zijn geheel en/of voor de gehele (semi)publieke sector verplichtend wordt. Ook brengen genoemde criteria mee, dat aanwijzing betrekking zal hebben op

[77] Voor een register met RWT's zie: www.algemenerekenkamer.nl
[78] Via onder meer rijksinstructies, begrotingsvoorschriften en bestuursakkoorden wordt bestuursorganen dringend aanbevolen dan wel hebben zij zichzelf verplicht om de open standaarden van de lijst na te leven. Het betreft standaarden die al breed gedragen of bruikbaar zijn en waarvan het vanzelfsprekend zou moeten zijn deze te gebruiken.
[79] Niet alle standaarden worden breed toegepast, zo blijkt uit de jaarlijkse monitor van het Forum Standaardisatie aan de hand van overlegde jaarverslagen en aanbestedingen.

niet-domeinspecifieke, dus op bovensectorale oftewel generieke standaarden.

Het tweede lid maakt voorts duidelijk dat bij het gebruik van de bevoegdheid om bepaalde standaarden aan te wijzen een zorgvuldig en transparant proces wordt doorlopen. De ingerichte en beproefde procedure voor plaatsing op de 'pas-toe-of-leg-uit' lijst waarborgt brede en representatieve betrokkenheid vanuit diverse geledingen van de overheid, wetenschap en uitvoering.[80] Aanwijzing zal doorgaans betrekking hebben op een standaard die reeds op de bestaande lijst van open standaarden is opgenomen danwel daarvoor is aangemeld; de punten a en b in het tweede lid corresponderen met criteria voor opname op de 'pas-toe-of-leg-uit' lijst. Voor nieuwe standaarden kan de procedure voor plaatsing op de lijst en de aanwijzing parallel lopen.

Lid 3
Bij de aanwijzing van een standaard zal het toepassingsbereik worden omschreven. Hierbij moeten zaken als voor welke (bestuurs)organen, colleges en RWT's de standaard toepasselijk is, in welke gevallen en vanaf welk moment, duidelijk blijken in de algemene maatregel van bestuur. Hierbij kan het toepassingsbereik van de aangewezen standaard beperkter zijn, bijvoorbeeld ten aanzien van het soort berichtenverkeer en geadresseerde organen, dan het toepassingsbereik van dezelfde standaard op de lijst, die een 'pas-toe-of-leg-uit-karakter' heeft. Een standaard kan bijvoorbeeld niet geschikt zijn om door b-bestuursorganen of door RWT's te worden toegepast. Het toepassingsbereik zal dus per geval, dat wil zeggen per aan te wijzen standaard, worden geregeld.

Benadrukt wordt dat de bevoegdheid om bij algemene maatregel van bestuur in bepaalde gevallen standaarden aan te wijzen, de mogelijkheid om in sectorregelgeving voor specifieke doelen standaarden aan te wijzen ongewijzigd laat. Sectorale standaarden mogen niet belemmerend of concurrerend werken in het bovensectorale verkeer; dat zou niet doelmatig zijn. De standaarden op de 'pas-toe-of-leg-uit-lijst' zijn naar hun aard sectoroverstijgend en interfereren niet onnodig met sectorale standaarden. Het open proces van totstandkoming van de lijst, waarbij sprake is van brede consultatie van betrokkenen en experts binnen en buiten de overheid alsmede breed samengestelde overleggremia, biedt hiervoor de waarborgen. Door aanwijzing van een standaard in een algemene maatregel van bestuur wordt vervolgens nogmaals brede interdepartementale afstemming bewerkstelligd in het voortraject.

Op basis van dit artikel zal in ieder geval de standaard inzake toegankelijkheid van overheidswebsites voor mensen met een functiebeperking worden aangewezen. Deze nationale open standaard incorporeert de internationale en in EU-verband ondersteunde Web Content Accessibility Guidelines ('WCAG versie 2.0') en betreft uitwerking van het uitgangspunt dat informatie op overheidswebsites waarneembaar, bedienbaar, begrijpelijk en consistent moet zijn.[81] Ook een aantal veiligheidsstandaarden zal worden aangewezen,[82] alsmede de (koppelvlak)standaarden Digikoppeling.[83] Benadrukt zij, dat het hierbij gaat om reeds bestaande standaarden. Inhoudelijk brengen deze derhalve niets nieuws; bij de toepassing ervan bestaat echter niet langer een inherente afwijkingsmogelijkheid.
Aanwijzing zal geschieden in de vorm van een statische verwijzing naar de desbetreffende standaard(en). Dit betekent dat ook nieuwe/andere standaarden of nieuwe versies van standaarden bij wijzigingsbesluit zullen worden aangewezen.

---

[80] Het Forum Standaardisatie, een door het kabinet ingesteld adviesplatform van (technische) experts vanuit de overheid, wetenschap en bedrijfsleven, adviseert het Nationaal Beraad Digitale Overheid over (door)ontwikkeling van standaarden, de toepassing van open standaarden binnen de overheid, het (her)toetsen van (bovensectorale) open standaarden, het monitoren van de adoptie van open standaarden, de internationale aansluiting binnen Europa en het signaleren van 'witte vlekken'. Op basis van deze pre-advisering adviseert het Nationaal Beraad vervolgens aan de minister. Zie: www.forumstandaardisatie.nl.
[81] ISO/IEC-standaard 40500:2012 en EU/EN-standaard 301 549 V1.1.1 (2014-02). Tevens: EU-richtlijn 2016….
[82] DNSSEC, TLS (ter vervanging van SSL 2.0), DKIM, SPF. Zie het algemeen deel van deze memorie voor een toelichting op de werking van deze standaarden.
[83] https://www.logius.nl/diensten/digikoppeling/

Artikel 3

Lid 1
Deze bepaling geeft aan dat waar in de hoofdstukken 2 tot en met 6 wordt gesproken over bestuursorganen, wordt gedoeld op bestuursorganen als bedoeld in artikel 1:1, eerste lid, onderdeel a, van de Algemene wet bestuursrecht. Bij deze zogeheten a-bestuursorganen gaat het om de organen van rechtspersonen die krachtens publiekrecht zijn ingesteld. Het gaat dan om alle organen van bijvoorbeeld de Staat, provincies, gemeenten en waterschappen. Aldus ziet de bepaling ook op bijvoorbeeld de Dienst Uitvoering Onderwijs (DUO), de Belastingdienst en zelfstandige bestuursorganen (ZBO's) als de Sociale Verzekeringsbank (SVB), de Kamer van Koophandel (KvK), Dienst Wegverkeer (RDW) en de Huurcommissie.[84] Bij de a-bestuursorganen brengen aard en kenmerken van hun taken en werkzaamheden elektronisch verkeer met en elektronische dienstverlening aan natuurlijke personen (burgers) en rechtspersonen (ondernemers) met zich. Daarom vallen deze bestuursorganen zonder meer binnen de werkingssfeer van de hoofdstukken 2 tot en met 6. Dit betekent dat b-bestuursorganen, organen, personen en colleges als bedoeld in artikel 1:1, tweede lid, van de Algemene wet bestuursrecht, alsmede rechtspersonen met een wettelijke taak voorzover deze geen a-bestuursorgaan zijn, niet onder het eerste lid worden begrepen.

Lid 2-4
Naast a-bestuursorganen, vallen onder de reikwijdte van de hoofdstukken 2 tot en met 6 de organisaties behorende tot een in de bijlage bij deze wet aangewezen categorie alsmede de organisaties die bij besluit van de minister in overeenstemming met de minister(s) wie het mede aangaat zijn aangewezen. Het gaat hierbij om (categorieën van) instanties die krachtens wettelijk voorschrift gerechtigd zijn om het burgerservicenummer te gebruiken voor de uitvoering van een specifieke (publieke) taak, zoals dienstverlening door zorgverleners, zorgverzekeraars, indicatieorganen en pensioenuitvoerders[85] of het toekennen van uitkeringen of het uitvoeren van keuringen, en die elektronische diensten verlenen aan natuurlijke personen en rechtspersonen waarvoor, gelet op de aard en kenmerken van deze diensten, veilige en betrouwbare authenticatie noodzakelijk is. Deze organisaties zijn thans veelal toegankelijk via het huidig beschikbare publieke middel (DigiD laag/basis).

Naast de categorieën van organisaties die in de bijlage bij deze wet zijn opgenomen, kunnen individuele organisaties worden aangewezen. Dit geschiedt bij besluit van de minister in overeenstemming met de ministers die het, gezien het desbetreffende beleidsdomein, aangaat. Een dergelijk besluit wordt aangemerkt als een voor bezwaar en beroep vatbare beschikking in de zin van artikel 1: 3, tweede lid van de Awb. Aanwijzing geschiedt al dan niet op verzoek van en in overleg met de betrokken instanties, zodat maatwerk kan worden gerealiseerd. Indien de aangewezen organisatie niet langer BSN-gerechtigd is of de aard en kenmerken van haar elektronische dienstverlening van dien aard is, dat voor de toegang ter zake niet langer hoogbetrouwbare authenticatie nodig is, zal het desbetreffende aanwijzingsbesluit worden ingetrokken.

Met de werkingssfeer, zoals hiervoor geschetst, wordt aangesloten bij Verordening (EU) Nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt. Deze zogenoemde 'eIDAS-verordening' hanteert voor de wederzijdse erkenning van hoogbetrouwbare authenticatiemiddelen het begrip "openbare instantie", hetgeen gedefinieerd is als een staat, regionale of lokale overheden, publiekrechtelijke instellingen en samenwerkingsverbanden bestaand uit één of meer van deze overheidsinstanties of een of meer van deze publiekrechtelijke instellingen, of een private entiteit die door ten minste een van deze autoriteiten, publiekrechtelijke instellingen of verenigingen is gemachtigd tot het verlenen van openbare diensten, wanneer zij in die hoedanigheid optreden (artikel 3, onderdeel 7, eIDAS-verordening).

[84] *https://almanak.zboregister.overheid.nl/*
[85] *Op www.wiekrijgtmijngegevens.nl staat een overzicht van instanties die bsn verstrekt krijgen en op basis van welke publieke taak en/of wettelijke bepalingen.*

Artikel 4

Lid 1

Onderdeel a
Teneinde zorg te kunnen dragen voor veilige en betrouwbare toegang tot elektronische diensten van bestuursorganen en aangewezen organisaties, bevat onderdeel a de verantwoordelijkheid van de minister van BZK voor het bestaan van een publieke authenticatiedienst en, daarmee onlosmakelijk samenhangend, het van overheidswege uitgeven van middelen waarmee natuurlijke personen (burgers en ondernemers die als natuurlijk persoon een onderneming drijven, bijv. eenmanszaak), zich kunnen identificeren ('wie ben je?') en authenticeren ('ben je wie je zegt te zijn?') bij het afnemen van oftewel toegang verkrijgen tot publieke diensten zoals een vergunning of een toeslag. Op dit moment functioneert als publiek middel het van overheidswege uitgegeven DigiD, op betrouwbaarheidsniveau laag. Dit wordt om redenen van betrouwbaarheid en veiligheid doorontwikkeld.

Deze wet heeft betrekking op private en publieke middelen met betrouwbaarheidsniveau substantieel en hoog. Het streven is erop gericht dat op het moment dat dit wetsvoorstel in werking treedt, sprake zal zijn van één of meerdere nieuw(e), hoogbetrouwbare publiek(e) elektronisch middel(en), die erkenning behoeven in de zin van artikel 6 van deze wet. Het gaat daarbij in de eerste plaats om 'DigiD substantieel'.[86] In de tweede plaats worden een e-NIK (elektronische Nederlandse identiteitskaart) en een e-rijbewijs ontwikkeld. Dat zijn publieke middelen met betrouwbaarheidsniveau hoog. Voor het toevoegen van de extra functionaliteit (opname van data in een chip ten behoeve van elektronische authenticatie) op bestaande dragers is de minister primair verantwoordelijk. De verantwoordelijkheid van de minister van Infrastructuur en Milieu voor de uitgifte van het rijbewijs wordt niet uitgebreid tot deze extra functionaliteit. Doordat de authenticatiefunctie op de NIK respectievelijk het rijbewijs wordt aangebracht, treden echter wel afhankelijkheden op met de processen die te maken hebben met de aanvraag, productie, uitreiking en intrekking van deze fysieke documenten. Dit betekent dat in de wet- en regelgeving betreffende de NIK en het rijbewijs nieuwe taken en grondslagen voor gegevensverwerking zullen worden opgenomen die verband houden met het opnemen van de authenticatiefunctie op deze documenten.[87]

De aan erkende authenticatiediensten en door hen uitgegeven erkende middelen te stellen eisen worden bij of krachtens algemene maatregel van bestuur gesteld ingevolge artikel 7. Voor zover het gaat om publieke middelen zal daar in de bovengenoemde wet- en regelgeving bij worden aangesloten. Veilige en betrouwbare authenticatie omvat eveneens de verantwoordelijkheid voor de personalisering van de authenticatiefunctie op de NIK en het rijbewijs. De voorziening die van overheidswege deze personalisering voor haar rekening neemt (anders gezegd: een publiek middel uitgeeft) en daarmee uiteindelijk de elektronische identificatie mogelijk maakt, is een publieke authenticatiedienst. Deze is bereikbaar via het webadres www.digid.nl.

De zorg voor de beschikbaarheid van publieke middelen op een hoger betrouwbaarheidsniveau dan DigiD, betreft elke burger met DigiD die tevens houder is van een paspoort, identiteitskaart of rijbewijs (DigiD substantieel), en elke houder van een voor elektronische authenticatie geschikt document als bedoeld in artikel 2, tweede lid, van de Paspoortwet en artikel 107, eerste lid, van de Wegenverkeerswet 1994 (eNIK en eRijbewijs). Voor wat betreft de hoogbetrouwbare elektronische

---

[86] DigiD substantieel werkt als volgt. Een burger bevestigt eenmalig bij de publieke authenticatiedienst zijn identiteit door met zijn reguliere DigiD in te loggen op de website van DigiD en daar aan te tonen dat hij in bezit is van een geldig Nederlands identiteitsdocument, te weten een paspoort, identiteitskaart of rijbewijs. Dat aantonen doet hij door zijn identiteitsdocument te laten lezen met een kaartlezer. De kaartlezer communiceert hiertoe met de contactloze chip in het reisdocument en stelt via cryptografische processen vast dat de chip authentiek en onveranderd is en toebehoort aan de persoon die inlogt. Tijdens dit proces wordt door de authencatiedienst gecontroleerd of het betreffende identiteitsdocument nog in omloop is. Na deze eenmalige bevestiging van de identiteit werkt DigiD zoals altijd, maar is het 'opgewaardeerd' in die zin, dat de authenticatiedienst het betrouwbaarheidsniveau 'substantieel' afgeeft aan het bestuursorgaan of de aangewezen organisatie waarbij de betreffende burger inlogt.
[87] Vanzelfsprekend mogen de nieuwe data niet interfereren met de informatie die (ingevolge Europese regelgeving) op rijbewijzen moet worden opgenomen.

publieke middelen is vooralsnog dus sprake van een beperktere groep rechthebbenden dan ter zake van het huidige publieke middel DigiD, dat beschikbaar is voor ingezetenen alsmede voor niet-ingezetenen met de Nederlandse nationaliteit. Op termijn wordt gestreefd naar een bredere kring rechthebbenden op een hoogbetrouwbaar publieke middel. Voor de goede orde wordt opgemerkt, dat voor wat betreft private middelen het aan de desbetreffende authenticatiedienst is om de kring van rechthebbenden te bepalen en ter zake gebruiksvoorwaarden te hanteren.

Voor gebruikers van het publieke middel DigiD gelden voorschriften over aanvraag, activatie, zorgvuldig gebruik, blokkeren etc.[88] Voor het gebruik van hoogbetrouwbare publieke middelen zullen eveneens gebruiksvoorschriften worden gesteld (lid 2).

Onderdeel b
Teneinde bij te dragen aan veilige en betrouwbare elektronische authenticatie in het verkeer met bestuursorganen en aangewezen organisaties, draagt de minister tevens zorg voor een publieke machtigingsdienst; deze geeft bij gebruik van een publiek middel ten behoeve van toegang tot elektronische dienstverlening een verklaring af waaruit blijkt dat een natuurlijke persoon of rechtspersoon optreedt namens een andere natuurlijke persoon. Een machtigingsdienst legt vast dat de elektronische bevoegdheid ('wat mag je') is terug te voeren op de wil van de vertegenwoordigde om zich op die wijze te laten vertegenwoordigen. In dit verband functioneert DigiD Machtigen. In DigiD Machtigen kan een machtiging voor een of meerdere elektronische dienst(en) worden geregistreerd als een natuurlijke persoon een ander (natuurlijke persoon of rechtspersoon) wil machtigen om zijn zaken met de overheid elektronisch te regelen. Dit geschiedt op basis van vrijwilligheid; er is sprake van wilsovereenstemming tussen de volmachtgever (een natuurlijk persoon die zich ter behartiging van zijn belangen in het verkeer met publieke dienstverleners laat vertegenwoordigen) en de gemachtigde (een andere natuurlijke persoon of rechtspersoon). Bij de vastlegging in elektronische vorm wordt de strekking van de vertegenwoordigingsbevoegdheid uitgedrukt in termen van de elektronische diensten (wat) die de gemachtigde namens de vertegenwoordigde mag uitvoeren. Hierbij moet bedacht worden, dat registratie geen voorwaarde is voor het ontstaan van een machtiging; het is een hulpmiddel voor een bestuursorgaan of aangewezen organisatie om te bepalen of iemand is gemachtigd, oftewel het vormt een aanwijzing op basis waarvan bestaan, aard en omvang van de machtiging bepaald kan worden. De machtigingsdienst controleert ook niet of aan de registratie daadwerkelijk een rechtsgeldige volmacht ten grondslag ligt, dus bijvoorbeeld of de vertegenwoordigde handelingsbekwaam was op het moment van afgeven van de machtiging en registratie ervan (autorisatie). Het is om redenen van duidelijkheid en rechtszekerheid voor vertegenwoordigde en beoogd gemachtigde wenselijk om voorschriften te stellen over (het proces van) aanvraag, registratie, gebruik, intrekken etc.[89] Hiertoe dient het tweede lid.

De publieke machtigingsdienst zal bij de inwerkingtreding van deze wet tevens een functionaliteit bevatten waarmee een burger als vertegenwoordiger van de wettelijke erfgenamen toegang heeft tot diensten van bestuursorganen en aangewezen organisaties en met behulp waarvan verkeer tussen de nabestaanden en bestuursorganen en aangewezen organisaties kan worden afgewikkeld met betrekking tot zaken die een overledene betreffen. Overwogen wordt voorts de publieke machtigingsdienst verder door te ontwikkelen en uit te breiden met het elektronisch ontsluiten van registers of informatie inzake wettelijke vertegenwoordiging. Bezien zal onder meer worden of en onder welke voorwaarden het mogelijk is de bevoegdheden van bewindvoerders en curatoren met betrekking tot elektronische dienstverlening te verifiëren en inzichtelijk te maken.

De in onderdeel b bedoelde publieke machtigingsdienst moet worden onderscheiden van de mogelijkheid om de vertegenwoordigingsbevoegdheid van de gebruiker van een privaat middel te verifiëren.[90] Dat kan gebeuren in een private machtigingsdienst. Benadrukt wordt, dat zowel private als publieke machtigingsdiensten erkenning door de minister behoeven (artikel 6). De aan machtiging bij publieke en private middelen te stellen eisen (proces, gegevens, betrokkenen, duur etc.) zullen bij of krachtens algemene maatregel van bestuur worden gesteld ingevolge artikel 7.

---

[88] *Regeling voorzieningen GDI, Stcrt. 2015 nr 37158.*
[89] *Deze zijn thans opgenomen in de Regeling voorzieningen GDI, zie vorige voetnoot.*
[90] *https://www.eherkenning.nl/inloggen-met-eherkenning/middel-aanvragen/machtigen*

Onderdeel c
De zorg voor een voorziening die het mogelijk maakt om erkende middelen te gebruiken bij elektronische dienstverlening, is ingegeven door het feit dat naast hoogbetrouwbare publieke middelen ook hoogbetrouwbare private middelen moeten kunnen worden gebruikt jegens bestuursorganen en aangewezen organisaties. Het betreft de situatie waarin een private authenticatiedienst een middel uitgeeft waarmee natuurlijke personen *door tussenkomst van* een publieke voorziening toegang kunnen verkrijgen tot publieke dienstverlening. De generieke, oftewel publieke, voorziening die in dit kader wordt gerealiseerd is het zogeheten BSN-Koppelregister (BSN-K).[91] Via het BSN-K worden private middelen geschikt (gemaakt) voor het afnemen van elektronische diensten bij bestuursorganen en aangewezen organisaties. Het BSN-K speelt een rol bij het activeren van een middel en bij een daadwerkelijke authenticatie van een gebruiker ten behoeve van een specifiek(e) bestuursorgaan of aangewezen organisatie. Tot slot helpt het BSN-K bij het informeren van de gebruiker over zijn middelen met behulp van een inzageregister. Deze functies zijn zodanig ingericht, dat het BSN-K alleen bij de eenmalige activering van een nieuw middel kan herleiden tot een individuele gebruiker en zijn BSN. Bij de functies authenticeren en informeren is dit niet nodig en is herleiding vanuit privacy-overwegingen onmogelijk gemaakt door cryptografische maatregelen. Het BSN-K is tijdens het authenticeren van gebruikers niet direct betrokken, maar stelt uitsluitend cryptografische middelen beschikbaar aan de betrokken partijen. Van belang is, dat de verschillende functies vanuit het oogpunt van veiligheid en privacybescherming technisch van elkaar gescheiden zijn (*privacy by design*). Concreet doet het BSN-K het volgende.

Activering
Ten behoeve van activering verstrekt het BSN-K een zogeheten *polymorf pseudoniem* op basis van het, door de authenticatiedienst aangeleverde, BSN van de gebruiker (= houder van het middel). Dit polymorfe pseudoniem is cryptografisch zodanig versleuteld, dat de authenticatiedienst het kan omzetten naar een specifieke versie (verschijningsvorm) per bestuursorgaan of aangewezen organisatie.

Authenticeren
Bij het authenticeren van een gebruiker kan een authenticatiedienst een versleuteling zelf doen met behulp van cryptografisch middelen die door het BSN-K beschikbaar zijn gesteld. De authenticatiedienst kan er ook voor kiezen versleuteling door het BSN-K te laten uitvoeren. Dit is cryptografisch zodanig ingericht dat het BSN-K daarbij de individuele gebruiker niet kan herkennen. Bij gebruik in het publieke domein kan een bestuursorgaan of aangewezen organisatie hier het BSN uithalen. Daarvoor moet deze dan wel beschikken over een specifieke, door het BSN-K uitgegeven, cryptografische sleutel.

Informeren gebruiker
Het is, vanuit een oogpunt van dienstverlening en veiligheid, van belang dat de gebruiker een overzicht wordt geboden van zijn actieve middelen in het publieke domein. Op deze wijze kan eveneens eventueel misbruik of oneigenlijk gebruik, bijvoorbeeld door een ander dan gebruiker (identiteitsfraude), worden gesignaleerd. Hiertoe wordt verstrekking van een polymorf pseudoniem aan een authenticatiedienst in het BSN-K geregistreerd met behulp van een specifiek inzageregisterpseudoniem (dus niet het BSN) van de natuurlijke persoon. Daarnaast dient een authenticatiedienst elk uitgegeven middel dat actief is voor het publieke domein ook te registreren bij het inzageregister van het BSN-K onder vermelding van ditzelfde specifieke inzageregisterpseudoniem. Benadrukt wordt dat het BSN-K niet registreert welke transacties met welk(e) bestuursorgaan of aangewezen organisatie zijn verricht. Informatie over verrichte elektronische dienstverlening is verkrijgbaar bij de desbetreffende authenticatiedienst. Ingevolge de EU Verordening gegevenbescherming (AGV) is de authenticatiedienst gehouden deze informatie aan de gebruiker te verstrekken.

[91] *Het BSN-K functioneert niet bij authenticatie door rechtspersonen middels e-Herkenning, aangezien dit niet functioneert op basis van het bsn.*

Authenticatie binnen de EU
Ten behoeve van grensoverschrijdend inloggen door de houder van een in Nederland uitgegeven middel verstrekt de authenticatiedienst een versleuteld pseudoniem zonder BSN. Dit wordt in het zogeheten eIDAS knooppunt, waarvoor de minister van Economische Zaken verantwoordelijk is, omgezet in een Europees bruikbare *UniquenessID*. Dit is een persistent pseudoniem, dat als het ware over alle Europese authenticatiediensten heen functioneert en dat via het BSN-K uit het versleuteld pseudoniem wordt verkregen. Publieke dienstverleners in andere EU-lidstaten, die ingevolge Verordening (EU) nr. 910/2014 (eIDAS) verplicht zijn om in Nederland erkende middelen te accepteren, ontvangen derhalve geen BSN.[92] Omgekeerd zijn Nederlandse bestuursorganen en aangewezen organisaties verplicht om in andere EU-lidstaten toegelaten (dwz eIDAS genotificeerde) middelen te accepteren. Dit wordt geëxpliciteerd door de clausule van wederzijdse erkenning in artikel 5, lid 3.

Lid 2
Bij ministeriële regeling worden regels gesteld omtrent het gebruik van een erkend publiek middel en een erkende publieke machtigingsdienst. Dit is nodig om gebruikers en gemachtigden duidelijkheid en rechtszekerheid te bieden omtrent zaken als wijze van aanvraag, activering, gebruik (bijvoorbeeld de niet-overdraagbaarheid van een middel) en beëindigen. Voor private middelen en diensten wordt dit niet door de minister geregeld, maar wordt het aan de desbetreffende private partij overgelaten om gebruiksvoorwaarden aan de afnemer van een middel of dienst te stellen.[93]

Artikel 5

Lid 1-2
Bestuursorganen en aangewezen organisaties (publieke dienstverleners) verlenen slechts toegang tot hun elektronische dienstverlening met betrouwbaarheidsniveau substantieel of hoog, indien sprake is van door erkende authenticatiediensten uitgegeven erkende middelen; ook wanneer gebruik wordt gemaakt van machtigingsdiensten, attributendiensten en ontsluitende diensten, moeten deze erkend zijn. Bestuursorganen en aangewezen organisaties *mogen* dus *alleen* gebruik maken van erkende partijen en middelen. Reden hiervoor is dat de keten veilig en betrouwbaar moet zijn. Daarnaast *moeten* bestuursorganen en aangewezen organisaties alle erkende middelen en machtigingsdiensten *accepteren*. Bij afname van elektronische diensten, waarvoor niveau substantieel of hoog nodig is, hebben gebruikers er dus recht op om met erkende middelen bij de betreffende publieke dienstverleners terecht te kunnen. Op deze wijze wordt uitgesloten dat bestuursorganen en aangewezen organisaties op het niveau substantieel of hoog niet-erkende middelen accepteren. Middelen op een lager betrouwbaarheidsniveau dan substantieel of hoog, zoals het bestaande DigiD, dat wordt uitgefaseerd, zullen niet worden erkend ingevolge artikel 6. Bestuursorganen en aangewezen organisaties mogen deze middelen echter nog enige tijd accepteren voor diensten waarvoor een laag betrouwbaarheidsniveau geldt (zie artikel 23, vierde lid). Zij moeten evenwel met inwerkingtreding van deze wet erkende middelen accepteren. Dit brengt tevens met zich, dat de gebruiker voor alle publieke diensten met een hoogbetrouwbaar middel terecht kan, ook als het bestuursorgaan of de aangewezen organisatie slechts een middel met een lager betrouwbaarheidsniveau vereist. Het is tot op zekere hoogte aan de desbetreffende publieke dienstverlener om te bepalen welk betrouwbaarheidsniveau hij noodzakelijk acht voor een bepaalde door hem aangeboden dienst. Hierop wordt nader ingegaan onder lid 5.

Lid 3
Publieke dienstverleners zijn verplicht om in andere EU-lidstaten toegelaten en onder de eIDAS-Verordening genotificeerde[94] middelen te accepteren. Een beoordelingsprocedure en erkenningsbesluit door de minister als bedoeld in deze wet zijn dan niet nodig en zelfs niet toegestaan. Dit wordt geëxpliciteerd door de clausule van wederzijdse erkenning in het derde lid. Ingevolge de eIDAS-Verordening hebben EU-inwoners het recht om met een in de lidstaat van

[92] Zie hierover uitgebreid de Kamerstukken bij Uitvoeringswet eIDAS-verordening.
[93] Dit laat vanzelfsprekend onverlet dat private partijen de regels gesteld ingevolge artikel 7 moeten naleven.
[94] Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (PbEU 2014, L257).

herkomst toegelaten middel publieke diensten af te nemen in andere lidstaten, op basis van het principe van wederzijds vertrouwen in en daarmee erkenning van elkaars middelen. Elke EU-lidstaat kan zijn nationaal erkende ('toegelaten') middelen bij de Europese Commissie aanmelden (notificatie). Na het doorlopen van de aanmeldingsprocedure, waarin wordt getoetst of de middelen aan de normenkaders voor betrouwbaarheid voldoen, en de publicatie op een lijst door de Europese Commissie, moeten alle (publieke dienstverleners in de) lidstaten die middelen uit de desbetreffende lidstaat accepteren. Naar verwachting zal Nederland de ingevolge deze wet erkende middelen aanmelden. Opgemerkt wordt, dat de normenkaders voor betrouwbaarheid ingevolge de eIDAS-Verordening niet verplicht zijn in die zin, dat een lidstaat er voor kan kiezen deze niet te hanteren en geen middelen aan de Commissie te melden, met als gevolg dat andere lidstaten niet verplicht zijn de in die lidstaat fungerende middelen te accepteren. Om grensoverschrijdende authenticatie mogelijk te maken, wordt een netwerk van eIDAS-knooppunten in de lidstaten gerealiseerd die als overkoepelende (publieke) authenticatiediensten functioneren. De uitvoering van de eIDAS-Verordening wordt toegelicht in de Kamerstukken bij de wetgeving ter zake.[95]

Lid 4
Uit artikel 6 van de Dienstenrichtlijn volgt dat een dienstverrichter de gelegenheid moet hebben om via één loket alle procedures en formaliteiten af te wikkelen die nodig zijn voor de toegang tot zijn dienstenactiviteiten en via dat één loket ook vergunningaanvragen af moet kunnen wikkelen die nodig zijn voor de uitoefening van de dienst. Gelet op de doelstellingen van de Dienstenrichtlijn dient dit eenvoudig, op afstand en elektronisch te kunnen plaatsvinden. Het is niet uitgesloten dat een dienstverrichter als bedoeld in de Dienstenwet middels het in Nederland vormgegeven één loket (hierna: Centraal Loket) procedures wenst af te wikkelen waarvoor het betrouwbaarheidsniveau hoog of substantieel geldt. Uit artikel 5, eerste lid, vloeit voort dat de dienstverrichter dan over een erkend middel dient te beschikken. Niet uitgesloten is dat het voor dienstverrichters uit andere lidstaten die in Nederland hun diensten willen uitoefenen lastig of onmogelijk is om op eenvoudige wijze en op afstand te kunnen beschikken over een erkend middel. Om te verzekeren dat deze dienstverrichters de formaliteiten en vergunningaanvragen via het Centraal Loket te allen tijde in overeenstemming met de Dienstenrichtlijn kunnen afwikkelen, is in het vierde lid een specifieke voorziening getroffen. In geval van elektronische dienstverlening via het centraal loket, waarvoor betrouwbaarheidsniveau substantieel of hoog is vereist, dienen bestuursorganen en aangewezen organisaties tevens toegang te verlenen tot deze elektronische dienstverlening indien de voor deze dienstverlening benodigde elektronische gegevens voorzien zijn van een elektronische handtekening. In het geval van elektronische dienstverlening waarvoor het betrouwbaarheidsniveau substantieel geldt, betreft dit een geavanceerde elektronische handtekening als bedoeld in artikel 3, onderdeel 11 van de Verordening (EG) nr. 910/2014. Als sprake is van elektronische dienstverlening waarvoor het betrouwbaarheidsniveau hoog geldt, een gekwalificeerde elektronische handtekening als bedoeld in artikel 3, onderdeel 12, van de Verordening (EG) nr. 910/2014. Op deze wijze wordt, net als met gebruik van een erkend middel, een zeker betrouwbaarheidsniveau geborgd. Deze handtekeningen zijn bovendien binnen Europa uniform gereguleerd en eenvoudig beschikbaar.

Lid 5
Een bestuursorgaan of aangewezen organisatie bepaalt in beginsel zelf welk betrouwbaarheidsniveau hij passend acht voor welke soort dienstverlening. Bij het bepalen van het betrouwbaarheidsniveau moeten publieke dienstverleners zich evenwel houden aan de bij ministeriële regeling te stellen criteria inzake betrouwbaarheidsniveaus voor authenticatie bij elektronische publieke diensten; er zullen regels worden gesteld op basis waarvan een bestuursorgaan of aangewezen organisatie kan vaststellen voor welke elektronische dienst tenminste het betrouwbaarheidsniveau substantieel of hoog geldt. Doel van deze regeling, die in lijn zal zijn met de eIDAS verordening, is publieke dienstverleners te helpen een eenduidige, efficiënte en bewuste keuze te maken in de betrouwbaarheidsniveaus van hun digitale diensten. In de regeling zullen criteria worden opgenomen ('classificatiemodel') die relevant zijn voor het door de dienstverlener (kunnen) inschalen van het benodigde betrouwbaarheidsniveau zoals aard en

[95] *Wijziging van de Telecommunicatiewet, de Boeken 3 en 6 van het Burgerlijk Wetboek, de Algemene wet bestuursrecht alsmede daarmee samenhangende wijzigingen van andere wetten in verband met de uitvoering van de EU-verordening elektronische identiteiten en vertrouwensdiensten, TK…. Stb. 2016….*

rechtsgevolg van de desbetreffende dienst en wettelijke eisen betreffende ondertekening. Ook zal worden voorgeschreven dat bestuursorganen en aangewezen organisaties het betrouwbaarheidsniveau voor hun diensten (onderbouwd) bekend maken en dat zij in het proces van toegang kenbaar maken wat het betrouwbaarheidsniveau van de betrokken dienstverlening is. Dit schept ook voor gebruikers van authenticatiemiddelen duidelijkheid en rechtszekerheid.

Lid 6
Authenticatie in het elektronische verkeer met commerciële dienstaanbieders (ook wel aangeduid als "het private domein") bijvoorbeeld webwinkels, valt niet onder de werkingssfeer van deze wet.[96] Het gebruik van (al dan niet erkende) private authenticatiemiddelen in dit private domein is dus geen onderwerp van regulering. Het gebruiken van een publiek middel voor commerciële dienstverlening wordt voorts niet toegestaan, teneinde de markt niet te verstoren. Uitgangspunt is dat publieke middelen bedoeld zijn voor de toegang tot de dienstverlening door bestuursorganen en aangewezen organisaties voorzover het de uitoefening van hun publieke taken betreft. Dat betekent bijvoorbeeld dat een gemeente voor de elektronische verkoop van kaartjes voor een concert in het gemeentehuis of bij de elektronische aankoop van een bloemstuk niet om het gebruik van een publiek middel mag verzoeken.

Artikel 6

Lid 1-3
De taken en verantwoordelijkheden van de minister in deze wet zijn gericht op hetgeen nodig is om veilige en betrouwbare toegang tot elektronische diensten van bestuursorganen en aangewezen organisaties mogelijk te maken. Dit betreft (alleen) toegang op betrouwbaarheidsniveau substantieel en hoog. In dit verband besluit de minister in overeenstemming met de Minister van Economische Zaken tot het al dan niet erkennen van middelen die door een authenticatiedienst worden uitgegeven, van authenticatiediensten ten behoeve van een of meer bepaalde middelen, van ontsluitende diensten, van machtigingsdiensten en van attributendiensten. De bevoegdheid van de minister tot erkenning heeft zowel betrekking op publieke als op private middelen en diensten. Het besluit tot erkenning is een besluit in de zin van artikel 1:3 Awb waartegen bezwaar en beroep open staat. Indien een middel is erkend dan moet het betreffende middel geaccepteerd worden door bestuursorganen en aangewezen organisaties bij hun elektronische dienstverlening richting burgers en ondernemers en moet het betreffende middel gebruikt kunnen worden door burgers en ondernemers die elektronische publieke diensten willen afnemen (artikel 5). de minister erkent een middel of een dienst indien dit middel of deze dienst voldoet aan de eisen met betrekking tot de werking, beveiliging en betrouwbaarheid van dat middel of die dienst. Deze eisen worden gesteld bij of krachtens algemene maatregel van bestuur (artikel 7).

Teneinde erkende middelen te mogen leveren, moet een authenticatiedienst bij de minister een aanvraag voor erkenning indienen, waarbij wordt verklaard dat aan de ingevolge artikel 7 gestelde eisen wordt voldaan. Het gaat daarbij om de eisen die gelden voor (a) de authenticatiedienst en (b) het (de) desbetreffende door hem uitgegeven middel(en). Een authenticatiedienst wordt alleen erkend met betrekking tot een door hem aangeboden middel. Dit houdt in dat het niet mogelijk is een authenticatiedienst te erkennen indien deze geen middel aanbiedt. De erkenning van de authenticatiedienst en het door hem uitgebrachte middel vindt tegelijkertijd plaats. Indien echter een reeds erkende authenticatiedienst een nieuw middel wil laten erkennen, is dat mogelijk zonder dat de authenticatiedienst zelf nogmaals hoeft te worden erkend. Tenzij het nieuwe middel van een hoger betrouwbaarheidsniveau is; dit kan betekenen dat de authenticatiedienst in het kader van dat hogere niveau ook opnieuw erkend moet worden.
De minister besluit voorts tot erkenning van ontsluitende diensten. Een partij die een middel ontsluit wordt ook wel "makelaar", "herkenningsmakelaar" of "toegangsdienst" genoemd. 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

[96] *In de praktijk worden er privaatrechtelijk afspraken inzake werking, betrouwbaarheid en veiligheid gehanteerd tussen commerciële dienstaanbieders en leveranciers van private middelen.*

dienstverlening te faciliteren. Hierdoor kan een bestuursorgaan of aangewezen organisatie eenvoudiger aan zijn acceptatieplicht (artikel 5) voldoen.
Ook een machtigingsdienst, zijnde een partij die een verklaring afgeeft waaruit blijkt dat een natuurlijke persoon of rechtspersoon optreedt namens een andere natuurlijke persoon of rechtspersoon (zie tevens de toelichting bij artikel 4, eerste lid, onderdeel b) is aan een erkenning onderworpen. Dit geldt tot slot voor een attributendienst, zijnde een partij die ten behoeve van een bestuursorgaan of aangewezen organisatie een verklaring omtrent kenmerken en gegevens van een natuurlijke persoon verstrekt. Aan de hand van deze attributen kunnen vervolgens bevoegdheden van een gebruiker worden vastgesteld. Een voorbeeld is dat op grond van het verstrekte attribuut dat een gebruiker ouder is dan 18 jaar, de bevoegdheid van deze gebruiker kan worden vastgesteld voor het afnemen van een dienst bij een bestuursorgaan of aangewezen organisatie waaraan leeftijdsgrenzen zijn gesteld. Een ander voorbeeld is het verschaffen van een attribuut waaruit blijkt dat de gebruiker geregistreerd is in een bepaald beroepsregister.

Authenticatiemiddelen op betrouwbaarheidsniveau substantieel en hoog, en de partijen die een rol spelen bij het goed functioneren daarvan, worden slechts erkend indien ze voldoen aan de ter zake geldende eisen. Aldus wordt een keten van erkende partijen en middelen gerealiseerd waarbinnen men op elkaar kan vertrouwen. Het stellen van eisen aan betrokken partijen en middelen, hetgeen geschiedt ingevolge artikel 7, is tevens essentieel bij het effectief kunnen houden van toezicht, bedoeld in hoofdstuk 4. Benadrukt wordt, dat uitbesteding van werkzaamheden in de authenticatieketen op zichzelf is toegestaan, mits de naleving van de normen en het toezicht daarop gewaarborgd blijven. De erkenning (sprocedure) beslaat alle relevante processen, werkzaamheden etc.; uitbesteding aan een onderaannemer of opdrachtnemer ontheft de houder van de erkenning niet van zijn verplichtingen, verantwoordelijkheden en aansprakelijkheid.

Lid 4
De minister besluit over de aanvraag tot erkenning van een dienst of een middel in overleg met de minister van Economische Zaken. Naar verwachting zal de minister bij de uitvoering ondersteund worden door Agentschap Telecom: onderdeel van het ministerie van Economische Zaken en onder meer belast met het toezicht op de uitvoering van een aantal wetten. Het agentschap heeft technisch-inhoudelijke expertise op het terrein van toezicht in het elektronisch communicatiedomein. Om deze reden zal ook het toezicht op de naleving van de ingevolge artikel 7 gestelde eisen mogelijk door het Agentschap Telecom kunnen worden uitgeoefend (zie artikel 10).

Het oordeel van de minister over een aanvraag tot erkenning is mede gebaseerd op een conformiteitsverklaring van een geaccrediteerde certificerende instelling. Een dergelijke instelling toetst in opdracht van een authenticatiedienst, ontsluitende dienst, machtigingsdienst of attribuutdienst of de betreffende dienst dan wel het betreffende middel voldoet aan de eisen die op grond van artikel 7 zijn gesteld. Indien dat het geval is, dan wordt een conformiteitsverklaring in de vorm van een certificaat of rapport afgegeven.
Een dienst die een aanvraag voor erkenning doet, legt de conformiteitsverklaring voor aan de toezichthouder. De aanwezigheid van een conformiteitverklaring levert het bewijsvermoeden op dat aan de gestelde eisen wordt voldaan.[97] De toezichthouder beoordeelt vervolgens de aanvraag en adviseert de minister bij zijn besluitvorming omtrent erkenning. Een conformiteitsverklaring heeft de meeste waarde als de toetsende instelling deskundig, onafhankelijk en objectief is. Om deze reden is bepaald dat een certificerende instelling geaccrediteerd moet zijn bij de Raad voor Accreditatie.[98] De Raad voor Accreditatie controleert vooraf of de desbetreffende instelling competent is. Bij een goed resultaat wordt deze instelling geaccrediteerd.[99]

Lid 5
De minister kan in afwijking van het eerste tot en met het derde lid, een dienst of middel niet erkennen indien zwaarwegende redenen zich tegen erkenning verzetten. Op grond van

[97] Kabinetsstandpunt over conformiteitsbeoordeling en accreditatie, brief van 19 september 2016, TK nnb.
[98] In 2010 is de RvA aangewezen als nationale accreditatie-instantie, op basis van EU- Verordening 765/2008. Sindsdien is de RvA een zelfstandig bestuursorgaan, dat verantwoording aflegt aan de minister van Economische Zaken.
[99] Zie de lijst van door de Raad voor Accreditatie geaccrediteerde instanties op https://www.rva.nl/

zwaarwegende redenen kan de minister, ondanks een positieve conformiteitsbeoordeling en een positief advies van de toezichthouder, derhalve besluiten niet tot erkenning over te gaan. De reden hiervoor is dat de conformiteitsbeoordeling en het advies van de toezichthouder betrekking hebben op de vraag of aan de eisen is voldaan die bij of krachtens artikel 7 zijn gesteld, terwijl de minister ook andere overwegingen een rol kan laten spelen, zoals cybersecurity of staatsveiligheid. Dit zijn belangen van een andere orde dan de meer technische beoordeling van de eisen, bedoeld in artikel 7.

Lid 6
Bij de uitoefening van zijn taak, dat wil zeggen de beoordeling of een erkenning afgegeven kan worden, heeft de minister een zekere beleidsvrijheid. De minister kan een middel of een authenticatiedienst, ontsluitende dienst, machtigingsdienst of attribuutdienst erkennen, ook al voldoet deze niet volledig aan de gestelde eisen. Voorwaarde is dan wel dat binnen een door de minister te stellen termijn wordt aangetoond dat aan de gestelde eisen wordt voldaan. Indien dat het geval is, dan loopt de erkenning automatisch door. Indien dit niet het geval is, dan kan de toezichthouder als bedoeld in artikel 10, optreden wegens het niet naleven van de voorwaarde. Vanzelfsprekend zal afwijking van de eisen geen betrekking mogen hebben op cruciale onderdelen van deze eisen, maar slechts op ondergeschikte onderdelen die geen belemmering vormen voor de werking, beveiliging en betrouwbaarheid. Gelet op de bewoordingen van dit lid, dat onverkorte toepassing van de eisen tot een onaanvaardbaar resultaat zou leiden, zal de minister slechts terughoudend gebruik maken van deze bevoegdheid.

Lid 7
Het is noodzakelijk dat de minister beschikt over de bevoegdheid om aan het besluit tot erkenning van een middel of een dienst voorschriften en beperkingen te stellen. Het is immers denkbaar dat een erkenning zonder dergelijke voorschriften of beperkingen niet in alle gevallen voldoet.

Lid 8
Het is van belang dat geïnteresseerde of belanghebbende partijen op de hoogte zijn van de eisen met betrekking tot een erkenning. Op deze wijze zijn zij in staat om hun dienstverlening af te stemmen op de gestelde inhoudelijk eisen op het gebied van onder meer betrouwbaarheidsniveaus, informatiebeveiliging en privacy, en wordt helderheid geboden omtrent administratieve en procedurele vereisten. In een ministeriële regeling wordt de procedure voor het verkrijgen van een erkenning nader uitgewerkt. Deze ministeriële regeling schrijft onder meer voor wat de formaliteiten zijn, welke documenten moeten worden overlegd en welke termijnen er gelden voor de aanvraag.

Lid 9
In artikel 5 is vastgelegd dat bestuursorganen en aangewezen organisaties alleen toegang tot hun elektronische dienstverlening met betrouwbaarheidsniveau substantieel of hoog bieden indien de betrokken diensten en middelen zijn erkend. Zij mogen dus alleen gebruik maken van erkende partijen en middelen. Daarnaast moeten ze alle erkende middelen accepteren; gebruikers hebben er recht op om met erkende middelen bij de betreffende publieke dienstverleners terecht te kunnen. Het is daarom van belang dat breed bekend is gemaakt welke diensten en middelen zijn erkend. Publicatie van de erkende diensten en middelen in de Staatscourant maakt dit mogelijk. Om de lijst van erkende middelen en diensten actueel te houden, is de minister gehouden deze lijst aan te passen indien daartoe een reden is. Daarvan is sprake indien een nieuwe dienst of een nieuw middel wordt erkend, maar ook als de minister op grond van artikel 13 een erkende dienst of een erkend middel schorst of een erkenning intrekt.

Artikel 7

Lid 1
Ingevolge dit artikel worden eisen gesteld aan werking, beveiliging en betrouwbaarheid in de authenticatieketen. Deze eisen hebben betrekking op authenticatiediensten, ontsluitende diensten, machtigingsdiensten en attributendiensten. Benadrukt wordt dat, in het kader van een evenwichtige multi-middelen strategie, dezelfde eisen worden gesteld aan zowel de publieke als de private diensten. Aangezien er sprake is van ketens, is het vanuit een oogpunt van veilige en

betrouwbare elektronische authenticatie bij elektronische dienstverlening door bestuursorganen en aangewezen organisaties nodig om eisen te stellen aan de partijen die betrokken zijn bij het goed functioneren van de authenticatieketen. Deze eisen worden bij of krachtens algemene maatregel van bestuur gesteld.

In de eerste plaats richten deze eisen zich op diensten die private of publieke middelen uitgeven: authenticatiediensten die, als ze erkende middelen willen leveren, aan eisen zijn onderworpen. Voorts betreft het zogeheten ontsluitende diensten: in opdracht van (dus: via privaatrechtelijke contracten met) bestuursorganen en aangewezen organisaties werkende private partijen die zorgen voor het ontsluiten van erkende middelen, zodat de desbetreffende publieke dienstverlener wordt gefaciliteerd bij het voldoen aan de op hem rustende acceptatieplicht (artikel 5). Bij het in dit verband stellen van (technische) eisen zijn interoperabiliteit en de multi-middelenaanpak het uitgangspunt. Ook partijen die machtigingsdiensten of attributendiensten aanbieden, zijn aan regels onderworpen. Indien de minister van oordeel is dat voldaan wordt aan de gestelde voorschriften, geeft hij een erkenning af (artikel 6). Agentschap Telecom houdt ingevolge hoofdstuk 4 toezicht op de voortdurende naleving van deze eisen gedurende de periode dat een dienst of een middel wordt erkend.

Bij werking, beveiliging en betrouwbaarheid in de authenticatieketen gaat het om maatregelen om de betrouwbaarheid van processen, de ondersteunende informatiesystemen en de daarin opgeslagen gegevens te beschermen tegen al dan niet opzettelijke incidenten. Dit artikel bevat daarom de basis voor het stellen van strategische, tactische, operationele, organisatorische en technische eisen om processen en ketens zodanig in te richten dat de goede werking, veiligheid en betrouwbaarheid van authenticatie is gewaarborgd, daarover verantwoording kan worden afgelegd door partijen en hierop toezicht kan worden gehouden. De volgende met elkaar onlosmakelijk verbonden elementen zullen in dat verband worden gereguleerd:
Werking: maatregelen teneinde de beschikbaarheid en het gebruik van authenticatiemiddelen te kunnen realiseren. Hierbij gaat het onder meer om het aanvraag- en uitgifteproces, interoperabiliteit en samenwerking tussen de verschillende partijen in de keten.
Beveiliging: dit ziet onder andere op het beschermen van informatie tegen kennisname en mutatie door onbevoegden, door maatregelen inzake dataminimalisatie, versleuteling en encryptie, door normen en standaarden inzake toegang tot gebouwen, ruimten en systemen, alsmede het voorkomen en herstellen van inbreuken op en aantasting van de (technische) beveiliging en processen.
Betrouwbaarheid: hieronder wordt begrepen het waarborgen van de correctheid, volledigheid en tijdigheid van de gerealiseerde authenticatie en de controleerbaarheid daarvan. Daarnaast betreft het voorschriften omtrent de betrouwbaarheidsniveaus van de middelen en de integriteit van betrokken partijen.

Lid 2
Dit lid expliciteert dat middelen en de publieke voorziening moeten (blijven) voldoen aan de ter zake te stellen regels over de werking, beveiliging en betrouwbaarheid. Op deze voorschriften is toezicht en handhaving (zie hierna artikel 10 en volgende) gericht. De regels die worden gesteld aan de publieke middelen wijken niet af van de regels voor private middelen. Voor beide is het immers van belang dat zij voldoende waarborgen bieden voor een veilig en betrouwbaar gebruik. Dat doen zij indien zij aan de eisen inzake werking, beveiliging en betrouwbaarheid voldoen. Aldus wordt mede een *level playing field* bewerkstelligd. De eisen zullen betrekking hebben op middelen op de betrouwbaarheidsniveaus substantieel en hoog en betreffen de processen rond uitgifte en beëindiging, (technische en semantische) interoperabiliteit, beheer, techniek, functionaliteit, gebruiksgemak en privacybescherming. Hoewel deze eisen zich niet richten op de gebruikers van een middel - voor hen gelden immers gebruiksvoorschriften ingevolge artikel 4, tweede lid (publiek middel) of ingevolge de overeenkomst met de betreffende authenticatiedienst (privaat middel) -, zijn ze voor hen wel van belang, zoals bijvoorbeeld regels met betrekking tot het blokkeren en beëindigen van een individueel middel door een authenticatiedienst.

Doordat de eisen gelijkluidend zijn voor publieke en private middelen wordt een zoveel mogelijk uniform stelsel gerealiseerd en wordt recht gedaan aan de door het kabinet voorgestane

multimiddelen-aanpak.[100] De betekenis daarvan is tweeledig. In de eerste plaats kan de gebruiker van een middel dit jegens bestuursorganen en aangewezen organisaties gebruiken, ongeacht of sprake is van een publiek of privaat middel; de onderhavige wet creëert hiertoe het recht (aanspraak). In de tweede plaats moeten bestuursorganen en aangewezen organisaties naast publieke middelen ook private middelen accepteren (zie artikel 5). Vanzelfsprekend geldt hierbij als voorwaarde dat ze door de minister erkend zijn.

Ook ter zake van de publieke, dat wil zeggen door de minister beheerde, voorziening die het mogelijk maakt erkende middelen te gebruiken bij de toegang tot elektronische dienstverlening door bestuursorganen en aangewezen organisaties, thans het BSN-Koppelregister (zie de toelichting bij artikel 4, eerste lid, onder c), zullen nadere regels op het gebied van informatieveiligheid en systeemintegriteit worden gesteld bij of krachtens algemene maatregel van bestuur. Deze vervangen de voorschriften ter zake in de Regeling voorzieningen GDI.[101]

Lid 3 - 4
Bestuursorganen en aangewezen organisaties moeten er op kunnen vertrouwen dat zij zaken doen met veilige en betrouwbare partijen. Daarom is het voor een ontsluitende dienst, teneinde een erkenning ingevolge artikel 6 te kunnen verkrijgen, noodzakelijk dat hij alleen erkende middelen van erkende authenticatiediensten ontsluit.

Bestuursorganen en aangewezen organisaties kunnen worden gefaciliteerd ('ontzorgd') bij het voldoen aan hun acceptatieplicht ter zake van erkende middelen, wanneer zij hiertoe een erkende ontsluitende dienst inschakelen. Het is vooralsnog niet de verwachting dat ontsluitende diensten ieder erkend middel van iedere erkende authenticatiedienst zullen ontsluiten. Een verplichting hiertoe voor de ontsluitende diensten wordt voorshands ook niet voorzien, omdat dit voor hen technisch en organisatorisch complex zou zijn. De mogelijkheid bestaat dus, dat een ontsluitende dienst slechts een of een aantal middelen ontsluit. In theorie bestaat zelfs de mogelijkheid dat een ontsluitende dienst als enige een bepaald erkend middel aanbiedt en in dat verband een machtspositie heeft.
Vanwege de op hen rustende acceptatieplicht volgt uit het voorgaande, dat bestuursorganen en aangewezen organisaties genoodzaakt kunnen zijn met meer ontsluitende diensten een contract aan te gaan; zij moeten er immers voor zorgen dat hun elektronische dienstverlening toegankelijk is via alle erkende middelen (artikel 5). Indien zij verschillende ontsluitende diensten contracteren, worden bestuursorganen en aangewezen organisaties mogelijk geconfronteerd met verschillende koppelvlakken. Het is namelijk waarschijnlijk dat niet alle ontsluitende diensten hetzelfde koppelvlak gebruiken. Dit brengt dan met zich, dat bestuursorganen en aangewezen organisaties zelf meer technische voorzieningen in hun systemen moeten treffen om de verschillende koppelvlakken te faciliteren. Dit kan ertoe leiden, dat zij een technische bewerker inschakelen die er in opdracht en onder de verantwoordelijkheid van een bestuursorgaan of aangewezen organisatie voor zorgt, dat de koppelvlakken die door de verschillende ontsluitende diensten worden aangeboden, gebruikt kunnen worden door het bestuursorgaan of de aangewezen organisatie.

Niettemin wordt benadrukt dat bij het stellen van eisen aan werking, beveiliging en betrouwbaarheid in de authenticatieketen, vanuit een oogpunt van interoperabiliteit, facilitering van bestuursorganen, aangewezen organisaties én gebruikers (burgers en bedrijven) gestreefd zal worden naar stapsgewijze harmonisering en stroomlijning van technische eisen (groeimodel). Er wordt, mede op basis van opgedane ervaringen en ontwikkelingen in de praktijk, naar gestreefd in de eisen, gesteld ingevolge het eerste lid, zoveel mogelijk toe te werken naar het gebruik van standaardwijzen van ontsluiten door bepaalde diensten. Het vierde lid specificeert deze intentie, door te expliciteren dat nadere regels kunnen worden gesteld over de wijze van ontsluiten. Denkbaar is bijvoorbeeld dat in de toekomst ontsluitende diensten worden verplicht voor iedere

[100] De regels zullen in belangrijke mate zijn gebaseerd op en behelzen daarmee de nationale uitwerking en inkleuring van de eIDAS-verordening en vooral de eIDAS uitvoeringsverordening 2015/1502. Hierin worden de minimale technische specificaties en procedures voor het uitgeven van authenticatiemiddelen op de betrouwbaarheidsniveau's substantieel en hoog geregeld. De uitvoeringsregels zijn tevens geïnspireerd op de authenticatieregels die voor banken worden gehanteerd (IDIN).
[101] Stcrt. 2015 nr 37158.

wijze van ontsluiten (ieder koppelvlak) alle erkende middelen die via die wijze van ontsluiten kunnen worden ontsloten (via dat koppelvlak lopen) ook daadwerkelijk ontsluit , en dat authenticatiediensten hieraan hun medewerking moeten verlenen.
De mogelijkheid om deze materie bij of krachtens algemene maatregel van bestuur te regelen is ingegeven door de wenselijkheid om ruimte voor beheersstappen te bieden, onbekendheid met het gedrag van de (private) partijen en de noodzaak tot het inspelen op ontwikkelingen.

Lid 5 - 6
Aan authenticatiediensten, ontsluitende diensten, machtigingsdiensten en attributendiensten alsmede de minister als verantwoordelijke voor - en beheerder van - de voorziening BSN-Koppelregister, wordt de verplichting opgelegd om incidenten te melden aan de toezichthouder, te weten Agentschap Telecom. Deze meldplicht sluit aan bij artikel 19, tweede lid, van verordening (EU) nr. 910/2014 (eIDAS) en houdt in dat de veiligheidsinbreuken en integriteitsverliezen zonder onnodige vertraging maar in ieder geval binnen 24 uur moeten worden gemeld aan Agentschap Telecom. Indien de veiligheidsinbreuk of het integriteitsverlies negatieve gevolgen zal hebben voor een natuurlijke persoon of een rechtspersoon aan wie de betrokken dienst is aangeboden, stelt de betreffende melder, dat wil zeggen de betrokken dienst of de minister, bovendien de natuurlijke persoon of de rechtspersoon in kennis van de veiligheidsinbreuk of het integriteitsverlies. Omdat het voorgaande inhoudelijk en procesmatig nauw aansluit bij hetgeen ingevolge de eIDAS-verordening geldt voor verleners van vertrouwensdiensten[102], is de administratieve lastendruk voor de diensten in de zin van deze wet, die veelal ook vertrouwensdiensten in de zin van de eIDAS-verordening leveren, beperkt. Ook is het, teneinde dubbele melding door de betrokken diensten te voorkomen, Agentschap Telecom dat gegevens en inlichtingen over de gedane meldingen 'doormeldt', in het kader van de informatieverstrekking aan de minister (artikel 16, tweede lid).
Overigens moet bedacht worden, dat niet te snel mag worden aangenomen dat melding achterwege kan blijven. Dat wil zeggen dat ook sprake is van aanzienlijke gevolgen indien een veiligheidsinbreuk of integriteitsverlies aanzienlijke gevolgen *kan* hebben voor de veilige en betrouwbare toegang tot elektronische dienstverlening, ongeacht of het zeker is dat die zullen intreden. Slechts indien vaststaat dat sprake is van beperkte impact kan melding achterwege blijven.
Voor de goede orde wordt opgemerkt, dat melding in de zin van dit artikel onderscheiden moet worden van de meldplicht datalekken, zoals deze geldt jegens de Autoriteit Persoonsgegevens.[103]

Lid 7
De meldplicht zoals geregeld in dit artikel is niet van toepassing op verleners van vertrouwensdiensten die de betrokken veiligheidsinbreuk of het integriteitsverlies al op grond van de EU Verordening 910/2014 moeten melden. Vanzelfsprekend moeten zij dergelijke inbreuken wel melden, maar dan op basis van de genoemde verordening.

Artikel 8

Lid 1
Artikel 8 biedt de grondslag voor vaststelling van regels over de werking, betrouwbaarheid en beveiliging van de toegang tot elektronische diensten door bestuursorganen en aangewezen organisaties. Zonder dit artikel zou het niet mogelijk zijn dergelijke regels aan hen op te leggen. Bestuursorganen en aangewezen organisaties vormen een belangrijke schakel in de authenticatieketen. Het zijn immers hun elektronische diensten die door natuurlijke personen en rechtspersonen worden afgenomen. Burgers en ondernemers moeten zich daarvoor bij de bestuursorganen en aangewezen organisaties authenticeren met erkende middelen. Indien de ICT-systemen van de bestuursorganen en aangewezen organisaties de werking, betrouwbaarheid en beveiliging van de toegang tot hun eigen elektronische diensten onvoldoende zouden beschermen, zou daarmee een risico voor de gehele keten ontstaan. Om deze reden is het noodzakelijk aan bestuursorganen en aangewezen organisaties de benodigde regels te stellen. Gelet op de aard en

[102] *Uitvoeringswet in verband met de eIDAS verordening, Stb. 2016 nr… TK 2015/2016, 34 413. Hierin wordt de minister van Economische Zaken aangewezen als degene tot wie de melding zich richt; het Agentschap Telecom is hiermede belast. Ook is de Telecommunicatiewet aangevuld met een bepaling inzake bij de melding te verstrekken gegevens (artikel 18.15a).*
[103] *Artikel 34a, eerste lid, Wet bescherming persoonsgegevens.*

de werkzaamheden van bestuursorganen en aangewezen organisaties, zullen de te stellen regels een algemeen karakter hebben. Ook zullen de regels aansluiten bij hetgeen reeds voor hen gebruikelijk is. Wat betreft de aangewezen organisaties laten de te stellen regels de eventuele regels op grond van sectorspecifieke voorschriften onverlet.

In de praktijk hanteren bestuursorganen thans reeds diverse documenten over beveiliging van ICT-voorzieningen van de overheid. Het betreft de zogeheten *baselines* informatiebeveiliging[104] en normen (primair: NEN-ISO/IEC 27001/27002) en standaarden van de 'pas-toe-of-leg-uit-lijst' van het Forum Standaardisatie. Hieraan hebben alle overheden zich via zelfregulering (programma's NUP en iNUP) verbonden. Ook aangewezen organisaties hanteren reeds (eigen) normenkaders informatieveiligheid. Genoemde documenten en kaders vormen de basis voor de ingevolge dit artikellid te stellen eisen aan bestuursorganen en aangewezen organisaties met betrekking tot de toegang tot hun elektronische dienstverlening. Bij het opstellen van deze eisen zal tevens worden bezien welke relevante en toepasselijke (elementen van) standaarden, zoals DNSSEC, TLS, SAML, SPF, DKIM en DMARC, zullen worden opgenomen. Verder kan gedacht worden aan specificaties en beschrijvingen zoals het maken en naleven van veiligheidsplannen, het nemen van maatregelen op basis van een risicoanalyse en risicowaardering van de geïdentificeerde risico's (risicomanagement), het doen uitvoeren van audits, koppelvlakspecificaties, functionele (ontwerp)normen, technische procesbeschrijvingen en testbepalingen. Ingevolge deze bepaling dienen bestuursorganen en aangewezen organisaties aan die regels te voldoen. Het is aan deze publieke dienstverleners zelf om er zorg voor te dragen dat hun systemen daadwerkelijk aan de gestelde eisen voldoen.

Lid 2
Om onafhankelijk te laten toetsen of de publieke dienstverleners daadwerkelijk voldoen aan de eisen die op grond van het eerste lid zijn gesteld, voorziet het tweede lid in een verplichting voor bestuursorganen en aangewezen organisaties om jaarlijks een verklaring van een onafhankelijke auditor over te leggen aan de minister. Onder onafhankelijk auditor wordt verstaan een externe auditor die niet in dienstverband werkzaam is bij of anderszins verbonden aan het betreffende bestuursorgaan of de betreffende aangewezen organisatie. De verklaring van de onafhankelijke auditor sluit aan bij de systematiek die thans gehanteerd wordt bij DigiD en die sinds 2011 functioneert. Op grond van de DigiD-aansluitvoorwaarden dienen alle afnemers jaarlijks een audit te laten uitvoeren en de auditverklaring aan de minister te doen toekomen. Indien uit de verklaring volgt dat er niet aan alle eisen wordt voldaan, dan wordt contact opgenomen met de betrokken dienstverlener. Gezamenlijk wordt dan bezien welke verbeteringen nodig zijn en worden daarover afspraken gemaakt. de minister zal op soortgelijke wijze optreden indien uit de jaarlijkse rapporten van de auditor blijkt dat een bepaald bestuursorgaan of een aangewezen organisatie niet aan de gestelde regels voldoet. De minister zal in een dergelijk geval contact opnemen met de betreffende publieke dienstverlener en in gezamenlijk overleg afspreken welke maatregelen nodig zijn en op welke termijn die genomen worden. Indien uit de auditverklaringen zou blijken dat de informatieveiligheid in het geding is en ook na herhaaldelijke aanmaningen de benodigde en noodzakelijke verbeteringen niet worden aangebracht, kan als uiterste middel de in artikel 15 opgenomen bijzondere bevoegdheid voor de minister om een noodmaatregel te treffen, uitkomst bieden.

De over te leggen auditverklaringen bieden, naast een handvat voor gesprek en verdere afspraken, ook inzicht in de wijze waarop de bestuursorganen en aangewezen organisaties voldoen aan de krachtens deze bepaling gestelde regels. Dit biedt inzicht in de naleving daarvan en de stand van zaken omtrent informatieveiligheid bij de toegang tot elektronische dienstverlening. Bij de evaluatie van de wet (zie artikel 22) kan op basis van die ontvangen verklaringen het functioneren van de wet in relatie tot de gewenste informatiebeveiliging bij authenticatie worden onderzocht en kunnen waar nodig voorstellen worden gedaan voor aanpassing van het systeem van auditverklaringen. Indien nodig kunnen dan ook stringente handhavingsinstrumenten worden overwogen. Het wetsvoorstel voorziet niet in een formeel handhavingsinstrument met betrekking

[104] Zo geldt voor de Rijksoverheid de Baseline Informatiebeveiliging Rijksoverheid (BIR), voor de gemeenten de (op de BIR gebaseerde) Baseline Informatiebeveiliging Nederlandse Gemeenten (BIG) en voor waterschappen de Baseline Informatieveiligheid Waterschappen (BIWA).

tot de krachtens dit artikel gestelde regels. Het toezicht dat Agentschap Telecom krachtens artikel 10 uitoefent, heeft geen betrekking op bestuursorganen en aangewezen organisaties. Dit houdt mede verband met het uitgangspunt dat de betrokken publieke dienstverleners een eigenstandige verantwoordelijkheid hebben voor informatiebeveiliging. Dit sluit ook aan bij het kader van generiek interbestuurlijk toezicht, dat uitgaat van het vertrouwen dat betrokken overheden de wettelijke voorschriften naleven. Het ligt in de rede dat de jaarlijkse rapporten van de auditors onderwerp zullen zijn van democratische controle door bijvoorbeeld de gemeenteraad. Ook ten aanzien van de aangewezen organisaties wordt van dit vertrouwen uitgegaan. Ten aanzien van die aangewezen organisaties ligt het voorts voor de hand dat, in geval er verbeteringen in de informatiebeveiliging nodig blijken te zijn, het vakdepartement dat op het betrokken domein bevoegd is, al dan niet via de eigen inspectiediensten of toezichthouders (zie artikel 14), actie onderneemt en de betrokken organisatie aanspreekt.

De voorgeschreven audit beslaat alle regels die ingevolge het eerste lid vastgesteld worden. Echter: omdat deze regels voor bestuursorganen en aangewezen organisaties inhoudelijk niet nieuw zullen zijn en het moeten overleggen van een auditverklaring ook niet (dat geschiedt namelijk veelal reeds ingevolge de voor hen geldende veiligheidsvoorschriften, *baselines*, ISO-normen etc.), is de lastendruk voor de bestuursorganen en aangewezen organisaties naar verwachting beperkt. Verantwoording afleggen over het naleven van de veiligheidseisen, het gehanteerde risicomanagement en de naleving van aanbevelingen en opvolging van opmerkingen van de controlerende accountant gebeurt nu feitelijk veelal (ingevolge DigiD assessments of andere uitgevoerde audits) in de *planning en control cyclus* van bestuursorganen en aangewezen organisaties. Hierbij kan door bestuursorganen en aangewezen organisaties worden aangesloten in die zin, dat relevante informatie kan worden hergebruikt, bijvoorbeeld door het jaarverslag van een gemeente niet alleen aan de gemeenteraad toe te sturen, maar ook te gebruiken ter informering van de minister.[105]

Artikel 9

Lid 1-2
Dit artikel verankert de wettelijke grondslag voor specifiek genoemde bij authenticatie betrokken erkende private diensten om persoonsgegevens, waaronder het BSN, te verwerken voor zover dit noodzakelijk is voor de goede vervulling van hun respectievelijke taken (doelbinding).

Het eerste lid betreft erkende private authenticatiediensten en erkende private machtigingsdiensten. Zij oefenen, ongeacht of zij een privaat of een publiek middel uitgeven, taken uit die verband houden met de verantwoordelijkheid van de minister voor het functioneren van de voorziening bedoeld in artikel 4, eerste lid, onderdeel c. De goede werking van deze voorziening is namelijk afhankelijk van de aanlevering van bepaalde persoonsgegevens over de gebruiker van een middel, die dit wil gebruiken voor de afname van diensten in het publieke domein (zie de functiebeschrijving van deze voorziening, het BSN-K, in de toelichting bij artikel 4, eerste lid, onderdeel c).
De aanlevering van de benodigde persoonsgegevens is belegd bij de authenticatiedienst. Reden hiervoor is dat de *core business* van authenticatiediensten het authenticeren van gebruikers is. Aangezien zij uit dien hoofde beschikken over persoonsgegevens en het functioneren van de voorziening als bedoeld in artikel 4 onderdeel c, daarmee onlosmakelijk verbonden is, is ervoor gekozen hen een taak toe te delen in het kader van deze wet. Voor de vervulling van deze taak verwerken authenticatiediensten persoonsgegevens waaronder het BSN; deze worden aangeleverd aan onze Minister als beheerder van de voorziening BSN-K. Om de verkregen gegevens te controleren op juistheid, vraagt hij gegevens op uit de basisregistratie personen (BRP): verificatie geschiedt door de opgegeven gegevens van de aanvrager (aspirant gebruiker) te controleren aan de hand van de in de BRP opgenomen gegevens. De authenticatiedienst controleert deze gegevens aan de hand van het overlegde identificatiemiddel en bewaart geen integrale kopie, maar een

[105] *Het is wenselijk om het aantal auditverplichtingen zo beperkt mogelijk te houden en deze zoveel mogelijk te stroomlijnen, teneinde een effectievere en efficiëntere verantwoordingssystematiek ter zake van informatieveiligheid te realiseren. Hiertoe dient onder meer het project ENSIA van de VNG, gemeenten, de ministeries van Binnenlandse Zaken en Koninkrijksrelaties, Sociale Zaken & Werkgelegenheid en Infrastructuur & Milieu. www.ensia.nl*

kopie waarop de gelaatsfoto en het BSN zijn verwijderd. Hierdoor ontstaat er bij de authenticatiediensten geen verzameling van persoonsgegevens (zogeheten hotspot), waardoor de privacy van de gebruikers wordt beschermd.

Voor het BSN als basis voor de uit te voeren controle is gekozen omdat alleen op basis hiervan de grootst mogelijke zekerheid wordt verkregen omtrent de identiteit van de gebruiker. Als alternatief is overwogen om het nummer van het document als bedoeld in artikel 1 van de Wet op de Identificatieplicht te hanteren. Op zichzelf is een WID-documentnummer geschikt als basis voor de controle. Het BSN is echter een meer betrouwbare en persistente manier om uniciteit te verzekeren. Hiermee is voldaan aan de eisen van doelbinding, noodzaak, proportionaliteit en dataminimalisatie, zoals deze volgen uit artikel 8 EVRM en de artikelen 7 - 11 van de Wet bescherming persoonsgegevens.[106]
De functie van (private) authenticatiediensten en de werking van de voorziening BSN-K bij toegang tot publieke dienstverlening zijn beproefd in - naar aard en omvang beperkte - *pilots*. Nu deze een vervolg krijgen[107] wordt de basis voor de persoonsgegevensverstrekking opgenomen in deze wet. Voor wat betreft erkende private machtigingsdiensten worden deze in het eerste lid genoemd omdat ook zij BSN, namelijk van de vertegenwoordigde, doorgeven aan het BSN-K. Immers: zij verwerken persoonsgegevens, waaronder het BSN, voor zover dit noodzakelijk is voor de betrouwbare toegang - van de gemachtigde namens de vertegenwoordigde (volmachtgever) - tot elektronische dienstverlening.
Het tweede lid voorziet in de wettelijke grondslag voor een ontsluitende dienst om persoonsgegevens, waaronder het BSN, te verwerken voor zover dit noodzakelijk is voor de betrouwbare toegang tot elektronische dienstverlening. Hoewel ontsluitende diensten alleen versleutelde gegevens verwerken bij hun taak (te weten het routeren van het elektronisch verkeer tussen een bestuursorgaan of aangewezen organisatie en erkende authenticatiediensten, machtigingsdiensten en attributendiensten, oftewel het 'ontzorgen' van publieke dienstverleners) en het BSN noch andere gegevens voor hen zichtbaar zijn, kan niettemin sprake zijn van verwerking van persoonsgegevens. Immers: deze gegevens zijn herleidbaar tot een persoon. Dat het niet de ontsluitende dienst zelf is die kan herleiden, is niet zonder meer doorslaggevend.[108] Een wettelijke grondslag ligt derhalve in de rede.

Voor de goede orde wordt opgemerkt, dat voor andere dan in het eerste en tweede lid genoemde bij authenticatie betrokken private diensten geen wettelijke grondslag voor de verwerking van persoonsgegevens, waaronder BSN, is opgenomen. Voor attributendiensten – die erkenning behoeven willen zij hun diensten kunnen aanbieden in het kader van deze wet - geldt dat, teneinde attributen (waaronder niet het BSN) te kunnen leveren, wordt geput uit gegevens die hen door gebruikers op basis van toestemming ter beschikking zijn gesteld.

Lid 3
Bij algemene maatregel van bestuur worden regels gesteld over de persoonsgegevens die gelet op de leden 1 en 2 worden verwerkt, aan wie deze worden verstrekt en hoe lang deze worden bewaard. Aan de eisen van doelbinding, subsidiariteit en proportionaiteit alsmede aan de uitgangspunten van kenbaarheid, voorzienbaarheid en transparantie voor degenen wiens gegevens het betreft, wordt aldus verder invulling gegeven. Het Besluit verwerking persoonsgegevens GDI zal in dit verband wordt gewijzigd en aangevuld met bepalingen over de bewaartermijnen van de gegevens, waarbij de bewaartermijn is onderbouwd en beperkt tot het doel van de verwerking. Ook wordt vastgelegd aan wie welke gegevens mogen worden verstrekt. Aldus word gewaarborgd dat gegevens niet langer worden bewaard en niet meer gegevens worden verstrekt dan noodzakelijk.

---

[106] De Privacy Impact Assessment inzake het Introductieplateau eID-stelsel van 31 juli 2015 concludeert in dit verband dat het gebruik van bsn zoveel mogelijk wordt beperkt en alleen wordt gebruikt voor het doel waarvoor dit nodig is:verificatie van de identiteit van de houder van een authenticatiemiddel die dit middel wil gebruiken in het publieke domein. Om uniciteit van de houder te kunnen vaststellen is de set gegevens ('attributen') zo effectief en minimaal mogelijk gehouden, aldus de PIA.
[107] Brief van de Minister van BZK inzake de uitkomsten van de evaluatie van de pilots met publieke en private middelen "Impuls eID", Kamerstuk 26 643 nr 419.
[108] Autoriteit Persoonsgegevens, Wbp-naslag met betrekking tot artikel 1, sub a.

Voor de volledigheid en uit een oogpunt van rechtszekerheid en duidelijkheid, zullen de te stellen regels niet alleen betrekking hebben op de in het eerste en tweede lid opgenomen private diensten, maar zullen deze regels tevens betrekking hebben op de verwerking van persoonsgegevens door de minister, bestuursorganen en aangewezen organisaties in het kader van de uitvoering van hun taken en verplichtingen ingevolge deze wet. Zo is het bijvoorbeeld om activiteiten in het kader van herkennen en herstellen van misbruik adequaat te kunnen uitvoeren (artikel 15), noodzakelijk om persoonsgegevens te verwerken.

Artikelen 10 - 13

De artikelen 10 tot en met 13 voorzien in toezicht op en handhaving van de voorschriften en beperkingen die op grond van artikel 6, zevende lid, en de regels die op grond van artikel 7 gesteld zijn aan de partijen in de authenticatieketen. Dit toezicht betreft de beperkingen en voorschriften die kunnen worden gesteld aan een erkenning alsmede de regels aan de erkende diensten, middelen en de publieke voorziening. Uitgangspunt bij het toezicht is dat eventuele interventies primair gericht zijn op herstel of op totstandkoming van de gewenste situatie. In situaties waarin dat nodig is, kan ook direct en repressief worden ingegrepen. Na de erkenning van een publiek of privaat middel en publieke of private authenticatiedienst, ontsluitende dienst, machtigingsdienst of attributendienst is het noodzakelijk om toezicht uit te oefenen op de naleving van de aan deze middelen en diensten gestelde regels. Ook wordt toezicht gehouden op de publieke voorziening die het mogelijk maakt om erkende middelen te gebruiken bij elektronische dienstverlening (BSN-Koppelregister). De voorschriften als bedoeld in artikel 6, zevende lid, en artikel 7 hebben immers betrekking op de normadressaten in de keten, oftewel de bovengenoemde (publieke en private) partijen die een rol spelen bij het goed functioneren van middelen in het publieke domein.

Het toezicht op de naleving van de regels die op grond van artikel 6, zevende lid en artikel 7 bij of krachtens algemene maatregel van bestuur worden gesteld, zal ingevolge artikel 10 naar verwachting worden belegd bij Agentschap Telecom, onderdeel van het ministerie van Economische Zaken. Reden hiervoor is de (technische) expertise en ervaring van Agentschap Telecom op het gebied van elektronische communicatie en communicatienetwerken, waaronder het toezicht op de naleving van de EU-verordening over het grensoverschrijdend gebruik van elektronische middelen en vertrouwensdiensten tussen lidstaten (eIDAS). Een andere reden om het toezicht bij Agentschap Telecom te beleggen is de beoogde betrokkenheid van het agentschap bij de erkenningsprocedure van partijen en middelen op grond van artikel 6.
Het toezicht heeft ook betrekking op veiligheidsinbreuken en integriteitsverliezen met aanzienlijke gevolgen voor de authenticatiedienst of de betrokken persoonsgegevens. De opgenomen meldplicht voor dergelijke veiligheidsinbreuken en integriteitsverliezen is vergelijkbaar met de meldplicht voor verleners van vertrouwensdiensten als opgenomen in artikel 19, tweede lid, van de eIDAS verordening. Agentschap Telecom houdt toezicht op de naleving van dit artikel voor vertrouwensdiensten.[109] Het toebedelen van dit toezicht aan Agentschap Telecom bij authenticatiediensten kan daarom in de rede liggen. In de Staatscourant zal worden gemeld welke toezichthouder op grond van dit wetsvoorstel wordt aangewezen.

Hoe de toezichthouder invulling geeft aan zijn taak wordt neergelegd in een in door de minister vastgesteld toezichtarrangement, dat mede gebaseerd is op een strategisch toezichtplan en uitgaat van programmatisch handhaven.[110] Een en ander geschiedt eveneens in afstemming met eventuele andere relevante toezichthouders. In dit verband moet bijvoorbeeld worden gedacht aan De Nederlandsche Bank, in het geval middelen van banken een rol gaan vervullen bij authenticatie voor elektronische dienstverlening door bestuursorganen en aangewezen organisaties. Dubbele toezichtslasten voor de diensten waarop toezicht wordt gehouden, zal worden voorkomen. Wel moeten betrokken toezichthouders van elkaar weten wat ze (moeten) doen (bijvoorbeeld: aan welke eisen en op welke wijze wordt getoetst) en ingevolge welke bevoegdheid, zodat waar nodig en mogelijk onderlinge afstemming en informatiedeling kan plaatsvinden.

[109] *Stb. 2016, nr…. TK 2015/2016, 34 413.*
[110] *www.agentschaptelecom.nl*

Het intrekken of schorsen van de erkenning van een partij in de authenticatieketen is een eigenstandige bevoegdheid van de minister op grond van artikel 13. Hij zal slechts tot schorsing of intrekking van een erkenning overgaan indien daartoe voldoende aanleiding is. Zo mogelijk zal de minister voorafgaand aan schorsing of intrekking van een erkenning overleg voeren met de betrokken partij. In dit overleg geeft de minister aan welke eisen de betreffende partij schendt en geeft deze een termijn om alsnog aan de eisen te voldoen. Indien de betrokken partij aantoont dat hij redelijkerwijs niet aan deze termijn kan voldoen, kan Onze Minster de termijn verlengen. Bij deze beslissing zal de minister vanzelfsprekend niet alleen de belangen van de betrokken partij, maar alle belangen meewegen.
De noodzaak van deze zorgvuldige procedure is, gelet op de ingrijpende gevolgen van schorsing of intrekking van een erkenning, evident. Zonder erkenning wordt een middel of een partij niet geaccepteerd voor elektronische dienstverlening van de bestuursorganen en de aangewezen organisaties. De schorsing of intrekking heeft verder direct gevolgen voor de gebruikers van het betreffende middel, omdat zij dit middel niet meer kunnen gebruiken.
Bij deze procedure tot schorsing of intrekking van een erkenning heeft de toezichthouder geen formele rol. Dit staat er niet aan in de weg dat, indien de toezichthouder van oordeel is dat een partij de eisen niet (langer) naleeft en schorsing of intrekking van de erkenning moet worden overwogen, de toezichthouder in het kader van zijn toezichtstaak de minister gevraagd of ongevraagd kan adviseren om tot schorsing of intrekking van de erkenning over te gaan. Uiteindelijk is het de minister die hiertoe beslist.

Met het instrumentarium van de artikelen 10 tot en met 13 is een afgewogen toezicht- en handhavingssysteem met betrekking tot de in artikel 6 bedoelde diensten gecreëerd. De verschillende bevoegdheden op grond van deze artikelen kunnen, waar nodig, in samenhang worden toegepast. Zo kan de minister, in een situatie dat een erkende partij een of meer eisen niet naleeft, aan de desbetreffende partij sancties opleggen. Deze sancties hebben geen gevolgen voor de erkenning van de betreffende partij of het betrokken middel. Indien sprake is van een dusdanig ernstige inbreuk dat de erkenning als authenticatiedienst wordt ingetrokken, dan is er ook aanleiding om de erkenning van het middel in te trekken.
De toezichts- en sanctiebevoegdheden en instrumenten zijn gekozen vanuit een oogpunt van goede werking, veiligheid en betrouwbaarheid van authenticatie in het publieke domein. De toepasselijke sancties zijn repressief; er gaat evenwel een preventieve werking van uit.

Benadrukt zij, dat de krachtens deze wet aangewezen toezichthouder in die hoedanigheid geen toezicht op bestuursorganen en aangewezen organisaties uitoefent. Uitgangspunt is dat publieke dienstverleners een eigenstandige verantwoordelijkheid hebben voor de werking, betrouwbaarheid en beveiliging van de toegang tot de elektronische diensten die zij bieden aan natuurlijke personen (burgers) en rechtspersonen (bedrijven). Dit sluit aan bij het kader van generiek toezicht, dat uitgaat van het vertrouwen dat betrokken overheden de wettelijke voorschriften naleven (zie artikelen 14 - 16).

Artikel 14

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 de 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. De zinsnede "Onze Minister wie het aangaat" verwijst naar de minister op wiens beleidsterrein het desbetreffende zelfstandige bestuursorgaan of aangewezen organisatie werkzaam is. Voor wat betreft de toezichthouders zal het daarbij in de regel gaan om het ter zake van de desbetreffende organisaties reeds functionerende toezicht. Voor wat betref het toezicht op de ministeries zelf, dient onder 'Onze Minister wie het aangaat' de minister van BZK te worden verstaan.

Artikel 15

Lid 1
Teneinde veilige en betrouwbare elektronische authenticatie in het publieke domein te kunnen realiseren, is het nodig dat de minister beschikt over de mogelijkheid om maatregelen te nemen om compromittering van de veilige en betrouwbare toegang tot elektronische dienstverlening door bestuursorganen en aangewezen organisaties te voorkomen of beëindigen. Dit artikellid biedt de minister bijzondere bevoegdheden voor het geval reguliere (interbestuurlijke) instrumenten niet toereikend blijken om veilige en betrouwbare toegang tot publieke dienstverlening te realiseren. Artikel 15, eerste en tweede lid, dienen te worden gelezen in samenhang met artikel 8, op basis waarvan eisen worden gesteld aan werking, betrouwbaarheid en beveiliging van de toegang tot elektronische dienstverlening door bestuursorganen en aangewezen organisaties, waaronder het jaarlijks overleggen van een auditverklaring. Zoals ook in de toelichting bij artikel 8 is aangegeven, voorziet dit wetsvoorstel niet in aanvullende instrumenten met betrekking tot handhaving van de gestelde regels. Uitgangspunt – en aansluitend bij het kader van generiek toezicht - is dat de betrokken bestuursorganen en aangewezen organisaties een eigenstandige verantwoordelijkheid hebben voor informatiebeveiliging en dat er op mag worden vertrouwd dat zij de eisen ter zake naleven. Indien evenwel uit de te overleggen auditverklaringen zou blijken, dat de informatieveiligheid in het geding is en ook na herhaaldelijke aanmaningen de benodigde verbeteringen niet worden aangebracht, kan als uiterste middel de in het onderhavige artikel opgenomen bevoegdheid tot het treffen van noodmaatregelen uitkomst bieden. Ook het stelselmatig niet overleggen van een auditverklaring of anderszins niet nakomen van bestuurlijke afspraken kan een aanleiding vormen voor het nemen van een noodmaatregel.
Tevens kan de minister noodmaatregelen nemen bij ernstige storingen, ernstige aantasting van de werking beveiliging of betrouwbaarheid van de elektronische dienstverlening, of misbruik of oneigenlijk gebruik van de toegang ter zake. Onder "misbruik of oneigenlijk gebruik" wordt begrepen zowel aantastingen van, en inbreuken op de (technische) beveiliging (hacken, DDoS-aanvallen, dat wil zeggen pogingen om een computer, computernetwerk onbeschikbaar te maken voor gebruik) als bewuste inbreuken op de processen voor publieke dienstverlening en systemen van bestuursorganen en aangewezen organisaties, waarvan burgers, bedrijven en de overheid zelf het slachtoffer kunnen worden. Teneinde de veiligheid en betrouwbaarheid van de toegang tot elektronische dienstverlening te waarborgen en misbruik of oneigenlijk gebruik ervan zoveel mogelijk te voorkomen, is het nodig dit te kunnen herkennen, vroegtijdig te signaleren en, bij constatering daarvan, herstel- en noodmaatregelen te kunnen nemen. Concreet gaat het daarbij om het wegnemen van een acuut risico, door middel van het tijdelijk (doen) onderbreken (schorsen) van de toegang tot publieke dienstverlening (afsluiten van authenticatie).

Artikel 15, eerste lid, faciliteert (nood)maatregelen om in het kader van vermoede of manifeste integriteits- of beveiligingsinbreuken maatregelen te treffen die zich richten op de dienstverlening van bestuursorganen en aangewezen organisaties met als doel de borging of het herstel van de betrouwbare toegang tot hun elektronische diensten. Dit betekent dat de genoemde bevoegdheden hun grens kennen. Wanneer bijvoorbeeld een burger met gebruik van zijn publieke middel een frauduleuze aanvraag voor toeslagen indient door bewust verkeerde posten in te vullen om meer toeslag te verkrijgen dan waar hij recht op heeft, is er geen sprake van aantasting van de betrouwbaarheid van de toegang tot publieke diensten. Het is immers de burger die misbruik pleegt, met andere woorden het *gebruik* van zijn middel is frauduleus. In dat geval bestaat voor de minister geen wettelijke grondslag om uit eigen beweging dergelijke (vermoedens van) fraude te onderzoeken en hiervan melding te doen aan betrokken bestuursorganen.
Tot de in dit artikel bedoelde taak behoort ook niet opsporing ten behoeve van strafvorderlijke vervolging. Wel kunnen politie, justitie en daartoe bevoegde publieke dienstverleners zoals de Belastingdienst, de desbetreffende minister of het desbetreffende bestuursorgaan om informatie en gebruik(er)sgegevens verzoeken. Alsdan zal afgewogen worden of de relevante informatie kan worden aangeleverd overeenkomstig de daarvoor geldende wettelijke kaders. Ook binnen de voorziening als bedoeld in artikel 4, eerste lid, onderdeel c, van deze wet (BSN-K) is ten behoeve van het operationeel beheer (goede werking, probleemanalyse etc.) sprake van (technische) controlemaatregelen met betrekking tot persoonsgegevens en digitale identiteit, logging en het bijhouden van een audittrail, bijvoorbeeld over (afwijkend) gedrag van authenticatiediensten, dat gebruikt kan worden voor het herkennen van misbruik (zie ook de toelichting op het derde lid).

Lid 2
Teneinde vast te (kunnen) stellen of sprake is van een ernstige situatie, is het van belang dat een bestuurorgaan of een aangewezen organisatie de minister onverwijld in kennis stelt 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 en dat daarbij alle benodigde informatie word verstrekt. Deze verplichting is in feite de pendant van de meldplicht jegens Agentschap Telecom voor (publieke en private) diensten als bedoeld in artikel 7, vijfde lid.

Voor de goede orde wordt opgemerkt, dat melding in de zin van dit artikel onderscheiden moet worden van de meldplicht datalekken; ingevolge artikel 34a Wbp moet het lekken van persoonsgegevens als gevolg van beveiligingsproblemen, met nadelige gevolgen voor de bescherming van de persoonsgegevens (diefstal, verlies of misbruik) worden gemeld aan de Autoriteit Persoonsgegevens. Voorts kan in de toekomst eventueel de jegens het Nationaal Cyber Security Centrum (NCSC) geldende meldplicht voor ernstige ICT-inbreuken toepasselijk zijn. Deze meldplicht geldt alleen voor (nader aan te wijzen) aanbieders van diensten waarvan de beschikbaarheid of betrouwbaarheid van vitaal belang is voor de Nederlandse samenleving.[111]

Lid 3
Ook bij het vermoeden van misbruik of oneigenlijk gebruik van een individueel middel dat gebruikt wordt voor elektronische dienstverlening (dus: in het publieke domein), is het van belang dat de minister de mogelijkheid heeft om snel en doeltreffend te handelen en het desbetreffend middel 'uit de roulatie' te halen. Bij private middelen, die niet van overheidswege worden uitgegeven, is het niet opportuun om bij het nemen van acute maatregelen afhankelijk te zijn van de medewerking van de desbetreffende private authenticatiedienst. Het is immers de verantwoordelijkheid van de minister te zorgen voor veilige en betrouwbare toegang tot elektronische dienstverlening; hij moet indien nodig zelf maatregelen kunnen nemen om dit te borgen. De te nemen maatregel bestaat in het schrappen van de registratie van het desbetreffende middel in de voorziening, bedoeld in artikel 4, eerste lid, onder 2, het BSN-K. Benadrukt wordt dat deze acute maatregel mogelijk is bij vermoed misbruik van hetzij een publiek hetzij een privaat middel, en is gericht tot een individueel middel. De erkenning van het type middel wordt derhalve ongemoeid gelaten.

Artikel 16

Lid 1-3
Alleen indien hij over juiste en volledige informatie beschikt, kan de minister zijn taken en verantwoordelijkheden voor een veilige en betrouwbare toegang tot elektronische dienstverlening waarmaken. Naast het monitoren, onderzoeken en analyseren zoals dat in het kader van het operationeel beheer gebeurt, is wederzijdse informatieverschaffing (uit eigen beweging en op verzoek) door partijen in de authenticatieketen nodig. Dit artikel voorziet daarin. Alle benodigde informatie - over de werking van de toegang en dus *niet* over de *inhoud* van de in het kader van de dienstverlening uitgewisselde berichten - moet daarbij worden verstrekt, zodat de minister kan beoordelen of er maatregelen moeten worden getroffen. Een wederzijds afgestemde aanpak ligt daarbij om redenen van effectiviteit en doelmatigheid in de rede; van bestuursorganen en aangewezen organisaties kan, gezien het belang om veiligheid ketenbreed op te pakken, bijvoorbeeld medewerking verlangd worden op het moment dat mogelijk misbruik (bijvoorbeeld een integriteits- of beveiligingsinbreuk) wordt geconstateerd. Omgekeerd moet de minister gegevens en inlichtingen verstrekken aan partijen in de authenticatieketen over de compromittering van de veilige en betrouwbare toegang elektronische dienstverlening voor zover dit noodzakelijk is voor een goede uitoefening van hun taken respectievelijk te verlenen diensten. Welke gegevens in het concrete geval moeten worden uitgewisseld is afhankelijk van de omstandigheden van het geval. Om die redenen kan niet op voorhand een inperking worden aangebracht in de gegevens die dienen te worden verstrekt en verwerkt. De gegevensverwerking kan daarmee in potentie ieder gegeven betreffen dat beschikbaar is binnen de autheticatieketen.

[111] *TK 34 388, Wet gegevensverwerking en meldplicht cybersecurity.*

Vanzelfsprekend gelden daarbij de uitgangspunten van noodzakelijkheid, doelbinding, proportionaliteit en subsidiariteit. Ook gegevensverwerking in het kader van veilige en betrouwbare authenticatie omvat immers (mede) de verwerking van persoonsgegevens, zodat aan de bepalingen van de Wet bescherming persoonsgegevens (Wbp) en de EU Verordening gegevensbescherming moet worden voldaan.

De toezichthouder meldt de aan hem gedane meldingen over veiligheidsinbreuk of integriteitsverlies met aanzienlijke gevolgen voor de veilige en betrouwbare toegang tot elektronische dienstverlening aan de minister (tweede lid). Aldus behoeven de betrokken diensten slechts een keer te melden en wordt dubbele melding voorkomen.

Artikel 17

Dit artikel regelt dat het Rijk leges kan heffen bij de authenticatiediensten, ontsluitende diensten, machtigingsdiensten en attributtiediensten voor hun erkenning (en voor wat betreft de authenticatiediensten tevens voor het middel) door de minister van BZK. Het gaat hier om een vergoeding van met name de personele kosten die het Rijk (lees: het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en de aangewezen toezichthouder/Agentschap Telecom) zal maken voor het beoordelen van de aanvragen. Dit zal worden geregeld bij of krachtens algemene maatregel van bestuur.

De kosten zullen ook verschuldigd zijn, indien de minister besluit om de erkenning niet te verlenen. Bij de formulering van het artikel is zoveel mogelijk aangesloten bij Aanwijzing 163a van de Aanwijzigingen voor de regelgeving. Aangezien de kosten per categorie dienst kunnen uiteenlopen, zal per categorie dienst een tarief kunnen worden vastgesteld. De hoogte van het tarief zal een forfaitair bedrag zijn.

Artikel 18

Lid 1
Dit lid regelt het algemene uitgangspunt dat de burger zal moeten betalen voor de aanschaf van erkende publieke middelen en voor het middel zelf. De hoogte van deze leges is nog niet bekend en kan per publiek middel verschillen.

Lid 2
Het tweede lid biedt een grondslag voor het bij ministeriële regeling vaststellen van een tarief voor publieke middelen waarvan het tarief niet in een ander wettelijk voorschrift wordt geregeld. Vooralsnog betreft dit uitsluitend de grondslag voor een mogelijk tarief voor DigiD substantieel. De kosten voor de extra functie van authenticatie op de e-NIK zullen namelijk worden verdisconteerd in het tarief voor de NIK. De kosten die de RDW maakt worden aan de hand van de rijkskostencomponent ingevolge artikel 121, eerste lid, Wegenverkeerswet via gemeenten bij de burger in rekening gebracht, dan wel via het tarief van de RDW voor een door de RDW afgegeven e-rijbewijs.

Artikel 19

Dit artikel biedt de grondslag voor het vaststellen van de tarieven die de tot het Rijk behorende publieke authenticatiedienst(en) en de tot het Rijk behorende publieke machtigingsdienst in rekening zal brengen bij de ontsluitende dienst. Deze tarieven worden vastgesteld overeenkomstig bij of krachtens algemene maatregel van bestuur te stellen regels.

Artikel 20

Op grond van dit artikel kunnen de kosten voor de voorziening BSN-koppelregister, alsmede voor het toezicht, worden doorbelast aan de erkende diensten, te weten de erkende authenticatiediensten, ontsluitende diensten, machtigingsdiensten en attributendiensten, overeenkomstig bij of krachtens algemene maatregel van bestuur te stellen regels. Voor wat het BSN-koppelregister betreft gaat het zowel om de kosten van instandhouding, als om de kosten van

aansluiting en het gebruik. Op dit moment is het niet goed mogelijk om de totale kosten van de voorziening en het toezicht (in de tijd) in beeld te brengen. Evenmin is bekend in welke mate er gebruik zal worden gemaakt van de voorziening en hoeveel partijen zullen deelnemen. Daarmee is ook nog niet duidelijk wat het gewenste bekostigingsmodel is. Ook kan het bijvoorbeeld zijn dat het voor de totstandkoming van de markt van publieke en private middelen gewenst is om de eerste jaren de desbetreffende kosten niet of niet geheel door te belasten. In de algemene maatregel van bestuur kan op al deze aspecten worden ingespeeld.

Artikel 21

Dit artikel biedt de mogelijkheid om bij algemene maatregel van bestuur regulerend op te treden in de tarieven en voorwaarden die de erkende diensten voor hun dienstverlening hanteren.

Het stellen van regels over tarieven kan bijvoorbeeld inhouden het vaststellen van een maximumtarief of het voorschrijven van een kaders voor een redelijk tarief. Vanwege de samenhang van de tarieven met de voorwaarden die worden gehanteerd, geldt de mogelijkheid van ingrijpen ook ten aanzien van de voorwaarden.

Met de zinsnede 'dienstverlening, ten aanzien waarvan bij of krachtens deze wet regels zijn gesteld' wordt duidelijk gemaakt dat de regulering alleen betrekking heeft op de in dit wetsvoorstel gereguleerde dienstverlening in het publieke domein waarvoor het betrouwbaarheidsniveau substantieel of hoog geldt. Zo geldt de mogelijkheid van ingrijpen in de tarieven niet ten aanzien van mogelijke andere diensten die de (private) authenticatiedienst levert, zoals bijvoorbeeld authenticaties in het private (oftewel: commerciële) domein of authenticaties in het publieke domein waarvoor niet het betrouwbaarheidsniveau substantieel of hoog geldt.

Artikel 22

Deze wet zal binnen vijf jaar na inwerkingtreding worden geëvalueerd. Op basis van de uitkomsten zal worden bezien of en zo ja, in hoeverre wijziging in de rede ligt.

Artikel 23

Lid 1 -3
Partijen die in de aanloop naar inwerkingtreding van deze wet, te weten in de maand voorafgaand aan inwerkingtreding, meedoen aan *pilots*, waardoor middelen voor publieke dienstverlening worden gebruikt, dienen gedurende deze beproevingsfase te voldoen aan eisen inzake werking, betrouwbaarheid en veiligheid. Deze zijn opgenomen in privaatrechtelijke overeenkomsten, waaronder deelnemersovereenkomsten en aansluitvoorwaarden. Ook zijn zij onderworpen aan toezicht. Om redenen van duidelijkheid en rechtszekerheid is het van belang deze partijen perspectief te bieden inzake de continuïteit van hun dienstverlening , zonder afbreuk te doen aan doel en strekking van deze wet. Daarom is bij wijze van overgangsrecht bepaald dat deze partijen en middelen worden geacht over een erkenning als bedoeld in artikel 6 te beschikken tot een jaar na inwerkingtreding van deze wet. Uiterlijk na een jaar moet ten aanzien van de desbetreffende partij en ten aanzien van het desbetreffende middel een (formeel) besluit tot erkenning zijn genomen. Een aanvraag voor erkenning dient daartoe ruim binnen dat jaar te worden ingediend conform de toepasselijke bepalingen van de Algemene wet bestuursrecht. Indien na een jaar geen besluit tot erkenning is genomen, dan geldt de desbetreffende partij niet langer als erkend. Ditzelfde geldt voor het publieke middel (DigiD) op betrouwbaarheidsniveau substantieel, dat beschikbaar komt in de periode van voorbereiding van deze wet. Vanzelfsprekend gelden gedurende de overgangstermijn ter zake van de diensten en middelen als bedoeld in de leden 1 - 3 wel de overige bepalingen die in en op basis van deze wet zijn gesteld.

Lid 4
Hoewel authenticatiemiddelen op een lager betrouwbaarheidsniveau dan substantieel of hoog niet zullen worden erkend ingevolge artikel 6, kunnen ze nog worden geaccepteerd door bestuursorganen en aangewezen organisaties gedurende drie jaar na inwerkingtreding van deze wet voor diensten waarvoor een laag betrouwbaarheidsniveau geldt. Achtergrond hiervan is het

feit, dat in de toekomst alleen nog publieke middelen op hogere betrouwbaarheidsniveau's beschikbaar zullen zijn voor gebruik in het publieke domein; DigiD op betrouwbaarheidsniveau laag wordt uitgefaseerd (zie ook de toelichting bij artikel 4, eerste lid, onderdeel a).

Lid 5
Met betrekking tot het publieke middel DigiD op betrouwbaarheidsniveau laag, blijven gedurende drie jaar na de inwerkingtreding van deze wet de regels van toepassing die ter zake gelden op de dag voor inwerkingtreding van deze wet. Het gaat om (de desbetreffende regels in) het Besluit verwerking persoonsgegevens GDI en de Regeling voorzieningen GDI.

Lid 6
Sinds het op de markt komen van dit middel is het gebruik van DigiD gratis, zowel voor de gebruiker als voor de dienstverlener. Dit betekent dat het Rijk thans alle kosten hiervan draagt. Op grond van het zesde lid zullen tijdens de uitfasering van deze middelen de kosten wel worden doorberekend. In principe zal hiervoor een tarief in rekening worden gebracht bij een ontsluitende dienst, aangezien DigiD op betrouwbaarheidsniveau laag na de inwerkingtreding van de wet via een ontsluitende dienst ontsloten zal worden (dat is nu niet het geval). In de overgangsfase zal nog niet bij alle dienstverleners DigiD op betrouwbaarheidsniveau laag via een ontsluitende dienst ontsloten worden. Daarom voorziet het lid voor deze fase in de grondslag voor het in rekening brengen van een tarief bij de dienstverleners zelf.

Artikel 24

Tot op heden geldt het bepaalde in artikel X, eerste lid, van de Wet Elektronisch berichtenverkeer Belastingdienst (WEBV) als grondslag voor de taken en verantwoordelijkheden van onze Minister ter zake van elektronische authenticatie, inclusief elektronische registratie van machtigen, in het publieke domein. Dit vormde de opmaat naar de wet GDI. Bij inwerkingtreding van deze wet zal derhalve het bepaalde inzake authenticatie in artikel X, eerste lid, WEBV komen te vervallen en wordt dit artikel beperkt tot de zorg voor voorzieningen voor elektronisch berichtenverkeer en informatieverschaffing (MijnOverheid).

Artikel 25

In verband met de ontwikkeling en afgifte van een eRijbewijs (zie ook de toelichting bij de artikelen 4 en 18) is het van belang een grondslag te scheppen voor de door gemeenten aan de RDW te vergoeden kosten. Om die reden wordt artikel 121, eerste lid, van de Wegenverkeerswet 1994 aangepast.

Artikel 26

Na inwerkingtreding van deze wet berust het Besluit verwerking persoonsgegevens GDI op artikel X, derde lid van de WEBV, te weten voor zover het de verwerking betreft van persoonsgegevens in MijnOverheid en DigiD op betrouwbaarheidsniveau laag alsmede op artikel 9, derde lid, van deze wet, te weten voor zover het de verwerking betreft van persoonsgegevens terzake van authenticatie in de zin van deze wet.

De Minister van Binnenlandse Zaken en Koninkrijksrelaties,

De Minister van Economische Zaken,