Besluit van ……. , houdende vaststelling van regels inzake de aanwijzing en erkenning van publieke en private identificatiemiddelen (Besluit identificatiemiddelen voor natuurlijke personen Wdo)

Wij Willem-Alexander, bij de gratie Gods, Koning der Nederlanden, Prins van Oranje-Nassau, enz. enz. enz.

Op de voordracht van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van ……, nr. ……..;

Gelet op artikel 9, eerste, tweede, derde, vierde en negende lid, van de Wet digitale overheid;

De Afdeling advisering van de Raad van State gehoord (advies van ……nr. W…….);

Gezien het nader rapport van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van ……, nr. ……;

Hebben goedgevonden en verstaan:

Hoofdstuk 1 Algemeen

Artikel 1 Begripsbepalingen

In dit besluit en de daarop berustende bepalingen wordt verstaan onder:

- *erkenning:* erkenning als bedoeld in artikel 9, tweede lid, van de wet;
- *gebruiker:* natuurlijke persoon die gebruik maakt van een identificatiemiddel als bedoeld in artikel 9 van de wet en die een overeenkomst heeft gesloten met de aanbieder van dat identificatiemiddel;
- *Onze Minister*: Onze Minister van Binnenlandse Zaken en Koninkrijksrelaties;
- *transparante software*: software die onder een open source licentie is gepubliceerd en software waarvan de broncode openbaar is gemaakt;
- *Uitvoeringsverordening (EU) 2015/1502*: 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 (PbEU 2015, L235);

- *wet*: Wet digitale overheid.

Hoofdstuk 2 Privaat identificatiemiddel voor natuurlijke personen

Paragraaf 2.1 Eisen voor toelating van een privaat identificatiemiddel

Artikel 2 Eisen privaat identificatiemiddel

De eisen, bedoeld in artikel 9, tweede lid, van de wet, voor erkenning van een privaat identificatiemiddel zijn de eisen die zijn opgenomen in artikel 3 en 4 en de nadere eisen gesteld krachtens artikel 7 voor het betrouwbaarheidsniveau van het desbetreffende identificatiemiddel.

Artikel 3 Eisen aan aanvrager

1. De aanvrager:

a. verkeert niet in staat van faillissement of liquidatie, en voor of door hem is geen faillissement aangevraagd;

b. is geen surseance van betaling verleend en daarvoor is geen aanvraag ingediend;

c. voldoet aan de eisen, bedoeld in paragraaf 2.4 van de bijlage bij Uitvoeringsverordening (EU) 2015/1502, voor zover deze het betrouwbaarheidsniveau betreffen waarop de aanvraag ziet;

d. kan, op het moment dat deze voor hem gelden, voldoen aan de eisen voor een houder van een erkenning, bedoeld in artikel bij en krachtens paragraaf 2.3;

e. verwerkt gegevens over een gebruiker van een identificatiemiddel zodanig dat voor het combineren van die gegevens met de gegevens over het gebruik van dat identificatiemiddel door die gebruiker, een nadere handeling nodig is, voor zover het gegevens betreft die in het kader van de erkenning zijn verkregen;

f. registreert het moment waarop een handeling als bedoeld in onderdeel e is verricht en de persoon die deze handeling heeft uitgevoerd;

g. heeft een vestiging in Nederland waar kan worden aangetoond dat de aanvrager voldoet aan de eisen voor erkenning;

h. kan de gebruiker inzicht geven in:

i. de authenticatiehandelingen die met dat identificatiemiddel zijn verricht;

ii. de datum en het tijdstip waarop voor dat identificatiemiddel een handeling als bedoeld in het eerste lid, onderdeel e, is uitgevoerd, met uitzondering van de gevallen waarin die handeling plaatsvond op verzoek van Onze Minister.

2. Het eerste lid, onderdelen a en b, zijn van overeenkomstige toepassing indien ten aanzien van de aanvrager in een van de overige lidstaten van de Europese Unie of een van de overige staten die partij zijn bij de Overeenkomst betreffende de Europese Economische Ruimte een met de in die onderdelen vergelijkbare procedure is gestart of aangevraagd.

3. De eisen, bedoeld in het eerste lid, met uitzondering van de onderdelen a en b, zijn van overeenkomstige toepassing op een derde voor zover aan deze derde in het kader van de erkenning werkzaamheden worden uitbesteed.

Artikel 4 Eisen aan identificatiemiddel

Het identificatiemiddel waarop de aanvraag ziet:

a. functioneert in samenwerking met de daarvoor benodigde onderdelen van de generieke digitale infrastructuur, bedoeld in artikel 5 van de wet, en, in voorkomend geval, andere voor de werking van het identificatiemiddel noodzakelijke voorzieningen;

b. functioneert overeenkomstig artikel 5b, 5e, 9b en 14b van het Besluit digitale overheid;

c. voldoet aan de eisen die voor het desbetreffende betrouwbaarheidsniveau worden gesteld in de paragrafen 2.1.1, 2.1.2, 2.2.1, 2.2.2, 2.2.3, 2.3 en 2.4 van de bijlage bij Uitvoeringsverordening (EU) 2015/1502.

Artikel 5 Inkomsten uit verstrekken van gegevens over gebruikers of authenticatie

In de overeenkomst die door een aanvrager met een gebruiker wordt gesloten voor het gebruik van een identificatiemiddel is een verplichting opgenomen voor de aanvrager om het verstrekken van persoonsgegevens van de gebruiker of daarvan afgeleide informatie aan derde partijen op verzoek van de gebruiker te beëindigen zonder dat die beëindiging voor de gebruiker nadelige gevolgen heeft ten aanzien van de kosten voor de gebruiker of de gebruiksfunctionaliteit.

Artikel 6 Toepassing van software met openbare broncode

1. Een identificatiemiddel waarop een aanvraag ziet voldoet ten minste aan een door Onze Minister vaststellen norm voor het gebruik van software die onder een open source licentie is gepubliceerd en voor het gebruik van software waarvan de broncode openbaar is gemaakt.

2. Bij ministeriële regeling worden regels gesteld over de wijze waarop wordt bepaald of aan het eerste lid is voldaan, waarbij in ieder geval rekening wordt gehouden met:

a. de beschikbaarheid van transparante software voor bij authenticatie noodzakelijke processen;

b. de veiligheid van beschikbare transparante software;

c. de gevolgen van het implementeren van beschikbare transparante software voor de het aanbod van identificatiemiddelen, waaronder in ieder geval de continuïteit, gebruiksvriendelijkheid en beschikbaarheid van het aanbod.

d. de haalbaarheid van het implementeren van beschikbare transparante software in aan het identificatiemiddel gerelateerde technische en organisatorische maatregelen en processen.

3. Bij toepassing van het eerste lid kan voor de verschillende functionaliteiten van een identificatiemiddel een verschillende norm worden vastgesteld.

Artikel 7 Nadere eisen bij ministeriële regeling

1. Bij ministeriële regeling worden nadere eisen gesteld met betrekking tot:

a. het aanvragen van het identificatiemiddel bij een aanbieder door en het registreren van een beoogd gebruiker;

b. de wijze waarop de identiteit van de aanvrager van het identificatiemiddel wordt bewezen en geverifieerd;

c. de kenmerken en het ontwerp van het identificatiemiddel;

d. uitgifte, uitreiking en activering van het identificatiemiddel;

e. schorsing, intrekking en reactivering van het identificatiemiddel;

f. verlenging en vervanging van het identificatiemiddel;

g. het authenticatiemechanisme dat het identificatiemiddel toepast;

h. het beheer en de organisatie, waaronder het beheer van informatiebeveiliging, bijhouden van de administratie, faciliteiten en personeel, technische controles en controles op conformiteit met andere dan technische eisen;

i. de beveiliging van de processen, bedoeld in onderdeel a tot en met g;

j. de inhoud van de overeenkomst die de aanvrager zal sluiten met een gebruiker van het identificatiemiddel;

k. periodieke actualisatie en controle van de juistheid van voor het authenticatieproces gebruikte gegevens;

l. voorzieningen die worden gebruikt bij toepassing van het identificatiemiddel of bij het verwerken van gegevens;

m. de integriteit en kwalificaties van het bestuur van de organisatie van de aanbieder van het identificatiemiddel en van het personeel dat betrokken is bij de inzage of het beheer van identificatiemiddelen;

n. het herkennen en het voorkomen van misbruik, fraude en incidenten gerelateerd aan de aanvraag, registratie en gebruik van het identificatiemiddel en het herstel van de gevolgen daarvan, waaronder het herleiden van handelingen die met een identificatiemiddel en ten behoeve van het verkrijgen daarvan zijn verricht en het overleggen van gegevens over dit onderwerp aan Onze Minister;

o. de wijze van verwerking van in het kader van authenticatie verkregen persoonsgegevens en de beveiliging of organisatorische of technische inrichting daarvan;

p. de gebruiksvriendelijkheid van een identificatiemiddel.

2. Bij ministeriële regeling kunnen tevens nadere eisen worden gesteld met betrekking tot de interoperabiliteit met en het aansluiten op de onderdelen van de infrastructuur, bedoeld in artikel 5, eerste en tweede lid, van de wet, en op andere voor de werking van het identificatiemiddel noodzakelijke voorzieningen.

3. Bij toepassing van het eerste en tweede lid kan onderscheid worden gemaakt tussen verschillende betrouwbaarheidsniveaus.

Paragraaf 2.2 Procedurele voorschriften erkenning

Artikel 8 Erkenning op aanvraag

Een erkenning wordt slechts op aanvraag verstrekt.

Artikel 9 Aanvraaggerechtigden erkenning

Een aanvraag wordt ingediend door een rechtspersoon of onderneming in de zin van de Handelsregisterwet 2007.

Artikel 10 Aanvraagvereisten

1. Onverminderd artikel 9, vijfde lid, van de wet gaat een aanvraag in ieder geval vergezeld van:

a. bewijsstukken waarmee wordt onderbouwd dat wordt voldaan aan de eisen die van toepassing zijn op het betrouwbaarheidsniveau waarop de aanvraag ziet;

b. een beschrijving van de organisatie van de rechtspersoon of onderneming en de wijze waarop de zeggenschap daarbinnen is georganiseerd;

c. een model van de overeenkomst die de aanvrager zal sluiten met gebruikers van het identificatiemiddel waarop de aanvraag ziet;

d. een onderbouwing dat met de aanvraag wordt voldaan aan artikel 25 van de Algemene verordening gegevensbescherming;

e. een onderbouwing dat met de aanvraag wordt voldaan aan de norm, bedoeld in artikel 6, eerste lid;

f. het adres van de vestiging bedoeld in artikel 3, eerste lid, onderdeel g.

2. Bij ministeriële regeling worden nadere regels gesteld met betrekking tot de inhoud van een aanvraag, de vorm waarin deze wordt ingediend en de documenten die daarbij worden verstrekt, waarbij onderscheid kan worden gemaakt tussen een aanvrager als bedoeld in het derde lid en overige aanvragers.

3. Het eerste lid, aanhef en onderdeel a, d en e, zijn niet van toepassing op een aanvrager die tevens houder is van een erkenning als bedoeld in artikel 11, tweede lid, van de wet.

Artikel 11 Medewerking aanvrager

Een aanvrager verleent Onze Minister ten behoeve van de beoordeling van een aanvraag medewerking binnen een door Onze Minister gestelde termijn.

Artikel 12 Eisen aan een verklaring van certificering

1. Een verklaring als bedoeld in artikel 9, vijfde lid, van de wet ziet op de norm ISO 27001 en heeft een afgiftedatum die niet meer dan een jaar in het verleden ligt.

2. De verklaring is afgegeven door een instelling die voor het afgeven van een certificaat als bedoeld in het eerste lid is geaccrediteerd door een nationale accreditatie-instantie als bedoeld in artikel 2, onderdeel 11, van de verordening (EG) nr. 765/2008 van het Europees Parlement en de Raad van 9 juli 2008 tot vaststelling van de eisen inzake accreditatie en markttoezicht betreffende het verhandelen van producten en tot intrekking van Verordening (EG) nr. 339/93 (PbEU 2008, L 218).

3. Een verklaring als bedoeld in het eerste lid ziet op het identificatiemiddel waarvoor de erkenning wordt aangevraagd op het betrouwbaarheidsniveau waarop de aanvraag ziet.

4. De verklaring, bedoeld in het eerste lid, gaat vergezeld van alle rapportages van de instelling die de verklaring heeft afgegeven waarin is opgenomen ten aanzien van welke aspecten gedurende de onderzoeken die aan de verklaring ten grondslag liggen is geconstateerd dat niet is voldaan aan de eisen waaraan is getoetst.

Artikel 13 Verlening erkenning

1. Onverminderd artikel 9, zesde lid, van de wet wordt een aanvraag afgewezen indien de aanvrager niet voldoet aan artikel 11 van dit besluit.

2. Indien op een aanvraag positief wordt beslist wordt een erkenning verleend aan de aanvrager.

Artikel 14 Beslistermijn

1. Onze Minister beslist binnen twaalf weken na ontvangst van een aanvraag.

2. Op aanvragen die ten minste twaalf weken voor het aflopen van de termijn bedoeld in artikel 24 van de wet zijn ingediend is in afwijking van het eerste lid een termijn van achttien weken van toepassing.
3. Paragraaf 4.1.3.3 van de Algemene wet bestuursrecht is niet van toepassing op een erkenning.

Artikel 15 Bekendmaking erkenning

Van een erkenning of wijziging, schorsing of intrekking daarvan wordt mededeling gedaan in de Staatscourant.

Artikel 16 Geldigheidsduur erkenning

1. Een erkenning wordt voor onbepaalde tijd verleend.

2. Onze minister bepaalt het moment waarop een verleende erkenning van kracht wordt met inachtneming van de periode die voor betrokken bestuursorganen, aangewezen instanties en rechterlijke organisaties nodig is om te kunnen voldoen aan artikel 7 van de wet.

Paragraaf 2.3 Eisen aan houders van een erkenning

Artikel 17 Voldoen aan erkenningseisen en uitbesteding van werkzaamheden

1. Een houder van een erkenning voldoet aan de eisen die in paragraaf 2.1 en die in artikel 9, zesde lid, van de wet zijn gesteld voor het verlenen van een erkenning.

2. Bij ministeriële regeling kan worden bepaald dat op een houder van een erkenning gedurende een bij die regeling te bepalen periode een andere eis van toepassing is dan een eis als bedoeld in het eerste lid.

3. Een houder van een erkenning draagt er zorg voor dat een derde waaraan in het kader van de erkenning werkzaamheden worden uitbesteed zich verplicht alle medewerking te verlenen en informatie te verstrekken die voor het toezicht op de naleving van de beveiligings- en geheimhoudingsverplichtingen noodzakelijk is.

Artikel 18 Beschrijving van de dienstverlening

Een houder van een erkenning publiceert een actuele beschrijving van zijn dienstverlening voor gebruikers, met in ieder geval:

a. een beschrijving van de technische werking van het authenticatiemiddel waaronder de ontwikkelprocessen, de toegepaste maatregelen rond beveiliging, betrouwbaarheid en cryptografie alsmede van de toepassing van de stand der techniek daarbij;

b. een beschrijving van de wijze waarop de werking van het identificatiemiddel en het authenticatieproces gebaseerd is op software:

i. waarvan de broncode openbaar is gemaakt; of

ii. waarvan de broncode valt onder een open-source licentie, waarbij deze licentie wordt beschreven;

c. in voorkomend geval, de overwegingen om voor delen van de werking van het authenticatiemiddel en het authenticatieproces geen gebruik te maken van broncode bedoeld in onderdeel b, subonderdeel i. en ii, gerelateerd aan de overwegingen genoemd in artikel 6, tweede lid.

Artikel 19 Actuele verklaring van certificering

1. Een houder van een erkenning beschikt over een geldige verklaring als bedoeld in artikel 12, eerste lid:

a. die ziet op het identificatiemiddel waarvoor de erkenning is verleend;

b. waarvan de afgiftedatum niet meer dan drie jaar in het verleden ligt; en

c. waarvan validiteit ten minste jaarlijks door de afgevende instantie is getoetst en herbevestigd.

2. Een houder van een erkenning verstrekt onverwijld na ontvangst daarvan aan Onze Minister een rapportage die wordt opgemaakt in het kader van de toetsing, bedoeld in het eerste lid, onderdeel c.

Artikel 20 Rapportage

Een houder van een erkenning rapporteert op bij ministeriële regeling bepaalde wijze aan Onze Minister over bij die regeling vastgestelde onderwerpen.

Artikel 21 Uitvoeren van een onafhankelijk onderzoek

1. Onze Minister kan een houder van een erkenning bij beschikking verplichten dat deze:

a. een onafhankelijke deskundige laat onderzoeken of de houder voldoet aan de voor hem geldende eisen gesteld bij of krachtens dit besluit; of

b. een onafhankelijke deskundige een boekhoudkundig onderzoek laat uitvoeren om te bepalen of de houder handelt of heeft gehandeld in strijd met artikel 24, eerste lid, aanhef en onderdeel b.

2. Het onderzoek wordt uitgevoerd binnen een bij de beschikking vermelde termijn, op een in de beschikking vermelde wijze en de houder van de erkenning draagt de kosten voor het uitvoeren ervan.

3. Bij ministeriële regeling kunnen nadere regels worden gesteld over het eerste en tweede lid.

Artikel 22 Leveringsplicht en beschikbaarheid

1. Binnen een bij ministeriële regeling te bepalen termijn nadat de erkenning van kracht wordt biedt de houder van de erkenning het identificatiemiddel aan waarvoor hij is erkend.

2. Een houder van een erkenning draagt er zorg voor dat het identificatiemiddel waarop de erkenning ziet in ieder geval voldoet aan een bij ministeriële regeling te stellen beschikbaarheidsnorm, die voor verschillende betrouwbaarheidsniveaus verschillend kan worden vastgesteld.

3. Bij ministeriële regeling worden regels gesteld over de wijze waarop de beschikbaarheid wordt gemeten of berekend en nadere regels over de beschikbaarheid, bedoeld in het tweede lid.

4. Het eerste lid is niet van toepassing vanaf het moment waarop een besluit als bedoeld in artikel 28, derde lid, aanhef van kracht wordt.

5. Een houder van een erkenning beschikt over een loket voor vragen of meldingen aangaande ontstane problemen in de toegang van gebruikers tot elektronische dienstverlening.

Artikel 23 Meldingsplicht

1. Een houder van een erkenning meldt ontwikkelingen die van belang zijn voor de erkenning onverwijld aan onze minister, waaronder in ieder geval worden begrepen:

a. wijzigingen die worden aangebracht in de werking van het identificatiemiddel waarop de erkenning betrekking heeft, of de bijbehorende processen ten opzichte van de omschrijving daarvan in de aanvraag voor die erkenning, voor zover de houder voor die wijzigingen geen andere erkenning of wijziging van de erkenning aanvraagt;

b. wijzigingen in de organisatie of de zeggenschap, bedoeld in artikel 10, eerste lid, onderdeel b, ten opzichte van de omschrijving daarvan in de aanvraag voor die erkenning;
c. elke inbreuk op de veilige en betrouwbare toegang tot elektronische dienstverlening als bedoeld in artikel 19, eerste lid, van de wet, waarvan de duur en de gevolgen van zodanige aard zijn dat de veilige en betrouwbare toegang op significante wijze in het geding is of dreigt te komen of de continuïteit van de betrouwbare toegang anderszins op significante wijze verstoord wordt of dreigt te worden.

2. Bij ministeriële regeling worden nadere regels gesteld over de verplichting, bedoeld in het eerste lid, de inhoud van een melding, de termijn waarbinnen en de wijze waarop deze wordt gedaan en kunnen regels worden gesteld over de beoordeling of sprake is van een wijziging of inbreuk als bedoeld in het eerste lid.

Artikel 24 Omgaan met persoonsgegevens en transparantie over verdienmodel

1. Een houder van een erkenning draagt er zorg voor dat binnen zijn organisatie alle persoonsgegevens die in het kader van de diensten waarvoor hij is erkend worden verwerkt:

a. vertrouwelijk worden behandeld;

b. niet worden gebruikt voor een voor ander doel dan voor het uitgeven van een identificatiemiddel of authenticatie van de identiteit van gebruikers.

2. Een houder van een erkenning maakt openbaar op welke wijze met de erkenning en de persoonsgegevens die voor de uitvoering van die erkenning worden verwerkt inkomsten worden verkregen.

Artikel 25 Nadere eisen bij ministeriële regeling

1. Bij ministeriële regeling kunnen nadere eisen worden gesteld aan een houder van een erkenning met betrekking tot:

a. de mogelijkheden voor gebruikers om contact op te nemen met de houder van de erkenning voor vragen of meldingen over de toegang tot elektronische dienstverlening of een website met informatie over die toegang;

b. de vertrouwelijke behandeling van gegevens;

c. het bewaren van gegevens met het oog op herstelvermogen voor onder meer het beslechten van geschillen, het inzien door een gebruiker van zijn gegevens en het verstrekken van dergelijke gegevens aan Onze Minister;

d. een periodieke controle van juistheid van gebruikte gegevens;

e. de wijze waarop gebruikers door de houder van een erkenning worden geïnformeerd over het feit dat het identificatiemiddel waarop de erkenning ziet tijdelijk of permanent niet bruikbaar zal zijn of de wijze waarop gegevens die zijn verwerkt in het kader van de erkenning voorafgaand aan intrekking van een erkenning worden overgedragen aan andere partijen;

f. de bereikbaarheid van de houder van de erkenning in het kader van het tegengaan of het oplossen van incidenten die de beschikbaarheid of betrouwbaarheid raken;

g. de tijdsduur die het oplossen van incidenten ten hoogste vergt;

h. de onderwerpen, bedoeld in artikel 7, eerste en tweede lid;

i. de wijze waarop wordt voldaan aan artikel 18;

j. de toepassing van de gronden, bedoeld in artikel 9, zesde lid, onderdeel b tot en met e.

2. Bij toepassing van het eerste lid kan onderscheid worden gemaakt tussen verschillende betrouwbaarheidsniveaus.

Paragraaf 2.4 Wijziging of intrekking van een erkenning

Artikel 27 Wijziging van een erkenning

1. Artikel 11 is van overeenkomstige toepassing op een aanvraag tot wijziging van een erkenning.

2. Een aanvraag tot wijziging van een erkenning wordt afgewezen indien:

a. met de aangevraagde wijziging niet wordt voldaan aan de eisen, bedoeld paragraaf 2.1;

b. de wijziging ziet op de houder van de erkenning en de beoogde houder niet een rechtspersoon of onderneming is als bedoeld in artikel 9.

c. de aanvrager niet de medewerking, bedoeld artikel 11, verleent.

Artikel 28 Intrekking erkenning op verzoek

1. Een erkenning wordt op aanvraag van de houder van de erkenning ingetrokken indien de aanvrager aannemelijk heeft gemaakt dat:

a. de gegevens die in het kader van de erkenning zijn verwerkt na intrekking van de erkenning op deugdelijke wijze worden vernietigd, bewaard of ter bewaring worden overgedragen aan een partij die daarmee op veilige en betrouwbare wijze zal omgaan;

b. de houder gebruikers tijdig en deugdelijk informeert over het moment waarop het identificatiemiddel niet meer beschikbaar zal zijn en de wijze waarop wordt omgegaan met gegevens die in dat verband zijn verkregen.

2. Een aanvraag als bedoeld in het eerste lid bevat in ieder geval:

a. een beschrijving van de wijze waarop invulling wordt gegeven aan de eisen bedoeld in het eerste lid;

b. een aanduiding van het moment waarop de aanvrager het aanbieden van het identificatiemiddel wil staken.

3. Indien is voldaan aan de eisen in het eerste lid, besluit Onze Minister tot intrekking van de desbetreffende erkenning onder de opschortende voorwaarde dat de houder van de erkenning:

a. handelt overeenkomstig de beschrijving, bedoeld in het tweede lid, onderdeel a;

b. gebruikers gedurende zes maanden na het van kracht worden van het intrekkingsbesluit in de gelegenheid stelt om gegevens die over die gebruiker zijn verkregen over te laten dragen aan een andere door de gebruiker gekozen partij.

4. Bij ministeriële regeling kunnen nadere regels worden gesteld over:

a. de onderwerpen, bedoeld in het eerste lid, onderdeel a en b;

b. de inhoud en de vorm van een aanvraag als bedoeld in het eerste lid.

Artikel 29 Ambtshalve intrekking of schorsing erkenning

Onze Minister kan een erkenning intrekken of schorsen indien de houder van de erkenning niet aannemelijk heeft gemaakt dat wordt voldaan aan de verplichtingen die aan de erkenning zijn verbonden.

Artikel 30 Advies Landelijk Bureau BIBOB

Alvorens te beslissen over het wijzigen, schorsen of intrekken van een erkenning vanwege zwaarwegende redenen als bedoeld in artikel 9, zesde lid, van de wet, kan aan het Bureau bevordering integriteitsbeoordelingen door het openbaar bestuur, bedoeld in artikel 8 van de Wet bevordering integriteitsbeoordelingen door het openbaar bestuur, om een advies als bedoeld in artikel 9 van die wet worden gevraagd.

Hoofdstuk 3 Publiek identificatiemiddel voor natuurlijke personen

Paragraaf 3.1 Eisen voor aanwijzing van een publiek identificatiemiddel

Artikel 31 Eisen publiek identificatiemiddel

1. De eisen, bedoeld in artikel 9, eerste lid, van de wet, voor het aanwijzen van een publiek identificatiemiddel zijn de eisen die zijn opgenomen in paragraaf 2.1 voor het betrouwbaarheidsniveau van het desbetreffende identificatiemiddel, tenzij bij ministeriële regeling is bepaald dat een eis niet van toepassing is.

2. Op een publiek identificatiemiddel dat krachtens artikel 9, eerste lid, van de wet is aangewezen zijn de eisen die zijn opgenomen in de artikelen 17, 18, 22, tweede en derde lid, 23, eerste lid, onderdeel c, en 24 en de eisen gesteld krachtens artikel 25 van overeenkomstige toepassing, tenzij bij ministeriële regeling is bepaald dat een eis niet van toepassing is.

3. Bij ministeriële regeling kunnen per betrouwbaarheidsniveau nadere eisen voor aanwijzing worden gesteld aan een publiek identificatiemiddel over de onderwerpen, bedoeld in artikel 7,

eerste en tweede lid en eisen voor een aangewezen publiek identificatiemiddel over de onderwerpen, bedoeld in artikel 25, eerste lid.

Paragraaf 3.2 Procedurele voorschriften aanwijzing

Artikel 32 Aanwijzing ambtshalve

Een aanwijzing als bedoeld in artikel 9, eerste lid, van de wet geschiedt ambtshalve.

Artikel 33 Mededeling aanwijzing

Van een aanwijzing of wijziging of intrekking daarvan wordt mededeling gedaan in de Staatscourant.

Artikel 34 Geldigheidsduur aanwijzing

Een aanwijzing geldt voor onbepaalde tijd.

Hoofdstuk 4. Ontsluitende diensten

(Gereserveerd)

Hoofdstuk 5. Slotbepalingen

Artikel 35 Inwerkingtreding

Dit besluit treedt in werking op een bij koninklijk besluit te bepalen tijdstip, dat voor de verschillende artikelen of onderdelen daarvan verschillend kan worden vastgesteld.

Artikel 36 Citeertitel

Dit besluit wordt aangehaald als: Besluit identificatiemiddelen voor natuurlijke personen Wdo.

Lasten en bevelen dat dit besluit met de daarbij behorende nota van toelichting in het Staatsblad zal worden geplaatst.

De minister van Binnenlandse Zaken en Koninkrijksrelaties,

Nota van toelichting

1. Algemeen

Burgers en bedrijven communiceren steeds meer digitaal met de publieke en semipublieke organisaties. Hierbij kan bijvoorbeeld worden gedacht aan een burger die een vergunning aanvraagt of een dossier wil inzien. Bij deze communicatiemomenten zal telkens op betrouwbare wijze de identiteit moeten worden vastgesteld van degene die communiceert terwijl de privacy en de gegevens van die persoon worden beschermd en beveiligd. Burgers en bedrijven moeten erop kunnen vertrouwen dat anderen dan zij zelf geen toegang kunnen krijgen tot gegevens en diensten die voor hen bedoeld zijn. Een veilig en betrouwbaar identificatiesysteem is daarvoor cruciaal. Door dit besluit wordt dat verzekerd.

De Wet digitale overheid (hierna: de wet) regelt de manier waarop identificatie van burgers en ondernemingen bij publieke dienstverleners kan plaatsvinden. Voor natuurlijke personen bevat die wet in artikel 5, eerste lid, onderdeel a, een taak voor de minister van Binnenlandse Zaken en Koninkrijksrelaties om op verschillende betrouwbaarheidsniveaus identificatiemiddelen aan te bieden. Voor natuurlijke persoon is daarom altijd een publiek identificatiemiddel beschikbaar. Dat middel moet voldoen aan eisen op het gebied van onder meer veiligheid en betrouwbaarheid.

Dit besluit ziet enkel op de toelating van identificatiemiddelen voor burgers tot het Nederlandse stelsel. De toelating van identificatiemiddelen voor bedrijven en organisaties wordt op grond van de Wet digitale overheid separaat geregeld in het Besluit bedrijfs- en organisatiemiddel Wdo.

De wet bevat verder een mogelijkheid om door private partijen aangeboden identificatiemiddelen toe te laten tot het Nederlandse stelsel. Artikel 9 van de wet regelt dat identificatiemiddelen voor burgers door de minister van Binnenlandse Zaken en Koninkrijksrelaties kunnen worden toegelaten door middel van een erkenning als deze voldoen aan in dat artikel en daarop gebaseerde eisen. Een toelating van een middel leidt tot acceptatie van dat middel door organisaties in het publieke domein. Verder regelt artikel 9 van de wet dat een toegelaten middel gedurende de toelatingsperiode moet blijven voldoen aan bepaalde eisen.

Artikel 9, zesde lid, van de wet bevat een aantal afwijzingscriteria die bij het beoordelen van een toelatingsaanvraag worden toegepast. Die criteria zien op de toepassing van software die onder een open source licentie is gepubliceerd, de toepassing van privacy by design, het verdienen aan handel in gegevens en ernstig gevaar voor de staatsveiligheid, cyberveiligheid of misbruik van een toelating voor strafbare feiten. In dit besluit worden deze criteria voor zover nodig verder uitgewerkt.

Nadere eisen voor toetsing en de eisen waaraan een identificatiemiddelen in het Nederlandse stelsel, publiek of privaat, moeten voldoen worden ook met dit besluit en de onderliggende ministeriële regeling vastgelegd. Enkel identificatiemiddelen waarvan na een toetsingsprocedure

onder meer is vastgesteld dat deze veilig en betrouwbaar zijn worden tot het stelsel toegelaten. Bij deze toetsing worden alle aspecten van het identificatieproces betrokken en wordt zowel de werking van het middel als de organisatie van de aanbiedende partij onderzocht. Met de eisen die daaraan worden gesteld wordt onder meer geborgd dat toegelaten partijen op veilige en vertrouwelijke wijze omgaan met de gegevens die verwerken om het inloggen mogelijk te maken. Verder wordt in dit besluit geregeld op welke wijze een erkenning kan worden verkregen en in welke gevallen deze wordt geschorst of ingetrokken en aan welke eisen een door de overheid verschaft middel moet voldoen.

In dit besluit wordt derhalve de basis gelegd voor een betrouwbaar en veilig stelsel van identificatiemiddelen waarop zowel de publieke dienstverleners als burgers kunnen vertrouwen. De waarborgen die bepalend zijn voor het beschermingsniveau voor natuurlijke personen die deze middelen gebruiken zijn vastgelegd in dit besluit. Gelet op het detailniveau van de te stellen eisen bevat dit besluit voor het overige een basis om deze bij ministeriële regeling vast te stellen.

2. Juridische context: Betrouwbaarheidsniveaus en acceptatieplicht van toegelaten identificatiemiddelen

2.1 Betrouwbaarheidsniveaus

De wet beoogt betrouwbare en veilige identificatie te borgen van zowel burgers als bedrijven in het kader van elektronische dienstverlening door publieke dienstverleners. In artikel 2 van de wet is geregeld welke dienstverleners onder de reikwijdte van de wet vallen. Artikel 6 van de wet regelt dat de dienstverlener waarbij wordt ingelogd bepaalt op welk betrouwbaarheidsniveau moet worden ingelogd. Die instantie, bepaalt op basis van een set met door de Minister van Binnenlandse Zaken en Koninkrijksrelaties vastgestelde criteria, welk niveau op de desbetreffende dienst van toepassing is.

Daarbij worden drie niveaus onderscheiden; laag, substantieel en hoog. Deze inschaling van deze niveaus voor publieke dienstverleners sluit aan bij de niveaus die worden gehanteerd voor identificatiemiddelen in Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (hierna: de eIDAS-verordening).

2.2 Door Nederland toegelaten middelen

Op grond van artikel 7, eerste lid, aanhef en onderdeel a, van de wet mogen voor een dienst waarvoor betrouwbaarheidsniveau substantieel en hoog vereist is identificatiemiddelen worden geaccepteerd waarvan is vastgesteld dat deze voldoen aan de eisen die bij of krachtens algemene maatregel van bestuur worden gesteld aan een identificatiemiddel op het desbetreffende niveau.

De artikelen 9 en 11 van de wet regelen de Nederlandse toelating van middelen voor burgers en bedrijven. Een middel kan worden toegelaten als het voldoet aan de eisen die voor het desbetreffende betrouwbaarheidsniveau zijn gesteld. De inhoud van die eisen en het proces van toelating worden gedeeltelijk op wetsniveau en voor het overige in lagere regelgeving vastgelegd. Voor identificatiemiddelen voor burgers vindt invulling plaats met dit besluit en de ministeriële regeling die op dit besluit wordt gebaseerd.

2.3 Verhouding tot de eIDAS-verordening

Dit besluit regelt de toelating van identificatiemiddelen tot het Nederlandse eID-stelsel. Een middel wordt toegelaten tot dat stelsel wanneer het voldoet aan de eisen die in en op grond van dit besluit worden gesteld. Zoals in paragraaf 3.2 uiteen wordt gezet vormen de eisen uit het Europese eIDAS-regelgevingscomplex de basis voor deze eisen. Op grond van artikel 7, eerste lid, onderdeel a, van de wet worden middelen die zijn toegelaten tot het Nederlandse stelsel geaccepteerd door dienstverleners in het publieke domein.

De Wet digitale overheid bepaalt verder dat ook middelen die behoren tot een stelsel dat in een Europese context is genotificeerd worden geaccepteerd door publieke dienstverleners. Dat is het gevolg van het Europese eIDAS-verordening. Die verordening regelt de wederzijdse erkenning van identificatiemiddelen voor burgers en bedrijven op niveau substantieel en hoog die behoren tot stelsels van andere EU-lidstaten. Een identificatiemiddel dat onderdeel is van een stelsel dat voldoet aan de eisen die op grond van die verordening worden gesteld kan door een lidstaat worden aangemeld. Indien na aanmelding met positief resultaat een door die verordening voorgeschreven procedure wordt doorlopen wordt het stelsel door de Europese Commissie geplaatst op een lijst. Identificatiemiddelen op de niveaus substantieel en hoog die worden uitgegeven in het kader van een stelsel dat op die lijst is geplaatst moeten op grond van die verordening ook in andere lidstaten worden geaccepteerd door dienstverleners in het publieke domein. Artikel 7, eerste lid, onderdeel c, van de wet regelt deze acceptatieplicht voor middelen op die lijst in de Nederland, voor zover het middelen voor burgers betreft.

Gelet op het voorgaande hoeft een middel dat behoort tot een genotificeerd stelsel dus niet het nationale toelatingstraject te doorlopen om te worden geaccepteerd, omdat deze middelen al op grond van artikel 7, eerste lid, onderdeel c, van de wet worden geaccepteerd. De verantwoordelijkheid voor de conformiteit met de eIDAS en AVG eisen voor een genotificeerd middel, en aansprakelijkheid bij falen, ligt bij de lidstaat die dit heeft genotificeerd.

Middelen die behoren tot stelsels van andere EU-lidstaten kunnen niet zonder meer functioneren binnen het Nederlandse stelsel. Om de werking van die middelen mogelijk te maken is een voorziening gecreëerd, het eIDAS-knooppunt, waarop genotificeerde stelsels moeten aansluiten. Doordat via dit knooppunt wordt aangesloten op het Nederlandse stelsel worden de identificatiemiddelen die behoren tot deze stelsels bruikbaar binnen de Nederlandse context. Voor gebruikers is het onderscheid merkbaar tussen een middel dat behoort tot het nationale stelsel en

een middel dat behoort tot een stelsel van een andere EU-lidstaat. In het inlogproces krijgt een gebruiker eerst de keuze uit de middelen die behoren tot het nationale stelsel. Om te kiezen voor een middel dat behoort tot een stelsel van een andere lidstaat zal de gebruiker moeten kiezen voor de optie "eIDAS" waarna de verschillende genotificeerde stelsels kunnen worden gekozen. Met deze indeling blijft het inlogproces overzichtelijk, gelet op het feit het gebruik van een middel uit een andere EU-lidstaat verhoudingsgewijs een uitzondering vormt. Deze werkwijze past binnen het principe van wederzijdse erkenning, dat de basis vormt voor de regulering van identificatiemiddelen in het eIDAS-regelgevingscomplex. Daarop wordt in paragraaf 3.3 uitgebreid ingegaan.

2.4 Verhouding tot toelating van identificatiemiddelen voor bedrijven en organisaties

Dit besluit ziet enkel op de toelating van identificatiemiddelen voor burgers tot het Nederlandse stelsel. De toelating van identificatiemiddelen voor bedrijven en organisaties wordt op grond van de Wet digitale overheid separaat in een andere algemene maatregel van bestuur geregeld. Beoogd wordt om op termijn, in de tweede tranche van de Wet digitale overheid, het wettelijke regime te uniformeren, zodat één toelatingsregime ontstaat. Als gevolg daarvan zal dit besluit moeten worden gewijzigd. De eisen die worden gesteld op grond van dit besluit en het besluit dat ziet op bedrijfsmiddelen worden vooruitlopend op deze wijziging reeds in één ministeriele regeling ondergebracht en zoveel mogelijk met elkaar in overeenstemming gebracht.

3. Toelating van identificatiemiddelen tot het Nederlandse stelsel

3.1 Beleidsmatige achtergrond

Het kabinet streeft naar een stelsel waarmee burgers "veilig, betrouwbaar, gebruiksvriendelijk kunnen inloggen zodat zij transacties kunnen verrichten in de digitale wereld[1]". Tot het moment van inwerkingtreding van de wet en dit besluit kon identificatie door burgers slechts plaatsvinden met gebruik van het publieke identificatiemiddel DigiD en met middelen die in het kader van de Europese eIDAS-verordening zijn genotificeerd. De wettelijke taak voor de minister om zorg te dragen voor voorzieningen voor authenticatie was vastgelegd in artikel X van de Wet elektronisch berichtenverkeer Belastingdienst. Met de Wet digitale overheid wordt de positie van DigiD wettelijk verankerd in artikel 5, eerste lid, onderdeel a. Daarin is vastgelegd dat de minister van Binnenlandse Zaken en Koninkrijksrelaties een wettelijke taak heeft om publieke identificatiemiddelen aan te bieden op verschillende betrouwbaarheidsniveaus[2]. Daarmee is geborgd dat burgers gebruik kunnen maken van een publiek identificatiemiddel. Dit middel zal derhalve moet voldoen aan de daaraan gestelde eisen, zodat het op grond van artikel 9, eerste lid, van de wet kan worden toegelaten toe het Nederlandse stelsel.

[1] Kamerstukken II, 34972, nr. 11, p. 3.
[2] Voor het inwerkingtreden van de wet werd de taak om een publiek middel aan te bieden gebaseerd op artikel X van de Wet elektronisch berichtenverkeer Belastingdienst.

Met de inwerkingtreding van de wet wordt het daarnaast voor private partijen mogelijk om een identificatiemiddel voor burgers aan te bieden voor de toegang tot publieke dienstverlening, indien zij voldoen aan eisen die onder meer de veiligheid en de betrouwbaarheid borgen. Veel mensen beschikken al over een identificatiemiddel dat in het commerciële domein wordt gebruikt. Gedacht kan worden aan identificatie bij webwinkels. Voor deze gebruikers kan het handig zijn als deze identificatiemiddelen ook kunnen worden gebruikt om in te loggen bij publieke dienstverleners. Die ruimte wordt geboden door deze identificatiemiddelen ook toe te laten, mits deze voldoen aan de in en op grond van dit besluit gestelde eisen.

Verder wordt met de keuze om ook private identificatiemiddelen toe te laten meer ruimte geboden voor de innovatieve kracht van de markt en te komen tot een systeem waarin gebruikers kunnen kiezen welk middel aansluit bij hun gebruikswensen[3]. Daarnaast is een systeem met meerdere voor burgers beschikbare middelen minder kwetsbaar voor uitval, hetgeen de stabiliteit van de toegang tot overheidsdienstverlening ten goede komt. Immers, indien een middel onverhoopt niet beschikbaar is, kan de gebruiker terugvallen op een ander middel. Daarmee wordt de kans dat die burgers geen toegang kunnen krijgen tot publieke dienstverlening verkleind. In dat licht is het tevens van belang dat de middelen die zijn toegelaten slechts zeer beperkte uitval vertonen en voldoende beschikbaar zijn voor gebruik.

Tegelijkertijd moet met deugdelijke randvoorwaarden worden geborgd dat private partijen zorgvuldig omgaan met gegevens van gebruikers en dat gebruikers van het stelsel zo gebruiksvriendelijk mogelijk zijn. Zo moet worden voorkomen dat de gegevens van burgers als handelswaar worden verkocht, moet vast staan dat deze veilig worden bewaard en verzonden en moet er voor alle gebruikers een manier zijn om toegang te krijgen tot publieke diensten. Als deze randvoorwaarden zijn vervuld kunnen private partijen een rol spelen bij de identificatie van natuurlijke personen voor de toegang tot publieke dienstverlening.

In het licht van het voorgaande moeten de eisen voor toelating van identificatiemiddelen borgen dat toegelaten middelen voldoende veilig, betrouwbaar en gebruiksvriendelijk zijn, en laten deze ruimte voor nieuwe innovatieve mogelijkheden die de bescherming, en het gebruiksgemak of de keuzevrijheid voor burgers kunnen vergroten. In dit hoofdstuk wordt het beleid ten aanzien van deze waarborgen uitgebreid uiteengezet.

3.2 Toelatingseisen op wetsniveau

Artikel 9, zesde lid van de wet bevat een aantal afwijzingscriteria waaraan erkenningsaanvraag moet worden getoetst. Een deel van deze criteria is in opgenomen in het oorspronkelijke wetsvoorstel voor de Wet digitale overheid[4] en een deel is daaraan toegevoegd met een novelle[5]. Op deze criteria wordt in het hiernavolgende ingegaan voor zover nadere uitwerking daarvan plaatsvindt met dit besluit en de daarop gebaseerde regels.

[3] Kamerstukken II, 34972, nr. 11, p. 2.
[4] Kamerstukken II, 34972, nr. 2.
[5] Kamerstukken II, 35868, nr. 2.

3.2.1 Privacy by design

Artikel 9, zesde lid, aanhef en onderdeel b, van de wet bepalen dat een erkenning niet wordt verleend indien "het ontwerp van het identificatiemiddel of de ontsluitende dienst naar de stand der techniek en andere redelijkerwijs beschikbare mogelijkheden op het moment van aanvraag onvoldoende voorziet in de bescherming van gegevens". In de memorie van toelichting[6] wordt daarbij aangegeven dat met dit criterium wordt vastgelegd dat geen toelating wordt verleend voor identificatiemiddelen die niet voldoen aan artikel 25 van de Europese Algemene verordening gegevensbescherming (AVG). Met dit besluit wordt van aanvragers van een erkenning gevraagd om bij een erkenningsaanvraag te onderbouwen dat is voldaan aan artikel 25 van de AVG.

3.2.2 Verhandelen van gegevens

Onderdeel c van artikel 9, zesde lid, van de wet bepaalt dat een erkenning niet wordt verleend indien "de aanvrager niet aannemelijk heeft gemaakt dat met de erkenning geen inkomsten worden verkregen uit het verhandelen of verstrekken van gegevens over gebruikers of authenticatie van gebruikers". Dat artikel is een onderdeel van een pakket aan waarborgen om het verhandelen van gebruikersdata tegen te gaan. In het hiernavolgende wordt ingegaan op het totaal van die maatregelen en specifiek op de toepassing van dit wettelijk afwijzingscriterium binnen die context.

Het kabinet vindt het bij identificatie in het publieke domein niet acceptabel dat gegevens die door private partijen worden verkregen voor inloggen bij de overheid, commercieel gebruikt worden. In dit besluit is daarom bepaald dat het niet is toegestaan om gegevens die zijn verkregen in verband met identificatie van gebruikers wordt gebruikt voor andere doeleinden dan authenticatie. Op deze zogenaamde doelbinding wordt ingegaan in paragraaf 6.1. In dit verband is ook de verplichte scheiding van gegevens van gebruikers en gebruik van belang. Wanneer gegevens over het gebruik zonder nadere handelingen niet herleidbaar zijn tot de desbetreffende gebruikers kunnen deze niet worden gebruikt voor commerciële doeleinden. Gebruikers krijgen vervolgens de mogelijkheid om in te zien op welke momenten deze scheiding is doorbroken, waardoor zelfcontrole mogelijk wordt. Deze eisen zijn een verdere explicitering van de eisen die al zijn opgenomen in artikel 16 van de wet en in artikel 5b en 5e van het Besluit digitale overheid.

Profilering of verkoop van de gegevens is door deze eisen nadrukkelijk verboden. Op overtreding daarvan staat in ultimo intrekking van een erkenning of een omzetgerelateerde boete op grond van de Uitvoeringswet AVG.

Door de bredere bruikbaarheid van inlogmiddelen voor de toegang elektronische overheidsdienstverlening zijn inlogmiddelen een aantrekkelijk doelwit voor kwaadwillenden die fraude of misbruik willen plegen, waardoor burgers en bedrijven slachtoffer kunnen worden. Door de genoemde maatregelen wordt ook het risico teruggedrongen dat gegevens die bijvoorbeeld als

[6] Kamerstukken II, 35868, nr. 3

gevolg van een datalek worden verkregen bruikbaar zijn voor andere partijen is in dit besluit opgenomen dat private aanbieders van identificatiemiddelen gegevens over gebruikers gescheiden moeten opslaan van gegevens over het gebruik. Op deze eis wordt nader ingegaan in paragraaf 4.1.3. Dit besluit maakt het ook mogelijk om regels te stellen die tegengaan dat gebruikers worden omgeleid naar een andere website dan waar zij denken in te loggen.

Wanneer vermoeden bestaat dat het verhandelverbod voor persoonsgegevens wordt overtreden kan aan een houder van een erkenning worden gevraagd om een boekhoudkundig onderzoek te laten uitvoeren om te laten onderzoeken of sprake is van een overtreding. Dit instrument dient ter aanvulling van het bestaande toezichtsinstrumentarium dat de toezichthouder, Agentschap Telecom, op grond van de Algemene wet bestuursrecht ter beschikking staat.

Het verhandelverbod bevat een strikte regeling om handel in gegevens te voorkomen. Mocht blijken dat aanbieders gegevens verwerken die naar de letter van de regels geen overtreding van de gestelde regels inhoudt, maar die de gebruiker desondanks niet wenselijk vindt, dan wordt gebruikers een middel in handen gegevens om zelf in te grijpen om deze gegevensverwerking te beëindigen. Dit besluit schrijft namelijk voor dat aan gebruikers altijd een mogelijkheid moet worden geboden om levering van gegevens te beëindigen zonder dat sprake is van nadelige financiële gevolgen of verlies van functionaliteiten van het inlogmiddel. Een erkenninghouder moet deze optie expliciet opnemen in een met de gebruiker te sluiten overeenkomst. Die overeenkomst wordt in het kader van de aanvraagprocedure overgelegd.

Met de bovenstaande randvoorwaarden, te weten een verhandelsverbod, aanvullende toezichtsinstrumenten en een vangnet voor onvoorziene gevallen, is naar het oordeel van de regering voldoende voorzien in bescherming van gebruikers tegen datahandel. Onder deze voorwaarden is het voor bedrijven die hun verdienmodel hebben gebaseerd op datahandel niet aantrekkelijk om deel te nemen aan het stelsel. Wanneer een aanvrager van een erkenning aantoont dat aan deze voorwaarden is voldaan wordt aangenomen dat geen inkomsten worden verkregen uit de het verhandelen of verstrekken van gegevens over gebruikers of authenticatie van gebruikers.

3.2.3 Gebruik van software met een open source-licentie

Artikel 9, zesde lid, onderdeel d, van de wet schrijft voor dat een erkenning niet wordt verleend indien naar het oordeel van de minister onvoldoende gebruik wordt gemaakt van software die onder een open source licentie is verleend. In de nota naar aanleiding van het verslag bij het wetsvoorstel waarmee dit criterium in de wet is genomen wordt uitgebreid ingegaan op de beleidsmatige achtergrond van dit toetsingscriterium[7]. In deze paragraaf wordt daarom kort op die achtergrond ingegaan.

Het gebruik van software met een open source licentie kan grote voordelen hebben. Zo is het, wanneer de software goed wordt ondersteund door een actieve gebruikersgemeenschap, voor

[7] Kamerstukken II, 35868, nr. 6.

gebruikers mogelijk om inzichtelijk te maken op welke wijze de aanboden dienst wordt uitgevoerd en of er ongewenste processen worden uitgevoerd bij het gebruik van deze software. Verder kunnen derde partijen een oordeel vormen over de kwaliteit van de beveiliging en de veiligheid van de software en daarmee ook van het identificatiemiddel waarvoor deze wordt gebruikt. Deze transparantie kan dus bijdragen aan de beleidsmatige doelen van het kabinet bij toegang tot overheidsdienstverlening. Er zijn uiteraard ook aandachtspunten. Zo kan inzicht in de broncode van software ook ten koste gaan van de veiligheid van de software, omdat het, in sommige gevallen, eenvoudiger wordt voor kwaadwillenden om de zwakke plekken van de beveiliging te vinden. Met deze aandachtspunten moet rekening worden gehouden om te zorgen dat toegang tot digitale overheidsdienstverlening mogelijk blijft en dat daarvoor een toenemend aanbod van identificatiemiddelen dat gebruik maakt van open source beschikbaar komt.

Zoals in de nadere memorie van antwoord bij het wetsvoorstel voor de Wet digitale overheid wordt vermeld is open source de weg die we opgaan. Om dat einddoel te bereiken wordt in diezelfde memorie aangekondigd dat een groeimodel wordt gehanteerd. Met dit besluit wordt dit groeimodel mogelijk gemaakt. Op grond van dit besluit stelt een minister een norm vast waaraan een aanvrager moet voldoen met betrekking tot het gebruik van open source software in de processen van het identificatiemiddel. De norm wordt vastgesteld met inachtneming van de beschikbare software met een open source-licentie, de veiligheid van die software en de gevolgen van het implementeren voor het aanbod van identificatiemiddelen voor gebruik bij overheidsdienstverlening. Om groei naar meer open source af te dwingen wordt de norm zodra dat mogelijk is gelet op de relevant belangen, naar boven bijgesteld.

Het is zeer denkbaar dat voor verschillende functionaliteiten van een identificatiemiddel op verschillende momenten nieuwe veilige open source-software beschikbaar komt. Daarom maakt dit besluit het mogelijk om voor verschillende functies een verschillende norm vast te stellen.

Bij ministeriële regeling wordt vastgesteld op welke wijze wordt bepaald of aan de desbetreffende norm is voldaan.

Met deze eisen wordt de weg naar open source ingezet , met als doel transparantie te verkrijgen over de inzet van open source software in de processen van de aanbieders van identificatiemiddelen.

3.3 Eisen met betrekking tot betrouwbaarheid van inlogmiddelen en bescherming van persoonsgegevens: eIDAS en AVG

Het basisniveau van bescherming op het gebied van betrouwbaarheid wordt geboden door de eisen die de eIDAS-regelgeving stelt aan inlogmiddelen. Deze eisen gaan bijvoorbeeld over de onderliggende uitgifte-, activerings- en authenticatieprocessen en de daaraan gerelateerde betrouwbaarheidsniveaus die met deze middelen worden behaald. Zoals in paragraaf 2.1 is aangegeven worden in het eIDAS-regelgevingscomplex drie betrouwbaarheidsniveaus onderscheiden; laag, substantieel en hoog. De eisen die worden gesteld aan middelen die op deze niveaus worden uitgegeven zijn opgenomen in 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 (hierna: eIDAS-uitvoeringsverordening 1502). Daarin wordt voor niveau laag in veel gevallen gebruik gemaakt van "one-factor" authenticatie. Het gaat ruwweg om middelen met het betrouwbaarheidsniveau van DigiD basis, zoals dat op het moment van inwerkingtreding van dit besluit in werking was. De niveaus substantieel en hoog zijn beide gebaseerd op "two-factor" authenticatie. Daarbij heeft niveau hoog een hogere weerstand tegen (technische) aanvallen dan niveau substantieel. De eIDAS-uitvoeringsverordening 1502 stelt per betrouwbaarheidsniveau nadere eisen. Zoals in paragraaf 2.3 uiteen is gezet gelden deze Europese eisen niet rechtstreeks voor het Nederlandse stelsel, maar enkel bij grensoverschrijdend gebruik van identificatiemiddelen binnen de Europese Unie. Met dit besluit wordt geregeld dat eIDAS-eisen ook gelden voor het toelaten van identificatiemiddelen voor natuurlijke personen tot het Nederlandse stelsel.

De AVG bevat verplichtingen en waarborgen op het gebied van bescherming van persoonsgegevens. Anders dan de Europese eIDAS-regels voor de werking van identificatiemiddelen werken de regels van de AVG rechtsreeks in de Nederlandse rechtsorde. De overheid, onder meer in de rol als aanbieder van een publiek middel, en private aanbieders van zo'n middel moeten zich dus houden aan de regels van de AVG. Omdat de AVG rechtstreeks werkt is het niet nodig om de inhoud daarvan toepassing te verklaren op het Nederlandse stelsel. Dit besluit biedt een basis om daaraan uitvoering te geven.

De toepassing van eIDAS-eisen en de verplichtingen op grond van de AVG vormen het basisniveau voor de bescherming op het gebied van betrouwbaarheid, veiligheid en privacybescherming bij het inloggen bij de overheid. Voor de Nederlandse context wordt daaraan, met dit besluit en de daarop gebaseerde ministeriële regeling, verdere invulling gegeven. Op dit dynamische beleidsterrein, waarin ontwikkelingen elkaar snel opvolgen, moet de overheid snel kunnen inspelen op veranderende omstandigheden en technische ontwikkelingen. Dit besluit biedt daarom de noodzakelijke ruimte om bij ministeriële regeling aanvullende eisen te stellen waar ter borging van de beleidsdoelen. Deze context stelt Nederland in staat om de eisen te stellen die nodig zijn voor een veilig en betrouwbaar systeem voor identificatie, dat werkt binnen de nationale digitale infrastructuur en specifieke Nederlandse regels (bijvoorbeeld met betrekking tot het gebruik van het burgerservicenummer) en waarmee Nederland recht kan doen aan de verantwoordelijkheden van en aansprakelijkheid voor het stelsel.

3.4 Bescherming tegen misbruik: herstelvermogen

Volledige veiligheid is nooit te garanderen, ook niet in de digitale systemen. Daarom wordt voorzien in een vangnet, herstelvermogen, dat ervoor zorgt dat misbruik zo snel mogelijk wordt

herkend, en de gevolgen voor burgers en bedrijven zowel mogelijk worden beperkt of zo spoedig mogelijk worden hersteld.

Op basis van dit besluit wordt geregeld dat partijen binnen het stelsel zelf een verantwoordelijkheid hebben om misbruik te herkennen en te herstellen, doordat over dit onderwerp regels kunnen worden gesteld. Daarvoor worden nadere regels te stellen invulling te geven aan de Europese eIDAS- en AVG-eisen over dit onderwerp.

Waar de eIDAS-regelgeving bijvoorbeeld eisen bevat voor de mate waarin het authenticatiemechanisme bestand moet zijn tegen aanvallen daarop, ligt het voor de hand om deze eis ook voor de andere noodzakelijke processen, zoals het aanvraag- en registratieproces, te stellen. Een aanvaller zal immers het meest kwetsbare onderdeel van het proces aanvallen om een inbreuk te forceren.

Misbruik en fraude kunnen met preventieve maatregelen gericht op veilige uitgifte en werking van middelen en toezicht daarop niet geheel worden voorkomen. Volledige zekerheid is, zeker ook met steeds wijzigende digitale dreigingen, niet haalbaar. Daarom is het noodzakelijk om ook het herstelvermogen van het stelsel te borgen. Daarmee wordt bedoeld het vermogen en de plicht van aanbieders van inlogmiddelen om fraude vroegtijdig te kunnen herkennen en de gevolgen ervan te herstellen en om daaruit lering te trekken om toekomstige gevallen te voorkomen. Dit besluit maakt het daarom tevens mogelijk om dat herstelvermogen voor te schrijven. Een voorbeeld is de eis dat gebruikers inzicht moet hebben in het gebruik van de middelen die op hun naam zijn geregistreerd, waardoor problemen door de gebruiker zelf kunnen worden opgemerkt. Dat maakt het mogelijk dat gebruikers frauduleuze identificatiepogingen herkennen en maatregelen nemen om verder gevolgen daarvan te voorkomen.

3.5 Kosten voor gebruikers

Het is van belang dat burgers zo laagdrempelig mogelijk kunnen inloggen om toegang te krijgen tot publieke dienstverlening. De wet regelt daarvoor dat er publieke identificatiemiddelen beschikbaar moeten zijn op verschillende betrouwbaarheidsniveau. Die wettelijke taak is opgedragen aan de minister van Binnenlandse Zaken en Koninkrijksrelaties[8].

De minister van Binnenlandse Zaken en Koninkrijksrelaties biedt deze middelen als "nutsvoorziening" gratis of tegen beperkte kosten aan. Zo wordt voor burgers te allen tijde laagdrempelige toegang tot publieke voorzieningen verzekerd.

3.6 Beschikbaarheid en bereikbaarheid voor gebruikers

Zoals in paragraaf 3.1 uiteen is gezet is het voor het kabinet van belang dat de toegelaten middelen ook daadwerkelijk beschikbaar zijn voor gebruikers. Voor houders van een erkenning zal

[8] Doordat sprake is van een wettelijke taak is geen sprake van een economische activiteit waarvoor op grond van Hoofdstuk 4b van de Mededingingswet de integrale kostprijs in rekening moet worden gebracht.

daarom een verplichting gelden om het aantal technische storingen en onderbrekingen van de werking bij het middel waarop de erkenning ziet zoveel mogelijk te beperken. De details met betrekking tot de wijze waarop de beschikbaarheid wordt berekend en de wijze waarop daarover wordt gerapporteerd worden bij ministeriële regeling verder uitgewerkt.

3.7 Gebruiksgemak van middelen, iedereen moet mee kunnen doen

Om laagdrempelige toegang tot publieke diensten mogelijk te maken is het belangrijk dat het inlogproces en de daarin te maken keuzes voor burgers overzichtelijk zijn. Daarbij is bijzondere aandacht nodig voor kwetsbare groepen in de samenleving, zoals personen die minder digivaardig zijn of personen die een beperking hebben, want voor hen is gebruik van digitale voorzieningen vaak lastiger of minder goed toegankelijk. Het kabinet vindt digitale inclusie, het zorgen dat iedereen ook digitaal kan meedoen, essentieel. Op grond van dit besluit kunnen eisen worden gesteld aan gebruiksgemak van identificatiemiddelen. Daarmee wordt vooraf getoetst of een middel voldoende gebruiksvriendelijk is voor eenieder. Deze eisen kunnen bij ministeriële regeling worden gesteld.

Verder wordt een doenvermogentoets uitgevoerd ten aanzien van de eisen die in de ministeriële regeling aan identificatiemiddelen worden gesteld. Ook daarbij wordt de mentale belasting beoordeeld van gestelde eisen op gebruikers.

3.8 Ruimte voor innovatie en doorontwikkeling: doelvoorschriften

De technische aspecten van het identificatieproces zijn aan verandering onderhevig. Wanneer specifieke techniek zou worden opgenomen in de geldende regels wordt de huidige situatie bepalend voor datgene dat is toegestaan. Om toekomstige (technische) ontwikkelingen mogelijk te maken, en “state of the art” bescherming te kunnen blijven bieden zou regelgeving dan telkens moeten worden aangepast. Dat is onwenselijk, gelet op de voordelen die innovatie kan bieden voor het veilige gebruik door en het gebruiksgemak en de keuzevrijheid voor burgers. De eisen die met en op grond van dit besluit zijn gesteld zijn daarom als doelvoorschriften geformuleerd. Hiermee wordt bedoeld dat er eisen worden gesteld aan het resultaat, namelijk het bieden van waarborgen, en in beginsel niet aan de wijze waarop dit resultaat gehaald moet worden. Dat betekent dat in principe dan ook geen specifieke technische maatregelen worden voorgeschreven. Als deze specifieke technische maatregelen wel geregeld worden, wordt de noodzaak daarvan onderbouwd.

3.9 Nederlands stelsel in Europese context: gelijk speelveld

In het kader van de consultatie is door verschillende partijen opgemerkt dat een gelijk speelveld behouden moet blijven tussen partijen die worden toegelaten tot het Nederlandse stelsel en partijen die in het kader van het Europese eIDAS-regelgevingscomplex worden geaccepteerd. Hierover wordt het volgende gemeld. Het Europese eIDAS-complex beoogt geen

(minimum)harmonisatie tot stand te brengen, maar ziet op wederzijdse erkenning van nationale stelsels voor identificatie. Het uitgangspunt is daarbij dat EU-lidstaten hun eigen stelsels voor identificatie ontwikkelen. Identificatiemiddelen die behoren tot nationale stelsels kunnen op grond van de eIDAS-verordening ook in andere lidstaten worden gebruikt, wanneer deze stelsels voldoen aan minimumeisen en zijn genotificeerd bij de Europese Commissie. De notificerende lidstaat is volgens aansprakelijk voor het genotificeerde stelsel. Het doel van deze verordening is dus niet het creëren van een gelijk speelveld voor aanbieders van identificatiemiddelen, maar het vergemakkelijken van toegang tot publieke dienstverlening in andere EU-lidstaten doordat burgers en bedrijven de middelen die zij in hun land van herkomst gebruiken ook in andere landen te gebruiken. Daarmee wordt het grensoverschrijdend digitaal zakendoen in den brede bevorderd.

Binnen deze context is het aan lidstaten om hun nationale stelsel zodanig in te richten dat gegevensbescherming, betrouwbaarheid en de verantwoordelijkheid daarvoor bij grensoverschrijdend gebruik zijn geborgd. Lidstaten kunnen daarbij aan identificatiemiddelen de eisen stellen die zij daarvoor nodig achten. Wanneer een lidstaat wil dat deze middelen ook in andere EU-lidstaten kunnen worden gebruikt zijn de eIDAS-eisen relevant.

Met dit besluit wordt een basis gelegd voor een Nederlands stelsel dat voldoet aan de kwaliteitsnormen die het kabinet wenselijk vindt. Zoals in paragraaf 3.2 uiteen is gezet zijn deze eisen gebaseerd op de eisen van het eIDAS-regelgevingscomplex en de AVG, maar is in bepaalde gevallen een aanvulling of invulling wenselijk. Op grond van dit besluit is het bijvoorbeeld mogelijk om aanbieders van een identificatiemiddel te verplichten om een actieve rol te nemen in het herkennen en herstellen van misbruik en bereikbaar te zijn voor gebruikers en voor de overheid, zodat burgers bijvoorbeeld bij geconstateerd misbruik zo efficiënt mogelijk kunnen worden geïnformeerd. Deze aanvullende eisen gelden alleen voor identificatiemiddelen die, door het verlenen van een erkenning door de minister van Binnenlandse Zaken en Koninkrijksrelaties, worden toegelaten in het kader van artikel 9 van de Wet digitale overheid. Alleen die middelen worden getoetst aan de eisen die worden gesteld op grond van deze wet. Met middelen die in een andere EU-lidstaat zijn toegelaten en die behoren tot een stelsel dat genotificeerd is volgens de eIDAS-verordening, kan ook worden ingelogd bij dienstverleners in Nederland. Die positie van deze genotificeerde middelen in het inlogproces wijkt wel af van de middelen in het Nederlandse stelsel. In paragraaf 2.3 is hier nader op ingegaan.

3.10 Werking binnen de digitale overheidsinfrastructuur

Gebruik van een identificatiemiddel door een burger vindt plaats in het kader van de digitale infrastructuur van de overheid. Een publieke dienstverlener laat een burger een authenticatieverzoek doen bij de aanbieder van het middel. De aanbieder beantwoordt met een authenticatierespons, waarbij gebruik wordt gemaakt van de uitgegeven middelen. Een publieke dienstverlener kan rechtstreeks aansluiten op de diensten van een middelenaanbieder of dit laten faciliteren via de zogenaamde routeringsvoorziening, die ervoor zorgt dat een dienstverlener alle toegelaten middelen kan accepteren. In het laatste geval richt de publieke dienstverlener het authenticatieverzoek aan de routeringsvoorziening die dit doorzet naar de aanbieder; de

routeringsvoorziening zet vervolgens de authenticatierespons ook weer door naar de publieke dienstverlener.

Bij deze opzet is het van essentieel belang dat de middelenaanbieder hiervoor kan samenwerken met de overige onderdelen van de generieke digitale infrastructuur (GDI) zoals die nu binnen de overheid worden gebruikt en zoals uiteengezet in het eerste lid artikel 5 van de wet. Te denken valt aan een door de overheid beheerde routeringsvoorziening of een publiek machtigingenregister. Een aanvrager van een erkenning moet in zijn aanvraag uiteenzetten dat en op welke wijze het middel werkt binnen die infrastructuur. Als op basis van een aanvraag een erkenning wordt verleend moet de houder van die erkenning er vervolgens zorg voor dragen dat het middel blijft werken binnen de infrastructuur, ook als daaraan (technische) aanpassingen worden gedaan. Als gevolg van deze feitelijke omstandigheden zal de minister van Binnenlandse Zaken en Koninkrijksrelaties er zorg voor moeten dragen dat de technische specificaties voor aanvragers en houders van een erkenning niet verder gaan dan redelijkerwijs noodzakelijk is. Verder zullen de wijzigingen voldoende kenbaar worden gemaakt en dat wijzigingen daarin worden doorgevoerd met een voldoende tijdige aankondiging. Het ligt in de rede dat de specificaties bijvoorbeeld op een vaste website bekend worden gemaakt en dat ook aanpassingen daarvan op deze site worden aangekondigd.

Het is dus aan de aanvrager van een erkenning om in de aanvraag aan te tonen dat het middel waarvoor een erkenning wordt aangevraagd alle gewenste en vereiste functies heeft. Daarvoor zal de aanvrager in beginsel zelf moeten nagaan welke specificaties noodzakelijk zijn. Dit besluit voorziet met artikel 5, tweede lid, tevens in een mogelijkheid om regels te stellen met betrekking tot de interoperabiliteit. Dat artikel maakt het mogelijk om, bijvoorbeeld als dat in het kader van de rechtszekerheid gewenst is, specificaties voor te schrijven.

3.11 Delegatiesystematiek

Artikel 9 van de wet bepaalt, voor zover in dit verband relevant, dat bij of krachtens algemene maatregel van bestuur:

- eisen worden gesteld met betrekking tot de werking, beveiliging en betrouwbaarheid aan een publiek identificatiemiddel (eerste lid);
- eisen worden gesteld met betrekking tot de werking, beveiliging en betrouwbaarheid aan een privaat identificatiemiddel, welke in ieder geval betrekking hebben op uitgifte en beëindiging (tweede lid);
- eisen worden gesteld aan een houder van een erkenning, welke in ieder geval een leveringsplicht en regels inzake tarieven behelzen (vierde lid);
- regels worden gesteld over de procedure van erkenning, wijziging, schorsing of intrekking en de in dat verband over te leggen gegevens en informatie (negende lid).

Deze artikelleden bieden een grondslag voor het stellen van regels ter uitvoering van het beleid voor het toelaten van identificatiemiddelen zoals dat in dit hoofdstuk uiteen is gezet. In dit besluit zijn de hoofdelementen van de toelatingsprocedure en de verplichtingen voor houders van een

erkenning opgenomen. Zo is bijvoorbeeld vastgelegd dat gegevens van gebruikers en van het gebruik gescheiden moeten worden bewaard en dat gebruikers inzicht moeten krijgen in het doorbreken van die scheiding. Verder is vastgelegd dat de eisen die op grond van de eIDAS-verordening worden gesteld voor grensoverschrijdend gebruik ook gelden voor het toelaten van identificatiemiddelen tot het Nederlandse stelsel.

Uitwerking van deze hoofdelementen is noodzakelijk. Het detailniveau en technisch karakter van aanvullende specifieke toetsingscriteria is hoog. Te denken valt aan de specifieke en de technische specificaties van de verplicht te gebruiken koppelvlakken, de berekening van het beschikbaarheidsniveau of aan de wijze waarop een identificatiemiddel moet worden geactiveerd in de context van het Nederlandse stelsel. Het is mogelijk dat deze eisen door snelle technologische ontwikkelingen soms op korte termijn moeten worden gewijzigd. Door dit hoge technische karakter en de noodzaak van spoedige wijziging is ervoor gekozen de aanvullende eisen te stellen bij ministeriële regeling. Dit besluit biedt daarvoor een basis. In de paragrafen 4.1.2 en 6.6 van deze toelichting wordt uitgebreid uiteengezet op welke onderwerpen deze regels kunnen zien.

3.12 Verduidelijking van doelvoorschriften met "good practices"

Door te werken met doelvoorschriften wordt, in tegenstelling tot gedetailleerde technische voorschriften, ruimte geboden voor innovatie. Tegelijkertijd onderkent het kabinet dat bij private aanbieders behoefte kan bestaan aan duidelijkheid over de wijze waarop in ieder geval aan die voorschriften kan worden voldaan. Om daaraan tegemoet te komen wordt bekend gemaakt welke invulling van deze voorschriften in de praktijk in ieder geval werkbaar en acceptabel blijkt. In dergelijke "good practices" wordt uiteengezet welke praktische invulling van een doelvoorschrift zal leiden tot de conclusie dat is voldaan aan het voorschrift. De aanvrager of de houder van een erkenning mag er vervolgens op vertrouwen dat aan de desbetreffende voorschriften wordt voldaan als de "good practices" worden gevolgd. Daarmee kan zekerheid worden geboden aan marktpartijen die op basis van een beproefde praktijk een identificatiemiddel willen ontwikkelen, terwijl de ruimte die doelvoorschriften bieden voor innovatie, behouden blijft. Aan de hand van ervaringen in en signalen uit de uitvoeringspraktijk wordt bepaald of en in welke gevallen deze "good practices" worden opgesteld.

3.13 Verhouding met de dienstenrichtlijn

Met het aanbieden van een privaat identificatiemiddel voor natuurlijke personen wordt aan hen een dienst geleverd. Met de regels in dit besluit wordt het aanbieden van die dienst gereguleerd. Daarom is de richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten op de interne markt (hierna: de Dienstenrichtlijn) van toepassing. De artikelen 9 en verder van die richtlijn zijn van toepassing op de erkenning voor private identificatiemiddelen voor burgers. Als gevolg daarvan gelden eisen aan de criteria die worden gesteld aan de verlening van een erkenning. Artikel 10, tweede lid onderdeel d, van die richtlijn bepaalt bijvoorbeeld dat die eisen duidelijk en ondubbelzinnig moeten zijn. In de formulering en de

motivering van bijvoorbeeld de verleningscriteria in dit besluit en in de onderliggende ministeriële regeling wordt daarmee rekening gehouden. In het hoofdstuk van deze toelichting waarin wordt ingegaan op verschuldigde heffingen wordt ook ingegaan op de verhouding tussen die heffingen en artikel 13 van de dienstenrichtlijn.

4. Eisen aan een identificatiemiddel

Dit besluit bevat een kader voor zowel de eisen die gelden voor een privaat als voor een publiek identificatiemiddel. Op grond van dit besluit zijn de eisen aan een privaat middel in beginsel van toepassing op een publiek middel tenzij dit expliciet anders is geregeld. In dit hoofdstuk wordt dit systeem en op de eisen aan beide typen middelen nader ingegaan. Doordat een publiek middel ambtshalve wordt aangewezen is de procedure aanzienlijk eenvoudiger en dat heeft gevolgen voor de wijze waarop aan de gestelde eisen wordt getoetst.

In het hiernavolgende wordt deze procedure verder uiteengezet.

4.1 Erkenning van private identificatiemiddelen

Een erkenning van een privaat identificatiemiddel wordt op aanvraag verleend. Degene die een erkenning aanvraagt zal bij de aanvraag moeten aantonen dat aan de gestelde eisen wordt voldaan. Zoals in hoofdstuk 3 van deze toelichting is aangegeven worden de eisen in het kader van de eIDAS-verordening en de AVG als uitgangspunt genomen voor de eisen aan de veiligheid, betrouwbaarheid en privacybescherming van identificatiemiddelen. Daarnaast bevat dit besluit een aantal aanvullende waarborgen voor burgers in de vorm van eisen aan de aanvrager en aan het middel.

4.1.1 Eisen aan de aanvrager

Een aanvraag kan slechts worden ingediend door een rechtspersoon, naar Nederlands recht of naar het recht van een andere EU-lidstaat. Een aanvraag die bijvoorbeeld wordt ingediend door een natuurlijke persoon, niet handelend als onderneming, wordt buiten behandeling gelaten op grond van artikel 4:5 van de Algemene wet bestuursrecht. Verder wordt een aanvraag afgewezen als een aanvrager in staat van faillissement of liquidatie verkeert of als daarvoor een aanvraag is ingediend. Hetzelfde geldt in geval van surseance van betaling. Deze eisen zijn wenselijk om te borgen dat burgers niet worden geconfronteerd met een middel waarvan de werking kort na het beschikbaar worden vanwege financiële omstandigheden wordt beëindigd. Wanneer deze financiële omstandigheden bij het beoordelen van de aanvraag reeds kenbaar zijn wordt de aanvraag afgewezen.

Op grond van artikel 9, zesde en zevende lid, van de wet wordt een aanvraag verder afgewezen "in geval ernstig gevaar bestaat voor de cyberveiligheid of staatsveiligheid of in geval ernstig gevaar bestaat dat de erkenning mede zal worden gebruikt om strafbare feiten te plegen of uit

strafbare feiten verkregen of te verkrijgen voordelen te benutten of anderszins de betrouwbaarheid en veiligheid van het Nederlandse stelsel voor elektronische dienstverlening in gevaar komt". Om invulling te geven aan deze afwijzingsgrond zal informatie over de aanvrager mede bepalend zijn.

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

In de eIDAS uitvoeringsverordening 1502 van 8 september 2015, worden vier aspecten van het middel en de organisatie van de aanbieder gereguleerd:

1. de identiteitscontrole voorafgaand aan de afgifte van een identificatiemiddel aan een burger door de aanbieder;
2. het beheer van identificatiemiddelen voor burgers (waaronder middel uitgifte, schorsing en intrekking);
3. het authentiseren van burgers voor publieke dienstverleners met behulp van middelen uitgegeven door de aanbieder;
4. beheersactiviteiten en de inrichting van de organisatie van de aanbieder voor zover deze relevant is voor de identificatiedienst.

De eisen die noodzakelijk zijn om deze verordening binnen de Nederlandse context vorm te geven zijn gedetailleerd van aard. De onderdelen a tot en met i van artikel 5 bieden derhalve een basis voor het vaststellen van eisen over deze onderwerpen bij ministeriële regeling. Met deze onderdelen kunnen de eIDAS-gerelateerde eisen bij ministeriele regeling worden vastgesteld. Dit besluit biedt verder de mogelijkheid om over een aantal andere onderwerpen regels te stellen. Deze regels kunnen worden beschouwd als aanvullingen of invullingen die strikt noodzakelijk zijn om uitvoering te geven aan de AVG of om de eIDAS-eisen in de Nederlandse context toe te passen.

Artikel 7, eerste lid, biedt daarom een basis om bij ministeriële regeling bijvoorbeeld de volgende nadere eisen te stellen:

- Verplicht uit te voeren identiteitscontroles in de Basis Registratie Personen (BRP) aanvullend op de controles die de aanbieder zelf aanvoert (onderdeel a). Deze controles zijn bedoeld om het middel te kunnen laten werken met een afgeleide van het BSN.
- Een verplichting om in de overeenkomst met gebruikers op te nemen om zorgvuldig met een verstrekt identificatiemiddel om te gaan, bijvoorbeeld door anderen geen toegang te geven tot het gebruik van het middel (onderdeel j).
- Controles die, al dan niet periodiek, moeten worden uitgevoerd (onderdeel k). Gedacht kan worden aan een verplichting om periodiek na te gaan of een gebruiker nog in leven is. Een dergelijke verplichting kan misbruik van en fraude met identificatiemiddelen tegengaan.
- Een verplichting dat een op gegevensverwerking gericht antecedentenonderzoek met positief resultaat moet zijn afgerond voor personeel en bestuurders die werken aan kritieke processen (onderdeel m).

- De verplichte toepassing van bepaalde technologie, bijvoorbeeld voor het herkennen en herleiden van misbruik (onderdeel n).
- Het borgen van herstelvermogen in geval van fraude en misbruik, waaronder proactief melden van incidenten of misbruik (onderdeel n);
- De wijze waarop wordt omgegaan met versleutelde persoonsgegevens (onderdeel o).

Bij regels rond de verwerking van persoonsgegevens, waarvoor onderdeel o een basis biedt, kan bijvoorbeeld ook worden gedacht aan nadere eisen, zoals wissen van verwerkte gegevens als het bewaren daarvan niet meer nodig is, of de verplichte versleuteling waardoor bijvoorbeeld het BSN van gebruikers waar mogelijk alleen versleuteld wordt verwerkt. Dergelijke eisen zullen ook gebaseerd zijn op open standaarden en ondersteund worden door gangbare, open bibliotheken.

4.1.3 Verplicht scheiden van gegevens van gebruiker en gebruik

Dit besluit schrijft voor dat gegevens over gebruikers op zodanige wijze moeten worden bewaard dat gegevens over gebruikers niet herleidbaar zijn tot gegevens over het gebruik van het middel door die gebruikers, in dit geval identificatie bij publieke dienstverleners. Een dergelijke scheiding zorgt ervoor dat bij een eventuele inbreuk op een van de beide databases geen bruikbare gegevens worden verkregen. Verder kan een aanbieder van een identificatiemiddel zonder nadere handeling geen gegevens commercieel verhandelen. In het kader van het toelaten van identificatiemiddelen voor natuurlijke personen wordt vooraf getoetst of aan deze eis daadwerkelijk wordt voldaan. Een aanvraag wordt derhalve afgewezen als daaruit blijkt dat gegevens over gebruikers niet gescheiden worden bewaard van gegevens over het gebruik van het middel. Het betreft een functionele scheiding, waarbij voor het combineren van de gegevens een handeling nodig is. Combineren kan noodzakelijk zijn om, binnen de kaders van dit besluit, misbruik of incidenten te herkennen, te herstellen en gebruikers op de hoogte te stellen. In nadere regels op grond van dit besluit worden bijvoorbeeld regels gesteld over de kwalificaties van medewerkers die de gegevens mogen combineren. Wanneer het combineren van deze gegevens door een houder van een erkenning onrechtmatig heeft plaatsgevonden kan worden achterhaald op welk moment en door wie de handeling is uitgevoerd, omdat die informatie moet worden geregistreerd. Daarbij kunnen ook sancties, waaronder intrekking van de erkenning, worden opgelegd aan de desbetreffende aanbieder.

4.1.4 Eisen aan de werking van het middel

Zoals in paragraaf 3.10 uiteen is gezet is een aanvrager of een houder van een erkenning in beginsel verantwoordelijk voor de interoperabiliteit van het middel binnen het systeem waarbinnen dat middel werkt. Als gevolg daarvan is het aan de aanvrager of de houder om na te gaan welke specificaties het middel moet hebben om als authenticatiemiddel te kunnen functioneren. In beginsel worden derhalve geen eisen gesteld waarin specifieke techniek wordt voorgeschreven waaraan wordt getoetst.

Dit besluit bevat in artikel 5, tweede lid, een grondslag voor stellen van nadere technische eisen bij ministeriële regeling. Deze eisen kunnen nodig zijn als de specifieke inrichting van de Nederlandse GDI daartoe noopt.

4.1.5 Centrale versus decentrale architectuur

Een aantal van de reacties in het kader van de internetconsultatie wordt gesteld dat dit besluit in de weg staat aan het verlenen van een erkenning voor een identificatiemiddel met een decentrale architectuur. Met een decentrale architectuur wordt in de reacties gedoeld op een architectuur waarbij gegevens niet centraal worden opgeslagen, maar decentraal, bij de gebruiker.
Gepleit wordt voor een decentrale architectuur omwille van privacybescherming.

Het gestelde dat het besluit in de weg staat aan een decentrale architectuur is onjuist. Uitgangspunt van het besluit is dat er sprake moet zijn van een adequate bescherming van persoonsgegevens zoals vereist op basis van de AVG. Dat kan op verschillende wijze plaatsvinden.

De eisen in dit besluit zijn, conform het in paragraaf 3.8 vermeldde uitgangspunt, als doelvoorschriften geformuleerd. Dit besluit staat daarom niet in de weg aan het verlenen van een erkenning voor een middel met een centrale of een decentrale opzet. De eisen die in dit besluit zijn gesteld laten ruimte aan een aanvrager van een erkenning om daaraan op verschillende wijze invulling te geven, met inachtneming van de Algemene verordening gegevensbescherming en de eIDAS-verordening. Het is daarom mogelijk voor aanbieders van decentrale oplossingen om te worden toegelaten. Echter het is daarbij belangrijk dat zij aantoonbaar maken dat zijn aan de AVG voldoen en de geldende waarborgen voor burgers invullen, waarbij oog moet zijn voor het feit dat bij decentrale oplossingen meer verantwoordelijkheid, en daarmee ook risico, bij de gebruiker wordt gelegd, en de mogelijkheden op ondersteuning en herstelvermogen bij problemen doorgaans beperkt zijn.

4.2 Eisen aan een publiek identificatiemiddel

Met dit besluit worden tevens eisen gesteld aan het publieke identificatiemiddel. Daarbij wordt het uitgangspunt gehanteerd dat eisen die voor private partijen gelden ook op het publieke middel van toepassing zijn. De eisen met betrekking tot de veiligheid en betrouwbaarheid van een middel wijken derhalve inhoudelijk niet af van de eisen aan private identificatiemiddelen. Dat geldt voor de eisen die in dit besluit zijn vastgelegd, met dien verstande dat de eisen met betrekking tot de financiële positie van de aanbieder van het middel niet van toepassing zijn. Als gevolg daarvan wordt bij de beoordeling of een publiek middel kan worden aangewezen niet beoordeeld wat de financiële positie van het Rijk is. Het Rijk wordt verondersteld het financiële risico te kunnen dragen.

Bij ministeriële regeling worden nadere eisen vastgesteld voor private identificatiemiddelen. Ook ten aanzien van die eisen wordt met dit besluit vastgelegd dat deze in beginsel van toepassing zijn

op een publiek identificatiemiddel. Op een aantal punten is het publieke middel echter wezenlijk anders dan een privaat middel. Zo wordt bijvoorbeeld met gebruikers geen overeenkomst gesloten voor gebruik. De rechten en plichten gelden op grond van publiekrecht. Dit besluit maakt het mogelijk om regels te stellen over de inhoud van de overeenkomst tussen aanbieder en gebruiker van een middel. Deze regels kunnen derhalve niet op het publieke middel van toepassing zijn. Dit besluit maakt het mogelijk om recht te doen aan dergelijke verschillen, doordat kan worden bepaald dat specifieke eisen niet van toepassing zijn op het publieke middel. Een dergelijke uitzondering wordt uiteraard gemotiveerd gemaakt. Daarbij wordt aan de materiele eisen, die zijn op de betrouwbaarheid, de veiligheid en de bescherming van privacy, geen afwijking geregeld. Voor een publiek middel geldt verder dat deze niet wordt erkend op basis van een aanvraag, maar dat daarvoor een ambtshalve aanwijzing plaatsvindt als het middel aan de eisen voldoet.

5. Aanvraagprocedure

Degene die een erkenning voor een privaat identificatiemiddel aanvraagt moet met de aanvraag onderbouwen dat aan alle gestelde eisen is voldaan. Dit besluit regelt welke documenten bij een aanvraag in ieder geval moeten worden aangeleverd. Als een van deze documenten ontbreekt kan een aanvraag buiten behandeling worden gelaten.
Artikel 9, vijfde lid, van de wet schrijft voor dat bij een aanvraag in ieder geval een verklaring wordt overgelegd van een geaccrediteerde certificerende instelling. Op grond van het negende lid van dat artikel kunnen nadere regels worden gesteld over onder meer die verklaring. In dit hoofdstuk wordt nader ingegaan op de aanvraagprocedure.

5.1 Kring van aanvraaggerechtigden

Een beoordeling van integriteit wordt verder gebaseerd op een doorlichting van de bedrijfsstructuur en de informatie die daarover wordt aangeleverd. Een aanvraag kan daarom slechts worden ingediend door een onderneming naar Nederlands recht of naar het recht van een andere EU-lidstaat of een staat in Europese Economische Ruimte. Als een aanvraag wordt ingediend door een natuurlijke persoon wordt deze niet in behandeling genomen.

5.2 Verklaring van een geaccrediteerde certificerende instelling

Bij de aanvraag en continuering van een erkenning moet op grond van artikel 9, vijfde lid, van de wet een verklaring van een geaccrediteerde certificerende instelling worden overhandigd, waaraan het vermoeden kan worden ontleend dat aan de eisen die voor dat middel gelden is voldaan. De minister beslist op mede op basis van die verklaring op de aanvraag.

Een certificaat of conformiteitsverklaring is in het algemeen een zelfstandig document met eigen rechtsgevolg (keurmerk of toelating).[9] In dit geval geeft de certificerende instelling een verklaring af, die echter niet meer is dan een vermoeden dat aan de geldende normen en eisen is voldaan.

[9] Kabinetsstandpunt over conformiteitsbeoordeling en accreditatie in het overheidsbeleid. Kamerstukken II 2015/16, 29304, nr. 6, bijlage. Een voorbeeld is het systeem van certificering in de Jeugdwet (artikel 3.4, vierde lid, van de Jeugdwet).

Het is in feite een advies aan de minister, die zelf op de aanvraag en continuering moet beslissen. Daarom toetst hij, zo volgt uit het zorgvuldigheidsbeginsel, of de (geaccrediteerde) certificerende instelling zorgvuldig onderzoek heeft verricht.[10] Het Agentschap Telecom verricht deze toets, gelet op deskundigheid inzake (technisch-) inhoudelijke, procesmatige en juridische kennis en ervaring van die organisatie.

Dit besluit bevat algemene eisen met betrekking tot de certificeringsverklaring die bij een aanvraag moet worden overgelegd. In dit besluit is vastgelegd dat die verklaring moet zijn opgesteld door een instantie die is geaccrediteerd door de Raad voor accreditatie of een vergelijkbare instantie in een andere EU-lidstaat. Verder is bepaald dat de rapportages die zijn opgesteld bij de totstandkoming van de certificering ook moeten worden overgelegd. Op grond van welke ISO-norm wordt gecertificeerd wordt bij ministeriële regeling bepaald. ISO- norm 27001 is de leidende norm rond informatiebeveiliging. Het ligt voor de hand om in de ministeriële regeling op te nemen dan een aanvrager op grond van die ISO-norm moet zijn gecertificeerd.

5.3 Overige bij de aanvraag te voegen documenten

Naast de verklaring waarop in paragraaf 5.2 is ingegaan moet een aanvrager met documenten onderbouwen dat het middel waarop de aanvraag ziet, voldoet aan de eisen voor erkenning. Omdat deze eisen zoveel mogelijk als doelvoorschrift zijn geformuleerd bieden deze ruimte voor invulling op verschillende wijzen. Een aanvrager moet derhalve in eerste instantie inschatten op welke wijze aanvullende documentatie nodig is voor het onderbouwen van de aanvraag. Indien voor het beoordelen van een aanvraag extra informatie door de minister van Binnenlandse Zaken en Koninkrijksrelaties nodig wordt geacht kan deze worden opgevraagd.

Artikel 9, zesde lid, van de wet bepaalt dat een aanvraag voor een erkenning wordt afgewezen indien ernstig gevaar bestaat dat de erkenning mede zal worden gebruikt om strafbare feiten te plegen of uit strafbare feiten verkregen of te verkrijgen voordelen te benutten. Voor het uitvoeren van deze toets wordt onder meer de organisatiestructuur en de verbanden met andere rechtspersonen onderzocht. Daarom is in dit besluit bepaald dat van een aanvrager wordt gevraagd om daarover documentatie aan te leveren.

Bij ministeriële regeling worden nadere eisen gesteld waaraan een middel moet voldoen om te worden erkend. Die eisen kunnen tot gevolg hebben dat voor de toetsing aan die eisen nadere documentatie nodig is. Daarom maakt dit besluit het mogelijk om bij ministeriële regeling aanvullende eisen te stellen aan de inhoud van een aanvraag.

6. Eisen aan de houder van een erkenning

Aan de houder van een erkenning worden ook gedurende de looptijd van de erkenning eisen gesteld om het belang van veilige, betrouwbare en gebruiksvriendelijke identificatie te borgen. Aan

[10] Artikel 3:9 van de Algemene wet bestuursrecht.

deze eisen vindt toetsing plaats door de toezichthouder. In het hiernavolgende wordt op een aantal van die eisen ingegaan. Bij overtreding daarvan kan worden overgegaan tot het opleggen van een bestuurlijke boete of het intrekken of opschorten van de erkenning.

6.1 Vertrouwelijk omgaan met gegevens

Van belang is dat bedrijven die authenticatie verzorgen alle gegevens die hen ter kennis komen vertrouwelijk behandelen. Een betrouwbare toegang van burgers tot elektronische dienstverlening valt of staat immers met een organisatie die de haar ter beschikking staande gegevens van derden vertrouwelijk behandelt. Dit houdt onder meer in dat toegang tot de gegevens beperkt is tot daartoe gerechtigde personen en dat er technische en organisatorische beveiligingsmaatregelen zijn genomen. Dit besluit regelt ook dat gegevens die zijn verkregen in het kader van het aanbieden en het gebruik van een identificatiemiddel niet voor andere doeleinden mogen worden gebruikt dan voor identificatie. Dat geldt onverminderd wanneer de gebruiker toestemming verleent. Deze eis wordt gesteld om te borgen dat gegevens die burgers verstrekken of die over burgers worden verzameld in het kader van toegang kunnen krijgen tot dienstverlening door de overheid niet commercieel worden gebruikt.

6.2 Eisen voor verlening blijven van toepassing

Verder moet een houder van een erkenning blijven voldoen aan de eisen die gelden voor verlening van een erkenning aan het desbetreffende identificatiemiddel. Wanneer deze eisen wijzigen moeten houders van een erkenning derhalve vanaf het moment van wijziging aan die eisen voldoen. Uiteraard worden deze wijziging op bekendgemaakt op de wijze die voor regelgeving gebruikelijk is. Tevens vindt overeenkomstig het kabinetsbeleid consultatie van belanghebbenden plaats.

Evenals bij de verlening van een erkenning is het aan de houder van de erkenning om te onderbouwen dat aan deze eisen wordt voldaan. Daarvoor moet de houder in ieder geval beschikken over een geldige verklaring van certificering die niet ouder is dan drie jaar. Op deze verklaring is uitgebreid ingegaan in paragraaf 5.2 van deze toelichting.

6.3 Leveringsplicht en beschikbaarheid

Verder geldt voor houders van een erkenning een leveringsplicht, die inhoudt dat een houder van een erkenning het middel ook daadwerkelijk zal moeten gaan aanbieden nadat de erkenning van kracht is geworden. Verder moet de houder van een erkenning zorgen dat het middel ten minste voldoet aan een door de Minister van Binnenlandse Zaken en Koninkrijksrelaties vastgestelde beschikbaarheidsnorm. Burgers moeten in voldoende mate toegang kunnen krijgen tot publieke digitale dienstverlening. Daarvoor is het identificatie met een identificatiemiddel onmisbaar. Wanneer een burger heeft gekozen voor een bepaald identificatiemiddel moet dat middel vervolgens in voldoende mate beschikbaar zijn. Het is derhalve niet acceptabel als een middel

veelvuldig gedurende lange tijd niet beschikbaar is. Wanneer een dergelijke regel wordt gesteld is het op grond van de wettelijke systematiek mogelijk om op te treden, bijvoorbeeld door een erkenning in te trekken of een bestuurlijke boete op te leggen.

6.4 Meldingsplicht

De digitale wereld en daarin gebruikte methoden en standaarden zijn voortdurend in beweging. Dat geldt zowel voor beschermende technieken als veranderende dreigingen. Een houder van een erkenning zal het middel dan ook regelmatig moeten aanpassen om te zorgen dat het veilig kan blijven werken. Buiten deze noodzakelijke aanpassingen kan de houder van een erkenning er ook eigenstandig voor kiezen om de werking van het middel of de processen die daarmee verband houden te wijzigen. Deze wijzigingen kunnen een wezenlijke invloed hebben op de veiligheid, de betrouwbaarheid en de gebruiksvriendelijkheid van het middel. Omdat de erkenning is verleend op basis van de aanvraag kan een wijziging ertoe leiden dat de erkenning niet meer geldt voor het middel. Dat is het geval als de wijzigingen niet van ondergeschikte aard zijn. In dat geval is het aan de houder van een erkenning om een wijziging van die erkenning aan te vragen. Om te voorkomen dat de minister van Binnenlandse Zaken en Koninkrijksrelaties en de aangewezen toezichthouder een informatieachterstand oplopen waardoor een situatie ontstaat die niet meer kan worden rechtgezet, moeten wijzigingen van enige omvang actief worden gemeld. Daarom is in dit besluit geregeld dat wijzigingen moeten worden gemeld voor zover deze zouden hebben geleid tot een andere aanvraag. Een houder van een erkenning zal dus bij het doorvoeren van een wijziging moeten nagaan of de inhoud van de aanvraag voor de verkregen erkenning anders was geweest wanneer de desbetreffende wijziging voor de aanvraag was doorgevoerd. Dit besluit biedt een mogelijkheid om bij ministeriële regeling nadere regels te stellen over deze verplichting, bijvoorbeeld om onduidelijkheid te voorkomen.

Verder is aan een erkenning de verplichting verbonden om incidenten te melden, indien door die incidenten de veilige en betrouwbare toegang op significante wijze in het geding is of dreigt te komen.

6.5 Nadere regels bij ministeriele regeling

Dit besluit biedt de mogelijkheid om bij ministeriële regeling nadere verplichtingen op te leggen aan de houder van een erkenning. Het gaat om verplichtingen die op een hoger detailniveau invulling geven aan het belang van veilige, betrouwbare en gebruiksvriendelijke identificatie door burgers. Aan een houder van een erkenning kunnen op grond van artikel 26, eerste lid, bijvoorbeeld de volgende aanvullende eisen worden gesteld:

- Het bereikbaar zijn voor gebruikers, waardoor deze terecht kunnen als het door hen gebruikte middel niet werkt (onderdeel a). Gelet op het belang van toegang is het nodig dat burgers met problemen worden geholpen bij het oplossen daarvan.
- Het treffen van organisatorische waarborgen ter bescherming van gegevens van gebruikers (onderdeel b). In paragraaf 6.1 is uiteengezet dat aan een houder van een

erkenning eisen worden gesteld met betrekking tot de betrouwbare behandeling van gegevens. Bij ministeriële regeling kunnen aanvullende eisen worden gesteld.
- Een inzagemogelijkheid voor bepaalde gegevens (onderdeel c). Gegevens van gebruikers kunnen bijvoorbeeld noodzakelijk zijn in het kader van het afhandelen van geschillen.
- Een verplichting om gebruikers binnen een bepaalde termijn of op een specifieke wijze te informeren wanneer het middel door onderhoudswerkzaamheden niet beschikbaar zal zijn (onderdeel e).
- Een verplichting om bereikbaar te zijn voor medewerkers van dienstverleners of beheerders van de GDI (onderdeel f).

6.6 Heffingen

Op grond van artikel 22 van de wet kunnen heffingen in rekening worden gebracht voor het behandelen van een erkenningsaanvraag en voor het toezicht dat wordt gehouden op toegelaten partijen. In een separate AMvB is vastgelegd dat een dergelijke heffing voor toelating en toezicht verschuldigd is en zijn de hoofdelementen voor de berekenings- en inningswijze bepaald.

7. Wijziging, schorsing en intrekking

De wet maakt het wijzigen, schorsen of intrekken van een erkenning mogelijk. Deze bevoegdheden kunnen worden ingezet indien wordt vastgesteld dat een houder van een erkenning niet voldoet aan de voor hem geldende eisen. Tevens kan een houder van een erkenning verzoeken om wijziging daarvan. Op grond van het negende lid van artikel 9 van de wet kunnen over deze onderwerpen nadere regels worden gesteld. Dit besluit bevat regels over het op verzoek wijzigen van een erkenning.

Over de ambtshalve inzet van deze bevoegdheden in het kader van toezicht en handhaving worden in dit besluit geen nadere regels gesteld. Gebruik van deze bevoegdheden zal plaatsvinden met inachtneming van de omstandigheden van het geval en binnen de kaders van de algemene beginselen van behoorlijk bestuur.

7.1 Wijzigen erkenning op verzoek, algemeen

Beëindiging van een erkenning op aanvraag of anderszins is mogelijk op grond van de wet. In het geval van beëindiging op aanvraag is het wenselijk nadere regels te stellen over het proces. Dit besluit bevat die regels.

Een houder van een erkenning kan een verzoek indienen tot wijziging van een aan hem verleende erkenning. Een dergelijke wijziging is bijvoorbeeld nodig indien in de werking van het middel zodanige wijzigingen worden aangebracht dat de erkenning niet meer kan worden geacht te zijn verleend voor het gewijzigde middel. Een aanvraag om een wijziging wordt getoetst aan de eisen die ook gelden voor het middel gelden bij het verlenen van de erkenning. Deze toets houdt in dat de wijzigingen die in de werking van het middel worden aangebracht, worden getoetst op

conformiteit met de verleningscriteria. Er wordt dus niet getoetst of is voldaan aan de eisen die worden gesteld aan de aanvrager. Dat komt de efficiënte inzet van beschikbare uitvoeringscapaciteit ten goede.

7.2 Beëindiging erkenning op verzoek van de houder

Een houder van een erkenning is gehouden het middel daadwerkelijk aan te bieden en te borgen dat het middel beschikbaar is voor gebruikers. Op die verplichtingen is nader ingegaan in de paragrafen 6.3 van deze toelichting. Deze verplichtingen gelden zolang de erkenning geldt. Een houder van een erkenning die het middel niet langer wil blijven aanbieden zal daarom om beëindiging van de erkenning moeten verzoeken. Een dergelijke beëindiging heeft gevolgen voor gebruikers. Daarom wordt met dit besluit vastgelegd dat de beëindigingsprocedure de noodzakelijke waarborgen heeft om te zorgen dat burgers voldoende tijdig op de hoogte worden gebracht en dat hun gegevens waar nodig beschikbaar blijven zonder afbreuk te doen aan de veiligheidseisen die daarmee gepaard gaan.

Een houder van een erkenning zal in een aanvraag om beëindiging moeten aangeven wat hij een redelijke termijn voor beëindiging vindt. Daarbij wordt hij geacht rekening te houden met de noodzaak om gebruikers te informeren en informatie elders onder te brengen. Dit voorstel wordt getoetst. Als op de aanvraag positief kan worden beslist, wordt een moment bepaald waarop de houder niet meer gebonden is aan de leveringsplicht. Dat is het moment waarop de intrekking van de erkenning van kracht wordt. De minister van Binnenlandse Zaken en Koninkrijksrelaties bepaalt dit moment en houdt daarbij rekening met het voorstel van de aanvrager.

Verder wordt aan de houder van de erkenning door middel van een voorschrift een verplichting opgelegd om de gegevens voor een bepaald moment over te dragen overeenkomstig het voorstel. De daadwerkelijke einddatum van de erkenning wordt bepaald op een zodanig moment dat kan worden getoetst of de houder aan zijn verplichtingen heeft voldaan. Deze datum moet tevens ruimte bieden om eventueel handhavend op te treden.

8. Toezicht en handhaving

Agentschap Telecom (hierna: AT) houdt toezicht op de naleving onder meer artikel 9 van de Wet digitale overheid. Op grond van dat artikel worden identificatiemiddelen toegelaten tot het Nederlandse stelsel. Daarbij kan het agentschap de bevoegdheden toepassen die op grond van hoofdstuk 5 van de Algemene wet bestuursrecht aan toezichthouders ter beschikking staan.

Deze bevoegdheden kunnen slechts in Nederland worden toegepast. Toezicht op bedrijven zonder vestiging in Nederland is derhalve niet effectief. Daarom wordt met dit besluit geregeld dat een aanvrager een vestiging in Nederland moet hebben. De toezichthouder kan bij deze vestiging bijvoorbeeld inzicht vragen in processen of documenten.

In dat verband heeft het AT een uitvoerings- en handhavingstoets verricht. Naar aanleiding van die toets adviseert het AT om de eisen voor identificatiemiddelen zoveel mogelijk gelijk te trekken met de eisen voor bedrijfs- en organisatiemiddelen en daarover in overleg te treden met AT. In reactie daarop wordt het volgende gemeld. De wet bevat twee verschillende regimes voor identificatiemiddelen voor natuurlijke personen enerzijds en voor bedrijven en organisaties anderzijds. In het kader van de plenaire behandeling van de wet is aangekondigd dat de twee regimes worden samengevoegd. Tot dat moment wordt getracht zoveel mogelijk dezelfde eisen te hanteren, voor zover dat in deze fase en context efficiënt is. Bij het opstellen van de eisen wordt uiteraard overlegd met het AT.

Het AT geeft verder aan dat het noodzakelijk is om, naast de gevraagde ISO-27001 certificering, aanvullende bewijsstukken te vragen op basis waarvan de conformiteit van een aanvraag kan worden beoordeeld. Dit besluit bevat een grondslag om bij ministeriële regeling te regelen dat aanvullende bewijsstukken bij een aanvraag moeten worden gevoegd.

In de uitvoerings- en handhavingstoets wordt verder ingegaan op de ambtshalve verlening van een aanwijzing voor een publiek identificatiemiddel. Zoals door het AT wordt aangegeven kan een publiek middel inderdaad pas worden aangegeven wanneer is gebleken en kan worden gemotiveerd dat aan alle eisen is voldaan. Het is aan de minister van Binnenlandse Zaken om dat aan te tonen.

9. Regeldruk en administratieve lasten

9.1 Kosten voor het indienen van een aanvraag en voor houders van een erkenning

Het indienen van een aanvraag vergt een investering, zowel in tijd als financieel. Voor zover de kosten voorvloeien uit dit besluit is gepoogd deze zo laag mogelijk te houden. Een aanvrager en een houder van een erkenning moet beschikken over een geldig certificaat. De inhoud van dat certificaat wordt bij ministeriële regeling vastgesteld. In dit besluit wordt vastgelegd dat een aanvrager op grond van ISO 27001 gecertificeerd moet zijn.

De kosten die een private partij moet maken om erkend te worden bestaan in ieder geval uit de kosten voor deze certificering. Het vereiste certificaat wordt op grond van een audit door een geaccrediteerde auditpartij afgegeven. Die auditpartij doet dit in opdracht en op kosten van de partij die zijn diensten wil laten erkennen. De kosten van een audit bestaan uit de kosten van de uitvoering van de audit en de kosten van de partij die erkend wil worden voor de voorbereiding van de audit. Deze voorbereidingskosten zijn voor de eerste keer dat de audit wordt uitgevoerd een factor 2 tot 4 hoger dan voor de jaarlijkse herhaalaudits omdat voor de eerste audit het bewijs dat aan de eisen wordt voldaan en het ophalen van de daarvoor benodigde informatie voor het eerst moet worden gestructureerd. Het ervaringsniveau van de te erkennen partij ten aanzien van het ondergaan van audits en de voorbereiding daarop is in dit kader bepalend voor de omvang van de benodigde voorbereiding.

Verder zal een aanvrager moeten voldoen aan de eisen die op grond van dit besluit bij ministeriële regeling worden gesteld. In de toelichting bij die ministeriële regeling wordt ingegaan of de effecten van die eisen op de regeldruk.

Tot slot zal een te erkennen aanbieder van een identificatiemiddel in het kader van de productie van bewijs, dat aan specifieke eisen moet worden voldaan, een technische beveiligingstest moeten uitvoeren en deze driejaarlijks moet herhalen. Deze audit vloeit voort uit de eisen van de eIDAS-uitvoeringsverordening, die met dit besluit van toepassing worden verklaard. Deze audit wordt beschouwd als normale 'productiekosten' van een dienst, de kosten daarvan worden in dit kader niet beschouwd als 'additioneel' ten gevolge van deze regelgeving. Naar schatting zal een dergelijke test per identificatiemiddel en bijbehorend authenticatiemechanisme plusminus 25.000 euro bedragen al naar gelang de complexiteit van een middel en mechanisme. Hier geldt dat bij beperkte wijziging van een middel een herhaalde audit minder kosten met zich meebrengt dan bij een fundamentelere wijziging van middel en mechanisme.

De kosten van een erkenning zijn afhankelijk van:

- De specifieke infrastructuur van de erkende of te erkennen dienst of diensten;
- Het al dan niet reeds in bezit zijn van een certificering zoals ISO 27001;
- De complexiteit van het middel en het bijbehorende authenticatiemechanisme;
- De aard, omvang en frequentie van wijzigingen die in de tijd worden aangebracht aan het middel en het authenticatiemechanisme.

Een compleet beeld van de eisen waaraan een aanvrager of een erkende partij moet voldoen ontstaat in combinatie met de ministeriële regeling, waarin de meer gedetailleerde eisen voor deze partijen worden ingevuld.

9.2 Advies Adviescollege toetsing regeldruk

Een concept van dit besluit is voor advies voorgelegd aan het Adviescollege toetsing regeldruk. In het hiernavolgende wordt ingegaan op de punten uit het advies van dat college.

Ten eerste adviseert het college om duidelijk aan te geven of in de toekomst een publiek middel zal blijven bestaan en of dat kosteloos is. Naar aanleiding van dat advies is de toelichting uitgebreid. Hier wordt volstaan met de opmerking dat de wet de minister van Binnenlandse Zaken en Koninkrijksrelaties een wettelijke taak geeft om te zorgen dat er een publiek identificatiemiddel beschikbaar is op de verschillende betrouwbaarheidsniveaus. Daarbij is laagdrempelige toegang een uitgangspunt, ook vanuit financieel perspectief. Voor DigiD hoog is wel aangekondigd dat een beperkt bedrag zal moeten worden betaald voor het fysieke identificatiemiddel waarop dit wordt geplaatst.

Ten tweede wordt geadviseerd om toe te staan dat met een identificatiemiddel wordt ingelogd dat een hoger betrouwbaarheidsniveau heeft dan voor de desbetreffende publieke dienst is vereist. Dat is inderdaad mogelijk, en dat volgt uit de formulering van de relevante wetsartikelen. Daarin is

vermeld dat toegang wordt verleend met gebruik van een middel dat "ten minste" het vereiste betrouwbaarheidsniveau heeft.

Ten derde adviseert het adviescollege het aantal private aanbieders en het aantal contractsvormen te limiteren of in de toelichting te motiveren waarom daarvoor niet is gekozen. In dit besluit is niet gekozen voor een beperkt aantal aanbieders of een beperking van de mogelijkheden om verschillende contractsvormen aan te bieden. Het aanbieden van een publiek middel is een wettelijke taak van de minister van Binnenlandse Zaken en koninkrijksrelaties. De voorwaarden waaronder dat publieke middel kan worden gebruikt worden door de minister bepaald. Daarbij zijn overzichtelijkheid en gebruiksgemak bepalend. In dit context acht het kabinet een systeem met schaarse erkenningen en een beperking van bedrijven om het verdienmodel te bepalen niet evenredig.

Ten vierde wordt geadviseerd om de wijze waarop burgers kunnen inloggen met een authenticatiemiddel per betrouwbaarheidsniveau te uniformeren. Hieraan wordt gehoor gegeven door het aanbod van middelen in het Nederlandse stelsel uniform te presenteren. Bij het inloggen wordt een gebruiker de keuze geboden tussen de verschillende identificatiemiddelen die zijn toegelaten tot het stelsel. Dit proces wordt voor alle middelen uniform ingericht. Daarna zal de gebruikers zijn middel moeten gebruiken, waardoor er onvermijdelijk verschillen optreden. Een middel dat werkt met het uitlezen van een identificatiedocument wordt immers anders gebruikt dan een middel dat bijvoorbeeld een vingerafdruk gebruikt. Deze beide processen passen in beginsel in de eIDAS-systematiek en deze ruimte voor verschillen is wenselijk.

Als laatste adviseert het Adviescollege toetsing regeldruk om een grondslag op te nemen om eisen te kunnen stellen aan het gebruiksgemak voor burgers van een middel. Daaraan is gehoor gegeven en het besluit is hierop aangepast. Hierop is in paragraaf 3.7 van deze toelichting ingegaan.

10. Advies Autoriteit Persoonsgegevens

Bij brief van 6 augustus 2020 heeft de Autoriteit persoonsgegevens een advies uitgebracht over een concept van dit besluit. Daarin wordt geadviseerd te onderzoeken of het wenselijk en haalbaar is om naast ISO 27001 ook ISO 27701 of een vergelijkbaar aantoonbaar beschermingsniveau verplicht te stellen.

Naar aanleiding van dit advies is onderzocht of het wenselijk is een dergelijke certificering voor te schrijven. Inhoudelijk sluit deze certificering aan bij de beleidsmatige wensen ten aanzien van het veilig en betrouwbaar inloggen bij overheidsdiensten. Het verkrijgen van een dergelijke certificering brengt ongeveer een verdubbeling van de certificeringskosten met zich, terwijl van partijen al zal worden gevraagd dat zij tijdens het aanvraagproces voor een erkenning op andere wijze aantonen dat zij de noodzakelijke randvoorwaarden zijn geborgd ten aanzien van management van privacygevoelige gegevens. Daarom is ervoor gekozen om de norm ISO 27701 niet te verplichten voor deze partijen.

11. Consultatie

Dit besluit is vanaf 1 april tot en met 13 mei 2020 voor reacties openbaar gemaakt op internetconsultatie.nl. Daarop zijn in totaal 13 reacties binnengekomen. Verschillende van deze reacties zien op de verhouding van het Nederlandse stelsel, waarop dit besluit ziet, tot stelsels in andere EU-lidstaten. Als gevolg van deze opmerkingen zijn de paragrafen 2.3 en 3.3 van deze toelichting aangevuld. Daarin wordt uitgebreid ingegaan op dit onderwerp. Ook naar aanleiding van opmerkingen over de mogelijkheid om middelen met een decentrale architectuur te erkennen en het verplichtstellen van open source is de toelichting uitgebreid.

Meerdere opmerkingen gaan in op artikel 3, eerste lid, onderdeel e, dat ziet op het verplicht scheiden van gegevens. Die opmerkingen hebben geleid tot het aanpassen van het artikelonderdeel en de daarbij behorende toelichting.

Een van de respondenten geeft aan dat het, behalve de erkenning van soorten middelen ook mogelijk moet zijn om stelsels te erkennen. Daarmee wordt gedoeld op een wettelijke goedkeuring waarbij wordt bewerkstelligd dat alle middelen die door een groep samenwerkende partijen wordt uitgegeven wordt geaccepteerd voor overheidsdienstverlening. Artikel 9 van de wet, maakt slechts het erkennen van soorten middelen mogelijk en koppelt deze aan toetsing van onderneming die deze uitgeeft. Een erkenning wordt verleend aan de aanvrager daarvan en anderen dan de houder van de erkenning kunnen daarvan geen gebruik maken. Daarvan kan met dit besluit niet worden afgeweken. Deze constructie maakt het wel mogelijk dat een erkenninghouder onderaannemers gebruikt voor de uitvoering van bepaalde werkzaamheden. Bij de aanvraag moet worden aangegeven of daarvan sprake is en eventuele wijzigingen moeten worden doorgegeven.

Verder wordt in een aantal reacties gesteld dat het wenselijk is dat de broncode van erkende identificatiemiddelen inzichtelijk moet zijn voor gebruikers. Dit besluit bevat de hoofdelementen voor een toetsingssysteem voor open source. Op dit onderwerp is in paragraaf 3.2.3 uitgebreid ingegaan.

Een respondent stelt voor slechts het betrouwbaarheidsniveau hoog te hanteren en daarmee een vereenvoudiging van het systeem te bewerkstelligen. Dat komt niet overeen met de keuzevrijheid die voor gebruikers wenselijk is en zal voor sommige gebruikers een lastenverzwaring tot gevolg hebben omdat middelen met niveau hoog doorgaans duurder zijn dan op niveau substantieel. De eIDAS verordening maakt het ook om deze redenen mogelijk om te differentiëren, zodat kosten efficiënte beveiliging kan worden ingezet.

Een respondent stelt dat voorkeur zou moeten worden gegeven aan aanvragers van een erkenning die zonder winstoogmerk opereren. Omdat het aantal erkenningen niet in aantal is beperkt is het verlenen van voorrang aan bepaalde aanvragers niet aan de orde. Het feit dat private partijen winst maken met het aanbieden van authenticatiedienstverlening is niet ten principale onwenselijk. Voorkomen moet worden dat gegevens van burgers die inloggen bij de overheid als handelswaar worden gebruikt door deze partijen. Daarvoor bevat het besluit de nodige waarborgen. Het zou disproportioneel zijn om vervolgens partijen met een winstoogmerk uit te sluiten van het

verkrijgen van een erkenning. Bovendien worden gebruikers daarmee mogelijk goede oplossingen of alternatieven onthouden.

In een van de ingediende reacties wordt verder voorgesteld om bij het hanteren van doelvoorschriften in de vorm van open normen richtlijnen openbaar te maken over de wijze waarop aan die open normen kan worden voldaan. Deze suggestie is overgenomen en daarop wordt in paragraaf 3.12 ingegaan.

Voor zover in de reacties wordt ingegaan op nadere eisen die op basis van dit besluit bij ministeriële regeling kunnen worden gesteld wordt daarop in deze toelichting niet nader ingegaan. Aan deze onderwerpen zal in de toelichting bij de regeling aandacht worden besteed.

Artikelsgewijze toelichting

Artikel 3

Eerste lid

In dit eisen zijn eisen opgenomen die zijn gericht op de aanvrager. Die eisen zien bijvoorbeeld op de wijze waarop de aanvrager processen heeft ingericht of de financiële positie van de aanvrager.

De organisatie van de aanvrager moet de eisen die aan gelaten partijen worden gesteld kunnen uitvoeren. Dat principe is vastgelegd in onderdeel d van dit artikellid. Het gaat niet om het voldoen aan eisen voor toelating, maar om het kunnen voldoen aan eisen dus vanaf het moment van toelating van kracht worden. Gedacht kan bijvoorbeeld worden aan de eisen met betrekking tot beschikbaarheid, waaraan moet worden voldaan door erkende partijen. Een aanvraag van een partij die onvoldoende voorzieningen heeft getroffen om aan die eisen te voldoen, kan worden afgewezen.

Onderdeel e bevat de verplichting om gegevens over gebruikers en gebruik gescheiden te bewaren. Hierop wordt in paragraaf 4.1.3 uitgebreid ingegaan. Het gaat om gegevens die in het kader van de erkenning zijn verkregen. De verplichting geldt derhalve niet voor gegevens die voorafgaand aan de erkenning zijn verkregen, of die na het van kracht worden daarvan door de houder van de erkenning zijn verwerkt voor een ander doel dan authenticatie bij publieke dienstverleners. Als gevolg van dit onderdeel kan een aanvraag worden afgewezen indien de aanvrager niet kan aantonen dat de gegevens over de gebruiker worden bewaard op zodanige wijze dat deze niet zijn te herleiden tot de gegevens over het gebruik door die gebruiker.

Met onderdeel f wordt voorgeschreven dat moet worden geregistreerd op welk moment en door wie gegevens over gebruiker en gebruik zijn gecombineerd. Dit voorschrift maakt het mogelijk om maatregelen te nemen tegen onbevoegde inzage in gebruiksgegevens. Verder maakt dit onderdeel het mogelijk om gebruikers inzage te geven in de momenten waarop de gegevens zijn gecombineerd. Daardoor kunnen gebruikers zelf controle uitoefenen op de momenten waarop gegevens zijn gecombineerd.

Onderdeel g van het eerste lid schrijft voor dat een aanvrager een vestiging moet hebben in Nederland. Niet vereist is dat de rechtspersoon in Nederland is gevestigd, maar om effectief toezicht mogelijk te maken moet de toezichthouder bij een Nederlandse vestiging inzicht kunnen krijgen in de vereiste gegevens en processen. Een dergelijke eis is niet verboden in artikel 14 van de Europese dienstenrichtlijn.

In onderdeel i is geregeld dat gebruikers inzage krijgen in de authenticatiehandelingen die met een middel zijn verricht en de momenten waarop persoonsgegevens over de gebruiker zijn gecombineerd met de gegevens over het gebruik door die gebruiker. Op dit eis is in paragraaf 4.1.3 van deze toelichting uitgebreid ingegaan.

Derde lid

Een aanvraag kan worden ingediend door een partij die een deel van de werkzaamheden uitbesteed aan een derde partij. Een dergelijke derde partij moet ook voldoen aan de eisen in het eerste lid, met uitzondering van de eisen met betrekking tot de financiële positie.

Artikel 4

Een identificatiemiddel werkt samen met verschillende onderdelen van het stelsel, zoals publieke ontsluitende diensten, het BSN-koppelregister en voorzieningen die gebruik in andere lidstaten mogelijk maken. In artikel 4, aanhef en onderdeel a is de eis vervat dat een middel moet kunnen functioneren met de onderdelen die nodig zijn voor het functioneren daarvan. In het aanvraagproces wordt dit getoetst door middel van een uitvoerige praktijktoets waarover bij ministeriële regeling nadere regels worden gesteld.

Onderdeel b, regelt dat een identificatiemiddel moet kunnen functioneren in overeenstemming met de relevante verplichtingen uit het Besluit digitale overheid. Deze verplichtingen gelden uiteraard zelfstandig op grond van het Besluit digitale overheid, maar niet als afwijzingscriterium voor een aanvraag. Met dit onderdeel is geborgd dat een aanvraag kan worden afgewezen wanneer die artikelen niet kunnen worden nageleefd.

Onderdeel c van dit artikel bepaalt dat een identificatiemiddel moet voldoen aan de eisen die gelden voor wederzijdse erkenning op grond van de Europese eIDAS-systematiek. In paragraaf 4.1.2 van deze toelichting wordt hierop uitgebreider ingegaan.

Artikel 5 en 6

Deze artikelen zijn een uitwerking van de artikelen 9, zesde lid, onderdeel b en d, van de wet. In paragraaf 3.2 van het algemene deel van deze toelichting wordt de inhoud van deze artikelen uiteengezet.

Artikel 7

Eerste lid

Artikel 5 biedt een basis om nadere eisen te stellen aan een middel en de aanbieder daarvan. De onderdelen a tot en met h van het eerste lid maken het mogelijk om eisen te stellen met betrekking tot de onderwerpen waarop het Europese eIDAS-regelgevingscomplex ziet. Daartoe zijn in deze onderdelen de onderwerpen gehanteerd uit de bijlage bij eIDAS-uitvoeringsverordening 1502. Een uitzondering is het begrip "intrekking" in onderdeel e, dat beter aansluit bij het woordgebruik in de praktijk dan het in de verordening gebruikte "herroeping".

Tweede lid

In paragraaf 4.1.4 van het algemene deel van deze toelichting is ingegaan op artikel 5, tweede lid.

Artikel 9

Een aanvraag kan op grond van artikel 7 slechts worden ingediend door een rechtspersoon of andere onderneming naar Nederlands recht of naar het recht van een andere EU-lidstaat. Daarmee wordt voorkomen dat de integriteitstoetsing onmogelijk wordt. Als een aanvraag wordt ingediend door een natuurlijke persoon wordt deze op grond van artikel 4:5 van de Algemene wet bestuursrecht niet in behandeling genomen.

Artikel 10

Eerste lid

Artikel 9, vijfde lid van de wet bepaalt dat een aanvraag voor een erkenning vergezeld moet gaan van een certificeringsverklaring. Op grond van het achtste lid van dat artikel kunnen bij of krachtens algemene maatregel van bestuur nadere eisen worden gesteld over de aanvraag. Met dit artikel wordt daaraan invulling gegeven. Het is aan een aanvrager om aan te tonen dat wordt voldaan aan alle toelatingseisen. Voor zover die eisen volgen uit dit besluit bevat artikel 10, eerste lid, van dit besluit de stukken die ter onderbouwing moeten worden ingediend.

Tweede lid

Bij ministeriële regeling worden, op grond van artikel 7 van dit besluit, nadere toelatingseisen gesteld. Voor die eisen worden de stukken die ter onderbouwing moeten worden ingediend ook bij ministeriële regeling vastgesteld. Het tweede lid biedt daarvoor een basis. Te denken valt aan het voorschrijven van specifieke documenten, zoals een bankverklaring of een afschrift van een aansprakelijkheidsverzekeraar. Ook kunnen bij ministeriële regeling bijvoorbeeld regels worden gesteld aangaande de actualiteit van te overleggen gegevens, of kan juist worden bepaald dat in sommige situaties bepaalde bewijsstukken niet overgelegd hoeven te worden.

Verder kan op grond van het tweede lid onder meer het gebruik van een aanvraagformulier worden verplicht.

Artikel 12

Op grond van artikel 9, vijfde lid, van de wet moet bij een aanvraag voor erkenning een verklaring worden gevoegd van een geaccrediteerde certificerende instelling. In dit artikel worden eisen gesteld aan de inhoud van die verklaring en aan de instelling die deze afgeeft.

Tweede lid

In paragraaf 5.2 van het algemene deel van deze toelichting is uiteengezet welke eisen worden gesteld aan de instelling die de in artikel 9, vijfde lid, van de wet bedoelde verklaring heeft afgegeven. In dit verband wordt verstaan met een verwijzing naar die paragraaf.

Derde lid

Certificering op grond van bijvoorbeeld ISO 27001 ziet op algemene aspecten van gegevensbeveiliging. Daarom schrijft artikel 9, derde lid, van dit besluit specifiek voor dat een certificeringsverklaring moet zien op de processen die samenhangen met de werking van het identificatiemiddel.

Vierde lid

Met een verklaring van een certificerende instelling wordt doorgaans enkel vastgesteld dat aan de relevante eisen is voldaan. In het kader van besluitvorming op een aanvraag is dat onvoldoende. Als onderdeel van de verklaring wordt daarom een rapportage gevraagd waaruit kan worden opgemaakt welke onvolkomenheden zijn geconstateerd en op welke wijze deze zijn aangepast. Het betreft een rapportage die standaard wordt opgemaakt door de certificerende instelling.

Artikel 13

Het tweede lid van dit artikel bepaalt dat een erkenning persoonsgebonden is. Als uit toetsing is gebleken dat de aanvrager voldoet aan de gestelde eisen wordt de erkenning verleend aan de aanvrager. Op grond van artikel 3:83, derde lid, van het Burgerlijk Wetboek is een erkenning niet overdraagbaar.

Artikel 14

In paragraaf 3.13 is uiteengezet dat de erkenning waarop dit besluit ziet een vergunning is in de zin van de Dienstenrichtlijn. Op grond van artikel 28 van de Dienstenwet wordt een dergelijke vergunning na het verstrijken van de beslistermijn in beginsel verleend, tenzij bij wettelijk voorschrift anders is bepaald.

Deze regel zou zonder nadere regeling ook gelden voor de erkenning van een privaat identificatiemiddel voor natuurlijke personen. Met het uitvoeren van een beoordeling van een identificatiemiddel voor natuurlijke personen worden burgers beschermd. Met het van rechtswege verlenen van de erkenning, zonder die beoordeling, wordt dit belang op onaanvaardbare wijze geschaad. Daarom wordt met artikel 14 geregeld dat de vergunning niet van rechtswege wordt verleend.

Artikel 16

Het eerste lid van artikel 16 bepaalt dat een erkenning voor onbepaalde tijd wordt verleend. Verlening voor onbepaalde tijd is het uitgangspunt in gevallen waarin geen sprake is van schaarste.

Op grond van het tweede lid wordt bij het vaststellen van de ingangsdatum rekening gehouden met de handeling die nodig zijn om te zorgen dat het middel kan worden geaccepteerd. Een erkend middel moet worden geaccepteerd door een groot aantal publieke dienstverleners met een verschillende technische inrichting. Voorkomen moet worden dat een houder van een erkenning moet wachten voordat van die erkenning gebruik kan worden gemaakt omdat een publieke dienstverlener of een beperkt deel daarvan een langere implementatieperiode nodig heeft. Dit kan worden voorkomen door aan de erkenning een tijdelijke beperking te verbinden. Artikel 9, vierde lid, van de wet biedt daarvoor een mogelijkheid.

Artikel 17

Een houder van een erkenning en de door die partij ingeschakelde derde moet ook na het verlenen van de erkenning blijven voldoen aan de erkenningseisen. Dat principe is vastgelegd in het eerste lid van artikel 17. Wanneer de toelatingseisen worden gewijzigd zullen ook toegelaten partijen aan de nieuwe eisen moeten voldoen, omdat het hanteren van verschillende regimes binnen een stelsel niet werkbaar is. Wel zal het veelal redelijk zijn om tijdelijk voor reeds toegelaten partijen de eerder geldende norm te blijven hanteren. Het tweede lid van artikel 17 maakt dat mogelijk.

Artikel 18

Op grond van artikel 18 is een houder van een erkenning gehouden om een beschrijving openbaar te maken van de dienstverlening die met de erkenning aan gebruikers wordt aangeboden en waarmee duidelijk wordt gemaakt welke keuzes zijn gemaakt ten aanzien van het gebruik van software met een open source-licentie. Op deze verplichting wordt ingegaan in paragraaf 3.2.3 van

het algemene deel van deze toelichting in samenhang met de overige verplichtingen die zien op het gebruik van open source- software.

Artikel 21 Auditverplichting voor houder van een erkenning

Dit artikel maakt het mogelijk dat de minister aan een erkende partij een verplichting oplegt om een externe audit te laten uitvoeren. Met die audit geeft een onafhankelijke deskundige een oordeel over de conformiteit van een erkende partij met de eisen die voor die partij gelden. Daarbij kan het ook specifiek gaan over een boekhoudkundig onderzoek om te bepalen of sprake is geweest van overtreding van het verbod om persoonsgegevens te gebruiken voor een ander doel dan authenticatie.

Bij het opleggen van een onderzoeksverplichting zal telkens rekening moeten worden gehouden met de kosten die het uitvoeren van een degelijke audit met zich brengt en moet een afweging worden gemaakt tussen die kosten en de efficiënte inzet van toezichtscapaciteit en bij de toezichthouder beschikbare kennis.

Artikel 22

Artikel 9, vierde lid, van de wet bepaalt dat aan de houder van een erkenning eisen worden gesteld, waaronder in ieder geval regels over een leveringsplicht. Met eerste tot en met het derde lid van artikel 22 wordt deze leveringsplicht uitgewerkt. Een identificatiemiddel moet na verlening van een erkenning daadwerkelijk worden aangeboden, als gevolg van het eerste lid. Verder moet een middel daadwerkelijk beschikbaar zijn voor gebruikers. Daarom moeten houders van een erkenning voldoen aan een beschikbaarheidsnorm, die bij ministeriële regeling wordt vastgelegd. Te denken valt aan een percentage van de tijd waarin het middel ononderbroken moet functioneren. Omdat er geen bestaande praktijk is met ervaring over de te hanteren norm, wordt dat percentage bij ministeriële regeling vastgesteld. Het is denkbaar dat een onderscheid tussen verschillende soorten identificatiemiddelen wenselijk is. Dit artikellid biedt daarvoor de ruimte. Op grond van het derde lid kan worden geregeld op welke wordt gemeten of aan de verplichting is voldaan.

Artikel 23

Dit artikel regelt de meldingsplicht voor houders van een erkenning. Daarop is in paragraaf 6.4 van deze toelichting ingegaan. In dit verband wordt nog vermeld dat een houder van een erkenning op grond van het eerste lid, onderdeel c, gehouden is wijzigingen in de organisatie of de zeggenschap te melden. Dat maakt het mogelijk om ook na verlening van een erkenning een beoordeling te doen in het kader van de Wet bevordering integriteitsbeoordelingen door het openbaar bestuur. Op grond van artikel 9, zevende lid, van de wet kan een verleende erkenning

worden geschorst of ingetrokken als is gebleken dat ernstig gevaar bestaat dat de erkenning wordt gebruikt voor het plegen van strafbare feiten.

Artikel 24

Met dit artikel wordt geregeld dat een houder van een erkenning ervoor moet zorgen dat alle gegevens die bij de houder ter kennis komen, vertrouwelijk behandelt. Een betrouwbare toegang van natuurlijke personen tot elektronische dienstverlening valt of staat immers met een organisatie die de haar ter beschikking staande gegevens van derden vertrouwelijk behandelt. Dit houdt onder meer in dat toegang tot de gegevens beperkt is tot daartoe gerechtigde personen en dat er technische en organisatorische beveiligingsmaatregelen zijn genomen. Daarbij past tevens dat de houder beschikt over een loket waar betrokkenen in de toegang van elektronische dienstverlening aan ondernemingen en rechtspersonen terecht kunnen in geval van vragen of ontstane problemen in die toegang, bijvoorbeeld in het geval van security-meldingen. Die verplichting wordt uitgewerkt op grond van artikel 25, eerste lid, onderdeel a.

Artikel 24, onderdeel b, regelt dat gegevens die door een houder van een erkenning worden verwerkt niet voor andere doeleinden mogen worden gebruikt dan voor authenticatie in het kader van de erkenning, dus bij de publieke dienstverleners waarop de wet ziet. Artikel 6, eerste lid, onderdeel a, van de Algemene verordening gegevensbescherming kan niet worden toegepast om de gegevens toch voor deze doeleinden te gebruiken als de gebruiker daarvoor toestemming heeft verleend. Dit artikel staat er niet aan in de weg dat erkende private inlogmiddelen kunnen worden gebruikt in het commerciële domein.

Artikel 25

In paragraaf 6.6 is ingegaan op de noodzaak en de inhoud van dit artikel. Het betreft nadere eisen aan een houder van een erkenning, dus eisen waaraan een erkende private aanbieder van een identificatiemiddel moet voldoen. Het betreft eisen die naar hun aard en detailniveau vergelijkbaar zijn met de eisen, bedoeld in artikel 5. Daarom regelt dit besluit dat deze nadere eisen ook kunnen worden gesteld bij ministeriële regeling. De eisen die op grond van artikel 7 worden gesteld gelden ook voor de houder van een erkenning, door de koppelbepaling in artikel 17.

Artikel 27

Een erkenning kan worden gewijzigd, bijvoorbeeld wanneer de houder van een erkenning ingrijpende wijzigingen wil doorvoeren in de werking van het middel waarop de erkenning ziet. In dat geval zou de erkenning niet meer zien op het gewijzigde middel. Dit artikel regelt dat een wijziging wordt beoordeeld op wijze waarop een eerste aanvraag ook wordt behandeld.

Als gevolg van artikel 9 kan een aanvraag slechts worden ingediend door een onderneming binnen de Europese Unie of de Europese Economische zone. Het tweede lid regelt dat een erkenning door

middel van een wijziging niet kan worden overgezet naar een rechtspersoon buiten de Europese Unie of de Europese Economische Ruimte.

Artikel 28

Dit artikel regelt de wijze waarop wordt omgegaan met een verzoek om een verleende erkenning te beëindigen. Op dit onderwerp wordt in paragraaf 7.2 uitgebreid ingegaan.

Artikel 29

He belang van een stelsel voor veilige en betrouwbare identificatie is afhankelijk van alle deelnemers aan dat stelsel. Op grond van artikel 18, eerste en vierde lid, van de wet kan de minister ingrijpen indien er een ernstige storing of aantasting is van de veiligheid of betrouwbaarheid van het stelsel of wanneer wordt vermoed dat met erkende identificatiemiddelen misbruik wordt gepleegd of dat deze oneigenlijk worden gebruikt.

Verder wordt toezicht gehouden op de naleving van de aan erkende partijen opgelegde eisen. Dit toezicht kan afhankelijk zijn van volledige en tijdige medewerking van een erkende partij. Wanneer deze medewerking niet plaatsvindt kan de minister op grond van artikel 24a de aan die partij verleende erkenning intrekken of schorsen om het belang van veilig en betrouwbare toegang tot publieke dienstverlening te borgen.

Artikel 30

Artikel 9, zevende lid, van de wet bevat een grondslag om een erkenning te wijzigen, schorsen of in te trekken vanwege zwaarwegende redenen als bedoeld in artikel 9, zesde lid, van de wet. Niet is geregeld dat het Landelijk Bureau Bibob om een advies kan worden gevraagd, aangezien dat uitsluitend is geregeld voor de fase van aanvraag van een erkenning. Artikel 9, negende lid, van de wet biedt een delegatiegrondslag om nadere regels te stellen over de procedure van erkenning, wijziging, schorsing of intrekking. Op grond van dat lid wordt in dit artikel geregeld dat ook over wijziging, schorsing of intrekking van de erkenning advies kan worden gevraagd aan het Landelijk Bureau Bibob.

Artikel 31

Dit artikel ziet op de eisen die gelden voor een publiek middel. Voor een inhoudelijke uiteenzetting wordt verwezen naar paragraaf 4.2 van deze toelichting.