Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2017–2018

34 972 Algemene regels inzake het elektronisch verkeer in het publieke domein en inzake de generieke digitale infrastructuur (Wet digitale overheid)

Nr. 3

MEMORIE VAN TOELICHTING

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. Het Regeerakkoord Vertrouwen in de toekomst (2017 – 2021) benadrukt dat aanpassing aan de digitale samenleving van de overheid niet alleen noodzakelijk is, maar dat het ook mogelijkheden biedt voor een betere dienstverlening. Het kabinet ontwikkelt daartoe een ambitieuze, brede agenda voor de verdere digitalisering van het openbaar bestuur op verschillende niveaus. Het onderhavige wetsvoorstel past in die ambitie en legt de basis voor die verdere digitalisering, waaronder regulering van de digitale overheid en meer in het bijzonder de generieke digitale voorzieningen in een gemeenschappelijke infrastructuur van de overheid. Dit wetsvoorstel vormt een eerste tranche van regelgeving ten behoeve van de verdere digitalisering van de overheid op de verschillende niveaus. Het wetsvoorstel bevat de meest urgente onderwerpen van regelgeving, te weten:

– de bevoegdheid om bepaalde standaarden te verplichten in het elektronisch verkeer van de overheid;
– het stellen van regels over informatieveiligheid;
– de verantwoordelijkheid voor het beheer van de voorzieningen en diensten binnen de generieke digitale overheidsinfrastructuur (GDI);
– de digitale toegang tot publieke dienstverlening voor burgers (natuurlijke personen) en bedrijven (rechtspersonen en ondernemingen).

Het wetsvoorstel bevat kaders voor verdere ontwikkeling op basis van de hiervoor genoemde, thans meest noodzakelijke maatregelen, maar biedt nadrukkelijk de basis voor verdere uitbreidingen verdere modernisering. Daarvoor bevat het wetsvoorstel vooral kaders die kunnen worden uitgewerkt in nadere regelgeving, die snel aangepast kan worden om ruimte te bieden voor verdere ontwikkeling van de digitale overheid en biedt ruimte voor innovatie.

kst-34972-3
ISSN 0921 - 7371
's-Gravenhage 2018

Standaarden

Alhoewel in de praktijk in het elektronisch verkeer reeds veelvuldig gebruik wordt gemaakt van open standaarden en hierover ook instructies en afspraken bestaan, acht de regering het, nu op dit moment 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. 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. De aanwijzing van een standaard kan 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. De grondslag is mede noodzakelijk ter implementatie van de Europese richtlijn inzake de toegankelijkheid van de websites en mobiele applicaties van overheidsinstanties.[1]

Informatiebeveiliging

Door de vergaande digitalisering van processen in de samenleving, waaronder processen bij de rijksoverheid en medeoverheden, is de beveiliging van (digitale) informatie en ICT-systemen van essentieel belang. Informatiestromen beperken zich daarbij niet tot de eigen organisaties; er is sprake van ketens. Burgers, bedrijven, bestuursorganen en aangewezen organisaties moeten erop 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.

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 identificatiemiddelen dienen dan ook te voldoen aan strenge eisen ten aanzien van werking, veiligheid en betrouwbaarheid. Dit betekent dat de Minister terzake een beheersbaar risico moet realiseren en moet kunnen aantonen dat hij redelijkerwijs passende maatregelen heeft genomen om de risico's te beperken.
Ook bestuursorganen en aangewezen organisaties moeten voldoen aan eisen voor de beveiliging van de eigen onderliggende systemen, teneinde veilige toegang tot elektronische diensten mogelijk te maken. 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 maatregelen worden door de dienstverleners getroffen en onderhouden op basis van een daartoe door hen vast te stellen informatiebeveiligingsbeleid en daaruit voortvloeiende informatiebeveiligingsplannen. De informatiebeveiligings-

[1] *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.*

maatregelen (zoals technische toegangsbeveiliging en scheiding van verantwoordelijkheden) worden opgenomen in de genoemde plannen en worden op basis van risicoanalyse geselecteerd en geïmplementeerd om de doelmatigheid en proportionaliteit van de maatregelen te realiseren. Teneinde de veiligheid, betrouwbaarheid en continuïteit te borgen kunnen de maatregelen tussentijds worden aangepast indien daartoe aanleiding bestaat. Doel is inbreuken op en aantastingen van de (technische) beveiliging dan wel de processen ten behoeve van deze toegang te voorkomen. Om dit te realiseren wordt bij het stellen van nadere regels op basis van het wetsvoorstel in ieder geval aansluiting gezocht bij de geldende rijksbrede informatieveiligheidsnormen en bij de (open) standaarden die op grond van het wetsvoorstel bij algemene maatregel van bestuur zullen worden aangewezen.

1.2. Het beheer van de GDI

Het wetsvoorstel verankert de verantwoordelijkheid van de Minister van Binnenlandse Zaken en Koninkrijksrelaties (BZK) voor het beheer van het geheel van voorzieningen inzake de generieke digitale infrastructuur (GDI). Het gaat hierbij om (ICT-)voorzieningen die overheden, (semi)publieke organisaties en bepaalde organisaties die het burgerservicenummer verwerken in staat stellen hun primaire (digitale) processen doelmatig in te richten. De GDI is naar zijn aard niet organisatie-, sector- of domeinspecifiek. De GDI is een dynamisch geheel dat continu wordt doorontwikkeld, aangepast en uitgebreid. Het wetsvoorstel geeft een niet-limitatieve opsomming van voorzieningen die functioneren binnen de context van de overige bepalingen van dit wetsvoorstel, inzake veiliger en betrouwbaarder elektronische publieke dienstverlening en de elektronische toegang daartoe. In het wetsvoorstel is de GDI (functioneel) omschreven en is omschreven welke taken de Minister in dit verband in ieder geval heeft. De GDI zal op basis van technologische ontwikkelingen of nieuwe inzichten gewijzigd worden door het toevoegen van nieuwe (functionaliteiten van) generieke voorzieningen of door het uitfaseren van bestaande voorzieningen. Op termijn kunnen ook andere onderdelen van de GDI in of bij deze wet worden geregeld. De intentie is dat de komende jaren voorzieningen worden (door)ontwikkeld of afgebouwd, en dat nieuwe functionaliteiten aan de voorzieningen worden toegevoegd.

In het kader van dit wetsvoorstel heeft de Minister van BZK een zorgplicht terzake van thans voorziene en in de toekomst te ontwikkelen generieke publieke voorzieningen (artikel 5). Deze wettelijke taak van de Minister van BZK inzake de generieke digitale infrastructuur brengt mee dat ontwikkeling en het beheer van (ICT-) producten en diensten voor de digitale overheid, dwz bruikbaar door alle (semi-)overheden en bsn-verwerkende organisaties in het kader van hun digitale dienstverlening, benodigd is. Deze activiteiten worden uitgevoerd door het BZK-dienstonderdeel dat daarvoor aangewezen wordt, bijvoorbeeld Logius of RVIG. Er is hier geen sprake van economische activiteiten in de zin van de Wet Markt en Overheid; ook is de overheid geen ondernemer en dus niet BTW-plichtig. Het gaat immers naar zijn aard om specifiek wettelijk ingekaderde overheidstaken.

1.3. Elektronische identificatie (eID)

Elektronische dienstverlening vergt (de beschikbaarheid van) oplossingen om de identiteit van natuurlijke personen, ondernemingen en rechtspersonen op een betrouwbare wijze digitaal vast te kunnen stellen. Dit wetsvoorstel codificeert de huidige verantwoordelijkheden van de Minister van BZK ten behoeve van de werking van de infrastructuur voor authenticatie in het publieke domein door burgers en bedrijven. De

Minister van BZK draagt onder meer zorg voor de ontwikkeling van inlogmiddelen voor burgers, op een hoger betrouwbaarheidsniveau dan het huidige DigiD basis, zodat diensten die een hoge of zeer hoge mate van betrouwbaarheid vereisen ook digitaal kunnen worden verleend. De regering heeft de ambitie om te bevorderen dat in 2020 in beginsel alle actieve DigiD gebruikers – thans ruim 13,5 miljoen burgers – kunnen beschikken over een elektronisch identificatiemiddel op het betrouwbaarheidsniveau substantieel of hoog. Dit wetsvoorstel verplicht bestuursorganen en aangewezen organisaties, vanwege het feit dat een groot deel ervan een publieke taak uitoefent in het spraakgebruik ook wel aangeduid als «(semi)publieke dienstverleners» of kortweg «dienstverleners», voor hun elektronische diensten waarvoor, gelet op de aard ervan veilige toegang in de rede ligt, het betrouwbaarheidsniveau «substantieel» of «hoog» gebruiken. De verplichtingen gelden ook voor daartoe aangewezen private organisaties, die elektronische diensten verlenen aan burgers of bedrijven waarvoor een veilige en betrouwbare authenticatie essentieel is, zoals bij zorgverzekeraars en pensioenuitvoerders.
Dit wetsvoorstel strekt er tevens toe dat de digitale toegang tot dienstverlening van bestuursorganen en aangewezen organisaties generiek wordt ingericht zodat burgers en bedrijven met één of meer generieke identificatiemiddelen overheidsbreed en op een passend betrouwbaarheidsniveau toegang kunnen krijgen tot elektronische diensten.

2. Standaarden

2.1. Inleiding

Standaardisering is randvoorwaardelijk om te kunnen communiceren.[2] 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 eruitzien, 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

[2] *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.*

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 gegevensformaat XBRL, een open standaard, op jaarbasis tientallen miljoenen euro's bespaart.[3]

2.2. De 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 dat veel instellingen knelpunten ervaren met betrekking tot de afhankelijkheid van leveranciers en de gegevensuitwisseling.[4]

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 aan een doelmatige informatiehuishouding, waarin digitale documenten die ten behoeve van wettelijke eisen[5], 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[6] 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

---

[3] *Kamerstukken II 2014/15, 34 262, nr. 3.*
[4] *Kamerstukken II 2013/14, 26 643 nr. 295, blz. 5.*
[5] *Zoals artikel 3 Archiefwet 1995.*
[6] *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.*

beperkte groep softwareleveranciers moeten communiceren met de overheid. Het kabinet voert vanwege de bovengenoemde voordelen sinds 2007 een op open standaarden gericht beleid.[7]
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 veiligheid, de betrouwbaarheid, de duurzame toegankelijkheid 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.

2.3. 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»).[8] 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 vanaf € 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, gebruiken en hierbij werken volgens het principe «pas toe of leg uit».[9] Gemeenten hebben zich aan deze resultaatverplichting gecommitteerd door middel van het Bestuursakkoord 2011–2015.[10] Op 18 mei 2015 werd in het Nationaal Beraad Digitale Overheid, waarin alle overheden waren vertegenwoordigd, de afspraak verlengd tot eind december 2017.

---

[7] *Kamerstukken II 2007/08, 26 643, nr. 98.*
[8] *Stcrt. 2008, nr. 227, bijlage, art. 3.*
[9] *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.*
[10] *Kamerstukken II 2010/11, 32 749, nr. 1, blg-110123, p. 52 en p. 53.*

2.4. Noodzaak van wetgeving

Diverse instrumenten zijn ingezet om overheidsbreed gebruik van open standaarden te realiseren, zoals het actieplan Nederland Open in Verbinding[11], 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 bleek 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 meting informatieveiligheidstandaarden en de Monitor Open Standaarden Beleid over de afgelopen jaren, 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»[12] 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 beval aan dat de overheid voortaan daadwerkelijk toeziet op naleving van haar «pas toe of leg uit»-beleid rondom open standaarden.[13] De Commissie Elias sloot zich aan bij het rapport «Geen goede overheidsdienstverlening zonder een uitstekende generieke digitale infrastructuur»[14] 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.[15] 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.[16]

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 niet kan worden afgewacht.

---

[11] *Kamerstukken II 2007/08, 26 643, nr. 98.*
[12] *Kamerstukken II 2010/11, 32 679, nr. 2.*
[13] *Kamerstukken II 2014/15, 33 326, nr. 5, p. 21.*
[14] *Kamerstukken II 2013/14, 26 643, nr. 314.*
[15] *Kamerstukken II 2014/15, 33 326, nr. 13, p. 15.*
[16] *Kamerstukken II 2016/17, 32 802, nr. 31 (motie Oosenbrug).*

Dit wetsvoorstel biedt daarom een grondslag om bij algemene maatregel van bestuur een verplicht toe te passen open standaard aan te wijzen. Een dergelijke 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 betrekken bij de voorbereiding van een algemene maatregel van bestuur en zal deze voorts aan een brede consultatie onderwerpen. Het gebruik van de verplichte standaarden zal vervolgens jaarlijks worden gemonitord.

2.5. De toegankelijkheidstandaard

Het is van groot belang dat de diensten van de overheid toegankelijk zijn voor eenieder. 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) is toegankelijk voor iedereen, inclusief 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(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 krachtens dit wetsvoorstel bij algemene maatregel van bestuur de Europese toegankelijkheidsnorm EN 301 549 aan te wijzen als een verplicht toe te passen standaard. Het wetsvoorstel voorziet daartoe het Tijdelijk besluit digitale toegankelijkheid overheid[17] van een duurzame formeel-wettelijke basis in artikel 28, onderdeel b. Het verplichten van de toepassing van deze Europese standaard is noodzakelijk ter implementatie van 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

[17] *Stb. 2018, 141.*

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 (EN 301 549). Deze Europese norm is gebaseerd op de wereldwijd toegepaste internationale standaard «Web Content Accessibility Guidelines» (WCAG) versie 2, waarop ook Webrichtlijnen versie 2 is gebaseerd. Om eenduidigheid te realiseren is Webrichtlijnen versie 2 van de «pas toe of leg uit»-lijst afgehaald en wordt EN 301 549 bij algemene maatregel van bestuur verplicht ter implementatie van Richtlijn 2016/2102/EU.

2.6. Informatieveiligheid

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[18] 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 beveiligt de netwerkverbinding waarover gegevens worden uitgewisseld en de toepassing van de standaard HTTPS beveiligt interactieve websites. 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 mogelijkheden van fraude en misbruik, zoals «phishing» of «spoofing» worden bestreden. Daarbij 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.

---

[18] *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.*

Brede adoptie van de standaard Digikoppeling is wenselijk 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.[19]

Informatieveiligheid is essentieel voor het vertrouwen in de digitale overheid. Gezien het belang van informatieveiligheid is het toepassen van bepaalde standaarden niet vrijblijvend voor de overheid. Derhalve komen – naast de toegankelijkheidstandaard – informatieveiligheidstandaarden zoals HTTPS en TLS, die reeds op de «pas toe of leg uit»-lijst staan, in aanmerking te worden verplicht bij algemene maatregel van bestuur op grond van dit wetsvoorstel. Daarmee vormt het voldoen aan de verplichte informatieveiligheidstandaarden een wettelijke ondergrens voor overheidsorganisaties om informatie met burgers, bedrijven en onderling veilig te kunnen uitwisselen en hergebruiken.

3. Elektronische identificatie (eID)

3.1. Inleiding

De afgelopen decennia is het gebruik van de elektronische weg in de contacten tussen burgers en bedrijven met de overheid toegenomen en breed geaccepteerd. In bijzondere wetten is soms al de elektronische weg met uitsluiting van de papieren weg voorgeschreven.[20]Hierbij zijn er sterke verschillen tussen de elektronische wegen. Dit hangt onder meer samen met verschillen in tempo waarop bestuursorganen digitaliseren en de invloed van nieuwe technologische ontwikkelingen. Van de overheid mag echter worden verwacht dat zij organisatieoverstijgend opereert, zodat informatie makkelijk vindbaar is en transacties eenvoudig uitvoerbaar zijn. Zo blijkt bijvoorbeeld uit onderzoek dat burgers en bedrijven bijvoorbeeld één overheidsportaal prettig vinden.[21] Om burgers en bedrijven een uniforme en veilige wijze van inloggen te bieden en om organisaties die handelen ter uitoefening van een publieke taak, in het algemeen belang of die het burgerservicenummer verwerken (hierna ook wel aangeduid als «dienstverleners»), te faciliteren, biedt de rijksoverheid al jaren generieke elektronische authenticatie- en machtigingsdiensten aan voor burgers, te weten het huidige DigiD en DigiD Machtigen[22]. Voor bedrijven is eHerkenning ontwikkeld. Dit is thans een publiek-private

---

[19] *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», PriceWaterhouse-Coopers, 23 februari 2010 (gepubliceerd op www.rijksoverheid.nl/documenten).*

[20] *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 met de Belastingdienst (Stb. 2015, 378).*

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

[22] *Om mogelijk te maken dat gemachtigden kunnen inloggen, registreert DigiD machtigen dat een persoon een andere persoon heeft gemachtigd namens hem of haar diensten af te nemen bij een dienstverlener. DigiD machtigen 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.*

samenwerking, waarbij in tegenstelling tot DigiD de inlogmiddelen uitsluitend door toegelaten private partijen worden uitgereikt. Door middel van deze generieke identificatiemiddelen kan een dienstverlener de identiteit en bevoegdheid van de burger of het bedrijf vaststellen alvorens persoons- of bedrijfsgebonden informatie uit te wisselen. Het gaat daarbij om een antwoord op de vragen «Wie ben je?», «Ben je wie je zegt dat je bent?» en «Wat mag je?» Hierbij wordt gebruik gemaakt van elektronische authenticatiediensten en in voorkomende gevallen ook van elektronische machtigingsdiensten. Met de laatstgenoemde diensten wordt de bevoegdheid van degene die inlogt vastgesteld (Wat mag je?). Elektronische identificatie vormt de sleutel voor de toegang van burgers en bedrijven tot de elektronische dienstverlening door de overheid en andere dienstverleners.

3.2. Noodzaak van wetgeving

Dit wetsvoorstel codificeert de huidige taken en verantwoordelijkheden, die nodig zijn om de infrastructuur voor identificatie en authenticatie in het publieke domein te doen functioneren. De Minister van BZK krijgt in dit wetsvoorstel taken en verantwoordelijkheden toebedeeld betreffende identificatie door bedrijven. Hij draagt in dit verband zorg voor het beheer van het stelsel voor identificatie van ondernemingen en rechtspersonen en voor een (knooppunt)voorziening met functionaliteiten om identificatie en soepele dienstverlening binnen de EU mogelijk te maken.
De Minister heeft daarnaast een zorgplicht voor generieke digitale infrastucturele voorzieningen zoals onder meer het BSN-koppelregister en een machtigingsvoorziening. De Minister van BZK is – naast het ontwikkelen en in stand houden van (voorzieningen van) de generieke digitale infrastructuur voor de (semi)publieke sector – verantwoordelijk voor het ontwikkelen van publieke identificatiemiddelen voor burgers op een voldoende hoog betrouwbaarheidsniveau.

Beschikbaarheid van publieke middelen met een hoger betrouwbaarheidsniveau

Voor een goede digitale dienstverlening is het noodzakelijk dat de brede basisinfrastructuur robuust en toekomstbestendig is.[23] Het aantal diensten dat digitaal kan worden afgenomen neemt in de loop der tijd toe en dat vergt het treffen van maatregelen om elektronische identificatie ook in de toekomst goed geborgd te hebben. Het huidige publieke identificatiemiddel DigiD heeft voor een deel van de dienstverlening adequate mate van veiligheid door onder meer eisen, die worden gesteld aan de wachtwoorden van burgers, en de beschikbaarheid van een bijzonder veilige infrastructuur. Het betrouwbaarheidsniveau van het huidige DigiD[24]is niet toereikend voor diensten met betekenisvolle rechtsgevolgen of waarbij uiterst vertrouwelijke informatie (zoals medische gegevens) wordt uitgewisseld. Dienstverleners moeten om bepaalde diensten digitaal te kunnen aanbieden, met meer zekerheid dan het huidige DigiD biedt, kunnen vaststellen of zij met de juiste (natuurlijke- of rechts-)persoon te maken hebben. De beschikbaarheid van de hoogste betrouwbaarheid van de authenticatie zou onder andere in de zorgsector en in de strafrechtketen nieuwe vormen van digitale dienstverlening mogelijk

[23] *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*

[24] *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.*

maken, zodat innovaties kunnen worden gerealiseerd, conform de doelstellingen van het regeerakkoord, de Digitale agenda gemeenten 2020 en de *eHealth* agenda van de Minister van VWS.[25]

Burgers kunnen in de toekomst de beschikking krijgen over publieke identificatiemiddelen op een hoger betrouwbaaheidsniveau dan het huidige DigiD. Reden voor het ontwikkelen van deze *publieke* middelen is dat de regering wil dat uiteindelijk voor iedere burger een betrouwbaar en veilig identificatiemiddel beschikbaar is en dat burgers niet afhankelijk zijn van de beschikbaarheid van private middelen voor het verkijgen van toegang tot digitale dienstverlening in het publieke domein. De kosten, die het Rijk maakt samenhangend met de verstrekking van een publiek identificatiemiddel en de kosten van dit identificatiemiddel zelf, worden ten laste gebracht van de burger. Dit wetsvoorstel voorziet in de grondslag voor het heffen van de leges en regelt dat de (variabele) kosten van het gebruik van de identificatiemiddelen ten laste komen van dienstverleners.

Aanvraag en uitgifte van publieke identificatiemiddelen

Ingevolge dit wetsvoorstel worden nadere eisen gesteld aan de uitgifte van identificatiemiddelen op de verschillende betrouwbaarheidsniveaus. Hiervoor gelden de relevante bepalingen uit de Europese eIDAS-verordening[26] inzake de betrouwbaarheid en het uitgifteproces. De in deze verordening opgenomen classificatie van identificatiemiddelen naar betrouwbaarheidsniveau («laag», «substantieel» en «hoog») wordt hierbij gevolgd. Aanvullende nationale regelgeving is noodzakelijk voor de aanvraag en de uitgifte van Nederlandse publieke identificatiemiddelen. Bij wettelijk voorschrift zal onder meer worden bepaald wie in aanmerking komt voor een publiek identificatiemiddel, 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.

Authenticatie op een bij de digitale dienstverlening passend betrouwbaarheidsniveau

Betrouwbare toegang tot digitale dienstverlening en de continuïteit van deze dienstverlening is een publiek belang dat overheidsinterventie rechtvaardigt. Bij digitale contacten kan het wenselijk zijn uiterst vertrouwelijke informatie (zoals medische gegevens of bepaalde bedrijfsgegevens) uit te wisselen tussen de dienstverlener en de burger of het bedrijf. Alvorens de dienstverlener deze informatie kan vrijgeven of

---

[25] *Onderzoek naar het betrouwbaarheidsniveau voor patiëntauthenticatie bij elektronische gegevensuitwisseling in de zorg wijst uit dat voor inlogmiddelen, die gebruikt worden in de zorg, minimaal niveau substantieel nodig is. Als het gaat om gegevens waarop het medisch beroepsgeheim van de zorgverlener rust is het hoogste betrouwbaarheidsniveau aangewezen. Betrouwbaardere identificatiemiddelen zijn derhalve nodig voor het realiseren van de eHealthdoelstelling en (die onder meer inhouden dat een groter aantal chronisch zieken digitale toegang tot bepaalde medische gegevens gaat krijgen) en het op termijn vervangen van de UZI-pas voor zorgverleners.*

[26] *De verificatie van de identiteit van de aanvrager is voor deze betrouwbaarheidsniveaus van groot belang; identificatiemiddelen 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.*
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.

aanvaarden, moet met voldoende mate van zekerheid worden vastgesteld aan wie die informatie wordt verstrekt of van wie de informatie afkomstig is. Dit vereist adequate elektronische identificatie en authenticatie. Op basis van de voorgestelde wet zullen bestuursorganen en aangewezen organisaties («dienstverleners») verplicht worden voor hun elektronische diensten waarvoor, gelet op de aard ervan, veilige toegang in de rede ligt, het betrouwbaarheidsniveau substantieel (inclusief «twee factor authenticatie»[27]) of hoog te gebruiken. Deze verplichting borgt dat de wijze van inloggen is toegesneden op de vertrouwelijkheid van de gegevens die worden uitgewisseld met de overheid. Bij het bepalen van het bij de dienstverlening passende betrouwbaarheidsniveau zullen dienstverleners zich moeten houden aan de krachtens dit wetsvoorstel te stellen regels. Deze uitvoeringsregelgeving zal het kader bieden voor dienstverleners om het vereiste betrouwbaarheidsniveau bij hun dienstverlening te bepalen.

Het wetsvoorstel biedt voldoende ruimte om in de uitvoeringsregelgeving passende overgangstermijnen te bepalen teneinde rekening te houden met de beschikbaarheid van identificatiemiddelen op de desbetreffende betrouwbaarheidsniveaus. De beschikbaarheid (dekkingsgraad) onder de desbetreffende doelgroep – burgers dan wel bedrijven – en de mogelijkheid van dienstverleners om aan te sluiten op de daarvoor bedoelde infrastructuur, bepaalt het tempo waarop de betrouwbaarheid van de dienstverlening zal kunnen toenemen.

Continuïteit van dienstverlening

Anders dan voor bedrijven, is er voor burgers op dit moment slechts één publiek identificatiemiddel: DigiD. Dit heeft bovendien slechts het betrouwbaarheidsniveau laag. Het komt voor dat DigiD het mikpunt is van zogeheten DDoS aanvallen.[28] In het verleden is het daarnaast voorgekomen dat 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. De toegang tot digitale dienstverlening voor burgers in het publieke domein is immers afhankelijk van één authenticatievoorziening.[29] Indien DigiD door een ernstige storing of inbraak in het informatiesysteem (tijdelijk) niet gebruikt kan worden, lopen bepaalde vormen van digitale dienstverlening aan burgers vast, met alle maatschappelijke gevolgen van dien. Indien de veiligheid van DigiD gecompromitteerd is, moet de Minister van BZK kunnen ingrijpen zonder dat de ingreep grotere complicaties zou opleveren dan de situatie waarvoor de ingreep een oplossing beoogd te zijn. Het is van belang dat de rijksoverheid anticipeert op het feit dat een overheidsbreed gebruikt inlogmiddel op stel en sprong (tijdelijk) vervangen moet kunnen worden indien de veiligheid niet kan worden gegarandeerd. De regering biedt met dit wetsvoorstel de Minister van BZK de mogelijkheid om één of meerdere door private partijen uitgegeven identificatiemiddelen te laten fungeren als een gelijkwaardige elektro-

---

[27] *De Tweede Kamer verzocht bij motie van het lid Van Engelshoven (Kamerstukken II 2016/2017, 34 725 VII, nr. 9) de regering actief te bevorderen dat mensen met 2-staps identificatie inloggen binnen het eID-stelsel. Deze vorm van authenticatie vereist dat de gebruiker niet alleen iets weet (een wachtwoord), maar ook ergens over beschikt (zoals de code in een sms-bericht, dat naar de telefoon van de gebruiker wordt verzonden).*

[28] *DigiD was door een DDos-aanval op 29 januari 2018 circa vijf kwartier beperkt beschikbaar. Verschillende overheidswebsites zijn op 7 maart getroffen door DDoS-aanvallen. De aanvallen waren gericht op DigiD en de Belastingdienst. Beide diensten waren daardoor niet volledig bereikbaar.*

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

nische toegangsvoorziening bij dienstverlening van de overheid.[30] Deze aanpak maakt deze dienstverlening – met name het inlogproces – minder kwetsbaar, waardoor de continuïteit van de dienstverlening beter is geborgd. Daarnaast biedt deze aanpak burgers de mogelijkheid om te kiezen voor het toegelaten middel, dat zij het prettigst hanteerbaar vinden (mits het voldoet aan het bij de dienstverlening vereiste betrouwbaarheidsniveau). Voorts draagt de toelating van private middelen bij aan de dekkingsgraad van middelen onder burgers.

Het is van groot belang dat burgers en bedrijven met een toegelaten respectievelijk erkend middel hun zaken met waarborgen voor de privacy digitaal kunnen afhandelen. Dat veronderstelt dat de Minister bij de verwerving van een privaat uitgegeven middel terzake eisen stelt.
Om als reëel alternatief voor publieke middelen te kunnen fungeren, is naast privacywaarborging toegankelijkheid van het private middel voor natuurlijke personen in Nederland vereist; in dit verband is onder andere de betaalbaarheid voor burgers en dienstverleners van belang. Indien de Minister besluit een privaat middel toe te laten, vindt de uitgifte ervan aan de gebruiker plaats door een private partij. Deze bepaalt in beginsel de kring van rechthebbenden van het middel, waarbij het in ieder geval zal gaan om burgers die over een bsn en een wettig identiteitsdocument beschikken. Met inachtneming daarvan is het aan de desbetreffende partij om te bepalen aan welke categorie burgers hij dit middel wil uitgeven, waarbij onder meer het aantal burgers dat over het private middel beschikt of kan beschikken (dekkingsgraad) mee zal wegen in de afweging om dit middel al dan niet aan te wijzen als toegelaten authenticatiemiddel in het (semi-)publieke domein.

Voor bedrijven zullen naar verwachting meerdere (private) identificatiemiddelen beschikbaar zijn; deze behoeven erkenning door de Minister. 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.

Verplichte acceptatie voor dienstverleners

De regering ziet digitalisering als een belangrijk middel om een betere dienstverlening aan burgers en bedrijven te kunnen leveren, zo mogelijk in combinatie met een hogere efficiëntie en minder administratieve lasten. Breed gebruik van de GDI-voorzieningen voorkomt versnippering in de dienstverlening en voorzieningen worden kosteneffectiever. Bij breed gebruik daalt de prijs per transactie en hoeven alternatieve voorzieningen niet meer doorontwikkeld en beheerd te worden. Er ontstaan op macroniveau efficiencyvoordelen. Burgers en bedrijven kunnen bij breed gebruik erop vertrouwen dat zij met een toegelaten respectievelijk erkend identificatiemiddel in het publieke domein terecht kunnen. Met name vanuit het belang van het faciliteren van burgers en bedrijven en het belang van een veilige en betrouwbare identificatie- en authenticatieketen, verplicht dit wetsvoorstel a-bestuursorganen en aangewezen organisaties om bij elektronische dienstverlening de toegelaten identificatiemiddelen, erkende middelen en voor wat betreft bestuursorganen tevens de bij de

[30] *Zie onder meer de brief van de Minister aan de Tweede Kamer van 25 augustus 2016, Kamerstukken II 2015/16, 26 643, nr. 419.*

Europese Commissie genotificeerde[31] middelen te accepteren, voor zover de middelen minimaal het voor de af te nemen dienst vereiste betrouwbaarheidsniveau hebben. Zonder wettelijke regeling zouden dienstverleners zelf kunnen bepalen welke identificatiemiddelen zij accepteren. In dat geval zou niet geborgd zijn dat burgers en bedrijven met één of enkele middelen bij alle dienstverleners terecht kunnen, wat de (wild)groei van hun digitale sleutelbos tot gevolg kan hebben.

Dienstverleners kunnen volgens bij ministeriële regeling te stellen regels voor een welbepaalde doelgroep afwijken van de acceptatieplicht, indien de acceptatie van andere identificatiemiddelen onder uitsluiting van toegelaten of erkende identificatiemiddelen nodig is om redenen van op die doelgroep gerichte elektronische dienstverlening. Authenticatie door middel van generieke identificatiemiddelen kan namelijk in voorkomende gevallen onmogelijk of onwenselijk zijn. Het kan bijvoorbeeld nodig zijn om meer voorwaarden te verbinden aan de toegang tot bepaalde elektronische systemen voor berichtenverkeer dan enkel de vaststelling van de identiteit van een natuurlijke persoon of rechtspersoon. Zo hebben bijvoorbeeld advocaten of gemachtigden een advocatenpas nodig om in te kunnen loggen bij elektronische diensten van zowel de Nederlandse Orde van Advocaten (NOvA) als de Rechtspraak. Met deze inlogmethode wordt de rechtsgang beschermd tegen handelingen door personen die de titel van advocaat (al dan niet tijdelijk) niet mogen voeren, aangezien de NOvA als houder van het advocatentableau de advocatenpassen en de daaraan verbonden bevoegdheden beheert.
Daarnaast kan bij algemene maatregel van bestuur, met het oog op het onderzoeken van nieuwe methoden waarmee authenticatie doeltreffender kan plaatsvinden, worden afgeweken van de plicht om alleen generiek toegelaten en erkende middelen te accepteren. Deze grondslag om te experimenteren is noodzakelijk om redenen van innovatie of doorontwikkeling van de toegang tot elektronische dienstverlening.[32]
Bovengenoemde uitzonderingen op de acceptatieplicht gelden voor bestuursorganen niet met betrekking tot de acceptatie van een identificatiemiddel dat behoort tot een door een lidstaat van de Europese Unie ingevolge de eIDAS-verordening bij de Europese Commissie aangemeld en goedgekeurd stelsel.

Verwerking persoonsgegevens

Wettelijke grondslag is tenslotte noodzakelijk vanwege het feit, dat in het kader van authenticatie sprake is van de verwerking van persoonsgegevens, waaronder het bsn, door publieke en private partijen.

---

[31] *Burgers en bedrijven uit EU-lidstaten moeten bij overheidsinstanties kunnen inloggen met door een lidstaat van de Europese Unie ingevolge de eIDAS-verordening bij de Europese Commissie aangemeld en goedgekeurd stelsel. De acceptatie van deze identificatiemiddelen uit EU-lidstaten draagt bij aan de internationale economische positie van Nederland als digitaal aantrekkelijk land om zaken mee te doen. Aangewezen organisaties en rechterlijke instanties hoeven in tegenstelling tot a-bestuursorganen alleen alle identificatiemiddelen die behoren tot een door een lidstaat van de Europese Unie ingevolge de eIDAS-verordening bij de Europese Commissie aangemeld en goedgekeurd stelsel te accepteren, indien dit is bepaald bij besluit van de Minister van BZK in overeenstemming met de Minister, die het mede aangaat.*

[32] *Bijvoorbeeld de innovatieve toepassing of het in het kader van de doorontwikkeling testen van een nieuw publiek middel bij specifieke dienstverleners. De uitzonderingsbepaling maakt het mogelijk om pilots te doen waarbij erkende identificatiemiddelen gedurende een bepaalde tijd niet hoeven te worden geaccepteerd door dienstverleners.*

3.3. Reikwijdte: bestuursorganen

De acceptatieplicht met betrekking tot toegelaten en erkende middelen (en daarmee verband houdende verplichtingen) geldt op grond van dit wetsvoorstel in de eerste plaats voor zogenaamde «a-bestuursorganen», voor zover zij elektronische diensten ter uitvoering van een publieke taak (ook wel aangeduid met «publieke diensten») verlenen aan natuurlijke personen, ondernemingen of rechtspersonen waarvoor elektronische authenticatie op het betrouwbaarheidsniveau substantieel of hoog in de zin van de eIDAS-verordening noodzakelijk is.[33] Dit betekent dus dat niet alle a-bestuursorganen onder de reikwijdte van dit onderdeel van het wetsvoorstel vallen, en dat voor de bestuursorganen die er wel onder vallen, dit slechts een gedeelte van hun dienstverlening kan betreffen.

Bestuursorganen

Met de term «a-bestuursorganen» wordt gedoeld op organen als bedoeld in artikel 1:1, eerste lid, onder a, van de Algemene wet bestuursrecht (hierna: Awb). Het betreft organen van rechtspersonen die krachtens publiekrecht zijn ingesteld, en die niet zijn uitgezonderd in artikel 1.1, tweede lid, van de Awb. Dit betekent dat het gaat om organen van de Staat (mits niet uitgezonderd), provincies, gemeenten of waterschappen, en om andere rechtspersonen die krachtens publiekrecht zijn ingesteld. Bij organen van de Staat valt onder meer te denken aan de Belastingdienst (Minister van Financiën) en de Dienst Uitvoering Onderwijs (Minister van Onderwijs, Cultuur en Wetenschap). Bestuursorganen met een eigen rechtspersoonlijkheid zijn bijvoorbeeld de Sociale Verzekeringsbank en het Uitvoeringsinstituut werknemersverzekeringen. Publiekrechtelijke organen die in artikel 1.1, tweede lid, van de Awb van het begrip «bestuursorgaan» zijn uitgezonderd en daarmee niet als bestuursorgaan worden aangemerkt, kunnen onder de reikwijdte van het wetsvoorstel vallen, als ze daartoe worden aangewezen, hetzij in de bijlage bij het wetsvoorstel, hetzij bij afzonderlijk besluit (zie de volgende paragraaf).

Bestuursorganen met een privaatrechtelijke grondslag, de zogenaamde «b-bestuursorganen» (daarbij verwijzende naar artikel 1:1, eerste lid, onder b, van de Awb), vallen in dit wetsvoorstel niet onder het begrip «bestuursorgaan». Hetzelfde geldt voor rechtspersonen met een wettelijke taak die niet als bestuursorgaan kunnen worden aangemerkt. In beginsel vallen deze organisaties dus niet onder het wetsvoorstel. Zij kunnen evenwel onder de reikwijdte van het wetsvoorstel worden gebracht door ze aan te wijzen.

Publieke diensten aan natuurlijke personen, ondernemingen en rechtspersonen

De acceptatieplicht geldt voor bestuursorganen alleen indien sprake is van elektronische diensten door een bestuursorgaan aan natuurlijke personen, ondernemingen of rechtspersonen. Het begrip «diensten» dient breed te worden uitgelegd en ziet op de hele taakuitoefening van het bestuursorgaan, mits het gaat om taakuitoefening ter uitvoering van een publieke taak en in direct verkeer met een natuurlijk persoon, onderneming of rechtspersoon. Van dienstverlening in de zin van dit wetsvoorstel is dus zowel sprake als een uitkering wordt aangevraagd of verstrekt of aangifte van een geboorte of overlijden wordt gedaan, als bij de aangifte voor de belasting, of de aanvraag voor een bijzondere vergunning.

---

[33] *Zie de definitiebepaling in het wetsvoorstel.*

Dat sprake dient te zijn van diensten aan natuurlijke personen en rechtspersonen of ondernemingen, betekent dat bestuursorganen die dergelijke diensten niet verlenen, bijvoorbeeld omdat ze uitsluitend onderzoek verrichten, niet onder de werkingsfeer van dit onderdeel van het wetsvoorstel vallen. Bestuursorganen wier taakuitoefening slechts gedeeltelijk dienstverlenend is, vallen ook slechts gedeeltelijk onder het wetsvoorstel.

Het karakter van dienstverlening aan natuurlijke personen en rechtspersonen betekent tevens dat het wetsvoorstel niet ziet op interne processen binnen een bestuursorgaan. Zo heeft het wetsvoorstel geen betrekking op de (elektronische) toegang van bij het bestuursorgaan werkzaam personeel tot bepaalde netwerken of informatie, dan wel tot zijn eigen personeelsdossier.

Evenmin heeft dit onderdeel van het wetsvoorstel betrekking op contacten tussen bestuursorganen onderling[34], dan wel op contacten met zakelijke partners van het bestuursorgaan. De acceptatieplicht geldt derhalve niet voor zakelijke diensten aan vaste ketenpartners. Zo is de acceptatieplicht niet van toepassing op de elektronische toegang van notarissen op de systemen van de Koninklijke Nederlandse Beroepsorganisatie, of op de elektronische toegang op de systemen van de Rijksdienst voor het Wegverkeer door zijn zakelijke partners. In dat geval is sprake van verlening van diensten die uitsluitend binnen gesloten systemen gebruikt worden tussen een welbepaalde groep deelnemers, en die geen (directe) gevolgen hebben voor derden. Dit is in lijn met de eIDAS-verordening. De acceptatieplicht ziet voor wat betreft bestuursorganen niet op de uitvoering van privaatrechtelijke overeenkomsten, ook niet als deze worden ingezet voor de taakuitoefening van bestuursorganen. Zo is dit onderdeel van het wetsvoorstel bijvoorbeeld niet van toepassing op elektronische facturering voor aan bestuursorganen geleverde diensten of producten.

3.4. Reikwijdte: aangewezen organisaties

Naast a-bestuursorganen vallen onder de reikwijdte van de hoofdstukken 3 tot en met 7 de organisaties behorende tot een in de bijlage bij deze wet aangewezen categorie, de organisaties die bij gezamenlijk besluit van de Minister van BZK en de betrokken vakminister zijn aangewezen alsmede rechterlijke instanties.

Bij de aan te wijzen organisaties gaat het om (categorieën van) instanties die elektronische diensten verlenen ter uitvoering van een publieke taak, in het algemeen belang of of waarbij het burgerservicenummer (bsn) wordt verwerkt, waarvoor, gelet op de aard en kenmerken van deze diensten, veilige en betrouwbare authenticatie noodzakelijk is. Het gaat hier in feite om organisaties die elektronische diensten verlenen waarvoor een elektronische authenticatie op het betrouwbaarheidsniveau substantieel of hoog als bedoeld in de eIDAS-verordening noodzakelijk zou zijn, indien sprake zou zijn van een openbare dienst in de zin van deze verordening. Deze organisaties zijn thans veelal toegankelijk via het huidig beschikbare publieke middel DigiD laag. Bij de aanwijzing van organisaties is niet doorslaggevend of de betrokken organisatieonderdeel is van de (semi)publieke sector. Een groot deel van de organisaties dat krachtens wettelijk voorschrift gerechtigd is het burgerservicenummer te gebruiken voor de uitvoering van een specifieke taak, behoort evenwel tot de (semi)publieke sector. Echter, ook terzake van van bepaalde private

[34] *Zoals bijvoorbeeld het inloggen in elektronische systemen van de RDW door garages die gerechtigd zijn APK te keuren.*

organisaties zoals zorgaanbieders, kan het vanwege de aard en kenmerken van hun werkzaamheden, in de rede liggen om hen aan te wijzen. Kortweg worden de onder de reikwijdte van dit wetsvoorstel vallende bestuursorganen en aangewezen organisaties ook wel aangeduid als «dienstverleners».

Individuele organisaties

De aanwijzing van individuele organisaties geschiedt bij besluit van de Minister van BZK, in overeenstemming met de Ministers die het, gezien het desbetreffende beleidsdomein, aangaat. Aanwijzing geschiedt al dan niet op verzoek van en in overleg met de betrokken instanties, zodat maatwerk kan worden gerealiseerd. Indien de aard en kenmerken van de elektronische dienstverlening van een organisatie van dien aard is, dat voor de toegang ter zake niet langer hoogbetrouwbare authenticatie nodig is, zal het desbetreffende aanwijzingsbesluit worden ingetrokken.

Wanneer aanwijzen?

In welke gevallen worden (categorieën) van organisaties aangewezen? Bepalend is de aard van de dienstverlening die wordt verricht. Zo komt een deel van de organisaties die het bsn gebruiken niet voor aanwijzing op grond van onderhavig wetsvoorstel in aanmerking, omdat zij überhaupt geen elektronische diensten aan burgers verlenen, danwel weliswaar elektronische diensten verlenen, maar geen diensten waarvoor elektronische authenticatie op het niveau «substantieel» of «hoog» noodzakelijk is. Ook is het mogelijk dat een sector of een organisatie al een eigen systeem van betrouwbare en veilige authenticatie kent, waardoor er geen noodzaak tot aanwijzing bestaat.

Voor aanwijzing komen daarmee primair in aanmerking organisaties die:
a. elektronische diensten verlenen waarbij inzicht kan worden gegeven in de (huidige of toekomstige) financiële (inkomens)situatie van betrokkene;
b. elektronische diensten verlenen met periodieke financiële aanspraken;
c. elektronisch diensten verlenen met betrekking tot medische gegevens en/of medicijnen, of de ingediende declaraties voor zorg of medicijnen.

De bijlage

Voor de vaststelling van de bijlage is als vertrekpunt genomen de lijst van organisaties die thans het bsn verwerken en diensten verlenen waartoe toegang met gebruikmaking van DigiD mogelijk is. Per saldo heeft dit opgeleverd, dat in de bijlage vooralsnog de volgende categorieën van instanties zijn aangewezen: de pensioenuitvoerders, zorgaanbieders, de ziektekostenverzekeraars, indicatieorganen en de universiteiten en hogescholen.

Consequentie van aanwijzing en niet aanwijzing.

De belangrijkste consequentie van de aanwijzing is dat de organisaties alle toegelaten en erkende middelen, zowel publiek als privaat, moeten accepteren voor hun elektronische dienstverlening op betrouwbaarheidsniveau substantieel en hoog. Het is echter in principe aan deze organisaties zelf om te bepalen *of* zij diensten elektronisch aanbieden, tenzij uit een wettelijk voorschrift voortvloeit dat zij hiertoe verplicht zijn. Uit de aanwijzing in de zin van de onderhavige wet vloeit derhalve geen verplichting tot het aanbieden van elektronische diensten voort. Aan de andere kant zullen slechts organisaties worden aangewezen die elektro-

nisch diensten op het betrouwbaarheidsniveau substantieel of hoog aanbieden.

Andere uit dit wetsvoorstel voortvloeiende consequenties van de aanwijzing zijn, dat de betrokken organisaties voor hun diensten moeten bepalen wat het betrouwbaarheidsniveau is, dat zij moeten voldoen aan bij of krachtens algemene maatregel van bestuur te stellen regels met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang tot de elektronische dienstverlening en dat ze dit moeten laten *auditen*. Ook kunnen ze de (toegelaten en erkende) publieke en private middelen accepteren voor dienstverlening waarvoor een laag betrouwbaarheidsniveau geldt.

Dat een organisatie niet wordt aangewezen, betekent niet dat deze helemaal geen toegelaten identificatiemiddelen kan gebruiken bij de (toegang tot haar) dienstverlening. Toegelaten publieke middelen mogen in beginsel uitsluitend gebruikt worden voor de toegang tot elektronische dienstverlening door bestuursorganen en aangewezen organisaties. Voor toegelaten private middelen geldt deze beperking echter niet.

3.5. Identificatiemiddelen voor burgers

Elektronische dienstverlening vs toegang daartoe

Het verlenen van elektronische diensten *als zodanig* behoort tot de verantwoordelijkheid van het desbetreffende bestuursorgaan of de desbetreffende aangewezen organisatie. In dat verband kan in beleid en regelgeving worden voorzien door de Ministers wie het aangaat. De Minister van BZK van BZK heeft hiermee inhoudelijk geen bemoeienis. Dit wetsvoorstel moet derhalve worden onderscheiden van sectorale ontwikkelingen op het gebied van digitalisering; het wetsvoorstel als zodanig verplicht niet tot elektronische dienstverlening op bepaalde beleidsterreinen en verplicht burgers niet tot elektronische afname van diensten. Het wetsvoorstel geeft slechts regels *voor het geval* diensten – al dan niet onder uitsluiting van de schriftelijke weg – elektronisch worden aangeboden door bestuursorganen of aangewezen organisaties. Met andere woorden: dit wetsvoorstel maakt het mogelijk dat elektronische dienstverlening op verschillende betrouwbaarheidsniveaus wordt ontsloten. Primair van belang hierbij is dat de Minister van BZK voorziet in veilige en betrouwbare toegang tot die elektronische dienstverlening. Het is om die reden dat hij onder meer verantwoordelijk is voor de uitgifte van publieke identificatiemiddelen en voor de toelating van eventuele private identificatiemiddelen. Dit brengt met zich, dat wordt gestreefd naar een brede beschikbaarheid van (publieke én private) elektronische identificatiemiddelen op de verschillende, hogere, betrouwbaarheidsniveaus, opdat de daadwerkelijke toegang van burgers tot – sectoraal aangeboden – elektronische dienstverlening gewaarborgd is.

Gelet op het voorgaande, alsmede op de trend om steeds vaker in contacten met dienstverleners elektronische communicatie verplicht te stellen, is het van belang een zo ruim mogelijke kring van rechthebbenden op de publieke identificatiemiddelen te realiseren. Hierbij is sprake van een groeimodel. Er worden op dit moment twee publieke middelen op een hoog betrouwbaarheidsniveau ontwikkeld waarbij de Nederlandse identiteitskaart (NIK) en het rijbewijs de drager zijn. De bestaande chip in deze dragers wordt uitgerust met de daarvoor noodzakelijke functionaliteit (applet) om elektronische authenticatie mogelijk te maken. Inherent aan de keuze om de NIK 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 in het bezit is van dan wel

recht heeft op een NIK of een Nederlands rijbewijs. Naast deze twee middelen op betrouwbaarheidsniveau hoog, zal een publiek middel op betrouwbaarheidsniveau substantieel beschikbaar komen, dat niet geplaatst is op een fysieke drager maar dat een versterkte versie van het huidige DigiD behelst. Hiervoor is thans wel een elektronisch uitleesbaar identiteitsdocument (WID) noodzakelijk.

Het streven is er op gericht dat in de toekomst voor alle personen met een bsn[35] een elektronisch identificatiemiddel op de betrouwbaarheidsniveaus substantieel en hoog beschikbaar komt. Voor burgers die niet de beschikking kunnen hebben over een geschikt identiteitsdocument, wordt onderzocht op welke andere wijze(n) zij een middel op de betrouwbaarheidsniveaus substantieel en hoog kunnen verkrijgen.
Bij het beschikbaar komen voor de afzonderlijke groepen spelen beleidsmatige, juridische, technische en financiële overwegingen een rol. Hoewel hiermee voor een bepaalde periode een zekere ongelijkheid ontstaat, is het feit dat een groep personen nog geen toegang heeft tot een publiek middel op een hoger betrouwbaarheidsniveau, geen reden om dit middel te onthouden aan personen die wel in het bezit zijn van de benodigde identiteitsdocumenten respectievelijk een NIK of rijbewijs kunnen aanschaffen. Bovendien is het aan de beleidsverantwoordelijke Minister om in voorkomende, sectorspecifieke, gevallen de digitale weg niet verplicht te stellen, danwel met een beroep op de noodzaak van een alternatieve inlogmethode de Minister te verzoeken een afwijkende regeling terzake vast te stellen ingevolge artikel 7, derde lid, van het wetsvoorstel.[36]

Gelet op de dynamiek van de bovenstaande ontwikkelingen bevat dit wetsvoorstel zelf geen regeling over de categorieën van personen die in aanmerking komen voor de publieke elektronische identificatiemiddelen. Voor wat betreft deze middelen zal dit – analoog aan de wijze waarop dit reeds met betrekking tot 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 met betrekking tot het uitgifteproces en de in dat verband te verifiëren identiteitsdocumenten.

Gebruik publiek middel in publieke domein

Het behoort niet tot de taak van de rijksoverheid om publieke middelen te ontwikkelen en uit te geven die ook voor strikt commerciële transacties als het online kopen van kleding, boeken of meubelen gebruikt kunnen worden. De regering acht het onwenselijk indien de rijksoverheid zich zou mengen in deze markt. Het uitgangspunt dat publieke middelen niet buiten het publieke of semipublieke domein worden gebruikt, is daarom in het wetsvoorstel opgenomen. Wel is bij wijze van uitzondering onder strikte voorwaarden gecombineerde elektronische dienstverlening door welbepaalde aangewezen organisaties mogelijk (artikel 8, tweede lid) alsmede het gebruik van een publiek middel ten behoeve van welbepaalde aangewezen organisaties voor het verlenen van toegang tot een (intern) systeem voor de elektronische uitwisseling van gegevens (artikel 8, derde lid).

---

[35] *Dit zijn: de ingeschrevenen in de BRP, ongeacht of deze als ingezetene of niet-ingezetene zijn ingeschreven. Met het bsn als uniek persoonsgebonden nummer kan onder andere met de (semi)overheid gecommuniceerd worden.*

[36] *Deze situatie moet worden onderscheiden van de situatie dat burgersrechthebbende op een publiek middel zijn, maar ondersteuning nodig hebben bij hun digitale communicatie met de overheid. Hiertoe kan machtiging uitkomst bieden. Zie ook het voorgestelde artikel 2.13 Awb.*

BSN-Koppelregister en routeringsvoorziening

Het BSN-Koppelregister (BSN-K) en de routeringsvoorziening zijn generieke voorzieningen.
De Minister van BZK is verantwoordelijk voor de werking, betrouwbaarheid en veiligheid ervan. Het BSN-K speelt een rol in het identificatieproces door een koppeling te leggen tussen een elektronisch identificatiemiddel en het bsn van de houder. Het BSN-K stelt een authenticatiedienst hierdoor in staat om een dienstverlener op een veilige en betrouwbare manier het burgerservicenummer (bsn) te leveren van een gebruiker van een identificatiemiddel. Het BSN-K stelt daarnaast de burger in staat om met behulp van een inzagefunctie informatie te krijgen over zijn identificatiemiddelen. Een burger kan aldus vaststellen of zijn identificatiemiddel actief is of is geweest binnen het publieke domein. De inzagefunctie biedt alleen de desbetreffende burger inzicht in de status van het identificatiemiddel (bijvoorbeeld: actief, inactief of ingetrokken).
Het BSN-K is een reeds bestaande voorziening.
De routeringsvoorziening is generieke voorziening die thans wordt ingericht en waarmee verschillende koppelvlakken (verbindingen die volgens een bepaalde standaard de uitwisseling van gegevens tussen informatiesystemen mogelijk maken) zullen worden ontsloten, waardoor bestuursorganen en aangewezen organisaties eenvoudig kunnen aansluiten op de verschillende identificatiemiddelen voor burgers – publieke, private, Europese – die zij moeten accepteren. Aldus worden zij bij hun elektronische dienstverlening aan burgers «ontzorgd». De Minister van BZK kan toestaan dat dienstverleners (tijdelijk) aansluiten op een andere routeringsvoorziening dan bovengenoemde routeringsvoorziening, teneinde het accepteren van toegelaten middelen door dienstverleners te faciliteren.

3.6. Identificatiemiddelen voor bedrijven

Dienstverlening door bestuursorganen en aangewezen organisaties richt zich zowel op burgers (natuurlijke personen) als op bedrijven (ondernemingen en rechtspersonen). Wel zijn er enkele verschillen tussen de mogelijkheden voor authenticatie voor de dienstverlening aan burgers en aan bedrijven. Publieke middelen zijn bedoeld om als burger in contact te komen met bestuursorganen en aangewezen organisaties. Indien een KvK-nummer[1] of RSIN-nummer[2] vereist is voor authenticatie, kan niet 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 bedrijf (niet zijnde de eigenaar van een eenmanszaak) veelal niet het geval. Voor het handelen als bedrijf is destijds het stelsel voor eHerkenning ontwikkeld. Het aantal op eHerkenning aangesloten overheidsorganisaties en het aantal transacties groeit gestaag. In 2016 was al meer dan de helft van de gemeenten aangesloten op eHerkenning naast een dertigtal toepassingen bij de rijksoverheid waaronder het Omgevingsloket *online* en de VOG-verklaring. Medio 2017 hebben enkele grote uitvoeringsorganisaties, waaronder Belastingdienst en UWV, een intentie-overeenkomst getekend waarin zij aangeven vanaf eind 2017 gefaseerd een deel of al hun digitale diensten met eHerkenning te ontsluiten.

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 bijna 6 miljoen authenticaties in 2016. In 2013 was dit aantal nog circa een miljoen. Het aantal uitgegeven eHerkenningsmiddelen steeg eind 2016 tot ca. 275.000. Ultimo 2013 waren er 94.000 eHerkenningsmiddelen uitgegeven. Van de eHerkenningsmid-

delen wordt inmiddels de helft gebruikt voor meer dan één toepassing. Er waren eind 2016 ongeveer 200.000 ondernemers, die een of meer inlogmiddelen van eHerkenning hadden aangeschaft, tegen 81.000 ultimo 2013. De eHerkenningsmiddelen die thans worden gebruikt, zullen op grond van dit wetsvoorstel erkend moeten worden door de Minister van BZK 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 bedrijven eisen worden gesteld. Daarbij is sprake van dezelfde betrouwbaarheidsniveaus als voor de middelen voor burgers. In wezen zijn het vergelijkbare middelen. Maar daar waar een middel voor burgers wordt gekoppeld aan een bsn, wordt dit bij middelen voor bedrijven gekoppeld aan een KvK- of RSIN-nummer. En waar een burger in beginsel voor alles wat hemzelf betreft bevoegd is, zal, net als nu al het geval is, bij een middel voor een bedrijf vastgelegd worden waarvoor de betreffende gemachtigde 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.

Bij de uitgifte van middelen voor bedrijven 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 het bedrijf. 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 bedrijven wordt uitgegeven, moet de authenticatiedienst vaststellen 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 bedrijven en burgers of alleen voor bedrijven of alleen voor burgers uit te geven. Publieke authenticatiediensten geven alleen middelen voor natuurlijke personen uit.

3.7. Samenloop van identificatiemiddelen

Ten aanzien van ondernemingen die toebehoren aan een natuurlijk persoon (er is dan sprake van een natuurlijk persoon in de uitoefening van beroep of bedrijf), is er voor de dienstverlener ten aanzien van die ondernemingen in beginsel de keuze om bij zijn dienstverlening een bedrijfs- en organisatiemiddel te verlangen dan wel om tevens toe te staan dat een identificatiemiddel voor burgers wordt gebruikt. Deze vrijheid van dienstverleners om hun dienstverlening naar eigen inzicht in te richten, kan echter vanuit het oogpunt van de ondernemer in de praktijk tot ondoelmatige werkwijzen leiden. Met name als er binnen een bepaalde sector geen eenduidige keuze wordt gemaakt. Dan kan het met het oog op het voorkomen van onnodige kosten voor verschillende middelen voor één ondernemer en rompslomp in de uitvoering door het steeds moeten wisselen van verschillende soorten middelen door één ondernemer, wenselijk zijn dat de betrokken bestuursorganen en aangewezen organisaties worden verplicht ook een identificatiemiddel voor burgers

(toegelaten middel) te accepteren. Om die reden bevat het wetsvoorstel de mogelijkheid om dit te reguleren in overeenstemming met de betrokken Ministers die verantwoordelijk zijn voor de beleidsterreinen waarop de betrokken dienstverleners respectievelijk de betrokken ondernemingen werkzaam zijn.

4. Privacy

Het wetsvoorstel bevat tevens regels om de bescherming van de persoonlijke levenssfeer te waarborgen. De in dit wetsvoorstel genoemde adressaten (Ministers, bestuursorganen en aangewezen organisaties, private partijen) verwerken ten behoeve van goede toegang tot elektronische dienstverlening en, in het verlengde daarvan, het voorkomen van misbruik of oneigenlijk gebruik van de toegang tot elektronische dienstverlening, persoonsgegevens en dienen derhalve aan geldende privacy wet- en regelgeving te voldoen. Teneinde de persoonlijke levenssfeer te beschermen beoogt het wetsvoorstel daarom tevens eisen te stellen inzake verwerking, beveiliging en betrouwbaarheid van persoonsgegevens. Deze eisen, waarin privacybeginselen zijn vervat, zullen, in toenemende mate, in de architectuur vam de stelsels – identificatiemiddelen, private en publieke voorzieningen en bijbehorende interne systemen en werkprocessen – moeten worden verdisconteerd en door de betrokken partijen moeten worden meegenomen. Bij nieuwe ontwerpen dient ook «*privacy by design»* te worden gerealiseerd.
De volgende beginselen komen daarin naar voren:

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

Rond deze beginselen zullen de benodigde gegevensverwerkingen verder worden gekaderd in de uitvoering. Deze zullen voorts in het functioneel ontwerp van de systemen (techniek en processen) hun beslag krijgen, conform het wettelijk kader inzake de bescherming van persoonsgegevens. De Algemene verordening gegevensbescherming (hierna: AVG) vormt het voornaamste kader.[37]

[37] *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 Richtlijn 95/46/EG.*

De Algemene verordening gegevensbescherming (AVG)

De AVG is sinds 25 mei 2018 rechtstreeks van toepassing. Met de Uitvoeringswet Algemene verordening gegevensbescherming is de Wet bescherming persoonsgegevens ingetrokken.

Privacybepalingen in dit wetsvoorstel in relatie tot de AVG

Dit wetsvoorstel bevat bepalingen die een aanvulling zijn op de waarborgen van de AVG. Deze regels, waartoe de AVG ruimte biedt, zijn noodzakelijk om een goede uitvoering van de AVG te bewerkstelligen. Er worden regels gesteld inzake grondslagen, doelen, waarborgen en beveiliging alsmede worden taken, verantwoordelijkheden en bevoegdheden voor de betrokken Ministers vastgelegd. Ook bevat het verplichtingen voor bestuursorganen en aangewezen organisaties en voor private partijen. De grondslag om persoonsgegevens te verwerken vloeit voort uit deze bepalingen, in samenhang met artikel 6, eerste lid, onder e, van de AVG. In het wetsvoorstel zijn grondslagen neergelegd voor de verwerking van persoonsgegevens door de genoemde adressaten voorzover dat noodzakelijk is voor de uitvoering en het verlenen van veilige toegang tot elektronische dienstverlening. Krachtens het wetsvoorstel zullen nadere regels worden gesteld, waaronder over de verstrekking van persoonsgegevens en de bewaartermijnen die in acht moeten worden genomen. In dit verband zal het Besluit verwerking persoonsgegevens GDI worden uitgebreid en gewijzigd. Reden voor het regelen van de verwerking van persoonsgegevens bij algemene maatregel van bestuur is het feit, dat het wetsvoorstel het karakter heeft van een kaderwet waarin hoofdzaken zijn geregeld en het om redenen van flexibiliteit opportuun is gedetailleerde (technische) uitwerking in de uitvoering vorm te geven. In dit verband kan tevens worden aangesloten bij hetgeen reeds is neergelegd in bestaande regelgeving op het gebied van de verwerking van persoonsgegevens terzake van GDI-voorzieningen, te weten voornoemd besluit. Bij de nadere uitwerking zullen onder meer de beginselen van proportionaliteit en subsidiariteit leidend zijn. Het wetsvoorstel en de daarop gebaseerde algemene maatregel van bestuur werken, waar mogelijk, nodig en passend, de normen van de AVG uit. Deze nationale normen met betrekking tot onder meer grondslagen, doelen, waarborgen en beveiliging zijn noodzakelijk zijn om een goede uitvoering van de AVG te bewerkstelligen.[38] Voor alles wat dit wetsvoorstel en het daarop gebaseerde besluit 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 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 gegevensbeschermingseffectbeoor-

[38] *Bij algemene maatregel van bestuur wordt bijvoorbeeld geconcretiseerd welke bewaartermijnen gelden, omdat de AVG hieromtrent geen concrete eisen stelt. Het uitgangspunt van de AVG is dat persoonsgegevens niet langer mogen worden bewaard dan noodzakelijk voor het doel van uw verwerking. Hoe lang gegevens mogen worden bewaard, verschilt dus per geval waardoor uitwerking in nationale regels geboden is.*

deling (PIA)[39] voorafgaand aan de verwerking dient te worden uitgevoerd. In het onderstaande wordt ingegaan op de wijze waarop hiermee bij de toegang tot elektronische dienstverlening rekening is gehouden.

Privacy-by-design en uitvoering gegevensbeschermingseffectbeoordeling

Bij de voorbereiding van dit wetsvoorstel is een aantal maatregelen getroffen om een effectieve toepassing van de AVG te borgen. Belangrijk is het gedurende de voorbereiding meermalen uitvoeren van een PIA, 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 ontwerp van de betrokken voorzieningen. Ter zake zij verwezen naar de rapportage van de PIA inzake het eID-stelsel van 28 juni 2017.[40] Daarnaast is ervoor gezorgd dat de (technische) inrichting plaatsvindt volgens de privacyeisen die voortvloeien uit de AVG, waaronder het vormgeven van een functionaliteit ten behoeve van inzage voor de houder van een identificatiemiddel waarvan gegevens worden verwerkt. De belangrijkste aanpassingen als gevolg van de uitgevoerde PIA's betreffen de functionaliteit die de houder van een toegelaten identificatiemiddel inzage biedt in de status van dit middel en het feit, dat de gegevensverwerking (technisch) zodanig wordt ingericht, dat geen van de bij authenticatie betrokken partijen (inclusief dienstverleners) kan zien welke andere websites door de houder van het middel worden bezocht. Dit is niet alleen belangrijk voor de bescherming van persoonsgegevens als zodanig, maar doet tevens recht aan de wens dat de betrokken partijen geen inzicht in of bemoeienis moeten kunnen hebben met zaken die gebruikers in het publieke domein afwikkelen. De PIA's hebben ook input geleverd voor de nog op te stellen uitvoeringsregelgeving bij dit wetsvoorstel en onderschrijving van verwerkingsgrondslagen in het wetsvoorstel voor het gebruik van het bsn door private partijen. Bij de verdere inrichting en ontwikkeling zullen er regulier PIA's worden uitgevoerd. De uitkomsten hiervan beogen doorlopende en blijvende expliciete aandacht voor privacybescherming, waaronder technische, procedurele, beleidsmatige en juridische maatregelen.

Transparantie

In hoofdstuk III van de AVG, waarin de rechten van burgers worden geregeld, zijn transparantievoorschriften opgenomen. Artikel 12 AVG stelt regels aan de begrijpelijkheid van informatie en communicatie over de verwerkingen van persoonsgegevens zodat burgers daadwerkelijk in staat worden gesteld om hun rechten uit te oefenen. Daarbij wordt een onderscheid gemaakt tussen het geval dat de verkrijging van de gegevens bij de burger zelf plaatsvindt (artikel 13 AVG) en dat waarbij de gegevens niet bij hem zijn verkregen (artikel 14 AVG). Ingevolge dit wetsvoorstel en de bijbehorende uitvoeringsregelgeving vindt het verkrijging van de gegevens op beide wijzen plaats. Bij aanvraag en registratie van identificatiemiddelen 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 burger om wordt verkregen, bijvoorbeeld gegevens die nodig zijn om de juistheid van gegevens te controleren, zoals de controle van de identiteit door het

---

[39] *PIA staat voor Privacy Impact Assessment. Het betreft 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, aanbevelingen worden gedaan om deze risico's te elimineren of te mitigeren en maatregelen worden genomen in (technische) architectuur, processen en regelgeving.*

[40] *Bijlage bij Kamerstukken II 2016/2017, 26 643 nr. 481.*

BSN-K. De Minister van BZK en de andere betrokkenen bij de toegang tot elektronische dienstverlening zullen uitvoering (moeten) geven aan de transparantieverplichtingen door een privacyverklaring op hun website te plaatsen. Hierin 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 een link worden opgenomen naar de bijbehorende wet- en regelgeving, waaronder deze wet en bijbehorende uitvoeringsregelgeving.

Het recht van inzage en rectificatie

Op grond van artikel 15 AVG heeft een burger 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 AVG heeft hij het recht de verantwoordelijke te verzoeken hem betreffende gegevens te rectificeren, gegevens te wissen, of de verwerking te beperken. De wijze waarop uitvoering wordt gegeven aan deze rechten, zal worden vastgelegd in uitvoeringsregelgeving op basis van dit wetsvoorstel en in de op te stellen privacyverklaringen die op de betrokken websites zullen worden geplaatst.

Grondslagen en beginselen voor verwerking van persoonsgegevens

Uit de AVG volgt dat de verzameling en verwerking van persoonsgegevens plaatsvindt op een rechtmatige en behoorlijke wijze (artikel 5, eerste lid AVG). Voorts dienen de doeleinden waarvoor verzameling en verwerking plaatsvindt gerechtvaardigd, welbepaald en uitdrukkelijk omschreven te zijn (doelbinding). De verwerkingen worden uitgevoerd door de betrokken Ministers en door bestuursorganen en aangewezen organisaties in het kader van de hen toegekende taken, en door specifiek genoemde private partijen indien dit noodzakelijk is voor de goede uitvoering van de wet. De verwerkingen vinden plaats teneinde veilige en betrouwbare toegang tot elektronische dienstverlening te realiseren. De verwerkingsdoelen worden beslagen door de onderscheiden artikelen in het wetsvoorstel. 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). Het wetsvoorstel bevat voorts de grondslag voor nadere regelgeving; hierin zullen de beginselen zoals hieronder aangegeven worden uitgewerkt.

Verwerking bsn

De AVG kent enkele bepalingen in verband met specifieke situaties op het gebied van gegevensverwerking, waaronder de verwerking van het nationaal identificatienummer. 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 te stellen voor de verwerking van een nationaal identificatienummer. De Uitvoeringswet AVG regelt het gebruik van wettelijk voorgeschreven nummers, overeenkomend met het huidige artikel 24 van de Wbp. Dit betekent dat voor de verwerking van het bsn dient te worden voorzien in een wettelijke grondslag. Om deze reden is in het wetsvoorstel opgenomen dat het bsn door de genoemde betrokkenen mag worden verwerkt voorzover dat noodzakelijk is voor de goede uitvoering van hun taken en verplichtingen ingevolge deze wet (artikel 16 lid 1; Ministers), voor een goede elektronische dienstverlening (artikel 16 lid 1; dienstverleners), voor de goede uitvoering van deze wet (artikel 16 lid 2; private

partijen) en voor de goede werking van het bedrijfs- en organisatiemiddel en goede toegang met dat middel tot elektronische dienstverlening (artikel 16 lid 3; private partijen). Daarbij geldt dat gebruik van het bsn tot een minimum wordt beperkt en zoveel mogelijk wordt gewerkt met pseudonimisering en versleuteling.

Dataminimalisatie

De gegevens die voor de toegang tot elektronische dienstverlening worden verwerkt moeten toereikend en terzake dienend zijn. Daarbij gaat het om proportionaliteit en subsidiariteit, waardoor een minimum aan verwerking van persoonsgegevens wordt gerealiseerd (artikel 5, lid 1, onder c, AVG). In de uitvoeringsregelgeving zal dit 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). In de uitvoeringsregelgeving zullen regels worden gesteld over de wijze waarop hieraan invulling wordt gegeven.

Opslagbeperking (bewaartermijnen)

Een belangrijk uitgangspunt is 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, AVG). In de uitvoeringsregelgeving zullen bewaartermijnen worden vastgelegd.

Beveiliging van persoonsgegevens

Bij de verwerking van persoonsgegevens voor toegang tot elektronische dienstverlening moeten technische en organisatorische maatregelen 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 uit. Bepaald wordt dat, waar passend, pseudonimisering en versleuteling dienen 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. De AVG bevat in artikel 33 tot slot de verplichting om melding te maken van een inbreuk in verband met persoonsgegevens.

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.

5. Misbruik van de GDI

5.1. Inleiding

In 2013[41] is 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.[42] Ramingen zijn 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.[43]

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.

5.2. Aanpak van misbruik en identiteitsfraude

Dit wetsvoorstel, de bijbehorende uitvoeringsregelgeving en de voorschriften die aan private aanbieders van toegelaten en erkende identificatiemiddelen en – diensten zullen worden opgelegd, zijn gericht op realisering van een betrouwbaar proces bij de inrichting van de toegang tot elektronische dienstverlening door de (semi)overheid. 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. Uiteraard moet ook de houder (gebruiker) van een uitgegeven identificatiemiddel zelf maatregelen nemen om misbruik, diefstal, verlies of verspreiding van zijn elektronisch identificatiemiddel te voorkomen en is het gebruiken van een elektronisch identiteitsmiddel, dat toebehoort aan een ander, verboden.[44]

---

[41] *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*

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

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

[44] *De artikelen 231 e.v. van het Wetboek van Strafrecht (Sr.) stellen verschillende vormen van identiteitsfraude strafbaar.*

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 en de betrouwbaarheid borgen. Het nemen van maatregelen door de aanbieders van toegelaten of erkende identificatiemiddelen en van erkende diensten en door 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, alsmede door de Minister te nemen (nood)maatregelen, bijvoorbeeld het onderbreken van de toegang tot elektronische dienstverlening via een welbepaald middel bij het vermoeden van misbruik of oneigenlijk gebruik en het onderbreken (afsluiten) van de toegang tot 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, bedrijven en overheden beschermd.

5.3. Herstel- en noodmaatregelen

In geval van herkend (geconstateerd) misbruik of waarschijnlijke mogelijkheid daartoe zal een toegelaten of erkende private partij, 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. Gelet op de mogelijke impact die dergelijke maatregelen kunnen hebben zal bij de (risico)afweging advies worden ingewonnen bij ter zake kundigen.
Voor de volledigheid wordt opgemerkt dat de hieronder beschreven maatregelen een reparerend en beschermend karakter hebben. Zij dienen geen punitief (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 bedrijven), dienstverleners, toegelaten of erkende private partijen, danwel kunnen gericht zijn op bescherming van de toegang tot elektronische dienstverlening zelf.

In het wetsvoorstel wordt erin 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 nemen.

Maatregelen ten behoeve van- en gericht tot gebruikers

In de wet wordt gesproken over «onderbreken» om aan te geven dat het om een tijdelijke maatregel gaat die zich richt op tijdelijke onbruikbaarheid van een identificatiemiddel. Bij onderbreking is «deblokkering» van een middel mogelijk, waardoor het gebruik kan worden voortgezet. Van «intrekking» of «revocatie» wordt gesproken om aan te geven dat een gebruik van een identificatiemiddel definitief onbruikbaar wordt gemaakt.

Voor hernieuwd gebruik of toegang dient opnieuw een middel te worden aangevraagd.

Onderbreking van een identificatiemiddel voor een gebruiker

Een herstelmaatregel gericht op burgers en bedrijven kan zijn het tijdelijk blokkeren van een welbepaald identificatiemiddel. Dit kan worden ingezet op het moment dat er aanwijzingen zijn dat bijvoorbeeld een identificatiemiddel 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 worden gedeblokkeerd, waarna het 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 identificatiemiddel uiteindelijk wordt ingetrokken.

Intrekken van identificatiemiddelen wegens misbruik[45]

Hierbij moet gedacht worden aan het intrekken van identificatiemiddelen 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 identiteitsfraudes met DigiD waarbij DigiD codes van gebruikers uit brievenbussen zijn gehengeld en vervolgens misbruikt.[46]

Onderbreking van de toelating of erkenning

In het wetsvoorstel is de mogelijkheid voorzien om als tijdelijke maatregel een toegelaten of erkende partij te onderbreken (uit de lucht te halen, schorsen), als deze niet aan de hem opgelegde (veiligheids)eisen voldoet.

Onderbreking van toegang tot dienstverlening

Ten slotte is het voor de Minister mogelijk om voor een of meer dienstverleners 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 de aanleiding gevormd voor het instellen van de beveiligingsassessments, waarmee is beoogd om deze situaties zoveel mogelijk te voorkomen.

---

[45] *Intrekking van een middel kan ook om andere redenen plaatsvinden, zoals bij overlijden van een gebruiker. In deze paragraaf wordt revocatie voor misbruikbestrijding bedoeld.*

[46] *http://www.ad.nl/amsterdam/amsterdammers-slachtoffer-van-fraude-digid~aaebcb30/*

5.4. 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 toegelaten en erkende partijen 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 identificatiemiddel, 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 het wetsvoorstel is voor de Minister de mogelijkheid opgenomen om bij bestuursorganen en aangewezen organisaties en bij (private) aanbieders van een toegelaten identificatiemiddel en een erkend identificatiemiddel of erkende dienst 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 zijn 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 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 private aanbieders van toegelaten middelen of 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 te verstrekken is geregeld in het wetsvoorstel. Misbruikbestrijding wordt in het onderhavige wetsvoorstel vormgegeven als een operationele beheertaak. Dit betekent dat herkenning van misbruik en het treffen van herstel- en noodmaatregelen de verantwoordelijkheid is van alle betrokkenen in de keten. Het toezicht 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 organisatie operationeel in staat is om

misbruik te bestrijden. Dit houdt overigens in dat de organisatie informatie moet kunnen verschaffen waaruit dit aantoonbaar blijkt.

6. Toezicht en handhaving

6.1. Inleiding

Het toezicht op de naleving van de verplichtingen in dit wetsvoorstel richt zich niet rechtstreeks op burgers. Burgers bepalen zelf of ze toegelaten publiek of privaat inlogmiddel willen gebruiken. De Minister van BZK kan op verzoek van een burger diens DigiD laten blokkeren of opheffen. Voorts kan de Minister de toegang tot elektronische dienstverlening via een bepaald middel onderbreken bij het vermoeden van misbruik of oneigenlijk gebruik van het desbetreffende middel. Indien een privaat middel is toegelaten worden signalen van fraude of misbruik gedeeld met de verantwoordelijke aanbieder van een privaat inlogmiddel teneinde het middel in de voorkomende gevallen te laten blokkeren.

6.2. Toezicht op bestuursorganen en aangewezen organisaties

De digitale dienstverlening van bestuursorganen en aangewezen organisaties is allereerst een aangelegenheid van de desbetreffende organen en organisaties zelf. Een goede taakuitvoering door hen vergt ook naleving van de aan hen gestelde normen, zoals de acceptatieplicht en het voldoen aan de eisen met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang tot de elektronische dienstverlening. Voorts geldt voor bestuursorganen (en eventueel rechtspersonen met een wettelijke taak) het verplicht gebruik van bij algemene maatregel van bestuur voorgeschreven standaarden. Voor wat betreft de naleving van deze wet door bestuursorganen, aangewezen organisaties (en rechtspersonen met een wettelijke taak waar het de open standaarden betreft) geldt het reguliere toezicht en de reguliere ministeriële verantwoordelijkheid. Voor de overheidsorganen op niveau van het rijk en de aangewezen organisaties is daarbij voorzien in het aanwijzen van toezichthouders. In deze paragraaf zal worden ingegaan op wat dat betekent voor de verschillende dienstverleners.

De centrale overheid

Waar de ministeries zelf als dienstverlener uitvoering geven aan het wetsvoorstel, is het aan de betrokken Ministers er voor zorg te dragen dat de eigen uitvoeringsorganisaties, 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. Dit wetsvoorstel creëert geen nieuwe, formele toezichtsbevoegdheden ten aanzien van deze zelfstandige bestuursorganen. Dit betekent dat de Minister, ook al is deze overheidstaak op afstand gezet, vanuit zijn algemene ministeriële verantwoordelijkheid de betrokken zelfstandige bestuursorganen zo nodig tot naleving dient te bewegen.

De aangewezen organisaties

Het streven is om het toezicht op de aangewezen organisaties en overheidsorganen op het niveau van het rijk ook zo veel als mogelijk binnen de bestaande toezichtstructuren en met gebruik van bestaande instrumenten te laten plaatsvinden. Om dit te kunnen realiseren, is de vakminister op grond van dit wetsvoorstel gehouden om personen aan te

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

De decentrale overheden

In lijn met de Wet revitalisering generiek toezicht is het toezicht van de hogere overheid op de naleving van het 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 binnen een bestuurslaag. Het gaat dan om het toezicht op een juiste en toereikende naleving. In de tweede plaats komt pas het interbestuurlijk toezicht op de decentrale overheden, conform het beginsel dat slechts één bestuurslaag – de naast hoger gelegen bestuurslaag – toezicht houdt. In lijn met dit beginsel houdt de Minister toezicht op overheidsorganen op het niveau van de provincies en houden provincies toezicht op overheidsorganen op het niveau van gemeenten. Dit wetsvoorstel verplicht het provincies om de Minister te informeren over de (mate van) naleving door overheidsorganen op het niveau van gemeenten. Het interbestuurlijk toezicht biedt de naast hoger gelegen bestuurslaag (uitsluitend) 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 in uiterste gevallen indeplaatsstelling (bij taakverwaarlozing).

Toezicht op informatieveiligheid bij dienstverleners door middel van 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. Om die reden kent het toezicht op de naleving van de eisen aan de werking, betrouwbaarheid en beveiliging van de toegang van de elektronische dienstverlening van de bestuursorganen en aangewezen organisaties, naast de bestaande toezichtstructuren, een aanvullende verplichting. In aanvulling op het generiek toezicht moet het bestuursorgaan of de aangewezen organisatie regulier een verklaring van een auditor aan de Minister overleggen. Deze auditor toetst of de dienstverlener aan de eisen voldoet. De verklaring van de auditor sluit aan bij de 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 te sturen. In lijn met de huidige praktijk bieden de auditverklaringen allereerst een handvat voor gesprek en verdere afspraken over de benodigde verbeteringen. Wanneer uit de rapporten van de auditor gebrekkige naleving blijkt of bestuurlijke afspraken stelselmatig niet nagekomen worden, kan de Minister tegen medeoverheden optreden.

Afsluiting

Als uit de te overleggen auditverklaringen blijkt, 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 of ook na aanmaningen de benodigde verbeteringen niet worden aangebracht, zal als uiterste middel de bevoegdheid tot het (doen) onderbreken van de toegang tot elektronische dienstver-

lening van een bestuursorgaan of een aangewezen organisatie uitkomst bieden. Ook het niet overleggen van een auditverklaring of anderszins gebrekkig naleven van de bij of krachtens algemene maatregel van bestuur te stellen regels met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang tot elektronische dienstverlening, in stand houden, kan aanleiding vormen om bestuursorganen of aangewezen organisaties af te sluiten van het gebruik van een publiek identificatiemiddel of een toegelaten privaat middel.

6.3. Controle op naleving van eisen m.b.t. een toegelaten eID-middel voor burgers

Op basis van artikel 9 van de wet kan de Minister van BZK een privaat uitgegeven inlogmiddel verwerven en bij besluit aanwijzen als toegelaten inlogmiddel bij digitale dienstverlening van bestuursorganen en aangewezen organisaties. Om te kunnen fungeren als inlogmiddel bij digitale dienstverlening in het (semi)publiek domein, moeten de middelen voldoen aan de eisen van de Minister van BZK. Vanzelfsprekend zullen deze eisen uitgaan van hetzelfde veiligheids- en betrouwbaarheidsniveau als terzake van publieke identificatiemiddelen (zie toelichting bij lid 1). Indien aan de eisen is voldaan komt het middel in aanmerking voor aanwijzing als toegelaten identificatiemiddel voor de digitale dienstverlening van bestuursorganen en aangewezen organisaties. Het contract, dat voortvloeit uit de verwerving van het privaat uitgegeven middel, zal onder meer eisen bevatten die betrekking hebben op beveiliging en privacybescherming, waaronder te nemen technische en organisatorische maatregelen, zoals eisen inzake de integriteit van het bij de dienstverlening betrokken personeel en regels betreffende de intrekking of schorsing van het identificatiemiddel. Zo zal de leverancier van het privaat uitgegeven middel worden verplicht te voorzien in de beschikbaarheid en werking van het toegelaten identificatiemiddel volgens de aan het contract verbonden voorschriften. In het kader van contractbeheer zal de Minister van BZK de naleving van de voorschriften door de private leverancier controleren, mede aan de hand van een te overleggen auditverklaring en zo nodig feitelijke toetsing bij de aanbieder van het privaat uitgegeven middel. Daartoe wordt vereist dat de auditor de overwegingen waarop hij zijn oordeel baseert, in het auditrapport kenbaar maakt opdat het oordeel controleerbaar is.
De Minister en zijn ambtenaren krijgen contractueel de bevoegdheid om te allen tijde zelf een inspectie of audit uit te (doen) voeren. De controlerende ambtenaren en auditors stellen niet alleen vast of (management-)processen bestaan, maar kennen 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.[47] Bij de controle wordt afstemming gezocht met eventuele publieke toezichthouders, indien die op dit taakveld eigenstandige taken en bevoegdheden kennen. De ratio hierachter is onder andere de vermindering van de toezichtlast en voorkomen van dubbel toezicht. Wanneer werkzaamheden, die worden gereguleerd door het wetsvoorstel, door de aanbieder van het privaat uitgegeven middel worden uitbesteed aan onderaannemers, zijn deze onderaannemers net als de aanbieder verplicht aan de controlerende ambtenaren de benodigde medewerking te verlenen zodat de onafhankelijke informatieverzameling, oordeelsvorming en interventie verzekerd is.

Indien de controlerende ambtenaren vaststellen dat de leverancier van een toegelaten middel een of meer van de regels niet (meer) naleeft, zullen zij vanuit het contractbeheer in beginsel eerst met de betrokken

[47] *Zie het Onderzoeksrapport van de Raad voor de Veiligheid, het DigiNotarincident, Waarom digitale veiligheid de bestuurstafel te weinig bereikt, 2012.*

partij in contact treden om deze alsnog binnen een bepaalde termijn in overeenstemming met de gemaakte afspraken te laten handelen. Als het gewenste resultaat uitblijft of te lang op zich laat wachten, kan de Minister van BZK overgaan tot het initiëren van privaatrechtelijke handhaving, eventueel aangevuld met het schorsen of intrekken van een toelating als bedoeld in artikel 9, tweede lid, en het (al dan niet tijdelijk) feitelijk beëindigen van de aansluiting van de systemen van de private aanbieder op de publieke infrastructuur.

6.4. Toezicht op de erkende diensten en bedrijfs- en organisatiemiddelen

Als bedrijven inloggen in het publieke domein, zijn daarbij authenticatiediensten, machtigingsdiensten en ontsluitende diensten betrokken. Deze – private – diensten moeten, naast de identificatiemiddelen zelf, aan eisen voldoen om erkend te worden door de Minister van BZK alvorens ze in het publieke domein hun diensten mogen aanbieden. Om erop toe te zien dat de betrokken partijen ook na hun erkenning aan de gestelde eisen blijven voldoen, is de aanwijzing van een toezichthouder onontbeerlijk. De Minister van BZK wijst bij besluit ambtenaren aan om toezicht te houden op de naleving van de verplichtingen, die gelden voor de erkende diensten. Het Agentschap Telecom is de logische keuze voor de taak van toezichthouder op erkende diensten, 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). Thans vervult het Agentschap Telecom de secretariaatsfunctie voor de Commissie van Deskundigen voor het toezicht op het Elektronische Toegangsdiensten-stelsel.

Instrumentarium

De eerste waarborg om conformiteit af te dwingen, is dat middelen en diensten gecertificeerd moeten zijn. Een erkende dienst is gebonden aan de bij algemene maatregel van bestuur te stellen regels en de aan de erkenning verbonden voorschriften en beperkingen. Conformiteitsbeoordeling van de erkende dienst 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 door de Minister van BZK aan te wijzen 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.[48] Wanneer uit constatering van de toezichthouder blijkt dat niet (langer) wordt voldaan aan de bij algemene maatregel van bestuur gestelde regels en de aan de erkenning verbonden voorschriften en beperkingen, kan de Minister van BZK de verleende erkenning voor een bij dat besluit te bepalen periode schorsen of intrekken. De Minister van BZK is tevens bevoegd tot het opleggen van een last onder bestuursdwang.

---

[48] *Vergaderjaar 2015–2016, Kamerstuk 29 304 nr. 6*

6.5. Veiligheidsinbreuk

Het nemen van 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 volledig uitsluiten. Indien zich een incident met diensten in de authenticatieketen voordoet, dient vertrouwen zoveel mogelijk behouden te blijven of te worden hersteld. Een bestuursorgaan of een aangewezen organisatie is verplicht de Minister onverwijld in kennis te stellen van een inbreuk op de beveiliging of de integriteit van een eigen elektronische dienst of van misbruik of oneigenlijk gebruik van de toegang tot de eigen elektronische dienstverlening. Bestuursorganen en aangewezen organisaties zijn verplicht een veiligheidsinbreuk of integriteitsverlies van een eigen elektronische dienst of van misbruik of oneigenlijk gebruik van de toegang tot de eigen elektronische dienstverlening, zo spoedig mogelijk, na ontdekking te melden bij de Minister.

Indien het algemeen belang daarmee wordt gediend, kan het nodig zijn om het publiek te informeren over een veiligheidsinbreuk of integriteitsverlies. Het doel hiervan 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 bij een bestuursorgaan of aangewezen organisatie in de authenticatieketen kan veroorzaken, dient deze plicht ruim opgevat te worden. Dat wil zeggen dat ook sprake is van aanzienlijke gevolgen 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 en de inbreuk snel en adequaat kan worden hersteld, kan een melding achterwege blijven.

Ook de eIDAS-verordening (artikel 19 lid 2) kent een meldplicht. Deze geldt voor verleners van vertrouwensdiensten, welke veelal zullen samenvallen met private aanbieders van erkende diensten en middelen (bedrijven) en van toegelaten middelen (burgers). Met dit wetsvoorstel wordt de meldplicht ook toepasselijk voor bestuursorganen en aangewezen organisaties. De meldplicht uit de eIDAS-verordening en uit dit wetsvoorstel zijn, mede ter beperking van administratieve lasten, gelijksoortig vormgegeven.
Ook het bij de Eerste Kamer aanhagige voorstel voor de Wet beveiliging netwerk- en informatiesystemen[49] kent een meldplicht, te weten de plicht om incidenten met aanzienlijke gevolgen te melden bij van de Minister van Justitie en Veiligheid. Dit dient ter voorkoming of beperking van het uitvallen van de beschikbaarheid of het verlies van integriteit van netwerk- en informatiesystemen van vitale aanbieders, en van andere aanbieders die onderdeel zijn van de rijksoverheid, ter verdere versterking van de digitale weerbaarheid van de Nederlandse samenleving en ter uitvoering van de NIB-richtlijn. Het voorstel voor de Wet beveiliging netwerk- en informatiesystemen beoogt de Minister van Jusitie en Veiligheid te belasten met de taak om te fungeren als het centrale contactpunt voor incidenten met aanzienlijke gevolgen. De meldplicht is gericht op

[49] *Kamerstukken I 2017/18, 34 883, nr. A.*

aanbieders van een essentiële dienst als bedoeld in artikel 4 van de NIB-richtlijn[50] en aanbieders van een andere dienst, waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving.
De meldplicht in onderhavig wetsvoorstel ziet daarentegen alleen op het waarborgen de veiligheid van (de toegang tot) aangeboden diensten in de authenticatieketen. Ter beveiliging van door de Minister van BZK toegelaten identificatiemiddelen geldt de plicht om veiligheidsinbreuken en integriteitsverlies bij de Minister van BZK te melden derhalve alleen voor aangesloten dienstaanbieders, oftewel voor bestuursorganen en aangewezen organisaties die digitale diensten verlenen waarvoor authenticatie op het betrouwbaarheidsniveau substantieel of hoog noodzakelijk is.

Verstrekken van inlichtingen op verzoek

Naast de informatie, die de Minister op grond van de meldplicht krijgt, ontvangt hij desgevraagd gegevens en inlichtingen van bestuursorganen, aangewezen organisaties, de Minister van BZK, aanbieders van een toegelaten identificatiemiddel of erkend identificatiemiddel of erkende dienst. Het betreft inlichtingen die de Minister nodig heeft om maatregelen te kunnen nemen om inbreuk op de veilige en betrouwbare toegang tot elektronische dienstverlening te voorkomen of beëindigen. De Minister van BZK verstrekt op zijn beurt aan deze partijen inlichtingen over een inbreuk op de veilige en betrouwbare toegang tot elektronische dienstverlening voor zover dit noodzakelijk is voor een goede uitoefening van hun taken of te verlenen diensten in het kader van deze wet.

7. Financiële bepalingen en -gevolgen

7.1. 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 een aantal variabelen afhankelijk, zoals de mate waarin gebruik wordt gemaakt van de diverse identificatiemiddelen, de individuele inrichting van de interne ICT-voorzieningen en de mate waarin partijen de komende jaren bij aanpassing van hun ICT-voorzieningen (kunnen) voorsorteren op de nieuwe situatie.

De belangrijkste kostencomponenten van dit wetsvoorstel zijn:
– De kosten van de infrastructuur, waaronder de kosten van instandhouding, beheer en exploitatie van publieke voorzieningen zoals het BSN-Koppelregister[51], de machtigingsvoorziening en de routeringsvoorziening[52].
– De kosten van ontwikkeling, instandhouding, beheer en exploitatie van de publieke authenticatiedienst en de uitgifte van publieke middelen.
– De kosten die dienstverleners maken om aan te sluiten zodat burgers en bedrijven met de toegelaten en erkende identificatiemiddelen toegang tot hun elektronische dienstverlening kunnen krijgen.

---

[50] *Richtlijn (EU) 2016/1148 van het Europees Parlement en de Raad van 6 juli 2016 houdende maatregelen voor een hoog gemeenschappelijk niveau van beveiliging van netwerk- en informatiesystemen in de Unie (PbEU 2016, L 194).*

[51] *Het BSN-koppelregister is een voorziening, die het mogelijk maakt dat de identiteit van een natuurlijke persoon die een elektronische dienst afneemt bij een bestuursorgaan of aangewezen organisatie op unieke wijze geïdentificeerd kan worden.*

[52] *De routeringsvoorziening faciliteert de toegang tot elektronische dienstverlening. In deze (technische) voorziening worden verschillende koppelvlakken (verbindingen die volgens een bepaalde standaard de uitwisseling van gegevens tussen informatiesystemen mogelijk maken) ontsloten, waardoor bestuursorganen en aangewezen organisaties eenvoudig kunnen aansluiten op de identificatiemiddelen, die zij moeten accepteren.*

– De kosten als gevolg van het gebruik van het identificatiemiddel door burgers en bedrijven.

7.2. Financiële bepalingen

Grondslag voor doorberekening aan dienstverleners

De kosten die het Rijk maakt samenhangend met het realiseren van publieke identificatiemiddelen en voorzieningen, en het eventueel toelaten van private middelen en toezicht op de naleving van toelatingseisen, worden door de Minister ten laste gebracht van de bestuursorganen en aangewezen organisaties. Bij ministeriële regeling worden hierover nadere regels gesteld. Op dit moment is het nog niet goed mogelijk om de totale kosten in beeld te brengen. De ontwikkeling van de kosten van de infrastructuur voor authenticatie is van een aantal factoren afhankelijk. Kosten van publieke middelen en de infrastructuur hangen grotendeels samen met de mate van gebruik van alle publieke middelen (ook in verhouding tot elkaar), wat nog onvoorspelbaar is.[53]Het gebruik evenals exogene technologische ontwikkelingen zullen periodiek nieuwe en aanvullende eisen stellen aan de infrastructuur. Kosten van beheer, exploitatie en doorontwikkeling zullen daarom pas gedurende de rit volledig duidelijk worden. Het uitgangspunt is dat de kosten van het gebruik van het publieke authenticatiemiddel naar rato van gebruik worden doorbelast aan dienstverleners. Er is wel een redelijk beeld van de kosten die op korte termijn gepaard gaan met een stapsgewijze uitrol van een robuuste infrastructuur voor authenticatie en identificatie, inclusief eventuele toelating en toezicht. Het gaat dan om de kosten van de basisinrichting en, onder bepaalde veronderstellingen, voor het gebruik. De kosten van de uitrol zullen via de begroting worden gedekt en departementen dragen hieraan naar rato bij. Daarbij is het uitgangspunt uiteraard dat de uitrol zo doelmatig mogelijk wordt uitgevoerd en budgetten disciplinerend werken, zonder daarbij uit het oog te verliezen dat een toekomstbestendige financieringsstrategie moet kunnen mee-ademen met de implicaties van meergebruik en nieuwe technologische eisen.

Grondslag voor het heffen van leges

Het kabinet wil de aanschafkosten van de publieke middelen verbonden aan e-rijbewijs en e-NIK via het heffen van leges bij de gebruiker in rekening brengen.[54] Via de leges worden de kosten van het identificatiemiddel zelf en de verstrekking ervan in rekening gebracht bij degenen die het middel aanschaffen. Voor het heffen van de leges voor de kosten van het plaatsen van de chip op de NIK bestaat reeds een wettelijke basis in de Paspoortwet. Dit wetsvoorstel bevat een voorstel tot wijziging van de Wegenverkeerswetgeving voor het creëren van een wettelijke grondslag voor het heffen van leges, die de kosten van het plaatsen van de chip op het e-rijbewijs dekken. Ten slotte voorziet het wetsvoorstel in een grondslag voor het vaststellen van een tarief voor publieke middelen, waarvan het tarief niet in een ander wettelijk voorschrift wordt geregeld. Of hiervoor daadwerkelijk een tarief wordt gesteld is afhankelijk van de daadwerkelijke kosten van uitgifte van dit middel.

---

[53] *Burgers kunnen kiezen welk toegelaten middel zij gebruiken. 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 totale aantal authenticaties met dat middel. Bij hogere aantallen nemen de kosten significant af. Het is dus voor een authenticatiedienst in de beginperiode lastig in te schatten tegen welke prijs een middel moet worden aangeboden.*

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

Doorberekening kosten van erkenning en toezicht op naleving erkenningseisen

Het wetsvoorstel regelt dat de Minister van BZK de kosten voor het behandelen van een erkenningsaanvraag, alsmede voor het toezicht op de naleving van de aan de erkende dienst opgelegde eisen, kan doorberekenen aan de erkende private dienst. Voor wat betreft de doorberekening van de kosten van toezicht is 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 uitvoeringsregelgeving zal belang worden gehecht aan het feit dat het voorzien in identificatiemiddelen, of een ontsluitende dienst of machtigingsdienst geen (klassieke) overheidstaak betreft en het derhalve niet vereist is dat de kosten van toezicht uit de algemene middelen worden voldaan. Voorts gaat de regering ervanuit dat het aantal partijen waarop op grond van dit wetsvoorstel toezicht zal worden gehouden overzichtelijk zal zijn, zodat er geen pragmatische redenen zijn om deze kosten niet door te belasten.

7.3. Financiële gevolgen

Voor de gebruikers (burgers en bedrijven)

In de nieuwe situatie zal de gebruiker verschillende middelen kunnen afnemen om zich bij dienstverleners elektronisch te kunnen identificeren. Bij de publieke identificatiemiddelen op het hoogste niveau, het e-rijbewijs en de e-NIK, wordt een gedeelte van de kosten die het Rijk maakt al gedekt doordat bij het uitgifteproces gebruik wordt gemaakt van het uitgifteproces van de fysieke documenten en vindt er via het heffen van leges een verplichte doorberekening van de extra kosten voor de vervaardiging van deze documenten plaats aan de burgers, die het middel aanschaffen. Ingevolge het wetsvoorstel wordt per publiek identificatiemiddel de hoogte van het bedrag vastgesteld en de wijze van betaling worden vastgesteld voor zover deze vergoeding niet krachtens een andere wet wordt vastgesteld. De kosten van het gebruik van de publieke identificatiemiddelen zijn niet voor rekening van de gebruiker; deze worden doorbelast aan de dienstverlener.

De door de Minister van BZK erkende private partijen zijn op grond van dit wetsvoorstel vrij om bedrijven te laten betalen voor de aanschaf- of het gebruik van het identificatiemiddel, dat zij aanbieden. Er zullen naar verwachting verschillende authenticatiediensten worden erkend, waardoor bedrijven kunnen kiezen met welk identificatiemiddel zij willen inloggen in het publieke domein. Indien de private partijen, die een identificatiemiddel voor bedrijven aanbieden, te hoge tarieven zullen stellen voor de gebruiker voor de aanschaf of het gebruik van het middel, zullen zij zichzelf vanzelf uit de markt prijzen en zijn hun ontwikkelingskosten voor niets geweest. Prijsstelling kan daarom worden overgelaten aan de marktwerking.

Voor dienstverleners

Uitgangspunt is dat de dienstverleners (zoals de Belastingdienst, het Uitvoeringsinstituut werknemersverzekeringen, de Sociale Verzekeringsbank, gemeenten, ziektekostenverzekeraars etc.) bij de verlening van hun diensten de kosten dragen voor het identificeren van burgers en bedrijven. Dit geldt evenzeer bij digitale identificatie en authenticatie, waarbij toegelaten of erkende middelen worden gebruikt. Dienstverleners worden niet door het Rijk gecompenseerd voor het feit dat zij – voor zover

zij diensten verlenen op betrouwbaarheidsniveau substantieel of hoog – als gevolg van dit wetsvoorstel hun digitale infrastructuur moeten aanpassen om de toegelaten en erkende identificatiemiddelen te kunnen accepteren. Naast kosten zullen dienstverleners baten genereren door het gebruik van een generieke, betrouwbare infrastructuur voor het digitaal inloggen. Zij zullen meer diensten aan burgers of bedrijven digitaal kunnen verlenen en door de hogere betrouwbaarheid van de inlogmethoden minder risico's lopen. Het is niet goed mogelijk om de precieze kosten van aansluiting en het gebruik van de identificatiemiddelen, en de baten hiervan vooraf te kwantificeren. De kostencomponenten zijn helder. Deze worden hieronder uiteengezet.

Voor rekening van de dienstverleners komen in de eerste plaats de kosten voor het aansluiten op de routeringsvoorziening in het geval dat sprake is van digitale dienstverlening (op betrouwbaarheidsniveau substantieel of hoog) aan burgers. Indien sprake is van digitale dienstverlening aan bedrijven zijn er kosten voor aansluiting op de ontsluitende dienst. Ook zal de interne digitale infrastructuur geschikt gemaakt moeten worden om met de berichten van de routeringsvoorziening en/of ontsluitende dienst te kunnen werken en (zo nodig) om aan de 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. Het aansluiten op de routeringsvoorziening brengt mee dat de dienstverlener op grond van dit wetsvoorstel regulier een *audit* moet laten uitvoeren om te toetsen of de digitale infrastructuur van de dienstverlener 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.

Daarnaast zullen de dienstverleners betalen naar rato van gebruik van de identificatiemiddelen en voor het inschakelen van de machtigingsdienst. In het geval dat de Minister een of meerdere private identificatiemiddelen toelaat ten behoeve van authenticatie in het publieke domein, zal de tariefstelling voor het gebruik van het middel centraal geschieden op basis van afspraken, die aan de toelating worden verbonden. Gekozen is om centraal afspraken te maken met een aanbieder van een privaat middel, omdat een dienstverlener verplicht is de toegelaten middelen te accepteren, waardoor zijn onderhandelingsvrijheid bij het maken van prijsafspraken voor deze dienstverlening afwezig tot (zeer) beperkt is. Op voorhand valt de prijsstelling niet te bepalen. De marktconsultatie en de daaropvolgende procedure, die vooraf gaat aan het toelaten van een privaat middel, verschaffen de Minister de benodigde informatie over een redelijke prijsstelling. Van potentiële aanbieders van een privaat middel is de benodigde infrastructuur al voor een aanzienlijk deel bekostigd (bijvoorbeeld in het kader van de bancaire dienstverlening), terwijl dit bij andere potentiële aanbieders mogelijk niet het geval is.

Dit wetsvoorstel brengt voor overheidsinstanties 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 ervanuit 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.[55] De jaarlijkse kosten variëren per standaard van ongeveer zevenhonderd tot vijfduizend euro.

Voor het Rijk

Het zorg dragen voor de beschikbaarheid en de werking van de infrastructuur voor het gebruik van identificatiemiddelen brengt voor het Rijk uiteenlopende kosten met zich mee. Het gaat om de volgende kostenposten:

- De kosten van (door)ontwikkelingen en beheer van de middelen e-NIK, e-rijbewijs, DigiD op het betrouwbaarheidsniveau substantieel en het 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 de voorzieningen, die deel uitmaken van de infrastructuur voor authenticatie in het publieke domein (zoals de routeringsvoorziening, het BSN-Koppelregister en het eIDAS-knooppunt);
- De kosten van de inzagefunctie bij het BSN-Koppelregister;
- De kosten voor instandhouding en gebruik van de publieke machtigingsdienst;
- De kosten gemoeid met het erkennen van de diverse diensten;
- De kosten van toezicht op de erkende diensten, erkende- en toegelaten authenthicatiemiddelen;
- De kosten, die als gevolg van het gebruik van identificatiemiddelen bij bepaalde dienstverleners (bijv. de Belastingdienst) ten laste van de rijksbegroting komen.

Hiertegenover staan de volgende inkomsten:

- Inkomsten door het doorberekenen van de kosten van de vervaardiging en de uitgifte van publieke middelen;
- Inkomsten door het doorbelasten van de kosten van het gebruik van het publieke middel;
- Inkomsten als erkenningsinstantie voor het erkennen van de diverse diensten;
- Inkomsten door het doorbelasten van kosten voor exploitatie en beheer van de algemene voorzieningen van het Rijk aan bestuursorganen en aangewezen organisaties;
- Inkomsten uit het doorbelasten van het toezicht op erkende diensten, erkende- en toegelaten authenthicatiemiddelen.

8. Verhouding tot andere wetgeving

8.1. Algemene wet bestuursrecht

Het onderhavige wetsvoorstel heeft een relatie met het wetsvoorstel tot wijziging van de Awb inzake modernisering elektronisch bestuurlijk verkeer. Ingevolge dat wetsvoorstel krijgen burgers en bedrijven het recht

[55] *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.*

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.[56] 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 krachtens de wet 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 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 voorgenomen 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 toegelaten identificatiemiddelen. 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.

8.2. Paspoortwet

Voor de invoering van een publiek middel op betrouwbaarheidsniveau hoog, is 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. Geregeld wordt het plaatsen van een chip op de identiteitskaart («drager») met daarin de versleutelde persoonsgegevens van de houder van het document. Hierdoor wordt van de NIK een elektronische identiteitskaart (eNIK) gemaakt. De Paspoortwet creëert derhalve de grondslag om de chip op de NIK aan te vullen met gegevens die elektronische authenticatie mogelijk maken. Ook zal de Paspoortwet gaan voorzien in de instelling van een centraal systeem voor de opslag van reisdocumentengegevens dat als bron dient voor het verstrekken van de gegevens ten behoeve van het functioneren van de e-NIK. Voor deze verwerking van persoonsgegevens, inclusief het bsn, is een wettelijke grondslag vereist. Aangezien de Paspoortwet een rijkswet is, kan deze wijziging niet worden meege-

[56] *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.*

nomen met dit wetsvoorstel, doch zal worden opgenomen in een eigenstandig wetsvoorstel tot wijziging van de Paspoortwet.

8.3. Wegenverkeerswet

In dit wetsvoorstel is een wijziging van de Wegenverkeerswet opgenomen die regelt dat de zogenoemde rijkskostencomponent van het rijbewijs ook het identificatiemiddel 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. Hierin wordt tevens geregeld welke chip op het rijbewijs wordt opgenomen.

8.4. 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 elektronische identificatiemiddelen aangewezen moeten worden, voor de gevallen waarin de identiteit langs elektronische weg wordt vastgesteld.

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 eenieder 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 is 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.

De WID en de verschillende wetten waarin identificatieplichten zijn opgenomen en waarin verwezen wordt naar een of meer documenten genoemd in de WID, gaan 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 elektronische identificatiemiddelen 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 elektronisch identificatiemiddel ook bepaalde attributen (aanvullende gegevens zoals de nationaliteit of leeftijd) aan de betrokken dienstverlener verstrekt moeten worden.

8.5. Wet elektronisch berichtenverkeer Belastingdienst

De Wet elektronisch berichtenverkeer Belastingdienst (EBV) schept het wettelijk kader voor het verplichten van elektronisch berichtenverkeer in het contact met de Belastingdienst. In artikel X van deze wet is bovendien een grondslag opgenomen voor voorzieningen voor elektronisch berichtenverkeer, elektronische authenticatie en elektronische registratie van machtigingen en het raadplegen ervan, 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 hij persoonsgegevens verwerkt, waaronder het BSN, voorzover dit noodzakelijk is voor de goede vervulling van zijn taken. Met de Wet EBV, in werking getreden op 1 november 2015, is een eerste fundament gelegd onder de GDI, met het oog op de reeds in de praktijk functionerende voorzieningen MijnOverheid, DigiD en DigiD Machtigen. Ook het BSN-Koppelregister, essentieel voor het functioneren van identificatiemiddelen in het publieke domein, is nader gereguleerd. Conform hetgeen in de memorie van toelichting bij de Wet EBV is vermeld, zal artikel X komen te vervallen wanneer een specifieke wet in werking treedt. Hiervan is sprake met het onderhavige wetsvoorstel. Voor wat betreft de onder de Wet EBV tot stand gekomen uitvoeringsregelgeving geldt dat het Besluit verwerking persoonsgegevens GDI zal worden gebaseerd op dit wetsvoorstel. Ook de Regeling voorzieningen GDI, waarin onder meer gebruik(ers) voorschriften terzake van authenticatie en machtigen zijn opgenomen zal worden aangevuld en gewijzigd naar aanleiding van dit wetsvoorstel.

8.6. EIDAS-verordening en -uitvoeringsverordeningen

Dit wetsvoorstel bevat regels voor de toegang door burgers en bedrijven tot elektronische diensten van dienstverleners in Nederland. Voor grensoverschrijdende elektronische authenticatie door burgers en bedrijven gelden rechtstreeks werkende (minimum)eisen die bij en krachtens de eIDAS-verordening zijn gesteld. Deze eisen betreffen onder andere de betrouwbaarheid van elektronische identificatiemiddelen en uitgifteprocessen op de betrouwbaarheidsniveaus laag, substantieel en hoog. Om redenen van veiligheid en betrouwbaarheid alsmede om grensoverschrijdend gebruik mogelijk te maken, vormen deze eisen tevens de maatstaf voor regulering van nationale publieke diensten en de elektronische toegang daartoe. Voor de betrouwbaarheidsniveaus substantieel en hoog wordt in de verordening geregeld dat de lidstaten hun stelsels voor elektronische identificatie bij de Europese Commissie kunnen notificeren. Genotificeerde identificatiemiddelen moeten met ingang van medio september 2018 door dienstverleners in andere lidstaten geaccepteerd worden, mits tenminste passend bij het door hen in nationaal verband vereiste betrouwbaarheidsniveau van hun dienstverlening (interoperabiliteit/wederzijdse erkenning). Het ligt in de rede om de in Nederland toegelaten en erkende identificatiemiddelen op de niveaus substantieel en hoog bij de Commissie te notificeren, zodat deze ook in andere lidstaten gebruikt kunnen en moeten worden.

De eIDAS-verordening wordt uitgewerkt in een meerdere uitvoeringverordeningen van de Europese Commissie. Verordening 2015/1502 bevat technische normen, specificaties en procedures voor de identificatiemiddelen op de diverse betrouwbaarheidsniveaus, bijvoorbeeld inzake aanvraag, verificatie van identiteit (authenticatie), uitgifte en activering, blokkeren en reactiveren en informatiebeveiliging. Deze zullen de basis vormen voor de uitvoering van dit wetsvoorstel, alsmede voor de aan private partijen op te leggen eisen. Daarnaast geldt uitvoeringsverordening 2015/1501, die rechtstreeks werkende regels bevat over de in de

lidstaten in te stellen knooppunten die interoperabiliteit oftewel interconnectie binnen de EU mogelijk moeten maken. De Minister van BZK draagt zorg voor deze infrastructurele voorziening,[57] die het mogelijk maakt genotificeerde identificatiemiddelen uit andere lidstaten op toegankelijke wijze te ontsluiten voor dienstverleners in Nederland en vice versa. Dienstverlening die samenhangt met grensoverschrijdende authenticatie wordt dus via dit knooppunt afgehandeld.

9. Gevolgen voor burgers en bedrijven

9.1. Gevolgen voor burgers

Zoals in de visiebrief digitale overheid 2017[58] reeds is aangegeven, draagt dit wetsvoorstel bij aan de verbetering van de kwaliteit van digitale overheidsinformatie en overheidsdienstverlening. Het gebruik van onderdelen van de generieke digitale infrastructuur door zoveel mogelijk overheidsorganisaties draagt bij aan een efficiëntere overheid en uniforme dienstverlening. Het wetsvoorstel regelt het voor authenticatie relevante deel van de infrastructuur bij bestuursorganen en aangewezen organisaties, zodat burgers met een toegelaten identificatiemiddel van het juiste betrouwbaarheidsniveau toegang hebben tot de digitale dienstverlening van alle bestuursorganen en aangewezen organisaties. Het wetsvoorstel beoogt een bijdrage te leveren aan vermindering van de regeldruk en administratieve lasten voor burgers, doordat de toegang tot digitale dienstverlening wordt geüniformeerd. De burger zal immers als gevolg van de plicht voor bestuursorganen en aangewezen organisaties om een door de Minister toegelaten identificatiemiddel te accepteren met een dergelijk middel bij vele verschillende dienstverleners kunnen inloggen[59].

Continuïteit en keuzevrijheid

Continuïteit van digitale dienstverlening betekent voor burgers en bedrijven 24/7 beschikbaarheid en locatie-onafhankelijke toegang. Dit wetsvoorstel maakt het mogelijk dat een burger of bedrijf met verschillende (publieke en private) middelen kan inloggen. Hierdoor is de beschikbaarheid en bereikbaarheid van dienstverlening beter geborgd. Werkt het ene inlogmiddel niet, dan kan men ervoor kiezen in te loggen met een ander middel. Er is keuzevrijheid.

Veiligheid en aanbod van digitale dienstverlening

Bestuursorganen en aangewezen organisaties moeten, om bepaalde diensten digitaal te kunnen aanbieden, met meer zekerheid dan het huidige DigiD laag biedt, kunnen vaststellen of zij met de juiste (natuurlijke- of rechts)persoon te maken hebben (zie ook paragraaf 3.2). Het gaat hierbij onder meer om diensten in het domein van de zorg (eHealth) en bij gemeenten (wijkzorg, WMO, jeugdzorg). Dit wetsvoorstel regelt dat diensten op het betrouwbaarheidsniveau hoog of substantieel ook daadwerkelijk op een veilige en betrouwbare manier online afgenomen kunnen worden waar dat nu nog niet mogelijk is. Het betrouwbaarheidsniveau van DigiD laag is niet toereikend voor diensten waarbij uiterst vertrouwelijke informatie (zoals medische gegevens) wordt uitgewisseld. De beschikbaarheid van inlogmiddelen van hogere betrouwbaarheidsniveaus schept de mogelijkheid voor bestuursorganen en aangewezen organisaties om meer diensten digitaal aan te bieden,

---

[57] *Zie MvT bij de Uitvoeringswet eIDAS-verordening, p. 32–38.*
[58] *Kamerstukken II 2012/13, 26 643, nr. 280.*
[59] *Er zijn enkele dienstverleners waar niet met DigiD kan worden ingelogd.*

waardoor voor het afnemen van diensten minder vaak de fysieke aanwezigheid van burgers nodig zal zijn. Door het aanbod van digitale diensten te vergroten zijn burgers over het algemeen minder (reis- en/of wacht)tijd kwijt en kunnen diensten plaats- en tijdsonafhankelijk worden afgenomen.
Identiteitsfraude is strafbaar, ook in de digitale omgeving. Doordat als gevolg van dit wetsvoorstel de identiteit van de burger met een hogere mate van zekerheid kan worden vastgesteld, wordt het lastiger om identiteitsfraude te plegen.

Enkele voorbeelden van baten die voor burgers kunnen ontstaan:
– Door met DigiD hoog een Nederlandse identiteitskaart of een rijbewijs digitaal aan te vragen hoeft een burger slechts één keer naar het gemeentehuis, namelijk om het af te halen (i.p.v. twee keer).
- De processen jeugdzorg, WMO, medisch gerelateerde processen en (financiële) transacties vergen een hoger niveau van betrouwbaarheid en kunnen met DigiD hoog worden afgedaan.
– Van digitale toepassingen in de zorgsector (eHealth) worden grote voordelen verwacht, zoals het thuis uitvoeren van metingen waarvan de uitslag digitaal wordt doorgegeven aan de arts. De burger bespaart daarmee tijd en kosten van een reis naar de zorgverlener. Ook kunnen burgers elektronisch inzage krijgen in hun patiëntendossier.
– Digitale inzage in gerechtelijke dossiers.
– Minder gevallen van identiteitsfraude scheelt de burger veel tijd (en ergernis) en mogelijk ook geld.

Lasten

Het gebruik van betrouwbaarder inlogmiddelen verhoogt de betrouwbaarheid van overheidshandelen en veiliger communicatie met die overheid. Een hogere graad van veiligheid betekent doorgaans extra lasten in de vorm van investering in geld en/of tijd. Dat geldt voor fysieke veiligheid (bijvoorbeeld verscherpte toegangscontroles, poortjes e.d.) en evenzo in de digitale omgeving. Inloggen met een hogere betrouwbaarheid zal lasten veroorzaken in de vorm van tijd (activeren, heractiveren). Met het oog op deze lasten wordt niet per definitie voorgeschreven om de meest betrouwbare inlogmiddelen te hanteren. In uitvoeringsregelgeving zullen criteria worden opgenomen («classificatiemodel») die relevant zijn voor het door de dienstverlener (kunnen) inschalen van het benodigde betrouwbaarheidsniveau zoals aard en rechtsgevolg van de desbetreffende dienst.

Dit wetsvoorstel verplicht dienstverleners om de toegelaten middelen te accepteren en biedt daarmee burgers en bedrijven de mogelijkheid om bestaande diensten af te nemen met inlogmiddelen van een hoger betrouwbaarheidsniveau. Het wetsvoorstel bevat geen verplichting tot het gebruiken van deze inlogmiddelen. Burgers kunnen voor bestaande diensten vooralsnog[60] gewoon blijven inloggen met het hun vertrouwde DigiD of desgewenst via de papieren weg diensten van de overheid afnemen voor zover niet anders is bepaald in sectorale wetgeving. In het geval dat in sectorale wetgeving het gebruik van de elektronische weg verplicht wordt gesteld voor een dienst op het betrouwbaarheidsniveau substantieel of hoog, zullen burgers als indirect gevolg van dit

[60] *Voor elektronische dienstverlening waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is, wordt het dienstverleners toegestaan om tot uiterlijk vier respectievelijk zeven jaar of een bij koninklijk besluit te bepalen eerder tijdstip na de inwerkingtreding van artikel 6 toegang tot die dienstverlening te verlenen indien gebruik wordt gemaakt van door de Minister aangewezen identificatiemiddelen, die het betrouwbaarheidsniveau laag respectievelijk substantieel hebben.*

wetsvoorstel diensten moeten afnemen met de inlogmiddelen die de Minister op dat betrouwbaarheidsniveau heeft toegelaten. Hieronder volgt een opsomming van (mogelijke) administratieve lasten voor burgers:

– Een merkbaar effect op de lasten voor burgers kan ontstaan als gevolg van het doorberekenen (in leges) van kosten voor het plaatsen van een chip op identiteitsdocumenten zoals het rijbewijs en de Nederlandse identiteitskaart.
– De tijd die de burger nodig heeft om een inlogmiddel op het niveau DigiD substantieel en/of hoog te installeren, te activeren en te upgraden: over DigiD substantieel[61] kan voor worden beschikt door het gratis downloaden van een applicatie en het (huidige) wettelijke identiteitsdocument tegen de telefoon te houden. Dat vergt een korte tijdsinvestering. Andere vormen van uitgifte van niveau substantieel kunnen omslachtiger zijn.
– DigiD hoog is gekoppeld aan een wettelijk identiteitsdocument, dat afgehaald dient te worden op het gemeentehuis. Door gebruik te maken van het bestaande uitgifteproces van deze documenten, waarbij een fysieke controle van de persoon en zijn of haar identiteitsbewijs reeds plaatsvindt, zijn de lasten van het uitgifteproces van Digid hoog geminimaliseerd. Eenvoudigere methoden kunnen afbreuk doen aan het betrouwbaarheidsniveau van het publieke middel. Als alternatief kan de Minister van BZK op grond van dit wetsvoorstel een privaat middel aanwijzen waarmee in het publieke domein ingelogd kan worden op het niveau substantieel. Dat zal voorzover mogelijk een middel zijn dat het overgrote deel van de burgers al heeft.
– De tijd die het inloggen met publieke identificatiemiddelen op het betrouwbaarheidsniveau substantieel of hoog kost ten opzichte van het inloggen met het huidige DigiD. De gebruiksvriendelijkheid van de techniek van deze middelen is nog niet uitontwikkeld. Inloggen kan straks meer of minder tijd kosten dan met DigiD laag.
– Het periodiek heractiveren van publieke identificatiemiddelen met een hoger betrouwbaarheidsniveau dan het huidige DigiD zal burgers tijd kosten.
– Burgers die niet beschikken over een mobiele telefoon met een zogeheten Android besturingssysteem met een bepaalde vorm van contactloze communicatie[62] voor het uitlezen van het wettelijke identiteitsdocument, zullen een kaartlezer moeten aanschaffen om op het betrouwbaarheidsniveau hoog in te kunnen loggen.

Ingroeitraject

Grootschalige introducties van nieuwe inlogmiddelen zoals DigiD op het betrouwbaarheidsniveau substantieel en DigiD hoog kennen een meerjarig uitroltraject. DigiD wordt op dit moment gebruikt door ca. 13,6 miljoen Nederlanders, die in 2016 zo'n 280 miljoen keer inlogden bij overheidsdienstverleners. Het betreft dus een hele grote groep burgers die in een aantal jaren inlogmiddelen op een hoger betrouwbaarheidsniveau moeten gaan gebruiken. Dit zal een meerjarig zorgvuldig uitrolprogramma vergen. DigiD hoog komt als extra functie beschikbaar op rijbewijzen en (later) op de NIK's. Gelet op de vervangingstermijn van deze wettelijke identiteitsdocumenten zal de volledige uitrol van DigiD op het betrouwbaarheidsniveau hoog (op deze middelen) tien jaar vergen.

De berekening van de administratieve lasten voor burgers is niet anders dan met grove aannames en marges te maken. De techniek achter DigiD substantieel en DigiD hoog is nog niet uitontwikkeld en daarom nog niet uitgebreid getest onder groepen burgers. Het is dus niet mogelijk nu al te

[61] *Regeling voorzieningen GDI, Stcrt. 2017, nr 59901.*
[62] *Near-field communication of NFC.*

meten hoeveel tijd het kost om een middel aan te schaffen en te activeren en hoeveel meer of minder tijd het inloggen gaat kosten. Het is daarnaast onzeker in welke mate burgers de komende jaren feitelijk over een middel met hogere betrouwbaarheid gaan beschikken en welke dekkingsgraad wordt bereikt. Met het oog op het sneller bereiken van een hoge dekkingsgraad en teneinde ook de continuïteit van de dienstverlening te borgen bij uitval van DigiD, is onderzocht of er een alternatief privaat identificatiemiddel kan worden toegelaten. Eind 2018 zal naar verwachting duidelijk zijn of er een privaat middel daadwerkelijk wordt toegelaten voor gebruik bij publieke dienstverlening en welke dekkingsgraad dat middel zal hebben. Vanwege deze onzekerheden is in deze fase niet aan te geven wanneer de verplichting, om elektronische identificatiemiddelen met een hogere betrouwbaarheid te gebruiken, van kracht wordt. Het is dus nog niet mogelijk aan te geven vanaf welk jaar de administratieve last ontstaat. Met het oog op massale processen zoals het doen van belastingaangifte ligt het voor de hand de verplichting voor bestuursorganen en aangewezen organisaties om identificatiemiddelen van betrouwbaarheidsniveau substantieel of hoog te gebruiken niet eerder in werking te laten treden, dan nadat DigiD substantieel – in combinatie met een eventueel toegelaten privaat identificatiemiddel – een zeer hoge graad van dekkingsgraad heeft binnen de doelgroep van de 13,6 miljoen DigiD-gebruikers.[63]

Ook voor de baten geldt dat deze niet anders dan met grote aannames in te schatten zijn wegens onzekerheid met betrekking tot het feitelijk aanbod van nieuwe diensten, de uitrolstrategie, dekkingsgraad van de middelen e.d.

9.2. Gevolgen voor bedrijven

Het wetsvoorstel beoogt een bijdrage te leveren aan vermindering van de regeldruk en administratieve lasten voor bedrijven, doordat er verplichtingen voor 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. Het wetsvoorstel heeft vooral effect op bestuursorganen en aangewezen organisaties, oftewel dienstverleners, omdat de reikwijdte van het wetsvoorstel zich uitstrekt tot toegang tot hun dienstverlening. Voor bedrijven ontstaan geen nieuwe verplichtingen, behoudens voor private rechtspersonen die in de bijlage bij het wetsvoorstel of in een aanwijzingsbesluit worden aangewezen. Deze aangewezen organisaties kunnen privaatrechtelijke organisaties zoals pensioenfondsen of zorgverleners zijn. Met de acceptatieplicht terzake van de toegelaten en erkende middelen zijn kosten gemoeid voor de aangewezen organisaties. Daarnaast ontstaat voor hen een administratieve last, omdat zij periodiek een verklaring van een auditor moeten overleggen, waaruit blijkt of zij voldoen aan de ingevolge deze wet gestelde bepalingen over de werking, de betrouwbaarheid en de beveiliging van de toegang tot de elektronische diensten die zij in stand houden. Voor deze organisaties, die thans veelal gebruikmaken van DigiD, zijn die *audits* reeds verplicht ingevolge de huidige aansluitvoorwaarden voor DigiD. Het wetsvoorstel codificeert die verplichting.

---

[63] *Het ingevolge artikel 29, derde lid, op te stellen aansluitschema kan erin voorzien dat de acceptatieplichten voor verschillende diensten van een bestuursorgaan of aangewezen organisatie op verschillende momenten van toepassing worden.*

Voor een specifieke categorie van bedrijven is er een regeldrukeffect, te weten 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. Authenticatiediensten, ontsluitende diensten of machtigingsdiensten moeten worden erkend door de Minister van BZK, alvorens zij hun diensten mogen leveren. Hierbij is geen sprake van een marktverstorend effect omdat het iedereen vrij staat de erkenning aan te vragen. Voor deze erkenning kunnen leges in rekening worden gebracht. Het gaat hier om maximaal enkele tientallen bedrijven. De kosten van toezicht kunnen eveneens worden doorberekend aan de erkende diensten.

eHerkenning

De verwachting is dat eHerkenning erkend zal worden als bedrijfs- en organisatiemiddel. eHerkenning kent verschillende betrouwbaarheidsniveaus, waarbij de prijs van het inlogmiddel toeneemt naarmate het betrouwbaarheidsniveau oploopt. eHerkenning kent een systeem van machtigingen, waardoor bedrijfsmedewerkers kunnen worden gemachtigd voor één specifieke dienst of voor een deel van de overheidsdiensten. De regeldruk is dus ook afhankelijk van de vraag hoeveel bedrijven ervoor kiezen om meer dan één middel aan te schaffen. Overheidsorganisaties kunnen er ook voor kiezen om het papieren kanaal open te houden. Enkele grote uitvoeringsorganisaties staan ook toe dat eenmanszaken bij hen met DigiD inloggen en het is dus vraag hoeveel eenmanszaken een eHerkenningsmiddel zullen aanschaffen voor andere toepassingen. Een laatste onzekerheid is het tempo waarmee betrouwbaarheidsniveau 3 (eIDAS: substantieel) de standaard wordt en of in de toekomst meer dan incidenteel niveau 4 vereist zal worden.

Met zoveel onzekerheid is alleen in de vorm van een scenario aan te geven hoeveel regeldruk bedrijven zullen ondervinden. Dat scenario ziet er als volgt uit: over ca. 5 jaar zullen alle bedrijven een of meer eHerkenningsmiddelen hebben aangeschaft, omdat zij altijd wel met een bestuursorgaan zakendoen die (a) alleen erkende middelen accepteert, (b) het eigen inlogmiddel heeft uitgefaseerd en (c) ook het gebruik van andere kanalen niet toestaat. Vanwege de tendens om hogere betrouwbaarheidsniveaus te vereisen zullen bedrijven een inlogmiddel op het vrij hoge niveau 3 moeten aanschaffen. In dit scenario wordt uitgegaan van 1,5 mln. bedrijven en organisaties, die een abonnement voor 3 jaar afsluiten, waarbij het huidige tarief voor inlogmiddelen op niveau 3 door de concurrentie daalt naar 30 euro per jaar. Omdat 96% van het bedrijfsleven uit ZZP'ers en microbedrijven bestaat, wordt hier afgezien van kosten die ontstaan doordat bedrijven (uit vrije wil) meer dan één middel aanschaffen, en daarbij medewerkers machtigen voor specifieke diensten. De regeldruk bestaat uit drie componenten: eenmalige kennisnamekosten, aanschafprocedure en abonnementstarief:

– Kennisname: 1,3 mln. bedrijven (want 200.000 bedrijven en organisaties hebben al een eHerkenningsmiddel) zijn gemiddeld 1 uur kwijt om zich in de materie te verdiepen: 1,3 mln. x 1 uur x 37 euro per uur = 48,1 mln. euro.
– Aanschafprocedure initieel: 1,3 mln. bedrijven doen een aanvraag, moeten een contract tekenen, evt. een machtigingenbeheerder aanstellen, een face-to-face controle doorlopen, etc.: 1,3 mln. x 2 uur x 37 euro per uur = 96,2 mln. euro.
– Aanschafprocedure initieel bij verlengen van contract en upgraden naar hoger betrouwbaarheidsniveau: 0,2 mln. x 1 uur x 37 = 7,4 mln. euro.

De structurele kosten bedragen:

– Aanschafprocedure bij elke 3 jaar verlengen: 1,5 mln. x 0,5 uur x 37 euro per uur x 1/3 = 9,25 mln. per jaar.
– Aanschafkosten middel eens per 3 jaar op niveau 3: 1,5 mln. x 30 euro = 45 mln. per jaar.

De regeldruk voor het bedrijfsleven zal ook structureel dalen om de volgende redenen:
– Door het hogere betrouwbaarheidsniveau zullen sommige bestuursorganen ervoor kiezen om diensten, waarvoor nu nog een bezoek aan een overheidsloket nodig is, of die op papier verlopen (al dan niet met tussenkomst van notaris), voortaan online te laten verlopen. Dat bespaart in sommige gevallen reiskosten, maar ook het online aanvragen kost minder tijd dan die op papier.
– Een belangrijke besparing zit in de nieuwe functie van digitaal ondertekenen, waardoor voor het afsluiten van contracten geen bijeenkomsten noodzakelijk zijn, dan wel contracten op papier rondgestuurd hoeven te worden. Deze functie is alleen van belang voor bepaalde contracten, omdat de handtekening (nog) geen gekwalificeerde handtekening is. Ook het ondertekenen van meldingen, aanvragen, etc. kan met deze functie.
– De mogelijkheid om een bedrijfsmedewerker te machtigen om bepaalde zaken namens het bedrijf online af te handelen bespaart directeuren en managers (met een hoog uurtarief) veel tijd.
– Het feit dat er één enkel inlogmiddel beschikbaar is voor de gehele overheid, waardoor men niet meer aparte namen/wachtwoorden hoeft te onthouden, betekent gemak en een tijdsbesparing. Idem voor de mogelijkheid om papieren machtigingen te vervangen door online machtigingen en de mogelijkheid om overzicht te behouden op allerlei soorten machtigingen, ook voor de machtigingen die intermediairs krijgen van hun klanten.

Naast de lagere regeldruk bij het voldoen aan informatieverplichtingen vanuit de rijksoverheid, zullen zich soortgelijke kostenbesparingen voordoen bij het voldoen aan verplichtingen vanuit medeoverheden, die trouwens niet tot regeldruk worden gerekend. En in de contacten tussen bedrijven onderling zijn er nog andere voordelen, namelijk:
– Een belangrijke besparing zit in het feit dat commerciële dienstverleners ook hun websites met eHerkenning kunnen ontsluiten als alle bedrijven en organisaties een middel van eHerkenning bezitten, omdat zij dat voor de overheid nodig hebben. Dit levert ook efficiencywinst op de *Business-to-Business*-markt. De mogelijkheid om ook bepaalde commerciële contracten online met een digitale handtekening van eHerkenning te ondertekenen bespaart potentieel ook veel reiskosten.
– Het vrij hoge betrouwbaarheidsniveau verkleint ook het risico op fraude, maar dat voordeel slaat in contacten met overheidsorganisaties bij overheden neer. De kostenbesparing als gevolg van minder schade door identiteitsfraude doet zich ook voor op de *Business-to-Business*-markt.
– Door de eIDAS-verordening ontstaat de mogelijkheid voor bedrijven om digitaal zaken te doen met uitvoeringsorganisaties in alle EU-lidstaten, voor zover die diensten aanbieden op een hoog of vrij hoog betrouwbaarheidsniveau (substantieel). Hierbij is onzeker of die uitvoeringsorganisaties nog aanvullende informatie-eisen stellen voordat zij Nederlandse bedrijven daadwerkelijk toegang geven, dan wel of zij ook toegang verlenen als met een inlogmiddel voor burgers wordt ingelogd.

Minder belastende alternatieven zijn overwogen en soms doorgevoerd. Zo is met enkele grote uitvoeringsorganisaties afgesproken dat zij voor hun digitale dienstverlening in de toekomst een middel op niveau 3 zullen

vereisen. Dit maakt de keuze voor bedrijven, die een eHerkenningsmiddel moeten aanschaffen, een stuk eenvoudiger en kost de kennisname hen minder tijd. Bij de start van eHerkenning is er bewust voor gekozen om eHerkenning niet uit algemene belastinginkomsten te financieren, maar door de partijen te laten betalen die er voordeel bij hebben. Doordat er concurrentie tussen commerciële aanbieders van eHerkenning bestaat, heeft dit o.a. een gunstig effect op prijs. Verder is overwogen om face-to-face controles te vereenvoudigen, zodat dit bedrijven tijd scheelt. De eIDAS-verordening sluit dit uit op betrouwbaarheidsniveau hoog, maar op niveau substantieel is dit wel gerealiseerd.

9.3. Beoordeling door Adviescollege Toetsing Regeldruk[64]

Het college constateert dat de memorie van toelichting na de consultatie op onderdelen is aangepast. De memorie van toelichting geeft invulling aan het advies om de noodzaak van wetgeving scherper te onderbouwen en daarbij aan te geven waarom voor de identificatiemiddelen nieuwe wetgeving noodzakelijk is. Tevens motiveert de toelichting waarom wordt gekozen om publieke en private middelen naast elkaar toe te laten. Het Adviescollege concludeert dat nut en noodzaak van het wetsvoorstel hiermee voldoende zijn toegelicht.

Aan de aanbeveling van het Adviescollege om de betrouwbaarheidsniveaus van eHerkenning te uniformeren en terug te brengen tot de drie niveaus wordt uitvoering gegeven. Aanbevolen is om in overleg met aanbieders van eHerkenningsmiddelen te komen tot een standaardisering van abonnementen en aanvullende diensten. Het is mogelijk dat een standaardisering tot minder kosten zal leiden, maar eHerkenning is een stelsel met concurrerende aanbieders van inlogmiddelen die zich juist moeten onderscheiden om keuzemogelijkheden voor klanten te bieden, zodat klanten optimaal bediend kunnen worden. Geadviseerd wordt het gebruik van machtigingsvoorzieningen bij eHerkenning te vereenvoudigen. Bij de uitwerking van de lagere regelgeving zal rekening gehouden worden met de behoefte aan gebruiksvriendelijke machtigingssystemen.

10. Overgangsrecht en inwerkingtreding

Vanaf de inwerkingtreding van het wetsvoorstel – de inwerkingtreding kan overigens voor de verschillende artikelen of onderdelen daarvan verschillend worden vastgesteld – geldt voor bestuursorganen en aangewezen organisaties de plicht om de toegelaten identificatiemiddelen (burgers) en de erkende identificatiemiddelen (bedrijven) op het niveau substantieel en hoog te accepteren. Bestuursorganen en aangewezen organisaties mogen middelen met betrouwbaarheidsniveau laag – die niet zullen worden toegelaten of erkend – na de inwerkingtreding van dit wetsvoorstel nog wel accepteren voor diensten waarvoor een laag betrouwbaarheidsniveau geldt. Hiervoor zal bij hen een tarief in rekening worden gebracht.

Voor bestuursorganen en aangewezen organisaties geldt voorts dat zij vanaf inwerkingtreding van het wetsvoorstel aan eisen inzake werking, beveiliging en betrouwbaarheid moeten voldoen. Dit is een verantwoord tijdspad, ervan uitgaande dat zij deze eisen reeds in de praktijk hanteren en zij bovendien vanaf het moment van de (internet)consultatie (eind 2016) konden beginnen met een eerste oriëntatie op hetgeen deze wet voor hen meebrengt, en hiermee rekening hebben kunnen houden bij beslissingen over hun toekomstige investeringen voor digitale voorzieningen.

---

[64] *Ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer*

Voor bedrijfs- en organisatiemiddelen en de terzake betrokken (private) diensten die, conform daartoe met de Staat gemaakte afspraken, reeds functioneerden voorafgaand aan inwerkingtreding van dit wetsvoorstel, geldt een overgangsperiode van 18 maanden.

Voorts wordt voorzien in overgangsrecht voor het geval dat een of meerdere private identificatiemiddelen vooruitlopend op de inwerkingtreding van de wet, – na de daarvoor ingerichte procedure – wordt toegelaten. In dat geval wordt de met de desbetreffende private authenticatiedienst gesloten overeenkomst, bedoeld om met private identificatiemiddelen overheidsbreed toegang te verkrijgen tot publieke elektronische dienstverlening, voor de duur van die overeenkomst aangemerkt als een toelating op grond van dit wetsvoorstel.

Tot slot wordt bij wijze van overgangsrecht voor het publieke domein het tijdelijke gebruik van identificatiemiddelen, die het betrouwbaarheidsniveau laag respectievelijk substantieel hebben, mogelijk gemaakt voor elektronische dienstverlening waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is. In algemene zin geldt dat voor het publieke domein dat de acceptatieplicht ingevolge deze wet pas van kracht zal worden, zodra voor de desbetreffende dienstaanbieder de overheidsinfrastuctuur gereed is en de dekkingsgraad van de eID-middelen voor burgers bij de desbetreffende doelgroep adequaat is.

11. Consultatie en advies Autoriteit Persoonsgegevens

11.1. Consultatie

In de periode van 21 december 2016 tot en met 31 maart 2017 is het voorontwerp van dit wetsvoorstel – met als titel »Wet generieke digitale infrastructuur» – aan een brede consultatie onderworpen. Uit deze consultatie is breed draagvlak gebleken voor de centrale doelstellingen van het wetsvoorstel, te weten het verhogen van het betrouwbaarheidsniveau van de digitale toegang tot overheidsdienstverlening, het waarborgen van de continuïteit van het stelsel van elektronische identificatie en het kunnen verplichten van het gebruik van bepaalde standaarden. Uit de consultatie is voorts gebleken dat het nodig is om bij de verdere uitwerking het authenticatiestelsel op enkele onderdelen te vereenvoudigen om de uitvoerbaarheid beter te realiseren. Het wetsvoorstel is op basis daarvan aangepast.

Koppelvlakken en kosten

Het wetsontwerp ging uit van een aansluitplicht voor alle bestuursorganen en aangewezen organisaties van alle erkende identificatiemiddelen, met elk hun eigen, verschillende, technische koppelvlakken: dit zijn de verbindingen die volgens een bepaalde standaard de uitwisseling van gegevens tussen informatiesystemen mogelijk maken. Voor gemeenten en kleinere uitvoeringsorganisaties, zoals de eerstelijns zorgaanbieders, betekent dit een behoorlijke uitvoeringslast. Medeoverheden dringen aan op aansluiting op de identificatieketen met behulp van één koppelvlak. Het blijkt ook voor grote uitvoeringsorganisaties technisch onuitvoerbaar om een groot aantal technische koppelingen te moeten maken. Uit de consultatie blijkt dat met name ook kleine dienstverleners moeten worden «ontzorgd», wat inhoudt dat het makkelijker wordt gemaakt in technisch opzicht om aan te sluiten op het stelsel en dat dit ook juridisch en administratief niet te veel rompslomp oplevert. Uit de consultatiereacties bleek ook een breed gedragen behoefte onder dienstaanbieders om helderheid te krijgen over de verwachte (aansluit)kosten. Partijen wijzen op meerdere koppelvlakken als belangrijke kostendrijver.

De Minister van BZK wil het makkelijker maken voor dienstverleners om aan te sluiten op de nieuwe identificatiemiddelen voor burgers (natuurlijke personen): één koppelvlak, één contract en één factuur voor dienstverleners. Dit vermindert de complexiteit en drukt de aansluitkosten. De beoogde vereenvoudiging vereist nader onderzoek op een aantal punten, waaronder de relatie met de tijdige uitvoering van Europese regelgeving ter zake het gelijkelijk toelaten van Europees erkende identificatiemiddelen op het betrouwbaarheidsniveau «substantieel» of «hoog». De tijdige uitvoering van deze Europese regelgeving, die vanaf medio september 2018 van kracht zal zijn, dient gewaarborgd te zijn. Er is een (technische) voorziening noodzakelijk waardoor bestuursorganen en aangewezen organisaties eenvoudig kunnen aansluiten op de identificatiemiddelen die zij moeten accepteren. Aldus worden zij bij hun elektronische dienstverlening «ontzorgd». Naar aanleiding van de consultatiereacties is in het wetsvoorstel opgenomen dat de Minister verantwoordelijk is voor de inrichting en werking van een routeringsvoorziening, teneinde de toegang tot elektronische dienstverlening te faciliteren.

Multimiddelenaanpak

Uit de consultatie bleek voorts dat de opvattingen over de (uniforme) eisen aan private middelen sterk divergeren onder potentiële leveranciers van private identificatiemiddelen. Sommige potentiële leveranciers kunnen zich niet vinden in de eisen aan de identificatiemiddelen en stellen dat met andere oplossingen dezelfde mate van beveiliging tegen lagere kosten gerealiseerd kan worden. Zonder aanpassing van de eisen (maatwerk) zullen zij waarschijnlijk niet participeren in het publieke deel van het eID-stelsel. Andere partijen vinden dat de eisen uniform moeten worden opgelegd aan alle erkende leveranciers en verzoeken maatregelen te treffen om het commerciële perspectief van de multimiddelenaanpak voor private middelenleveranciers te vergroten, anders bestaat het risico dat er onvoldoende private middelen beschikbaar komen.

De erkenning van de verschillende identificatiemiddelen en gerelateerde diensten die aan uniforme eisen voldoen, onder uitsluiting van andere middelen, en het bijbehorende bestuursrechtelijk toezicht op die middelen, is komen te vervallen. In het wetsvoorstel is de mogelijkheid opgenomen van de toelating van een of meer private middelen, als alternatief naast publieke middelen, op basis van op de eIDAS-verordening gebaseerde eisen waarop gericht controle kan worden uitgeoefend. Om de kosten te beheersen is een brede (markt)verkenning uitgevoerd naar de wijze waarop het gebruik van private middelen op een financieel haalbare wijze is te realiseren. In het vervolg hierop zal de Minister van BZK een privaat authenticatiemiddel toelaten indien uit het proces van verwerving blijkt dat een of meerdere private middelen aan de eisen van BZK voldoen om als betrouwbaar en betaalbaar marktalternatief voor DigiD te kunnen fungeren.

Maatwerk

Verder is in de consultatie door organisaties naar voren gebracht dat maatwerk en uitzonderingen mogelijk moeten zijn, bijvoorbeeld op de regel dat uitsluitend toegang wordt verleend met toegelaten middelen. Het wetsvoorstel is aangepast zodat volgens bij lagere regelgeving te stellen regels dienstverleners mogen afwijken van de plicht om de toegelaten en erkende middelen accepteren. Dit kan slechts met het oog op innovatie of dienstverlening aan een welbepaalde doelgroep. Ten behoeve van maatwerk is ook artikel 3, dat het gebruik van open standaarden reguleert, hergeformuleerd. In de wetsbepaling is geëxplici-

teerd dat bij de aanwijzing van de standaard het organisatorisch en functioneel toepassingsgebied van de standaard wordt omschreven. Zaken als voor welke (bestuurs)organen, colleges en rechtspersonen met een wettelijke taak, in welke gevallen en vanaf welk moment de standaard toepasselijk is, moeten worden omschreven in de algemene maatregel van bestuur. Het functionele en organisatorische toepassingsbereik zal per geval, dat wil zeggen per aan te wijzen standaard, worden geregeld. Een standaard kan bijvoorbeeld ongeschikt zijn om door de zogeheten b-bestuursorganen of door rechtspersonen met een wettelijke taak te worden toegepast. In dat geval biedt een beperkt organisatorisch of functioneel toepassingsgebied uitkomst.

Tijdens de consultatie en in de daaropvolgende periode is de uitvoerbaarheid van het wetsvoorstel beoordeeld. Het wetsvoorstel bevat een aantal delegatiebepalingen op basis waarvan (lagere) regelgeving tot stand zal komen. Ook deze regelgeving zal steeds worden getoetst op uitvoerbaarheid, opdat hiervan een volledig beeld ontstaat. De besluitvorming omtrent de vaststelling van deze regelgeving zal, nadat de departementen in de gelegenheid zijn gesteld de uitvoerbaarheid te (laten) toetsen, via de ministerraad verlopen – voor zover in het interdepartementale voortraject geen overeenstemming is bereikt – zodat de betrokkenheid van de verschillende departementen en daarmee de uitvoerbaarheid in alle beleidsdomeinen wordt bevorderd.

11.2. Advies Autoriteit Persoonsgegevens

Naar aanleiding van het advies van de Autoriteit Persoonsgegevens[65] zijn het wetsvoorstel en de memorie van toelichting op een aantal punten aangevuld. In artikel 16, eerste lid, zijn de doelen voor de verwerking van persoonsgegevens aangescherpt, waardoor de beginselen van proportionaliteit en subsidiariteit beter kunnen worden uitgewerkt in de voorgenomen algemene maatregel van bestuur. In artikel 23 is gespecificeerd dat bij de evaluatie van de wet aandacht zal worden geschonken aan de vraag, of de getroffen (technische, organisatorische en juridische) maatregelen op het gebied van beveiliging en privacybescherming nog steeds voldoende zijn.
Voor wat betreft identificatiemiddelen op betrouwbaarheidsniveau laag is een overgangsbepaling in het wetsvoorstel opgenomen, die mogelijk maakt dat deze middelen tijdelijk gebruikt worden voor dienstverlening waarvoor authenticatie op een hoger betrouwbaarheidsniveau vereist is.

Gevolg gevend aan het advies van de Autoriteit Persoonsgegevens is nader toegelicht waarom de regels met betrekking tot de verwerking van persoonsgegevens niet worden uitgewerkt in de wet zelf maar bij algemene maatregel van bestuur en wordt benadrukt dat het wetsvoorstel en de daarop gebaseerde algemene maatregel van bestuur de normen van de AVG nader uitwerken (verdiepen). Ten aanzien van te nemen cryptografische maatregelen is in de toelichting aangegeven dat deze om redenen van techniek-onafhankelijkheid en toekomstbestendigheid niet in de wet worden opgenomen. Verduidelijkt is voorts op welke wijze in de voorziening BSN-K de functies authenticeren en informeren technisch van elkaar gescheiden zijn. Technische scheiding vormt een onderdeel van *privacy by design*; het geheel van privacyverhogende maatregelen waaraan al tijdens de ontwikkeling van producten en diensten aandacht wordt besteed. Toegelicht is dat nadere regulering van de door een bestuursorgaan of aangewezen organisatie te overleggen auditverklaring bij of krachtens algemene maatregel van bestuur zal geschieden.

---

[65] *Advies van 13 oktober 2017, nr Z2017–06920, ter inzage gelegd bij het Centraal Informatiepunt Tweede Kamer*

II Artikelsgewijs

Artikel 1

Dit artikel bevat de begripsomschrijvingen. Deze spreken voor zich. Voor wat betreft terminologie wordt in deze wet zoveel mogelijk aangesloten bij de eIDAS-verordening en de op grond daarvan vastgestelde uitvoeringsverordeningen.

Authenticatie, identificatiemiddel en elektronische dienstverlening

Het woord «elektronisch» ziet in onderhavig wetsvoorstel uitsluitend op dienstverlening via internet via elektronische authenticatie, dat wil zeggen de dienstverlening via internet waarbij de identiteit van de natuurlijke persoon of de rechtspersoon door een (elektronisch) identificatiemiddel wordt geverifieerd. Alhoewel het woord «elektronisch» in andere wetgeving zoals in de Algemene wet bestuursrecht onderscheidenlijk in de praktijk ook wel een bredere betekenis heeft, en mede betrekking heeft op verkeer per fax of sms, of op een telefoongesprek, dan wel communicatie via internet die niet via elektronische authenticatie plaatsvindt, zoals het e-mailverkeer, betreft het in dit wetsvoorstel dus uitsluitend de online-communicatie waarvoor online-authenticatie is vereist. In de eIDAS-verordening wordt in dit verband gesproken over «het aanbieden van een onlinedienst waarvoor elektronische identificatie met gebruikmaking van een elektronisch identificatiemiddel vereist is».

Gevolg is, dat deze wet niet van toepassing is voor dienstverlening waarvoor de elektronische weg niet openstaat. De elektronische weg staat onder meer niet open, als a. bij of krachtens de wet is bepaald dat een bericht niet langs elektronische weg kan worden verzonden of b. een vormvoorschrift zich tegen elektronische verzending verzet. Van dergelijke gevallen is bijvoorbeeld sprake als bij of krachtens de wet is bepaald dat een aanvraag in persoon dient te geschieden of dat het hieruit impliciet volgt. Zo dient betrokkene voor aanvraag van een Paspoort een vingerafdruk te geven. Dit laatste kan niet via internet. Daarnaast staat voor het bestuursorgaan in principe de elektronische weg niet open als de burger heeft aangegeven niet van de elektronische weg gebruik te willen maken.

De elektronische weg kan expliciet bij wettelijk voorschrift voorgeschreven worden, zoals ingevolge de Wet elektronisch berichtenverkeer belastingdienst en de Omgevingswet. Voorts wordt op grond van het voorstel van wet modernisering elektronisch bestuurlijk verkeer (Awb) de beschikbaarheid (openstelling) van de elektronische weg verplicht gesteld bij berichten die onderdeel uitmaken van een procedure inzake een besluit, een voorgeschreven melding of een klacht; burgers krijgen het recht op elektronische communicatie met de overheid. Dit hoeft overigens niet te betekenen dat onderhavig wetsvoorstel van toepassing is op deze berichten. Dit is alleen het geval indien een elektronische authenticatie voor dit elektronisch verkeer vereist is, en wel op het betrouwbaarheidsniveau substantieel of hoog. Het wetsvoorstel spreekt in dit verband over elektronische dienstverlening.

Betrouwbaarheidsniveaus

Acceptatie heeft betrekking op diensten via internet waarvoor een substantiële of hogere mate van vertrouwen vereist is terzake van de vraag, of de gebruiker ook degene is die hij opgeeft of beweert te zijn.[66] Dit is de terminologie die de eIDAS-verordening hanteert voor elektro-

[66] *Zie artikel 8, tweede lid, onderdelen b en c, van de eIDAS-verordening.*

nische authenticatie op het niveau substantieel en hoog. Dit zal nader uitgewerkt worden. Op grond van dit wetsvoorstel zullen bij ministeriële regeling regels worden gesteld over het vereiste betrouwbaarheidsniveau van dienstverlening. Aan de hand hiervan dienen bestuursorganen en aangewezen organisaties zelf hun diensten in te delen (classificeren). Het Forum Standaardisatie heeft een handreiking voor overheidsorganisaties ontwikkeld onder de titel «Betrouwbaarheidsniveaus voor digitale dienstverlening». De uitgangspunten van deze handreiking zal mede als basis dienen voor de op te stellen ministeriële regeling. Zo zal voor de aanvraag van een reguliere omgevingsvergunning geen elektronische authenticatie op het betrouwbaarheidsniveau substantieel of hoog nodig zijn. Dit geldt bijvoorbeeld wel voor de aanvraag van een sociale uitkering of een toeslag, om aanvragen waarbij medische gegevens van de betrokkene een rol spelen of bij het doen van aangifte van bepaalde misdrijven. Bij voorgeschreven meldingen op het niveau substantieel of hoog gaat het bijvoorbeeld om de aangifte van een geboorte, huwelijk of overlijden, of om een belastingaangifte.

Artikel 2

Lid 1

Dit artikel regelt de reikwijdte van de wet, primair toegesneden op de publieke en semipublieke sectoren, die gebruik maken van de generieke digitale infrastructuur. Deze wet is toepasselijk wanneer het gaat om elektronische dienstverlening zoals gedefinieerd in artikel 1: verlening van elektronische diensten aan natuurlijke personen, ondernemingen of rechtspersonen ter uitoefening van een publieke taak, in het algemeen belang of waarbij het burgerservicenummer wordt verwerkt, door een bestuursorgaan als bedoeld in artikel 1:1, eerste lid, onderdeel a, van de Algemene wet bestuursrecht of een aangewezen organisatie, waarvoor ingevolge artikel 6, tweede lid, authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is.
Waar in deze wet 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 op bijvoorbeeld de Dienst Uitvoering Onderwijs (DUO), de Belastingdienst en zelfstandige bestuursorganen (ZBO's) als de Sociale Verzekeringsbank (SVB), de Kamer van Koophandel (KvK), de Rijksdienst voor het Wegverkeer (RDW) en de Huurcommissie. [67] Bij de a-bestuursorganen kunnen aard en kenmerken van hun taken en werkzaamheden elektronische dienstverlening aan burgers en bedrijven met zich brengen. Daarom vallen deze bestuursorganen binnen de werkingssfeer van de hoofdstukken 3 tot en met 7 voorzover zij elektronische diensten verlenen waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is.

De zogenaamde 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, worden niet onder het eerste lid begrepen.

[67] *https://almanak.zboregister.overheid.nl/*

Lid 2–3

Naast a-bestuursorganen, vallen onder de reikwijdte van de hoofdstukken 3 tot en met 7 de organisaties behorende tot een in de bijlage bij deze wet aangewezen categorie alsmede de organisaties die bij besluit van de Minister van BZK in overeenstemming met de Minister(s) wie het mede aangaat zijn aangewezen. Het gaat hierbij om semipublieke of private organisaties die elektronische diensten verlenen ter uitoefening van een publieke taak, in het algemeen belang of waarbij het burgerservicenummer wordt verwerkt, waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is. Deze organisaties hebben gemeen dat het hen (wettelijk) is toegestaan bij hun taken en werkzaamheden het burgerservicenummer te gebruiken. De door hen alsmede de door (a-) bestuursorganen gerealiseerde elektronische dienstverlening wordt kortheidshalve ook wel aangeduid met «publiek domein». Bestuursorganen en aangewezen organisaties in de zin van de onderhavige wet worden ook wel aangeduid als «dienstverleners». Voorts zijn expliciet rechterlijke instanties opgenomen. Het betreft onafhankelijke, bij de wet ingestelde organen die met rechtspraak zijn belast. Voor hen gelden, tenzij anders is bepaald, dezelfde rechten en verplichtingen ingevolge deze wet als voor bestuursorganen en aangewezen organisaties. Benadrukt zij, dat deze wet de rechterlijke onafhankelijkheid niet doorkruist. De beslissingsvrijheid van de rechter en de toegang tot de rechter worden niet ondergraven door de bij of krachtens deze wet gestelde regels over de acceptatie van toegelaten en erkende identificatiemiddelen, de classificering van de betrouwbaarheidsniveaus en de werking, betrouwbaarheid en beveiliging van de toegang tot elektronische diensten die zij verlenen, aangezien het hierbij gaat om de daaraan gerelateerde informatiesystemen (ICT) en bedrijfsvoering. Hierop wordt, voor wat betreft rechtbanken en hoven, toezicht gehouden door de Raad voor de Rechtspraak; voor wat betreft de Afdeling Bestuursrechtspraak en de Hoge Raad, zijn in dit verband de Ministers van BZK respectievelijk Justitie en Veiligheid verantwoordelijk.

Lid 4–8

De in het vierde en vijfde de lid opgenomen criteria voor toevoeging respectievelijk verwijdering van categorieën aan de bijlage bij algemene maatregel van bestuur zijn ook de criteria die zijn gehanteerd bij de opstelling van de in dit wetsvoorstel opgenomen bijlage. Organisaties die niet in een categorie zijn onder te brengen, zullen op grond van dezelfde criteria bij een gezamenlijk besluit van de Minister van BZK en de betrokken vakminister worden aangewezen. Het gaat hierbij om (categorieën van) instanties die handelen ter uitoefening van een (semi-)publieke taak, in het algemeen belang of waarbij het burgerservicenummer wordt verwerkt; ze hebben gemeen dat ze krachtens wettelijk voorschrift gerechtigd zijn om het burgerservicenummer te gebruiken voor de uitvoering van hun taken en verlenen elektronische diensten aan natuurlijke personen en ondernemingen of rechtspersonen op het betrouwbaarheidsniveau hoog of substantieel. Deze organisaties zijn momenteel doorgaans toegankelijk via het huidig beschikbare publieke identificatiemiddel op betrouwbaarheidsniveau laag. Vooralsnog zijn op de bijlage de volgende categorieën van organisaties aangewezen:

Universiteiten en hogescholen

Er is een aantal organisaties dat op basis van de onderwijswetgeving het burgerservicenummer gebruikt en voor bepaalde diensten ook het beschikbare identificatiemiddel (DigiD) op betrouwbaarheidsniveau laag gebruikt. Dit zijn de onderwijsinstellingen vallend onder de Wet op het

hoger onderwijs en wetenschappelijk onderzoek. Het gaat hier om de universiteiten, hogescholen, de Open Universiteit, de levensbeschouwelijke universiteiten, de rechtspersoon met volledige rechtsbevoegdheid die initiële opleidingen verzorgen en de instellingen of rechtspersonen met volledige rechtsbevoegdheid die postinitiële masteropleidingen verzorgen. Een deel van de universiteiten heeft een publiekrechtelijke grondslag, en valt daarom reeds onder onderhavig wetsvoorstel omdat zij a-bestuursorgaan zijn.

Pensioenuitvoerders

Onder «pensioenuitvoerders» wordt in artikel 1 van de Pensioenwet verstaan een ondernemingspensioenfonds, een bedrijfstakpensioenfonds, een algemeen pensioenfonds, of een premiepensioeninstelling of (pensioen)verzekeraar die zetel heeft in Nederland. Hierbij gaat het zowel om organisaties die ouderdomspensioen en nabestaandenpensioen, als de organisaties die een arbeidsongeschiktheidpensioen aanbieden.

Zorgaanbieders, indicatieorganen en zorgverzekeraars

In 2008 en 2009 is de Wet gebruik burgerservicenummer in de zorg in werking getreden. De onder deze wet vallende organisaties en beroepsuitoefenaars zijn verplicht het burgerservicenummer van hun cliënten te gebruiken. Het betreft hier zorgaanbieders als bedoeld in de Wet kwaliteit, klachten en geschillen zorg,indicatieorganen en zorgverzekeraars; zij verlenen diensten aan private afnemers. Als zorgverzekeraars zijn aan te merken de uitvoerders als bedoeld in artikel 1.1.1 van de Wet langdurige zorg, zorgverzekeraars als bedoeld in artikel 1, onder b, van de Zorgverzekeringswet en verzekeringsondernemingen als bedoeld in de EU-richtlijn solvabiliteit II voorzover deze verzekeringen aanbieden of uitvoeren krachtens welke het verzekerde risico de behoefte aan zorg is waarop bij of krachtens de Algemene Wet Bijzondere Ziektekosten geen aanspraak bestaat en waarbij de verzekerde prestaties het bij of krachtens de Zorgverzekeringswet geregelde te boven gaat.

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 van BZK 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 elektronische diensten verleent waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist, zal het desbetreffende aanwijzingsbesluit worden ingetrokken.

De werkingssfeer, zoals hiervoor geschetst, sluit zoveel mogelijk aan bij de werkingssfeer van de eIDAS-verordening. Teneinde de wederzijdse erkenning van identificatiemiddelen op betrouwbaarheidsniveau substantieel en hoog te realiseren (artikel 6 eIDAS-verordening), hanteert deze verordening het begrip «openbare instantie», dat 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, punt 7, eIDAS-verordening).

Artikel 3

Lid 1

Dit artikel 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 (o.a. de Eerste en Tweede Kamer, de rechterlijke macht, de Raad van State en de Nationale ombudsman) en zogeheten rechtspersonen met een wettelijke taak (RWT)[68] tot de toepassing van de ingevolge het tweede lid aangewezen standaarden.

Standaarden zijn afspraken over bijvoorbeeld elektronische gegevensuitwisseling, toegankelijkheid of beveiliging, vastgelegd in zogeheten specificatiedocumenten, die beschrijven hoe gegevens eruitzien, 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.[69] Afwijken mag alleen in geval van zwaarwegende redenen; verantwoording hierover moet worden afgelegd in het jaarverslag. In bepaalde gevallen kan echter de inherente afwijkingsmogelijkheid[70] 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 BZK, 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

---

[68] *Voor een register met RWT's zie: www.algemenerekenkamer.nl*

[69] *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.*

[70] *Niet alle standaarden worden breed toegepast, zo blijkt uit de jaarlijkse monitor van het Forum Standaardisatie aan de hand van overlegde jaarverslagen en aanbestedingen.*

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 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.[71] 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 *s*tandaard 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

[71] *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.*

algemene maatregel van bestuur wordt vervolgens nogmaals brede interdepartementale afstemming bewerkstelligd in het voortraject.

Een voorbeeld van toepassing van dit artikel is het verplicht stellen van de standaard inzake toegankelijkheid van overheidswebsites voor mensen met een functiebeperking. 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.[72]Deze standaard is wegens het ontbreken van een formeel-wettelijke basis nu op grond van artikel 89 Gondwet, tijdelijk, in afwachting van de voorgestelde bepaling, geregeld in het Tijdelijk besluit digitale toegankelijkheid overheid.
Daarnaast zal een aantal veiligheidsstandaarden in aanmerking komen om te worden aangewezen,[73] alsmede de (koppelvlak)standaarden Digikoppeling.[74] Benadrukt zij, dat het hierbij gaat om reeds bestaande standaarden. Inhoudelijk brengen deze derhalve niets nieuws; bij de toepassing ervan zal echter niet langer een inherente afwijkingsmogelijkheid bestaan.

Lid 4

Bij algemene maatregel van bestuur kunnen nadere regels worden gesteld omtrent aan te wijzen standaarden. Onder meer kan worden bepaald dat de betrokken organen op hun website een actuele verklaring over de toepassing van de aangewezen standaard publiceren. Dit bevordert transparantie in de richting van burgers, bedrijven en de Minister van BZK. Benadrukt zij dat het bij algemene maatregel van bestuur verplichten van de toepassing van een standaard (tevens) strekt tot bescherming van burgers en bedrijven. Ook kan bij algemene maatregel van bestuur aan organen die onder het toepassingsbereik van de voorgeschreven standaard vallen een auditplicht worden opgelegd. Alsdan worden tevens regels gesteld over de wijze waarop aan de Minister moet worden gerapporteerd, de frequentie etc.

Lid 5

De Minister van BZK is bevoegd een – bindende – aanwijzing te geven aan een orgaan waarvoor de verplichting tot toepassing van een standaard geldt, indien dit orgaan een concurrerende standaard hanteert en er sprake is van niet-naleving van de desbetreffende algemene maatregel van bestuur. In casu geldt de aanwijzingsbevoegdheid dus veeleer als reguleringsinstrument en sluitstuk op de bovenliggende amvb dan als bestuurlijke sanctie. Het ligt in de rede deze te hanteren in overeenstemming met de Minister die het mede aangaat. Het betreft een besluit in de zin van de Awb, waartegen bezwaar en beroep open staat.

---

[72] *ISO/IEC-standaard 40500:2012 en EU/EN-standaard 301 549 V1.1.1 (2014–02). Tevens: richtlijn (EU) 2016/2102 van 26 oktober 2016 inzake de toegankelijkheid van de websites en mobiele applicaties van overheidsinstanties, geïmplementeerd in het Besluit digitale toegankelijkheid overheid (zelfstandige amvb, welke zal worden gebaseerd op de onderhavige wet wanneer deze in werking treedt).*

[73] *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.*

[74] *https://www.logius.nl/diensten/digikoppeling/*

Artikel 4

Lid 1

Dit artikel biedt de grondslag voor vaststelling van regels over de werking, betrouwbaarheid en beveiliging van de toegang tot elektronische diensten door bestuursorganen en aangewezen organisaties. Bestuursorganen en aangewezen organisaties vormen een belangrijke schakel in de authenticatieketen waarin de processen op elkaar zijn aangesloten om erkende of toegelaten identificatiemiddelen te kunnen accepteren. Het zijn immers hun elektronische diensten die door burgers en bedrijven worden afgenomen; zij moeten zich daarvoor bij de bestuursorganen en aangewezen organisaties authenticeren met al dan niet toegelaten respectievelijk 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 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[75] 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, in samenspraak met de medebetrokken Ministers, worden bezien welke relevante en toepasselijke (elementen van) standaarden zullen worden opgenomen en met ingang van welke datum verplichtstelling dan in de rede ligt. 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 de dienstverleners zelf om er zorg voor te dragen dat hun systemen daadwerkelijk aan de gestelde eisen voldoen.

Lid 2–3

Om te laten toetsen of de 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 regulier een verklaring van een auditor te overleggen aan de Minister. De

---

[75] *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).*

verklaring van de auditor sluit aan bij de systematiek die in de praktijk reeds sinds 2011 functioneert (de zgn. DigiD-assessments). Indien uit de verklaring van de auditor blijkt dat een bepaald bestuursorgaan of een aangewezen organisatie niet (volledig) aan de gestelde regels voldoet, zal contact worden opgenomen met de betreffende dienstverlener en wordt, afhankelijk van aard en ernst van de niet-naleving, afgesproken welke maatregelen nodig zijn en op welke termijn die genomen worden. Indien uit de auditverklaringen zou blijken dat verbetering nodig is en na herhaaldelijke aanmaningen de benodigde en noodzakelijke verbeteringen niet worden aangebracht, en in ieder geval indien de informatieveiligheid in het geding is, kan *ultimo* de bijzondere bevoegdheid voor de Minister om een noodmaatregel te treffen, uitkomst bieden.
De te overleggen 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 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 stringentere handhavingsinstrumenten worden overwogen. Uitgangspunt is, dat de betrokken 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 reguliere 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, in overleg met het vakdepartement dat op het betrokken domein bevoegd is, al dan niet via de eigen inspectiediensten of toezichthouders actie wordt ondernomen en de betrokken organisatie wordt aangesproken. De voorgeschreven audit beslaat de 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* en ISO-normen), 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 zogeheten 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.[76] Over het uitvoeren van de audits (proces, periodiciteit etc.) worden nadere regels gesteld, waarbij zoveel mogelijk zal worden aangesloten bij de door de dienstverleners in

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

de desbetreffende sectoren reeds gehanteerde systemen en gebruiken. De auditrapporten zijn om redenen van veilgheid in beginsel niet openbaar. Hierop zijn de geldende regels ten aanzien van openbaarheid, zoals neergelegd in de Wet openbaarheid van bestuur, van toepassing.

Artikel 5

Dit artikel betreft de ministeriële verantwoordelijkheid voor het beheer van de GDI.

Lid 1

Aanhef en onderdeel a

Op de Minister rust de zorgplicht voor de generieke digitale infrastructuur. Het gaat hierbij om vele (ICT-)voorzieningen en functionaliteiten, die voortdurend aan ontwikkeling onderhevig zijn. Dit wetsvoorstel heeft als belangrijkste onderwerp (naast standaarden, zie artikel 3) elektronische identificatie. Om die reden bevat het onderhavige artikel een aanduiding van de op dit moment voorziene eID-gerelateerde voorzieningen. Deze zijn, omwille van een zekere toekomstbestendigheid, functioneel en techniekonafhankelijk geformuleerd, en worden nader uitgewerkt, zo blijkt uit de delegatiebepalingen elders in het wetsvoorstel. De opsomming is indicatief («waaronder»), hetgeen betekent dat de zorgplicht van de Minister zich ook uitstrekt tot andere infrastructuur van generieke aard die de (verdere) digitalisering van het openbaar bestuur beoogt. Zie voorts de toelichting bij het vijfde lid.

Teneinde zorg te kunnen dragen voor veilige en betrouwbare toegang tot elektronische diensten van bestuursorganen en aangewezen organisaties, bevat onderdeel a de verantwoordelijkheid voor identificatiemiddelen waarmee natuurlijke personen (burgers) zich kunnen identificeren («wie ben je?») en authenticeren («ben je wie je zegt te zijn?») bij het afnemen van oftewel toegang verkrijgen tot *online* diensten zoals een vergunning of een toeslag. Op dit moment functioneert als publiek identificatiemiddel het van overheidswege uitgegeven middel met de merknaam «DigiD», dat betrouwbaarheidsniveau laag heeft. Dit wordt om redenen van betrouwbaarheid en veiligheid uitgefaseerd. Het onderhavige wetsvoorstel heeft daarom primair betrekking op identificatiemiddelen 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). Het gaat daarbij in de eerste plaats om een middel op betrouwbaarheidsniveau substantieel.[77] In de tweede plaats worden een e-NIK (elektronische Nederlandse identiteitskaart) en een e-rijbewijs ontwikkeld. Dat zijn publieke identificatiemiddelen 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 van BZK primair verantwoordelijk. De verantwoordelijkheid van

[77] *Authenticatie op niveau substantieel werkt als volgt. Een burger bevestigt eenmalig 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 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 gecontroleerd of het betreffende identiteitsdocument nog in omloop is. Na deze eenmalige bevestiging van de identiteit is DigiD «opgewaardeerd» in die zin, dat het betrouwbaarheidsniveau substantieel wordt afgegeven aan het bestuursorgaan of de aangewezen organisatie waarbij de betreffende burger inlogt.*

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 (Paspoortwet) en het rijbewijs (Wegenverkeerswet 1994) nieuwe taken en grondslagen voor gegevensverwerking zullen worden opgenomen die verband houden met het opnemen van de authenticatiefunctie op deze documenten.[78]
De zorg voor publieke middelen op de betrouwbaarheidsniveaus substantieel en hoog betreft elke natuurlijke persoon (burger) waaraan een burgerservicenummer is uitgegeven, die tevens houder is van een Nederlands paspoort, identiteitskaart of rijbewijs (ten behoeve van uitgifte van een middel op niveau 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 (ten behoeve van uitgifte van een middel op niveau hoog, d.w.z. eNIK en eRijbewijs). Voor wat betreft deze publieke middelen is vooralsnog dus sprake van een beperktere groep rechthebbenden dan terzake van het huidige DigiD, dat beschikbaar is voor ingezetenen alsmede voor niet-ingezetenen met de Nederlandse nationaliteit. Er wordt evenwel toegewerkt naar een bredere kring rechthebbenden, en uiteindelijk ook feitelijk een hoge dekkingsgraad, op een hoogbetrouwbaar middel.

Onderdeel b

Zowel burgers als bedrijven (waaronder natuurlijke personen die een onderneming drijven) hebben behoefte om anderen («de gemachtigde») te machtigen om voor hen overheidsdiensten te verrichten of af te nemen. Een machtiging is een verklaring of actie waarmee de bevoegdheid wordt verleend om in naam van de verlener van de machtiging een feitelijke handeling uit te voeren. De wens van zowel publieke als private organisaties om diensten in toenemende mate elektronisch aan te bieden brengt met zich mee dat burgers en bedrijven gebruik moeten kunnen maken van voorzieningen die hen in staat stellen om machtigingen elektronisch te (laten) registreren en te effectueren.
Teneinde bij te dragen aan een veilige en betrouwbare elektronische authenticatie in het verkeer met bestuursorganen en aangewezen organisaties, draagt de Minister zorg voor een voorziening die het mogelijk maakt dat een elektronische verklaring wordt afgegeven waaruit blijkt dat een natuurlijke persoon, al dan niet handelend als drijver van een onderneming, of rechtspersoon gemachtigd is namens een (andere) natuurlijke persoon op te treden bij de toegang tot elektronische dienstverlening. In deze voorziening, ook wel aangeduid als publieke machtigingsdienst, wordt vastgelegd 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 op dit moment DigiD Machtigen. Met behulp van deze voorziening 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. Veelvoorkomend is het machtigen van een familielid, belastingadviseur of accountant. 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

[78] *Vanzelfsprekend mogen de nieuwe data niet interfereren met de informatie die (ingevolge Europese regelgeving) op rijbewijzen moet worden opgenomen.*

met 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.[79] De machtigingsdienst controleert thans niet of de aan de registratie ten grondslag liggende volmacht in alle opzichten rechtsgeldig is, dus bijvoorbeeld of de vertegenwoordigde handelingsbekwaam was op het moment van afgeven van de machtiging en registratie ervan.

De publieke machtigingsdienst kan op den duur 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 deze 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 voorziening verschaft in ieder geval de mogelijkheid om de bevoegdheid tot het handelen namens natuurlijke personen te verifiëren. Daarnaast bestaat de noodzaak om vertegenwoordigingsbevoegdheid te kunnen verifiëren in een stelsel van authenticatie van rechtspersonen en natuurlijke personen die een onderneming drijven (handelen in de uitoefening van een beroep of bedrijf). Ook hier heeft de Minister een verantwoordelijkheid (zie onderdeel f en de artikelen 11–15). Veel bestuursorganen en aangewezen organisaties verlenen diensten aan burgers (natuurlijke personen) en bedrijven (rechtspersonen en natuurlijke personen die een onderneming drijven). Zij hebben derhalve van doen met authenticatie («ben je wie je zegt te zijn») en autorisatie («wat mag je») door of namens burgers en bedrijven. Vanuit de ambitie van het kabinet dat dienstverleners moeten kunnen vertrouwen op veilige en betrouwbare elektronische vastlegging (registratie) van authenticaties en bevoegdheden en ten bewijze hiervan geleverde kenmerken en gegevens van natuurlijke personen of rechtspersonen (attributen, zoals burgerservicenummer of Kamer van Koophandelnummer), kan worden bezien op welke wijze dienstverleners gefaciliteerd kunnen worden bij het verifiëren van vertegenwoordigings-bevoegdheid bij diverse typen machtigingsrelaties waarmee dienstverleners geconfronteerd worden. Mogelijk resulteert dit in een ontwerp van een stelsel van voorzieningen waarin diverse typen machtigingen geregistreerd, geëffectueerd en ingezien kunnen worden. De verdere ontwikkeling op het gebied van machtigen en attributen kan de ambitie vormen voor een volgende tranche.

[79] *Voor de volledigheid wordt er op gewezen, dat in het kader van de publieke machtigingsdienst ook telefonische helpdesk functies worden ondersteund.*

Onderdeel c

De Minister van BZK is verantwoordelijk voor de inrichting en werking van een routeringsvoorziening, teneinde de toegang tot elektronische dienstverlening te faciliteren. In deze (technische) voorziening worden verschillende koppelvlakken (verbindingen die volgens een bepaalde standaard de uitwisseling van gegevens tussen informatiesystemen mogelijk maken) ontsloten, waardoor bestuursorganen en aangewezen organisaties eenvoudig kunnen aansluiten op de identificatiemiddelen voor burgers die zij moeten accepteren. Aldus worden zij bij hun elektronische dienstverlening aan burgers «ontzorgd». De Minister van BZK kan toestaan dat dienstverleners (tijdelijk) aansluiten op een andere routeringsvoorziening dan bovengenoemde routeringsvoorziening, teneinde het accepteren van toegelaten middelen door dienstverleners te faciliteren.

Onderdeel d

Om redenen van veiligheid en betrouwbaarheid draagt de Minister zorg voor een voorziening die het mogelijk maakt dat de identiteit van een natuurlijke persoon, onderneming of rechtspersoon die een elektronische dienst afneemt bij een bestuursorgaan of aangewezen organisatie op unieke wijze geïdentificeerd kan worden. Deze voorziening wordt ook wel het BSN-Koppelregister (BSN-K) genoemd. Via het BSN-K worden toegelaten identificatiemiddelen geschikt (gemaakt), zodat hiermee elektronische diensten kunnen worden afgenomen 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. 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 technische, maatregelen. Het gaat hierbij om feitelijke maatregelen die, om tegemoet te kunnen komen aan het benodigde beveiligings- en betrouwbaarheidsniveau (onder meer om herleiding tot een natuurlijke persoon te voorkomen) voortdurend in ontwikkeling zijn, zoals cryptografische maatregelen. De genomen maatregelen zullen regelmatig onderhevig zijn aan een privacy impact analyse, teneinde te bezien of ze uit een oogpunt van veiligheid en privacybescherming nog steeds voldoende zijn.

De verschillende functies van het BSN-K zijn vanuit het oogpunt van veiligheid en privacybescherming zoals gezegd technisch van elkaar gescheiden (onderdeel van *privacy by design*). Uit beveiligingsoogpunt wordt de gebruiker geïnformeerd over de status van zijn middelen; dit geschiedt met behulp van een inzagefunctie. Op deze wijze kan eveneens eventueel misbruik of oneigenlijk gebruik, bijvoorbeeld door een ander dan gebruiker (identiteitsfraude) worden gesignaleerd. Niet geregistreerd wordt welke transacties met welk(e) bestuursorgaan of aangewezen organisatie zijn verricht. Deze transacties worden geregistreerd bij de authenticatiedienst van het betreffende middel.

Onderdeel e

Dit onderdeel verankert de verantwoordelijkheid van de Minister voor het beheer van het stelsel voor identificatie van ondernemingen en rechtspersonen, zoals dit nader wordt uitgewerkt in de artikelen 11–15. Benadrukt zij dat, hoewel dit wetsvoorstel een onderdeel inzake elektronische dienstverlening aan burgers (natuurlijke personen) en een onderdeel

inzake dienstverlening aan bedrijven (ondernemingen of rechtspersonen) bevat, er sprake is van samenhang. Zo geschiedt de beoordeling van toe te laten middelen (burgers) en te erkennen middelen (bedrijven) op vergelijkbare wijze, wordt deels van dezelfde voorzieningen gebruik gemaakt en gelden er gemeenschappelijke bepalingen, bijvoorbeeld op het gebied van (classificering van) betrouwbaarheidsniveaus en informatieveiligheid. Uitgangspunt is – zie de slotzin van dit lid – dat de Minister in het kader van zijn verantwoordelijkheid voor de toegang tot elektronische dienstverlening door bestuursorganen en aangewezen organisaties aan burgers en bedrijven zorg draagt voor interoperabiliteit.

Onderdeel f

De Minister van BZK is verantwoordelijk voor voorzieningen voor elektronisch berichtenverkeer met en informatieverschaffing aan natuurlijke personen, ondernemingen en rechtspersonen. Het gaat hierbij in de eerste plaats om hetgeen (tijdelijk, te weten in de opmaat naar dit wetsvoorstel) is verankerd in artikel X, eerste lid, van de Wet Elektronisch Berichtenverkeer Belastingdienst (Wet EBV). Het bepaalde wordt nu, conform hetgeen in de memorie van toelichting bij de Wet EBV werd aangegeven, opgenomen in het onderhavige wetsvoorstel. Het betreft onder meer de functionaliteit die bekend staat als MijnOverheid, via welke burgers langs elektronische weg, en met gebruik van een publiek middel, toegang wordt geboden tot elektronische informatie en berichten van bestuursorganen op het gebied van hun dienstverlening. Naar verwachting zal deze functionaliteit in de toekomst onder meer worden uitgebreid met MijnOverheid voor bedrijven (ondernemingen en rechtspersonen).

Lid 2–3

Tot slot heeft de Minister van BZK taken en verantwoordelijkheden op het gebied van de grensoverschrijdende toegang tot elektronische dienstverlening. Hij draagt in dit verband zorg voor een knooppunt als bedoeld in de verordening die op grond van artikel 12 van de eIDAS-verordening is vastgesteld[80] Deze voorziening maakt het mogelijk dat Nederlandse bestuursorganen en aangewezen organisaties de in andere EU-lidstaten ingevolge de eIDAS-verordening genotificeerde middelen kunnen accepteren (wederzijdse erkenning). In geval Nederlandse toegelaten of erkende elektronische identificatiemiddelen zijn genotificeerd, vindt routering van de authenticatie met dat Nederlandse middel naar een andere lidstaat ook via dat knooppunt plaats.[81] Ten behoeve van grensoverschrijdend inloggen door de houder van een in Nederland toegelaten en bij de Europese Commissie genotificeerd middel, wordt een via het BSN-K verkregen versleuteld pseudoniem omgezet in een Europees bruikbare *UniquenessID*. Dit UniquenessID is weliswaar gebaseerd op het burgerservicenummer, maar publieke dienstverleners in andere EU-lidstaten, die ingevolge de eIDAS-verordening verplicht zijn om de door Nederland genotificeerde en op de Commissielijst geplaatste identificatiemiddelen te accepteren teneinde toegang te verlenen tot hun elektronische diensten, ontvangen dus zelf het betrokken burgerservicenummer niet.[82]

---

[80] *EIDAS-uitvoeringsverordening inzake het interoperabiliteitskader, (EU) 2015/1501, Pb EU 2015, L 235/1.*

[81] *EIDAS-uitvoeringsverordening inzake het interoperabiliteitskader, (EU) 2015/1501, Pb EU 2015, L 235/1.*

[82] *Zie hierover uitgebreid de Kamerstukken bij Uitvoeringswet eIDAS-verordening.*

Uit het derde lid volgt dat het knooppunt, aan de uit een andere lidstaat ontvangen set gegevens een burgerservicenummer of andere aan de natuurlijke persoon of rechtspersoon gekoppelde gegevens, toe te voegen voor zover die gegevens noodzakelijk zijn voor bestuursorganen en aangewezen organisaties om de betrokken natuurlijke persoon of rechtspersoon ten behoeve van het verrichten van de elektronische dienstverlening in hun systemen te herkennen. In geval toevoeging van het burgerservicenummer aan het setje eIDAS-gegevens door een andere voorziening reeds mogelijk is, bijvoorbeeld middels het eerdergenoemde BSN-k, zal het knooppunt zelf het nummer niet toevoegen en ook niet in kunnen zien.

Het hier bedoelde knooppunt maakt deel uit van een netwerk van knooppunten in de lidstaten dat wordt gerealiseerd om grensoverschrijdende authenticatie mogelijk te maken wordt. De uitvoering van de eIDAS-verordening wordt toegelicht in de Kamerstukken bij de wetgeving terzake.[83]

Lid 4

Tot slot heeft ook de Dienst Wegverkeer (Ministerie van Infrastructuur en Waterstaat) een verantwoordelijkheid, zoals reeds toegelicht onder a. Voor de authenticatiefunctionaliteit (opname van data in een chip ten behoeve van elektronische authenticatie) op de bestaande drager (rijbewijs) is niet deze dienst maar de Minister van BZK verantwoordelijk. De Minister van Infrastructuur en Waterstaat is ervoor verantwoordelijk dat de Dienst Wegverkeer in staat is om voldoende mensen en middelen beschikbaar te stellen, van de juiste kwaliteit, zodat de opdracht tot het plaatsen van de authenticatiefunctionaliteit op het rijbewijs wordt gerealiseerd. De verantwoordelijkheid van de Dienst Wegverkeer betreft de productie en de levering van rijbewijzen. Doordat echter de authenticatiefunctie op het rijbewijs wordt aangebracht, treden 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 Wegenverkeerswet nieuwe taken en grondslagen voor gegevensverwerking zullen worden opgenomen die verband houden met het opnemen van de authenticatiefunctie op deze documenten.

Lid 5

Zoals bij het eerste lid is aangegeven, wordt de kern van dit wetsvoorstel gevormd door het bepaalde inzake voorzieningen en functionaliteiten in relatie tot de toegang tot elektronische dienstverlening (eID). Dat wil echter niet zeggen dat andere, waaronder op dit moment nog niet voorziene, voorzieningen niet tot de zorgplicht van de Minister behoren. Om het proces van uitbouw, aanbouw en doorontwikkeling van de digitale overheid daadwerkelijk en voortvarend te kunnen realiseren, bevat dit lid een grondslag voor het bij algemene maatregel van bestuur stellen van regels die nodig zijn in het kader van de inrichting, beschikbaarstelling, instandhouding, werking en beveiliging van de generieke digitale infrastructuur, waaronder inzake andere gdi-voorzieningen. Hierbij kan tevens een aansluitplicht worden opgelegd in de richting van de daarbij bepaalde bestuursorganen en aangewezen organisaties. Ook kan gedacht worden aan regels inzake het gebruik van of aansluiten op attributendiensten of beroepsregisters.

---

[83] *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 (Stb. 2017, 13).*

Reden voor het in dit lid tevens noemen van artikel 5, eerste lid, onderdeel f, is dat de zorg voor elektronisch berichtenverkeer en informatieverschaffing, zoals verankerd in de Wet Elektronisch Berichtenverkeer Belastingdienst (Wet EBV), naar het onderhavige wetsvoorstel wordt «verplaatst». Aangezien echter dit wetsvoorstel primair elektronische identificatie betreft en vooral grondslagen voor de uitwerking in dat verband bevat, is het nodig om, teneinde nadere regels inzake elektronisch berichtenverkeer, waaronder een aansluitplicht, te kunnen stellen, daar een grondslag voor op te nemen.
Indien de in dit lid bedoelde uitvoeringsregels worden vastgesteld, worden ook de kosten samenhangend met de uitvoering doorberekend, zo volgt uit dit wetsvoorstel. Beoogd wordt de kosten voor het gebruik naar rato door te belasten. In het geval een (overheids)orgaan, anders dan wordt voorgeschreven, geen gebruik maakt van de desbetreffende gdi-voorziening zal door de Minister desalniettemin een forfaitair bedrag in rekening worden gebracht.

Artikel 6

Lid 1

Bij dienstverlening waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is, dient gebruik gemaakt te worden van middelen die *ten minste* het voor de betreffende dienstverlening vereiste betrouwbaarheidsniveau hebben: «wie het meerdere mag, mag het mindere». Een gebruiker kan derhalve voor alle diensten met een middel op betrouwbaarheidsniveau hoog terecht, ook als het bestuursorgaan of de aangewezen organisatie voor de desbetreffende dienst slechts een middel met een lager betrouwbaarheidsniveau vereist en een publiek middel op niveau laag wordt geaccepteerd door het bestuursorgaan of de aangewezen organisatie. Middelen op een lager betrouwbaarheidsniveau dan substantieel of hoog, zullen niet worden toegelaten. Echter, het huidige publieke middel (DigiD) op betrouwbaarheidsniveau laag kan door bestuursorganen en aangewezen organisaties geaccepteerd blijven voor diensten waarvoor een laag betrouwbaarheidsniveau geldt.
Een middelenuitgever of authenticatiedienst die op grond van artikel 11 erkend is, kan ook bedrijfs- of organisatiemiddelen met het betrouwbaarheidsniveau laag uitgeven. Het voordeel hiervan is dat deze middelen op betrouwbaarheidsniveau laag via de overige erkende diensten dan makkelijk ontsloten kunnen worden.

Lid 2

Het in dit artikellid bepaalde betreft hetgeen nodig is om veilige en betrouwbare toegang tot elektronische diensten van bestuursorganen en aangewezen organisaties mogelijk te maken. 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 dienstverleners zich evenwel houden aan de bij ministeriële regeling te stellen criteria inzake betrouwbaarheidsniveaus voor authenticatie bij elektronische 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 en de in de praktijk reeds gehanteerde Handreiking betrouwbaarheidsniveaus[84], is dienstverleners te helpen een eenduidige, efficiënte en bewuste keuze te

[84] *https://www.forumstandaardisatie.nl/nieuws/nieuwe-versie-handreiking-betrouwbaarheidsniveaus*

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 rechtsgevolg van de desbetreffende dienst. 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 identificatiemiddelen duidelijkheid en rechtszekerheid. Naar verwachting betekent het bovenstaande dat het aantal diensten, waarbij met authenticatie op betrouwbaarheidsniveau laag kan worden volstaan, de komende jaren zal afnemen.

Lid 3

Zoals hierboven aangegeven is het, met inachtneming van de op te stellen ministeriële regeling terzake, aan de dienstverlener om te bepalen op welk betrouwbaarheidsniveau een gebruiker zich moet identificeren om toegang te krijgen tot een elektronische dienst. Dit geldt ook voor de toegang voor gemachtigden. Met andere woorden: de dienstverlener bepaalt in beginsel ook het betrouwbaarheidsniveau van een machtiging. Het lijkt logisch dat dienstverleners de betrouwbaarheidsniveaus dan zullen koppelen. Dit is echter niet altijd het geval. Reden is dat hoogbetrouwbare machtiging een relatief complex registratieproces meebrengt. Dit doet afbreuk aan het gebruiksgemak voor degene die een elektronische dienst wil afnemen. Hij/zij ervaart dan een hoge drempel om te machtigen. Dit leidt er in de praktijk toe dat een belangrijke, veelal kwetsbare, doelgroep het machtigingsproces niet kiest maar zijn identificatiemiddel «uitleent». Hierdoor wordt feitelijk afbreuk gedaan aan de betrouwbaarheid en nemen de risico's juist toe. Om deze paradox te voorkomen hebben dienstverleners binnen de grenzen van de op te stellen ministeriële regeling de ruimte om, afhankelijk van de aard van hun dienstverlening en de beoogde gebruikers, de betrouwbaarheidsniveaus te koppelen of de totstandkoming van de machtiging op een lager niveau te laten plaatsvinden. Op basis van een risicoafweging kan de dienstverlener na het moment van machtiging nog een andere technische of fysieke vorm van controle laten plaatsvinden, waardoor de identiteitsvaststelling bij het registeren van de machtigingsrelatie met inbegrip van deze controle op een vergelijkbaar betrouwbaarheidsniveau plaatsvindt als het vereiste niveau voor afname van de dienst. De identiteitsvaststelling dient uiteindelijk met voldoende waarborgen te zijn omkleed, gegeven het betrouwbaarheidsniveau waarop de dienstverlening moet plaatsvinden.

Lid 4

Naar aanleiding van het advies van de Autoriteit Persoonsgegevens is in het wetsvoorstel de mogelijkheid opgenomen om tijdelijk een lager betrouwbaarheidsniveau toe te staan. De duur ervan is in dit stadium nog erg lastig in te schatten. Dit hangt af van het tempo van de uitgifte van publieke middelen en de dekkingsgraad op de niveaus substantieel en hoog, alsmede de beschikbaarheid van toe te laten private middelen en de dekkingsgraad daarvan. Indien de aard van de dienstverlening noopt tot toepassing van een identificatiemiddel op een bepaald betrouwbaarheidsniveau, het middel beschikbaar is en de dekkingsgraad op een adequaat niveau is, ligt het niet in de rede om de acceptatie van een lager betrouwbaarheidsniveau door bestuursorganen en aangewezen organisaties nog langer toe te staan. Zolang de dekkingsgraad echter niet op een adequaat niveau is, is het echter nog niet mogelijk te eisen dat de dienstverlening

voldoet aan de krachtens de wet gestelde eisen. Het tijdelijk toestaan van een lager betrouwbaarheidsniveau dan eigenlijk gewenst, is daarom noodzakelijk. Terzake van niveau substantieel wordt voorshands gedacht aan een termijn van 4 jaar voordat volledige dekking van dat niveau binnen de populatie die nu DigiD op het lage betrouwbaarheidsniveau gebruikt. Terzake van niveau hoog is een nog langere termijn nodig. Brede dekking zal pas na vele jaren mogelijk zijn, ervan uitgaande dat in 2018 met de eerste uitgifte van het e-rijbewijs en in 2019 met de e-NIK wordt gestart. Bij ministeriële regeling kunnen bepaalde (nieuwe) vormen van dienstverlening op niveau hoog worden uitgesloten van het overgangsrecht, bijvoorbeeld omdat dit de ontwikkeling van die diensten zou kunnen belemmeren of wegens de hoge risico's van het toelaten van identificatiemiddelen op het lagere niveau. In het wetsvoorstel, zoals voorgelegd ter consultatie, was een overgangsbepaling van drie jaar opgenomen terzake van DigiD op niveau laag. Op basis van de huidige bepaling is het mogelijk om de uitfasering van het niveau laag in de dienstverlening gefaseerd te laten plaatsvinden. Daarbij zal rekening kunnen worden gehouden met de wenselijkheid dat voor dienstverlening, waarvoor niveau laag tijdelijk is toegestaan, dan ten minste 2-factor authenticatie wordt gebruikt; dit mede naar aanleiding van de op 21 juni jl. ingediende motie van het lid Van Engelshoven inzake het bevorderen van inloggen met 2-staps identificatie.[85]

Artikel 7

Lid 1–2

Bestuursorganen mogen uitsluitend toegelaten middelen accepteren en moeten met toegelaten middelen toegang verlenen tot hun elektronische dienstverlening. Burgers die houder zijn van een toegelaten middel hebben aldus een *aanspraak* op het gebruik ervan. Aldus kan het recht op elektronisch zakendoen met de overheid, zoals neergelegd in afdeling 2.3 van de Algemene wet bestuursrecht inzake elektronisch bestuurlijk verkeer, geëffectueerd worden. Op deze wijze worden bovendien middelen uit andere EU-lidstaten, terzake waarvan immers een Europeesrechtelijke plicht tot wederzijdse erkenning bestaat (b) en nationaal toegelaten middelen (a) *non discriminatoir* behandeld. Vanzelfsprekend geldt ook het omgekeerde: in Nederland toegelaten middelen, die bij de Europese Commissie succesvol zijn genotificeerd, moeten door overheidsorganisaties in de andere lidstaten worden geaccepteerd.[86]

De toegelaten identificatiemiddelen worden bij besluit van de Minister aangewezen (artikel 9). Het gaat hierbij om identificatiemiddelen voor natuurlijke personen ten behoeve van authenticatie in het publieke domein. In dit verband zullen primair publieke middelen op de betrouwbaarheids-niveaus substantieel en hoog worden aangewezen. De formulering laat ruimte voor het in de toekomt eventueel toelaten van een of meerdere privaat uitgegeven (i.e. niet door de overheid verstrekte) identificatiemiddelen. Naar verwachting zal dienstverlening, waarvoor het bsn wordt gebruikt, over het algemeen op betrouwbaarheidsniveau substantieel of hoog worden geclassificeerd aan de hand van de

---

[85] *Kamerstukken 34 725 VII, nr. 8.*

[86] *Elke EU-lidstaat kan zijn nationaal 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 Commissie, moeten alle (publieke dienstverleners in de) lidstaten die middelen uit de desbetreffende lidstaat accepteren. Naar verwachting zal Nederland de ingevolge deze wet toegelaten middelen aanmelden. Een lidstaat kan ervoor kiezen geen middelen aan de Commissie te melden, met als gevolg dat andere lidstaten niet verplicht zijn de in die lidstaat fungerende middelen te accepteren.*

ministeriële regeling zoals bedoeld in artikel 6, tweede lid, van dit wetsvoorstel. In het proces van totstandkoming van deze ministeriële regeling zal duidelijker worden in welke mate er diensten, waarvoor het bsn wordt gebruikt, op betrouwbaarheidsnivau laag overblijven. In aansluiting op het voorgaande geldt de acceptatieplicht ook voor een elektronische verklaring cq machtiging afgegeven in het kader van de voorziening als bedoeld in artikel 5, eerste lid, onderdeel b (machtiging).

Benadrukt zij, dat de acceptatieplicht terzake van toegelaten middelen ook voor rechterlijke instanties zal gelden; artikel 3 onder c van het Besluit digitalisering burgerlijk procesrecht en bestuursprocesrecht, dat een beslissingsbevoegdheid van de rechterlijke instanties bevat, zal worden aangepast. Voor aangewezen organisaties en rechterlijke instanties geldt evenals voor bestuursorganen dat zij bij hun elektronische dienstverlening aan natuurlijke personen waarvoor authenticatie op betrouwbaarheidsniveau substantieel of hoog vereist is, alle toegelaten identificatiemiddelen en elektronische verklaringen als bedoeld in artikel 5, eerste lid, onderdeel b, moeten accepteren. De wederzijdse erkenning van identificatiemiddelen, die behoren tot een door een lidstaat van de Europese Unie ingevolge de eIDAS-verordening bij de Europese Commissie aangemeld en goedgekeurd stelsel, vloeit voort uit artikel 6 van de eIDAS-verordening. Deze acceptatieplicht geldt alleen voor openbare instanties als bedoeld in de eIDAS-verordening. Voor zover aangewezen organisaties of rechterlijke instanties niet zijn aan te merken als openbare instantie geldt deze plicht tot wederzijdse erkenning in principe dus niet. Voor die organisaties en instanties geldt dat de genotificeerde eIDAS-middelen uitsluitend geaccepteerd hoeven te worden *indien* dit is bepaald bij besluit van de Minister in overeenstemming met de Minister die het mede aangaat.

Lid 3

Zoals bij het eerste en tweede lid wordt toegelicht, mag dienstverlening aan natuurlijke personen alleen geschieden door gebruikmaking van toegelaten middelen. Echter, wanneer sprake is van machtiging door een natuurlijke persoon aan een onderneming of rechtspersoon (bijvoorbeeld aan een accountant voor het doen van belastingaangifte) en derhalve namens de natuurlijke persoon een dienst wordt afgenomen, kan dit met gebruikmaking van een erkend bedrijfs- en organisatiemiddel.

Lid 4

Bestuursorganen, aangewezen organisaties en rechterlijke instanties kunnen volgens bij – door de Minister in nauwe samenspraak met de Minister wie het mede aangaat te formuleren – ministeriële regeling vast te stellen regels voor welbepaalde, dus afgebakende, groepen afwijken van het eerste respectievelijk tweede lid onder a en kunnen dus in plaats van een toegelaten middel een *alternatief* middel hanteren, indien dit noodzakelijk is om redenen van op die doelgroep gerichte elektronische dienstverlening, gelet op de specifieke aard van die diensten. Gedacht kan bijvoorbeeld worden aan bepaalde onderwijsinstellingen, die om technische redenen voor bepaalde groepen studenten een eigen identificatiemiddel hanteren. Het bepaalde zal terughoudend worden toegepast; er wordt geen algemene ontsnappingsmogelijkheid geboden voor bestuursorganen, aangewezen organisaties en rechterlijke instanties die de acceptatieplicht in het eerste of tweede lid bezwaarlijk vinden. Vanzelfsprekend kunnen bestuursorganen niet van de plicht tot wederzijdse erkenning afwijken. Het betreft immers een Europeesrechtelijke verplichting.

Consequentie van het bepaalde is dat in overeenstemming met bij ministeriële regeling vast te stellen regels domeinspecifieke of door dienstverleners gehanteerde «eigen» identificatiemiddelen (bijvoorbeeld voor mensen die niet kunnen beschikken over een burgerservicenummer, waaronder die afkomstig zijn van buiten de EU) mogen worden toegepast. Door de toenemende beschikbaarheid van toegelaten middelen – waarbij gewaarborgd is dat die aan de terzake gestelde (eIDAS) eisen voldoen – is evenwel de verwachting, dat op termijn het gebruik van niet-toegelaten middelen zal afnemen voor dienstverlening aan natuurlijke personen.

Lid 5

Hoewel in het vierde lid van artikel 15 voor bestuursorganen en aangewezen organisaties de bevoegdheid is opgenomen om met betrekking tot natuurlijke personen die een onderneming drijven (d.w.z. natuurlijke personen in de uitoefening van beroep of bedrijf) voor het gebruik van een bedrijfsmiddel te kiezen (en daarmee een toegelaten middel te weigeren), geldt dit niet indien en voorzover bij ministeriële regeling anders is bepaald. Het vierde lid hanteert het begrip «in de uitoefening van beroep of bedrijf» om te expliciteren dat het aanbieden van elektronische diensten door een ZZP'er of beroepsbeoefenaar onder deze formulering wordt begrepen. In het voorkomende geval wordt de desbetreffende persoon geaccommodeerd; hij kan dan – in een specifieke sector – ook een toegelaten identificatiemiddel gebruiken.

Artikel 8

Lid 1

Een publiek middel en de (machtigings)voorziening, bedoeld in artikel 5, eerste lid, onderdeel b, worden uitsluitend gebruikt voor de toegang tot elektronische dienstverlening door bestuursorganen en aangewezen organisaties. 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.[87] Het gebruik van (al dan niet toegelaten) private identificatiemiddelen in dit verband is dus geen onderwerp van regulering.
Het gebruiken van een publiek middel voor commerciële dienstverlening is niet toegestaan, teneinde de markt niet te verstoren. Uitgangspunt is dat publieke middelen en publieke voorzieningen bedoeld zijn voor de toegang tot de dienstverlening door bestuursorganen en aangewezen organisaties voorzover het de uitoefening van hun publieke (openbare) 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.

Lid 2:

Bij ministeriële regeling kan worden bepaald, dat een publiek middel tevens voor de toegang tot welbepaalde private elektronische diensten van deze dienstverleners kan worden gebruikt. Het zal hierbij gaan om nader omschreven aangewezen organisaties, voor nader omschreven diensten anders dan diensten ter uitoefening van een publieke taak, in het algemeen belang of waarbij het burgerservicenummer wordt verwerkt. Gedacht kan bijvoorbeeld worden aan zorgverzekeraars en zorgverleners.

---

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

Vanzelfsprekend gelden in dit voorkomende geval alle regels van het wetsvoorstel, waaronder die met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang tot de desbetreffende private diensten, op de naleving waarvan wordt toegezien door de Minister.

Lid 3

Bij ministeriële regeling kan worden bepaald dat een publiek identificatiemiddel tevens ten behoeve van aangewezen organisaties kan worden gebruikt voor het verlenen van toegang tot een systeem voor de elektronische uitwisseling van gegevens waarbij het burgerservicenummer wordt verwerkt, anders dan een systeem voor elektronische dienstverlening. Gedacht kan hierbij worden aan het gebruik binnen gesloten («interne») systemen zoals dat bijvoorbeeld binnen en tussen zorginstellingen bestaat voor het – binnen de grenzen van de wet – onderling digitaal uitwisselen van patiëntgegevens. Zorginstellingen zijn private organisaties die ten behoeve van hun dienstverlening de identiteit van patiënten moeten vaststellen. Het is van belang dat deze identiteitsvaststelling bij zorgverlening, indicatiestelling en zorgverzekering plaatsvindt. Het gebruik van persoonsgegevens, inclusief het bsn, in de zorg is om die reden nadrukkelijk wettelijk geregeld. In aansluiting daarop geldt ingevolge het onderhavige wetsvoorstel voor zorginstellingen een acceptatieplicht, opdat patiënten met hun publieke identificatiemiddel bij hen terecht kunnen. Wat betreft de interne bedrijfsvoering en uitwisseling van medische gegevens binnen het zorgdomein is het voorts van belang dat gegevens aan de juiste persoon gekoppeld worden en dat alleen bevoegd zorgpersoneel de individuele medische gegevens kan verwerken. Zekerheid omtrent de identiteit van degenen die met die privacygevoelige gegevens omgaan, zoals zorgverleners, is daarbij van groot belang. Om die reden bevat het derde lid de mogelijkheid om een publiek middel tevens voor een gesloten systeem te gebruiken. De zorgmedewerker gebruikt in dat geval zijn publieke middel (niet dat van de patiënt) om in te loggen in het gesloten systeem. Vanzelfsprekend gelden in dit voorkomende geval alle regels van het wetsvoorstel, waaronder die met betrekking tot de werking, betrouwbaarheid en beveiliging van de toegang tot de desbetreffende diensten en met betrekking tot toezicht.

Artikel 9

Lid 1

Ingevolge artikel 5, eerste lid onder a, jo artikel 9, eerste lid, draagt de Minister zorg voor de beschikbaarheid van publieke middelen op de betrouwbaarheidsniveaus substantieel en hoog. De regels waaraan deze middelen moeten voldoen zijn primair de eisen ten aanzien van werking, veiligheid en betrouwbaarheid die voortvloeien uit de eIDAS-verordening. Op onderdelen worden, om redenen van veiligheid en privacybescherming, voor in Nederland toe te laten middelen de Europese eisen ingevuld en «vertaald» naar de nationale situatie en daarmee toetsbaar gemaakt. Dit is ingevolge de eIDAS-verordening toegestaan. Deze regels, alsmede hoe deze zich verhouden tot de eIDAS-verordening (transponeringstabel) worden gepubliceerd. Het gaat hier derhalve om eisen die de Minister terzake van de door hemzelf uitgegeven (= publieke) identificatiemiddelen hanteert en die aan voortdurende (technische) ontwikkeling onderhevig zijn.

Lid 2

De Minister van BZK kan besluiten om een of meerdere privaat uitgegeven middelen op de betrouwbaarheidsniveaus substantieel en hoog toe te laten voor gebruik in het publieke domein. Op deze manier wordt burgers de mogelijkheid geboden over meerdere identificatiemiddelen te beschikken voor gebruik in de richting van bestuursorganen en aangewezen organisaties (keuzevrijheid) en is sprake van een minder kwetsbaar stelsel van identificatiemiddelen in het publieke domein. Om deze terugvaloptie te realiseren, is de aanbieder van een door de Minister toegelaten privaat identificatiemiddel verplicht dit aan te bieden aan burgers in het openbaar belang. Alleen op initiatief van de Minister van BZK kan een dergelijk privaat «burgermiddel» worden toegelaten. De uitoefening van de in het tweede lid gegeven bevoegdheid is ingekaderd. Teneinde een of enkele private middelen te kunnen selecteren, wordt binnen de kaders van de Aanbestedingswet 2012, een selectieprocedure doorlopen. Toelating geschiedt in de eerste plaats slechts indien dit noodzakelijk is voor de beschikbaarheid en toegankelijkheid van identificatiemiddelen voor natuurlijke personen in Nederland, waardoor dekkingsgraad, stabiliteit en continuïteit van de toegang tot elektronische dienstverlening gewaarborgd kan worden. Voorts dient het middel te voldoen aan de – in het verlengde van de eIDAS-verordening, zie toelichting bij het eerste lid – gestelde (beleids)regels ten aanzien van werking, veiligheid en betrouwbaarheid. Deze regels zullen de ruimte bieden voor (innovatieve) authenticatiemethoden, die qua werking afwijken van de norm maar desalniettemin een gelijkwaardige zekerheid bieden over, bijvoorbeeld, de identiteit van de gebruiker. Met betrekking tot de toelating van private middelen wordt vanzelfsprekend – en voortbordurend op de eIDAS-verordening – hetzelfde veiligheids- en betrouwbaarheidsniveau gehanteerd als voor de publieke middelen. Tot slot moet de geschiktheid van het middel zijn gebleken in een (vergelijkende) toets op basis van vooraf bekendgemaakte criteria. Van belang is immers dat sprake is van objectieve en vooraf algemeen kenbare toepassingsnormen; deze bieden waarborgen aan de gegadigden en zijn toetsbaar door de rechter. Indien er slechts een gegadigde is die aan de eisen voldoet, wordt een vergelijkende toets achterwege gelaten en vindt een individuele beoordeling plaats.

Lid 3

Voorafgaand aan de verdeling als bedoeld in het tweede lid moet kenbaar zijn aan welke regels de aanbieder van het private middel moet voldoen om in aanmerking te komen voor aanwijzing als toegelaten identifcatiemiddel voor de digitale dienstverlening van bestuursorganen en aangewezen organisaties. In dat kader zal de Minister aan het leveren van een privaat middel cq. private authenticatiedienst contractuele voorwaarden verbinden, die vanzelfsprekend zullen uitgaan van hetzelfde veiligheids- en betrouwbaarheidsniveau als terzake van publieke identificatiemiddelen (zie toelichting bij lid 1), en die onder meer betrekking zullen hebben op verplichte uitvoering, beveiliging, prijsstelling, privacybescherming (bijvoorbeeld te nemen technische en organisatorische maatregelen, zoals regels inzake de integriteit van het bij de dienstverlening betrokken personeel en intrekking of schorsing van het identificatiemiddel) en geldigheidsduur.
De leverancier van het privaat uitgegeven middel is verplicht te voorzien in de beschikbaarheid en werking van het toegelaten identificatiemiddel volgens de aan het contract verbonden voorschriften. De aanwijzing van een identificatiemiddel als toegelaten identificatiemiddel op het betrouwbaarheidsniveau substantieel of hoog, kan worden opgeschort en zonodig definitief worden ingetrokken (lid 3). Aanleiding kan bijvoorbeeld zijn het

in gevaar komen van de betrouwbaarheid van de grensoverschrijdende authenticatie (artikel 10 van de eIDAS-verordening). Van een besluit tot toelating, wijzigen, schorsen of intrekking wordt mededeling gedaan door plaatsing in de Staatscourant (lid 4).

Lid 4–5

Zoals gesteld is duidelijkheid vooraf omtrent inhoudelijke aspecten inzake toelating, wijziging, schorsing en intrekking van belang, gelet op het bieden van rechtszekerheid omtrent de toelating van publieke en, in voorkomend geval, private identificatiemiddelen, de wijze van toetsing door de Minister, de gronden voor (verlenen, wijzigen, schorsen en intrekken van) toelating en de hieraan te verbinden voorschriften en beperkingen. Hiertoe kunnen beleidsregels vastgesteld worden, gebaseerd op de eIDAS-uitvoeringsverordening[88], waarin de normen en inrichtingskeuzes zijn uitgewerkt waaraan identificatiemiddelen moeten voldoen om te kunnen worden gekwalificeerd op het betrouwbaarheidsniveau substantieel dan wel hoog. In ieder geval worden er beleidsregels opgesteld die een handreiking vormen voor de controle (door een auditor) op de naleving van de in het eerste lid bedoelde technische specificaties en procedures.

Artikel 10

Hoewel deze wet vooral regels bevat voor de overheid zelf, bevat dit artikel in het tweede lid de grondslag voor regels met betrekking tot het gebruik door natuurlijke personen van de publieke middelen en de voorzieningen, bedoeld in artikel 5, eerste lid. Het betreft regels die betrekking hebben op de publieke middelen en de voorzieningen die van belang zijn voor danwel een directe relatie hebben met natuurlijke personen (gebruikers), zoals de eisen inzake aanvraag, activatie, uitgifte, blokkeren en beëindiging van publieke middelen, aanvraag, registratie, reikwijdte, geldigheid en intrekken van een machtiging in relatie tot de vertegenwoordigde en beoogd gemachtigde, het zorgvuldig gebruik van de inzagefunctie en van MijnOverheid. Voorheen waren deze primair vindbaar in (privaatrechtelijke) gebruiksvoorwaarden die golden in de relatie de Minister – gebruiker.[89] Om redenen van duidelijkheid en rechtszekerheid ligt het echter in de rede algemeen verbindende voorschriften te stellen. De gebruik(ers)voorschriften met betrekking tot een eventueel ingevolge artikel 9, tweede lid, toe te laten privaat identificatiemiddel dienen door de aanbieder van dat middel in een gebruiksovereenkomst met de houder te worden vastgelegd.

Een essentiële plicht voor de rechtmatige houder van een elektronisch identificatiemiddel is opgenomen in deze wet, te weten in het eerste lid van dit artikel. De burger die in het bezit is van een elektronisch identificatiemiddel heeft een aantal verplichtingen ter bescherming van zijn elektronische identificatiemiddel. Hij moet zorgen dat hij het middel onder zijn exclusieve controle houdt, wat onder meer inhoudt dat wachtwoorden en pincodes strikt geheim moeten worden gehouden. Hij moet alle nodige maatregelen nemen om diefstal, verlies of verspreiding van zijn elektronisch identificatiemiddel te voorkomen en om ingeval van diefstal, verlies

---

[88] *Uitvoeringsverordening (EU) 2015/1502 van de Commissie van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt.*

[89] *Zie ook: Regeling voorzieningen GDI, Stcrt. 2015 nr 37158.*

of verspreiding zijn elektronisch identificatiemiddel onmiddellijk te laten intrekken.
De artikelen 231 e.v. van het Wetboek van Strafrecht (Sr.) stellen verschillende vormen van identiteitsfraude strafbaar. In dit verband wordt opgemerkt dat het gebruik van een elektronisch identiteitsmiddel van een ander verboden is. Ook het gebruik van een (fysiek) reisdocument of identiteitsbewijs van een ander om daarmee een elektronisch ID-middel van die ander te verkrijgen, is wederrechtelijk en strafbaar ingevolge artikel 231, tweede lid, Sr. Daarbij kan gedacht worden aan het op naam van iemand anders aanvragen van een eID-middel en/of het gebruik van het middel van een ander bij een overheidsorganisatie, zoals het doen van een aangifte of het aanvragen van een subsidie of toeslag voor iemand anders met gebruik van het elektronisch identificatiemiddel van diegene. Ook het vervalsen van een identificatiemiddel met de kennelijke intentie om zich met een andere identiteit voor te doen en daarmee fraude mogelijk te maken/te vergemakkelijken, kan hieronder worden begrepen.

Artikel 11

Paragraaf 4.3 heeft betrekking de authenticatie en identificatie van ondernemingen en rechtspersonen in hun toegang tot elektronische dienstverlening door bestuursorganen en aangewezen organisaties. Aangezien dit stelsel op onderdelen afwijkt van de bepalingen aangaande de toegelaten middelen (voor natuurlijke personen/burgers), en teneinde verwarring met de daarin gehanteerde termen te voorkomen, is een apart begrip voor deze identificatiemiddelen geïntroduceerd (zie ook artikel 1). De term bedrijfs- en organisatiemiddel maakt duidelijk dat het middel zowel bestemd is voor bedrijven, oftewel ondernemingen, als voor het handelen door (onderdelen) van publieke organisaties, zoals Rijkswaterstaat. Dit laatste betreft uiteraard het handelen van deze organisatie in de hoedanigheid van afnemer van elektronische dienstverlening bij een bestuursorgaan of aangewezen organisatie.

Anders dan bij authenticatie door burgers, terzake waarvan in dit wetsvoorstel de focus ligt op het van overheidswege uitgeven van identificatiemiddelen, worden de bedrijfs- en organisatiemiddelen niet door de overheid zelf uitgegeven en worden de voor het stelsel benodigde diensten niet door de overheid geleverd. Het stelsel voor bedrijfs- en organisatiemiddelen is voor alle (private) partijen toegankelijk, mits zij aan de gestelde eisen voldoen en erkend worden. Artikel 11 bevat de grondslag voor de erkenning van middelenuitgever, authenticatiedienst, machtigingsdienst en ontsluitende dienst.

Een middelenuitgever wordt erkend met betrekking tot het middel dat door hem wordt uitgegeven. De erkenning van een middelenuitgever ziet dus op een specifiek bedrijfs- en organisatiemiddel. Indien een middelenuitgever meerdere middelen wenst uit te geven, dient hij voor elk middel erkend te worden.

Ook een authenticatiedienst wordt erkend met betrekking tot een middel. Het kan dan gaan om een middel dat door hemzelf, in de hoedanigheid van erkend middelenuitgever, wordt uitgegeven. Maar het kan ook gaan om een middel dat door een andere erkend middelenuitgever wordt uitgegeven en waar de authenticatiedienst een overeenkomst mee heeft. Bij de aanvraag tot erkenning moet dan duidelijk zijn dat de betrokken authenticatiedienst inderdaad gerechtigd is om authenticatiediensten te verlenen ten aanzien van het door een erkende middelenuitgever uitgegeven bedrijfs- en organisatiemiddel.

De ontsluitende dienst draagt zorg voor de ontsluiting van alle andere erkende diensten. Wanneer een onderneming of rechtspersoon een elektronische dienst wil afnemen en de (gemachtigde) natuurlijke persoon daarbij gebruik maakt van een bepaalde erkend bedrijfs- en organisatiemiddel, zorgt de ontsluitende dienst dat de authenticatie van de gebruiker bij de erkende authenticatiedienst, die met betrekking tot dat middel is erkend, wordt opgehaald. Ook haalt de ontsluitende dienst de benodigde elektronische verklaring op bij een erkende machtigingsdienst. De ontsluitende dienst draagt de opgehaalde gegevens over aan de dienstverlener die daarmee de dienstverlening kan voortzetten.

Teneinde te verzekeren dat de middelen worden ontworpen en de diensten worden verricht met een voldoende veiligheids- en betrouwbaarheidsniveau worden bij of krachtens algemene maatregel van bestuur nadere regels gesteld. Deze betrouwbaarheids- en veiligheidsregels zullen in elk geval overeenkomen met de krachtens de eIDAS-verordening gestelde kaders. Daarnaast zullen eisen worden gesteld et betrekking tot bijvoorbeeld financiële gezondheid van de partij, de governance, etc. Voorts is voor een deugdelijke toegang van een ondernemer tot de elektronische dienstverlening van belang dat de verschillende onderdelen waar nodig goed op elkaar aan sluiten. Daarom bevat het artikel ook een grondslag om ten behoeve van de interoperabiliteit regels te stellen.

In aanvulling op de interoperabiliteitsregels voor het stelsel voor een bedrijfs- en organisatiemiddel kan ervoor worden gekozen om ook regels te stellen op basis waarvan interoperabiliteit tussen het stelsel voor het bedrijfs- en organisatiemiddel en de toegelaten middelen voor natuurlijke personen geborgd kan worden. Een dergelijke interoperabiliteit kan tegemoetkomen aan een effectieve toegang tot elektronische dienstverlening en een efficiënt gebruik van beschikbare voorzieningen en middelen. Op die manier kan bijvoorbeeld geborgd worden dat een burger een ondernemer kan machtigen namens hem of haar te handelen richting de overheid en andersom.[90]

De procedure aangaande het indienen en behandelen van een aanvraag om erkenning zal bij of krachtens algemene maatregel van bestuur nader worden uitgewerkt. Het gaat daarbij bijvoorbeeld om de bij de aanvraag te overleggen documenten. In dit kader zal in elk geval een certificaat van conformiteit moeten worden overgelegd. Een geldig certificaat levert een vermoeden op dat de betrokken partij voldoet aan de voor zijn dienst gestelde eisen, voor zover deze als te auditen eisen zijn aangemerkt. Het certificaat moet zijn afgegeven door een door de Minister aangewezen conformiteitsbeoordelingsinstantie. Bij of krachtens algemene maatregel van bestuur worden nadere regels gesteld aan deze aanwijzing. Zo zal de instantie in elk geval geaccrediteerd moeten zijn op grond van ISO 17065. Aangezien voor de hier aan de orde zijnde activiteiten op dit moment geen uniform (Europees) accreditatieschema voor handen is, zal de Minister het accreditatieschema vaststellen.

Bij of krachtens algemene maatregel van bestuur zullen voorts regels worden gesteld aangaande de bewijsstukken die, naast het certificaat van conformiteit, overgelegd moeten worden.

---

[90] *Een burger kan reeds een toegelaten middel in bezit hebben voordat hij een machtigingsrelatie aan gaat. De uitgifte aan hem van een bedrijfsmiddel kan dan mede gebaseerd worden op hetgeen al aan gegevens beschikbaar is, bijvoorbeeld het bsn. Voor de alsdan te verwerken persoonsgegevens door de private authenticatiedienst (uitgever bedrijfsmiddel) en de machtigingsdienst (die persoonsgegevens verwerkt om betrouwbaar de koppeling tussen vertegenwoordiging en gebruiker te maken) wordt een wettelijke basis gerealiseerd.*

Hoewel het wetsvoorstel betrekking heeft op elektronische dienstverlening waarvoor authenticatie op het betrouwbaarheidsniveau hoog of substantieel is vereist, is het ook mogelijk dat een middelenuitgever of een authenticatiedienst middelen op niveau laag uitgeeft. De algemene maatregel van bestuur zal ook voor dergelijke middelen eisen bevatten. Het voordeel hiervan is dat het lage middel aansluit op de overige erkende diensten. Een bestuursorgaan dat de erkende bedrijfs- en organisatiemiddelen op het niveau substantieel of hoog accepteert via een erkende ontsluitende dienst, zal dan op gemakkelijke wijze ook een erkend bedrijfs- en organisatiemiddel op het niveau laag kunnen accepteren. Hoewel die acceptatie dus niet verplicht wordt, zal in de praktijk het effect zijn dat het middel voor de toegang tot elektronische dienstverlening gemakkelijk beschikbaar is.

Een aanvraag wordt in principe afgewezen indien niet aan de gestelde regels wordt voldaan.
Voorts wordt niet uitgesloten dat een dienst wel aan alle eisen voor erkenning voldoet, maar dat verlenen van een erkenning om zwaarwegende redenen niet gewenst wordt geacht. Het gaat daarbij om situaties waarin de betrouwbaarheid en veiligheid van het stelsel mogelijk in gedrang komt, zoals in de situatie dat bij de te verlenen dienst betrokken personen verdacht worden van of veroordeeld zijn van ernstige strafbare feiten. In dat kader kan ook een integriteitsbeoordeling in het kader van de Wet bevordering integriteitsbeoordeling (Bibob) aan de orde zijn. Het achtste lid bevat de grondslag om de erkenning in geval van dergelijke omstandigheden toch te kunnen weigeren.

Artikel 12

Binnen het huidig wettelijk kader zijn er verschillende registers voorhanden die attributen bevatten aan de hand waarvan een onderneming of rechtspersoon kan worden geïdentificeerd. Te denken valt aan het BIG-register in de zorg. Deze attributen kunnen van belang zijn voor de toegang tot bepaalde elektronische dienstverlening. Voor die situaties bevat artikel 12 de grondslag voor de Minister om attributen aan te wijzen. Een dergelijke aanwijzing geschiedt in overeenstemming met de betrokken vakminister.
De aanwijzing van een attribuut heeft uitsluitend effect daar waar deze in het stelsel ook daadwerkelijk bij de authenticatie wordt betrokken. Teneinde dit te bereiken zullen bij ministeriële regels nadere regels worden gesteld. Deze regels zien onder meer op de wijze waarop erkende diensten geacht worden het betrokken attribuut bij hun activiteiten te betrekken en aan welke betrouwbaarheidsniveaus dan moet worden voldaan.

Artikel 13

Dit artikel bevat een aantal verplichtingen ten behoeve van het stelsel voor bedrijfs- en organisatiemiddelen erkende diensten. Het eerste lid bevat een grondslag voor het stellen van regels waaraan erkende middelenuitgevers en erkende diensten na erkenning blijvend aan moeten voldoen. Deze regels kunnen overlappen met de op grond van artikel 11 te stellen eisen.

Verder dient elke ontsluitende dienst alle erkende bedrijfs- en organisatiemiddelen en in dat kader alle door een erkende machtigingsdienst afgegeven machtigingen te ontsluiten. Dit is van belang voor het ontzorgen van de bestuursorganen en aangewezen organisaties. Zij hoeven als gevolg van deze plicht voor ontsluitende diensten maar met één ontsluitende dienst een contract te sluiten teneinde toch met alle

erkende bedrijfs- en organisatiemiddelen toegang tot hun elektronische dienstverlening te kunnen accepteren. Een ontsluitende dienst kan aan deze plicht alleen voldoen als de erkende middelenuitgever en andere erkende diensten daar hun medewerking aan verlenen. Daarbij kan bijvoorbeeld gedacht worden aan tijdige melding van aanpassing van software.

Expliciet is vermeld dat de middelenuitgever, authenticatiedienst en machtigingsdienst voor hun activiteiten geen kosten in rekening brengen bij de ontsluitende dienst. Een ontsluitende dienst dient immers alle middelen te kunnen ontsluiten. Het kan dan niet zo zijn dat de andere diensten de ontsluitende dienst vanwege die verplichte afhankelijkheid op kosten jaagt. Het reguleren van een tarief is onwenselijk en bovendien complex, aangezien een dergelijk tarief objectief en met goede kennis van de activiteiten en bijbehorende kosten moet worden vastgesteld. Om die reden is ervoor gekozen dat geen kosten bij de ontsluitende dienst in rekening gebracht mogen worden. De kosten zullen door de diensten daarom aan de afnemers van hun diensten doorberekend moeten worden.

De bij of krachtens algemene maatregel van bestuur aan de erkende diensten te stellen eisen dienen ervoor dat op structurele wijze de betrouwbare toegang van ondernemingen en rechtspersonen tot elektronische dienstverlening wordt geborgd. Voorts wordt van de erkende diensten verwacht dat zijn, net als nu in het civielrechtelijke afsprakenstelsel e-Herkenning, samenwerken. Maar niet kan worden uitgesloten dat er situaties ontstaan waarvoor een meer specifieke aanwijzing nodig is om de betrouwbaarheid in de toegang te borgen. Dit kan bijvoorbeeld aan de orde zijn naar aanleiding van een incident of verstoring. Maar ook kan een aanwijzing nodig zijn aan een erkende partij indien deze een innovatieve ontwikkeling waarmee de betrouwbaarheid van de toegang kan worden vergroot, tegen houdt. Voor die situaties geeft het vijfde lid aan de Minister de bevoegdheid om aanwijzingen te geven. Bij of krachtens algemene maatregel van bestuur wordt die bevoegdheid nader ingevuld.

In het verlengde hiervan kan een ontheffing van de generieke regels nodig zijn. Gedacht kan worden aan ontheffing van regels die in de weg staan aan een innovatieve ontwikkeling.

Artikel 14

De erkenning van de diensten is de basis van de toegang van ondernemingen en rechtspersonen tot elektronische dienstverlening. Indien niet langer voldaan wordt aan de gestelde eisen die de betrouwbaarheid van het stelsel moeten verzekeren, moet intrekking van die erkenning dan ook mogelijk zijn. Daarnaast kan het vóórkomen dat een partij niet langer de betrokken activiteiten wenst te verrichten, bijvoorbeeld omdat binnen de betrokken rechtspersoon een andere focus van business wordt gekozen.

Maar intrekking kan verstrekkende gevolgen hebben, bijvoorbeeld als een authenticatiedienst niet langer de authenticatie in geval van gebruik van een bepaald middel verzorgt. Om die reden zijn in dit artikel nadere regels opgenomen om de gevolgen van een intrekking te mitigeren. Zo dient een erkende dienst die verzoekt om intrekking zorg te dragen voor een beëindigingsplan. Een dergelijk beëindigingsplan kan ook door de Minister worden geëist indien de erkenning door hem is ingetrokken wegens het niet naleven van de gestelde eisen. Bij ministeriële regeling kunnen nadere regels aan een dergelijk plan gesteld worden. Het plan zal ten minste een beschrijving moeten bevatten van de wijze waarop

continuïteit van betrouwbare toegang door ondernemingen en rechtspersonen tot elektronische dienstverlening geborgd is.
Ten behoeve van die continuïteit kan het ook nodig zijn dat de verzoekende erkende dienst zijn diensten toch nog enige tijd voortzet. Voor die situaties biedt het artikel de bevoegdheid om een dergelijke verplichting aan de betrokken dienst op te leggen. Voor die periode heeft de dienst nog te gelden als erkende dienst en dient hij aan alle verplichtingen te voldoen.

Ook kan het voorkomen dat een erkende dienst zijn activiteiten wenst over te dragen aan een andere rechtspersoon. Aangezien voor de erkenning ook eisen worden gesteld die gericht zijn tot de rechtspersoon, kan een overdracht niet zonder toestemming van de Minister plaatsvinden. Onderzocht moet immers worden of de nieuwe rechtspersoon ook aan alle eisen voldoet.
Artikel 14 biedt de grondslag en kaders voor een dergelijke toestemming.

In het artikel wordt voorts benadrukt dat de intrekking van een erkenning van een middelenuitgever ook consequenties heeft voor het middel waarvoor hij erkend is. Die middelen hebben dan niet meer te gelden als erkende bedrijfs- en organisatiemiddelen.

Artikel 15

Het stelsel voor de authenticatie en autorisatie van ondernemingen en rechtspersonen is bedoeld voor de toegang tot elektronische dienstverlening die zij nodig hebben voor de uitoefening van hun beroep of bedrijf. Voor deze dienstverlening wordt in het algemeen gebruik gemaakt van het KvK- of RSIN-nummer van de betrokken onderneming. Met het eerste lid wordt benadrukt dat de acceptatieplicht die met dit artikel wordt vormgegeven uitsluitend van toepassing is op dienstverlening aan ondernemingen en rechtspersonen die over een dergelijk nummer kunnen beschikken. Daartoe wordt verwezen naar ondernemingen en rechtspersonen als bedoeld in de Handelsregisterwet. Het betreft onder meer eenmanszaken, BV's, CV's, VOF's en maatschappen, maar ook verenigingen en bijvoorbeeld kerkgenootschappen.

Het eerste lid leidt er dus toe dat de plicht van bestuursorganen en aangewezen organisaties om erkende bedrijfs- en organisatiemiddelen te accepteren niet geldt voor de toegang tot hun dienstverlening aan een onderneming die niet is aan te merken als onderneming als bedoeld in artikel 5 van de Handelsregisterwet. Dit houdt in dat het in de toegang van dergelijke ondernemingen een bestuursorgaan of aangewezen organisatie vrij staat om de toegang middels andere methoden te verlenen, bijvoorbeeld middels een eigen inlogsysteem. Uiteraard moet bij deze vrijheid wel de Europeesrechtelijke kaders aangaande de interne markt, zoals bijvoorbeeld verankerd in de Dienstenrichtlijn, in acht worden genomen.

Uit het tweede lid volgt dat bestuursorganen en aangewezen organisaties alle erkende bedrijfs- en organisatiemiddelen en door erkende machtigingsdiensten afgegeven elektronische (machtigings)verklaringen moet accepteren. Het kan dus niet zijn dat een bestuursorgaan de toegang uitsluitend mogelijk maakt met een bepaald middel. In dit kader wordt ook verwezen naar de rol van de ontsluitende dienst, wiens taak het is om ontsluiting van alle erkende bedrijfs- en organisatiemiddelen en alle erkende machtigingsdiensten mogelijk te maken.

Voorts volgt uit het tweede lid dat in geval van elektronische dienstverlening aan ondernemers en rechtspersonen, bedoeld in het eerste lid, bestuursorganen en aangewezen organisaties uitsluitend toegang mogen

verlenen tot hun dienstverlening voor zover gebruik wordt gemaakt van een erkend bedrijfs- en organisatiemiddel. Dit laatste is uiteraard onverminderd het bepaalde in artikel 7 van dit wetsvoorstel, waaruit volgt dat zij tevens (alle) toegelaten middelen moeten accepteren. Aan laatstgenoemde middelen, die uitsluitend aan natuurlijke personen worden uitgegeven, is doorgaans (uitsluitend) een bsn gekoppeld.

Een natuurlijk persoon die een onderneming drijft kan in beginsel dus kiezen of hij gebruik wil maken van zijn toegelaten middel of van een erkend bedrijfs- en organisatiemiddel in de toegang tot de voor hem in de uitoefening van zijn onderneming gewenste dienstverlening. In geval hij kiest voor gebruik van een toegelaten middel, brengt dit met zich dat wel een bsn, maar geen KvK-nummer of RSIN wordt meegeleverd. Terwijl voor dienstverlening aan ondernemingen en rechtspersonen ten behoeve van de uitoefening van hun beroep of bedrijf over het algemeen wel een KvK-nummer of RSIN noodzakelijk is. Een dienstverlener moet de onderneming of rechtspersoon immers als zodanig in zijn eigen systemen kunnen herkennen.

Om bestuursorganen en aangewezen organisaties in deze dienstverlening te ontzorgen, wordt hen in het vierde lid de mogelijkheid geboden om, daar waar naar hun oordeel voor de dienstverlening toch een KvK-nummer of RSIN-nummer noodzakelijk is, de toegang met een toegelaten middel, gekoppeld aan het bsn, te weigeren en te verlangen dat gebruik wordt gemaakt van een erkend bedrijfs- of organisatiemiddel. Dat betekent dat bijvoorbeeld een café-eigenaar, die inlogt met zijn publieke identificatiemiddel wanneer hij een terrasvergunning aanvraagt, de toegang tot die dienstverlening door de betrokken gemeente mag worden geweigerd. Tenzij de gemeente in staat is om de onderneming ook als zodanig te herkennen indien gebruik wordt gemaakt van een toegelaten middel voor natuurlijke personen en de ontvangst van alleen een bsn niet in de weg staat aan de gewenste dienstverlening. In dat geval is er immers geen noodzaak voor de gemeente om de café-eigenaar te weigeren. Een aantal bestuursorganen, waaronder de Belastingdienst, vraagt in zo'n geval zelf een KvK-nummer op of kan het betreffende dossier ook op basis van het bsn uit de eigen bestanden selecteren. Daar waar een bestuursorgaan of een aangewezen organisatie daartoe in staat is, kan derhalve de toegang met een toegelaten middel (gebaseerd op bsn) worden toegestaan en is er geen reden om van de weigeringsbevoegdheid gebruik te maken.

In het derde lid zijn twee situaties opgenomen in welk geval de acceptatieplicht niet van toepassing is. Dit houdt verband met de Dienstenrichtlijn. Daaruit volgt dat een bedrijf de gelegenheid moet hebben om via één loket alle procedures en formaliteiten af te wikkelen die nodig zijn voor de toegang tot zijn activiteiten en via dat één loket ook vergunningaanvragen af moet kunnen wikkelen die nodig zijn voor de uitoefening van de activiteit. Gelet op de doelstellingen van de Dienstenrichtlijn dient dit eenvoudig, op afstand en elektronisch te kunnen plaatsvinden. Dat geldt ook voor een Europees bedrijf dat middels het in Nederland hiertoe vormgegeven Centraal Loket procedures wenst af te wikkelen waarvoor het betrouwbaarheidsniveau hoog of substantieel geldt. In geval een Europese dienstverlener zich ingevolge de Handelsregisterwet niet kan inschrijven in het handelsregister, zal de in dit artikel vormgegeven acceptatieplicht niet belemmerend werken. Die is dan immers niet van toepassing.

Niet uitgesloten is echter, dat er bedrijven uit andere lidstaten zijn die zich wel kunnen inschrijven in het handelsregister, maar waarvoor het lastig of onmogelijk is om op eenvoudige wijze en op afstand te kunnen

beschikken over een erkend middel. Om te verzekeren dat deze bedrijven de formaliteiten en vergunningaanvragen via het Centraal Loket te allen tijde in overeenstemming met de Dienstenrichtlijn kunnen afwikkelen, is in het derde lid bepaald dat de acceptatieplicht niet geldt voor het aanmaken van en de toegang tot een elektronische postbus in het Centraal loket en niet voor de dienstverlening die via die postbus plaatsvindt.

Het vijfde lid is voorts bedoeld voor situaties dat sprake is van een min of meer gesloten systeem van elektronische dienstverlening tussen bepaalde bestuursorganen of aangewezen organisaties en bepaalde beroepsgroepen. Te denken valt aan de elektronische communicatie met de rechterlijke macht door advocaten. In dergelijke min of meer gesloten systemen wordt nogal eens gebruik gemaakt van een ander, specifiek voor die dienst of die doelgroep bedoeld identificatiemiddel. Zo maken advocaten gebruik van de advocatenpas. Het vijfde lid kent voor die situatie de bevoegdheid aan de Minister toe om dat andere specifieke identificatiemiddel aan te wijzen. Dit middel mag dan in afwijking van de plicht om uitsluitend toegang te verlenen in geval gebruik wordt gemaakt van erkende bedrijfs- en organisatiemiddelen (of van toegelaten middelen) ook worden geaccepteerd in de toegang tot de bij dat aanwijzingsbesluit bepaalde elektronische dienstverlening. Van belang is uiteraard dat daarbij eenduidig wordt bepaald om welke dienstverlening het gaat en welke ondernemers en rechtspersonen daar gebruik van kunnen maken. Voorts is van belang dat ook dit specifieke middel op betrouwbaarheidsniveau substantieel of hoog kan worden gebruikt en ook aan de daarvoor geldende eisen voldoet. Is dat niet het geval, dan wordt het middel niet aangewezen. Bovendien mag van dat middel dan, zonder die aanwijzing, geen gebruik worden gemaakt bij de elektronische dienstverlening op niveau substantieel of hoog. Dat laatste volgt uit artikel 7, eerste lid. Daarin is bepaald dat een bestuursorgaan of aangewezen organisatie bij de toegang tot zijn elektronische dienstverlening op het niveau substantieel of hoog uitsluitend middelen van ten minste datzelfde niveau accepteert.

Tot slot is in het kader van de acceptatieplicht van belang dat uit artikel 6 van de eIDAS-verordening voor openbare instanties rechtstreeks een plicht tot erkenning volgt van alle bij de Europese Commissie genotificeerde en geaccepteerde middelen. In het achtste lid is benadrukt dat de in dit artikel geformuleerde acceptatieplicht die rechtstreeks uit de verordening voortvloeiende plicht tot wederzijdse erkenning onverlet laat. Het uitgangspunt dat uitsluitend erkende en toegelaten middelen worden geaccepteerd, laat dus onverlet dat bestuursorganen en aangewezen organisaties, voor zover zij zijn aan te merken als openbare instantie, ook de genotificeerde en geaccepteerde eIDAS-middelen moeten erkennen. Ook in een min of meer gesloten stelsel zal een eIDAS-middel dus geaccepteerd moeten worden.

Artikel 16

Lid 1

De in dit wetsvoorstel genoemde Ministers, alsmede bestuursorganen en aangewezen organisaties verwerken persoonsgegevens, waaronder het burgerservicenummer (bsn), voor zover dit noodzakelijk is voor de goede uitvoering van hun taken en verplichtingen ingevolge deze wet. Het gaat hierbij om gegevensverwerking in het kader van authenticatie en de in dat verband betrokken voorzieningen (zie artikel 5, eerste lid), en in het kader van de toegangsverlening tot cq het ontsluiten van elektronische diensten op de betrouwbaarheidsniveaus substantieel en hoog. Ook om activiteiten

in het kader van voorkomen, herkennen en herstellen van misbruik en oneigenlijk gebruik adequaat te kunnen uitvoeren is het noodzakelijk om persoonsgegevens te verwerken. Gegevensverwerking in het kader van de elektronische dienstverlening als zodanig wordt niet onder dit artikellid begrepen. Het verlenen van elektronische diensten behoort tot het beleidsdomein en de verantwoordelijkheid van het desbetreffende bestuursorgaan of aangewezen organisatie en valt buiten de werkingssfeer van deze wet.

Lid 2

De aanbieder van een toegelaten privaat middel moet burgers in staat stellen toegang te verkrijgen tot elektronische diensten van bestuursorganen en aangewezen organisaties. Voorwaarde voor dit functioneren is de verwerking van persoonsgegevens en derhalve een wettelijke grondslag terzake. *Core business* van dergelijke partijen, ook wel authenticatiediensten genoemd, is het authenticeren van gebruikers. In het kader van deze wet oefenen zij functies uit die onlosmakelijk verband houden met het functioneren van de voorziening bedoeld in artikel 5, eerste lid, onderdeel d. De goede werking van deze voorziening is namelijk afhankelijk van de aanlevering van bepaalde persoonsgegevens over de gebruiker van een identificatiemiddel, die dit wil gebruiken voor de afname van diensten in het publieke domein. Het bsn wordt eenmalig aangeleverd aan de Minister als beheerder van de voorziening BSN-K. Om de verkregen gegevens te controleren op juistheid, vraagt hij gegevens op uit de basisregistratie personen; verificatie geschiedt door de opgegeven gegevens van de aanvrager (burger) te controleren aan de hand van de hierin opgenomen gegevens.[91] De authenticatiedienst controleert deze gegevens aan de hand van het overlegde identificatiemiddel en bewaart geen integrale kopie, maar een kopie waarop de gelaatsfoto en het bsn zijn verwijderd. Hierdoor ontstaat er bij de authenticatiediensten geen verzameling van persoonsgegevens (hotspot), waardoor de privacy van de gebruikers wordt beschermd.[92] 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.[93]

---

[91] *Dit kan via het geheel van onder de verantwoordelijkheid van de Minister ressorterende voorzieningen dat zorgt voor het genereren, distribueren, beheren en raadplegen van het bsn, bijvoorbeeld de toegang tot de identificerende gegevens in de achterliggende authentieke registraties van persoonsgegevens (BRP). www.digitaleoverheid.nl/voorzieningen/gegevens/beheervoorziening-bsn.*

[92] *Niettemin is hierbij sprake van verwerking van persoonsgegevens door de authenticatiedienst.*

[93] *De Privacy Impact Assessment inzake de introductie van eID 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, te weten verificatie van de identiteit van de houder van een identificatiemiddel 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.*

Lid 3

Ook voor een aantal specifieke partijen dat betrokken is bij de goede werking van het stelsel inzake elektronische authenticatie van ondernemingen en rechtspersonen is een wettelijke grondslag gerealiseerd voor de verwerking van persoonsgegevens. Authenticatie is in dit verband een samenspel tussen publieke en private partijen. Te denken valt aan het controleren van het bsn bij de uitgifte van een bedrijfs- en organisatiemiddel en het ten behoeve van authenticatie verkrijgen van een pseudoniem voor dat bsn, vast te stellen door het BSN-K. De uitgever van het bedrijfs- en organisatiemiddel baseert zich bij de uitgifte op hetgeen aan kenmerken en gegevens beschikbaar wordt gesteld (bijvoorbeeld KvK-nummer, RSIN, OIN, bsn) door een partij die hiertoe een verklaring afgeeft. Een machtigingsdienst verwerkt gegevens om betrouwbaar de koppeling tussen vertegenwoordiging en bedrijvenmiddel te maken. Een ontsluitende dienst verwerkt tot slot (versleutelde) gegevens bij het routeren van het elektronisch verkeer tussen een bestuursorgaan of aangewezen organisatie en erkende aanbieders van een bedrijvenmiddel en machtigingsdiensten in het kader van het «ontzorgen» van dienstverleners.

Lid 4

Bij algemene maatregel van bestuur zullen regels worden gesteld over de precieze persoonsgegevens die gelet op de voorgaande leden worden verwerkt, het doel van de verwerking, aan wie deze gegevens worden verstrekt en hoe lang deze worden bewaard. Aan de eisen van doelbinding, subsidiariteit en proportionaliteit alsmede aan de uitgangspunten van kenbaarheid, voorzienbaarheid en transparantie voor degenen wiens gegevens het betreft, zal aldus verder invulling worden gegeven. Het Besluit verwerking persoonsgegevens GDI zal hiertoe worden gewijzigd en aangevuld.

Artikel 17

Lid 1

Het toezicht op de naleving van de toe te passen standaarden, van de plicht tot acceptatie en classificering en van het gebruik van publieke middelen in het publieke domein door decentrale overheden loopt via reguliere (interbestuurlijke) lijnen. Er wordt voor die niveau's dus geen afzonderlijke toezichthouder aangewezen; terzake gelden de Gemeente- en Provinciewet. Voor de naleving door overheidsorganen op het niveau van het Rijk respectievelijk bestuursorganen op het niveau van de rijksoverheid (ministeries en zelfstandige bestuursorganen) en door de aangewezen organisaties geldt dat de Minister, op wiens beleidsterrein het betreffende overheidsorgaan of het desbetreffende zelfstandige bestuursorgaan of aangewezen organisatie werkzaam is, een toezichthouder aanwijst. Het daarbij in de regel gaan om het terzake 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.

Lid 2

Met het toezicht op de naleving van de artikelen 3, 6, 7, 8, eerste lid, en 15 door bestuursorganen op het niveau van de provincies zijn belast de bij besluit van de Minister aangewezen ambtenaren. In lijn met het reguliere interbestuurlijke toezicht houdt de Minister toezicht op provincies en

bestuursorganen op het niveau van provincies (gemeenschappelijke regelingen waaraan provincies deelnemen).

Lid 3

In lijn met het reguliere interbestuurlijke toezicht houden de provincies toezicht op de naleving van de artikelen 3, 6, 7, 8, eerste lid, en 15 door gemeenten en waterschappen alsmede de bestuursorganen op het niveau van gemeenten en waterschappen, zoals gemeenschappelijke regelingen. Het provinciebestuur informeert de Minister over de (mate van) naleving zodat de Minister zijn rol als stelselverantwoordelijke kan vervullen.

Lid 4

Op de naleving door bestuursorganen en aangewezen organisaties van de eisen inzake informatieveiligheid en de in dit verband opgelegde auditverklaring alsmede van de regels inzake gebruik buiten het publieke domein wordt toezicht gehouden door de Minister.

Lid 5

Met het toezicht op de naleving van het bepaalde bij of krachtens de artikelen 11 en 13 zijn belast de bij besluit van de Minister aangewezen ambtenaren. Het gaat hierbij om toezicht op private partijen die erkend zijn in het stelsel voor elektronische authenticatie van ondernemingen en rechtspersonen. Naar verwachting worden hiertoe ambtenaren van het Agentschap Telecom aangewezen. Hiervan wordt mededeling gedaan in de Staatscourant.

Lid 6–8

Ingevolge artikel 14 heeft de Minister de bevoegdheid om een verleende erkenning op te schorten of in te trekken. Daarnaast is hij ingevolge het onderhavige artikel bevoegd om terzake een last onder bestuursdwang op te leggen. In aanvulling daarop is ook de bevoegdheid opgenomen tot het opleggen van een bestuurlijke boete.

Artikel 18

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 (dreigende) compromittering van de veilige en betrouwbare toegang tot elektronische dienstverlening door bestuursorganen en aangewezen organisaties te voorkomen of beëindigen. Dit artikellid biedt hem bevoegdheden indien andere instrumenten (afspraken, waarschuwing, bestuurlijk overleg) niet toereikend blijken om veilige en betrouwbare toegang tot publieke dienstverlening te realiseren.

Het bepaalde dient in de eerste plaats te worden gelezen in samenhang met artikel 4, op basis waarvan eisen worden gesteld aan werking, betrouwbaarheid en beveiliging van de toegang tot elektronische dienstverlening door bestuursorganen en aangewezen organisaties, waaronder het regulier overleggen van een auditverklaring. Zoals ook in de toelichting bij dat artikel is aangegeven, is het uitgangspunt dat de betrokken bestuursorganen en aangewezen organisaties een eigenstandige verantwoordelijkheid hebben voor informatiebeveiliging en dat erop mag worden vertrouwd dat zij de eisen terzake naleven. Indien

echter uit de auditverklaringen zou blijken, dat de informatieveiligheid in het geding is en ook na herhaaldelijke aanmaningen de benodigde verbeteringen niet worden aangebracht (escalatieladder), 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. Voorts kan de Minister noodmaatregelen nemen bij (dreigende) ernstige storingen, ernstige aantasting van de werking beveiliging of betrouwbaarheid van de elektronische dienstverlening, of misbruik of oneigenlijk gebruik van de toegang terzake. 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 dienstverlening en systemen van bestuursorganen en aangewezen organisaties, waarvan burgers, bedrijven en de overheid zelf het slachtoffer kunnen worden. Tot slot kan een noodmaatregel bij niet-naleving door het betrokken bestuursorgaan of de betrokken aangewezen organisatie van het bij of krachtens de artikelen 7, 15 (acceptatie) en 8 (publiek middel in publiek domein) bepaalde gerechtvaardigd zijn, omdat door niet-naleving hiervan de goede werking van de generieke infrastructuur, in het bijzonder van publieke middelen en voorzieningen als bedoeld in artikel 5, eerste lid, kan worden verstoord. Het voordien informeren van de betreffende toezichthouder is hierbij opportuun.
Teneinde de veiligheid en betrouwbaarheid van de toegang tot elektronische dienstverlening te waarborgen, misbruik of oneigenlijk gebruik en ernstige niet naleving zoveel mogelijk te voorkomen, is het nodig dit te kunnen herkennen, vroegtijdig te signaleren en, bij constatering daarvan, herstel- en noodmaatregelen te kunnen nemen. De Minister van BZK heeft hierbij doorzettingsmacht. De Minister van BZK onderkent het onder a-c genoemde veelal vroegtijdig en kan dan preventief optreden; een acuut risico kan vervolgens worden weggenomen door middel van het tijdelijk (doen) onderbreken van de toegang tot dienstverlening (afsluiten van authenticatie).
Operationele uitwerking van misbruikbestrijding geschiedt op basis van een – door de Minister in afstemming met de dienstverleners op te stellen – plan van aanpak, waarbij een risico-gerichte benadering en heldere afwegingskaders terzake van de betrokken belangen en de te nemen maatregelen voorop staan.

Het eerste lid faciliteert, mits proportioneel, maatregelen van de Minister 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 dienstverleners zoals de Belastingdienst, de desbetreffende Minister of het desbetreffende bestuursorgaan om informatie en gebruik(er)sge-

gevens verzoeken. Alsdan zal afgewogen worden of de relevante informatie kan worden aangeleverd overeenkomstig de daarvoor geldende wettelijke kaders. Ook binnen de voorzieningen als bedoeld in artikel 5, eerste lid, 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 gebruikers van een publiek middel, dat gebruikt kan worden voor het herkennen van misbruik.

Ernstige, waaronder voortdurende, niet nakoming van de plicht tot het betalen van de (o.a. aansluit) kosten bedoeld in artikel 21 kan tot slot ook aanleiding vormen voor door de Minister te nemen maatregelen.

Lid 2–3

Teneinde vast te (kunnen) stellen of sprake is van een situatie als bedoeld in het eerste lid, is het van belang dat de Minister op de hoogte is. Een bestuursorgaan of een aangewezen organisatie moet daarom de Minister onverwijld in kennis stellen van een inbreuk op de beveiliging of de integriteit van een eigen elektronische dienst of van misbruik of oneigenlijk gebruik van de toegang tot de eigen elektronische dienstverlening. Het bestuursorgaan of de aangewezen organisatie verstrekt daarbij alle benodigde informatie. Hetzelfde geldt voor een (interbestuurlijke) toezichthouder die ernstige niet naleving door een bestuursorgaan of aangewezen organisatie van het bij of krachtens de artikelen 7, 8 en 15 bepaalde constateert.

Voor de goede orde wordt opgemerkt, dat melding in de zin van dit artikel onderscheiden moet worden van de meldplicht datalekken; ingevolge artikel 33 AVG 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 is de jegens het Nationaal Cyber Security Centrum geldende meldplicht voor ICT-inbreuken, die aanzienlijke gevolgen kunnen hebben voor de continuïteit van vitale dienstverlening, toepasselijk. 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.[94] Verder kan, op grond van het voorstel voor de Wet beveiliging netwerk- en informatiesystemen, in de toekomst voor aanbieders van essentiële diensten de plicht toepasselijk zijn om incidenten met aanzienlijke gevolgen bij het bevoegd gezag en bij de Minister van Justitie en Veiligheid als het CSIRT (*computer security incident response team*) te melden. Ingeval sprake is van een inbreuk op de beveiliging of de integriteit van een eigen elektronische dienst, en deze inbreuk aanzienlijke gevolgen kan hebben op de veilige en betrouwbare toegang tot elektronische dienstverlening of van misbruik of oneigenlijk gebruik van de toegang tot de eigen elektronische dienstverlening, is de Minister van BZK het bevoegd gezag.

Lid 4–5

Ook bij het vermoeden van misbruik of oneigenlijk gebruik van een individueel middel dat gebruikt wordt voor elektronische dienstverlening (dus: in het publieke domein), heeft de Minister van BZK de mogelijkheid om snel en doeltreffend te handelen en het desbetreffend middel «uit de roulatie» te halen. Het kan hierbij gaan om een welbepaald toegelaten

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

middel van hetzij publieke aard, hetzij (ingevolge artikel 9, tweede lid) private aard of om een (ingevolge artikel 11) erkend middel. Benadrukt wordt dat deze acute maatregel is gericht tot een individueel middel en dat deze bevoegdheid toekomt aan de Minister en niet aan dienstverleners. Bestuursorganen en aangewezen organisaties hebben, gezien hun verantwoordelijkheid voor (bescherming van hun) bedrijfsvoering, ingeval van door hen geconstateerde integriteitsproblemen vanzelfsprekend wel de mogelijkheid om hun dienstverlening op te schorten.

Het (tijdelijk) onderbreken door de Minister betekent dat de toelating van het type middel in beginsel ongemoeid wordt gelaten (zie evenwel artikel 9, derde lid, respectievelijk artikel 14, eerste lid). Het is niet wenselijk om bij het nemen van acute maatregelen afhankelijk te zijn van de medewerking van de desbetreffende private aanbieder; het is immers de verantwoordelijkheid van de betrokken Minister om te zorgen voor veilige en betrouwbare toegang tot elektronische dienstverlening. Hij moet indien nodig zelf maatregelen kunnen nemen om dit te borgen. Indien nodig zullen hiertoe technische aanpassingen binnen de infrastructuur plaatsvinden.

Als blijkt dat een EU-genotificeerd middel gecompromitteerd is en de betrouwbaarheid van de grensoverschrijdende authenticatie in gevaar komt, geldt ingevolge artikel 10, eerste lid, van de eIDAS-verordening dat de aanmeldende lidstaat onverwijld de grensoverschrijdende authenticatie of de delen waarvan de integriteit geschonden is, moet opschorten of intrekken, en de andere lidstaten en de Commissie hiervan op de hoogte moet stellen.

Artikel 19

Lid 1–2

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 betrokkenen in de authenticatieketen nodig. Dit artikel voorziet daarin. De plicht om desgevraagd of uit eigen beweging de informatie te verschaffen die de Minister van BZK nodig heeft om maatregelen te kunnen nemen om inbreuk op de veilige en betrouwbare toegang tot elektronische dienstverlening te voorkomen of te beëindigen, omvat het melden van incidenten of andere zaken die aanzienlijke gevolgen hebben of kunnen hebben op de veilige en betrouwbare toegang tot elektronische dienstverlening. 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 betrokken partijen 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 uitge-

wisseld 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. 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.

Artikel 20

Lid 1

Dit lid verankert het algemene uitgangspunt dat de burger zal moeten betalen voor de aanschaf van een publiek identificatiemiddel 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. De kosten voor de extra functie van authenticatie op de e-NIK zullen worden verdisconteerd in het tarief voor de NIK. Hiertoe zal het Besluit Paspoortgelden worden aangepast. 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. Op basis van de voorgestelde bepaling zal een tarief kunnen worden geheven voor een publiek middel op betrouwbaarheidsniveau substantieel.

Artikel 21

De kosten die het Rijk maakt samenhangend met de uitvoering van de artikelen 5 (realiseren van publieke middelen en voorzieningen) en 9 (toelaten van private middelen) worden door de Minister ten laste gebracht van de bestuursorganen en aangewezen organisaties respectievelijk (namelijk indien ingevolge artikel 5, vijfde lid, voorzieningen en een aansluitplicht worden gereguleerd) andere organen die het betreft. Op dit moment is het nog niet goed mogelijk om de totale kosten en de componenten daarvan in beeld te brengen. Evenmin is bekend in welke mate er gebruik zal worden gemaakt van de voorzieningen. In de methode van doorberekening kan daarom nog geen inzicht worden geven. Zodra daarover meer duidelijkheid bestaat, worden hierover bij ministeriële regeling nadere regels gesteld.

Artikel 22

Dit artikel biedt voor de Minister van BZK de grondslag om de kosten door te berekenen voor het behandelen van een erkenningsaanvraag, alsmede voor het toezicht op de naleving van de aan de erkende dienst opgelegde eisen.

Hoewel identificatiemiddelen op een lager betrouwbaarheidsniveau dan substantieel of hoog niet ingevolge deze wet zullen worden toegelaten, zullen ze om praktische redenen voorshands beschikbaar blijven; ze

kunnen worden geaccepteerd door bestuursorganen en aangewezen organisaties voor diensten waarvoor een laag betrouwbaarheidsniveau geldt.

Artikel 23

Binnen vijf jaar na de inwerkingtreding van deze wet zal deze worden geëvalueerd, teneinde de doeltreffendheid en de effecten ervan in kaart te brengen. In het bijzonder wordt hierbij – mede naar aanleiding van gehouden privacy impact analyses – aandacht geschonken aan de vraag, of de getroffen (technische, organisatorische en juridische) maatregelen op het gebied van beveiliging en privacybescherming nog steeds voldoende zijn. Ook zaken als het systeem van de wet, de werking van de voorzieningen, de mate waarin behoefte bestaat aan nieuwe of andere functionaliteiten en interoperabiliteit komen bij gelegenheid van de evaluatie aan de orde.

Artikel 24

Het stelsel voor bedrijfs- en organisatiemiddelen is grotendeels gebaseerd op het zogenoemde Afsprakenstelsel e-Herkenning. Dit betreft een civielrechtelijk stelsel waar partijen zich bij kunnen aansluiten in het kader van de uitgifte en ontsluiting van elektronische identificatiemiddelen onder de naam e-Herkenning en waarbij ook de Staat partij is. Bij de eisen voor erkenning van diensten wordt zoveel mogelijk aangesloten bij de afspraken die in dit stelsel zijn gemaakt en bij de wijze van functioneren van het stelsel. De partijen die zijn aangesloten bij het afsprakenstelsel en de in dat kader uitgegeven middelen zullen dan ook grotendeels overeenkomen met de gestelde eisen.

Teneinde te verzekeren dat bestuursorganen en aangewezen organisaties direct na inwerkingtreding van artikel 15 aan de acceptatieplicht kunnen voldoen en anderzijds betrokken partijen de gelegenheid te geven een aanvraag in te dienen voor erkenning, voorziet dit artikel in overgangsrecht. Het uitgangspunt is dat de middelen die binnen het kader van het afsprakenstelsel worden uitgegeven en de partijen die tot het afsprakenstelsel zijn toegetreden, geacht worden erkende middelen onderscheidenlijk erkende diensten te zijn. Daarbij is van belang dat binnen het afsprakenstelsel een andere duiding van betrouwbaarheidsniveau wordt gehanteerd dan in de eIDAS-verordening. Om die reden wordt in het derde lid expliciet gemaakt dat niveau 4 correspondeert met het betrouwbaarheidsniveau hoog, niveau 3 met substantieel en niveau 2 (en 2+) met laag.

Binnen het stelsel zijn ook middelen of diensten aan de orde die voldoen aan niveau 1. Dit niveau correspondeert niet met een in de eIDAS-verordening geformuleerd betrouwbaarheidsniveau en komt na inwerkingtreding van de wet ook niet terug. Het overgangsrecht is dan ook niet van toepassing op diensten of middelen van dat niveau 1.

Het vijfde lid bevat tot slot overgangsrecht voor de in artikel 15, vijfde lid, bedoelde situaties. Daarmee wordt voorkomen dat een middel dat nu reeds door een specifieke doelgroep wordt gebruikt terstond na inwerkingtreding van artikel 15 niet langer geaccepteerd mag worden. Met het overgangsrecht wordt de gelegenheid geboden om de aanwijzing van dat middel op grond van artikel 15, vijfde lid, vorm te geven.

Artikel 25

Dit artikel voorziet in overgangsrecht terzake van een vooruitlopend op inwerkingtreding van de wet toegelaten privaat middel. Thans wordt ten behoeve van toelating van een of meerdere private middelen een verwervingsprocedure binnen de kaders van de Aanbestedingswet 2012 voorbereid. Voorzover deze in de aanloop naar inwerkingtreding van de wet zijn beslag krijgt, en leidt tot een voor inwerkingtreding van deze wet van kracht geworden overeenkomst van de Minister met een private authenticatiedienst, heeft een dergelijke toelating het rechtskarakter van een overeenkomst naar burgerlijk recht. Deze wordt voor de duur van die overeenkomst voor de toepassing van dit wetsvoorstel gelijkgesteld met een toelatingsbesluit op grond van deze wet. Op een zodanige overeenkomst en de rechtsverhouding tussen partijen zijn de bepalingen van het Burgerlijk Wetboek van kracht.

Artikel 26

Dit artikel voorziet in de mogelijkheid dat in een lagere regeling bij wijze van experiment van de acceptatieplicht in dit wetsvoorstel wordt afgeweken. Voor welbepaalde gevallen en dienstverleners kan bij algemene maatregel van bestuur worden bepaald dat, onder afwijking van artikel 7, eerste lid onder a, toegelaten en erkende middelen niet worden geaccepteerd met het oog op het onderzoeken van nieuwe methoden waarmee authenticatie doeltreffender kan plaatsvinden. Het betref de realisering van een innovatieve toepassing of het in het kader van de doorontwikkeling testen van een nieuw publiek middel bij specifieke bestuursorganen of aangewezen organisaties. Hierdoor kan proefondervindelijk worden vastgesteld of een een (door)ontwikkeld publiek of privaat middel een bijdrage kan leveren aan efficiënte, betrouwbare en gebruiksvriendelijke authenticatie in het publieke domein. Overheidsregie voeren met behulp van wettelijke kaders hoeft immers niet te betekenen dat geen ruimte wordt gegeven aan de improviserende, innoverende en proberende samenleving.[95] Hierbij geldt overigens dat van de (Europeesrechtelijke) plicht tot wederzijdse erkenning van bij de Europese Commissie genotificeerde middelen niet kan worden afgeweken (zie de toelichting bij artikel 7).

Artikel 27

In verband met de ontwikkeling en afgifte van een e-rijbewijs is het van belang een grondslag te scheppen voor de door gemeenten aan de RDW te vergoeden kosten. Ook wordt, in aansluiting op diens verantwoordelijkheid voor de uitgifte van het rijbewijs, de verantwoordelijkheid van de Dienst Wegverkeer (RDW) gespecificeerd voor wat betreft het plaatsen van een publiek identificatiemiddel op betrouwbaarheidsniveau hoog op het rijbewijs.

---

[95] *Zie het signalenrapport «Mobiliteit en elektriciteit in het digitale tijdperk. Publieke waarden onder spanning», waarin het Planbureau voor de Leefomgeving pleit voor een proces van kleine stappen en voortdurende bijsturing op basis van evaluatie: «Juist experimenten – die later kunnen worden teruggedraaid – verdienen intensieve aandacht van de rijksoverheid om zo de innovaties te steunen en richting te geven die vanuit publieke belangen gunstig uitpakken. Ze maken ook tijdig ingrijpen mogelijk als nieuwe ontwikkelingen onze publieke waarden onder druk zetten».*

A

Artikel 107, tweede en derde lid, van de Wegenverkeerswet 1994 regelt de verschijningsvorm van het rijbewijs. Teneinde het onderdeel te maken van het rijbewijs voorziet A in de toevoeging aan artikel 107, derde lid, dat het rijbewijs een publiek identificatiemiddel als bedoeld in artikel 1 van dit wetsvoorstel bevat. Omdat artikel 5, eerste lid, van dit wetsvoorstel bepaalt dat een publiek identificatiemiddel slechts kan worden afgegeven aan een natuurlijke persoon die beschikt over een burgerservicenummer is in het voorgestelde artikel 107, derde lid, van de Wegenverkeerswet 1994 als voorwaarde voor het plaatsen gesteld dat de aanvrager over een burgerservicenummer beschikt. Degene die een rijbewijs aanvraagt, maar niet beschikt over een burgerservicenummer krijgt derhalve een rijbewijs zonder publiek middel. Voor de volledigheid wordt er op gewezen dat degene die als niet-ingezetene beschikt over een burgerservicenummer toch geen rijbewijs met een publiek middel krijgt. De eisen die de eIDAS-verordening en de daarop gebaseerde bepalingen stellen aan identificatiemiddelen op het betrouwbaarheidsniveau hoog staan daaraan in het geval van het rijbewijs in de weg, aangezien niet-ingezetene niet altijd in persoon hoeven te verschijnen om een rijbewijs aan te vragen (zie artikel 49, derde lid, van het Reglement rijbewijzen). Het rijbewijs bevat reeds een chip, waarop het publieke identificatiemiddel kan worden geplaatst. Richtlijn 2006/126/EG van het Europees Parlement en de Raad van 20 december 2006 betreffende het rijbewijs (PbEU 2006, L 403) laat ruimte voor andere functionaliteiten op die chip dan die strekkende tot uitvoering van de die richtlijn op voorwaarde dat die uitvoering niet gehinderd wordt. Van dergelijke hinder is geen sprake en overeenkomstig artikel 1, derde lid, van richtlijn 2006/126/EG heeft afstemming plaatsgevonden met de Europese Commissie.

B

Op grond van artikel 5, vierde lid, van het wetsvoorstel heeft de RDW tot taak een publiek identificatiemiddel op het rijbewijs te plaatsen en af te geven. Omdat dat op het rijbewijs wordt geplaatst en daarmee onderdeel is van het verloopt de aanvraag en afgifte van dat middel op dezelfde wijze als voor het rijbewijs. Desondanks zijn er kosten gemoeid met het plaatsen en afgeven van een publiek identificatiemiddel. Daarbij gaat het om enerzijds de productiekosten van het middel, inclusief het personaliseren, en anderzijds de bijkomende handelingen als registratie van de gegevens van het middel en het na afgifte van het rijbewijs aan de aanvrager aanmaken en toezenden van een pincode voor het bewuste middel. Die kosten hebben geen betrekking op het rijbewijs als zodanig, daarom wordt in artikel 111, vijfde lid, Wegenverkeerswet 1994 toegevoegd dat de kosten met betrekking tot het publieke identificatiemiddel gedekt worden uit het tarief.

Zoals aangegeven worden de kosten voor het publieke identificatiemiddel doorbelast via de leges voor het rijbewijs. Naar verwachting is het productieproces van het rijbewijs reeds voor de inwerkingtreding van de Wet digitale overheid afgestemd op de plaatsing van het publieke identificatiemiddel. Het kan dus zijn, dat een houder van een publiek middel op een rijbewijs dat is uitgegeven voor inwerkingtreding van de wet dit, teneinde het te kunnen gebruiken als elektronisch identificatiemiddel, pas wil activeren na inwerkingtreding van de wet.
Alsdan wordt een bij ministeriële regeling te bepalen tarief in rekening gebracht.

C

Op grond van artikel 5, vierde lid, van het wetsvoorstel heeft de RDW tot taak een publiek identificatiemiddel op het rijbewijs te plaatsen en af te geven. Omdat dat middel op het rijbewijs wordt geplaatst en daarmee onderdeel is van het rijbewijs, verloopt de aanvraag en afgifte van dat middel op dezelfde wijze als voor het rijbewijs. Desondanks zijn er kosten gemoeid met het plaatsen en afgeven van een publiek identificatiemiddel. Daarbij gaat het om enerzijds de productiekosten van het middel, inclusief het personaliseren, en anderzijds de bijkomende handelingen als registratie van de gegevens van het middel en het na afgifte van het rijbewijs aan de aanvrager aanmaken en toezenden van een pincode voor het bewuste publieke identificatiemiddel. Die kosten hebben geen betrekking op het rijbewijs als zodanig, daarom wordt in artikel 121, eerste lid, van de Wegenverkeerswet 1994 toegevoegd dat de kosten met betrekking tot het publieke identificatiemiddel gedekt worden uit de zogenoemde rijkskostencomponent.

D

Met deze toevoeging wordt expliciet gemaakt dat de RDW in het rijbewijzenregister gegevens verwerkt omtrent de op rijbewijzen geplaatste publieke identificatiemiddelen.

Artikel 28

Tot op heden gold artikel X, eerste lid, van de Wet Elektronisch berichtenverkeer Belastingdienst (WEBV) als grondslag voor de taken en verantwoordelijkheden van Onze Minister terzake van voorzieningen voor elektronisch berichtenverkeer en informatieverschaffing en elektronische authenticatie, inclusief elektronische registratie van machtigen. Dit vormde de opmaat naar de onderhavige wet; met de inwerkingtreding komt artikel X van de WEBV te vervallen. De onderdelen en leden van artikel X krijgen een plek in deze wet. Ook worden het Besluit verwerking persoonsgegevens GDI en het Besluit digitale toegankelijkheid overheid «omgehangen».

Artikel 29

Onverwijlde inwerkingtreding van dit wetsvoorstel is nodig met het oog op de implementatie van richtlijn (EU) 2016/2102 inzake de toegankelijkheid van overheidswebsites benodigde grondslag (artikel 28, onderdeel b) en de voor kostendoorberekening benodigde grondslag (artikel 20), alsmede de goede uitvoering van de eIDAS-verordening, in het bijzonder terzake van de benodigde infrastructuur. Voor het overige wordt gestreefd naar gefaseerde inwerkingtreding van de wet met ingang van 1 januari 2019. Het daadwerkelijke tijdstip van inwerkingtreding zal bij koninklijk besluit worden bepaald, mede aan de hand van het tijdstip waarop technische randvoorwaarden gerealiseerd kunnen zijn, waaronder voorzieningen zoals de routeringsvoorziening en aansluiting door de bestuursorganen en aangewezen organisaties op die voorzieningen. Door in dit verband een aansluitschema op te stellen, worden zij in staat gesteld om hun elektronische dienstverlening en de toegang daartoe technisch en organisatorisch op orde te brengen; dit is nodig om gevolg te kunnen geven aan de acceptatieplichten. Het schema zal erop gericht zijn zo snel mogelijk na inwerkingtreding van de overige bepalingen van de wet alle in artikel 2 genoemde bestuursorganen en aangewezen instanties voor hun diensten aangesloten te hebben. Op basis van dit schema kunnen

koninklijke besluiten als bedoeld in het tweede lid worden voorbereid. De betrokkenen dragen er zorg voor dat zij op het desbetreffende tijdstip daadwerkelijk en volledig uitvoering kunnen geven aan de wet.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
R.W. Knops