Staatsblad
van het Koninkrijk der Nederlanden

Jaargang 2024

119

Besluit van 7 maart 2024, houdende vaststelling van regels inzake de erkenning van bedrijfs- en organisatiemiddelen en bijbehorende diensten (Besluit bedrijfs- en organisatiemiddel 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 20 juli 2023, nr. 2023-0000412720 /CZW/SB;

Gelet op de artikelen 11, eerste, tweede, derde en vijfde lid, en 13, eerste, vierde en vijfde lid, van de Wet digitale overheid;

De Afdeling advisering van de Raad van State gehoord (advies van 23 augustus 2023, nr. W04.23.00204/I);

Gezien het nader rapport van de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties van 04 maart 2024, nr. 2024-0000078257/CZW/SB;

Hebben goedgevonden en verstaan:

HOOFDSTUK 1. BEGRIPSBEPALINGEN

Artikel 1

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

– *erkende dienst:* partij die op grond van artikel 11 van de wet is erkend als authenticatiedienst of machtigingsdienst;

– *gebruiker:* natuurlijke persoon die gebruik maakt van een bedrijfs- en organisatiemiddel en die een overeenkomst heeft gesloten met de authenticatiedienst die de werking van dat middel verzorgt;

– *machtigingsverklaring:* door een erkende machtigingsdienst elektronisch afgegeven verklaring, waarmee de identiteit van een natuurlijke persoon wordt bevestigd en waaruit blijkt dat die natuurlijk persoon, of dat een onderneming of een rechtspersoon als bedoeld in artikel 5 onderscheidenlijk 6 van de Handelsregisterwet 2007 gemachtigd is op te treden namens die onderneming of die rechtspersoon ten behoeve waarvan toegang tot elektronische dienstverlening met gebruikmaking van een erkend bedrijfs- en organisatiemiddel wordt gevraagd;

– *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, derde lid, 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. EISEN ERKENDE DIENSTEN

Artikel 2 Algemene eisen erkende diensten

1. Een aanvraag voor een erkenning als bedoeld in artikel 11, tweede of derde lid, van de wet kan slechts worden ingediend door een rechtspersoon naar Nederlands recht of het equivalent daarvan naar het recht van 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, en die zijn statutaire zetel, zijn hoofdbestuur of zijn hoofdvestiging binnen de Europese Economische Ruimte heeft.

2. Een erkende dienst:

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

b. is geen surseance van betaling verleend, noch is voor hem surseance van betaling aangevraagd;

c. draagt er zorg voor dat binnen zijn organisatie alle persoonsgegevens die hem in het kader van de diensten waarvoor hij erkend is ter kennis komen vertrouwelijk worden behandeld en niet worden gebruikt voor een ander doel dan voor het uitgeven van een bedrijfs- en organisatiemiddel, authenticatie van een natuurlijke persoon of het afgeven van een verklaring dat die persoon bevoegd is om namens een onderneming of rechtspersoon te handelen;

d. verwerkt gegevens over een gebruiker van een bedrijfs- en organisatiemiddel op een wijze die is afgescheiden van gegevens over het gebruik van dat middel door die gebruiker;

e. heeft een vestiging in Nederland waar kan worden aangetoond dat de aanvrager voldoet aan de eisen, gesteld bij en krachtens dit besluit of bij artikel 11 of 13 van de wet;

f. functioneert in samenwerking met de benodigde onderdelen van de generieke digitale infrastructuur, bedoeld in artikel 5 van de wet, en, in voorkomend geval, andere voor de werking van het bedrijfs- en organisatiemiddel noodzakelijke voorzieningen;

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

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

i. geeft de gebruiker inzage in:

i. de authenticatiehandelingen die met dat bedrijfs- en organisatiemiddel zijn verricht;

ii. de datum en het tijdstip waarop voor dat bedrijfs- en organisatiemiddel een handeling als bedoeld in onderdeel h, is uitgevoerd, met uitzondering van de gevallen waarin die handeling plaatsvond op verzoek van Onze Minister;

j. 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 geheimhoudingsverplichting noodzakelijk is;

k. maakt openbaar op welke wijze met de erkenning en de persoonsgegevens die voor de uitvoering van die erkenning worden verwerkt inkomsten worden verkregen.

3. Een erkende dienst voldoet tevens aan de eisen aangaande beheer en organisatie die zijn opgenomen in paragraaf 2.4 van de bijlage bij de Uitvoeringsverordening (EU) 2015/1502 en aan de bij ministeriële regeling dienaangaande gestelde regels, welke regels kunnen verschillen per betrouwbaarheidsniveau.

4. De eisen, bedoeld in het tweede lid, met uitzondering van de onderdelen a en b, zijn van overeenkomstige toepassing op een derde voor zover die derde in het kader van de erkenning werkzaamheden uitvoert.

Artikel 3 Inkomsten uit verstrekken van gegevens over gebruikers of authenticatie

In de overeenkomst die door een aanvrager van een erkenning als bedoeld in artikel 11, tweede en derde lid, van de wet met een gebruiker wordt gesloten voor het gebruik van een bedrijfs- en organisatiemiddel is een verplichting opgenomen voor erkende dienst 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:

a. kosten voor de gebruiker, of

b. gebruiksfunctionaliteit in het kader van de erkenning.

Artikel 4 Toepassing van software met openbare broncode

1. Bij een erkende dienst wordt in ieder geval voor bij ministeriële regeling aan te wijzen componenten gebruik gemaakt van software:

a. die onder een open source licentie is gepubliceerd; of

b. waarvan de broncode openbaar is gemaakt.

2. Componenten die noodzakelijk zijn voor het gebruik van een machtigingsdienst, authenticatiedienst of identificatiemiddel en waarmee persoonsgegevens worden verwerkt worden op grond van het eerste lid aangewezen, tenzij een aanwijzing onaanvaardbare gevolgen heeft, gelet op:

a. de beschikbaarheid van software voor de desbetreffende componenten;

b. de veiligheid van die componenten;

c. het aanbod van machtigingsdiensten of identificatiemiddelen, waaronder in ieder geval de continuïteit, gebruiksvriendelijkheid en beschikbaarheid van breed aanbod.

3. Een authenticatiedienst of machtigingsdienst waarop een aanvraag ziet biedt aan derden een mogelijkheid om kwetsbaarheden van de software, bedoeld in het eerste lid, te melden en om voorstellen te doen voor aanpassing van die software, reageert adequaat op die voorstellen en meldingen en deelt aan de indiener daarvan mee tot welke handelingen de melding of het voorstel heeft geleid.

4. Bij een aanwijzing als bedoeld in het eerste lid kan onderscheid worden gemaakt tussen authenticatiediensten en machtigingsdiensten en de datum waarop de verplichting, bedoeld in het eerste lid ingaat.

5. Bij ministeriële regeling worden nadere regels worden gesteld over de wijze waarop openbaarmaking van de broncode van software als bedoeld in het eerste lid plaatsvindt.

Artikel 5 Eisen erkende authenticatiedienst

1. Een erkende authenticatiedienst draagt zorg voor:

a. de betrouwbare uitgifte van het bedrijfs- en organisatiemiddel waarvoor hij is erkend, waaronder in ieder geval de verificatie en registratie van de identiteit van de gebruiker wordt begrepen;

b. het op verzoek verzenden van een betrouwbare authenticatieverklaring aan de erkende machtingsdienst waarvan het verzoek afkomstig is ter bevestiging van de identiteit van een natuurlijke persoon; en

c. een loket voor vragen of meldingen aangaande ontstane problemen in de toegang van ondernemingen en rechtspersonen tot elektronische dienstverlening.

2. Onverminderd het eerste lid draagt een erkende authenticatiedienst er zorg voor dat het uitgifteproces en het ontwerp van het bedrijfs- en organisatiemiddel voor het desbetreffende betrouwbaarheidsniveau voldoen aan de op dat proces en het ontwerp betrekking hebbende eisen die zijn opgenomen in de bijlage bij de Uitvoeringsverordening (EU) 2015/1502 met betrekking tot:

a. de aanvraag en de registratie, opgenomen in paragraaf 2.1.1. van die bijlage;

b. het bewijs en de verificatie van de identiteit van een natuurlijke persoon, opgenomen in paragraaf 2.1.2. van die bijlage;

c. de verificatie van de identiteit van de rechtspersoon, opgenomen in paragraaf 2.1.4 van die bijlage; en

d. de kenmerken en het ontwerp van bedrijfs- en organisatiemiddelen, opgenomen in paragraaf 2.2.1. van die bijlage;

e. de uitgifte, de uitreiking en de activering, opgenomen in paragraaf 2.2.2. van die bijlage;

f. de schorsing, de herroeping en de reactivering, opgenomen in paragraaf 2.2.3. van die bijlage;

g. de authenticatie, opgenomen in paragraaf 2.3 van die bijlage, en

h. de verlenging en vervanging, opgenomen in paragraaf 2.2.4. van die bijlage.

Artikel 6 Eisen erkende machtigingsdienst

1. Een erkende machtigingsdienst draagt zorg voor:

a. het registreren van een bevoegdheid van een natuurlijk persoon of rechtspersoon om namens een onderneming of rechtspersoon te handelen;

b. het opvragen van authenticatieverklaringen als bedoeld in artikel 5, eerste lid, onderdeel b, van de erkende authenticatiedienst die erkend is voor het bedrijfs- en organisatiemiddel dat is uitgegeven aan de natuurlijke persoon waarop een verzoek als bedoeld in onderdeel c ziet; en

c. de afgifte op verzoek van betrouwbare machtigingsverklaringen aan de bevoegdheidsverklaringsdienst, bedoeld in het Besluit digitale overheid, het bestuursorgaan of de aangewezen organisatie waarvan het verzoek afkomstig is, op basis van;

i. een authenticatieverklaring als bedoeld in onderdeel b; en

ii. de informatie bedoeld in onderdeel a, of een machtigingsverklaring van een andere erkende machtigingsdienst.

2. Ten aanzien van de in het eerste lid opgenomen verantwoordelijkheden voldoet een erkende machtigingsdienst aan de eisen die zijn opgenomen in de bijlage bij de Uitvoeringsverordening (EU) 2015/1502 met betrekking tot:

a. de verificatie van de identiteit van de rechtspersoon, opgenomen in paragraaf 2.1.3 van die bijlage; en

b. de koppeling tussen een bedrijfs- en organisatiemiddel van een natuurlijke persoon en rechtspersonen, opgenomen in paragraaf 2.1.4 van die bijlage.

3. Een erkende machtigingsdienst registreert uitsluitend een bevoegdheid als bedoeld in het eerste lid, onderdeel a, na instemming van een wettelijke vertegenwoordiger van de betrokken onderneming of

rechtspersoon of na instemming van een door die wettelijke vertegenwoordiger gemachtigde.

4. Een erkende machtigingsdienst beëindigt de registratie van de bevoegdheid als bedoeld in het eerste lid, onderdeel a, indien deze wordt ingetrokken door de wettelijk vertegenwoordiger van de betrokken onderneming of rechtspersoon of een door die vertegenwoordiger gemachtigde.

Artikel 7 Aanvullende eisen erkende diensten en bedrijfs- en organisatiemiddelen

1. Het bedrijfs- en organisatiemiddel waarop de erkenning 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 bedrijfs- en organisatiemiddel noodzakelijke voorzieningen;

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

c. voldoet aan de eisen voor het verlenen van een erkenning, bedoeld in artikel 11, achtste lid, onderdelen b en d, van de wet.

2. Bij ministeriële regeling worden voor erkende diensten aanvullende eisen gesteld, die per soort erkende dienst van de wet kunnen verschillen en die betrekking hebben op:

a. het aanvragen van een bedrijfs- en organisatiemiddel door en het registreren van een beoogd gebruiker;

b. de wijze waarop de identiteit van de aanvrager van een bedrijfs- en organisatiemiddel wordt bewezen en geverifieerd;

c. de kenmerken en het ontwerp van een bedrijfs- en organisatiemiddel;

d. de uitgifte, de uitreiking en de activering van een bedrijfs- en organisatiemiddel;

e. de schorsing, de herroeping en de reactivering van een bedrijfs- en organisatiemiddel;

f. verlenging en vervanging van een bedrijfs- en organisatiemiddel;

g. het authenticatiemechanisme dat een bedrijfs- en organisatiemiddel toepast en de wijze waarop wordt voldaan aan artikel 6, eerste lid;

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. periodieke actualisatie en controle van de juistheid van voor het authenticatie- of machtigingsproces gebruikte gegevens;

k. voorzieningen die worden gebruikt bij toepassing van het bedrijfs- en organisatiemiddel of bij het verwerken van gegevens;

l. de integriteit en kwalificaties van het bestuur van de organisatie van de erkende dienst en van het personeel dat betrokken is bij de inzage of het beheer van bedrijfs- en organisatiemiddelen;

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

n. de wijze van verwerking van persoonsgegevens die zijn verkregen in het kader van authenticatie of het afgeven van een machtigingsverklaring en de beveiliging of organisatorische of technische inrichting daarvan;

o. de gebruiksvriendelijkheid van een bedrijfs- en organisatiemiddel;

p. de rapportages die periodiek aan Onze Minister worden overgelegd, de inhoud daarvan en de frequentie en het moment waarop dat overleggen plaatsvindt;

q. de toepassing van de gronden, bedoeld in artikel 11, achtste lid, onderdeel b tot en met e, van de wet.

3. Bij ministeriële regeling kunnen per soort erkende dienst aanvullende eisen worden gesteld, die betrekking hebben op de interoperabiliteit met en het aansluiten op de onderdelen van de infrastructuur, bedoeld in artikel 5, eerste en tweede lid, van de wet.

4. Bij ministeriële regeling worden regels gesteld over de voorwaarden die door een erkende dienst in elk geval worden opgenomen in de gebruiksvoorwaarden die zij stellen aan de gebruikers van hun diensten.

5. Bij ministeriële regeling kunnen regels worden gesteld aangaande de interoperabiliteit tussen de erkende diensten, voor zover dit voor de betrouwbare toegang van ondernemingen en rechtspersonen tot elektronische dienstverlening noodzakelijk is.

6. Bij ministeriële regeling worden nadere eisen gesteld aan het minimale niveau van dienstverlening door de erkende diensten, waaronder de beschikbaarheidsnorm die voor die diensten geldt en de wijze waarop wordt bepaald of aan die norm is voldaan. Deze eisen kunnen verschillen per soort erkende dienst.

7. Bij ministeriële regeling kan worden bepaald dat gedurende een bij die regeling te bepalen periode onderscheid wordt gemaakt tussen de toepassing van een eis op te erkennen en erkende diensten.

HOOFDSTUK 3. OVERIGE VERPLICHTINGEN ERKENDE DIENSTEN

Artikel 8 Meldingsplicht

1. Een houder van een erkenning meldt in ieder geval onverwijld aan onze minister:

a. wijzigingen die worden aangebracht in de werking van het bedrijfs- en organisatiemiddel 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 wijziging van de erkenning of een andere erkenning aanvraagt;

b. wijzigingen in de organisatie of de zeggenschap, bedoeld in artikel 12, tweede 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. Indien het incident of de verstoring naar verwachting negatieve gevolgen zal hebben voor een andere erkende dienst, een gebruiker van het betrokken bedrijfs- en organisatiemiddel of een onderneming of rechtspersoon ten behoeve waarvan het bedrijfs- en organisatiemiddel is gebruikt, stelt de erkende dienst ook die dienst, gebruiker of onderneming of rechtspersoon op de hoogte.

3. 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 9 Uitvoeren van onafhankelijk onderzoek

1. Onze Minister kan een houder van een erkenning bij bindende aanwijzing, als bedoeld in artikel 13, vijfde lid, van de wet 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; en

b. een onafhankelijke deskundige een boekhoudkundig onderzoek laat uitvoeren om te bepalen of de houder handelt of heeft gehandeld in strijd met artikel 2, tweede lid, aanhef en onderdeel d.

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 10 Geldig certificaat

1. Een erkende dienst beschikt over een geldige verklaring als bedoeld in artikel 16, eerste lid.

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.

Artikel 11 Beschrijving van de dienstverlening

Een houder van een erkenning publiceert een beschrijving van zijn dienstverlening voor gebruikers, die actuele informatie bevat over de volgende onderwerpen:

a. een omschrijving van de voor de uitvoering van de erkenning noodzakelijke technische werking van het bedrijfs- en organisatiemiddel waaronder de ontwikkelprocessen, de toegepaste maatregelen rond beveiliging, betrouwbaarheid en cryptografie alsmede van de toepassing van de stand der techniek daarbij;

b. de wijze waarop de werking van het bedrijfs- en organisatiemiddel en het authenticatie- en machtigingsproces 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.

HOOFDSTUK 4. AANVRAAG, CONFORMITEIT EN INTREKKING ERKENNING

Artikel 12 De erkenning en de aanvraag om erkenning

1. Een erkenning als bedoeld in artikel 11, tweede of derde lid, van de wet, wordt slechts op aanvraag verstrekt.

2. Onverminderd het bepaalde in artikel 11, vijfde lid, van de wet, gaat een aanvraag om erkenning in ieder geval vergezeld van:

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

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

c. een model van de overeenkomst die de aanvrager zal sluiten met gebruikers van het bedrijfs- en organisatiemiddel of met een rechtspersonen of organisatie waarvoor machtigingen worden geregistreerd door de machtigingsdienst 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 4, eerste lid; en

f. de adresgegevens van de vestiging, bedoeld in artikel 2, tweede lid, onderdeel e.

3. Bij ministeriële regeling kunnen nadere regels worden gesteld aangaande de procedure van het indienen van de aanvraag, de vorm waarin deze wordt ingediend en de gegevens die daarbij in ieder geval moeten worden verstrekt, waarbij onderscheid kan worden gemaakt tussen een aanvrager als bedoeld in het vierde lid en overige aanvragers.

4. Het tweede 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 9, tweede lid, van de wet, voor een identificatiemiddel met dezelfde werking.

Artikel 13 Beslissing

1. Een aanvraag om erkenning wordt afgewezen indien:

a. niet uit de aanvraag blijkt dat de aanvrager, de dienst en het bedrijfs- en organisatiemiddel waarop de aanvraag ziet kunnen voldoen aan de eisen die daarvoor zijn gesteld bij en krachtens dit besluit of indien de aanvrager niet voldoet aan artikel 14;

b. deze niet is ingediend door een rechtspersoon of onderneming in de zin van de Handelsregisterwet 2007;

c. de aanvraag niet ziet op erkenning van de aanvrager als authenticatiedienst of machtigingsdienst.

2. Een erkenning wordt verleend voor onbepaalde tijd.

3. Van een besluit tot erkenning of wijziging of intrekking daarvan doet Onze Minister mededeling in de Staatscourant.

4. Binnen een bij ministeriële regeling te bepalen termijn na de mededeling in de Staatscourant biedt de erkende dienst de dienst en het middel aan waarvoor hij is erkend.

Artikel 14 Medewerking aanvrager

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

Artikel 15 Beslistermijn

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

2. Op aanvragen die in een periode van twaalf weken of minder 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 16 Certificaat van conformiteit

1. Een certificaat van conformiteit als bedoeld in artikel 11, vijfde lid, van de wet:

a. ziet op de norm ISO 27001;

b. heeft een afgiftedatum die niet meer dan een jaar in het verleden ligt;

c. ziet op het bedrijfs- en organisatiemiddel of de machtigingsdienst waarvoor de erkenning wordt aangevraagd en de conformiteit van de systemen en processen die daarvoor worden gebruikt met de eisen, gesteld bij en krachtens dit besluit, voor het betrouwbaarheidsniveau waarop de aanvraag ziet;

d. 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).

2. Het certificaat, 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 17 Intrekking erkenning op verzoek

1. Een erkenning als bedoeld in artikel 11, tweede en derde lid, van de wet 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. zij gebruikers, rechtspersonen en ondernemingen waarvoor verklaringen worden verstrekt tijdig en deugdelijk informeert over het moment waarop het bedrijfs- en organisatiemiddel, waarop de erkenning ziet, niet meer bruikbaar 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 de authenticatiedienst 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 besluit 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 per soort erkende dienst 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 18 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 19 Wijziging van een erkenning

1. Artikel 13 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, gesteld in en krachtens hoofdstuk 2 en in artikel 11, achtste lid, van de wet;

b. de wijziging ziet op de houder van de erkenning en de beoogde houder niet een rechtspersoon of onderneming is als bedoeld in artikel 2, eerste lid;

c. de aanvrager niet de medewerking, bedoeld artikel 14, verleent.

Artikel 20 Advies Landelijk Bureau BIBOB

Alvorens te beslissen over het wijzigen, schorsen of intrekken van een erkenning vanwege zwaarwegende redenen als bedoeld in artikel 14, derde 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 5. OVERGANGSTERMIJN EX ARTIKEL 24 VAN DE WET

Artikel 21 Eisen voor partijen tijdens overgangstermijn

1. Bij ministeriële regeling:
a. kan worden bepaald dat bij die regeling te bepalen eisen, gedurende een periode binnen de termijn, bedoeld in artikel 24 van de wet, niet van toepassing zijn op partijen als bedoeld in dat artikel;
b. kan worden bepaald dat gedurende de periode, bedoeld in artikel 24 van de wet, eisen slechts van toepassing zijn op partijen als bedoeld in dat artikel.
2. Bij de toepassing van het eerste lid kan onderscheid worden gemaakt tussen een machtigingsdienst en een authenticatiedienst.

HOOFDSTUK 6. SLOTBEPALINGEN

Artikel 22 Inwerkingtreding

Dit besluit treedt in werking op een bij koninklijk besluit te bepalen tijdstip.

Artikel 23 Citeertitel

Dit besluit wordt aangehaald als: Besluit bedrijfs- en organisatiemiddel Wdo.

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

’s-Gravenhage, 7 maart 2024

Willem-Alexander

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
A.C. van Huffelen

Uitgegeven de *dertigste* april 2024

De Minister van Justitie en Veiligheid,
D. Yeşilgöz-Zegerius

stb-2024-119
ISSN 0920 - 2064
’s-Gravenhage 2024

NOTA VAN TOELICHTING

Algemeen deel

1. Aanleiding en uitgangspunten

Burgers en bedrijven moeten te allen tijde veilig en betrouwbaar met de overheid kunnen communiceren, ook digitaal. De minister van Binnenlandse Zaken en Koninkrijksrelaties (hierna: de minister) is verantwoordelijk voor de veilige toegang voor burgers en bedrijven tot digitale dienstverlening van de overheid. In de Wdo is deze verantwoordelijkheid vastgelegd. Daarbij is ook geregeld dat in nadere regelgeving normen worden gesteld waaraan publieke en private identificatiemiddelen die gebruikt kunnen worden bij het verlenen van toegang tot publieke dienstverlening, in het publieke domein moeten voldoen. Dit besluit bevat de nadere regels die worden gesteld aan bedrijfs- en organisatiemiddelen. Deze middelen worden gebruikt door bedrijven (ondernemingen en rechtspersonen) om toegang te krijgen tot elektronische overheidsdienstverlening. Met dit besluit wordt verzekerd dat deze toegang voor bedrijven veilig en betrouwbaar kan plaatsvinden.

Dit besluit geeft uitvoering aan de artikelen 11, eerste, tweede, derde en vijfde lid, en 13, eerste, vierde en vijfde lid, van de Wdo. Op grond van die artikelen zijn regels gesteld inzake de erkenning van partijen die elektronische identificatiemiddelen leveren en daarbij betrokken diensten aanbieden. Op grond van dit besluit zijn meer gedetailleerde regels gesteld bij ministeriële regeling.

Uitgangspunt van de regels: eIDAS-verordening en AVG

Het uitgangpunt voor deze nadere regels is de eIDAS-verordening en de daarop gebaseerde Uitvoeringsverordening (EU) 2015/1502 (hierna: de Uitvoeringsverordening). Deze bevat eisen voor (stelsels van) identificatiemiddelen indien lidstaten deze, ten behoeve van wederzijdse erkenning en grensoverschrijdende elektronische authenticatie, wensen te notificeren. Deze eisen betreffen onder andere de betrouwbaarheid van elektronische identificatiemiddelen en uitgifteprocessen op de betrouwbaarheidsniveaus laag, substantieel en hoog. Om veiligheid en betrouwbaarheid van ons stelsel te garanderen alsmede om notificatie, en daarmee grensoverschrijdend gebruik van erkende bedrijfs- en organisatiemiddelen mogelijk te maken, vormen deze eisen de basis voor dit besluit.

Daarnaast vormen de privacy-eisen uit de AVG, de Nederlandse implementatiewet UAVG en nationale privacyregelgeving zoals BSN-wetgeving, een belangrijk uitgangspunt voor de eisen die in dit besluit aan aanbieders van inlogmiddelen worden gesteld.

Ten slotte zijn in dit besluit de eisen uitgewerkt zoals deze naar aanleiding van het debat over de Wdo in de Eerste Kamer, door middel van een novelle (Kamerstukken II 2020–2021, 35 868) expliciet in de Wdo zijn opgenomen. Het betreft eisen over privacy by design, het verbod voor erkende partijen om gegevens van burgers te verhandelen en de inzet van open source licenties door erkenningshouders. Gezien het belang van deze eisen zijn deze eisen in de wet zelf vastgelegd, en in onderhavig besluit nader uitgewerkt. De inhoud van de eisen in dit besluit komt overeen met het spiegelbeeldige besluit identificatiemiddelen voor natuurlijke personen Wdo.

Privacy by design

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 (privacy by design). Voor de beoordeling of dit het geval is worden de richtsnoeren gebruikt die de European Data Protection Board hanteert.

Verhandelverbod van gegevens

In dit besluit is het verhandelverbod van gegevens ten eerste uitgewerkt door middel van de verplichting tot een gescheiden opslag van gebruiks- en gebruikersgegevens, waardoor de koppeling ervan niet meer of alleen geclausuleerd mogelijk is. Verder zijn erkende partijen verplicht openbaar te maken op welke wijze zij inkomsten genereren met een erkenning, en zijn zij verplicht om waar mogelijk met versleutelde gegevens te werken. Gebruikers moeten verder de mogelijkheid krijgen om het verstrekken van gegevens te beëindigen zonder verlies van functionaliteiten en zonder nadelige financiële gevolgen.

Open source

Dit besluit heeft als doel de inzet van open source software als onderdeel van de toegelaten inlogmiddelen op een verantwoorde manier mogelijk te maken, zonder dat dit ten koste gaat van de mogelijkheden voor gebruikers om op veilig wijze toegang te krijgen tot elektronische dienstverlening. 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.

In dit besluit is namelijk voorgeschreven dat een aanbieder van een identificatiemiddel voor bepaalde componenten van dat inlogmiddel software moet gebruiken waarvan de broncode openbaar is. Bij ministeriële regeling wordt bepaald welke componenten het betreft. Daarbij worden componenten aangewezen die persoonsgegevens verwerken, omdat bij die componenten het risico bestaat op ongewenst datagebruik. In beginsel moeten deze componenten worden aangewezen, tenzij dat aanwijzen onaanvaardbare gevolgen heeft voor de veiligheid in inlogmiddelen, de continuïteit van middelen die al worden gebruikt, of de beschikbaarheid van een breed aanbod. Daarmee wordt met dit besluit het principe «open, tenzij» vastgelegd, en wordt uitvoering gegeven aan de motie van kamerlid Dekker-Abdulaziz over dit onderwerp.

Wanneer een component is aangewezen moet daarvoor software worden gebruikt die onder een open source licentie is gepubliceerd (openbaarmaking van de broncode is een onderdeel van deze licenties) of waarvan de broncode op andere wijze openbaar is gemaakt. Op grond van dit besluit kunnen nadere regels worden gesteld aan de wijze waarop de broncode openbaar wordt gemaakt, bijvoorbeeld wanneer openbaarmaking op andere wijze dan via een open source-licentie plaatsvindt.

Verder wordt met dit besluit geregeld dat voor de aangewezen componenten een mogelijkheid moet bestaan voor derden om kwetsbaarheden van de software te melden en om voorstellen te doen voor aanpassing van die software. Daarmee wordt geborgd dat de community die gericht is op het monitoren en verbeteren van de software altijd een kanaal heeft om bevindingen te rapporteren. De aanbieder van een authenticatiedienst of machtigingsdienst is vervolgens gehouden om op

deze inbreng te reageren en om terugkoppeling te geven over de gevolgen die daaraan zijn gegeven.

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.

Toezicht op naleving

Aanbieders van private inlogmiddelen worden hier niet alleen bij de toelating op bovenstaande eisen gecontroleerd, maar ook tussentijds, als onderdeel van het doorlopende toezicht op de inlogmiddelen. Zo zijn partijen verplicht een onafhankelijke audit uit te voeren. Verder zijn zij verplicht om mee te werken aan het toezicht. Bij overtreding van de regels in dit besluit kan in voorkomende gevallen worden overgegaan tot schorsing, en uiteindelijk ook uitsluiting van de dienstverlening, waarbij de toelating wordt ingetrokken en de aanbieder zijn dienstverlening moet stoppen.

Daarnaast zijn er nog extra waarborgen ingebouwd in de vorm van de meldingsplicht. Wanneer het middel wijzigt moet in beginsel ook de verleende erkenning worden gewijzigd. Soms is geen wijziging van de erkenning nodig. In dat geval is het doen van een melding verplicht.

eHerkenning en de Wdo: overgangstermijn

In de Wdo is de veilige toegang voor bedrijven tot de digitale overheid publiekrechtelijk geregeld. De minister is eindverantwoordelijk en heeft bevoegdheden om deze verantwoordelijkheid waar te te kunnen maken. Ook regelt de Wdo dat publiekrechtelijk toezicht op de middelen worden gehouden, door de Rijksinspectie Digitale Infrastructuur.

Eerder is door de Minister van Economische Zaken en later de minister, het bedrijfsmiddel eHerkenning ontwikkeld in de vorm van een publiek-private samenwerking. Met de inwerkingtreding van de Wdo is dit veranderd. Voor eHerkenning betekent dit dat de op dit moment beschikbare bedrijfs- en organisatiemiddelen onder het publiekrechtelijke Wdo-regime vallen.

Voor hen betekent dat een wijziging op een aantal punten, waaronder governance, en op een aantal punten ook inhoudelijke eisen. Hierop passen de partijen hun bedrijfsvoering aan. Aangezien het belangrijk is continuïteit van de inlogmiddelen voor bedrijven te verzekeren, is voorzien in een overgangsperiode van 18 maanden.

2. Veilig inloggen voor bedrijven: inzet markt, rollen en samenwerking

Het kabinet heeft met het programma Digitaal 2017 de ambitie uitgesproken om alle dienstverlening van overheden digitaal beschikbaar te stellen. Bedrijven en organisaties kunnen bij de overheid steeds meer zaken digitaal regelen, bijvoorbeeld een vergunning aanvragen of Btw-aangifte indienen. Vanzelfsprekend kan dat alleen als de toegang tot die diensten veilig en betrouwbaar is.

Marktinzet en terugvalopties

Een belangrijke reden om te kiezen voor een systeem waarbij meerdere partijen worden erkend om inlogmiddelen te leveren, is dat op deze manier de afhankelijkheid van één enkele mogelijkheid (single point of

failure) voorkomen wordt. Door ervoor te kiezen private partijen te erkennen, wordt er gebruik gemaakt van een marktmechanisme, dat zorgt voor een continue verbeterslag van inlogmiddelen en inzet van innovatieve beschermingsmogelijkheden. Door de mogelijkheid om private middelen ook buiten de overheid te gebruiken, kunnen bedrijven zich ook buiten de overheid en in onderlinge relaties met deze middelen identificeren. Uiteraard zien de eisen in dit besluit en het toezicht dat daarop wordt gehouden niet op gebruik buiten het overheidsdomein.

Maatschappelijke belang staat voorop

De keuze voor de inzet van private partijen is bewust, en sluit ook aan bij keuzes die andere lidstaten maken binnen de eIDAS-verordening. De keus om private partijen in te zetten betekent echter ook dat marktbelangen een rol zullen gaan spelen bij de digitale toegang tot de overheid. Het fundamentele uitgangspunt bij de veilige digitale toegang tot de overheid is echter dat het maatschappelijk belang te allen tijde prevaleert. Dat is ook de reden dat de Wdo voorziet in een publiekrechtelijk kader, waarin veiligheid, betrouwbaarheid en privacybescherming voorop staat.

Stelsel toegang en bedrijfs- en organisatiemiddelen

Ten behoeve van de veilige toegang tot de overheid voor bedrijven en organisaties zijn verschillende rollen voorzien die worden erkend. Deze rollen zullen zowel onderling moeten samenwerken als met de randvoorwaardelijke voorzieningen van de overheid voor digitale toegang. Door middel van regels over interoperabiliteit wordt gezorgd dat al deze onderdelen in een stelsel kunnen samenwerken. Daarbij worden ook regels gesteld om te zorgen dat het stelsel verantwoord kan doorontwikkelen en de interoperabiliteit geborgd blijft. Hieronder wordt dit toegelicht.

Erkenning van authenticatiedienst en machtigingsdienst

Voor de beschikbaarheid van veilige toegang tot de digitale overheid zijn in het bedrijvendomein twee rollen voorzien, te weten de authenticatiedienst, die de identiteit vaststelt, en de machtigingsdienst, die de bevoegdheid om namens een bedrijf of organisatie te handelen koppelt aan de identiteit.

Aan deze rollen worden eisen gesteld die volgen uit de eIDAS verordening, de AVG, nationale privacyregelgeving en de gemaakte politiek-beleidsmatige keuzes, die in de Wdo zijn opgenomen.

In dit besluit zijn de verantwoordelijkheden die bij deze rollen horen vastgelegd. In het hiernavolgende wordt op de verschillende rollen ingegaan.

De authenticatiedienst

De authenticatiedienst is verantwoordelijk voor de uitgifte, het beheer en de intrekking van het bedrijfs- en organisatiemiddel waarvoor hij erkend is, en voor het zorgvuldig vastleggen van alle daarvoor geregistreerde gegevens in een administratie. De authenticatiedienst identificeert hiertoe een natuurlijke persoon en levert een verklaring waarin staat dat het inlogmiddel hoort bij die natuurlijke persoon. De activiteit die de authenticatiedienst hier verricht, is vergelijkbaar met het uitgifteproces van een identiteitsbewijs. In plaats van een fysiek document krijgt de natuurlijke persoon een elektronisch bewijs.

De authenticatiedienst is voorts verantwoordelijk voor het authenticeren van personen op basis van hun middel. Door deze diensten wordt vastgesteld of de identiteit van de persoon die wil inloggen overeenkomt met de identiteit van de persoon aan wie het middel is uitgegeven. Als deze authenticatie is gelukt, stelt de authenticatiedienst een elektronische authenticatieverklaring op.

De machtigingsdienst

De machtigingsdienst registreert en ontsluit de informatie over de bevoegdheid van de desbetreffende persoon om namens een onderneming of organisatie handelingen te verrichten («Wat mag je»). De kern van de machtigingsdienst bestaat eruit dat deze de interne vertegenwoordigingsstructuur van een organisatie up-to-date houdt en dat deze digitaal beschikbaar is.

Verder stelt de machtigingsdienst in samenwerking met de authenticatiedienst de verklaring samen over de koppeling tussen identiteit en bevoegdheid en zorgt dat deze verklaring aan de dienstverlener wordt gecommuniceerd.

Interoperabiliteit tussen diensten

Bedrijfs- en organisatiemiddelen dienen onderling samen te werken. Om te zorgen dat dit kan, en ook te zorgen dat andere partijen die erkend willen worden aan de samenwerking kunnen deelnemen, worden op basis van dit besluit bij ministeriële regeling regels gesteld om interoperabiliteit tussen de verschillende rollen te borgen.

Samenwerking met randvoorwaardelijke toegangsvoorzieningen binnen de overheid

Naast de bovenstaande onderlinge relaties tussen de erkende diensten bestaat er ook een relatie met een aantal generieke publieke voorzieningen als bedoeld in artikel 5 van de Wdo. Het stelsel heeft onder meer een verbinding met de infrastructuur die nodig is om grensoverschrijdende toegang tot elektronische dienstverlening mogelijk te maken (artikel 5, tweede en derde lid, van de Wdo). Ook maakt het stelsel gebruik van het BSN-koppelregister (artikel 5, eerste lid, onderdeel d, van de Wdo) die het mogelijk maakt dat de identiteit van een onderneming of rechtspersoon die een elektronische dienst afneemt bij een bestuursorgaan of aangewezen organisatie op unieke wijze geïdentificeerd kan worden. Het BSN-koppelregister verstrekt namelijk een versleutelde identiteit die zowel door authenticatiediensten als machtigingsdiensten wordt gebruikt in het machtigingsproces.

Ontwikkelingen van het stelsel

Het stelsel toegang functioneert in een snel innoverende digitale omgeving. Het stelsel zal daarin moeten kunnen meegroeien. In het geval dat veranderingen worden doorgevoerd in het netwerk, door een of meer erkende diensten, of in de infrastructuur van de overheid, is het van belang dat het stelsel als zodanig goed blijft werken en interoperabel en veilig en betrouwbaar blijft.

3. De erkenning

Een authenticatiedienst of een machtigingsdienst moet door de minister erkend zijn om diensten ten behoeve van veilige digitale toegang voor bedrijven en organisaties te mogen aanbieden. Het proces van erkenning start wanneer een partij daartoe een aanvraag indient bij de minister.

Om erkend te kunnen worden moet een partij bewijsstukken aanleveren die aantonen dat hij voldoet aan de door de minister gestelde eisen. Deze bewijsstukken worden beoordeeld, waarbij eventueel additioneel onderzoek kan plaatsvinden om het bewijs te verifiëren en aan te vullen. Indien de aanvrager en het door hem aangeboden identificatiemiddel voldoen aan de daarin in dit besluit en de daarop gebaseerde regeling gestelde regels wordt de aanvrager erkend. Met de erkenning wordt de aanvrager toegestaan om de rol te vervullen waarop de aanvraag ziet, zolang dat gebeurt voor het identificatiemiddel waarop de aanvraag ziet.

Certificaat van conformiteit

Bij de aanvraag dient in elk geval een certificaat van conformiteit inclusief het bijbehorende auditrapport te worden overgelegd van een conformiteit-beoordelende instantie (CBI). Deze CBI toetst op grond van de norm ISO 27001, die ziet op informatiebeveiliging. Verder kunnen op grond van dit besluit aanvullende rapportages worden voorgeschreven, die bij de aanvraag moeten worden overgelegd. Die aanvullende eisen worden gesteld in de ministeriële regeling waarvoor dit besluit een basis biedt.

De certificering door de CBI vindt, voorafgaand aan de aanvraag van een erkenning, plaats in opdracht – en op kosten – van de partij die erkend wil worden. Ook na het verlenen van een erkenning moet de erkende partij gecertificeerd zijn. Het certificaat is drie jaar geldig, maar moet op grond van dit besluit ten minste ieder jaar worden herbevestigd.

In dit besluit worden nadere eisen gesteld aan de CBI. In elk geval dient de instantie te zijn geaccrediteerd door de Raad van Accreditatie voor het certificeren op grond van ISO 27001. De Raad houdt toezicht op de kwaliteit van het werk van de geaccrediteerde CBI.

Verwerken van persoonsgegevens

Een erkenning heeft in ieder geval tot gevolg dat de door de erkende partij aangeboden dienst moet worden geaccepteerd door instanties die publieke diensten verlenen. Het Besluit digitale overheid regelt welke persoonsgegevens een erkende dienst mag verwerken. In de toelichting bij dat besluit wordt nader ingegaan op de relatie tot de AVG en verwerkingsverantwoordelijkheid van partijen. In dit besluit zijn de verantwoordelijkheden voor de verschillende partijen uitgebreid uitgewerkt. Daardoor is duidelijk welke handelingen deze partijen uitvoeren en wat daarvan de onderlinge samenhang is, ook in relatie tot de verantwoordelijkheid van de minister van Binnenlandse Zaken en Koninkrijksrelaties. Hierdoor wordt duidelijk dat partijen telkens onafhankelijk van elkaar verwerkingshandelingen uitvoeren en dat van gezamenlijke verwerking en gezamenlijke verwerkingsverantwoordelijkheid geen sprake is.

Toepasselijkheid Algemene wet bestuursrecht en rechtsbescherming

Een erkenning is een besluit in de zin van de Algemene wet bestuursrecht. Tegen het verlenen, weigeren, schorsen of intrekken daarvan staan bezwaar en beroep open op grond van die wet. De overige procedurele

bepalingen, bijvoorbeeld over het in behandeling nemen van een aanvraag en het tijdig nemen van een besluit, zijn ook van toepassing op een erkenning. Als gevolg daarvan kan bijvoorbeeld een aanvraag buiten toepassing worden gelaten wanneer daarbij niet de voorgeschreven documenten zijn gevoegd.

4. 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 dit besluit zijn dergelijke heffingen niet opgenomen. Wanneer dat wenselijk is wordt in een separate AMvB vastgelegd dat een dergelijke heffing voor toelating en toezicht verschuldigd is en zijn de hoofdelementen voor de berekenings- en inningswijze bepaald.

5. Handhaving en uitvoering

In artikel 17, vijfde lid, is bepaald dat de Rijksinspectie Digitale Infrastructuur is belast met toezicht op de naleving van de verplichtingen die voor erkende partijen gelden op grond van de wet. De toezichthouder ziet binnen de kaders van de Wdo en de daarop berustende bepalingen toe op de eisen die met en op grond van dit besluit worden gesteld aan erkende diensten. De toezichthouder vormt een oordeel over de mate waarin een partij met betrekking tot de erkende dienst alle regels naleeft die door de Wdo, dit besluit en de gebaseerde ministeriële regeling worden gesteld. Dit doet de toezichthouder onder meer door zelf inspecties uit te voeren.

Zowel in de erkenningsfase als in de fase waarin toezicht wordt gehouden op een verleende erkenning spelen externe onderzoeken een belangrijke rol. Bij het toetsen van een aanvraag wordt de minister bij het vormen van zijn oordeel ondersteund door de bevindingen van de CBI en andere overgelegde rapportages.

6. Regeldruk en administratieve lasten

Kosten voor de erkende partijen

Het certificaat voor erkenning 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 herhaalaudits, omdat voor de eerste audit het bewijs dat aan de eisen wordt voldaan en het ophalen daarvan nog 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.

De totale kosten voor een partij om erkend te worden en erkend te blijven worden vooral bepaald door het aantal en type diensten dat de partij wil laten erkennen. Een partij die zich voor zowel authenticatiedienst als machtigingsdienst wil laten erkennen heeft uiteraard meer kosten dan een partij die slecht voor een van beide diensten erkend wil worden, omdat aan de auditor en de toezichthouder aangetoond moet worden dat aan alle eisen wordt voldaan. Een deel van de eisen is echter generiek voor beide diensten en de naleving ervan hoeft uiteraard niet steeds voor

elke dienst opnieuw worden aangetoond. Bijvoorbeeld de eisen aan de organisatie.

Dit besluit vereist het bezit van een ISO 27001-certificaat met betrekking tot informatiebeveiliging. Naar verwachting hebben veel potentiele aanvragers reeds een dergelijk certificaat, waardoor de kosten voor het doorvoeren van de noodzakelijke wijzigingen voor het verkrijgen van een dergelijk certificaat laag relatief zullen zijn. De verlaging is mogelijk op voorwaarde dat de operationele infrastructuur, waaronder technische infrastructuur en generieke bedrijfsprocessen, waarop de te erkennen dienst draait in zijn geheel of deels in de scope van het genoemde certificaat is opgenomen. Een ISO 27001-certificaat is in beginsel passend voor alle te erkennen partijen en diensten.

Tot slot zal een te erkennen dienst om aan te tonen dat aan specifieke eisen wordt voldaan, een technische beveiligingstest moeten uitvoeren en deze tweejaarlijks moeten herhalen. Deze beveiligingstest vloeit voort uit de eIDAS-eisen. Deze test wordt beschouwd als normale «productie-kosten» 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 plusminus 25.000 euro bedragen al naar gelang de complexiteit van de dienst. Hier geldt dat bij beperkte wijziging van de dienst, in de regel, een herhaalde audit minder kosten met zich meebrengt dan bij een fundamentelere wijziging van de dienst.

Concluderend zijn de kosten van een erkenning afhankelijk van:
– Het aantal diensten dat erkend moet worden;
– De specifieke technische 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 technische complexiteit van de dienst;
– De aard, omvang en frequentie van wijzigingen die in de tijd worden aangebracht aan de dienst.

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

7. Delegatie naar ministeriële regeling

Dit besluit ressorteert onder de Wdo (de artikelen 11 tweede, derde en vijfde lid, en 13, eerste, vierde en vijfde lid).

Op grond van dit besluit wordt een ministeriële regeling opgesteld waarbij de volgende elementen worden geregeld:

Artikel besluit	Onderwerp
4, eerste tot en met derde lid	Norm voor het gebruik van open source software en berekeningswijze
7, tweede lid	Aanvullende eisen erkende diensten en door hen aangeboden identificatiemiddelen
7, derde lid	Regels over interoperabiliteit met de generieke digitale infrastructuur
7, vierde lid	Gebruikersvoorwaarden erkende diensten
7, vijfde lid	Regels over onderlinge interoperabiliteit van erkende diensten
7, zesde lid	Minimale niveau van dienstverlening
8, derde lid	Nadere regels meldingsplicht
9, derde lid	Nadere regels over auditverplichting
12, derde lid	Nadere regels indienen aanvraag
13, derde lid	Nadere regels verklaring van conformiteit
14, vierde lid	Termijn leveringsplicht

Artikel besluit	Onderwerp
17, vierde lid	Nadere regels met betrekking tot aanvraag beëindiging erkenning

De noodzaak om deze onderwerpen nader uit te werken in een ministeriële regeling volgt uit de aard van de betrokken bepalingen. Zij lenen zich niet goed voor uitwerking in dit besluit omdat zij een grote mate van detaillering bevatten, veelal technische, beheersmatige en operationele eisen stellen en mogelijk met enige regelmaat worden gewijzigd. In het artikelsgewijze deel van deze toelichtingen wordt bij de desbetreffende artikelen zoveel mogelijk een voorbeeld gegeven van de praktische uitwerking van deze grondslagen.

8. Consultatie

Het ontwerpbesluit is in de zomer van 2018 voorgelegd aan Agentschap Telecom (deze organisatie heet sinds januari 2023 Rijksinspectie digitale infrastructuur) en aan de uitvoeringsorganisatie Logius. Deze reacties hebben geleid tot aanpassing van dit oorspronkelijke concept. Omdat het concept mede in samenwerking met deze organisaties tot stand is gekomen gaat het om beperkte aanpassingen om de uitvoerbaarheid te borgen.

Vervolgens is op 17 juni 2019 het aangepaste ontwerpbesluit via internetconsultatie opengesteld voor reacties. Daar hebben zes partijen gebruik van gemaakt, al dan niet ten behoeve van diverse aangesloten partijen. Ook is het ontwerpbesluit voorgelegd aan de Autoriteit Persoonsgegevens en het Adviescollege toetsing regeldruk.

Uit de reacties is gebleken dat het besluit in zijn algemeenheid op steun kan rekenen, maar dat er op onderdelen vragen en opmerkingen zijn geplaatst. De vragen en opmerkingen van al deze partijen hebben op diverse plaatsen geleid tot aanpassing van het besluit en de Nota van Toelichting.

De Autoriteit Persoonsgegevens (hierna: AP) heeft op 19 september 2019 over een concept van dit besluit geadviseerd. De AP adviseert keuze voor delegatie van de diverse onderwerpen en de keuze voor bepaalde vormen van centrale opslag van gegevens nader te toe te lichten. Dit advies is opgevolgd. Op verschillende punten wordt in de aangepaste toelichting uitgebreider ingegaan op de regels die op grond van dit besluit kunnen worden gesteld en op de keuze voor centrale opslag van gegevens. Verder adviseert de AP in de nota van toelichting in te gaan op de verhouding van het gekozen betrouwbaarheidsniveau «laag» als basis tot de tendens om hogere betrouwbaarheidsniveaus te eisen. Dit advies is ook opgevolgd. In de toelichting is de tekst verduidelijkt, waardoor de onduidelijkheid die de AP constateert wordt weggenomen.

De AP adviseert verder om in de nota van toelichting in te gaan op concrete maatregelen met het oog op het vertrouwelijk behandelen van de persoonsgegevens, dan wel, zo nodig, het concept aan te passen. Dit advies is ook overgenomen. In de toelichting wordt ingegaan op de verplicht te nemen maatregelen om persoonsgegevens te beschermen, zoals het scheiden van gegevens en het gebruik van open source-software.

De AP adviseert ook om gelet op de voorgestelde samenwerkingsplicht te duiden in hoeverre sprake is van gezamenlijke verwerkingsverantwoordelijkheid en hoe deze zich verhoudt tot de verantwoordelijkheid van de

minister van BZK. Dit advies is ook overgenomen. De in het voor advies voorgelegde concept opgenomen samenwerkingsplicht is geschrapt en in de toelichting is verduidelijkt dat partijen onafhankelijk van elkaar gegevens verwerken in afzonderlijke handelingen. Verder is uiteengezet dat niet dit besluit maar het Besluit digitale overheid de verwerking van persoonsgegevens regelt.

Tot slot zijn de artikelen met betrekking tot gebruiksvoorwaarden en meldingsplicht en de daarbij behorende toelichtingen aangepast aan de hand van opmerkingen van de AP.

Het advies van het Adviescollege toetsing regeldruk heeft er onder meer toe geleid dat de regeldrukgevolgen beter en conform de Rijksbrede methodiek in kaart zijn gebracht.

Artikelsgewijs

Artikel 2 Algemene eisen erkende diensten

Deze bepaling bevat de eisen waaraan alle erkende diensten, ongeacht hun rol in het stelsel, moeten voldoen.

De bepaling bevat onder meer eisen aangaande de financiële gezondheid van de erkende dienst. Dit is van belang om te zorgen dat een aanzienlijke mate van zekerheid bestaat dat de middelen, waarvan bedrijven immers afhankelijk zijn voor de toegang tot de digitale dienstverlening van de overheid, beschikbaar zullen zijn en blijven.

Verder is een aantal eisen opgenomen aangaande de organisatie en werkwijze van de erkende diensten. Zo is van belang dat erkende diensten ervoor zorgen dat zij alle gegevens die hen ter kennis komen, vertrouwelijk behandelen. Een betrouwbare toegang van ondernemingen en rechtspersonen tot elektronische dienstverlening valt of staat immers met een organisatie die de haar ter beschikking staande gegevens van derden vertrouwelijk behandelt (tweede lid, onderdeel c). Verder is opgenomen dat de opslag van gegevens van de gebruiker gescheiden wordt van de opslag van gebruiksgegevens (tweede lid, onderdeel d). Op deze wijze wordt de privacy van gebruikers beter beschermd en kunnen de gebruiksgegevens bij een eventuele inbreuk op de beveiliging niet worden gekoppeld aan een bepaalde gebruiker. Dit besluit schrijft voor dat de scheiding met een specifieke handeling moet worden doorbroken, tenzij dat doorbreken plaatsvindt op verzoek van de minister. Het moment waarop een dergelijke handeling wordt verricht moet worden geregistreerd (tweede lid, onderdeel h) en een erkende dienst moet een gebruiker inzage geven in de momenten waarop de scheiding is doorbroken (tweede lid, onderdeel i). Dat maakt zelfcontrole door gebruikers mogelijk.

Tot slot dienen alle erkende diensten te voldoen aan de eisen aangaande beheer en organisatie die zijn opgenomen in paragraaf 2.4 van de bijlage bij de Uitvoeringsverordening (artikel 2, derde lid) en aan de regels die daaromtrent in de ministeriële regeling worden gesteld. Het gaat dan bijvoorbeeld om eisen aangaande informatiebeveiliging, informatievoorziening aan de afnemers van hun diensten of aan de kwaliteit en beschikbaarheid van hun personeel. De eisen in de Uitvoeringsverordening zijn uitgewerkt voor de betrouwbaarheidsniveaus laag, substantieel en hoog. Daarbij worden eerst de eisen benoemd voor betrouwbaarheidsniveau laag; deze eisen worden waar nodig met aanvullende eisen uitgebreid voor niveau substantieel of hoog. Aangezien een authenticatiedienst telkens wordt erkend in relatie met het aangeboden bepaald bedrijfs- en organisatiemiddel, gelden voor deze diensten

uitsluitend de in voornoemde paragraaf 2.4 opgenomen eisen te voldoen voor zover die op het betrouwbaarheidsniveau van het betrokken bedrijfs- en organisatiemiddel van toepassing zijn. De uitwerking van de eisen uit de Uitvoeringsverordening in de ministeriële regeling bevat dan ook met betrekking tot betrouwbaarheid voornamelijk regels die noodzakelijk zijn voor het daadwerkelijk toepassen van de bijlage van de Uitvoeringsverordening in Nederland.

Artikel 3 Inkomsten uit het verstrekken van gegevens of authenticatie

Artikel 2, tweede lid, onderdeel c, 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. Artikel 3 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 erkenningshouder moet deze optie expliciet opnemen in een met de gebruiker te sluiten overeenkomst. Die overeenkomst wordt in het kader van de aanvraagprocedure overgelegd.

Artikel 4 Toepassing van software met openbare broncode

Op grond van dit artikel worden componenten aangewezen waarvoor door aanvragers van een erkenning moet worden voorzien in software met gepubliceerde broncode. Op de beleidsmatige achtergrond wordt ingegaan in hoofdstuk 2 van het algemene deel van deze toelichting. Dit artikel bepaalt dat voor aangewezen componenten van authenticatiediensten en machtigingsdiensten software moet worden gebruikt waarvan de broncode openbaar is. Het kan gaan om software die onder een open source licentie is gepubliceerd (openbaarmaking van de broncode is een onderdeel van deze licenties) of om software waarvan de broncode op andere wijze openbaar is gemaakt. Op grond van het vijfde lid kunnen nadere regels worden gesteld aan de wijze waarop de broncode openbaar wordt gemaakt, bijvoorbeeld wanneer openbaarmaking op andere wijze dan via een open source-licentie plaatsvindt. Uit dit artikel blijkt verder dat de aanwijzing van componenten beperkt blijft tot componenten waarmee persoonsgegevens worden verwerkt.

Het derde lid regelt verder dat, ongeachte op welke wijze publicatie van de broncode plaatsvindt, voor de aangewezen componenten een mogelijkheid moet bestaan voor derden om kwetsbaarheden van de software te melden en om voorstellen te doen voor aanpassing van die software. Daarmee wordt geborgd dat de community die gericht is op het monitoren en verbeteren van de software altijd een kanaal heeft om bevindingen te rapporteren. De aanbieder van een authenticatiedienst of machtigingsdienst is vervolgens gehouden om op deze inbreng te reageren en om terugkoppeling te geven over de gevolgen die daaraan zijn gegeven.

Met de in dit artikel gekozen formuleringen is verder tot uitdrukking gebracht dat telkens zowel de machtigings- als de authenticatieprocessen aan toetsing onderhevig zijn. Het machtigingsproces is immers een wezenlijk onderdeel van het bedrijfs- en organisatiemiddel.

Artikel 5 Eisen erkende authenticatiedienst

Dit artikel legt vast welke rol een authenticatiedienst vervult en bevat de belangrijkste eisen voor het uitoefenen van die rol. Ook hier zijn de eisen uit de Uitvoeringsverordening het uitgangspunt. Het gaat dan om de eisen opgenomen in de in het tweede lid genoemde paragrafen uit de bijlage, voor zover die betrekking hebben op de uitgifte, het ontwerp (inclusief de productie en de distributie) en het authenticatiemechanisme van het bedrijfs- en organisatiemiddel met betrekking waartoe de betrokken authenticatiedienst erkend is (of wenst te worden). Aangezien de betrouwbaarheid van een middel vooral wordt bepaald door de uitgifte en het ontwerp van dat middel, zijn de aan die uitgifte, aan het ontwerp en aan het authenticatiemechanisme gerelateerde eisen uit de Uitvoeringsverordening op hem en zijn middel van toepassing. Ook hier geldt dat een authenticatiedienst aan deze eisen moet voldoen op het betrouwbaarheidsniveau van het bedrijfs- en organisatiemiddel waarvoor hij erkend is.

Paragraaf 2.3 van de Uitvoeringsverordening ziet op het authenticatiemechanisme. Ook met betrekking tot die eisen kunnen bij ministeriële regeling nadere eisen worden gesteld. Het gaat daarbij bijvoorbeeld om eisen voor de beveiliging van het authenticatiemechanisme.

Bij ministeriële regeling worden op grond van artikel 7, tweede lid, van dit besluit nadere eisen gesteld aan de uitgifte en het ontwerp van de bedrijfs- en organisatiemiddelen en het authenticatiemechanisme dat het middel gebruikt.

Artikel 6 Eisen erkende machtigingsdienst

Een erkende machtigingsdienst is het aanspreekpunt voor dienstverleners. Een machtigingsdienst ontvangt een verzoek om een machtigingsverklaring van een dienstverlener. In een dergelijke verklaring wordt bevestigd dat een natuurlijk persoon bevoegd is namens een onderneming of rechtspersoon toegang te krijgen tot door die onderneming of rechtspersoon bepaalde elektronische dienstverlening. Om een dergelijk verzoek te kunnen afhandelen vraagt de machtigingsdienst een authenticatiedienst om de identiteit van de gebruiker te bevestigen. De machtigingsdienst koppelt deze informatie aan de informatie in het machtigenregister over de bevoegdheden van de desbetreffende persoon om te handelen namens een bedrijf of organisatie.

Eerste lid, onderdeel a

Het is aan de machtigingsdienst om op verzoek een machtiging vast te leggen van natuurlijke persoon om te handelen namens een onderneming of rechtspersoon. Een verzoek om een dergelijke machtiging te registreren kan in beginsel uitsluitend worden gedaan door een ingevolge het handelsregister aangegeven wettelijke vertegenwoordiger van de onderneming of rechtspersoon.

Eerste lid, onderdeel b

Een machtigingsdienst verzoekt een authenticatiedienst om een authenticatieverklaring om de identiteit te bevestigen van degene op wie het machtingsverzoek ziet. Dat is een taak van de machtigingsdienst. De machtigingsdienst die het verzoek heeft gedaan ontvangt ook de authenticatieverklaring van de authenticatiedienst.

Eerste lid, onderdeel c

Op basis van de informatie die de machtigingsdienst heeft geregistreerd over bevoegdheden en de authenticatieverklaring wordt de machtigingsverklaring opgesteld en verzonden aan de dienstverlener. Een alternatief is het geval waarin een bedrijf handelt namens een ander bedrijf. In dat geval kan het nodig zijn dat de machtigingsdienst aan een andere machtigingsdienst een machtingsverklaring moet vragen om te bevestigen dat de organisatie waarvoor de gebruiker handelt inderdaad gemachtigd is om te handelen namens het bedrijf waarvoor de handeling moet worden verricht.

Artikel 7 Aanvullende eisen erkende diensten en bedrijfs- en organisatiemiddelen

Eerste lid

In het eerste lid van dit artikel zijn algemene eisen opgenomen die gelden voor bedrijfs- en organisatiemiddelen. Onderdeel a van dit artikellid bepaalt dat een middel voor zover nodig moet functioneren met de generieke digitale infrastructuur. Voor zover een specifiek middel ook gebruikt maakt van andere voorzieningen moet ook daarvan kunnen worden aangetoond dat het middel met die voorziening kan functioneren.

Op grond van artikel 11, achtste lid, onderdeel b en d, van de wet wordt een aanvraag afgewezen wanneer niet is voldaan aan het vereiste van «privacy by design» en wanneer voor aangewezen onderdelen van een identificatiedienst, machtigingsdienst of identificatiemiddel geen gebruik wordt gemaakt van software die onder een open source licentie is gepubliceerd of waarvan de broncode openbaar is. Uit onderdeel c van het eerste lid van artikel 7 van dit besluit volgt dat deze eisen niet enkel van toepassing zijn tijdens de toelatingsprocedure, maar ook na verlening van een erkenning.

Uit artikel 2, 5 en 6 van dit besluit volgt dat op erkende diensten de bij de Uitvoeringsverordening gestelde eisen ook van toepassing zijn binnen het Nederlandse stelsel. Deze eisen kunnen worden aangevuld bij ministeriële regeling, het tweede lid van dit artikel biedt daarvoor een grondslag.

Het tweede lid

In het tweede lid zijn de onderwerpen genoemd ten aanzien waarvan in ieder geval bij ministeriële regeling nadere regels worden gesteld. De onderdelen a tot en met h maken het mogelijk aanvullende regels op te stellen over de onderwerpen waarop de Uitvoeringsverordening ziet. Onderdeel i ziet op de beveiliging van die processen.

j. Periodieke controle van gegevens

Voor een betrouwbaar authenticatiesysteem zijn actuele gegevens van belang. Op grond van dit onderdeel kunnen regels worden gesteld over periodieke controles. 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.

k. Te gebruiken voorzieningen

Op grond van dit onderdeel kunnen erkende diensten bijvoorbeeld worden verplicht gebruik te maken van bepaalde technologie, bijvoorbeeld voor het herkennen en herleiden van misbruik.

l. Integriteit en kwalificaties van personeel en bestuur

Op grond van dit onderdeel kan bijvoorbeeld worden voorgeschreven dat personeel dat betrokken is bij processen waarbij persoonsgegevens kunnen worden herleid, moet beschikken over een verklaring omtrent het gedrag.

m. Bestrijding misbruik

In dit kader kan aan verschillende vormen van misbruik worden gedacht. Daarbij kan gedacht worden aan identiteitsfraude, waarbij een legitiem middel door iemand wordt gebruikt die niet gerechtigd is om met dat middel toegang tot elektronische dienstverlening te verkrijgen.

Teneinde dergelijk misbruik zoveel mogelijk te voorkomen en de gevolgen daarvan voor de gebruiker zoveel mogelijk te beperken is het bijvoorbeeld van belang dat gebruik dat kan duidelijk op mogelijk misbruik kan worden herkend en hersteld. Dit is het herstelvermogen. Bij ministeriële regeling worden daaromtrent nadere regels gesteld. Voorbeelden van deze regels zijn een verplichting om faciliteiten in te richten ten behoeve van het monitoren van afwijkende gebruikspatronen die erop wijzen dan gebruikers slachtoffer zijn van identiteitsfraude en het nemen van maatregelen om het te stoppen, een meldingsplicht voor vermoedens van misbruik, en een verplichting om mee te werken aan een onderzoek naar misbruik.

n. Verwerking van persoonsgegevens

Bij regels rond de verwerking van persoonsgegevens, waarvoor onderdeel n een basis biedt, kan bijvoorbeeld ook worden gedacht aan nadere eisen, zoals verwijderen van verwerkte gegevens als het bewaren daarvan niet meer nodig is voor de doeleinden zoals beschreven in het Besluit digitale overheid, of de verplichte versleuteling waardoor bijvoorbeeld het BSN van gebruikers zoveel mogelijk versleuteld wordt verwerkt. Dergelijke eisen zullen ook gebaseerd zijn op open standaarden en ondersteund worden door gangbare, open softwarebibliotheken.

o. Gebruiksvriendelijkheid

Behalve betrouwbaarheid is het noodzakelijk dat de middelen in dat stelsel gebruiksvriendelijk zijn. Onderdeel o biedt een basis voor het stellen van regels over dit onderwerp, bijvoorbeeld over de mogelijkheid om een identificatiemiddel op eenvoudige wijze te registreren, door een reeds verstrekt middel te gebruiken om daarvan een ander middel af te leiden.

Het derde lid

Interoperabiliteit met en aansluiten op GDI-voorzieningen

Op grond van artikel 5, eerste en tweede lid, van de wet is de minister verantwoordelijk voor het verzorgen van de in die leden genoemde voorzieningen. Een aantal van die voorzieningen is noodzakelijk voor de goede werking van het stelsel. Op grond van artikel 2, tweede lid,

onderdeel f, van dit besluit kunnen regels worden gesteld over het verplicht aansluiten op en de interoperabiliteit met deze voorzieningen.

Zo wordt in artikel 5, eerste lid, onderdeel d, van de Wdo een voorziening genoemd die het mogelijk maakt dat de identiteit van een natuurlijke persoon, onderneming of rechtspersoon die een elektronische dienst afneemt bij een bestuursorgaan of aangewezen organisatie op unieke wijze geïdentificeerd kan worden. Deze voorziening wordt ook wel het BSN-Koppelregister (BSN-K) genoemd. Bij de uitgifte van een bedrijfs- en organisatiemiddel aan een natuurlijk persoon kan het wenselijk zijn dat ook van dit BSN-k gebruik kan worden gemaakt. In dat geval is het wenselijk dat regels kunnen worden gesteld aan de erkende diensten die van dat BSN-k gebruik maken, bijvoorbeeld aangaande het door hen te hanteren koppelvlak. Dit derde lid biedt daar de grondslag voor.

Een ander voorbeeld is de voorziening die dient ter implementatie van de eIDAS-verplichtingen. Ingevolge artikel 5, tweede lid, van de Wdo draagt de minister zorg voor een voorziening die het uitgaande en inkomende elektronisch verkeer tussen Europese lidstaten mogelijk maakt, voor zover daarbij gebruik wordt gemaakt van elektronische identificatiemiddelen die onderdeel zijn van een bij de Europese Commissie aangemeld en goedgekeurd stelsel. Elke lidstaat dient ingevolge de eIDAS-verordening deze genotificeerde elektronische identificatiemiddelen in beginsel te accepteren. De interoperabiliteit van erkende diensten met deze voorziening kan ook op grond van het derde lid van artikel 7 worden geregeld.

Het vierde lid

Het vierde lid betreft de gebruiksvoorwaarden van de authenticatiedienst en de machtigingsdienst die zij hanteren bij de afnemers van hun diensten. Alleen authenticatiediensten en machtigingsdiensten zullen dergelijke gebruiksvoorwaarden gebruiken, omdat zij een commerciële relatie met hun afnemers (de gebruikers) zullen hebben. Bij ministeriële regeling wordt bepaald welke inhoud in deze gebruiksvoorwaarden in ieder geval moet worden opgenomen.

Het zesde lid

Tot slot bevat de bepaling een grondslag om bij ministeriële regeling regels te stellen over het minimale niveau van dienstverlening door de erkende diensten. In dit kader kan gedacht worden aan niet-functionele eisen zoals beschikbaarheid en responsetijden waarin de gebruikerservaring centraal staat. Het moet bijvoorbeeld niet 10 minuten duren om in te loggen bij een dienstverlener doordat een authenticatiedienst onvoldoende is toegerust.

Het zevende lid

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. 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 zevende lid van artikel 7 maakt dat mogelijk.

Artikel 8 Meldingsplicht

Eerste lid, onderdeel a

Een erkenning wordt verleend voor de dienst en het identificatiemiddel waarop de aanvraag ziet. Wanneer de werking van de dienst ingrijpend wordt gewijzigd is een wijziging van de erkenning nodig. Met dit onderdeel wordt geregeld dat in andere gevallen een melding moet worden gedaan van de door te voeren wijzigingen.

Eerste lid, onderdeel b

Op grond van de wet kan een Bibob-advies worden gevraagd over een aanvraag. Bij een dergelijke toets wordt onder meer de zeggenschapsstructuur van de aanvrager getoetst. Indien na het verlenen van een erkenning wijzigingen optreden in die zeggenschapsstructuur moet daarvan een melding plaatsvinden op grond van dit onderdeel.

Eerste lid, onderdeel c

Een incident of storing bij een erkende dienst kan de betrouwbaarheid van het gehele stelsel in het geding brengen. Het is dan ook van belang dat een erkende dienst een incident of verstoring die van zodanige aard is dat deze betrouwbaarheid in het geding komt, dient te melden bij de minister. Daartoe verplicht onderdeel c van het eerste lid van artikel 8. De minister kan dan waar nodig gebruik maken van zijn wettelijke bevoegdheden om de gevolgen in te perken.

Tweede lid

Daar waar een incident of storing zeer waarschijnlijk negatieve gevolgen heeft voor andere erkende diensten of gebruikers van het betrokken bedrijfs- en organisatiemiddel, brengt de erkende dienst ook die erkende dienst(en) en/of gebruikers op de hoogte. Dit is vergelijkbaar met de omvang van de meldplicht uit artikel 19 van de eIDAS-verordening voor vertrouwensdiensten. Het is dus niet per sé nodig om alle erkende diensten of gebruikers te informeren. Dit zal van het incident of de verstoring af hangen (artikel 8, tweede lid).

Derde lid

Bij ministeriële regeling worden nadere regels gesteld over de incidenten of verstoringen die in elk geval op grond van dit artikel gemeld moeten worden, de wijze waarop en de termijn waarbinnen een melding moet worden gedaan.

Artikel 9 Uitvoeren van onafhankelijk onderzoek

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 dergelijke verplichting 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 11 Beschrijving van de dienstverlening

Op grond van artikel 11 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 het gebruik van software met een openbare broncode. Deze maatregel is onderdeel van een breder pakket aan maatregelen die wordt ingezet om het gebruik van open source software te doen toenemen.

Artikel 12 De erkenning en de aanvraag om erkenning

Om erkend te kunnen worden moet een aanvraag worden ingediend. Bij de aanvraag moet de betrokken rechtspersoon bewijsstukken overleggen op basis waarvan kan worden beoordeeld dat hij voldoet of kan voldoen aan de in hoofdstuk 2 van dit besluit voor de aangevraagde erkende dienst gestelde eisen. Een aantal van deze eisen hebben betrekking op de uitoefening van de activiteiten. Dat daadwerkelijk aan die eisen wordt voldaan, kan pas bij het uitoefenen van die activiteiten worden aangetoond. Maar bij erkenning moet wel beoordeeld kunnen worden in hoeverre de aanvrager in staat is om na erkenning aan die eisen te voldoen.

Zo is de goede werking en interoperabiliteit van bijvoorbeeld een machtigingsdienst feitelijk pas zichtbaar zodra die beschikbaar is in de productieomgeving. Teneinde toch te kunnen beoordelen of die werking en interoperabiliteit dan plaats zal vinden overeenkomstig de eisen, ligt het voor de hand om een testfase te doorlopen. In geval deze testfase goed is doorlopen, kan omtrent de goede werking en interoperabiliteit ten behoeve van erkenning een verklaring worden afgegeven.

Bij de aanvraag voegt de aanvrager in principe alle bewijsstukken toe die nodig zijn om te beoordelen dat aan de gestelde eisen voldaan wordt of kan worden voldaan. Bij ministeriële regeling kunnen nadere eisen gesteld worden aan de bij de aanvraag te voegen bewijsstukken. Te denken valt aan het voorschrijven van specifieke documenten, zoals een bankverklaring of een afschrift van een aansprakelijkheidsverzekeraar. Maar 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. Het overleggen van bijvoorbeeld een afschrift van een aansprakelijkheidsverzekering is dan onnodig indien een dergelijk afschrift al bij een eerder verzoek om erkenning is overgelegd en van voldoende recente datum is. Aangezien de ministeriële regeling voor wat betreft de procedure van het indienen van een aanvraag tot erkenning vooral een uitwerking betreft van administratieve voorschriften, is delegatie aan de minister mogelijk.

Gelet op de technische aard van de eisen die nader zullen worden uitgewerkt bij ministeriële regeling, is ervoor gekozen ook een conformiteitsbeoordeling te eisen. De aanvrager moet een certificaat en het onderliggende auditrapport overleggen. Het certificaat levert in combinatie met andere bij de aanvraag aan te leveren rapportages een bewijsvermoeden op dat voldaan wordt aan een aantal van de gestelde eisen. Uiteindelijk is het aan de minister van Binnenlandse Zaken en Koninkrijksrelaties om te bepalen of de erkenning kan worden verleend.

Ook de uit het Besluit digitale overheid voor de erkende diensten volgende eisen aangaande gegevensbescherming kunnen bij ministeriële regeling als te auditen eisen worden aangewezen. Te denken valt aan eisen aan de organisatie of aan de bedrijfsprocessen, waarmee moet

worden geborgd dat aan de uit het Besluit digitale overheid volgende bewaartermijnen wordt voldaan.

Voorts is vereist dat bij de aanvraag inzicht wordt verschaft in de wijze waarop de zeggenschap in de rechtspersoon is georganiseerd. Dit houdt verband met de in artikel 11, achtste lid, van de Wdo opgenomen mogelijkheid voor de minister om in geval van zwaarwegende redenen de erkenning te weigeren. Daarvan kan sprake zijn indien de zeggenschap in handen is bij natuurlijke of rechtspersonen ten aanzien waarvan het gerechtvaardigde vermoeden is ontstaan dat zij de erkenning voor oneigenlijke doelstellingen zullen gebruiken. Het kan daarbij gaan om strafbare activiteiten, maar ook om zeggenschap die in handen is bij vreemde mogendheden.

Artikel 15 Beslistermijn

Eerste lid

Dit artikel regelt de beslistermijn de termijn waarbinnen een erkennings-aanvraag moet worden afgehandeld. Daarvoor geldt in het algemeen aan termijn van twaalf weken. Die termijn is gekozen vanwege de complexiteit van de materie, de aard en omvang van de documentatie bij een aanvraag, de noodzaak van fysieke inspecties en het belang van het toelatingsproces voor een veilig en betrouwbaar stelsel.

Tweede lid

Aanvragen voor erkenningen voor identificatiemiddelen voor natuurlijke personen worden gelijktijdig en door dezelfde personen behandeld, omdat de materie overeenkomt. In de eerste periode waarin aanvragen kunnen worden ingediend worden veel aanvragen verwacht. Het gaat dan om de periode vanaf het moment waarop aanvragen kunnen worden ingediend, tot het moment waarop de termijn bedoeld in artikel 24 van de wet afloopt. De laatstgenoemde termijn bepaalt dat partijen die op het moment van het inwerkingtreden van artikel 24 van de wet deel uitmaken van het huidige eHerkenningsafsprakenstelsel vanaf dat moment van inwerkingtreding gedurende 18 maanden worden beschouwd als erkende partijen. De termijn is bedoeld om een soepele overgang te borgen voor huidige aanbieders die hun activiteiten onder de Wdo willen blijven voortzetten. De 18 maanden kunnen worden gebruikt om een erkenning te verkrijgen via de aanvraagprocedure. In de periode vanaf het inwerking-treden van de artikelen over de aanvraagprocedure en het aflopen van de overgangstermijn kunnen zowel nieuwe aanbieders als bestaande partijen een erkenningsaanvraag indienen. Gelet op de grote hoeveelheid te verwachten aanvragen, de nieuwe materie, regelgeving en procedure en het feit dat de kennis die nodig is voor het afhandelen van deze aanvragen voor een aanzienlijk deel niet tijdelijk kan worden aangetrokken, wordt voor deze periode een langere behandeltermijn gehanteerd van 18 weken.

Derde lid

Op grond van artikel 28 van de Dienstenwet wordt een erkenning 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 burgers. Met het uitvoeren van een beoordeling van een identificatiemiddel voor burgers worden burgers beschermd. Met het van rechtswege verlenen van de erkenning, zonder die beoordeling, wordt het belang van burgers op onaanvaardbare wijze

geschaad. Daarom wordt met artikel 15, derde lid, bepaald dat de vergunning niet van rechtswege wordt verleend.

Artikel 16 Certificaat van conformiteit

Zoals bij artikel 12 van dit besluit is toegelicht moet bij de aanvraag om erkenning een certificaat van conformiteit, inclusief het daarbij behorende auditrapport worden overgelegd. Het is in dat kader dan ook van belang dat erkende diensten te allen tijde beschikken over een geldig certificaat van conformiteit (artikel 10). In hoofdstuk 3 van het algemene deel van deze toelichting wordt uitgebreid ingegaan op het vereiste certificaat.

Artikel 17 Intrekking van een erkenning op verzoek van erkenninghouder

Een houder van een erkenning is gehouden het middel daadwerkelijk aan te bieden en te borgen dat het middel beschikbaar is voor gebruikers. 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 gebruikers 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 het intrekkingsbesluit wordt genomen. De minister van Binnenlandse Zaken en Koninkrijksrelaties bepaalt dit moment en houdt daarbij rekening met het voorstel van de aanvrager.

De intrekking van de erkenning gaat in op een moment dat wordt bepaald aan de hand van het intrekkingsverzoek. 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.

Artikel 18 Ambtshalve intrekking of schorsing

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 18 de aan die partij

verleende erkenning intrekken of schorsen om het belang van veilig en betrouwbare toegang tot publieke dienstverlening te borgen.

Artikel 19 Wijziging van een erkenning

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 20 Advies Bureau Bibob over wijziging, schorsing of intrekking

Artikel 14, derde 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 11, vijfde 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 21 Eisen voor partijen tijdens overgangstermijn

Artikel 24 van de wet bepaalt dat de partijen die op het moment van inwerkingtreding van dat artikel deelnemen aan het publiek/private stelsel eHerkenning gedurende 18 maanden geacht worden te zijn erkend. Deze overgangstermijn is bedoel om de continuïteit van de bruikbaarheid van de desbetreffende middelen te faciliteren. Dat gebeurt enerzijds door partijen in de gelegenheid te stellen om het aanvraagproces te doorlopen terwijl de middelen nog kunnen worden gebruikt en anderzijds door partijen tijdens die periode in de gelegenheid te stellen om te voldoen aan de eisen die op grond van de wet gelden voor erkende partijen.

Als gevolg van artikel 24 van de wet zijn de rechten en plichten die de wet aan een erkenning verbindt ook op die partijen van toepassing. Zo mogen deze partijen bijvoorbeeld op grond van artikel 24 van de wet in combinatie met artikel 16, derde lid van de wet persoonsgegevens, waaronder het burgerservicenummer, verwerken voor zover dat noodzakelijk is voor de goede werking van een bedrijfs- en organisatiemiddel. Dit artikel maakt het mogelijk om bij ministeriële regeling een fasering mogelijk te maken, waarbij bepaalde eisen gedurende de overgangstermijn van 18 maanden voor de desbetreffende partijen gaan gelden.

Gedurende de overgangstermijn worden de partijen waarop artikel 24 van de wet ziet van rechtswege geacht te zijn erkend. In het kader van een deugdelijke regie op het stelsel is het noodzakelijk zicht te hebben op de partijen die hun diensten aanbieden binnen het stelsel. Daarom wordt het mogelijk gemaakt om aan deze partijen nadere eisen op te leggen.

Gedacht kan worden aan een meldingsplicht waarmee kan worden geborgd dat duidelijk is welke partijen hun van rechtswege ontstane erkenning actief zullen gaan gebruiken.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,
A.C. van Huffelen