**Besluit van ……. , 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 ……, nr. ……..;

Gelet op de artikelen 11, eerste, tweede, derde en vijfde lid, en 13, eerste, vierde en vijfde lid, en 22 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. Begripsbepalingen**

**Artikel 1**

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

- *certificaat van conformiteit;* certificaat, afgegeven door een conformiteitsbeoordelingsinstantie, op grond waarvan een gerechtvaardigd vermoeden bestaat dat een erkende dienst voldoet aan de toepassing zijnde certificatie-eisen;

- *certificatie-eisen:* bij of krachtens hoofdstuk 2 en hoofdstuk 4 gestelde eisen, voor zover die eisen bij ministeriële regeling als certificatie-eisen zijn aangewezen;

- *conformiteitsbeoordelingsinstantie*: door Onze Minister op grond van artikel 13 aangewezen instantie;

- *gebruiker:* rechtspersoon of onderneming die gebruik maakt van een identificatiemiddel en die een overeenkomst heeft gesloten met de aanbieder van dat middel;

- *machtigingsverklaring*: door een erkende machtigingsdienst elektronisch afgegeven verklaring, waaruit blijkt dat een 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 erkende dienst is 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 heeft zijn statutaire zetel, zijn hoofdbestuur of zijn hoofdvestiging binnen de Europese Economische Ruimte.
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 gegevens die hem in het kader van de diensten waarvoor hij erkend is ter kennis komen vertrouwelijk worden behandeld;
   d. beschikt over een loket voor vragen of meldingen aangaande ontstane problemen in de toegang van ondernemingen en rechtspersonen tot elektronische dienstverlening; en
   e. verwerkt gegevens over een gebruiker van een identificatiemiddel op een wijze die is afgescheiden van gegevens over het gebruik van dat middel door die gebruiker.
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. Een erkende middelenuitgever of een erkende authenticatiedienst voldoet slechts aan deze eisen op het betrouwbaarheidsniveau van het bedrijfs- en organisatiemiddel waarvoor hij erkend is.

### Artikel 3 Aanvullende eisen erkende diensten

1. Bij ministeriële regeling worden voor erkende diensten aanvullende eisen gesteld, die per erkende dienst als bedoeld in artikel 11, eerste tot en met derde lid, van de wet, kunnen verschillen en die betrekking hebben op:
   a. de bestrijding van misbruik van en met bedrijfs- en organisatiemiddelen;
   b. de interoperabiliteit met de voorziening, bedoeld in artikel 5, tweede lid, van de wet;
   c. de organisatorische of technische inrichting aangaande de op grond van het Besluit digitale overheid toegestane verwerking van persoonsgegevens;
   d. de verankering van een betrouwbaar spoor van controleerbare vastleggingen van door de erkende dienst verrichte essentiële handelingen inzake elk gebruik van een bedrijfs- en organisatiemiddel in de toegang van ondernemingen en rechtspersonen tot elektronische dienstverlening, zodanig dat deze handelingen achteraf herleid kunnen worden.
2. Bij ministeriële regeling kunnen per erkende dienst als bedoeld in artikel 11, eerste tot en met derde lid, van de wet, aanvullende eisen worden gesteld, die betrekking hebben op de interoperabiliteit met onderdelen van de infrastructuur, bedoeld in artikel 5, eerste lid, van de wet.
3. Bij ministeriële regeling worden regels gesteld over de voorwaarden die door een erkende middelenuitgever en een erkende machtigingsdienst in elk geval worden opgenomen in de gebruiksvoorwaarden die zij stellen aan de gebruikers van hun diensten. Deze voorwaarden hebben in ieder geval betrekking op het voorkomen van verlies, diefstal, misbruik of verspreiding van het bedrijfs- en organisatiemiddel.
4. 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.
5. Bij ministeriële regeling worden nadere eisen gesteld aan het minimale niveau van dienstverlening door de erkende diensten en daarbij te hanteren prestatie-indicatoren inzake de beschikbaarheid.

### Artikel 4 Eisen erkende middelenuitgever

1. Een erkende middelenuitgever draagt zorg voor de betrouwbare uitgifte van het bedrijfs- en organisatiemiddel waarvoor hij is erkend. Daartoe draagt hij er zorg voor dat het uitgifteproces en het ontwerp van het bedrijfs- en organisatiemiddel voldoen aan de op dat proces en het ontwerp

betrekking hebbende eisen die zijn opgenomen in de bijlage bij de Uitvoeringsverordening (EU) 2015/1502 en de dienaangaande bij ministeriële regeling gestelde eisen, 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 kenmerken en het ontwerp van elektronische identificatiemiddelen, opgenomen in paragraaf 2.2.1. van die bijlage;

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

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

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

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

Artikel 2, derde lid, laatste zin, is van overeenkomstige toepassing.

2. Een erkende middelenuitgever draagt zorg voor een voor de gebruiker van het door hem uitgegeven erkende bedrijfs- en organisatiemiddel kenbaar proces van intrekking of schorsing van het bedrijfs- en organisatiemiddel in de situatie dat de betrouwbaarheid of het gebruik van dat middel in het geding is en tevens voor een duidelijke beschrijving van de wijze waarop de erkende middelenuitgever er zorg voor draagt dat de toegang van de gebruiker tot elektronische dienstverlening geborgd blijft of zo spoedig mogelijk door de middelenuitgever hersteld wordt.

3. Een erkende middelenuitgever die niet tevens erkend is als authenticatiedienst beschikt over een rechtsgeldige overeenkomst met een erkende authenticatiedienst waaruit volgt dat deze authenticatiedienst verantwoordelijk is voor authenticatie met het erkende bedrijfs- en organisatiemiddel waarvoor de middelenuitgever is erkend.

**Artikel 5 Eisen erkende authenticatiedienst**

1. Een erkende authenticatiedienst draagt zorg voor een betrouwbare authenticatie ter bevestiging van de identiteit van een natuurlijk persoon, die voor de toegang tot elektronische dienstverlening namens een onderneming of rechtspersoon een erkend bedrijfs- en organisatiemiddel gebruikt. Daartoe draagt hij in elk geval zorg voor een authenticatiemechanisme waarmee authenticatie op betrouwbare wijze kan plaatsvinden en dat voldoet aan de voor het betrouwbaarheidsniveau van dat bedrijfs- en organisatiemiddel gestelde eisen aangaande authenticatie, opgenomen in paragraaf 2.3 van de bijlage bij de Uitvoeringsverordening (EU) 2015/1502. Bij ministeriële regeling kunnen hieromtrent nadere regels worden gesteld. Artikel 2, derde lid, laatste zin, is van overeenkomstige toepassing.

2. Een erkende authenticatiedienst die niet tevens erkend is als middelenuitgever beschikt over een rechtsgeldige overeenkomst met een erkende middelenuitgever waaruit volgt dat de authenticatiedienst verantwoordelijk is voor authenticatie met het erkende bedrijfs- en organisatiemiddel waarvoor die middelenuitgever is erkend.

3. Een erkende authenticatiedienst voorziet uitsluitend in authenticatie ter bevestiging van de identiteit van een natuurlijk persoon indien daartoe gebruik wordt gemaakt van een bedrijfs- en organisatiemiddel met betrekking waartoe hij als middelenuitgever is erkend of, indien hij niet tevens is erkend als middelenuitgever, een bedrijfs- en organisatiemiddel met betrekking waartoe de middelenuitgever is erkend waarmee hij een rechtsgeldige overeenkomst heeft als bedoeld in het tweede lid.

**Artikel 6 Eisen erkende ontsluitende dienst**

1. Een erkende ontsluitende dienst draagt zorg voor het technisch en functioneel aansluiten van bestuursorganen en aanwezen organisaties, voor zover hij daarmee een overeenkomst hieromtrent heeft gesloten, op iedere erkende authenticatiedienst en iedere erkende machtigingsdienst en daarmee voor de toegang van ondernemingen en rechtspersonen tot hun elektronische dienstverlening, voor zover daarbij gebruik wordt gemaakt van erkende bedrijfs- en organisatiemiddelen. Daartoe fungeert hij als tussenpersoon tussen de betrokken bestuursorganen en aangewezen organisaties en de erkende diensten en draagt hij er zorg voor dat de verzochte authenticatieverklaring of machtigingsverklaring en de berichten daaromtrent doorgegeven worden.

2. Een erkende ontsluitende dienst voldoet tevens aan de voor die dienst in paragraaf 2.3 van de bijlage bij de Uitvoeringsverordening (EU) 2015/1502 aangaande authenticatie gestelde eisen. Bij ministeriële regeling kunnen hieromtrent nadere regels worden gesteld.
3. Een erkende ontsluitende dienst informeert de overige erkende diensten over de bestuursorganen of aangewezen organisaties waarmee hij een overeenkomst als bedoeld in het eerste lid heeft gesloten alsmede over de aangesloten dienstverlening van de bedoelde bestuursorganen of aangewezen organisaties.
4. Erkende ontsluitende diensten werken gezamenlijk aan een uniforme wijze waarop de verzochte authenticatie- of machtigingsverklaringen en berichten daaromtrent worden doorgegeven. Bij ministeriële regeling kunnen voor die uniforme wijze van ontsluiten nadere regels worden gesteld.

**Artikel 7 Eisen erkende machtigingsdienst**

1. Een erkende machtigingsdienst is verantwoordelijk voor:
a. een betrouwbare verificatie van de onderneming of rechtspersoon namens wie de natuurlijke persoon aan wie een erkend bedrijfs- en organisatiemiddel is uitgegeven wenst op te treden;
b. het tot stand brengen van een betrouwbare koppeling tussen het bedrijfs- en organisatiemiddel dat is uitgegeven aan een natuurlijk persoon en de onderneming of rechtspersoon namens wie die natuurlijke persoon wenst te handelen, en
c. de afgifte van betrouwbare machtigingsverklaringen.
2. Ten behoeve van de in het eerste lid genoemde verantwoordelijkheden voldoet een erkende machtigingsdienst aan de eisen opgenomen in de bijlage bij de Uitvoeringsverordening (EU) 2015/1502 en de dienaangaande bij ministeriële regeling gestelde eisen, 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 de elektronische identificatiemiddelen van natuurlijke personen en rechtspersonen, opgenomen in paragraaf 2.1.4 van die bijlage.
3. Een erkende machtigingsdienst brengt uitsluitend een koppeling als bedoeld in het eerste lid, onderdeel b, tot stand op verzoek van een wettelijke vertegenwoordiger van de betrokken onderneming of rechtspersoon of op verzoek van een door die wettelijke vertegenwoordiger gemachtigde en als zodanig in het machtigingsregister van de erkende machtigingsdienst geregistreerde machtigingsbeheerder en overeenkomstig het betrouwbaarheidsniveau waarop die wettelijk vertegenwoordiger of machtigingsbeheerder zelf is geverifieerd en geregistreerd.
4. Een erkende machtigingsdienst geeft uitsluitend elektronische verklaringen af ten behoeve van de toegang van ondernemingen en rechtspersonen als bedoeld in artikel 5 onderscheidenlijk 6 van de Handelsregisterwet 2007 tot elektronische dienstverlening waarbij gebruik wordt gemaakt van een erkend bedrijfs- en organisatiemiddel.
5. Een erkende machtigingsdienst beëindigt de elektronische registratie van de machtiging indien deze wordt ingetrokken door de wettelijk vertegenwoordiger van de betrokken onderneming of rechtspersoon of een door die vertegenwoordiger gemachtigde en als zodanig door de erkende machtigingsdienst geregistreerde machtigingsbeheerder.

**Hoofdstuk 3. Overige verplichtingen erkende diensten**

**Artikel 8 Meldingsplicht**

1. Een erkende dienst meldt onverwijld aan Onze Minister 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. Bij ministeriële regeling worden hieromtrent nader regels gesteld.
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. Een erkende dienst meldt aan Onze Minister elke wijziging van bedrijfsprocessen die van significante invloed is op de uitvoering van de activiteiten waarvoor hij erkend is.

4. Een erkende dienst meldt aan Onze Minister elk voornemen tot zodanige wijziging van de samenstelling van het bestuur van zijn rechtspersoon of de zeggenschapsverhouding van zijn rechtspersoon, dat de zeggenschap over de rechtspersoon geheel of gedeeltelijk door of tezamen met een derde wordt uitgeoefend, dan wel waardoor deze derde daartoe feitelijk in de gelegenheid wordt gesteld.
5. Bij ministeriële regeling kunnen nadere regels worden gesteld ter invulling van de meldingsplicht.

**Artikel 9 Samenwerkingsplicht**

1. Een erkende dienst is gehouden om ten behoeve van een betrouwbare toegang van ondernemingen en rechtspersonen tot elektronische dienstverlening binnen een bij de erkenning te bepalen termijn afspraken te maken met andere erkende diensten te sluiten of toe te treden tot bestaande afspraken tussen erkende diensten. Deze afspraken bevatten voorwaarden voor een betrouwbare interoperabiliteit en continuïteit van dienstverlening van de erkende diensten, waaronder mede wordt verstaan de procedure voor wijzigingsbeheer en versiebeheer van de functionaliteit.
2. De afspraken bevatten een regeling op basis waarvan iedere nieuwe erkende dienst binnen de voor die dienst gestelde termijn kan toetreden tot de afspraken.
3. Een afschrift van de afspraken of de aangepaste afspraken wordt binnen vier weken na het maken daarvan toegezonden aan Onze Minister.

**Artikel 10 Aanwijzingen**

1. Onze Minister kan een erkende dienst een bindende aanwijzing als bedoeld in artikel 13, vijfde lid, van de wet geven:
   a. naar aanleiding van een incident of verstoring, als bedoeld in artikel 8, eerste lid;
   b. naar aanleiding van een wijziging als bedoeld in artikel 8, derde of vierde lid;
   c. op verzoek van een erkende dienst indien de erkende diensten geen overeenstemming kunnen bereiken over de voorwaarden, bedoeld in artikel 9, eerste lid, of over de toepassing daarvan.
2. Desgevraagd verstrekt een erkende dienst binnen een door Onze Minister te stellen termijn alle noodzakelijke gegevens of verleent de erkende dienst aan Onze Minister alle medewerking, voor zover die relevant is voor de beoordeling van de te geven aanwijzing.
3. Een aanwijzing als bedoeld in het eerste lid, onderdeel a en b, wordt niet gegeven dan nadat Onze Minister de betreffende erkende dienst in de gelegenheid heeft gesteld hieromtrent zijn zienswijze naar voren te brengen.

**Hoofdstuk 4. Aanvraag en conformiteit erkenning**

**Artikel 11 De erkenning en de aanvraag om erkenning**

1. Een erkenning als bedoeld in artikel 11, eerste tot en met 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 vergezeld van:
   a. gegevens waaruit blijkt dat de aanvrager voldoet of na erkenning kan voldoen aan de bij of krachtens hoofdstuk 2 gestelde eisen die op de te erkennen dienst van toepassing zijn; en
   b. een beschrijving van de organisatie van de rechtspersoon en de wijze waarop de zeggenschap daarbinnen is georganiseerd; en
   c. de adresgegevens van een vestiging in Nederland waar kan worden aangetoond dat de erkende dienst voldoet aan de erkenning.
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 elk geval moeten worden verstrekt.

4. Een aanvraag om erkenning wordt afgewezen indien uit de aanvraag blijkt dat de aanvrager niet kan voldoen aan de eisen, gesteld in artikelen 2 en 3.
5. De erkenning wordt verleend voor onbepaalde tijd.
6. Van een besluit tot erkenning doet Onze Minister mededeling in de Staatscourant.
7. 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 12 Certificaat van conformiteit**

1. Erkende diensten beschikken over een geldig certificaat van conformiteit waarvan de afgiftedatum niet meer dan twee jaar in het verleden ligt.
2. Een certificaat van conformiteit gaat vergezeld van een auditrapport, afgegeven door de betrokken conformiteitsbeoordelingsinstantie. Bij ministeriële regeling worden regels gesteld over de gegevens die in dit auditrapport worden opgenomen.
3. Een certificaat van conformiteit dat na intrekking van de aanwijzing van de betrokken conformiteitsbeoordelingsinstantie is afgegeven, wordt niet aangemerkt als een geldig certificaat van conformiteit.
4. Indien Onze Minister kan aantonen dat een certificaat van conformiteit voorafgaand aan de intrekking van de aanwijzing van de betrokken conformiteitsbeoordelingsinstantie, onterecht is afgegeven, wordt dat certificaat niet langer aangemerkt als een geldig certificaat van conformiteit.

**Artikel 13 Aangewezen conformiteitsbeoordelingsinstantie**

1. Onze Minister kan een conformiteitsbeoordelingsinstantie aanwijzen die:
    a. rechtspersoonlijkheid heeft;
    b. niet in staat van faillissement of liquidatie verkeert, noch waarvoor door hem faillissement is aangevraagd;
    c. geen surseance van betaling is verleend, noch waarvoor door hem surseance van betaling is aangevraagd;
    d. onafhankelijk is van de door haar beoordeelde organisaties, processen, diensten of producten;
    e. beschikt over voldoende kennis, deskundigheid en toerusting om de uitvoering van de taken naar behoren te vervullen;
    f. ten behoeve van een getrouwe weergave van de uitvoering en een effectief uitvoeringsproces een zodanige administratie voert dat de juiste, volledige en tijdige vastlegging is gewaarborgd van de gegevens die samenhangen met en betrekking hebben op de uitvoering van haar taken;
    g. verzekerd is tegen wettelijke aansprakelijkheid voor risico's die voortvloeien uit de uitoefening van haar taken;
    h. beschikt over een adequate klachtenregeling, en
    i. geaccrediteerd is 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 de Europese Unie 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) op grond van ISO 17065 voor het door Onze Minister vastgesteld certificatieschema.
2. Met een certificatieschema als bedoeld in het eerste lid, onderdeel i, wordt gelijkgesteld een document dat is vastgesteld in een andere lidstaat van de Europese Unie dan wel in een staat, niet zijnde een lidstaat van de Europese Unie, die partij is bij een daartoe strekkend of mede daartoe strekkend verdrag dat Nederland bindt, en een beschermingsniveau biedt dat naar het oordeel van Onze Minister ten minste gelijkwaardig is aan het beschermingsniveau dat met het vastgestelde certificatieschema wordt geboden.
3. De aanwijzing is niet overdraagbaar.
4. Van een besluit tot aanwijzing doet Onze Minister mededeling in de Staatscourant.

**Artikel 14 Intrekken aanwijzing conformiteitsbeoordelingsinstantie**

Onze Minister kan de aanwijzing van een conformiteitsbeoordelingsinstantie intrekken, indien deze niet meer voldoet aan de in artikel 13, eerste lid, gestelde eisen.

**Hoofdstuk 6. Financiële bepaling**

**Artikel 15 Tarieven**
1. Onze Minister kan een tarief vaststellen voor de diensten en werkzaamheden van een erkende dienst, indien het door de betreffende erkende dienst gehanteerde tarief hoger dan marktconform is.
2. Bij ministeriële regeling worden regels gesteld omtrent de wijze van opleggen en de hoogte van het door Onze Minister vast te stellen tarief van erkende diensten,

**Artikel 16 Doorberekening kosten aanvraag erkenning en toezicht**

Bij ministeriële regeling worden regels gesteld omtrent de hoogte en het opleggen van de heffing van het door Onze Minister vast te stellen tarief ter zake van:
a. de behandeling van een aanvraag tot erkenning als bedoeld in artikel 11 van de wet;
b. het toezicht op de naleving van het bepaalde bij of krachtens artikel 13 van de wet.

**Hoofdstuk 7. Slotbepalingen**

**Artikel 17 Inwerkingtreding**

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

**Artikel 18 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.

De staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

**Nota van Toelichting**

**Algemeen deel**

**1. Aanleiding en uitgangspunten**

De minister van Binnenlandse Zaken en Koninkrijksrelaties (hierna: de minister) heeft de Tweede Kamer toegezegd regelgeving op te stellen met betrekking tot publieke en private identificatiemiddelen die gebruikt kunnen worden bij het verlenen van toegang tot publieke dienstverlening in het publieke domein. Daartoe is de Wet digitale overheid (hierna: Wdo) vormgegeven. Het onderhavige besluit vormt op grond van die wet de nadere uitwerking van het stelsel aangaande bedrijfs- en organisatiemiddelen. Deze middelen worden gebruikt in het kader van de toegang van bedrijven (ondernemingen en rechtspersonen) tot elektronische overheidsdienstverlening. Het besluit stelt regels inzake de erkenning van partijen die elektronische identificatiemiddelen leveren en daarbij betrokken diensten aanbieden. Meer in het bijzonder dient het besluit tot uitvoering van de artikelen 11, eerste, tweede, derde en vijfde lid, en 13, eerste, vierde en vijfde lid, van de Wdo.

Teneinde bedrijven de mogelijkheid te bieden om toegang te verkrijgen tot elektronische dienstverlening in het publieke domein, is eerder door de Minister van Economische Zaken en later de minister, eHerkenning ontwikkeld. eHerkenning is een publiek-private samenwerking, waarbij de inlogmiddelen en onderliggende authenticatie-infrastructuur uitsluitend door toegelaten private partijen worden geleverd. In dat civielrechtelijke stelsel heeft de overheid een kader stellende en toezichthoudende rol. Door middel van deze afgesproken generieke infrastructuur kan een publieke dienstverlener, in geval gebruik wordt gemaakt van een eHerkenningsmiddel, de identiteit en bevoegdheid van de natuurlijke persoon, die stelt namens een onderneming of rechtspersoon op te treden, betrouwbaar vaststellen alvorens persoons- of bedrijfsgebonden informatie uit te wisselen.

Bij de uitwerking van onderhavig besluit bedrijfs- en organisatiemiddel is geborgd dat, uitgaande van (aanvragen om) erkenning van de betrokken partijen, de huidige middelen ook in de toekomst in het publieke domein gebruikt kunnen worden. De Wet digitale overheid heeft betrekking op toegang tot de elektronische dienstverlening van de overheid, maar de bedrijfs- en organisatiemiddelen waarop dit besluit betrekking heeft, kunnen, in tegenstelling tot toegelaten publieke middelen, ook in het private domein worden gebruikt.

Daarnaast is eveneens de eIDAS-verordening en de daarop gebaseerde Uitvoeringsverordening (EU) 2015/1502 (hierna: de Uitvoeringsverordening) van belang. 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 redenen van veiligheid en betrouwbaarheid alsmede om notificatie, en daarmee grensoverschrijdend gebruik van erkende bedrijfs- en organisatiemiddelen mogelijk te maken, vormen deze eisen tevens de basis voor dit besluit.

**2. Het stelsel van bedrijfs- en organisatiemiddelen**

Het kabinet heeft met 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 vertrouwd is. Met het afsprakenstelsel voor elektronische toegangsdiensten is in Nederland een basis gelegd om op eenduidige wijze veilige en betrouwbare uitwisseling van informatie mogelijk te maken voor bedrijven en organisaties. De normen met betrekking tot betrouwbaarheid zijn gebaseerd op de eIDAS-Uitvoeringsverordening 2015/1502. De spelregels om veiligheid te borgen zijn gebaseerd op internationale standaarden en best practices. Het afsprakenstelsel voor elektronische toegangsdiensten is als uitgangspunt genomen voor deze Uitvoeringsverordening, onder andere wat betreft de rollen die private partijen kunnen innemen in het netwerk en de eisen ten aanzien van de veiligheid en betrouwbaarheid van hun dienstverlening.

Het stelsel van bedrijfs- en organisatiemiddelen bestaat uit een netwerk van erkende partijen die een of meer diensten aanbieden ten behoeve van de goede werking van het bedrijfs- en organisatiemiddel en de goede toegang met dat middel tot elektronische dienstverlening van de overheid. Deze diensten zijn de middelenuitgever, de authenticatiedienst, de machtigingsdienst en de ontsluitende dienst. In het netwerk kunnen meer partijen in concurrentie dezelfde dienst aanbieden. Hierdoor ontstaan 'terugvalopties', waardoor het stelsel minder kwetsbaar is voor uitval en de beschikbaarheid en bereikbaarheid van dienstverlening zo goed mogelijk wordt geborgd.

Voor een deugdelijke toegang tot elektronische dienstverlening is het van belang dat de verschillende diensten waar nodig met elkaar samenwerken. Daartoe is in dit besluit een samenwerkingsplicht opgenomen en is de mogelijkheid gecreëerd om nadere eisen te stellen aan de interoperabiliteit tussen bepaalde diensten. Hierdoor maakt het niet uit bij wie een inlogmiddel is verkregen; als onderneming of rechtspersoon kun je inloggen bij alle diensten die op een ontsluitende dienst zijn aangesloten, mits het betrouwbaarheidsniveau van het inlogmiddel minimaal overeenkomt met het vereiste betrouwbaarheidsniveau voor het inloggen. Voor bedrijven zullen naar verwachting verscheidene erkende identificatiemiddelen beschikbaar zijn op de betrouwbaarheidsniveaus laag, substantieel en hoog. Kortom, er is keuzevrijheid.

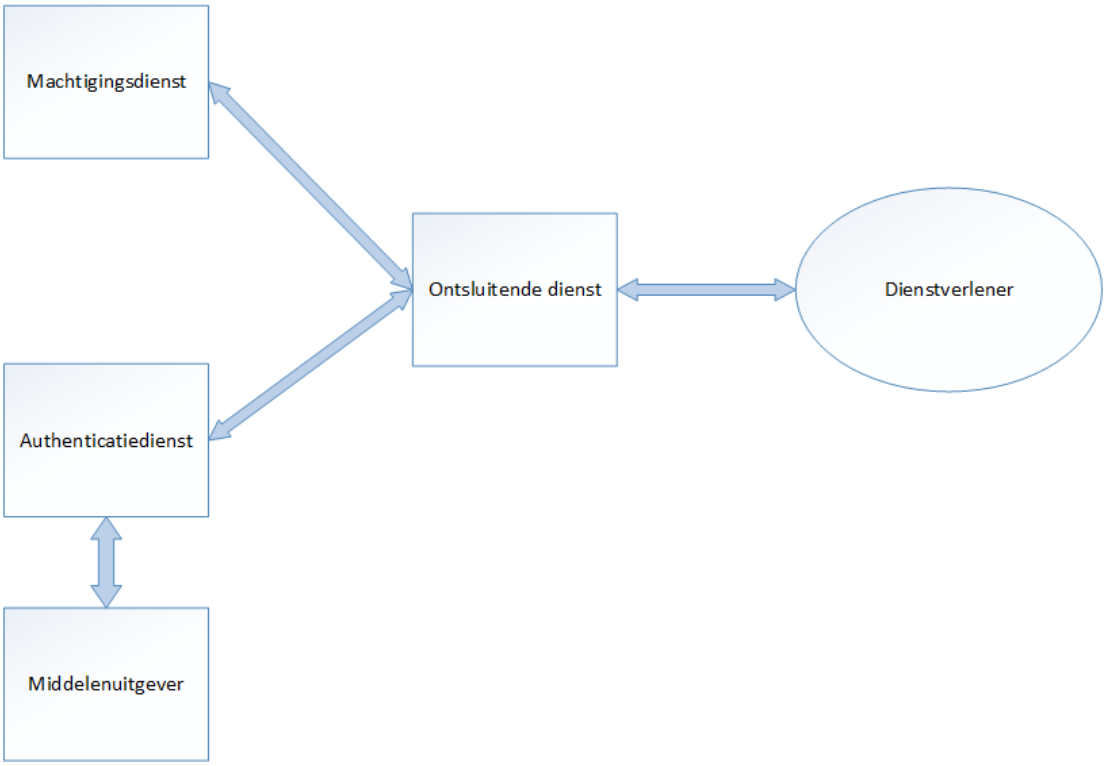
Hieronder volgt een nadere toelichting van de diensten, waarvoor in dit besluit de regels voor erkenning zijn vormgegeven.

De middelenuitgever is verantwoordelijk voor de uitgifte, het beheer en de intrekking van het bedrijfs- en organisatiemiddel waarvoor hij erkend is, alsmede het zorgvuldig vastleggen van alle daarvoor geregistreerde gegevens in een administratie. De middelenuitgever identificeert hiertoe de handelende natuurlijke persoon en levert op verzoek van de authenticatiedienst een verklaring inhoudende dat het inlogmiddel hoort bij die natuurlijke persoon. De activiteit die de middelenuitgever 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 verantwoordelijk voor het authentiseren van personen op basis van hun middel. Het gaat daarbij om het beantwoorden van de vragen 'Wie ben je?' en 'Ben je wie je zegt dat je bent?'. Als de authenticatie is gelukt, stelt de authenticatiedienst een elektronische verklaring op en deelt deze, via de ontsluitende dienst, met de dienstverlener.

De machtigingsdienst registreert en ontsluit de koppeling tussen het inlogmiddel van gemachtigde en de bevoegdheid ('Wat mag je'). Op basis van die gegevens samen kan de machtigingsdienst verklaren aan de dienstverlener voor welke zaken de houder van het middel bevoegd is namens de onderneming of rechtspersoon te handelen.

De ontsluitende dienst vormt de linking pin tussen authenticatiedienst en machtigingsdienst met de dienstverleners en heeft een routeer- en navigatiefunctie in het netwerk. Wanneer een onderneming of rechtspersoon een elektronische dienst wil afnemen en de (gemachtigde) natuurlijke persoon daarbij gebruik maakt van een erkend bedrijfs- en organisatiemiddel, zorgt de ontsluitende dienst dat de authenticatie van de gebruiker bij de erkende authenticatiedienst, die met betrekking tot dat middel is erkend, wordt opgehaald. Ook haalt de ontsluitende dienst de benodigde elektronische verklaring op bij een erkende machtigingsdienst. De ontsluitende dienst draagt de opgehaalde gegevens over aan de dienstverlener die daarmee de dienstverlening kan voortzetten.




*Figuur: diensten en onderlinge relatie*

Naast de bovenstaande onderlinge relaties tussen de erkende diensten bestaat er vanuit het stelsel 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.

## 3. De erkenning

Een partij moet door de minister erkend zijn om diensten ten behoeve van het stelsel te mogen aanbieden. Het proces van erkenning start wanneer een partij daartoe een verzoek richt aan daartoe door de minister aangewezen ambtenaren.

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 door de toezichthouder, die ook bij de verzoekende partij additioneel onderzoek kan verrichten om het bewijs te verifiëren en aan te vullen. Bij een positief oordeel zal de toezichthouder de minister adviseren om de partij te erkennen. Het is voorzien dat Agentschap Telecom het gremium is dat de minister behulpzaam zal zijn.

Bij de aanvraag dient in elk geval een certificaat van conformiteit inclusief het bijbehorende auditrapport te worden overgelegd van een – door de minister aangewezen – conformiteit-beoordelende instantie (CBI). Deze CBI toetst aan een deel van de door de minister gestelde eisen, dit zijn de 'te auditen eisen'. Het gaat dan bijvoorbeeld om eisen over de wijze waarop de middelenuitgever de aanvrager van een identificatiemiddel moet identificeren en registreren alvorens deze het middel krijgt uitgereikt en bijvoorbeeld eisen voor de technische kwaliteit en veiligheid van een identificatiemiddel en het de bijbehorende authenticatiemechanisme.

De toetsing door de CBI vindt plaats in opdracht - en op kosten - van de partij die erkend wil worden. Het certificaat dient tweejaarlijks te worden vernieuwd. De opzet en frequentie van het certificeringsproces is analoog aan de wijze waarop dit voor 'trustservices' (waaronder

PKIoverheid) in het kader van de eIDAS-verordening is geregeld. In essentie betekent dit dat het erkenningscertificaat tweejaarlijks met een volledige audit wordt vernieuwd en dat in de tussenliggende jaren een zogenaamde 'surveillance audit' plaatsvindt.

In dit besluit worden nadere eisen gesteld aan de CBI. In elk geval dient de instantie te zijn geaccrediteerd door de Raad van Accreditatie op grond van een door de minister vast te stellen certificeringsschema. De Raad houdt toezicht op de kwaliteit van het werk van de geaccrediteerde CBI.

**4. De samenwerking tussen en met erkende diensten**

Om te zorgen dat er een goedwerkend netwerk voor bedrijfs- en organisatiemiddelen beschikbaar is, moeten de erkende diensten interoperabel zijn met elkaar. Het moet de gebruiker van het bedrijfsmiddel niet uitmaken of hij een middel heeft van erkende middelenuitgever A, B of C: hij moet met elk erkend middel kunnen inloggen bij een bestuursorgaan of aangewezen organisatie die aangesloten is op een erkende ontsluitende dienst, mits het betrouwbaarheidsniveau van het middel minimaal gelijk is aan het vereiste berouwbaarheidsniveau voor het inloggen.

In het geval veranderingen worden doorgevoerd in het netwerk, door een of meer erkende diensten, is het van belang dat het netwerk goed blijft werken en met andere versies of implementaties interoperabel blijft. Dat is een gezamenlijke verantwoordelijkheid van de erkende diensten. Daarom zal de erkenning een plicht met zich meebrengen om met de andere erkende diensten ten behoeve van de interoperabiliteit en continuïteit van de dienstverlening samen te werken. Het is aan de erkende diensten om deze samenwerking vorm te geven.

Deze samenwerkingsplicht is in artikel 9 vastgelegd. Bij deze samenwerking wordt, indien noodzakelijk, informatie over technische en organisatorische aangelegenheden uitgewisseld tussen de betrokken erkende diensten. Het is niet voorzien dat bij deze samenwerking ook persoonsgegevens van gebruikers worden verwerkt. Daardoor zijn de erkende diensten bij de uitvoering van de samenwerkingsplicht niet aan te merken als gezamenlijke verwerkingsverantwoordelijken in de zin van artikel 26 AVG.

**5. Handhaving en uitvoering**

Het is voorzien dat het Agentschap Telecom op gaat treden als toezichthouder namens de minister. De toezichthouder ziet binnen de kaders van de Wdo en de daarop berustende bepalingen toe op zowel het stelsel, het adequaat in samenhang functioneren van alle erkende diensten, als de naleving door de individuele erkende dienst. De toezichthouder vormt zichzelf een oordeel over de mate waarin een partij met betrekking tot de te erkennen- of erkende dienst alle regels naleeft die door de Wdo, dit besluit en de daaronder ressorterende regelgeving worden gesteld. Dit doet de toezichthouder mede door zelf inspecties uit te voeren.

De toezichthouder publiceert informatie over de wijze waarop de erkende diensten adequaat hun bewijs van- en verantwoording over de naleving van de gestelde eisen kunnen inrichten.

De toezichthouder wordt bij het vormen van zijn eigenstandige oordeel ondersteund door de bevindingen van de CBI die het certificaat afgeeft aan de partij met een erkende of te erkennen dienst als onderdeel van het benodigde bewijs voor de erkenning. De erkende diensten moeten de auditrapporten die ten grondslag liggen aan hun certificaat delen met de toezichthouder zodat deze zich een eigen oordeel kan vormen over de consequenties van auditbevindingen, eventuele tekortkomingen die de auditor heeft geconstateerd en de afspraken voor herstel daarover. Tevens moeten de erkende of te erkennen diensten ervoor zorgdragen dat de toezichthouder toegang krijgt tot het bevindingendossier dat ten grondslag ligt aan de auditrapporten.

Dit betekent ook dat de toezichthouder zelf de erkende dienst aanspreekt op de naleving en in een uiterst geval de dienst sanctioneert of Onze Minister adviseert om de erkenning in te trekken. In het geval dat de toezichthouder van mening is dat de erkende dienst tekortschiet zal de toezichthouder zijn handhavingsbevoegdheden gebruiken en de erkende dienst een aanwijzing geven om de tekortkoming binnen gestelde termijn weg te nemen. Als de erkende dienst bij herhaaldelijk daarop gewezen te zijn in gebreke blijft kan ultimo de minister de erkenning intrekken.

## 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 jaarlijkse 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 enkel als ontsluitende dienst wil laten erkennen zal minder kosten hebben dan een partij die zich als middelenuitgever wil laten erkennen, omdat aan een middelenuitgever meer toepasselijke eisen worden gesteld dan aan een ontsluitende dienst. Een partij die zich voor alle diensten wil laten erkennen heeft uiteraard de meeste kosten omdat aangetoond moet worden aan de auditor en de toezichthouder dat aan alle eisen wordt voldaan. Een deel van de eisen is echter generiek voor alle diensten en de naleving ervan hoeft uiteraard niet steeds voor elke dienst opnieuw worden aangetoond.

Het bezit van een ISO/IEC 27001-certificaat met betrekking tot informatiebeveiliging of een ETSI 319 411-2-certificaat met betrekking tot de uitgifte van gekwalificeerde certificaten kan de additionele kosten voor de erkenning van een dienst verlagen. 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/IEC 27001-certificaat is in beginsel passend voor alle te erkennen partijen en diensten. Een ETSI-certificaat 319-411-2 zal doorgaans alleen in bezit zijn van een partij die zich als middelenuitgever en authenticatiedienst wil laten erkennen omdat de uitgifte van een gekwalificeerd certificaat veel overeenkomsten heeft met de uitgifte van een elektronisch identificatiemiddel. De wijze waarop de omvang van de audits voor erkenning bepaald worden door de certificerende conformiteit-beoordelende instantie zijn vergelijkbaar met de wijze waarop dit voor ETSI-audits wordt bepaald.

Tot slot zal een te erkennen authenticatiedienst en middelenuitgever in het kader van de productie van bewijs, dat aan specifieke eisen moet worden voldaan, een technische beveiligingstest moeten uitvoeren en deze tweejaarlijks moet herhalen. Deze audit vloeit voort uit de eisen van de 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.

*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/IEC 27001 en ETSI 319-411-2;
- Het aantal middelen dat moet worden erkend;
- De technische 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.

## 7. Verhouding overige regelgeving

Dit besluit ressorteert onder de Wdo *(*de artikelen 11, eerste, 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** |
|---|---|
| 2, derde lid | Algemene eisen erkende diensten |
| 3, eerste lid | Aanvullende eisen erkende diensten |
| 3, tweede lid | Aanvullende eisen (interoperabiliteit) |
| 3, derde lid | Gebruikersvoorwaarden erkende middelenuitgever en erkende machtigingsdienst |
| 3, vierde lid | Regels over interoperabiliteit |
| 3, vijfde lid | Minimale niveau van dienstverlening |
| 4, eerste lid | Eisen aanvraag c.a. erkende middelenuitgever |
| 5, eerste lid | Regels erkende authenticatiedienst |
| 6, tweede lid | Regels erkende ontsluitingsdienst |
| 7, tweede lid | Regels erkende machtigingsdienst |
| 8, vijfde lid | Meldingsplicht |
| 11, vierde lid | Regels indienen aanvraag |
| 12, tweede lid | Regels gegevens auditrapport |
| 15 | Tarieven |
| 16 | Doorberekening kosten |

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. De uitwerking in de ministeriele regeling laat de minimale technische specificaties uit de Uitvoeringsverordening onverlet, maar geeft regels voor de praktische toepassing daarvan. In het artikelsgewijze deel van deze nota van toelichting wordt daar nader op ingegaan.

## 8. Consultatie

Het ontwerpbesluit is in de zomer van 2018 voorgelegd aan Agentschap Telecom (hierna: AT) en aan de uitvoeringsorganisatie LOGIUS. Deze reacties hebben geleid tot aanpassing van dit oorspronkelijke concept.

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.

Op advies van de Autoriteit Persoonsgegevens is op verschillende plaatsen in de Nota van Toelichting verduidelijkt wat de gevolgen van het besluit voor de verwerking van persoonsgegevens zijn hebben de opmerkingen over onder meer de meldingsplicht en de gebruiksvoorwaarden geleid tot aanpassingen in de toelichting.

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 1 Begripsbepalingen*

De meeste begrippen in dit besluit zijn reeds in de Wdo gedefinieerd. Voor zover dit voor een begrip van de in dit besluit opgenomen bepalingen noodzakelijk is, zijn in dit artikel aanvullende definities opgenomen.

*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 rechtspersoon. 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. 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 alle erkende diensten beschikken 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). Het gaat daarbij niet alleen om de gebruikers van de bedrijfs- en organisatiemiddelen, maar ook om andere erkende diensten en bestuursorganen of aangewezen organisaties. Dit doet recht aan het idee dat sprake is van een keten, waarin elke schakel de andere schakel moet kunnen bereiken indien nodig (artikel 2, tweede lid). Tenslotte is opgenomen dat de gegevens van de gebruiker ergens anders worden opgeslagen dan de gebruiksgegevens. Op deze wijze wordt de privacy van de gebruiker beter beschermd en kunnen de gebruiksgegevens bij een eventuele inbreuk op de beveiliging niet worden gekoppeld aan een bepaalde gebruiker.

Het is niet wenselijk om de eisen uit het tweede lid aan te vullen met de voorwaarde dat de te erkennen dienst financieel gezond is, niet afhankelijk is van grote commerciële partijen (internetgiganten) en dat alle beleidsbepalers (aandeelhouders, belangrijke financiers en leidinggevenden) getoetst moeten worden op geschiktheid, betrouwbaarheid, integriteit en onafhankelijkheid. Niet alleen is dit niet volledig mogelijk (de onafhankelijkheid van grote commerciële partijen is thans nog geen afdoende juridische grondslag) en moeilijk te implementeren (de criteria van financiële gezondheid zijn niet duidelijk; het is bijvoorbeeld mogelijk dat een erkende dienst op deze markt bewust verlies accepteert om die op een andere markt te compenseren). Bovendien dienen technische maatregelen, zoals (polymorfe) pseudonimisering van persoonsgegevens, te leiden tot waarborgen dat de persoonsgegevens niet ongewenst worden gebruikt. Daarnaast voorziet artikel 11, zevende lid, Wdo in de bevoegdheid om het Bureau bevordering integriteitsbeoordelingen (Bureau Bibob) om advies te vragen. Ook kunnen, op basis van artikel 14, derde lid, Wdo zwaarwegende redenen leiden tot intrekking of schorsing van de erkenning.

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 (bijlage bij) 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 vormen de basis en zijn waar nodig met aanvullende eisen uitgebreid voor niveau substantieel of hoog. Aangezien een middelenuitgever of authenticatiedienst telkens wordt erkend in relatie met het aangeboden bepaald bedrijfs- en organisatiemiddel, hoeven deze diensten uitsluitend aan 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 betreft

voornamelijk regels voor het daadwerkelijk toepassen van de bijlage van de Uitvoeringsverordening in Nederland.

*Artikel 3 Aanvullende eisen erkende diensten*

Uit artikel 2 van dit besluit volgt dat voor de erkende diensten de bij de Uitvoeringsverordening gestelde eisen in beginsel leidend zijn. Deze eisen kunnen worden aangevuld door middel van een ministeriële regeling. Artikel 3 biedt een grondslag voor het stellen van eisen die aanvullend zijn aan de eisen uit de Uitvoeringsverordening en de ministeriële regeling.

Het eerste lid

In het eerste lid zijn de onderwerpen genoemd ten aanzien waarvan in ieder geval bij ministeriële regeling nadere regels worden gesteld.

*a. Bestrijding misbruik*

In dit kader kan aan verschillende vormen van misbruik worden gedacht. Het kan zijn dat een bedrijfs- en organisatiemiddel door de legitieme gebruiker misbruikt wordt voor frauduleuze handelingen. Maar ook 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 dergelijke vormen van misbruik zoveel mogelijk te voorkomen of aan te kunnen pakken is het bijvoorbeeld van belang dat ongebruikelijke patronen worden geregistreerd en/of daarop kan worden gemonitord. 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 en het nemen van maatregelen om het te stoppen, een meldingsplicht voor vermoedens van misbruik, een verplichting om mee te werken aan een onderzoek naar misbruik en het aanbrengen van functiescheiding in de organisatie.

*b. Interoperabiliteit eIDAS-voorzieningen*

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.

In het stelsel van elektronische dienstverlening in Nederland is er voor gekozen de ontsluiting van dit knooppunt via de erkende ontsluitende diensten te laten plaatsvinden. De verantwoordelijkheid van de erkende diensten om de bestuursorganen en aangewezen organisaties te ontzorgen, strekt in zoverre ook uit tot het gebruik van onder de eIDAS-verordening genotificeerde elektronische identificatiemiddelen. Teneinde een betrouwbare interoperabiliteit te verzekeren binnen het stelsel dat met dit besluit wordt gereguleerd, zullen voor de erkende ontsluitende dienst regels worden gesteld.

Voor het elektronische verkeer vanuit Nederland met andere Europese lidstaten is het gebruik van bedrijfs- en organisatiemiddelen die op grond van dit besluit zijn erkend, noodzakelijk. Het is thans nog niet mogelijk dat dit verkeer kan plaatsvinden met gebruikmaking van toegelaten publieke inlogmiddelen. Dit kan op termijn veranderen, waardoor dan ook toegelaten publieke middelen voor dit doel gebruikt kunnen worden.

*c. organisatorische en technische inrichting verwerking persoonsgegevens*

Nadere regels voor de verwerking van persoonsgegevens hebben betrekking op de invulling van vereisten uit het Besluit digitale overheid met betrekking tot de organisatorische of technische inrichting voor de verwerking van persoonsgegevens op zodanige manier dat deze door de toezichthouder en de auditor te toetsen zijn. Voorbeeld van dergelijke vereisten is een verplichting om processen in te richten waarmee bewaartermijnen en de vernietiging van gegevens na afloop van de bewaartermijn worden gewaarborgd. Een ander voorbeeld is een vereiste om in de opslag en verwerking de gegevens over de gebruiker van een middel te scheiden van de gegevens over het gebruik van het middel.

*d. audittrail*

Een belangrijk onderdeel van een betrouwbaar stelsel is dat achteraf authenticaties voor een elektronische dienst van een bestuursorgaan of aangewezen organisatie herleid kunnen worden tot een daadwerkelijke handeling van de natuurlijke persoon aan wie een middel is uitgegeven. Indien er met betrekking tot de plaatsgevonden handelingen een geschil zou ontstaan tussen de onderneming of rechtspersoon enerzijds en het bestuursorgaan of aangewezen organisatie anderzijds dan is het van belang de werkelijke toedracht te achterhalen. Deze mogelijkheid om dit spoor achteraf te herleiden, wordt ook wel audittrail genoemd. Bij ministeriële regeling worden regels gesteld waaraan de audittrail van de erkende diensten op zijn minst moet voldoen.

Het tweede lid

Uit artikel 5 van de Wdo volgt dat de minister verantwoordelijk is voor het beheer van de generieke digitale infrastructuur. Daarbij wordt een aantal onderdelen expliciet genoemd. Een aantal van deze onderdelen kunnen, nu of in de toekomst, ook relevant zijn voor het stelsel van toegang van ondernemingen en rechtspersonen tot elektronische dienstverlening. 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 tweede lid biedt daar de grondslag voor.

Het derde lid

Het derde lid betreft de gebruiksvoorwaarden van de middelenuitgever en de machtigingsdienst die zij hanteren bij de afnemers van hun diensten. Alleen middelenuitgevers en machtigingsdiensten zullen dergelijke gebruiksvoorwaarden gebruiken, omdat zij een commerciële relatie met hun afnemers (de gebruikers) zullen hebben. Bij ministeriële regeling wordt bepaald wat deze gebruiksvoorwaarden in elk geval moeten omvatten. Zo dienen in de gebruiksvoorwaarden in elk geval regels omtrent verlies, diefstal, misbruik of verspreiding van het bedrijfs- of organisatiemiddel te worden opgenomen. In de ministeriële regeling wordt niet bepaald dat de gebruiksvoorwaarden ook regels omtrent de kosten en de geldigheidsduur van het middel of de geleverde machtigingsdienst bevatten, omdat de verschillende middelenuitgevers en machtigingsdiensten op deze onderwerpen met elkaar in concurrentie kunnen treden.

Het is evenmin wenselijk om in de gebruiksvoorwaarden op te nemen dat gebruikers hun bedrijfsmiddelen en machtigingen over moeten kunnen zetten naar een andere middelenuitgever en machtigingsdienst bij het einde van de dienstverlening van hun huidige leveranciers. De technische, inhoudelijke en beheersmatige aspecten van de bedrijfs- en organisatiemiddelen en de machtigingen kunnen per leverancier aanzienlijk verschillen, waardoor een dergelijke algemene verplichting om alle dienstverlening integraal en ongewijzigd over te nemen, niet werkbaar is.

Het vierde lid

Bij de eisen die aan de afzonderlijke erkende diensten gesteld worden, wordt al zoveel mogelijk rekening gehouden met de noodzakelijke interoperabiliteit tussen die diensten. Voorts wordt het voornamelijk aan de erkende diensten overgelaten om, in het kader van de in artikel 9 van dit besluit opgenomen samenwerkingsplicht, onderling afspraken te maken over de interoperabiliteit. Niettemin is op voorhand niet uitgesloten dat in de toekomst en bij de verdere ontwikkeling van het stelsel generieke eisen aan de interoperabiliteit wenselijk zijn teneinde de betrouwbare toegang te borgen. Voor die situatie biedt het vierde lid de mogelijkheid hierover bij ministeriële regeling regels te stellen.

Het vijfde 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.

*Artikel 4 Eisen erkende middelenuitgever*

Deze bepaling vormt de basis van de eisen waar een middelenuitgever aan dient te voldoen. Ook hier zijn de eisen uit de Uitvoeringsverordening het uitgangspunt. Het gaat dan om de eisen opgenomen in de in het eerste lid genoemde paragrafen uit de bijlage, voor zover die betrekking hebben op de uitgifte en het ontwerp (inclusief de productie en de distributie) van het bedrijfs- en organisatiemiddel met betrekking waartoe de betrokken middelenuitgever 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 en aan het ontwerp gerelateerde eisen uit de Uitvoeringsverordening op hem en zijn middel van toepassing. Het gaat daarbij niet alleen om het proces van uitgifte, maar ook bijvoorbeeld om de authenticatie die op basis van dat middel moet kunnen plaatsvinden. De authenticatie vindt plaats door de authenticatiedienst. In de ministeriële regeling worden nadere eisen gesteld aan de uitgifte van de bedrijfs- en organisatiemiddelen en de authenticatie.

Ook hier geldt dat een middelenuitgever aan deze eisen moet voldoen op het betrouwbaarheidsniveau van het bedrijfs- en organisatiemiddel waarvoor hij erkend is.

Bij ministeriële regeling kunnen aanvullende eisen worden gesteld. Zo bepaalt de Uitvoeringsverordening van de omstandigheid dat de voorwaarden aangaande veiligheidsvoorzorgen bij de gebruiker van het middel bekend moeten zijn. Bij ministeriële regeling wordt opgenomen welke veiligheidsvoorschriften daarbij in elk geval moeten worden betrokken.

Uit de Uitvoeringsverordening volgt voorts dat schorsing en/of intrekking van het middel mogelijk moet zijn. Dit ziet op de situatie dat de betrouwbaarheid van het middel niet meer gegarandeerd kan worden, bijvoorbeeld door misbruik of fraude. In dat geval moet een middelenuitgever, ten behoeve van de betrouwbaarheid van het stelsel, snel kunnen reageren. Het intrekken van een bedrijfs- en organisatiemiddel heeft gevolgen voor de mogelijkheden van de betrokken rechtspersoon of onderneming om toegang te hebben tot elektronische dienstverlening. Hoewel de betrouwbaarheid van het stelsel bewaakt moet worden, is ook van belang dat een rechtspersoon of onderneming niet verstoken raakt van die toegang. Om die reden is het ten eerste van belang dat de gebruiker bekend is met de omstandigheden waarin een middel kan worden geschorst of ingetrokken inclusief de beschrijving van de intrekkingsprocedure (artikel 4, eerste lid).

Ten tweede moet er herstel van toegang tot elektronische dienstverlening mogelijk zijn voor de betrokken rechtspersoon of onderneming. In dat kader kan gedacht worden aan re-activatie van een bestaand middel of uitgifte van een nieuw middel. Aangezien dit aspect direct de toegang van de gebruiker tot elektronische dienstverlening raakt, is ervoor gekozen deze verplichting in dit besluit te verankeren (artikel 4, tweede lid).

Een erkende middelenuitgever is niet verantwoordelijk voor een betrouwbaar authenticatieproces; dat is de taak van een erkende authenticatiedienst. Maar uitgifte van een bedrijfs- en organisatiemiddel is slechts zinvol indien daarmee ook een betrouwbaar authenticatieproces kan plaatsvinden. Het ene kan in zoverre niet los van het andere worden gezien. Daarom wordt het van belang geacht dat, in geval een erkende middelenuitgever er niet voor kiest zich ook als authenticatiedienst te laten erkennen, hij een overeenkomst sluit met een erkende of te erkennen authenticatiedienst. Beschikt een middelenuitgever niet over een zodanige overeenkomst, dan kan van erkenning geen sprake zijn (artikel 4, derde lid).

*Artikel 5 Eisen erkende authenticatiedienst*

Wat de eisen uit de Uitvoeringsverordening betreft is voor de authenticatiedienst specifiek paragraaf 2.3 van de bijlage van belang. 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.

Zoals bij artikel 4 is toegelicht kan een betrouwbare uitgifte niet los worden gezien van een betrouwbare authenticatie. In artikel 5 is daarom voor de authenticatiedienst de spiegelbeeldige situatie geregeld; ofwel hij geeft zelf bedrijfs- en organisatiemiddelen uit en laat zich met betrekking tot die middelen erkennen als middelenuitgever, of hij sluit met betrekking tot een bepaald middel een overeenkomst met een erkende of nog te erkennen middelenuitgever. In het laatste geval wordt de authenticatiedienst erkend met betrekking tot het bedrijfs- en organisatiemiddel dat wordt uitgegeven door de erkende middelenuitgever waar hij de overeenkomst mee heeft gesloten.

Deze bepaling sluit niet uit dat een partij als authenticatiedienst wordt erkend voor bedrijfs- en organisatiemiddelen van een erkende middelenuitgever waarmee hij een overeenkomst heeft gesloten en tevens wordt erkend als middelenuitgever voor een door hem zelf uit te geven middel.

Net als bij de erkende middelenuitgever hoeft een authenticatiedienst uitsluitend te voldoen aan de in de Uitvoeringsverordening gestelde eisen voor het betrouwbaarheidsniveau van het bedrijfs- en organisatiemiddel met betrekking waartoe hij erkend is. Dit geldt uiteraard alleen daar waar een onderscheid in eisen tussen betrouwbaarheidsniveaus zijn gesteld.

Voorts is benadrukt dat een erkende authenticatiedienst uitsluitend het authenticatieproces verzorgt indien gebruik wordt gemaakt van een bedrijfs- en organisatiemiddel met betrekking waartoe hij als middelenuitgever is erkend, of dat wordt uitgegeven door een erkende middelenuitgever waarmee hij een contract heeft. Hij voert dus geen authenticatietaken uit ten aanzien van erkende bedrijfs- en organisatiemiddelen dat door een andere erkende middelenuitgever worden uitgegeven waarmee hij geen overeenkomst heeft. Ten aanzien van die middelen is hij immers bij de erkenning niet beoordeeld.

*Artikel 6 Eisen erkende ontsluitende dienst*

Binnen het stelsel van toegang van ondernemingen en rechtspersonen tot elektronische dienstverlening is de ontsluitende dienst het verbindend element tussen de bestuursorganen en aangewezen organisaties en de overige erkende diensten. Uit de wet volgt dat een ontsluitende dienst alle erkende bedrijfs- en organisatiemiddelen en alle elektronische verklaring van erkende machtigingsdiensten moet kunnen ontsluiten. Een bestuursorgaan of aangewezen organisatie hoeft derhalve ten behoeve van de toegang van ondernemingen en rechtspersonen tot hun elektronische dienstverlening maar met één ontsluitende dienst een overeenkomst te sluiten. Hier wordt op gedoeld met de verantwoordelijkheid van ontzorgen als bedoeld in het eerste lid. Tot het ontzorgen behoort ook de taak van de erkende ontsluitende dienst om met de andere erkende diensten afspraken te maken over de technische aspecten, zoals het koppelvlak. Indien individuele bestuursorganen en aangewezen organisaties zelf bepaalde technische voorzieningen zouden voorschrijven, dan zou dit leiden tot een groot aantal verschillende standaarden; dat zou niet goed werkbaar zijn. Evenmin is het wenselijk om in regelgeving voor te schrijven welke technische voorzieningen moeten worden ingezet, omdat dit de innovatie zou kunnen belemmeren en zou kunnen leiden tot stagnatie en vertraging.

De functie van ontsluitende dienst is niet specifiek gereguleerd in de Uitvoeringsverordening. Maar de ontsluitende dienst heeft wel een rol in de betrouwbaarheid van het authenticatiemechanisme. Hij draagt er zorg voor dat een authenticatieverzoek van een bestuursorgaan naar de juiste authenticatiedienst wordt gezonden en dat het authenticatieantwoord van de authenticatiedienst weer bij het juiste bestuursorgaan aankomt. Naast de eisen, opgenomen in paragraaf 2.3 van de Uitvoeringsverordening, kunnen bij ministeriële regeling eisen aan het authenticatiemechanisme ten behoeve van de taak van de ontsluitende dienst worden gesteld (artikel 6, eerste en tweede lid).

Voor de ontsluitende dienst is van belang dat hij de overige erkende diensten informeert met welke bestuursorganen of aangewezen organisaties hij een overeenkomst heeft gesloten. Dat is immers bepalend voor de vraag ten behoeve van welke dienstverlening hij de ontsluitingstaak uitvoert. Het is aan de erkende diensten om gezamenlijk te bepalen op welke wijze een ontsluitende dienst de betrokken erkende diensten hierover informeert, zowel over de vorm en inhoud. Benadrukt wordt dat met deze verplichting niet wordt beoogd dat een erkende ontsluitende dienst ook inzicht in de inhoud van de overeenkomst biedt. De verplichting omvat uitsluitend de mededeling van de benodigde informatie, zoals de naam van de dienst, het gevraagde betrouwbaarheidsniveau, de gevraagde identificerende attributen en zo voort van de bestuursorganen en aangewezen organisaties voor wiens elektronische dienstverlening hij de ontsluiting verzorgt (artikel 6, derde lid).

Deze ontzorgingstaak van de ontsluitende dienst laat uiteraard onverlet dat het bestuursorgaan of de aangewezen organisatie ervoor kan kiezen om meerdere ontsluitende diensten te contracteren. Dit is ook raadzaam als maatregel om hoge beschikbaarheid van de eigen dienst te garanderen. Bij een verstoring van de ene ontsluitende dienst kan dan worden overgeschakeld op de andere ontsluitende dienst. Van belang in dit kader is dat de ontsluitende dienst afspraken maakt met de overige erkende diensten om de interoperabiliteit te garanderen met de overige erkende diensten. Dit kan bijvoorbeeld in de vorm van afspraken over uniforme specificaties van het koppelvlak van alle erkende ontsluitende diensten. Waar nodig, kunnen dienaangaande bij ministeriële regeling nadere regels worden gesteld (artikel 6, vierde lid).

*Artikel 7 Eisen erkende machtigingsdienst*

Een erkende machtigingsdienst is verantwoordelijk voor de bevestiging dat een natuurlijk persoon bevoegd is namens een onderneming of rechtspersoon toegang te krijgen tot door die onderneming of rechtspersoon bepaalde elektronische dienstverlening. In het machtigingenregister wordt de koppeling gelegd tussen het authenticatiemiddel van de aldus gemachtigde natuurlijke persoon en de bevoegdheid om namens de betrokken onderneming of rechtspersoon op te treden. Een van de mogelijkheden om de rechtspersoon en de bevoegdheid om de rechtspersoon te vertegenwoordigen, is het raadplegen van het Handelsregister.

Het is aan de machtigingsdienst om op verzoek een betrouwbare koppeling te leggen tussen de te machtigen natuurlijke persoon en de onderneming of rechtspersoon namens welke de natuurlijke persoon wenst te handelen. Een verzoek voor zo'n koppeling kan in beginsel uitsluitend worden ingediend door een ingevolge het handelsregister aangegeven wettelijke vertegenwoordiger van de onderneming of rechtspersoon. Deze koppeling kan ook, op verzoek van de wettelijk vertegenwoordiger, omvatten dat de betrokken natuurlijke persoon gerechtigd is op te treden als machtigingenbeheerder. Dat betekent dat, naast de wettelijke vertegenwoordiger, ook die machtigingenbeheerder ten behoeve van de betrokken onderneming of rechtspersoon bij de machtigingsdienst verzoeken kan indienen om een koppeling tot stand te brengen of juist te verwijderen. Een machtigingsbeheerder wordt als zodanig in het machtigingsregister geregistreerd.

Ten behoeve van de registratie in het machtigingsregister dient de machtigingsdienst primair de identiteit van de onderneming of rechtspersoon (verificatie van de rechtspersoon of onderneming aan de hand van het handelsregister en het KvK-nummer) en de wettelijk vertegenwoordiger te verifiëren ("Is hij wie hij zegt dat hij is." en "Is hij ingevolge het handelsregister daadwerkelijk wettelijk vertegenwoordiger van de betrokken onderneming of rechtspersoon."). Vervolgens wordt de identiteit van de te machtigen natuurlijke persoon geverifieerd. Na succesvolle verificatie wordt de koppeling tussen die natuurlijke persoon en de betrokken onderneming of rechtspersoon opgenomen in het machtigingenregister dat door de machtigingsdienst beheerd wordt. Onder machtiging wordt in dit kader tevens de zogenoemde ketenmachtiging verstaan.

Naast deze taak aangaande het registreren van een machtiging is het de taak van de machtigingsdienst om, indien de gemachtigde natuurlijke persoon namens de betrokken onderneming of rechtspersoon toegang vraagt tot elektronische dienstverlening, een elektronische verklaring af te geven dat de natuurlijke persoon daadwerkelijk daartoe gerechtigd is (artikel 7, eerste lid).

Bij de uitvoering van deze activiteiten dient de erkende machtigingsdienst te voldoen aan de eisen van de paragrafen 2.1.3 en 2.1.4 van de bijlage van de Uitvoeringsverordening. Ook deze eisen zullen waar nodig bij ministeriële regeling nader worden uitgewerkt (artikel 7, tweede lid).

Een erkende machtigingsdienst moet in staat zijn om aan de eisen op alle betrouwbaarheidsniveaus te voldoen. Het is aan de wettelijk vertegenwoordiger of de machtigingsbeheerder om bij het verzoek tot een koppeling aan te geven op welke betrouwbaarheidsniveau de koppeling moet worden aangebracht. Daarbij kan het niet zo zijn dat een wettelijk vertegenwoordiger die zelf is geverifieerd op het betrouwbaarheidsniveau substantieel, verzoekt om een koppeling op het betrouwbaarheidsniveau hoog. Met artikel 7, derde lid, wordt dit benadrukt.

In artikel 7, vierde lid, is bepaald dat hij uitsluitend elektronische verklaringen afgeeft indien gebruik is gemaakt van erkende bedrijfs- en organisatiemiddelen of toegelaten middelen. Daarmee wordt benadrukt dat het niet mogelijk is een machtiging te koppelen aan een niet erkend middel.

In artikel 7, vijfde lid, is tot slot bepaald dat een machtigingsdienst er zorg voor dient te dragen dat zijn machtigingsregister op orde is en blijft. Daartoe dient hij in elk geval ingetrokken machtigingen uit zijn register te verwijderen. Ook dit komt de betrouwbaarheid van de hele keten ten goede.

*Artikel 8 Meldingsplicht*

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. Deze kan dan waar nodig gebruik maken van zijn wettelijke bevoegdheden om de gevolgen in te perken.

Bij ministeriële regeling worden nadere regels gesteld over de incidenten of verstoringen die in elk geval gemeld dienen te worden (artikel 8, eerste 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).

Daarnaast dient een erkende dienst elke wijziging in zijn bedrijfsprocessen te melden die van significante invloed is op de uitvoering van zijn activiteiten. Dit is nodig zodat kan worden gecontroleerd of ondanks de wijziging nog steeds aan de gestelde eisen wordt voldaan. Als een leverancier gebruik wil maken van nieuwe technologie om een inlogmiddel van betrouwbaarheidsniveau hoog efficiënter uit te reiken dan moet de toezichthouder toetsen of die in overeenstemming is met de geldende normen (artikel 8, derde lid).

Ook dient de erkende dienst een significante wijziging in de zeggenschap in de rechtspersoon te melden (artikel 8, vierde lid).

Bij ministeriële regeling kunnen regels worden gesteld omtrent de in het derde en vierde lid van dit artikel genoemde meldingsplichten. Daarbij kan gedacht worden aan de periode waarbinnen wordt gemeld en mogelijk de vaststelling van een meldingsformulier (artikel 8, vijfde lid).

*Artikel 9 Samenwerkingsplicht*

De betrouwbaarheid en de werking van het stelsel vallen of staan met een goede samenwerking tussen de betrokken erkende diensten. Het gaat dan met name om de samenwerking aangaande de interoperabiliteit en continuïteit van de diensten en het verandermanagement dienaangaande. De samenwerkingsplicht is beperkt tot dergelijke technische aspecten die voor een goed functioneren van het stelsel noodzakelijk zijn. Commerciële aspecten van de dienstverlening van erkende diensten vallen nadrukkelijk buiten deze plicht tot samenwerking. Erkende diensten blijven vrij hun dienstverlening binnen de grenzen van de wet vorm te geven, mits zij, vanwege de onderlinge technische afhankelijkheid van de erkende diensten, technische aspecten met betrekking tot interoperabiliteit en continuïteit afstemmen. Indien de ene erkende dienst een software-update uitvoert die van invloed is op de toegankelijkheid van die erkende dienst voor een andere erkende dienst, moet dit bijvoorbeeld in goed overleg plaatsvinden. Hoewel deze interoperabiliteit van belang is voor de betrouwbaarheid van het stelsel, is het niet wenselijk deze interoperabiliteit in algemeen verbindende voorschriften op te leggen aan de erkende diensten. De specificaties kunnen onder invloed van technische of functionele ontwikkelingen (zeer) frequent wijzigen. Bovendien hebben de erkende diensten het beste inzicht in de specificaties die mogelijk en wenselijk zijn. Om die reden is er voor gekozen de inrichting daarvan aan de erkende partijen zelf over te laten. Wel worden zij verplicht hieromtrent afspraken te maken. Dit komt de transparantie en gelijke verhoudingen ten goede.

De verplichting tot samenwerking door middel van het maken van afspraken zal als voorschrift aan de erkenning worden verbonden en zal gelden voor alle erkende diensten. Op die manier kan de samenwerkingsplicht worden aangescherpt voor de bij erkenning voorliggende situatie. Zo zal bij de eerste erkenningen het voorschrift veeleer betrekking hebben op het tot stand brengen van de afspraken, terwijl bij latere erkenning de aansluiting bij deze afspraken veeleer aan de orde zal zijn. Ten behoeve van dit laatste is het van belang dat de bestaande afspraken een regeling bevatten op basis waarvan het voor elke nieuwe erkende dienst mogelijk is om zonder onnodige drempels of tijdsverlies te kunnen toetreden. Erkende diensten die middels hun erkenning verplicht zullen worden om samenwerkingsafspraken te sluiten, zullen daarom ook verplicht worden om in die afspraken een goede toetredingsregeling op te nemen.

De verplichting tot samenwerking op grond van dit artikel geldt ook voor erkende diensten die dezelfde soort diensten verlenen. Indien een authenticatiedienst een technische wijziging doorvoert is dit ook voor de andere authenticatiediensten van belang. De minister kan erop toezien dat de afspraken in de samenwerkingsafspraken de concurrentie tussen de erkende diensten en de innovatie niet zal beperken.

De samenwerking tussen de erkende diensten leidt er niet toe dat zij onderling persoonsgegevens van de gebruikers zullen uitwisselen. De samenwerking betreft immers de uitwerking van

onderlinge technische afhankelijkheden en heeft geen betrekking op individuele of groepen gebruikers.

*Artikel 10 Aanwijzingen*

In artikel 13, vijfde lid, van de Wdo is bepaald dat de minister bindende aanwijzingen kan geven aan erkende diensten indien dit naar zijn oordeel voor de betrouwbare toegang noodzakelijk is. In dit artikel wordt deze bevoegdheid nader uitgewerkt.

Dergelijke aanwijzingen kunnen in drie situaties worden gegeven. Zo kan het in geval van een incident of verstoring nodig zijn om door middel van bindende aanwijzingen aan een of meerdere erkende diensten ervoor te zorgen dat bepaalde herstelmaatregelen worden getroffen. Ook naar aanleiding van een wijziging in de zeggenschap of een wijziging in de bedrijfsprocessen kan het nodig zijn om een bindende aanwijzing te geven. Daarbij is het niet de bedoeling om op de ondernemingsvrijheid inbreuk te maken. Een aanwijzing kan immers ook niet in strijd met het hogere recht zijn. Maar wel kan gedacht worden aan een aanwijzing om gebruikers van een middel of de andere erkende diensten over de wijziging van de bedrijfsprocessen te informeren, of een aanwijzing om een auditrapport over te leggen.

Tot slot kan een bindende aanwijzing nodig zijn indien in het kader van de verplichte samenwerking geen overeenstemming wordt bereikt. Indien bijvoorbeeld een erkende dienst een wijziging van de interoperabiliteitsafspraken wenst, maar daarbij geen gehoor krijgt bij de overige erkende diensten, kan hij de minister verzoeken een aanwijzing te geven.

*Artikel 11 Indienen van een aanvraag*

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. In dat kader kan worden gedacht aan een reeds erkende middelenuitgever die een verzoek indient om erkend te worden ten behoeve van een nieuw uit te geven bedrijfs- en organisatiemiddel. 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 van een door de minister op grond van artikel 13 van dit besluit aangewezen CBI.

De geaccrediteerde CBI zal niet alle eisen kunnen beoordelen en dat is ook niet de bedoeling. Bij ministeriële regeling zal worden bepaald op welke eisen de audit betrekking moet hebben (artikel 12, tweede lid). Het gaat dan ten eerste om de nadere invulling van de uit de Uitvoeringsverordening volgende eisen, bijvoorbeeld aangaande de uitgifte van middelen en registratie van machtigingen, of aan de informatieveiligheid. De te auditen eisen zullen worden

opgenomen in een bijlage bij de regeling die de conformiteitsbeoordelingsinstantie als auditschema kan hanteren. Op die manier wordt ruis tussen de audit en de bij de ministeriële regeling gestelde eisen voorkomen.

Het certificaat levert een bewijsvermoeden op dat voldaan wordt aan de gestelde eisen. Uiteindelijk is het aan Onze Minister om te bepalen of de erkenning kan worden verleend.

Op grond van artikel 13, zevende lid van de Wdo, zoals aangepast na de behandeling in de Tweede Kamer, rust er op de erkende diensten een leveringsplicht. Deze plicht is in artikel 11, zevende lid omschreven als een aanbiedingsplicht, omdat een erkende dienst zelf wel verantwoordelijk kan worden gehouden voor het aanbieden van de dienst waarvoor hij is erkend, maar niet voor het leveren van deze dienst. Dat is mede afhankelijk van de bereidheid van potentiële afnemers om de dienst daadwerkelijk te gaan gebruiken. De erkende dienst moet de dienst of het middel binnen een bij ministeriële regeling vast te stellen termijn aanbieden na de publicatie in de Staatscourant van de erkenning. Onder aanbieden wordt verstaan het daadwerkelijk beschikbaar hebben voor gebruik van de erkende dienst of het erkende middel door potentiele afnemers.

Een ander element van de leveringsplicht betreft de mate waarin de dienst en het middel daadwerkelijk door de afnemer kan worden gebruikt. Daarbij gaat het om de mate waarin deze dienst en dat middel beschikbaar zijn. In artikel 3, vijfde lid, wordt bepaald dat in de ministeriele regeling nadere eisen worden gesteld aan het minimale niveau van dienstverlening en aan de prestatie-indicatoren voor beschikbaarheid.

Ook de uit het Besluit digitale overheid voor de erkende diensten volgende eisen aangaande gegevensbescherming kunnen bij ministeriële regeling als te auditen eisen kunnen 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 12 Certificaat van conformiteit*

Zoals bij artikel 11 van dit besluit is toegelicht moet bij de aanvraag om erkenning een certificaat van conformiteit, inclusief het daarbij behorende auditrapport worden overgelegd. Ingevolge de certificatieprocedure is dit certificaat twee jaar geldig en dient dan een hernieuwde beoordeling plaats te vinden voor vernieuwing van het certificaat. Het is in dat kader dan ook van belang dat erkende diensten te allen tijde beschikken over een geldig certificaat van conformiteit (artikel 12, eerste en tweede lid). De frequentie van de tweejaarlijkse audit met een tussentijdse surveillance audit sluit aan bij de auditcyclus van de trustservices in het kader van de eIDAS-verordening. De inhoud van de audit is gebaseerd op de Set van Eisen die als bijlage aan de ministeriële regeling wordt toegevoegd.

Het is niet goed mogelijk om te volstaan met een certificaat dat afgegeven is voor een ander soort ICT-kader, zoals ISO-certificaten. De inhoud van het certificaat van conformiteit is afgestemd op de eisen uit de Uitvoeringsverordening. Die eisen zijn specifiek opgesteld voor eIDAS en de bestaande certificaten zijn daarvoor niet (volledig) geschikt.

Benadrukt is in het derde lid dat van een geldig certificaat geen sprake is, indien het is afgegeven door een CBI waarvan de aanwijzing is geschorst of is ingetrokken. In geval de minister reden heeft gehad voor schorsing of intrekking, brengt dit met zich dat niet langer met zekerheid van de betrouwbaarheid van de conformiteitsbeoordeling kan worden uitgegeven. Daarvan kan ook sprake zijn indien het certificaat is afgegeven door een CBI vlak voor de schorsing of intrekking. De omstandigheden die aanleiding zijn geweest voor schorsing of intrekking kunnen ten tijde van afgifte van het certificaat immers al hebben plaatsgevonden. Indien de minister kan aantonen dat dit inderdaad het geval is en het certificaat onterecht is afgegeven, is evenmin sprake van een geldig certificaat (artikel 12, vierde lid).

*Artikel 13 Aanwijzing conformiteitsbeoordelingsinstantie*

Uit artikel 11, eerste lid, onderdeel b, volgt dat rechtspersonen die erkend willen worden bij hun aanvraag een geldig certificaat van conformiteit en het bijbehorende auditrapport overleggen. Voor de betrouwbaarheid van het certificaat is van belang dat deze is afgegeven door een ter zake deskundige CBI. Een CBI kan op aanvraag door de minister als zodanig worden aangewezen, indien de CBI voldoet aan de in artikel 13 gestelde eisen.

De in artikel 13, eerste lid, van dit besluit gestelde eisen dienen ertoe om te borgen dat de CBI financieel en organisatorisch voldoende betrouwbaar en gezond is. Ten aanzien van de deskundigheid is vereist dat de CBI moet zijn geaccrediteerd door een nationale accreditatie-instantie als bedoeld in de verordening van het Europees Parlement en de Raad van de Europese Unie 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). In Nederland is dit de Raad van Accreditatie. De accreditatie vindt plaats op grond van ISO 17065. Bij een dergelijke accreditatie hanteert de Raad een accreditatieschema op basis waarvan de deskundigheid voor de specifieke certificeringsactiviteit kan worden beoordeeld. Vaak zijn geharmoniseerde Europese accreditatieschema's voor handen, maar dat is op dit moment niet het geval voor de in dit besluit aan de orde zijnde activiteiten op het gebied van elektronische identificatiemiddelen. Om die reden zal de minister een certificatieschema vaststellen. Dit schema zal worden gebaseerd op de norm ETSI EN 319403, het Europees geaccepteerd accreditatieschema aangaande elektronische handtekeningen.

Het vrij goederen- en dienstenverkeer in de Europese Unie brengt mee dat lidstaten diensten, die in een andere lidstaat rechtmatig worden verricht, niet mogen weigeren omdat ze niet voldoen aan de eigen nationale voorschriften ter zake. Dit wordt het beginsel van wederzijdse erkenning genoemd. In het kader van dit beginsel is in artikel 13, tweede lid, van dit besluit bepaald dat met het door de minister vastgestelde certificatieschema gelijk wordt gesteld een schema dat in een andere lidstaat is vastgesteld en naar het oordeel van de minister een vergelijkbaar beschermingsniveau biedt.

Tot slot is van belang dat de aanwijzing niet overdraagbaar is. De aanwijzing betreft immers een vaststelling dat de betrokken rechtspersoon voldoende deskundig en betrouwbaar is geacht. In geval van overdracht van de aanwijzing aan een andere rechtspersoon kan die deskundigheid en betrouwbaarheid niet meer worden gegarandeerd. Die andere rechtspersoon zal dan zelf een aanvraag moeten indienen (artikel 13, derde lid, van dit besluit).

Het is vooralsnog voorzien dat er meer CBI's worden aangewezen. Op die manier kunnen de te erkennen diensten een keuze maken tussen de verschillende CBI's en wordt het gemakkelijker de totale certificeringsduur van alle te erkennen diensten te beperken. Indien er onverhoopt te weinig CBI's zouden zijn, zal in overleg met de Raad van Accreditatie naar een oplossing worden gezocht.

*Artikel 14 Intrekken aanwijzing conformiteitsbeoordelingsinstantie*

Indien blijkt dat een aangewezen CBI niet langer aan de in artikel 13 van dit besluit gestelde eisen voldoet, bijvoorbeeld omdat de accreditatie is vervallen, kan de minister de aanwijzing intrekken. Of intrekking aan de orde is, zal ook afhangen van de mate waarin alsnog aan de eisen kan worden voldaan. In geval de instantie in staat van faillissement verkeert of een bestuurder daarvan veroordeeld is, ligt intrekking in de rede. Het niet voldoen aan daaromtrent gestelde eisen kan immers niet meer worden hersteld. Ook ligt intrekking in de rede indien de accreditatie is vervallen en hernieuwde accreditatie op korte termijn niet aan de orde zal zijn.

*Artikel 15 Tarieven*

In artikel 13, eerste lid Wdo, zoals deze luidt na de behandeling van het wetsvoorstel in de Tweede Kamer, is vastgelegd dat de eisen die aan een erkende dienst worden gesteld, ook regels inzake te hanteren tarieven kunnen behelzen. De erkende diensten zijn in principe vrij om hun eigen tarieven te bepalen. Daarbij dienen zij zich vanzelfsprekend aan wettelijke regels te houden. Daartoe behoort ook dit artikel 15, waarin de bevoegdheid van de minister is vastgelegd om tarieven vast te stellen indien door een bepaalde erkende dienst tarieven worden gehanteerd die hoger dan marktconform zijn.
De ratio achter deze bevoegdheid is dat alle soorten erkende diensten moeten samenwerken om het stelsel te laten werken. Hierdoor ontbreekt de noodzaak om scherpe of marktconforme tarieven te hanteren. Dit geldt voor alle soorten erkende diensten, waardoor zowel richting gebruiker als richting eindafnemer wellicht hogere tarieven dan marktconform kunnen worden gevraagd. De ontsluitende dienst is gehouden om met alle authenticatiediensten een overeenkomst aan te gaan; deze kunnen daarom hoge tarieven hanteren jegens de ontsluitende

diensten. De authenticatiediensten hebben daarom geen impuls om te proberen gunstige tarieven overeen te komen met een middelenuitgever (en soms zijn authenticatiediensten zelf ook middelenuitgever) en de ontsluitende diensten kunnen de hoge tarieven weer doorberekenen aan de bestuursorganen en de aangewezen organisaties met wie zij een overeenkomst aangaan. Kortom, er is eigenlijk geen 'echte' markt zodat er een mogelijkheid bestaat dat de tarieven te hoog worden.

De minister kan in een dergelijk geval, waarbij hogere, niet-marktconforme, tarieven worden gehanteerd, op basis van dit artikel ingrijpen en, met inachtneming van de regels uit de ministeriële regeling, zelf marktconforme tarieven vaststellen. Deze marktconforme tarieven kunnen opgelegd worden aan een bepaalde erkende dienst (bijv. erkende authenticatiedienst A) of een bepaald soort erkende diensten (bijv. alle authenticatiediensten). In de ministeriële regeling wordt onder meer vastgelegd wanneer sprake is van niet-marktconforme tarieven en op welke wijze de minister zelf de tarieven bepaalt die door de betreffende erkende dienst gehanteerd moet worden.

*Artikel 16 Doorberekening kosten aanvraag erkenning en toezicht*

Deze bepaling maakt het mogelijk in de ministeriële regeling nadere regels te stellen omtrent de doorberekening van de kosten in de in artikel 22 van de Wdo genoemde situaties.

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

drs. R.W. Knops