Regeling van de staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties [PM] 2022, nr CZW/S&B/…., houdende nadere eisen en regels voor het verlenen van een toelating voor publieke en private identificatiemiddelen (Regeling nadere eisen identificatiemiddelen, authenticatiediensten en machtigingsdiensten Wdo)

De Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties,

Gelet op artikel 5 en 25 van de Algemene verordening gegevensbescherming, artikel 2, derde lid, 4, eerste lid, 7, tweede tot en met zevende lid, 8, derde lid, 12, derde lid, 13, vierde lid, 17, vierde lid, en 21 van het Besluit bedrijfs- en organisatiemiddel Wdo, artikel 6, eerste, en derde lid, 7, eerste en tweede lid, 10, tweede lid, 17, tweede lid, 22, eerste tot en met derde lid, 23, tweede lid, 25, eerste lid, 27, vierde lid, 30, eerste tot en met derde lid, van het Besluit identificatiemiddelen voor natuurlijke personen Wdo;

Besluit:

Hoofdstuk 1 Algemeen

Artikel 1.1 Begripsbepalingen

In deze regeling wordt verstaan onder:

- *aanvalspotentieel*: maatstaf van de inspanning benodigd voor het succesvol doorbreken van een implementatie van een beveiligingsdoelstelling, bepaald op basis van de methode in Appendix B van ISO/IEC 18045;
- *aanvraag*: aanvraag voor een erkenning als bedoeld in artikel 9, tweede lid, of 11, tweede of derde lid van de wet;
- *Algemene verordening gegevensbescherming*: verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (algemene verordening gegevensbescherming) (PbEU 2016, L 119);
- *authenticatiecode*: door een houder van een erkenning op basis van de persoonlijke stelselcode versleutelde code voor een authenticatie bij een publieke dienstverlener;
- *authenticatiefraude*: authenticatie namens de gebruiker of namens een rechtspersoon of onderneming zonder diens toestemming;
- *authenticatiemechanisme*: processen en handelingen waarmee een authenticatie wordt uitgevoerd;
- *Besluit BO*: Besluit bedrijfs- en organisatiemiddel Wdo;
- *Besluit INP*: Besluit identificatiemiddelen voor natuurlijke personen Wdo;
- *beschikbaarheidsincident:* verstoring in de authenticatieprocessen, als gevolg waarvan authenticatie geheel of gedeeltelijk onmogelijk is;
- *beveiligingsincident:* gebeurtenis of een serie gebeurtenissen waarmee een inbreuk wordt
- met persoonsgegevens als bedoeld in artikel 4, onder 12, van de Algemene verordening gegevensbescherming;

- *BSN-koppelregister*: voorziening, bedoeld in artikel 5, eerste lid, onderdeel d, van de wet;
- *intrekken van een identificatiemiddel*: gebruik van een individueel, aan een gebruiker verstrekt identificatiemiddel permanent onmogelijk maken;
- *machtiging:* bevoegdheid als bedoeld in artikel 6, eerste lid, onderdeel a, van het Besluit BO;
- *middelbeheerkwaliteit:* kwaliteit van de processen waarmee de koppeling tussen een identificatiemiddel en de gebruiker van dat middel wordt gelegd of gewijzigd, waaronder in ieder geval worden begrepen de in Uitvoeringsverordening (EU) 2015/1502 beschreven processen voor:
  a. aanvraag en registratie van een identificatiemiddel,
  b. bewijs en verificatie van de identiteit van de beoogde gebruiker,
  c. uitgifte, uitreiking en activering van een identificatiemiddel,
  d. schorsing, herroeping en reactivering van een identificatiemiddel,
  e. verlenging en vervanging;
- *middelconformiteitsonderbouwing:* onderbouwing, bedoeld in artikel 3.1, eerste lid, onderdeel c;
- *middelkwaliteit:* kwaliteit van de processen die leiden tot het al dan niet afgeven van een authenticatieverklaring bij gebruik van het identificatiemiddel;
- *misbruik van een identificatiemiddel of een geregistreerde bevoegdheid:* gebruik van een identificatiemiddel of machtigingsdienst met het oogmerk om op onrechtmatige wijze een resultaat te bewerkstelligen, waaronder in ieder geval authenticatiefraude wordt begrepen;
- *minister:* minister van Binnenlandse Zaken en Koninkrijksrelaties;
- *persoonlijke stelselcode*: door het BSN-koppelregister tijdens het registratieproces van een identificatiemiddel verstrekte code;
- *publieke dienstverlener*: bestuursorgaan, aangewezen organisatie of rechterlijke instantie, als bedoeld in artikel 2 van de wet;
- *registratieproces*: processen bedoeld in onderdeel 2.1 van Uitvoeringsverordening (EU) 2015/1502;
- *schorsen van een identificatiemiddel*: gebruik van een individueel, aan een gebruiker verstrekt identificatiemiddel tijdelijk onmogelijk maken;
- *verificatieproces*: proces bedoeld in onderdeel 2.1.3. van Uitvoeringsverordening (EU) 2015/1502.

Artikel 1.2 Reikwijdtebepaling eisen identificatiemiddel voor natuurlijke personen

1. Nadere eisen als bedoeld in artikel 7, eerste lid, van het Besluit INP zijn de eisen, bedoeld in hoofdstuk 2, met uitzondering van paragraaf 2.5.

2. Nadere eisen als bedoeld in artikel 25, eerste lid, van het Besluit INP zijn de eisen, bedoeld in hoofdstuk 4, met uitzondering van [PM: uitzonderen specifieke eisen voor machtiging].

Artikel 1.3 Reikwijdtebepaling eisen erkenning bedrijfs- of organisatiemiddel

1. Aanvullende eisen als bedoeld in artikel 7, tweede lid, van het Besluit BO, voor een authenticatiedienst als bedoeld in artikel 11, tweede lid, van de wet, zijn de eisen, bedoeld in hoofdstuk 2, met uitzondering van paragraaf 2.5 en de eisen bedoeld in hoofdstuk 4, met uitzondering van 4.11.

2. Aanvullende eisen als bedoeld in artikel 7, tweede lid, van het Besluit BO, voor een machtigingsdienst als bedoeld in artikel 11, eerste lid, van de wet, zijn de eisen, bedoeld in:

a. paragraaf 2.1 en 2.5, tot en met 2.8, met uitzondering van artikel 2.16, tweede lid;

b. paragraaf 2.5;

c. hoofdstuk 4, met uitzondering van artikel 4.8, tweede en derde lid, 4.9, tweede lid, 4.10, 4.11, en 4.12.

Hoofdstuk 2 Aanvullende erkenningseisen

Paragraaf 2.1 Verzekering en certificering

Artikel 2.1 Verzekering

Een aanvrager heeft een verzekering voor contractuele en wettelijke aansprakelijkheid voor directe en indirecte schade die samenhangt met de activiteiten waarvoor de erkenning wordt aangevraagd tot een bedrag van ten minste € 10.000.000 per jaar bij een verzekeraar die:

a. onder toezicht staat van de Europese Autoriteit voor Verzekeringen en Bedrijfspensioenen;

b. een kredietbeoordeling heeft van een gerenommeerde kredietbeoordelaar die niet lager is dan A-.

Artikel 2.2 Certificering

Een aanvrager beschikt voor de activiteiten waarop de aanvraag ziet over een conform de norm ISO 27001 gecertificeerd beheerssysteem voor informatiebeveiliging.

Artikel 2.3 Voldoen aan verplichtingen bij beëindiging erkenning

Een aanvrager heeft geborgd dat bij beëindiging van de erkenning een deugdelijke afronding van de daaraan verbonden werkzaamheden conform de daarvoor geldende verplichtingen, waaronder de vernietiging en bewaring van persoonsgegevens, gegevens over het gebruik van identificatiemiddelen en gegevens over bevoegdheden als bedoeld in artikel 6 van het Besluit BO en het gebruik daarvan, kan plaatsvinden, ook in geval van faillissement of andere omstandigheden waarin de kosten niet door de aanvrager kunnen worden gedekt.

Paragraaf 2.2 Beveiliging en transparantie van processen en systemen

Artikel 2.4 Bestandheid tegen aanvallen

1. De middelkwaliteit en middelbeheerkwaliteit van het identificatiemiddel waarop de aanvraag ziet, alsmede de implementaties van de verplichtingen op grond van de artikelen 2.8, 2.12, 2.14, bieden bescherming tegen een aanval met aanvalspotentieel:

a. Moderate, voor zover de aanvraag ziet op een identificatiemiddel met betrouwbaarheidsniveau substantieel;

b. High, voor zover de aanvraag ziet op een identificatiemiddel met betrouwbaarheidsniveau hoog; of

c. enhanced-Basic, voor zover het processen betreft met betrekking tot het schorsen of intrekken op verzoek van de gebruiker.

2. De verplichting, bedoeld in het eerste lid ziet slechts op aanvallen die leiden tot:

a. een onjuiste koppeling tussen een middel en de daarvoor beoogde gebruiker; en

b. een authenticatie namens een gebruiker zonder diens toestemming.

3. De dienstverlening van aanvrager die via het internet kan worden bereikt is, op het niveau van een internationaal geaccepteerde industriestandaard, bestand tegen een representatieve aanval vanaf het internet.

Artikel 2.5 Gebruik van software met openbare broncode

De componenten, bedoeld in artikel 6, eerste lid, van het Besluit INP en artikel 6, eerste lid, van het Besluit BO, waarbij door de aanvrager van een erkenning gebruik wordt gemaakt van software die onder een open source licentie is gepubliceerd of waarvan de broncode openbaar is gemaakt, zijn de componenten die worden aangewezen in bijlage 1 bij deze regeling en waarvoor de datum, genoemd in de laatste kolom van die bijlage op het moment van indienen van de aanvraag is verstreken.

Artikel 2.6 Publicatie van broncode

Een publicatie van broncode als bedoeld in artikel 4, eerste lid, onderdeel b, of artikel 6, eerste lid, onderdeel b, van het Besluit INP of artikel is:

a. openbaar en op het internet vindbaar;

b. toegankelijk voor eenieder.

Paragraaf 2.3 Registratie- en verificatieproces

Artikel 2.7 Registratieproces

1. Bij het registratieproces voor een identificatiemiddel worden in ieder geval de volgende gegevens van de gebruiker verwerkt:

a. naam en voorletters en de noodzakelijke gegevens om deze correct weer te geven;

b. de geboortedatum;

c. het burgerservicenummer;

d. indien het registratieproces, bedoeld in paragraaf 2.1.2, onder substantieel, subonderdeel 2, van de bijlage bij Uitvoeringsverordening (EU) 2015/1502, wordt gehanteerd, het documentnummer van een identiteitsdocument als bedoeld in het derde lid;

e. de gegevens die noodzakelijk zijn om met de gebruiker te communiceren op andere wijze dan via toegang tot de authenticatiedienst.

2. Het proces voor inschrijving, bedoeld in paragraaf 2.1 van de bijlage bij Uitvoeringsverordening (EU) 2015/1502, voorziet in ieder geval in:

a. het ter controle verzenden van de gegevens, bedoeld in het eerste lid, onderdeel a, tot en met c aan het BSN-koppelregister;

b. indien de controle bedoeld in onderdeel a een positief resultaat heeft opgeleverd:

i. het verwerken van de persoonlijke stelselcodes die voor de desbetreffende gebruiker zijn aangemaakt;

ii. het verwijderen van het burgerservicenummer van de desbetreffende gebruiker;

c. het verwijderen van het burgerservicenummer van de desbetreffende gebruiker indien de controle bedoeld in onderdeel a een negatief resultaat heeft opgeleverd.

3. Indien bij het registratieproces een identiteitsdocument wordt overgelegd betreft het een document als bedoeld in artikel 1 van de Wet op de identificatieplicht.

4. De procedure, bedoeld in paragraaf 2.1.2, betrouwbaarheidsniveau hoog, onder 2, van de bijlage van Uitvoeringsverordening (EU) 2015/1502, wordt niet toegepast.

Artikel 2.8 Afgeleide verificatie

1. Bewijs en verificatie van de identiteit van een natuurlijke persoon kan overeenkomstig de procedure bedoeld in paragraaf 2.1.2, onderdeel 2, voor betrouwbaarheidsniveau substantieel en hoog, van de bijlage bij Uitvoeringsverordening 2015/1502 slechts plaatsvinden door middel van een authenticatie met een op grond van artikel 9, eerste lid, van de wet aangewezen publiek identificatiemiddel op hetzelfde of een hoger betrouwbaarheidsniveau als het middel ten behoeve waarvan het bewijs en de verificatie vereist zijn.

2. In afwijking van artikel 2.7, tweede lid, voorziet het proces van inschrijving, bedoeld in paragraaf 2.1 van de bijlage bij Uitvoeringsverordening (EU) 2015/1502, bij toepassing van het eerste lid in ieder geval in:

a. het verzenden van de persoonlijke stelselcode die door het publieke middel is verstrekt bij de authenticatie, bedoeld in het eerste lid, aan het BSN-koppelregister;

b. het verwerken van de persoonlijke stelselcodes die voor de desbetreffende gebruiker zijn aangemaakt.

Artikel 2.9 Inhoud van de overeenkomst tussen een authenticatiedienst en een gebruiker

Onverminderd artikel 5 van het Besluit INP en artikel 3 van het Besluit BO wordt in de overeenkomst die door een aanvrager van een erkenning voor een authenticatiedienst als bedoeld in artikel 9, tweede lid, van de wet, of artikel 11, tweede lid, van de wet, met een gebruiker wordt gesloten voor het gebruik van een identificatiemiddel een verplichting opgenomen voor de gebruiker om:

a. het identificatiemiddel dat op de naam van die gebruiker is geregistreerd niet door een ander te laten gebruiken;

b. verlies van en beveiligingsincidenten ten aanzien van het identificatiemiddel zo spoedig mogelijk te melden bij de verstrekker van dat middel;

c. de verstrekker van het identificatiemiddel binnen een redelijke termijn op de hoogte te stellen wanneer zich wijzigingen voordoen in de gegevens, bedoeld in artikel 2.7, eerste lid;

d. door de verstrekker van het identificatiemiddel gekozen beveiligingsmaatregelen te hanteren.

Paragraaf 2.4 Authenticatie en gebruik

Artikel 2.10 Gebruik van authenticatiecode bij authenticatie van natuurlijke personen

Het authenticatiemechanisme dat in de aanvraag voor een erkenning als bedoeld in artikel 9, tweede lid, van de wet is beschreven voorziet bij een positieve authenticatiehandeling in:

a. het omzetten van de persoonlijke stelselcode voor de persoon waarop de authenticatiehandeling ziet in een authenticatiecode;

b. het verzenden door de authenticatiedienst aan een publieke dienstverlener van de authenticatiecode die tijdens het authenticatieproces voor de desbetreffende authenticatiehandeling is aangemaakt en het betrouwbaarheidsniveau waarop de authenticatie plaatsvond.

Artikel 2.11 Gebruik van authenticatiecode bij bedrijfs- en organisatiemiddel

Het authenticatiemechanisme dat in de aanvraag voor een erkenning als bedoeld in artikel 11, tweede lid, van de wet is beschreven voorziet bij een positieve authenticatiehandeling in:

a. het omzetten van de persoonlijke stelselcode voor de persoon waarop de authenticatiehandeling ziet in een authenticatiecode;

b. het verzenden door de authenticatiedienst aan een erkende machtigingsdienst van de authenticatiecodes die tijdens het authenticatieproces voor de desbetreffende authenticatiehandeling zijn aangemaakt en het betrouwbaarheidsniveau waarop de authenticatie is uitgevoerd.

Artikel 2.12 Gebruik van een bezits- en kennisfactor

1. Indien als onderdeel van het authenticatieproces een op bezit gebaseerde authenticatiefactor als bedoeld in Uitvoeringsverordening (EU) 2015/1502 wordt gebruikt betreft het gegevens, zoals cryptografische sleutels, op een fysiek aanwijsbaar object, waarover uitsluitend de gebruiker beschikkingsmacht uitoefent en die voldoende zijn beschermd tegen kopiëren.

2. Indien voor een identificatiemiddel op betrouwbaarheidsniveau hoog als onderdeel van het authenticatieproces een op kennis gebaseerde authenticatiefactor als bedoeld in Uitvoeringsverordening (EU) 2015/1502 wordt gebruikt wordt met technische beveiligingsmaatregelen gerealiseerd dat:

a. de kennis waarop de authenticatiefactor is gebaseerd slechts bij de gebruiker beschikbaar is op het moment waarop de authenticatie wordt uitgevoerd;

b. de verificatie van de kennisfactor plaatsvindt aan de hand van gegevens die zijn verwerkt in een fysiek aanwijsbaar object, waarover uitsluitend de gebruiker of de aanvrager van de erkenning beschikkingsmacht uitoefent en die voldoende zijn beschermd tegen kopiëren van deze gegevens, en

c. indien de verificatie van de kennisfactor door de aanvrager van de erkenning wordt uitgevoerd, de verzoeken daartoe door de aanvrager worden vastgelegd.

Artikel 2.13 Gebruik van biometrie bij authenticatie uitgesloten

Het authenticatiemechanisme van een identificatiemiddel op betrouwbaarheidsniveau substantieel en hoog maakt geen gebruik van een inherente authenticatiefactor, als bedoeld in de bijlage bij Uitvoeringsverordening (EU) 2015/1502.

Artikel 2.14 Bescherming tegen misleiding bij authenticatie

1. Een gebruiker wordt tijdens het authenticatieproces door de aanvrager van de erkenning voor een authenticatiedienst als bedoeld in artikel 9, tweede lid, van de wet, of artikel 11, tweede lid, van de wet, op betrouwbare wijze van de volgende informatie voorzien:

a. de publieke dienstverlener waarvoor de authenticatie plaatsvindt;

b. in voorkomend geval, de specifieke dienst waarvoor de authenticatie plaatsvindt;

c. in voorkomend geval, een duiding van de persoonsgegevens die bij de authenticatie aan de publieke dienstverlener worden verstrekt.

2. Met de wijze waarop de informatie, bedoeld in het eerste lid, wordt getoond wordt geborgd dat de getoonde informatie niet door een derde partij kan worden gemanipuleerd.

3. Tijdens het authenticatieproces wordt een gebruiker in de gelegenheid gesteld het authenticatieproces af te breken tot het moment waarop dit is voltooid.

Artikel 2.15 Inzage in gegevens door gebruikers

Een aanvrager van een erkenning heeft voorzieningen om aan een gebruiker, na een authenticatie met een identificatiemiddel, in ieder geval elektronisch inzage te geven in:

a. de datum en het tijdstip waarop het desbetreffende identificatiemiddel is gebruikt voor authenticatie bij een publieke dienstverlener, onder vermelding van de publieke dienstverlener waarbij en de dienst waarvoor op dat tijdstip de authenticatie is verricht;

b. de gegevens, bedoeld in artikel 2.7, eerste lid, die over de desbetreffende gebruiker zijn verwerkt;

c. de identificatiemiddelen die door de aanvrager van de erkenning aan de desbetreffende gebruiker zijn uitgereikt en het moment waarop dat uitreiken plaatsvond;

d. overige gegevens die over de desbetreffende gebruiker zijn geregistreerd ten behoeve van authenticatie.

Paragraaf 2.5 Toegang tot publieke dienstverlening door rechtspersonen en ondernemingen

Artikel 2.16 Registratie van een machtiging door een rechtspersoon of onderneming

Het proces voor registratie van een bevoegdheid als bedoeld in artikel 6, eerste lid, onderdeel a, van het Besluit BO, van een natuurlijke persoon om namens een rechtspersoon of onderneming te handelen en voor wijziging van een registratie, voldoet aan de volgende eisen:

a. de identiteit van de natuurlijke persoon die de machtiging registreert is deugdelijk geauthentiseerd;

b. tijdens het registratieproces wordt deugdelijk vastgesteld dat de te registreren bevoegdheid rechtsgeldig tot stand is gekomen en dat is voldaan aan artikel 6, derde lid, van het Besluit BO;

c. de registratie bevat informatie over de handelingen waarop de geregistreerde bevoegdheid ziet en, in voorkomend geval, een moment waarop deze van kracht wordt of vervalt;

d. bij het registreren van een machtiging wordt voor de koppeling aan een natuurlijke persoon gebruik gemaakt van pseudonimisering met een voor dat doel verstrekte authenticatiecode.

Artikel 2.17 Beheer van machtigingen

Een aanvrager van een erkenning als bedoeld in artikel 11, tweede lid, van de wet heeft voorzieningen om te borgen dat geregistreerde bevoegdheden als bedoeld in artikel 2.16 deugdelijk worden beheerd, waaronder in ieder geval wordt begrepen zorg voor de actualiteit en juistheid van geregistreerde machtigingen.

Artikel 2.18 Gebruik van authenticatiecode bij bedrijfs- en organisatiemiddel

Het proces voor verzending door een machtigingsdienst van een machtigingsverklaring, dat in de aanvraag voor een erkenning als bedoeld in artikel 11, derde lid, van de wet wordt beschreven, voorziet, ter identificatie van de natuurlijke persoon die beoogt een handeling te verrichten, in het verzenden door de machtigingsdienst aan een publieke dienstverlener van de authenticatiecode die tijdens het authenticatieproces voor de desbetreffende machtigingsverklaring is aangemaakt.

Artikel 2.19 Inzage in gegevens door gebruikers machtigingsdienst

Een aanvrager van een erkenning voor een machtigingsdienst als bedoeld in artikel 11, derde lid, van de wet, heeft voorzieningen om:

a. aan een gebruiker, na een authenticatie van die gebruiker, in ieder geval elektronisch inzage te geven in:

i. de datum en het tijdstip waarop voor die gebruiker een machtigingsverklaring is verzonden aan een publieke dienstverlener of een andere erkende machtigingsdienst, onder vermelding van de publieke dienstverlener waarbij en de dienst waarvoor die machtigingsverklaring is verzonden;

ii. de persoonsgegevens die over de desbetreffende gebruiker zijn verwerkt;

iii. de bevoegdheden van de desbetreffende gebruiker die door de aanvrager van de erkenning zijn geregistreerd en het moment waarop die registratie plaatsvond;

iv. overige gegevens die over de desbetreffende gebruiker voor het gebruik van de machtigingsdienst zijn geregistreerd; en

b. aan een persoon als bedoeld in artikel 6, derde lid, van het Besluit BO, na een authenticatie van die persoon, elektronisch inzage te geven in:

i. alle machtigingen die bij de desbetreffende machtigingsdienst namens die rechtspersoon of onderneming zijn geregistreerd;

ii. de datum en het tijdstip waarop namens de desbetreffende rechtspersoon of onderneming een machtigingsverklaring is verzonden aan een publieke dienstverlener of een andere erkende machtigingsdienst, onder vermelding van de publieke dienstverlener waarbij en de dienst waarvoor die machtigingsverklaring is verzonden.

Artikel 2.20 Eisen aan inhoud machtigingsverklaring

Een aanvrager heeft voorzieningen om een machtigingsverklaring als bedoeld in artikel 6, eerste lid, onderdeel c, van het Besluit BO, af te geven die in ieder geval bevat:

a. de verklaring, bedoeld in artikel 6, eerste lid, onderdeel b, van het Besluit BO;

b. het door de Kamer van Koophandel voor de desbetreffende rechtspersoon of onderneming afgegeven nummer, of een ander nummer dat ter identificatie van de rechtspersoon of onderneming kan worden gebruikt of dat tot die rechtspersoon of onderneming kan worden herleid, of een versleutelde of afgeleide vorm daarvan.

Artikel 2.21 Inhoud van de overeenkomst tussen een machtigingsdienst en rechtspersoon of onderneming

Onverminderd artikel 3 van het Besluit BO wordt in de overeenkomst die door een aanvrager van een erkenning voor een machtigingsdienst als bedoeld in artikel 11, derde lid, van de wet, wordt gesloten met de rechtspersoon of onderneming een verplichting opgenomen voor de rechtspersoon of onderneming om:

a. wijzigingen in door de machtigingsdienst geregistreerde bevoegdheden zo spoedig mogelijk door te geven aan de machtigingsdienst;

b. beveiligingsincidenten die van invloed kunnen zijn op de werking van de machtigingsdienst onverwijld te melden aan de machtigingsdienst.

Paragraaf 2.6 Continuïteitsbeheer

Artikel 2.22 Continuïteitsbeheer

Een aanvrager van een erkenning heeft voorzieningen om te borgen dat kan worden voldaan aan artikel 4.4.

Paragraaf 2.7 Voorkomen van misbruik van identificatiemiddelen of herstellen van de gevolgen daarvan

Artikel 2.23 Herkennen en herstellen van beveiligingsinbreuken

1. Een aanvrager van een erkenning heeft voorzieningen om doeltreffend beveiligingsincidenten, pogingen tot het compromitteren van de beveiliging, en afwijkend gebruik van een middel ten opzichte van in de aanvraag beschreven processen en systemen te kunnen herkennen en herstellen, waarmee in ieder geval kan worden voldaan aan artikel 4.13.

2. De voorzieningen bedoeld in het eerste lid zijn dusdanig ingericht dat deze kunnen worden aangepast op basis van relevante ontwikkelingen en zien in ieder geval op:

a. potentiële en bekende kwetsbaarheden in de desbetreffende processen; en

b. het voorkomen van herhaling van beveiligingsincidenten die zich reeds hebben voorgedaan.

Artikel 2.24 Herkennen en herstellen van misbruik van identificatiemiddelen of machtigingsdiensten

1. Een aanvrager van een erkenning voor een authenticatiedienst als bedoeld in artikel 9, tweede lid, van de wet, of artikel 11, tweede lid, van de wet, heeft voorzieningen om misbruik van identificatiemiddelen of machtigingsdiensten te herkennen en herstellen overeenkomstig artikel 4.11.

2. Een aanvrager van een erkenning voor een machtigingsdienst als bedoeld in artikel 11, tweede lid, van de wet, heeft voorzieningen om misbruik van identificatiemiddelen of machtigingsdiensten te herkennen overeenkomstig artikel 4.12.

3. Een aanvrager van een erkenning voor een authenticatiedienst als bedoeld in artikel 9, tweede lid, van de wet, of artikel 11, tweede lid, van de wet, heeft voorzieningen om een identificatiemiddel in te trekken overeenkomstig artikel 4.13, eerste en derde lid.

Paragraaf 2.8 Technische werking en interoperabiliteit

Artikel 2.25 Aansluiting op GDI-voorzieningen en componenten van het stelsel

1. Een aanvrager van een erkenning voor een authenticatiedienst als bedoeld in artikel 9, tweede lid, of voor een machtigingsdienst als bedoeld in artikel 11, derde lid van de wet heeft voorzieningen om te worden aangesloten op:

a. de infrastructuur, bedoeld in artikel 5, eerste lid, onderdeel c, van de wet;

b. door de minister aangewezen registers;

c. de infrastructuur, bedoeld in artikel 5, eerste lid, onderdeel d, van de wet; en

d. de infrastructuur, bedoeld in artikel 5, tweede lid, onderdeel b.

2. Een aanvrager van een erkenning voor een authenticatiedienst als bedoeld in artikel 11, tweede lid, heeft voorzieningen om te worden aangesloten op:

a. door de minister aangewezen registers; en

b. de infrastructuur, bedoeld in artikel 5, eerste lid, onderdeel d, van de wet.

Artikel 2.26 Interoperabiliteit

1. Bij een aansluiting als bedoeld in artikel 2.25 wordt bij het uitwisselen van gegevens gebruik gemaakt van door de minister aangewezen standaarden.

2. Een aanwijzing als bedoeld in het eerste lid wordt in de Staatscourant bekendgemaakt.

Artikel 2.27 Naleving bewaartermijnen

De aanvrager van een erkenning heeft systemen voor het naleven van de bewaartermijnen die als gevolg van het Besluit digitale overheid van toepassing zijn.

Paragraaf 2.9 Publiek identificatiemiddel

Artikel 2.28 Afwijkende eisen voor publiek identificatiemiddel

1. Op een aanwijzing als bedoeld in artikel 9, eerste lid, van de wet van een publiek identificatiemiddel zijn de volgende eisen niet van toepassing:

a. paragraaf 2.1;

b. artikel 2.7, eerste lid, onderdeel a en e;

c. artikel 2.9;

d. artikel 2.15, onderdeel b.

2. Onverminderd artikel 2.15 geeft een publiek identificatiemiddel aan een gebruiker, na een authenticatie met zijn identificatiemiddel, in ieder geval elektronisch inzage in de wijze waarop met de gebruiker wordt gecommuniceerd anders dan via toegang tot de authenticatiedienst.

3. In afwijking van artikel 2.2 heeft een partij die onafhankelijk is van de aanvrager en die is aangesloten bij een beroepsorganisatie op het relevante werkgebied vastgesteld dat een aan te wijzen publiek identificatiemiddel voldoet aan de eisen voor informatiebeveiliging bij de overheid, die zijn opgenomen in de Baseline informatiebeveiliging Overheid.

Hoofdstuk 3 Regels over de aanvraag voor een erkenning

Paragraaf 3.1 Eisen aan een erkenningsaanvraag voor een authenticatiedienst

Artikel 3.1 Inhoud van de aanvraag

1. Onverminderd artikel 8 van het Besluit INP en artikel 10, tweede lid, van het Besluit BO gaat een aanvraag voor een erkenning voor een authenticatiedienst vergezeld van:

a. een beschrijving van de technische werking van het identificatiemiddel waaronder de ontwikkelprocessen en de toepassing van cryptografie daarbij;

b. een beschrijving van de processen en systemen waarop de aanvraag ziet, waaronder de interne controles op die processen en een onderbouwing dat daarmee wordt voldaan aan de eisen, gesteld krachtens artikel 9, tweede lid van de wet, met uitzondering van de eisen voor middelkwaliteit en middelbeheerkwaliteit;

c. een onderbouwing dat wordt voldaan aan de eisen die op de aangevraagde erkenning van toepassing zijn, voor zover deze zien op middelkwaliteit en middelbeheerkwaliteit, met uitzondering van artikel 2.4;

d. het certificaat, bedoeld in artikel 2.2, dat is verleend aan de aanvrager en, in voorkomend geval aan derde partijen, voor zover deze zien op processen waarop de erkenningsaanvraag ziet en de volgende daarbij behorende documenten:

i. de actuele resultaten van de risicobeoordeling en -behandeling zoals vereist door de norm ISO 27001;

ii. de verklaring van toepasselijkheid zoals vereist door de norm ISO 27001;

iii. de actuele feitenrapportage van de certificerende instelling bij het afgegeven ISO27001 certificaat waaronder de eventuele correctieve actieplannen, die zijn opgesteld door de aanvrager;

e. een beschrijving van de processen die worden uitgevoerd door een andere onderneming of rechtspersoon dan de aanvrager en de wijze waarop wordt geborgd dat die andere onderneming voldoet aan de eisen die worden gesteld aan deze processen en verwerkingsovereenkomsten die met die onderneming of rechtspersoon zijn gesloten over het verwerken van persoonsgegevens;

f. een beschrijving van de wijze waarop de aanvrager bereikbaar is voor de minister:

i. in geval van incidenten of misbruik van identificatiemiddelen; en

ii. voor operationeel overleg;

g. een beschrijving van de wijze waarop aan artikel 4.9 wordt voldaan;

h. een beschrijving van de wijze waarop een identificatiemiddel door een gebruiker kan worden geschorst of ingetrokken en waarop een schorsing kan worden opgeheven;

i. een beschrijving van de wijze waarop wordt voldaan aan artikel 2.23;

j. een beschrijving van de methode die wordt gebruikt voor het meten van de beschikbaarheid, bedoeld in artikel 4.4;

k. een uittreksel uit het handelsregister, dat op het tijdstip van het indienen van de aanvraag niet ouder is dan zes maanden;

l. een bewijs van de verzekering, bedoeld in artikel 2.1;

m. een beschrijving van de voorzieningen, bedoeld in artikel 2.22;

n. een document waaruit de structuur blijkt van de natuurlijke personen of rechtspersonen die in de aanvrager feitelijke zeggenschap of een overwegend belang in het geplaatste kapitaal hebben;

o. een geheimhoudingsverklaring die overeenkomt met de bijlage bij deze regeling en die is getekend door de aanvrager en door onderaannemers die gegevens verwerken waarop de aanvraag ziet;

p. een beschrijving van de wijze waarop de aanvrager voldoet aan artikel 4.16;

q. een beschrijving van de wijze waarop wordt voldaan aan artikel 2.3;

r. een concept van de beschrijving, bedoeld in artikel 18 van het Besluit INP of artikel 11 van het Besluit BO;

s. overige gegevens die nodig zijn om succesvol een authenticatieverzoek aan de aanvrager te kunnen verzenden, of om een authenticatieverklaring van de aanvrager te kunnen ontvangen;

t. een beschrijving van de componenten en systemen, waarin de gegevensverwerkingen, genoemd in bijlage 1, plaatsvinden, met informatie over de eventuele openbaarmaking van de broncode van de daarvoor gebruikte software en, in voorkomend geval, de open source licentie waaronder die software is gepubliceerd.

2. Onverminderd het eerste lid verstrekt de aanvrager bij de aanvraag:

a. een rapportage waarmee wordt verklaard dat er geen aanwijzingen zijn dat de middelconformiteitsonderbouwing onjuist is of dat niet aan artikel 2.4 wordt voldaan;

b. een rapportage waaruit blijkt dat de systemen die in de aanvraag worden beschreven in de praktijk met goed gevolg zijn getest op de eisen aan de internetbeveiliging, bedoeld in artikel 2.4, derde lid;

c. een rapportage waaruit blijkt dat de processen en systemen die in de aanvraag worden beschreven in de praktijk zijn getest en dat deze kunnen functioneren in samenwerking met de daarvoor benodigde onderdelen van de generieke digitale infrastructuur, bedoeld in artikel 5 van de wet, en, in voorkomend geval, andere voor de werking van het middel noodzakelijke voorzieningen;

d. een rapportage waaruit blijkt dat kan worden voldaan aan artikel 2.25.

3. Een aanvrager verstrekt bij een aanvraag verder ter onderbouwing van conformiteit met artikel 25 van de Algemene verordening gegevensbescherming:

a. een gegevensbeschermingseffectbeoordeling als bedoeld in artikel 35 van de Algemene verordening gegevensbescherming, die ziet op de activiteiten waarop de aanvraag ziet en die niet ouder is dan 12 maanden; en

b. een beschrijving van de wijze waarop de maatregelen die zijn beschreven in de gegevensbeschermingseffectbeoordeling bedoeld in het eerste lid zijn opgenomen in de processen van de aanvrager die voor de erkenning van belang zijn.

Artikel 3.2 Middeltoetsingsrapportage

1. De rapportage, bedoeld in artikel 3.1, tweede lid, onderdeel a;

a. is opgesteld door een partij die onafhankelijk is van de aanvrager en die is aangesloten bij een beroepsorganisatie op het relevante werkgebied;

b. is ten tijde van het indienen van de aanvraag niet ouder 12 maanden;

c. ziet op de beoogde wijze van implementatie van de processen en systemen die in de aanvraag worden beschreven en de daarbij gebruikte cryptografie;

d. bevat een verklaring dat er geen aanwijzingen zijn dat de onderbouwing, bedoeld in artikel 3.1, eerste lid, onderdeel c, onjuist is;

e. bevat een verklaring dat er geen aanwijzingen zijn dat met de aanvraag niet voldaan wordt aan artikel 2.4, eerste en tweede lid;

f. bevat een beschrijving van deze wijze waarop deze tot stand is gekomen, waarin in ieder geval wordt beschreven:

i. de wijze van toetsing;

ii. het gebruik van vaktechnische richtlijnen; en

iii. de competentie, ervaring, en onafhankelijkheid van de deskundigen die betrokken zijn geweest bij het opstellen van de rapportage, waarbij in ieder geval wordt ingegaan op hun kennis over de toepassing van cryptografie, en een onderbouwing dat deze voldoet aan een internationaal geaccepteerde industriestandaard rond het uitvoeren van soortgelijke toetsingen;

g. bevat een verklaring dat de overeenkomstig artikel 2.9, onderdeel d, voorgeschreven beveiligingseisen door gebruikers kunnen worden toegepast.

2. De verklaring, bedoeld in het eerste lid, onderdeel d, ziet op alle processen en systemen die nodig zijn om een authenticatie bij een publieke dienstverlener te voltooien.

3. De indiener van de rapportage draagt er zorg voor dat de partij, bedoeld in het eerste lid, onderdeel a, door de minister over de inhoud van de rapportage kan worden bevraagd.

Artikel 3.3 Rapportage van penetratietest

De rapportage, bedoeld in artikel 3.1, tweede lid, onderdeel c;

a. is opgesteld door een partij die onafhankelijk is van de aanvrager;

b. is ten tijde van het indienen niet ouder dan 12 maanden;

c. ziet op de beoogde implementatie van de processen en systemen die in de aanvraag worden beschreven;

d. beschrijft de uitgevoerde tests en de resultaten daarvan;

e. bevat in ieder geval voldoende informatie om vast te stellen dat er geen aanwijzingen zijn dat niet is voldaan aan artikel 2.4, derde lid;

f. bevat een beschrijving van deze wijze waarop deze tot stand is gekomen, waarin in ieder geval wordt beschreven:

i. het gebruik van internationaal geaccepteerde industriestandaarden;

ii. een onderbouwing dat de reikwijdte van de test de dienstverlening van de erkende dienst bereikbaar vanaf het internet omvat; en

iii. de wijze waarop bevindingen worden voorzien van een risico-inschatting op basis van impact en de kans van optreden.

Artikel 3.4 Aanvraag per identificatiemiddel

Een aanvraag voor een erkenning voor een authenticatiedienst als bedoeld in artikel 9, tweede lid, van de wet of artikel 11, tweede lid van de wet, ziet op een identificatiemiddel en een daarbij behorend proces voor:

a. verificatie van de identiteit van de beoogd gebruiker van een identificatiemiddel; en

b. authenticatie van de gebruiker bij gebruik van het identificatiemiddel.

Paragraaf 3.2 Eisen aan een erkenningsaanvraag voor een machtigingsdienst

Artikel 3.5

1. Onverminderd artikel 10, eerste lid, van het Besluit BO gaat een aanvraag voor een erkenning voor een machtigingsdienst als bedoeld in artikel 11, tweede lid, van de wet, vergezeld van:

a. een beschrijving van de technische werking van de machtigingsdienst waaronder de ontwikkelprocessen en de toepassing van cryptografie daarbij;

b. een beschrijving van de processen en systemen waarop de aanvraag ziet, waaronder de interne controles op die processen en een onderbouwing dat daarmee wordt voldaan aan de eisen, gesteld krachtens artikel 11, derde lid, van de wet;

c. het certificaat, bedoeld in artikel 2.2, en de volgende daarbij behorende documenten:

i. de actuele resultaten van de risicobeoordeling en -behandeling zoals vereist door de norm ISO 27001;

ii. de verklaring van toepasselijkheid zoals vereist door de norm ISO 27001;

iii. de actuele feitenrapportage van de certificerende instelling bij het afgegeven ISO27001 certificaat waaronder de eventuele plannen voor correctieve acties, die zijn opgesteld door de aanvrager;

d. een beschrijving van de processen die worden uitgevoerd door een andere onderneming of rechtspersoon dan de aanvrager en de wijze waarop wordt geborgd dat die andere onderneming voldoet aan de eisen die worden gesteld aan deze processen en verwerkingsovereenkomsten die met die onderneming of rechtspersoon zijn gesloten over het verwerken van persoonsgegevens;

e. een beschrijving van de wijze waarop de aanvrager bereikbaar is voor de minister:

i. in geval van incidenten of misbruik van identificatiemiddelen; en

ii. voor operationeel overleg;

f. een beschrijving van de wijze waarop wordt voldaan aan artikel 2.23;

g. een beschrijving van de methode die wordt gebruikt voor het meten van de beschikbaarheid, bedoeld in artikel 4.4;

h. een uittreksel uit het handelsregister, dat op het tijdstip van het indienen van de aanvraag niet ouder is dan zes maanden;

i. een bewijs van de verzekering, bedoeld in artikel 2.1;

j. een beschrijving van de voorzieningen, bedoeld in artikel 2.22;

k. een document waaruit de structuur blijkt van de natuurlijke personen of rechtspersonen die in de aanvrager feitelijke zeggenschap of een overwegend belang in het geplaatste kapitaal hebben;

l. een geheimhoudingsverklaring die overeenkomt met de bijlage bij deze regeling en die is getekend door de aanvrager en door onderaannemers die gegevens verwerken waarop de aanvraag ziet;

m. een beschrijving van de wijze waarop de aanvrager voldoet aan artikel 4.16;

n. een beschrijving van de wijze waarop wordt voldaan aan artikel 2.3;

o. een concept van de beschrijving, bedoeld in artikel 11 van het Besluit BO;

p. een beschrijving van de componenten en systemen, waarin de gegevensverwerkingen, genoemd in bijlage 1, plaatsvinden, met informatie over de eventuele openbaarmaking van de broncode van de daarvoor gebruikte software en, in voorkomend geval, de open source licentie waaronder die software is gepubliceerd.

2. Onverminderd het eerste lid verstrekt de aanvrager bij de aanvraag:

a. een rapportage waaruit blijkt dat de processen en systemen die in de aanvraag worden beschreven in de praktijk zijn getest en dat deze kunnen functioneren in samenwerking met de daarvoor benodigde onderdelen van de generieke digitale infrastructuur, bedoeld in artikel 5 van de wet, en, in voorkomend geval, andere voor de werking van het middel noodzakelijke voorzieningen;

b. een rapportage waaruit blijkt dat de systemen die in de aanvraag worden beschreven in de praktijk met goed gevolg zijn getest op internetbeveiliging en dat deze voldoet aan artikel 2.4, derde lid;

c. een rapportage waaruit blijkt dat kan worden voldaan aan artikel 2.25.

3. Een aanvrager verstrekt bij een aanvraag verder ter onderbouwing van conformiteit met artikel 25 van de Algemene verordening gegevensbescherming:

a. een gegevensbeschermingseffectbeoordeling als bedoeld in artikel 35 van de Algemene verordening gegevensbescherming, die ziet op de activiteiten waarop de aanvraag ziet; en

b. een beschrijving van de wijze waarop de maatregelen die zijn beschreven in de gegevensbeschermingseffectbeoordeling bedoeld in het eerste lid zijn opgenomen in de processen van de aanvrager die voor de erkenning van belang zijn.

Paragraaf 3.3 Nadere regels met betrekking tot het aanvraagproces

Artikel 3.6 Vereenvoudigde aanvraag

Een aanvrager die gelijktijdig een aanvraag indient voor een erkenning voor een authenticatiedienst als bedoeld in artikel 11, tweede lid, en voor een erkenning voor een machtigingsdienst als bedoeld in artikel 11, derde lid, van de wet kan volstaan met het eenmalig indienen van de documenten die zowel in artikel 3.1 als in artikel 2.5 worden genoemd.

Hoofdstuk 4 Verplichtingen voor houders van een erkenning

Paragraaf 4.1 Algemeen

Artikel 4.1 Blijvende conformiteit met aanvraag en eisen voor houders van een erkenning

1. Een houder van een erkenning:

a. hanteert bij gebruik van de erkenning de in de aanvraag beschreven processen en systemen; en

b. handelt overeenkomstig de in dit hoofdstuk opgenomen voorschriften;

c. sluit met gebruikers een overeenkomst die overeenkomt met het model dat bij de aanvraag is overgelegd.

2. Een houder van een erkenning verstrekt een bewijs van de herbevestiging, bedoeld in artikel 19, eerste lid, onderdeel c, van het Besluit INP of artikel 10, eerste lid van het Besluit BO onverwijld na ontvangst daarvan.

Artikel 4.2 Gebruik stelselcodes en authenticatiecodes

Een houder van een erkenning maakt bij elektronisch berichtenverkeer voor authenticatie- en machtigingshandelingen waarop de erkenning ziet gebruik van persoonlijke stelselcodes en authenticatiecodes die voor de desbetreffende gebruiker zijn aangemaakt.

Paragraaf 4.2 Beschikbaarheid van het middel voor gebruikers en prestatieverplichtingen

Artikel 4.3 Leveringsplicht

De termijn, bedoeld in artikel 19, eerste lid, van het Besluit INP en artikel 12, zevende lid, van het Besluit BO, waarbinnen een houder van een erkenning het identificatiemiddel of de machtigingsdienstverlening aanbiedt, is drie maanden na het van kracht worden van die erkenning.

Artikel 4.4 Beschikbaarheidsnorm

1. De beschikbaarheidsnorm, bedoeld in artikel 7, zesde lid, van het Besluit BO en artikel 22, tweede lid, van het Besluit INP, bedraagt 99,5 procent voor een erkende authenticatiedienst en voor een erkende machtigingsdienst.

2. De beschikbaarheid, bedoeld in het eerste lid, wordt voor een erkende authenticatiedienst per kalendermaand berekend door de tijdsduur waarbinnen een identificatiemiddel gedurende die kalendermaand door ten minste 99,5 procent van de gebruikers kon worden gebruikt voor authenticatie van een natuurlijke persoon te delen door de tijdsduur van de totale periode waarover de beschikbaarheid wordt berekend en het resultaat te vermenigvuldigen met 100.

3. De beschikbaarheid, bedoeld in het eerste lid, wordt voor een erkende machtigingsdienst per kalendermaand berekend door de tijdsduur waarbinnen de machtigingsdienst gedurende die kalendermaand voor ten minste 99,5 procent van de gebruikers de taken bedoeld in artikel 6, eerste lid, onderdelen b en c, subonderdeel i, van het Besluit BO kon uitvoeren te delen door de tijdsduur van de totale periode waarover de beschikbaarheid wordt berekend en het resultaat te vermenigvuldigen met 100.

4. Bij de tijdsduur, bedoeld in het tweede en derde lid, wordt de duur van een onderbreking aangemerkt als periode waarin het middel door gebruikers kon worden gebruikt, wanneer die onderbreking plaatsvindt:

a. ten behoeve van onderhoudswerkzaamheden:

i. tussen 0.00 uur en 6.00 uur die de houder van de erkenning ten minste tien dagen voorafgaand aan de werkzaamheden heeft aangekondigd op de website waarop gebruikers informatie over het middel kunnen vinden, en

ii. voor zover in de desbetreffende kalendermaand de totale tijdsduur daarvan niet meer dan 12 uur en het aantal onderbrekingen niet meer dan vier bedraagt, of

b. buiten de verantwoordelijkheid van de houder van de erkenning.

5. De beschikbaarheid wordt gemeten overeenkomstig de in de aanvraag opgenomen methode, bedoeld in artikel 3.1, eerste lid, onderdeel k.

6. Een houder van een erkenning rapporteert maandelijks, uiterlijk op de achtste werkdag na het verstrijken van de maand waarop de rapportage ziet, aan de minister over het beschikbaarheidsniveau, bedoeld in het eerste lid, in het jaar waarop de rapportage ziet, onderverdeeld per kalendermaand, onder vermelding van:

a. de periode waarover deze is gemeten;

b. een duiding van de periodes waarbinnen het identificatiemiddel of de machtigingsdienst niet door gebruikers kon worden gebruikt, waarbij voor de gevallen bedoeld in het vierde lid, onderdeel a, de aanleiding voor de onderbreking wordt beschreven, waarbij in ieder geval onderscheid wordt gemaakt tussen onderhoud als bedoeld in het vierde lid, onderdeel a, en andere oorzaken die binnen de verantwoordelijkheid van de houder van de erkenning hebben plaatsgevonden.

7. Met gebruik als bedoeld in het tweede lid wordt bedoeld het geval waarin een authenticatieverzoek van een dienstverlener aan de houder van de erkenning correct leidt tot een authenticatieresponse aan de dienstverlener door de houder van de erkenning onder de voorwaarde dat de gebruiker het authenticatiemiddel op de voorgeschreven wijze gebruikt.

Artikel 4.5 Beveiligingsrisico's

1. Houder van een erkenning herstelt de oorzaak van een beveiligingsincident zo spoedig mogelijk.

2. Een houder van een erkenning meldt een beveiligingsincident bij de minister zo spoedig mogelijk en in ieder geval binnen 24 uur na het bij hem bekend worden van dat incident en vermeldt daarbij:

a. een beschrijving van de kwetsbaarheid die ten grondslag lag aan het risico;

b. de gevolgen die de gebeurtenis heeft of naar verwachting kan hebben voor gebruikers of publieke dienstverleners;

c. de maatregelen die de houder van de erkenning heeft genomen of gaat nemen om herhaling te voorkomen, waaronder de maatregelen ter beperking van eventuele schade als gevolg van de gebeurtenis en in voorkomend geval een planning van nog te nemen maatregelen; en

d. de informatie, bedoeld in artikel 33, tweede lid, van de Algemene verordening gegevensbescherming, indien sprake is van een inbreuk in verband met persoonsgegevens als bedoeld in artikel 4, onder 12, van die verordening.

3. Wanneer de informatie bedoeld in het tweede lid bij het doen van de melding niet of onvolledig kan worden gerapporteerd wordt de melding zo spoedig mogelijk na het bekend worden van de ontbrekende informatie door de houder van de erkenning aangevuld.

Artikel 4.6 Herstel na beschikbaarheidsincidenten

1. Onverminderd artikel 4.5 herstelt een houder van een erkenning een beschikbaarheidsincident met betrekking tot een identificatiemiddel of de machtigingsdienst waarop de erkenning ziet en die door die houder kunnen worden beëindigd binnen:

a. 6 uur, indien het een beschikbaarheidsincident betreft waarbij authenticatie of het verzenden van een machtigingsverklaring voor geen van de gebruikers mogelijk is;

b. 10 uur, indien het een beschikbaarheidsincident betreft, anders dan een incident bedoeld in onderdeel a, waarbij authenticatie of het verzenden van een machtigingsverklaring voor 90 of meer procent van de gebruikers slechts beperkt mogelijk is;

c. 18 uur, indien het een beschikbaarheidsincident betreft waarbij authenticatie of het verzenden van een machtigingsverklaring voor minder dan 90 procent van de gebruikers slechts beperkt mogelijk is.

2. De hersteltijd, bedoeld in het eerste lid, wordt berekend vanaf het moment waarop de houder van de erkenning redelijkerwijs bekend kon zijn met het beschikbaarheidsincident, waarbij voor een situatie als bedoeld in het eerste lid, onderdeel b en c, de tijdsduur tussen 6 uur ’s avonds en 8 uur in de ochtend op werkdagen en de tijdsduur op weekend- en feestdagen niet wordt meegerekend.

3. Het eerste lid is niet van toepassing indien niet redelijkerwijs kan worden verwacht dat het incident binnen de in dat lid genoemde hersteltijd kan worden hersteld. In een dergelijk geval wordt de beschikbaarheid zo spoedig mogelijk hersteld.

4. Een houder van een erkenning beschikt over gegevens waarmee kan worden aangetoond dat hij voldoet aan dit artikel.

Artikel 4.7 Communicatie over onderbrekingen van de beschikbaarheid

1. Een houder van een erkenning maakt zo spoedig mogelijk na constatering van een beschikbaarheidsincident als bedoeld in artikel 4.6, eerste lid, onderdeel a of b, melding daarvan op een website en geeft een inschatting van het moment waarop het incident zal zijn hersteld.

2. Het eerste lid is niet van toepassing op beschikbaarheidsincidenten waarbij redelijkerwijs mag worden verwacht dat de beschikbaarheid binnen 30 minuten is hersteld.

Artikel 4.8 Bereikbaarheid voor gebruikers bij incidenten

1. Een houder van een erkenning is ten minste 60 uur per week telefonisch bereikbaar voor gebruikers.

2. De houder van een erkenning draagt er zorg voor dat het schorsen of intrekken van een identificatiemiddel door een gebruiker overeenkomstig artikel 4.12, eerste lid, onderdeel a, op ieder moment mogelijk is.

3. De houder van een erkenning maakt op een website de wijze kenbaar waarop hij bereikbaar is en op welke wijze een identificatiemiddel kan worden geschorst of ingetrokken.

Artikel 4.9 Bereikbaarheid voor minister bij incidenten en deelname aan periodiek stelseloverleg

1. De houder van een erkenning is op de overeenkomstig artikel 3.1, eerste lid, onderdeel g, subonderdeel i, opgegeven wijze op ieder moment bereikbaar voor overleg over het beheer van het stelsel, waaronder in ieder geval wordt begrepen overleg over het voorkomen of herstellen van beveiligings- of beschikbaarheidsincidenten of misbruik van identificatiemiddelen of machtigingsdiensten.

2. De houder van een erkenning gaat op verzoek van de minister onverwijld over tot het schorsen of intrekken van een identificatiemiddel.

3. De houder van een erkenning laat zich vertegenwoordigen tijdens een periodiek overleg over het beheer van het stelsel op verzoek namens de minister.

Paragraaf 4.3 Voorkomen en herstel van misbruik van identificatiemiddel en integriteit personeel

Artikel 4.10 Vervallen van middelen

1. Een houder van een erkenning:

a. verzendt aan het BSN-koppelregister ter controle ten hoogste vijf jaar na het verkrijgen van een persoonlijke stelselcode voor een gebruiker een authenticatiecode voor die gebruiker;

b. verwijdert een persoonlijke stelselcode ten hoogste vijf jaar na het verkrijgen daarvan.

2. Indien de controle, bedoeld in het eerste lid, onderdeel a, een positief resultaat heeft opgeleverd verwerkt de houder van de erkenning de persoonlijke stelselcode die voor de desbetreffende gebruiker is aangemaakt en die de houder van de erkenning na de controle ontvangt.

3. Indien de controle, bedoeld in het eerste lid, onderdeel a, geen positief resultaat heeft opgeleverd trekt de houder van de erkenning alle identificatiemiddelen in die door de houder van de erkenning aan de desbetreffende gebruikers zijn uitgegeven.

4. Een identificatiemiddel wordt door de houder van een erkenning die dat middel beheert ingetrokken of geschorst indien de gebruiker van het identificatiemiddel dat middel langer dan 5 jaar niet heeft gebruikt voor een authenticatie.

5. Een identificatiemiddel dat is geschorst als gevolg van de procedure bedoeld in het vierde lid wordt ingetrokken indien de gebruiker niet binnen 30 dagen na het ingaan van de schorsing met het desbetreffende identificatiemiddel een handeling uitvoert die zou hebben geleid tot een authenticatie in het geval waarin het desbetreffende identificatiemiddel niet zou zijn geschorst.

6. De houder van een erkenning stelt de gebruiker zo spoedig mogelijk op de hoogte van een intrekking of schorsing als bedoeld in de voorgaande leden en maakt daarvan melding tijdens het inlogproces bij gebruik van het identificatiemiddel.

7. Het derde en vierde lid zijn niet van toepassing op een identificatiemiddel dat voor de authenticatie gebruik maakt van een Nederlands identiteitsdocument.

Artikel 4.11 Gegevens ten behoeve van dispuutsafhandeling en bestrijding van misbruik van identificatiemiddelen

1. Een houder van een erkenning voor een authenticatiedienst als bedoeld in artikel 9, tweede lid, van de wet of artikel 11, tweede lid, van de wet:

a. bewaart voldoende gegevens voor onderzoeken naar misbruik van identificatiemiddelen en afhandeling van disputen over authenticatie met gebruikers of publieke dienstverleners;

b. registreert en analyseert informatie omtrent uitgifte en gebruik van identificatiemiddelen die duiden op misbruik van identificatiemiddelen op basis van patronen die zijn verstrekt door de minister;

c. draagt er zorg voor dat trends, voor zover deze duiden op authenticatiefraude worden herkend, tegengegaan en bestreden; en

d. draagt er zorg voor dat trends, voor zover deze duiden op misbruik van identificatiemiddelen anders dan authenticatiefraude, op basis van patronen die zijn verstrekt door de minister worden herkend, tegengegaan, bestreden of hersteld.

2. Een houder van een erkenning als bedoeld in het eerste lid meldt herkende trends als bedoeld in het eerste lid, onderdeel c en d aan de minister.

Artikel 4.12 Gegevens ten behoeve van dispuutsafhandeling en bestrijding van misbruik van machtigingsdiensten

1. Een houder van een erkenning voor een machtigingsdienst als bedoeld in artikel 11, derde lid, van de wet;

a. bewaart voldoende gegevens voor onderzoeken naar misbruik van identificatiemiddelen en afhandeling van disputen over verzonden machtigingsverklaringen met gebruikers of publieke dienstverleners;

b. registreert en analyseert informatie omtrent verzoeken als bedoeld in artikel 6, eerste lid, onderdeel c, van het Besluit BO die duiden op partijoverstijgend misbruik van identificatiemiddelen en geregistreerde bevoegdheden op basis van patronen die zijn verstrekt door de minister;

c. draagt er zorg voor dat trends, voor zover deze er duiden op authenticatiefraude, worden herkend, tegengegaan of bestreden; en

d. draagt er zorg voor dat trends, voor zover deze duiden op misbruik van identificatiemiddelen en geregistreerde bevoegdheden anders dan authenticatiefraude, op basis van patronen die zijn verstrekt door de minister worden herkend, tegengegaan, bestreden of hersteld.

2. Een houder van een erkenning als bedoeld in het eerste lid meldt herkende trends als bedoeld in het eerste lid, onderdeel c en d, aan de minister.

Artikel 4.13 Intrekking en schorsing van identificatiemiddelen door een authenticatiedienst

1. Een houder van een erkenning voor een authenticatiedienst als bedoeld in artikel 9, tweede lid, of artikel 11, tweede lid, van de wet:

a. stelt een gebruiker in de gelegenheid om zo spoedig mogelijk, en in ieder geval binnen 4 uur, een identificatiemiddel te laten intrekken, op een wijze die bestand is tegen een aanval met een aanvalspotentieel Enhanced-Basic;

b. gaat zo spoedig mogelijk en in ieder geval binnen 4 uur na ontvangst van een verzoek van de minister over tot schorsing of intrekking van een identificatiemiddel.

2. Indien een houder van de erkenning een identificatiemiddel op verzoek van de gebruiker kan schorsen zijn voor dat schorsen de in het eerste lid, onderdeel a, genoemde termijnen en bestandheid tegen aanvallerspotentieel van overeenkomstige toepassing.

3. Een houder van een erkenning gaat zo spoedig mogelijk, en in ieder geval binnen 4 uur, over tot intrekking of schorsing van een identificatiemiddel wanneer misbruik van dat identificatiemiddel is bevestigd of wordt vermoed als gevolg van de procedures bedoeld in artikel 4.11, eerste lid, onderdeel b, c of d.

4. Een schorsing als bedoeld in het derde lid geldt ieder geval voor de periode die nodig is om het vermoeden te onderzoeken.

5. De houder van een erkenning stelt de gebruiker zo spoedig mogelijk op een wijze die bestand is tegen een aanval met een aanvalspotentieel Enhanced-Basic op de hoogte van een intrekking of schorsing als bedoeld in de voorgaande leden en maakt daarvan melding tijdens het inlogproces bij gebruik van het identificatiemiddel.

6. Aan gebruikers wordt slechts een mogelijkheid geboden om een schorsing op te heffen wanneer die schorsing heeft plaatsgevonden op verzoek van de gebruiker. In dat geval wordt de identiteit van de gebruiker ten minste vastgesteld op een wijze die bestand is tegen een aanval met een aanvalspotentieel Enhanced-Basic.

Artikel 4.14 Verstrekken van gegevens door authenticatiedienst aan minister ten behoeve van bestrijding van misbruik van identificatiemiddelen en zelfcontrole door gebruiker

1. Een houder van een erkenning voor een authenticatiedienst als bedoeld in artikel 9, tweede lid, of artikel 11, tweede lid, van de wet, verstrekt tijdens het proces voor inschrijving, bedoeld in paragraaf 2.1 van de bijlage bij Uitvoeringsverordening (EU) 2015/1502, of bij intrekken of schorsen van een identificatiemiddel:

a. ten behoeve van partijoverstijgende detectie van misbruik van identificatiemiddelen aan een door onze minister aangewezen register:

i. de voor dat doel aangemaakte authenticatiecode voor de gebruiker, waaronder in ieder geval wordt begrepen de datum en het tijdstip waarop het middel aan de gebruiker is verstrekt en het betrouwbaarheidsniveau van het identificatiemiddel; en

ii. andere informatie die nodig is om het identificatiemiddel te herkennen, waaronder in ieder geval wordt begrepen de datum en het tijdstip waarop het middel aan de gebruiker is verstrekt en het betrouwbaarheidsniveau van het middel; en

b. ten behoeve van zelfcontrole door gebruikers aan een door de minister aangewezen register van ieder aan een gebruiker afgegeven middel:

i. de voor dat doel aangemaakte authenticatiecode voor de gebruiker; en

ii. andere informatie die nodig is voor de gebruiker om het identificatiemiddel te herkennen, waaronder in ieder geval wordt begrepen de datum en het tijdstip waarop het middel aan de gebruiker is verstrekt en het betrouwbaarheidsniveau van het middel; en

iii. informatie over de status van het identificatiemiddel waaronder informatie over schorsing, intrekking of activering van het middel.

2. Bij het verstrekken van gegevens als bedoeld in dit artikel of artikel 19 van de wet maakt de houder van een erkenning gebruik van een voor dat doel aangemaakte authenticatiecode.

Artikel 4.16 Inzet van personeel

1. Een houder van een erkenning geeft een persoon geen toegang tot vertrouwelijke informatie of processen en systemen die worden gebruikt voor registratie en uitgifte van identificatiemiddelen of

het registreren van een bevoegdheid als bedoeld in artikel 6 van het Besluit BO als deze persoon op het moment waarop deze toegang voor het eerst mogelijk wordt gemaakt geen verklaring heeft overgelegd van de overheid van het land of de landen waar de persoon de afgelopen 4 jaar woonachtig is geweest, waaruit blijkt dat er geen strafrechtelijke antecedenten bekend zijn die in de weg staan dat deze persoon:

a. bevoegd is om systemen te raadplegen die toegang geven tot vertrouwelijke gegevens of waarmee die gegevens kunnen worden gewijzigd;

b. met gevoelige informatie omgaat;

c. kennis draagt van veiligheidssystemen, controlemechanismen en verificatieprocessen.

2. Het vaststellen en controleren van de identiteit van gebruikers, waaronder het uitvoeren van een authenticiteitsonderzoek bij een fysiek identiteitsdocument, vindt plaats door middel van een proces waarmee de kwaliteit wordt geborgd en geschiedt slechts door medewerkers die daartoe een opleiding hebben gevolgd die periodiek wordt geactualiseerd.

3. Een houder van een erkenning registreert bij het combineren van gegevens als bedoeld in artikel 3, eerste lid, onderdeel e, van het Besluit INP:

a. de naam van degene die de handeling bedoeld in dat onderdeel heeft uitgevoerd;

b. het moment waarop de gegevens zijn gecombineerd.

4. Een houder van een erkenning draagt er zorg voor dat het registreren en het uitgeven van een identificatiemiddel geschiedt door verschillende personen.

5. Een houder van een erkenning draagt zorg voor de vertrouwelijke behandeling van vertrouwelijke gegevens die in het kader van de erkenning aan hem worden verstrekt, in ieder geval door medewerkers die deze gegevens kunnen inzien een geheimhoudingsverklaring te laten tekenen.

Paragraaf 4.4 Interoperabiliteit en notificatie eIDAS

Artikel 4.17 Aansluiten op stelsel

1. Een houder van een erkenning sluit aan op:

a. de infrastructuur en registers, bedoeld in artikel 2.25;

b. de voorziening, bedoeld in artikel 5, tweede lid, onderdeel a, van de wet, voor zover een notificatie als bedoeld in artikel 4.18 met succes is afgerond met inachtneming van de verplichtingen die aan die notificatie verbonden zijn.

2. Een houder van een erkenning meldt aan de minister wijzigingen met betrekking tot de gegevens, bedoeld in artikel 3.1, eerste lid, onderdeel s.

Artikel 4.18 Meewerken aan notificatie eIDAS

Een houder van een erkenning verleent in voorkomend geval medewerking aan een notificatie als bedoeld in artikel 7 van de eIDAS-verordening, welke medewerking in ieder geval inhoudt dat de

daarvoor benodigde documentatie wordt verstrekt en dat inzicht wordt geboden tot processen waarop de erkenning ziet.

Paragraaf 4.5 Beëindiging van een erkenning

Artikel 4.19 Exitplan

1. Een aanvraag voor intrekking van een erkenning als bedoeld in artikel 27 van het Besluit INP of artikel 17 van het Besluit BO wordt afgewezen wanneer de aanvrager niet heeft aangetoond dat:

a. met de aanvraag niet is geborgd dat gedurende een periode 18 maanden na het beëindigen van de dienstverlening, kan worden voldaan aan de eisen in artikel 4.11 voor zover die eisen zien op beschikbaarheid van gegevens voor dispuutafhandeling;

b. met de aanvraag niet is geborgd dat gedurende een periode van 6 maanden na het beëindigen van de dienstverlening, gebruikers en partijen onverminderd toegang hebben tot de gegevens bedoeld in onderdeel a, met uitzondering van de gegevens bedoeld in onderdeel c;

c. de te vernietigen gegevens veilig worden vernietigd.

2. Een aanvraag voor de beëindiging van een erkenning als bedoeld in het eerste lid bevat in ieder geval:

a. een omschrijving van de wijze van communicatie van de voorgenomen beëindiging van de dienstverlening aan gebruikers en andere betrokken partijen waaronder publieke dienstverleners en partijen die aan de dienstverlening gerelateerde activiteiten uitvoeren, ten minste 3 maanden voorafgaand aan de beëindigingsdatum;

b. een omschrijving van de wijze waarop de beëindiging van dienstverlening door partijen die aan de erkende dienstverlening gerelateerde activiteiten uitvoeren plaatsvindt;

c. een omschrijving van de veilige overdracht van de gegevens die in het kader van de erkenning zijn verkregen naar een houder van een soortgelijke erkenning of naar een beëindigingspartij die gebonden is aan dezelfde beschermingsmaatregelen als opgelegd vanuit de erkenning;

d. een geheimhoudingsverklaring, die overeenkomt met bijlage 1 bij deze regeling, die is getekend door derde partijen waaraan in het kader van de beëindiging gegevens worden overgedragen.

Paragraaf 4.6 Melding en rapportages

Artikel 4.20 Melden van wijzigingen

Een houder van een erkenning meldt aan Onze Minister:

a. een wijziging als bedoeld in artikel 23, eerste lid, onderdeel a, van het Besluit INP en artikel 8, eerste lid, onderdeel a, van het Besluit BO ten minste [PM] dagen voor het implementeren daarvan;

b. een wijziging in de organisatie of de zeggenschap als bedoeld in artikel 23, eerste lid, onderdeel b, van het Besluit INP en artikel 8, eerste lid, onderdeel a, van het Besluit BO ten minste [PM] dagen voordat de desbetreffende wijziging wordt doorgevoerd;

c. een wijzigingen ten aanzien van de bij een aanvraag aangeleverde beschrijving bedoeld in artikel 3.1, eerste lid, onderdeel t, of artikel 3.5, eerste lid, onderdeel p, of een publicatie van broncode voor een component, bedoeld in bijlage 1 bij deze regeling.

Artikel 4.21 Melding bij de minister

Een melding als bedoeld in artikel 4.5, tweede lid, of artikel 4.20 wordt gedaan met een door de minister beschikbaar gesteld formulier.

Artikel 4.22 Periodieke rapportages

1. Een houder van een erkenning levert aan de minister is verleend:

a. ten minste elke drie jaar een rapportage als bedoeld in artikel 3.2;

b. jaarlijks een actuele rapportage als bedoeld in artikel 3.3;

c. jaarlijks de documenten, bedoeld in artikel 3.1, eerste lid, onderdeel d, voor zover deze nog geldig zijn.

d. ten minste elke drie jaar een gegevensbeschermingseffectbeoordeling, voor zover deze moet worden opgesteld op grond van artikel 35 van de Algemene verordening gegevensbescherming.

2. De termijn, bedoeld in het eerste lid, wordt gerekend vanaf het moment van datering van de ingediende documenten.

3. Artikel 3.2, derde lid, is van overeenkomstige toepassing op een rapportage als bedoeld in het eerste lid, onderdeel a.

Paragraaf 4.7 Publiek identificatiemiddel

Artikel 4.23

1. Op een publiek identificatiemiddel is artikel 4.10, eerste lid, niet van toepassing.

2. In afwijking van artikel 4.1, eerste lid, onderdeel a, functioneert een publiek identificatiemiddel overeenkomstig de processen die aan de aanwijzing ten grondslag lagen.

Hoofdstuk 5 Slotbepalingen

Artikel 5.1 Citeertitel

Deze regeling wordt aangehaald als: Regeling nadere eisen identificatiemiddelen, authenticatiediensten en machtigingsdiensten Wdo.

Artikel 5.2 Inwerkingtreding

Deze regeling treedt in werking met ingang van [PM].

Deze regeling zal met de toelichting in de Staatscourant worden geplaatst.

Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties

Digitalisering en Koninkrijksrelaties

Alexandra C. van Huffelen

Bijlage 1 bij artikel 2.5

	Aangewezen (ja/nee)	Ingangsdatum aanwijzing
Authenticatiedienst (artt. 9, lid 1 en 2 en 11, lid 2 Wdo)		
Component: aanvraag en registratie		
Verwerking identiteitsgegevens (2.1.1 Vo)		
Gegevensverwerking tijdens het registratieproces (art. 2.7, lid 1)		
Verwerking bewijs opgegeven identiteit of bevragen gezaghebbende bron (2.1.2 Vo)		
Gegevensuitwisseling met BSNk (art. 2.7, lid 2 sub a en (indien van toepassing) art. 2.8, lid 2, sub a)		
Verwerken persoonlijke stelselcodes (art. 2.7, lid 2 sub b, i en (indien van toepassing) art. 2.8, lid 2, sub b)		
Verwijderen van BSN (art. 2.7, lid 2 sub b, ii en sub c)		
Vergelijking fysieke kenmerken (indien dit niet fysiek plaatsvindt) (2.1.2 Vo, betrouwbaarheidsniveau hoog)		
Component: uitgifte, uitreiking en activering		
Gegevensverwerking voor uitreiking (2.2.2 Vo)		
Gegevensverwerking voor activatieproces (2.2.2 Vo)		
Component: authenticatie		
Gegevensverwerking mbt authenticatiemechanisme (2.3.1 Vo)		
Gegevensverwerking tbv op bezit of kennis gebaseerde authenticatiefactoren (art. 2.12)		
Omzetting persoonlijke stelselcode naar authenticatiecode (art. 2.10, onderdeel a of art. 2.11, onderdeel a MR)		
Verstrekken authenticatiecode aan dienstverlener (art. 2.10, onderdeel b MR) of aan de machtigingsdienst (art. 2.11, onderdeel b MR)		
Component: schorsing, herroeping en reactivering		
Gegevensverwerking tbv schorsing, herroeping en reactivering (2.2.3 Vo)		
Gegevensverwerking periodieke controle inzake actualiteit en activiteit middelen (art. 4.10 MR)		
Component: verlenging en vervanging		
Gegevensverwerking tbv verlenging of vervanging (2.2.4 Vo)		
Component: bijhouden van de administratie		
Gegevensverwerking in documentenbeheersysteem (2.4.4 Vo)		
Gegevensverwerking ter naleving van de bewaartermijnen (art. 2.27 MR)		
Component: inzage		
Gegevensverwerking ihkv inzage in gebruiks- en gebruikersgegevens aan gebruiker (art. 2.15 MR)		
Gegevensverwerking tbv het centrale inzageregister (art. 4.14, lid 1, onderdeel b MR)		
Component: fraude, misbruik en dispuutafhandeling		
Gegevensverwerking tbv onderzoek naar fraude, misbruik en disputen en logging (art. 4.11, lid 1, onderdeel a en b MR)		
Gegevensverwerking tbv het herkennen, tegengaan en bestrijden van trends van authenticatiefraude (art. 4.11, lid 1, onderdeel c MR)		
Gegevensverwerking tbv het herkennen, tegengaan en bestrijden van misbruik op basis van trends verstrekt		

door de minister, onder uitsluiting van authenticatiefraude (art. 4.11, lid 1, onderdeel d MR)		
Gegevensverwerking tbv het centrale frauderegister (art. 4.14, lid 1 MR)		
Machtigingsdienst (art. 11, lid 3 Wdo)		
Component: aanvraag en registratie		
Verwerking identiteitsgegevens rechtspersoon (2.1.1 Vo)		
Verwerking bewijs opgegeven identiteit of bevragen gezaghebbende bron (2.1.3 Vo)		
Gegevensverwerking voor verificatie of persoon niet namens de rechtspersoon mag optreden (2.1.4 Vo)		
Gegevensverwerking voor de registratie en verificatie van de koppeling tussen natuurlijke persoon en rechtspersoon (2.1.4 Vo)		
Gegevensverwerking tbv de registratie van een machtiging (art. 2.16 MR)		
Gegevensverwerking tbv van het beheer van geregistreerde bevoegdheden (art. 2.17 MR)		
Component: machtigingenbeheer		
Gegevensverwerking tbv de registratie van een machtiging (art. 2.16 MR)		
Gegevensverwerking tbv van het beheer van geregistreerde machtigingen (art. 2.17 MR)		
Component: authenticatie		
Gegevensverwerking tbv het afgeven van een machtigingsverklaring (art. 2.20 MR)		
Verstrekken authenticatiecode aan dienstverlener (art. 2.18 MR)		
Component: schorsing en herroeping		
Gegevensverwerking voor de schorsing en/of herroeping van de koppeling tussen de natuurlijke persoon en rechtspersoon (2.1.4 Vo)		
Component: bijhouden van de administratie		
Gegevensverwerking in documentenbeheersysteem (2.4.4 Vo)		
Gegevensverwerking ter naleving van de bewaartermijnen (art. 2.27 MR)		
Component: inzage		
Gegevensverwerking ihkv inzage in gebruiks- en gebruikersgegevens aan gebruiker (art. 2.15 en 2.19 MR)		
Component: fraude, misbruik en dispuutafhandeling		
Gegevensverwerking tbv onderzoek naar fraude, misbruik en disputen en logging (art. 4.12, lid 1, onderdeel a en b MR)		
Gegevensverwerking tbv het herkennen, tegengaan en bestrijden van trends van authenticatiefraude (art. 4.12, lid 1, onderdeel c MR)		
Gegevensverwerking tbv het herkennen, tegengaan en bestrijden van misbruik op basis van trends verstrekt door de minister, onder uitsluiting van authenticatiefraude (art. 4.12, lid 1, onderdeel d MR)		

Artikelnummers verwijzen naar deze regeling, tenzij de aanduiding “VO” is toegevoegd. In dat geval wordt verwezen naar Uitvoeringsverordening (EU) 2015/1502.

Bijlage 2 bij artikel 3.1, eerste lid, onderdeel q

[PM: model voor geheimhoudingsverklaring]

Toelichting

1. Algemeen

Burgers, ondernemingen en rechtspersonen maken steeds meer gebruik van identificatiemiddelen om toegang te krijgen tot digitale dienstverlening in het publieke domein. De Wet digitale overheid (hierna: de wet) regelt onder meer op welke wijze die toegang kan worden verkregen. In de wet is bepaald dat toegang door natuurlijke personen, ondernemingen en rechtspersonen slechts mogelijk is met identificatiemiddelen die door de minister van Binnenlandse Zaken en Koninkrijksrelaties zijn erkend (voor zover het identificatiemiddel van private aanbieders betreft) of aangewezen (voor zover het een publiek identificatiemiddel betreft).

Aan deze erkenning of aanwijzing gaat een toetsingsprocedure vooraf, waarin wordt getoetst of de processen achter het identificatiemiddel voldoende betrouwbaar, veilig en gebruiksvriendelijk zijn. Voor een erkenning moet een aanvraag worden ingediend. De wet bepaalt dat eisen waaraan wordt getoetst en regels over de procedure voor erkenning of aanwijzing bij of krachtens algemene maatregel van bestuur worden gesteld. De wet maakt daarbij onderscheid tussen het krijgen van toegang tot publieke dienstverlening door natuurlijke personen en door ondernemingen of rechtspersonen.

In twee algemene maatregelen van bestuur zijn de kernbepalingen opgenomen ten aanzien van bescherming van gegevens, betrouwbaarheid van authenticaties en de besluitvormingsprocedure. Voor het overige bevatten deze algemene maatregelen van bestuur een basis om nadere eisen en regels te stellen bij ministeriële regeling. De onderhavige ministeriële regeling is daarop gebaseerd en bevat de aanvullende, meer gedetailleerde eisen waaraan wordt getoetst, aanvullende regels over de aanvraagprocedure voor een erkenning en nadere verplichtingen voor houders van een erkenning of aanwijzing.

2. Juridisch kader

2.1 De Wet digitale overheid

Op grond van artikel 6 van de wet moeten publieke dienstverleners de diensten die zij verlenen en waarbij elektronische toegang mogelijk is indelen in betrouwbaarheidsniveau laag, substantieel of hoog. In de Regeling betrouwbaarheidsniveaus authenticatie elektronische dienstverlening worden nadere regels gesteld over de criteria die bij dat vaststellen door publieke dienstverleners moeten worden gehanteerd.

Artikel 7 en 15 van de wet bepalen dat voor toegang tot publieke diensten op betrouwbaarheidsniveau substantieel of hoog uitsluitend identificatiemiddelen worden geaccepteerd die door de minister van Binnenlandse Zaken en Koninkrijksrelaties zijn toegelaten, of die bij de Europese Commissie zijn genotificeerd. Toelating vindt plaats op grond van de wet en notificatie op basis van de Europese verordening nr. 910/2014 (van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor

elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG, hierna: de eIDAS-verordening.[1]

De wet bevat verschillende regimes voor toetsing van identificatiemiddelen voor natuurlijke personen (artikel 9 van de wet) en voor ondernemingen en rechtspersonen (artikel 11 e.v. van de wet). Beide regimes zien op het vaststellen van de betrouwbaarheid, de veiligheid en de gebruiksvriendelijkheid van het proces waarbij de identiteit wordt bevestigd van degene die inlogt en, in het geval van ondernemingen en rechtspersonen, de bevoegdheid die deze persoon heeft om deze entiteit te vertegenwoordigen. De betrouwbaarheid van de authenticatie wordt daarbij ingeschaald in een van de betrouwbaarheidsniveaus substantieel of hoog. Voor toegang tot overheidsdienstverlening door ondernemingen en rechtspersonen maakt de wet onderscheid tussen het authentiseren van de identiteit van de natuurlijke persoon met een identificatiemiddel en het vaststellen van de bevoegdheid van die persoon om namens een onderneming of rechtspersoon te handelen.

Een toelating wordt telkens verleend voor een door een authenticatiedienst[2] aangeboden identificatiemiddel met het bijbehorende betrouwbaarheidsniveau of voor een machtigingsdienst[3] en het proces dat die dienst gebruikt om machtigingen te registreren en te beheren.

De eisen waaraan een identificatiemiddel, authenticatiedienst en een machtigingsdienst moeten voldoen om de toetsing met positief gevolg te doorlopen worden bij of krachtens algemene maatregel van bestuur vastgesteld en zien op de werking, de beveiliging en de betrouwbaarheid. In deze regelgeving worden ook regels gesteld over de toetsingsprocedure. Deze wet en onderliggende regelgeving vormen derhalve de basis voor het inrichten van een Nederlands stelsel voor toegang tot publieke diensten (hierna stelsel toegang).

Een aantal criteria voor toelating is op wetsniveau vastgelegd. Zo wordt op grond van artikel 9, zesde lid, en artikel 11, achtste lid, van de wet getoetst of voldoende gebruik wordt gemaakt van open source software, of is voldaan aan het principe van privacy by design en of met de erkenning geen inkomsten worden verkregen uit het verhandelen van persoonsgegevens. Deze criteria worden in de onderliggende algemene maatregelen van bestuur en in deze regeling verder uitgewerkt. Verder regelt de wet dat een erkenning door de minister kan worden geweigerd in het belang van de staatsveiligheid of cyberveiligheid of wanneer er sprake is van ernstig gevaar dat de erkenning wordt gebruikt voor strafbare feiten.

Voor natuurlijke personen geldt verder dat voor hen ook een publiek identificatiemiddel beschikbaar is. Artikel 5, eerste lid, onderdeel a, van de wet bepaalt dat de minister van Binnenlandse Zaken en Koninkrijksrelaties verantwoordelijk is voor het verzorgen van een dergelijk middel op verschillende betrouwbaarheidsniveaus. Een dergelijk publiek identificatiemiddel moet ook voldoen aan op grond van de wet gestelde eisen, voordat het wordt toegelaten tot het stelsel toegang.

---

[1] Artikel 9 van de wet regelt dat identificatiemiddelen voor natuurlijke personen worden toegelaten door middel van een erkenning (privaat middel) of aanwijzing (publiek middel) en dat partijen die verbonden zijn aan een identificatiemiddel voor ondernemingen en rechtspersonen worden erkend voor een dergelijk middel. In deze toelichting wordt voor de leesbaarheid de term “toelating” gehanteerd voor alle besluiten die een goedkeuring inhouden van een identificatiemiddel en die leiden tot acceptatie daarvan.

[2] Een authenticatiedienst is een partij die op basis van een identificatiemiddel een authenticatieverklaring afgeeft. Dit volgt uit artikel 1 Wdo.

[3] Een machtigingsdienst is een partij die ten behoeve van toegang tot dienstverlening een elektronische verklaring afgeeft waaruit blijkt dat een natuurlijke persoon, onderneming of rechtspersoon optreedt namens een andere natuurlijke persoon, onderneming of rechtspersoon. Dit volgt uit artikel 1 Wdo.

2.2 Twee algemene maatregelen van bestuur

In twee algemene maatregelen van bestuur is de toelatingssystematiek voor identificatiemiddelen en machtigingsdiensten nader uitgewerkt. Op grond van artikel 9 van de wet geldt het Besluit identificatiemiddelen voor natuurlijke personen WDO (hierna: Besluit INP) voor identificatiemiddelen voor natuurlijke personen. Het Besluit bedrijfs- en organisatiemiddel WDO (hierna: Besluit BO) ziet op identificatiemiddelen en machtigingsdiensten voor ondernemingen en rechtspersonen.

Het kabinet is voornemens in de tweede tranche van de WDO onder meer de regimes voor het inloggen door natuurlijke personen en door ondernemingen en rechtspersonen te uniformeren. Wanneer een dergelijke wetswijziging wordt doorgevoerd worden de beide genoemde besluiten vervangen door een geüniformeerde algemene maatregel van bestuur. Tot dat moment is ervoor gekozen de inhoud van de besluiten zoveel mogelijk te uniformeren.

Om de werking van de regels en eisen in deze ministeriële regeling te kunnen duiden is het nodig om kort in te gaan op de algemene maatregelen van bestuur waarop de regels zijn gebaseerd. In deze paragraaf wordt daarom ingegaan op de inhoud van deze beide besluiten voor zover deze relevant is voor deze ministeriële regeling. Voor een uitgebreide uiteenzetting over deze onderwerpen wordt verwezen naar de nota van toelichting bij de beide algemene maatregelen van bestuur.

2.2.1 Betrouwbaarheid van identificatiemiddelen en machtigingsdiensten: voldoen aan eisen uit eIDAS-uitvoeringsverordening

Een identificatiemiddel moet publieke dienstverleners voorzien van een betrouwbare conclusie over de identiteit van de persoon die inlogt en, in het geval van een bedrijfs- en organisatiemiddel, de bevoegdheden van die persoon om te handelen namens een onderneming of rechtspersoon. Het vaststellen van de betrouwbaarheid van een identificatiemiddel vindt primair plaats aan de hand van de eisen die zijn vastgelegd in de eIDAS-uitvoeringsverordening 2015/1502 (hierna: uitvoeringsverordening).

Het is wenselijk dat identificatiemiddelen die in Nederland door natuurlijke personen, ondernemingen en rechtspersonen kunnen worden gebruikt ook in andere lidstaten van de Europese Unie kunnen worden gebruikt voor toegang tot publieke diensten. In de algemene maatregelen van bestuur is daarom bepaald dat identificatiemiddelen in het stelsel toegang moeten voldoen aan de eisen die in uitvoeringsverordening worden gesteld, onder meer ten aanzien van de wijze waarop registratie, uitgifte van en authenticatie met een identificatiemiddel plaatsvinden. Voor zover in Europees verband richtlijnen zijn gegeven voor interpretatie en gebruik van de eisen in die verordening, worden deze ook gebruikt binnen de context van deze ministeriële regeling en de algemene maatregelen van bestuur waarop deze zijn gebaseerd.

De eisen in de uitvoeringsverordening bieden een basisniveau (minimale voorschriften) voor toetsing van de betrouwbaarheid van identificatiemiddelen en zien op alle processen die met het gebruik van een identificatiemiddel samenhangen, zoals het registeren van een middel, authenticatie en het beheer, maar ook het schorsen en intrekken ervan. Waar nodig worden deze eisen met deze regeling verder verduidelijkt of aangevuld, bijvoorbeeld wanneer dat nodig is in de Nederlandse context. In de onderdelen 2.2.2 en 2.2.3 en in hoofdstuk 3 wordt ingegaan op de eisen in deze regeling die dienen ter invulling of aanvulling van de eIDAS-eisen.

2.2.2 Verhandelverbod voor persoonsgegevens

Verder bevatten de beide algemene maatregelen van bestuur meerdere voorwaarden die borgen dat persoonsgegevens van gebruikers niet als handelswaar worden gebruikt. Partijen die betrokken zijn bij een toegang tot publieke dienstverlening mogen persoonsgegevens niet gebruiken voor andere doeleinden dan authenticatie of het verstrekken van machtigingsinformatie. Dat geldt zowel voor authenticatiediensten als voor machtingsdiensten. Ook gegevens over het inloggen namens een rechtspersoon of onderneming mogen niet worden gebruikt voor andere doeleinden.

Aan gebruikers van die diensten moet verder een mogelijkheid worden geboden om bepaalde specifieke verstrekkingen van persoonsgegevens te beëindigen. Deze verplichting ligt in het verlengde van de wettelijke toelatingseis dat geen inkomsten mogen worden verkregen uit het verhandelen van gegevens. Gebruikers van identificatiemiddelen of machtigingsdiensten krijgen een instrument om ook zelf ongewenste gegevensverstrekkingen te beëindigen.

Ook zijn er aanvullende waarborgen voorzien die bijdragen aan het effectueren van het verhandelverbod van gegevens. De beide besluiten schrijven voor dat gegevens over gebruikers gescheiden moeten worden bewaard van gegevens over het gebruik door die gebruikers. Authenticatie- en machtigingsdiensten dienen gebruikers bovendien inzage te geven in de momenten waarop scheiding tussen de gebruiksgegevens en de gebruikersgegevens is doorbroken.

2.2.3 Gebruik van software waarvan de broncode openbaar is

Door publicatie van de broncode van software wordt de werking van die software en de functies die daarmee worden uitgevoerd voor iedereen inzichtelijk. Dat vergroot de transparantie en het vertrouwen in de gepubliceerde software en betrouwbaarheid van de maker van de software. De publicatie van de broncode van identificatiemiddelen, authenticatiediensten en machtigingsdiensten past in het streven naar een transparante overheid. Daarom is in de beide algemene maatregelen van bestuur geregeld dat een erkenning slechts wordt verleend indien voor bepaalde bij ministeriële regeling aangewezen componenten software wordt gebruikt die is gepubliceerd onder een open source licentie (dat wil zeggen: waarbij in ieder geval de broncode openbaar) is of waarvan de broncode is gepubliceerd.

Componenten worden in beginsel aangewezen, zo is ook voorgeschreven in deze besluiten, tenzij een aanwijzing een risico oplevert voor de veiligheid, de continuïteit van toegang tot digitale dienstverlening van publieke dienstverleners of de beschikbaarheid van aanbod van identificatiemiddelen. Voor het aanwijzen geldt dus een “open, tenzij”- principe, terwijl relevante belangen worden meegewogen. In de motie van het lid Dekker-Abdulaziz[4] is verzocht om dit “open tenzij”-principe te hanteren.

<u>Veiligheid</u>

De verschillende genoemde belangen sluiten uit dat er een verplichting gaat gelden om open source software te gebruiken terwijl dat maatschappelijk niet verantwoord is. Een voorbeeld is het belang van veiligheid. Voor de veiligheid van software is goede ondersteuning randvoorwaardelijk. Om

[4] Kamerstukken II, 35868, nr. 11.

software in te kunnen zetten voor dienstverlening is veel nodig. Ter vergelijking: een CV-ketel is niet te gebruiken zonder dat deze wordt geïnstalleerd en regulier onderhoud krijgt. Zo zal er bij open source software hosting moeten zijn om de broncode te kunnen installeren. Maar ook beheerders die zorgen dat de software blijft draaien. Er zullen audits moeten worden gedaan die aantonen dat de software veilig is, etc. Daarvoor kan een bedrijf worden ingeschakeld dat dit organiseert, of het kan onder eigen verantwoordelijkheid (bijvoorbeeld door de overheid zelf) worden gedaan. Een essentiële randvoorwaarde voor het aanwijzen van een component waarvoor software met openbare broncode moet worden gebruikt is dan ook dat de software wordt onderzocht, onderhouden en verbeterd, waardoor de kwaliteit, veiligheid en betrouwbaarheid van de software, en daarmee de werking van inlogmiddel, geborgd is. Dit zal in het geval van deze regeling de aanbieder van een toegelaten inlogmiddel zijn die de software heeft ontwikkeld of een bedrijf dat het onderhoud en/of de ondersteuning van bepaalde open source software als dienst aanbiedt.

De sterkte, activiteit en omvang van de ondersteuning zijn randvoorwaardelijk voor de kracht en meerwaarde van open source. Is die ondersteuning er niet, dan vervalt het voordeel en kan er zelfs een risico ontstaan omdat veiligheidsproblemen niet opgemerkt worden en door kwaadwillenden benut kunnen worden.

Continuïteit van middelen

De continuïteit van de huidige – publieke en private – inlogmiddelen, veelal voor een groot deel niet open source, wordt meegewogen, om te zorgen dat burgers, ondernemingen en rechtspersonen op korte termijn niet zonder inlogmiddelen komen te zitten. Er is een redelijke termijn nodig om de software om te zetten in open source of de broncode te publiceren en daarom is gekozen om niet van de een op de andere dag een verplichting voor open source op te nemen. Deze termijn is nodig voor inlogmiddelen waarvan burgers en bedrijven nu reeds afhankelijk zijn, maar ook voor middelen van aspirant-aanbieders die graag op korte termijn toegelaten willen worden. Enerzijds om te zorgen dat burgers en bedrijven niet zonder hun bestaande middelen komen te zitten (continuïteit), maar ook om te zorgen dat nieuwe aanbieders – die waarschijnlijk ook – deels – closed source software gebruiken wel direct kunnen toetreden. Dat laatste is belangrijk omdat daarmee het aanbod spoedig kan worden vergroot en “vitaliteit” in het stelsel van middelen brengt. Aanbieders zullen dan binnen de strenge grenzen met elkaar concurreren, wat innovatie op veiligheidsmethoden en gebruiksvriendelijkheid bevorderd. Daarmee kan dus op basis van de algemene maatregelen van bestuur rekening worden gehouden bij het aanwijzen van componenten. Het toetsen aan de hand van de in het voorgaande genoemde belangen leidt ertoe dat zoveel als mogelijk componenten worden aangewezen waarvoor software met openbare broncode moet worden gebruikt. Waar dat aanwijzen nog niet verantwoord is, zal daartoe worden overgegaan zodra dat wel verantwoord kan. Dit zorgt voor een verantwoord groeimodel op basis van het genoemde “ja, tenzij”-principe.

Overige regels over open source

Verder moeten authenticatiediensten of machtigingsdiensten op grond van de beide algemene maatregelen van bestuur aan derden de mogelijkheid bieden om voorstellen voor aanpassing van de broncode te doen en kwetsbaarheden melden. Wanneer een dergelijke melding of voorstel is gedaan moet daaraan op adequate wijze opvolging worden gegeven. Aan degene die de melding doet moet worden teruggekoppeld welke acties zijn ondernomen als gevolg van deze inbreng.

Uit het voorgaande volgt dat een aanvrager van een erkenning voor componenten waarvoor dat verplicht is, kan kiezen tussen software die onder een open source licentie is gepubliceerd of

software waarvan de broncode op andere wijze openbaar is gemaakt. De gewenste transparantie wordt immers bereikt door publicatie van de broncode. Wanneer de gebruikte software niet onder een open source licentie is gepubliceerd, moet worden geborgd dat de publicatie voldoende vindbaar en toegankelijk is. De algemene maatregelen van bestuur bieden een basis voor het stellen van nadere regels in de onderhavige regeling over die publicatie en de aanwijzing van de componenten waarvan de broncode openbaar moet worden gemaakt of die onder een open source licentie zijn gepubliceerd. In paragraaf 3.2 wordt daarop ingegaan.

Behalve de bovenstaande verplichtingen in het kader software waarvan de broncode openbaar is moet een toegelaten partij op grond van de beide algemene maatregelen van bestuur een actuele beschrijving publiceren van de dienstverlening die wordt aangeboden, waaronder de ingezette softwarecomponenten en de onderlinge samenhang daartussen. In die publicatie moet onder meer worden ingegaan op de keuzes die worden gemaakt ten aanzien van het gebruik van open source software.

2.2.4 Positie van publieke identificatiemiddelen voor natuurlijke personen

In artikel 30 van het Besluit INP is vastgelegd dat eisen die voor private partijen gelden in beginsel ook op het publieke middel van toepassing zijn. In dat artikel is verder bepaald dat bij ministeriële regeling kan worden geregeld dat bepaalde eisen niet op het publieke middel van toepassing zijn. Verder maakt het besluit het mogelijk om specifieke regels te stellen aan een publiek identificatiemiddel. In deze ministeriële regeling wordt dat regime verder uitgewerkt.

2.2.5 Verhouding tussen authenticatiedienst en machtigingsdienst bij het inloggen namens een onderneming of rechtspersoon

Het Besluit bedrijfs- en organisatiemiddel beschrijft de verschillende taken van de authenticatiedienst bij het inloggen namens een onderneming of rechtspersoon. Omdat kennis daarvan nodig is om de inhoud van deze regeling te begrijpen wordt daarop kort ingegaan.

Het inlogproces start met een verzoek van de publieke dienstverlener waarbij het inloggen plaatsvindt. Dat verzoek is gericht aan de machtigingsdienst die de gebruiker heeft geselecteerd. De machtigingsdienst stuurt een authenticatieverzoek aan de authenticatiedienst waarvan de gebruiker het identificatiemiddel afneemt. De authenticatiedienst authentiseert de identiteit van een natuurlijke persoon, net als bij het inloggen door een natuurlijke persoon. De werking van dit proces en het uitgeven en registreren van een identificatiemiddel waarmee authenticatie plaatsvindt is dus hetzelfde bij een bedrijfs- en organisatiemiddel als bij een identificatiemiddel voor natuurlijke personen. De authenticatieverklaring wordt na een succesvolle authenticatie echter niet verstrekt aan de dienstverlener, maar aan de machtigingsdienst. De machtigingsdienst gaat vervolgens na of de desbetreffende persoon bevoegd is om te handelen namens de onderneming of rechtspersoon bij de betreffende dienstverlener en dienst. Bij een positief resultaat verzendt de machtigingsdienst aan de publieke dienstverlener een machtigingsverklaring, waarin de identiteit van de natuurlijke persoon wordt bevestigd en waarin wordt aangegeven namens welke onderneming of rechtspersoon de desbetreffende persoon bevoegd is te handelen.

2.3 Besluit digitale overheid

Het Besluit digitale overheid bevat onder meer regels voor het verwerken van persoonsgegevens door verschillende onderdelen van het stelsel toegang. Tot dat stelsel behoren ook de toegelaten aanbieders van identificatiemiddelen en machtigingsdiensten. Voor zover deze partijen persoonsgegevens willen verwerken moet dat zijn toegestaan op grond van de regels in het Besluit digitale overheid. Deze ministeriële regeling bevat een aantal verwerkingsverplichtingen, om bijvoorbeeld in bepaalde situatie gegevens te verstrekken aan het BSN-koppelregister. Die verstrekkingen zijn toegestaan op grond van de regels in het Besluit digitale overheid, omdat dat besluit telkens voorziet in een grondslag voor die verwerkingen.

2.4 De eIDAS-verordening

De eIDAS-verordening[5] regelt voorwaarden en de procedure voor wederzijdse erkenning van stelsels van identificatiemiddelen die een EU-lidstaat worden gebruikt. Wanneer een identificatiemiddel behoort tot een stelsel dat op grond van de eIDAS-verordening is genotificeerd, kan dat middel ook in andere EU-lidstaten worden gebruikt voor toegang tot publieke diensten. Voorwaarde voor notificatie is dat het desbetreffende middel voldoet aan de eisen die voor het betrouwbaarheidsniveau van dat middel zijn gesteld in de uitvoeringsverordening[6]. Zoals eerder vermeld in paragraaf 2.2.1 moeten aanvragers van een erkenning voldoen aan deze eisen om in aanmerkingen te komen voor een erkenning.

2.5 De Algemene verordening gegevensbescherming

De Algemene verordening gegevensbescherming (hierna AVG) bevat verplichtingen en waarborgen op het gebied van bescherming van persoonsgegevens. Anders dan de Europese eIDAS-regels voor de betrouwbaarheid van identificatiemiddelen bevat de AVG-verplichtingen die gevolgen hebben voor de inrichting van het stelsel toegang en voor de partijen die binnen dat stelsel actief zijn. De overheid, onder meer in de rol als aanbieder van een publiek middel, en private aanbieders van zo'n middel moeten zich dus houden aan de regels van de AVG. Omdat de AVG rechtstreeks werkt, wordt in regelgeving niet opgenomen dat de inhoud daarvan van toepassing is op het stelsel toegang. Wel zijn in de beide algemene maatregelen van bestuur voor zover nodig grondslagen gecreëerd om voor zover nodig of gewenst verdere uitvoering te geven aan de verplichtingen van de AVG.

2.6 De Europese dienstenrichtlijn

Het aanbieden van een privaat identificatiemiddel of een machtigingsdienst is een dienst. Met de regels in dit besluit wordt het aanbieden van die dienst gereguleerd. Daarom is de richtlijn 2006/123/EG van het Europees Parlement en de Raad van 12 december 2006 betreffende diensten

[5] Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG

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

op de interne markt (hierna: de Dienstenrichtlijn) van toepassing. De artikelen 9 en verder van die richtlijn zijn van toepassing op de erkenning voor private identificatiemiddelen voor burgers. De eisen waaraan een private partij moet voldoen om voor een erkenning in aanmerking te komen moeten dus voldoen aan de regels in die artikelen van de Europese dienstenrichtlijn. Artikel 10, tweede lid onderdeel d, van die richtlijn bepaalt bijvoorbeeld dat die eisen duidelijk en ondubbelzinnig moeten zijn. In de formulering en de motivering van bijvoorbeeld de verleningscriteria in dit besluit en in de onderliggende ministeriële regeling wordt daarmee rekening gehouden.

3. Nadere eisen in deze ministeriële regeling

3.1 Algemeen

Voordat een identificatiemiddel wordt toegelaten wordt getoetst of dat middel voldoet aan toelatingseisen. Wanneer dat niet het geval is wordt een toelating niet verleend. Behalve eisen voor toelating gelden voor toegelaten partijen ook aanvullende eisen, waarop niet voorafgaand aan toelating, maar daarna wordt gecontroleerd. Op de laatstgenoemde eisen wordt ingegaan in hoofdstuk 5 van deze toelichting.

Het beleid voor toelating van identificatiemiddelen ziet op de betrouwbaarheid, veiligheid en de werking van die middelen en de processen die de werking van het middel mogelijk maken. Zoals in paragraaf 2.2 uiteen is gezet worden voor toelating van identificatiemiddelen voor natuurlijke personen en ondernemingen en rechtspersonen zoveel als mogelijk dezelfde eisen gehanteerd. Daarmee wordt het nu al mogelijk voor aanbieders van dergelijke middelen om voor authenticatiedienstverlening aan natuurlijke personen, waarvoor een erkenning is verleend, ook op eenvoudige wijze een erkenning te verkrijgen op grond van artikel 11 van de wet.

Het toelatingsregime dient ertoe om te borgen dat identificatiemiddelen die mogen worden gebruikt om toegang te krijgen tot de overheid veilig en betrouwbaar zijn. De eisen zorgen er derhalve onder meer voor dat gegevens van gebruikers veilig worden bewaard, dat deze niet als handelswaar worden gebruikt en dat publieke dienstverleners betrouwbaar kunnen vaststellen wie de persoon is die toegang wenst te krijgen. Verder is het wenselijk dat de toelatingseisen zodanig zijn geformuleerd dat ze deze partijen ruimte bieden zelf invulling te geven aan de wijze waarop ze dat doen om het gewenste eindresultaat te bereiken. Daardoor blijft ruimte behouden om te innoveren, voor zover dat de betrouwbaarheid en veiligheid ten goede komt. Verder bevat deze regeling eisen die specifiek noodzakelijk zijn om te borgen dat een identificatiemiddel technisch kan functioneren binnen het stelsel toegang.

3.2 Gebruik van software met openbare broncode

3.2.1 Aanwijzing componenten en datum

In paragraaf 2.2.3 is ingegaan op het aanwijzen van componenten van authenticatie- en machtigingsdiensten waarvoor software met openbare broncode moet worden gebruikt. De aanwijzing vindt plaats met bijlage 1 bij deze regeling. In die tabel worden de verschillende componenten onderscheiden die in dit verband relevant zijn en deze worden voorzien van een datum waarop daarvoor software met openbare broncode moet worden gebruikt. De relevante componenten zijn de componenten waarmee persoonsgegevens worden verwerkt. Het doel van het

open source vereiste is namelijk het realiseren van een controleerbare en transparante verwerking van persoonsgegevens. Om de componenten te kunnen onderscheiden is gebruik gemaakt van de verschillende processen die de regeling onderscheidt en waarbij persoonsgegevens worden verwerkt.

Dat heeft geleid tot de lijst met componenten in bijlage 1 bij deze regeling. Voor deze componenten moet op de daarbij genoemde datum gebruik worden gemaakt van software waarvan de broncode openbaar is gemaakt of die onder een open source licentie is gepubliceerd.

3.2.2 Wijze van publicatie van de broncode.

Zoals eerder aangegeven is het doel van de regeling om voor de genoemde componenten de gebruikte broncode openbaar te maken en daarmee transparantie te bieden. Dit kan door de broncode te publiceren of onder een open source licentie beschikbaar te stellen.

Om eenieder een reële mogelijkheid te bieden om de broncode in te zien, worden in deze regeling ook eisen gesteld aan de wijze van publicatie van de broncode. Deze regeling schrijft voor dat de broncode in dat geval openbaar en online moet worden gepubliceerd en toegankelijk moet worden gemaakt. Aan deze eisen is bijvoorbeeld niet voldaan op het moment dat de broncode slechts op bepaalde locatie fysiek uitgeprint beschikbaar is. Ook zal het mogelijk moeten zijn, om de broncode op bijvoorbeeld een werkstation te kunnen laten draaien, omdat anders geen reële mogelijkheid bestaat om de broncode te bestuderen. Een laatste belangrijke voorwaarde is dat de broncode voor eenieder toegankelijk moet zijn. Er mogen bijvoorbeeld geen personen, organisaties of groepen worden uitgesloten van toegang tot de broncode. Wel is het mogelijk om, als inzage wordt geboden, gebruik te maken van een toegangssysteem, maar dus op voorwaarde dat iedereen dat mag doen.

3.3 Uniforme eisen voor het proces van authenticatie van natuurlijke personen voor alle identificatiemiddelen

De verklaring die aan een publieke dienstverlener wordt afgegeven bij gebruik van een bedrijfs- en organisatiemiddel ziet op twee zaken. Ten eerste wordt de identiteit geauthentiseerd van de natuurlijke persoon die toegang wenst te krijgen tot de dienst. Ten tweede wordt vastgesteld of deze persoon bevoegd is te handelen namens de onderneming of rechtspersoon waarvoor deze wil handelen. Dit komt overeen met de werking van een identificatiemiddel voor natuurlijke personen. Daarom worden in deze regeling, voor zover het de authenticatie betreft van natuurlijke personen, uniforme eisen gehanteerd die gelden ongeacht of authenticatie plaatsvindt ten behoeve van het inloggen door de natuurlijke persoon zelf of voor een onderneming of rechtspersoon.

In de volgende paragrafen wordt ingegaan op de specifieke eisen die in deze regeling worden gesteld aan de wijze waarop de processen van authenticatiediensten en machtigingsdiensten functioneren.

3.3.1 Registratie- en verificatieproces

Tijdens het registratie- en verificatieproces wordt nagegaan of de identiteit van een potentiële gebruiker van een middel overeenkomt met de identiteit die de gebruiker aan het middel wenst te koppelen. Dit proces wordt gereguleerd door de eisen die zijn opgenomen in paragraaf 2.1 van de bijlage bij uitvoeringsverordening. Bij het aanvragen van een erkenning zal moeten worden

aangetoond dat aan die eisen wordt voldaan en dat het onwaarschijnlijk is dat een aanval met een bepaald aanvalspotentieel bij de gebruikte processen succesvol is. Om te kunnen functioneren binnen de context van het stelsel toegang wordt in deze een aantal aanvullende eisen gesteld, die in deze paragraaf wordt toegelicht.

Te registreren gegevens (artikel 2.7, eerste lid)

De eerste stap die een gebruiker van een identificatiemiddel moet doorlopen is het registeren van het identificatiemiddel. Daarbij worden van die gebruiker gegevens vastgelegd en gecontroleerd. Met deze stap wordt bewerkstelligd dat het identificatiemiddel inderdaad wordt gekoppeld aan de persoon op wiens naam deze wordt aangevraagd. Voor een goede werking van identificatiemiddelen is het noodzakelijk dat tijdens dat proces een vaste geüniformeerde set van gegevens wordt vastgelegd van de persoon op wiens naam het middel wordt geregistreerd.

In het stelsel toegang wordt een pseudoniem van het burgerservicenummer gebruikt om bij elektronische dienstverlening te identificeren. Een publieke dienstverlener ontvangt dit pseudoniem en kan deze ontsleutelen naar het burgerservicenummer. Bij het registratieproces worden behalve het burgerservicenummer ook de voorletters, geslachtsnaam en de geboortedatum vastgelegd, zodat een verificatie kan plaatsvinden van die gegevens in de Basisregistratie personen.

Het kan noodzakelijk zijn om rechtstreeks met gebruikers in contact te treden, bijvoorbeeld wanneer wordt vermoed dat onbevoegden toegang hebben gekregen tot het identificatiemiddel. Daarom regelt artikel 2.7, eerste lid, onderdeel e, dat van een gebruiker gegevens moeten worden geregistreerd die noodzakelijk zijn om met die gebruiker via een separaat kanaal contact op te nemen. Gedacht kan worden aan een emailadres of telefoonnummer waarop de gebruiker een bericht kan ontvangen over vermoedens van misbruik.

Gebruik van stelselcodes

Binnen het stelsel toegang wordt gewerkt met gepseudonimiseerde en versleutelde gegevens. Bij het registreren van een identificatiemiddel worden persoonsgegevens door de authenticatiedienst geregistreerd, waaronder een burgerservicenummer. Dit nummer wordt na controle in de Basisregistratie personen verwijderd en vervangen door een pseudoniem. Bij een authenticatiehandeling wordt voor die handeling op basis van het pseudoniem een specifieke code aangemaakt die door de dienstverlener kan worden ontsleuteld. Op die manier kan de publieke dienstverlener weer de beschikking krijgen over het burgerservicenummer, terwijl private authenticatie- of machtigingsdiensten dit nummer niet verwerken. Met het gebruik van deze codes wordt invulling gegeven aan de verplichtingen op grond van de Algemene verordening gegevensbescherming. Deze regeling bevat verplichtingen voor toegelaten partijen om deze codes te gebruiken.

Controleren van te verwerken gegevens (artikel 2.7, lid 2, 2.13, 4.10)

De inrichting van het stelsel toegang en publieke dienstverlening draait om het gebruik van het burgerservicenummer. Binnen dat stelsel fungeert de Basisregistratie persoon als gezaghebbende bron voor gegevens. De gegevens die de gebruiker opgeeft bij het registratieproces moeten op grond

van deze ministeriële regeling worden gecontroleerd in die basisregistratie of een afgeleide van die registratie met een gelijke mate van betrouwbaarheid.

De overheid geeft erkende partijen toegang tot dergelijke (afgeleide) registraties via het BSN-koppelregister. Een andere mogelijkheid is dat erkende partijen hun registratieproces baseren op een Nederlands identiteitsdocument en daarbij naast de gegevens genoemd in artikel 2.7 ook het documentnummer vastleggen. Vervolgens vraagt de erkende partij dan na bij de uitgever van het document, de Rijksdienst voor identiteitsgegevens (RvIG) of de Rijksdienst voor het wegverkeer (RDW), of dit identiteitsdocument geldig is. Met die controle worden impliciet ook de geregistreerde gegevens gecontroleerd. Voor deze opzet is het wel nodig dat de erkende partij over een volledige registratie beschikt van alle uitgegeven identiteitsdocumenten. De RDW beschikt daar reeds over en vanuit RvIG zal dit over enige tijd beschikbaar komen vanuit het Programma Verbeteren Reisdocumentenstelsel (VRS).

Wanneer gebruik wordt gemaakt van een degelijke afgeleide moet deze uiteraard actueel zijn, zodat ervan uit mag worden gegaan dat in de Basisregistratie personen doorgevoerde wijzigingen ook in de afgeleide zijn verwerkt.

Pas wanneer uit de controle blijkt dat de door de gebruiker opgegeven gegevens juist en actueel zijn en dat de desbetreffende persoon niet is overleden, worden de gegevens verwerkt. Deze controle moet ten minste elke vijf jaar opnieuw plaatsvinden. Dat schrijft artikel 4.10 van deze regeling voor. In paragraaf 5.6.1 van deze toelichting wordt daarop uitgebreider ingegaan.

<u>WID-document (artikel 2.7, lid 3)</u>

Deze regeling stelt verder eisen aan het gebruik van fysieke identiteitsdocumenten tijdens het registratieproces. In Nederland wordt de identiteit van personen vastgesteld met de documenten die worden genoemd in artikel 1, eerste lid, van de Wet op de identificatieplicht. In deze ministeriële regeling wordt vastgelegd dat alleen die genoemde documenten mogen worden gebruikt in het registratieproces voor een identificatiemiddel. Indien het proces gebruik maakt van een ander fysiek document wordt het desbetreffende middel niet toegelaten. Voor het publieke identificatiemiddel heeft dit niet tot gevolg dat de kring van gebruiksgerechtigden verandert.

<u>Afgeleide verificatie (artikel 2.8)</u>

Deze ministeriële regeling maakt het mogelijk om de identiteit van een natuurlijke persoon bij het registreren van een identificatiemiddel af te leiden van een publiek identificatiemiddel. Het gebruikte publieke middel moet hetzelfde betrouwbaarheidsniveau of hoger hebben als het middel dat wordt geregistreerd. Het registreren van een identificatiemiddel volgens dit proces wordt in deze toelichting afgeleide verificatie genoemd.

Het is de keuze van de aanbieder van een identificatiemiddel of afgeleide verificatie mogelijk wordt gemaakt. Wanneer deze vorm van verificatie mogelijk is zal een aanvraag voor toelating daar melding van moeten maken, omdat in de aanvraag onder meer moet worden beschreven welke processen worden gehanteerd voor verificatie.

Een gebruiker voert bij het toepassen van afgeleide verificatie een authenticatie uit met het publieke identificatiemiddel. Bij een succesvolle authenticatie worden de benodigde gegevens via het publieke identificatiemiddel verstrekt aan de authenticatiedienst, die deze gegevens verwerkt.

In beginsel is het technisch ook mogelijk om afgeleide verificatie met private identificatiemiddelen te laten plaatsvinden. Er is niet voor gekozen om deze vorm van verificatie in deze regeling toe te staan. Wanneer dat wel zou gebeuren is het mogelijk van een gecompromitteerd identificatiemiddel een ander identificatiemiddel af te leiden en daarvan weer een ander identificatiemiddel. De traceerbaarheid in geval van misbruik wordt op onacceptabele wijze beperkt wanneer een dergelijke keten van afgeleide identificatiemiddelen kan worden geregistreerd.

Eisen aan de overeenkomst met gebruiker (artikel 2.9)

Tijdens het toelatingsproces wordt getoetst of de aanvrager van een door hem te verlenen authenticatie- of machtigingsdienstverlening voldoet aan de gestelde eisen. Toegelaten partijen moeten zich vervolgens houden aan de aanvraag en aan aanvullende eisen die vanaf het van kracht worden van de erkenning gelden. Daarmee kunnen aan gebruikers geen rechtstreekse verplichtingen worden opgelegd. Het is echter wel de bedoeling om aan gebruikers bepaalde verplichtingen op te leggen. Bijvoorbeeld om een aan hen verstrekt identificatiemiddel niet te laten gebruiken door een ander en om verlies en beveiligingsincidenten zo spoedig mogelijk te melden. Gebruikers hebben wel een contractuele relatie, een overeenkomst, met de partij die het middel aan hen beschikbaar stelt. Daarom schrijft deze regeling voor dat deze overeenkomst een verplichting voor gebruikers moet bevatten om het identificatiemiddel niet door een ander te laten gebruiken, verlies en beveiligingsincidenten zo spoedig mogelijk te melden en wijzigingen in gegevens binnen een redelijke termijn door te geven.

De algemene maatregelen van bestuur bevatten al een verplichting om in de overeenkomst met gebruikers de mogelijkheid op te nemen voor die gebruikers om gegevensverstrekking te beëindigen. De eisen in deze regeling zijn een aanvulling op die eis.

Eisen aan de overeenkomst met een rechtspersoon (artikel 2.21)

Voor de diensten van een machtigingsdienst wordt een overeenkomst gesloten met de onderneming of rechtspersoon waarvoor een machtiging wordt verstrekt. Voor die overeenkomst bevat deze regeling ook eisen, die vooral zien op het doorgeven van wijzigingen of risico's aan de machtigingsdienst. Die verplichtingen gelden niet voor de gebruiker, omdat die niet in rechtstreeks contact staat met de machtigingsdienst. Van ondernemingen en rechtspersonen mag worden verwacht dat deze een of meerdere personen aanwijzen voor al het contact met de machtigingsdienst.

3.3.2 Authenticatieproces

Deze regeling bevat verder eisen aan het gebruik van een op bezit of kennis gebaseerde authenticatiefactor[7] tijdens het authenticatieproces. Een authenticatiefactor is een factor (iets wat iemand in bezit heeft of specifieke kennis) heeft waarvan is bevestigd dat deze gebonden is aan een persoon. Met deze factoren toont een gebruiker zijn of haar relatie met het identificatiemiddel aan. Voorbeelden van in de praktijk gehanteerde authenticatiefactoren zijn wachtwoorden, het bezit tokens en biometrische kenmerken. De uitvoeringsverordening bevat algemene regels over het gebruik van deze factoren. In de overwegingen bij deze uitvoeringsverordening wordt verwezen naar

7

de norm ISO/IEC 29115, die als basis heeft gediend voor de in de uitvoeringsverordening geformuleerd eisen. De in deze regeling gekozen specificaties zijn daarom “principal based” formuleringen van de vereisten die over dit onderwerp zijn opgenomen in de norm ISO/IEC 29115.

Gebruik van een bezitsfactor (artikel 2.12, eerste lid)

Bij een bezitsfactor wordt de identiteit van een persoon bevestigd door de vaststelling dat de persoon waarop de authenticatie ziet een voorwerp voorhanden heeft. De aanvullende eisen rond het gebruik van de bezitsfactor zijn gericht op het tegengaan van de kopieerbaarheid van een dergelijk object. Deze aanvulling is nodig om ondubbelzinnig duidelijk te maken dat toetsing op de kopieerbaarheid onderdeel is van het toelatingsproces.

Gebruik van een kennisfactor (artikel 2.12, tweede lid)

De aanvullende eisen met betrekking tot het gebruik van een kennisfactor gelden slechts voor identificatiemiddelen van betrouwbaarheidsniveau hoog. Met deze eisen wordt tot uitdrukking gebracht dat slechts gebruik mag worden gemaakt van kennis waarvan mag worden aangenomen dat slechts de gebruiker daarover beschikt. Daarmee wordt aangesloten bij het begrip “sole control” uit de norm ISO/IEC 29115.

Het gebruik van een kennisfactor kan op grond van deze regeling op twee manieren worden ingevuld: met verificatie van de kennisfactor onder controle van de gebruiker, of onder controle van de houder van de erkenning. De krachtigste opzet is als de kennisfactor verificatie lokaal *in* het middel plaatsvindt onder volledige controle van de gebruiker. Dit is het bijvoorbeeld het geval bij de inzet van een smartcard waarbij authenticatie pas kan plaatsvinden nadat de kennisfactor (PIN) in de smartcard is geverifieerd. De aanvullingen laten ook toe dat de verificatie van de kennisfactor bij de houder van de erkenning plaatsvindt. Daarbij worden de beveiligingseigenschappen van lokale verificatie vertaald naar de context van verificatie bij de houder van een erkenning. Belangrijk zijn daarbij dat de verificatie dan gebonden is aan een fysiek (niet kopieerbaar) object en dat elke verificatie wordt vastgelegd door de houder van een erkenning voor het geval een dispuut ontstaat tussen een overheidsorganisatie en de gebruiker van het identificatiemiddel. Voor de realisatie van de niet-kopieerbaarheid van de kennisfactor bij de houder van de erkenning zal in de praktijk vaak gebruik worden gemaakt van een zogenaamde Hardware Security Module[8] (HSM). Dit is reeds staande praktijk.

Gebruik van biometrie bij authenticatie (artikel 2.13, eerste lid)

Het gebruik van biometrische kenmerken voor authenticatie is in de afgelopen jaren sterk toegenomen. In deze regeling is bepaald dat een erkenning niet wordt verleend voor een identificatiemiddel waarbij authenticatie plaatsvindt met gebruik van biometrische gegevens. De beschikbare techniek en de vele varianten die daarvoor in omloop zijn hebben nog niet een niveau bereikt dat voldoende is voor verantwoorde toepassing bij toegang tot elektronische overheidsdiensten. Wanneer de kwaliteit van deze techniek verbetert of wanneer internationale ontwikkelingen daartoe aanleiding geven kan deze regeling worden gewijzigd om authenticatie met

[8] Een HSM is een fysiek apparaat dat bescherming biedt voor de opslag, management en gebruik van cryptografisch materiaal.

gebruik van biometrische gegevens alsnog mogelijk te maken. Deze regeling staat in beginsel niet in de weg aan verificatie van de identiteit (dus vaststelling van de identiteit ten tijde van uitgifte van een identificatiemiddel) met gebruik van biometrie. Voor die toepassing zal in een aanvraag moeten worden onderbouwd dat de gebruikte techniek voldoende betrouwbaar is om op het gewenste betrouwbaarheidsniveau te worden gebruikt.

3.4 Aanvullende eisen ten aanzien van machtigingsverklaring (paragraaf 2.5)

Paragraaf 2.5 bevat regels over de wijze waarop wordt vastgesteld of een natuurlijke persoon bevoegd is om te handelen namens een onderneming of rechtspersoon. Deze paragraaf bevat tevens andere eisen die gerelateerd zijn aan het beheer van machtigingen. Uit artikel 6 van het Besluit BO volgt dat een machtigingsverklaring aan een publieke dienstverlener wordt afgegeven door een machtigingsdienst. Een machtigingsverklaring bevat een authenticatieverklaring over de identiteit van de natuurlijke persoon en informatie over de bevoegdheden van die persoon om te handelen namens een onderneming of rechtspersoon. Een machtigingsdienst moet in staat zijn om een authenticatieverklaring op te vragen bij alle op grond van artikel 11, tweede lid, van de wet erkende authenticatiediensten.

Artikel 6, derde lid, van het Besluit BO regelt welke personen een machtiging mogen registreren bij een machtigingsdienst. Het gaat om de wettelijke vertegenwoordiger en – indien van toepassing – om personen aan wie de bevoegdheid is verleend om machtigingen te registreren. Veelal is bij een onderneming of rechtspersoon een specifieke persoon belast met het registreren en beheren van machtigingen. Deze regeling bevat een aantal specifieke voorzieningen die gericht zijn op de overkoepelende beherende taak van deze persoon.

Ook bij deze eisen is aangesloten bij de eisen in de uitvoeringsverordening. Een deel van deze eisen heeft een open karakter. Dergelijke open normen kunnen op gespannen voet staan met het beginsel van rechtszekerheid en artikel 10, tweede lid, van de Europese dienstenrichtlijn. In dat geval wordt met “good practices” verduidelijkt op welke wijze in ieder geval kan worden voldaan aan de (open) toelatingseis. Met deze constructie is beoogd ruimte voor innovatie te behouden voor partijen die die ruimte willen benutten, terwijl potentiële aanvragers kunnen weten wat nodig is om een erkenning te verkrijgen.

3.4.1 Registratie van een machtiging door een machtigingsdienst (artikel 2.16)

Artikel 6, derde lid, van het Besluit BO bepaalt dat een bevoegdheid door een machtigingsdienst slechts mag worden geregistreerd “na instemming van een wettelijke vertegenwoordiger van de betrokken onderneming of rechtspersoon of na instemming van een door die wettelijke vertegenwoordiger gemachtigde”. In artikel 2.16 van deze regeling is verder uitgewerkt aan welke eisen de registratieprocedure voor een machtiging moet voldoen. Zo volgt uit onderdeel c van dat artikel dat de registratie informatie moet bevatten over de reikwijdte van de machtiging, dus over de handelingen die de gemachtigde namens de onderneming of rechtspersoon mag uitvoeren.

3.4.2 Beheer van machtigingen (artikel 2.17)

Nadat een machtiging is geregistreerd moet deze worden bewaard en kunnen daaraan wijzigingen plaatsvinden. De processen die daarvoor zijn ingericht moeten deugdelijk zijn. Bijvoorbeeld moet

worden voorkomen dat machtigingen niet meer actueel zijn of dat onjuiste gegevens niet tijdig worden gecorrigeerd. Het is aan aanvragers om te kiezen op welke wijze aan deze verplichting wordt voldaan. In de aanvraag moet daarop worden ingegaan. In good practices zal worden vastgelegd op welke wijze invulling kan worden gegeven aan deze verplichting, zodat potentiële aanvragers weten op welke wijze aan dit artikel kan worden voldaan.

3.4.3 Inzage in gegevens door gebruikers en degene die machtigingen registreert (artikel 2.19)

Een gebruiker van een bedrijfs- en organisatiemiddel moet op grond van artikel 2.15 bij een authenticatiedienst elektronisch gegevens kunnen inzien over het identificatiemiddel. Artikel 2.19, aanhef en onderdeel a, bepaalt verder dat een machtigingsdienst elektronisch inzage moet geven in de machtigingen die voor de desbetreffende persoon door die dienst zijn geregistreerd en de gegevens die daarvoor zijn verwerkt. Verder moet een gebruiker kunnen inzien welke machtigingshandelingen met het bedrijfs- of organisatiemiddel zijn verricht.

Artikel 2.19, aanhef en onderdeel b, regelt de elektronische inzage die mogelijk moet worden gemaakt voor de persoon die machtigingen registreert bij een machtigingsdienst. Die persoon kan bij een machtigingsdienst inzage krijgen in de verschillende machtigingen die namens het desbetreffende onderneming of rechtspersoon zijn geregistreerd en de momenten waarop namens de onderneming of rechtspersoon via de desbetreffende machtigingsdienst is ingelogd. Verder is er een centraal inzageregister, waarin deze persoon kan zien bij welke machtigingsdiensten namens de onderneming of rechtspersoon machtigingen zijn geregistreerd.

3.4.4 Inhoud van de overeenkomst met de onderneming of rechtspersoon (artikel 2.21)

Voor de veilige en betrouwbare werking van het stelsel toegang is het van belang dat wijzigingen en veiligheidsrisico's zo spoedig mogelijk worden doorgegeven. Een machtigingsdienst sluit hiertoe een overeenkomst met de onderneming of rechtspersoon namens welke het inloggen plaatsvindt.

3.5 Bescherming van burgers, ondernemingen en rechtspersonen tegen authenticatiefraude en misbruik, en herstel van de gevolgen daarvan (artikel 2.24)

De werking van een identificatiemiddel moet het herkennen van misbruik mogelijk maken, moet waarborgen bevatten om misbruik tegen te gaan en moet herstel van de gevolgen van misbruik vereenvoudigen. Burgers, ondernemingen en rechtspersonen die door misbruik van hun identificatiemiddel in de problemen komen moeten kunnen worden geholpen. De eisen die worden gesteld aan identificatiemiddelen en de achterliggende processen zijn erop gericht om dat mogelijk te maken. Daarvoor wordt van betrokken partijen geëist dat zij maatregelen nemen om misbruik te herkennen en tegen te gaan. Verder worden daarvoor op het niveau van het stelsel ook maatregelen genomen. Van partijen wordt geëist dat zij daaraan deelnemen. Die eisen zijn opgenomen in deze regeling.

Misbruik, waaronder ook wordt begrepen authenticatiefraude, kan met preventieve maatregelen, gericht op veilige uitgifte en werking van identificatiemiddelen en toezicht daarop, nooit geheel worden voorkomen. Volledige zekerheid is, met steeds wijzigende digitale dreigingen, niet haalbaar. Daarom is het verstandig en noodzakelijk om ook het herstelvermogen in het stelsel toegang te borgen. Daarmee wordt in dit verband bedoeld het vermogen en de plicht van aanbieders van

inlogmiddelen om misbruik vroegtijdig te kunnen herkennen en te zorgen dat een middel van de gebruiker niet (meer) misbruikt kan worden. Zodat de gevolgen ervan voor burgers, ondernemingen en rechtspersonen voorkomen kunnen worden of door overheden kunnen worden hersteld. Ook dient lering te worden getrokken uit opgetreden problemen ter voorkoming van toekomstige gevallen. De toelatingseisen zijn erop gericht om dit herstelvermogen te borgen.

Op grond van de beide besluiten worden daarom slechts identificatiemiddelen toegelaten indien aan gebruikers van die middelen inzage wordt geboden in de authenticatiehandelingen die met het identificatiemiddel zijn verricht en het moment waarop de scheiding tussen gebruikersgegevens en gegevens over het gebruik is doorbroken. Als gevolg van artikel 4.16, derde lid, moet ook worden geregistreerd welke medewerker de scheiding heeft doorbroken. Die informatie wordt niet aan gebruikers getoond.

Met deze ministeriële regeling worden aanvullende regels gesteld over het herkennen, voorkomen en herstellen van misbruik.

3.5.1 Bestandheid tegen aanvallen (artikel 2.4)

Uit de regels van de uitvoeringsverordening volgt al dat het authenticatiemechanisme en het ontwerp van een identificatiemiddel bestand moeten zijn tegen aanvallers met een aanvalspotentieel dat overeenkomt met het betrouwbaarheidsniveau van het desbetreffende middel. Deze regeling schrijft voor dat alle processen bestand moeten zijn tegen dergelijke aanvallen. De algemene maatregelen van bestuur regelen dat de eisen van uitvoeringsverordening van toepassing zijn in het Nederlandse toelatingsproces Als gevolg daarvan dient ieder identificatiemiddel te worden beoordeeld, waarbij onderzocht wordt hoeveel tijd en middelen een aanvaller moet investeren om een aanval te laten slagen.

In deze regeling wordt ervoor gekozen om toetsing op bestandheid tegen aanvallen met een bepaald aanvallerspotentieel breder toe te passen dan enkel bij het ontwerpen van en het toepassen van het authenticatiemechanisme. Een aanvaller kan er immers ook in slagen om ongeautoriseerd namens iemand anders te authentiseren door bijvoorbeeld het proces aan te vallen waarin een middel wordt gekoppeld aan de gebruiker. Daarom wordt voor alle relevant processen voorgeschreven dat deze bestand moeten zijn tegen het aanvalspotentieel dat correspondeert met het bijbehorende betrouwbaarheidsniveau.

Met aanvalspotentieel wordt in de onderhavige regeling hetzelfde bedoeld als in de uitvoeringsverordening. Processen van middelen met betrouwbaarheidsniveau laag, substantieel en hoog moeten bestand te zijn tegen respectievelijk een “enhanced-basic”, “moderate” en “high” aanvalspotentieel. Voor de wijze waarop het aanvalspotentieel wordt berekend verwijst deze regeling, evenals de uitvoeringsverordening, naar de norm ISO/IEC 18045. Deze norm, die vrij toegankelijk is, wordt gebruikt voor de zogenaamde Common Criteria certificatie van de beveiliging van producten. Vanuit de eIDAS-verordening en deze regeling wordt daarbij slechts gebruikt gemaakt van één deel van de zogenaamde Common Criteria certificatie, namelijk de bestandheid tegen aanvalspotentieel (*Advanced Vulnerability Assessment*).

Om aan te tonen dat de processen van een identificatiemiddel bestand zijn tegen een bepaald aanvalspotentieel moeten alle mogelijke relevante aanvallen op de technische werking van het identificatiemiddel en de koppeling van het middel aan de gebruiker systematisch worden geïnventariseerd en ingeschat op het benodigde aanvalspotentieel. Een identificatiemiddel is

bestand tegen een dergelijke aanval als een succesvolle aanval niet kan worden uitgevoerd met het gevraagde of een lager aanvalspotentieel.

3.5.2 Inzageverplichting (artikel 2.15)

Het is wenselijk om gebruikers in de gelegenheid te brengen om zelf controles uit te kunnen voeren op de uitreiking en het gebruik van het identificatiemiddel en de gebruikersgegevens die zijn verwerkt. Met de toelatingsregels wordt beoogd deze controles door gebruikers mogelijk te maken. De regeling schrijft voor welke informatie aan gebruikers moeten worden getoond ter invulling van deze inzageverplichting. Deze informatie maakt zelfcontrole door gebruikers mogelijk. Dit houdt in dat ze zelf kunnen inzien welk inlogmiddel aan hen is uitgereikt en waar en wanneer dit identificatiemiddel is gebruikt. Deze functionaliteit stelt gebruikers – wanneer daar aanleiding toe is – in staat om na te gaan of er ongebruikelijke transacties plaatsvinden. Authenticatiediensten dienen gebruikers toegang te geven tot de informatie nadat succesvol een authenticatie is uitgevoerd met het desbetreffende middel. Op grond van de beide algemene maatregelen van bestuur moet al aan gebruikers worden getoond op welke momenten gegevens over een gebruiker en het gebruik door die gebruiker zijn samengebracht. Artikel 2.15 regelt in welke gegevens een gebruiker verder inzage moet krijgen.

Randvoorwaardelijk voor deze zelfcontrole is dat de gebruiker (nog) weet dat er middelen op diens naam staan bij de betreffende authenticatiedienst. Deze informatie kunnen gebruikers desgewenst ook centraal achterhalen via het centrale inzageregister, als bedoeld in artikel 4.14, tweede lid, onderdeel b van deze regeling. Een houder van toegelaten partij is verplicht elk uitgereikt identificatiemiddel te registeren in een centraal register dat wordt beheerd door de minister. Bij deze registratie van een middel vermeldt de aanvrager het pseudoniem van de gebruiker in het stelsel en voldoende informatie om de gebruiker in staat te stellen het identificatiemiddel te kunnen herkennen. Dit laatste speelt met name als een gebruiker meerdere identificatiemiddelen bij dezelfde aanvrager heeft. De informatie kan dan bijvoorbeeld de laatste cijfers van een kaartnummer zijn of het type van het mobiele apparaat waarop het identificatiemiddel geïnstalleerd is. Indachtig de minimale verwerking van persoonsgegevens zullen aanvragers slechts de minimaal noodzakelijke informatie registreren.

<u>Het moment waarop een identificatiemiddel is gebruikt (onderdeel a)</u>

Aan gebruikers moeten de datum en het tijdstip kunnen worden getoond waarop met het identificatiemiddel een authenticatie is verricht. Daarbij moet worden vermeld bij welke dienstverlener de authenticatie is verricht en voor welke dienst. Gebruikers kunnen op basis van deze informatie misbruik tijdig constateren. Vervolgens kan de gebruiker nagaan welke handelingen bijvoorbeeld met een gecompromitteerd identificatiemiddel zijn verricht om eventuele onjuistheden te herstellen of schade te voorkomen. De verplichting om deze gegevens te kunnen tonen geldt slechts voor authenticaties die bij Nederlandse publieke dienstverleners zijn uitgevoerd. Dat volgt uit de definitie van het begrip “publieke dienstverlener” dat enkel op Nederlandse instanties ziet.

<u>De verwerkte gegevens (onderdeel b)</u>

Aan gebruikers worden de verwerkte gegevens getoond, zodat deze de juistheid daarvan kan controleren en voor zover nodig kan corrigeren. Op deze wijze kunnen gebruikers zelf aan de bel trekken als zij constateren dat er met hun middel acties zijn uitgevoerd, die zij niet herkennen.

De aan deze gebruiker uitgereikte identificatiemiddelen (onderdeel c)

Een gebruiker kan in voorkomende gevallen meerdere identificatiemiddelen gebruiken van dezelfde toegelaten aanbieder van een inlogmiddel. Die situatie doet zich bijvoorbeeld voor wanneer deze gebruiker bij een aanbieder identificatiemiddelen op verschillende betrouwbaarheidsniveaus afneemt. Voorkomen moet worden dat een gebruiker het zicht verliest op de middelen die op zijn of haar naam zijn geregistreerd. Deze regeling schrijft daarom voor dat een gebruiker dat (over)zicht moet worden geboden. Gebruikers kunnen vervolgens overbodig geworden of frauduleus geregistreerde identificatiemiddelen op hun naar intrekken bij de aanbieder van het betreffende inlogmiddel.

Overige gegevens die over de desbetreffende gebruiker zijn geregistreerd ten behoeve van authenticatie (onderdeel d)

Tijdens het registratieproces worden mogelijk ook andere gegevens verwerkt die nodig zijn om de authenticatie te laten slagen. De houder van een erkenning moet een gebruiker ook in die gegevens inzage geven. In bepaalde gevallen wordt bijvoorbeeld een EORI-nummer geregistreerd, dat wordt gebruikt voor uitvoeraangifte bij de Douane. Is daarvan sprake, dan moet ook dat nummer worden getoond.

3.5.3 Bescherming tegen misleiden bij inloggen (artikel 2.14)

Een vorm van fraude is het misleiden van gebruikers, waarbij deze inloggen bij een andere website dan gedacht. Om deze vorm van misleiding tegen te gaan schrijft deze regeling voor dat een gebruiker tijdens het authenticatieproces moet kunnen zien bij welke dienstverleners de authenticatie plaatsvindt. Wanneer de authenticatie wordt uitgevoerd voor een specifieke dienst moet ook aan de gebruiker worden gemeld welke dienst het betreft. Deze informatie moet aan gebruikers worden getoond op een wijze die niet door een derde partij kan worden gemanipuleerd. Daarbij kan bijvoorbeeld worden gedacht aan melding via een alternatief communicatiekanaal, dat niet wordt gebruikt voor het authenticatieproces.

Wanneer een gebruiker constateert dat de informatie die wordt getoond niet overeenkomt met de dienstverlener waarbij hij voornemens is in te loggen moet de gebruiker het authenticatieproces kunnen onderbreken.

3.5.4 Herkennen en herstellen van beveiligingsinbreuken (artikel 2.23)

Van partijen die een aanvraag indienen om te worden toegelaten wordt geëist dat zij voorzieningen hebben om beveiligingsinbreuken of pogingen daartoe te herkennen en te herstellen. Voor zover beveiligingsinbreuken of kwetsbaarheden bekend zijn moet daarmee in ieder geval rekening worden gehouden, moeten de voorzieningen daarop aangepast worden en dient herhaling voorkomen te worden. Het is aan de partij die een toelating aanvraagt om aan te geven op welke wijze aan deze verplichting wordt voldaan.

3.5.5 Gegevens bewaren om misbruik te constateren (artikel 2.24)

Om misbruik te kunnen constateren zal het nodig zijn om de werking van de systemen van de aanbieders te monitoren en daarop controles uit te voeren. Dat kan enkel plaatsvinden als gegevens die daarvoor nodig zijn beschikbaar zijn bewaard worden. Geregeld is dat een erkenning niet wordt verleend wanneer een aanvrager geen processen heeft om gegevens voor dit doeleinde te bewaren. Deze regeling gaat niet over de bevoegdheid om gegevens te verwerken. Dat regelt het Besluit digitale overheid.

3.5.6 Mogelijkheid om een identificatiemiddel in te trekken (artikel 2.24, derde lid)

Wanneer een gebruiker misbruik constateert of vermoedt dat een identificatiemiddel op zijn of haar naam is geregistreerd, moet het mogelijk zijn om de werking van dat middel te beëindigen. Artikel 4.13 bepaalt dat het voor gebruikers mogelijk moet zijn om de werking van een identificatiemiddel permanent te beëindigen. Bij de aanvraag wordt getoetst of de achterliggende processen een van deze functies of beide ondersteunen. Is dat niet het geval, dan wordt een aanvraag afgewezen. Dat is geregeld in artikel 2.24, derde lid, van deze regeling.

Wanneer een toelating is verleend gelden aanvullende regels over dit onderwerp. Die regels gaan onder meer over de snelheid waarbinnen het intrekken of schorsen moet worden uitgevoerd. Op die regels wordt ingegaan in paragraaf 5.6.7 van deze toelichting.

3.6 Continuïteitsbeheer (artikel 2.22)

Een gebruiker van een identificatiemiddel moet erop kunnen vertrouwen dat dat middel daadwerkelijk toegang geeft tot publieke dienstverlening. Met de eisen die aan aanbieders van een identificatiemiddel worden gesteld wordt dan ook geborgd dat het desbetreffende middel daadwerkelijk kan worden gebruikt wanneer de gebruiker dat wenst.

Wanneer een toelating is verleend gelden regels met betrekking tot de procentuele beschikbaarheid. Die regels bestaan uit een minimaal beschikbaarheidspercentage, 99,5 procent, en de wijze waarop wordt berekend of daaraan is voldaan. Op die regels wordt ingegaan in paragraaf 5.3 van deze toelichting.

Voorafgaand aan een toelating moet een aanvrager aangeven welke processen worden ingericht om te zorgen dat de vereiste beschikbaarheid ook daadwerkelijk zal worden gehaald. Een toelating wordt slechts verleend wanneer is gebleken dat in deze processen wordt voorzien.

3.7 Interoperabiliteit (artikel 2.26)

Tussen de componenten van het stelsel toegang vindt overdracht van gegevens plaats. Wanneer bij die communicatie geen gebruik wordt gemaakt van geüniformeerde technieken ontstaan efficiëntieverlies en risico's voor de veiligheid en betrouwbaarheid. Het stelsel toegang bestaat uit verschillende door de overheid beheerde componenten. De overheid heeft voor deze componenten in de hand welke technische standaarden worden gehanteerd. Efficiënte, veilige en betrouwbare

communicatie via of tussen deze publieke componenten kan derhalve worden geborgd door de daarvoor geëigende standaarden te hanteren.

Het stelsel toegang bestaat behalve uit publieke ook uit private componenten. Om te borgen dat de private partijen deze standaarden ook hanteren wordt gebruik daarvan ook verplicht voor de private partijen in het stelsel. Het hanteren van geüniformeerde standaarden maakt het bovendien eenvoudiger om een reeds erkend identificatiemiddel voor ondernemingen en rechtspersonen zonder veel aanpassingen te gebruiken als middel voor een natuurlijk persoon en andersom. Daarnaast is een uniformering van interoperabiliteitsstandaarden een grote stap voorwaarts richting een geharmoniseerd stelsel waarbij er geen onderscheid meer zal bestaan tussen identificatiemiddelen en authenticatiediensten voor natuurlijke personen en voor ondernemingen en rechtspersonen. Een dergelijke harmonisering wordt voorzien in de tweede tranche van de Wet digitale overheid. Deelnemende partij worden aanpassingen bespaard wanneer bij aanvang al een toekomstbestendig systeem van standaarden wordt gehanteerd.

Er wordt regelmatig een nieuwe standaard vastgesteld, vaak op korte termijn, bijvoorbeeld vanwege kwetsbaarheden in de beveiliging van bestaande standaarden. Daarom bepaalt deze regeling dat de te hanteren standaarden bij separaat besluit door de minister van Binnenlandse Zaken en Koninkrijksrelaties worden aangewezen. Wijzigingen worden ook met een dergelijk besluit vastgesteld. Uiteraard moet bij het vaststellen van gewijzigde standaarden rekening worden gehouden met de periode die redelijkerwijs nodig is om een deugdelijke implementatie van die standaarden te kunnen bewerkstelligen.

3.8 Publiek middel (artikel 2.28)

In paragraaf 2.2.4 is ingegaan op de positie van publieke identificatiemiddelen in het toelatingsproces. In beginsel zijn op het publieke identificatiemiddel de eisen van deze regeling van toepassing, tenzij deze expliciet zijn uitgezonderd. Artikel 2.28 regelt van welke eisen het publieke identificatiemiddel is uitgezonderd. In deze paragraaf wordt op die uitzonderingen ingegaan voor zover deze een beleidsmatige achtergrond hebben. Op de overige eisen, die vanuit een technisch perspectief noodzakelijk zijn, wordt ingegaan in de artikelsgewijze toelichting.

<u>Overeenkomst met gebruikers</u>

Voor private identificatiemiddelen geldt dat de aanbieder daarvan met de gebruiker een overeenkomst moet sluiten waarin regels zijn opgenomen rondom verantwoord gebruik van het middel. Voor het gebruik van een publiek identificatiemiddel wordt geen gebruikersovereenkomst afgesloten. De regels rondom het gebruik van het publieke identificatiemiddelen worden in de Regeling voorzieningen Wdo vastgelegd en hebben daarmee een publiekrechtelijke basis. Om die reden zijn eisen met betrekking tot de te sluiten overeenkomst niet van toepassing op het publieke identificatiemiddel. Verplichtingen rondom het verantwoord gebruik van een publiek identificatiemiddel zijn vastgelegd in regels die rechtstreeks van toepassing zijn op de gebruiker.

4. Regels over het aanvraagproces voor een toelating

4.1 Authenticatiediensten

Een erkenning op grond van artikel 9, tweede lid, van de wet (privaat identificatiemiddel voor natuurlijke personen) en op grond van artikel 11, tweede lid (authenticatiedienst voor een identificatiemiddel voor een onderneming of rechtspersoon) wordt op aanvraag verleend. Tijdens het beoordelen van een aanvraag wordt gecontroleerd of het identificatiemiddel dat een aanvrager wil aanbieden en de processen die daaraan gerelateerd zijn voldoen aan de daaraan gestelde eisen. De beide algemene maatregelen van bestuur schrijven voor dat de volgende documenten moet worden aangeleverd bij een aanvraag:

- bewijsstukken waarmee wordt onderbouwd dat wordt voldaan aan de eisen die van toepassing zijn op het betrouwbaarheidsniveau waarop de aanvraag ziet;
- een beschrijving van de organisatie van de onderneming of rechtspersoon en de wijze waarop de zeggenschap daarbinnen is georganiseerd;
- een model van de overeenkomst die de aanvrager zal sluiten met gebruikers van het identificatiemiddel waarop de aanvraag ziet;
- een onderbouwing dat met de aanvraag wordt voldaan aan het beginsel van privacy-by-design;
- een onderbouwing dat met de aanvraag wordt voldaan aan de verplichting om voldoende software met een open source licentie te gebruiken;
- het adres van de Nederlandse vestiging.

In deze regeling is bepaald dat een aantal aanvullende documenten moet worden toegevoegd aan een aanvraag.

4.1.1 Eigen onderbouwing middelkwaliteit en middelbeheerkwaliteit en conformiteit met overige eisen

Een identificatiemiddel moet voldoen aan de eisen met betrekking tot de betrouwbaarheid. Daarbij wordt onderscheid gemaakt tussen de kwaliteit van het middel, dus de betrouwbaarheid van het proces van authenticatie bij het inloggen, en middelbeheerkwaliteit, dat ziet op de registratie, het beheer en wijzigingen ten aanzien van een identificatiemiddel. Een aanvrager moet zelf onderbouwen waarom de authenticatie- en beheerprocessen voldoen aan de daaraan gestelde eisen. Dat volgt uit artikel 3.1, eerste lid, onderdeel c, van deze regeling. Daarnaast moet als gevolg van artikel 3.1, eerste lid, onderdeel b, worden onderbouwd dat is voldaan aan de overige eisen, die niet zien op middelkwaliteit en middelbeheerkwaliteit.

4.1.2 Middeltoetsingsrapportage (artikel 3.1, tweede lid, onderdeel a, en artikel 3.2)

Een aanvrager moet ook een rapportage aanleveren waarin een onafhankelijke derde partij de onderbouwing van de aanvrager over middelkwaliteit en middelbeheerkwaliteit toetst. Daarbij wordt onder meer getoetst of het waarschijnlijk is dat een aanval op de processen zal slagen. Hierbij wordt het begrip aanvalspotentieel gehanteerd. Met dat begrip wordt de potentie van een aanval bepaald aan de hand van onder meer de beschikbare voorbereidingstijd en middelen.

Het beoordelen van een dergelijke onderbouwing en het opstellen van een middeltoetsingsrapportage vergen specialistische kennis. Daarom wordt een door een externe partij opgestelde rapportage gevraagd. In artikel 3.2 is geregeld dat die externe partij ook tijdens de beoordeling van een aanvraag moet kunnen worden bevraagd over de bevindingen. Aanvragers zullen er dus in de afspraken die zij maken met deze partijen rekening mee moeten houden dat deze

bevraging moet kunnen plaatsvinden en daarover voor zover nodig contractuele afspraken moeten maken.

4.1.3 Penetratietest (artikel 3.1, tweede lid, onderdeel b, en artikel 3.3)

Uit artikel 2.4, derde lid, van deze regeling volgt dat de systemen van een aanvrager bestand moeten zijn tegen aanvallen vanaf het internet. Deze bestandheid moet worden onderbouwd met een door een derde partij opgestelde rapportage die voldoet aan de eisen in artikel 3.3.

4.1.4 Aansluit- en acceptatierapportage

Een houder van een erkenning moet aansluiten op het stelsel. Met een rapportage moet worden aangetoond dat daarvoor de nodige technische voorzieningen zijn ingericht. Logius heeft een test- en acceptatieomgeving ingericht binnen welke simulaties kunnen worden uitgevoerd. Van die omgeving kan een potentiële aanvrager gebruik maken om praktijktoetsen uit te voeren en de benodigde rapportage op te (laten) stellen.

4.2 Machtigingsdiensten

Ook voor machtigingsdiensten worden bij algemene maatregel van bestuur in het Besluit BO een aantal aan te leveren documenten voorgeschreven. Het gaat om de het eerste deel van paragraaf 4.1 genoemde stukken. Deze regeling bevat ook voor machtigingsdiensten aanvullende documenten die bij een aanvraag moeten worden gevoegd. Van machtigingsdiensten wordt ook een penetratietest en een aansluit- en acceptatierapportage gevraagd.

5. Eisen voor houders van een erkenning

Wanneer een verleende erkenning van kracht wordt geldt voor de houder daarvan een aantal verplichtingen. Artikel 9, vierde lid, en artikel 13, eerste lid, van de wet, bepalen dat dat een houder van een erkenning “voldoet aan de voor hem bij of krachtens algemene maatregel van bestuur gestelde eisen”.

Wanneer deze verplichtingen niet worden nageleefd kan handhavend worden opgetreden, bijvoorbeeld door het opleggen van een bestuurlijke boete of een last onder dwangsom. Op grond van de wet houdt Agentschap Telecom toezicht op de naleving van deze voorschriften. De minister van Binnenlandse Zaken en Koninkrijksrelaties is bevoegd tot het nemen van een handhavingsbesluit en verleent aan Agentschap Telecom mandaat voor deze besluiten. In die gevallen is sprake van handhaving op grond van de Wet digitale overheid.

Verder kan de Autoriteit Persoonsgegevens in bepaalde gevallen een boete opleggen op grond van de Uitvoeringswet AVG. Het gaat bijvoorbeeld om gevallen waarin persoonsgegevens zijn verwerkt zonder dat daarvoor een juridische basis bestond, of in strijd met regels voor het verwerken van die gegevens. In die gevallen is sprake van handhaving op basis van de Uitvoeringswet AVG en daarom wordt daarop in deze toelichting verder niet ingegaan.

5.1 Verplichtingen voor houders van een erkenning in de algemene maatregelen van bestuur

In de algemene maatregelen van bestuur zijn de verplichtingen voor houders van een erkenning verder uitgewerkt. Daarin is bijvoorbeeld geregeld dat een houder van een erkenning:

- moet beschikken over een actuele verklaring van certificering,
- over bepaalde onderwerp rapporteert op door de minister van Binnenlandse Zaken en Koninkrijksrelaties bepaalde wijze,
- het identificatiemiddel waarop de erkenning ziet daadwerkelijk aanbiedt binnen een bij ministeriële regeling te bepalen termijn,
- er zorg voor draagt dat wordt voldaan aan een bij ministeriële regeling te stellen beschikbaarheidsnorm,
- melding maakt van wijzigingen in de processen en de organisatie ten opzichte van de aanvraag en incidenten,
- zorgvuldig omgaat met gegevens en die gegevens niet gebruikt voor een ander doel dan authenticatie.

Over de gedetailleerde uitwerking van deze verplichtingen kunnen regels worden gesteld bij ministeriële regeling. In de volgende paragrafen wordt daarop ingegaan.

5.2 Leveringsplicht (artikel 4.3)

Wanneer voor een identificatiemiddel een erkenning wordt verleend moet het middel ook daadwerkelijk worden aangeboden. Daarmee wordt onnodige complexiteit voorkomen. Deze regeling bepaalt dat de termijn waarbinnen een middel daadwerkelijk moet kunnen worden gebruikt drie maanden is. Daarbij wordt gerekend vanaf het van kracht worden van de erkenning. Bij het verleningsbesluit voor de erkenning wordt bepaald wanneer deze van kracht wordt.

5.3 Beschikbaarheidsnorm en berekening daarvan (artikel 4.4)

Het is van belang dat toegang tot elektronische publieke dienstverlening in beginsel altijd mogelijk is. Onderbreking van die toegang is slechts in beperkte mate toelaatbaar. Voor houders van een erkenning geldt op grond van deze regeling dat het beschikbaarheidspercentage van de taken waarop de erkenning ziet ten minste 99,5 % moet zijn. Voor erkende authenticatiediensten geldt dat percentage dus voor het op basis van een correctie authenticatieverzoek kunnen verstrekken van een authenticatieverklaring aan publieke dienstverleners (voor het inloggen voor natuurlijke personen) of aan een machtigingsdienst (voor het inloggen namens ondernemingen en rechtspersonen). Voor een machtigingsdienst geldt dit percentage voor het opvragen van authenticatieverklaringen bij (alle) erkende authenticatiediensten en het verstrekken van een machtigingsverklaring aan publieke dienstverleners.

Deze regeling bepaalt ook de wijze waarop het beschikbaarheidspercentage wordt berekend. De beschikbaarheid wordt berekend per kalendermaand. In een kalendermaand wordt berekend welk percentage van de tijd in die maand het identificatiemiddel beschikbaar was voor tenminste 99,5 procent van de gebruikers. In het kader van onderhoudswerkzaamheden wordt het acceptabel geacht dat de beschikbaarheid van een middel wordt onderbroken. De duur van dergelijke onderbrekingen wordt dan aangemerkt als tijdsduur waarin het identificatiemiddel wel beschikbaar is en heeft dus geen negatieve gevolgen voor de beschikbaarheidsnorm van die maand. Het gaat om

onderhoudswerkzaamheden die plaatsvinden tussen 0.00 uur en 6.00 uur en ten minste tien dagen voorafgaand aan de werkzaamheden zijn aangekondigd op een website waarop de aanbieder informatie plaatst over het identificatiemiddel.

In de desbetreffende kalendermaand mag de totale tijdsduur van deze onderbrekingen niet meer dan 12 uur bedragen. Verder mag het aantal onderbrekingen in die maand niet meer zijn dan vier. Zijn er meer dan vier onderbrekingen, dan telt de vijfde mee als periode waarin het middel niet beschikbaar is. Hetzelfde geldt voor het aantal uren dat de 12 overschrijdt. Bedraagt het aantal onderhoudsuren 14 en is aan de overige criteria voldaan, dan worden twee uren aangemerkt als tijdsduur waarin het identificatiemiddel niet beschikbaar was.

Een aanvrager van een erkenning geeft in zijn erkenning aan op welke wijze de beschikbaarheid technisch wordt gemeten. Dat volgt uit artikel 3.1, eerste lid, onderdeel j.

5.6 Nadere eisen

Op grond van de algemene maatregelen van bestuur kunnen nadere eisen worden gesteld bij ministeriële regeling, bijvoorbeeld over de bereikbaarheid voor vragen van gebruikers en of over de hersteltijd van onderbrekingen in de werking van de processen. Daaraan wordt met deze regeling invulling gegeven. In de volgende paragrafen wordt ingegaan op deze nadere eisen.

5.6.1 Periodieke controle van de verwerkte gegevens en schorsing middel na inactiviteit (artikel 4.10)

De actualiteit van de gegevens over gebruikers en aan hen uitgegeven identificatiemiddelen moet zijn geborgd om de betrouwbaarheid van die middelen voldoende te kunnen garanderen. Daarom zijn processen ingeregeld om de actualiteit te kunnen borgen. In artikel 2.5, tweede lid, is geregeld dat de juistheid van te verwerken gegevens over de identiteit van de gebruiker bij registratie van een identificatiemiddel worden gecontroleerd. Vervolgens moet ten minste elke vijf jaar opnieuw een controle plaatsvinden. Deze regeling schrijft daartoe voor dat de stelselcode voor de desbetreffende gebruiker vijf jaar na uitgifte moet worden verwijderd en dat deze vervolgens opnieuw moet worden opgevraagd. Bij dat opvragen vindt een nieuwe controle plaats overeenkomstig de controle bij de eerste registratie. Wanneer uit deze controle blijkt dat de gegevens onjuist zijn wordt het desbetreffende identificatiemiddel geschorst of ingetrokken. De gebruiker wordt in dat geval van de schorsing op de hoogte gebracht. Wanneer uit een dergelijke controle blijkt dat de desbetreffende persoon is overleden, wordt het identificatiemiddel ingetrokken. Bij een volgende inlogpoging met dat middel moet tijdens het inlogproces worden gemeld dat het middel is ingetrokken.

Wanneer onjuiste gegevens de aanleiding zijn voor de schorsing, wordt de gebruiker in de gelegenheid gesteld de onjuiste gegevens te corrigeren. De houder van de erkenning mag de termijn kiezen waarbinnen een correctie mogelijk is. Wanneer de gebruiker gecorrigeerde gegevens aanlevert wordt de schorsing opgeheven, zodat het identificatiemiddel weer kan worden gebruikt.

Een schorsing of intrekking vindt ook plaats wanneer met een middel gedurende een periode van meer dan vijf jaar geen authenticatie is uitgevoerd. De gebruiker wordt daarvan op de hoogte gesteld. Een schorsing mag dan slechts worden opgeheven wanneer de desbetreffende gebruiker binnen een termijn van 30 dagen een authenticatie uitvoert met het middel. Vindt een authenticatie niet plaats binnen 30 dagen, dan wordt het middel ingetrokken. De aanleiding voor deze schorsing of intrekking is niet de juistheid van de gegevens, maar het risico dat een groot aantal actieve maar

ongebruikte identificatiemiddelen met zich brengt. Er is immers een kans dat deze middelen kwijt zijn geraakt of op andere wijze in handen komen van anderen dan de rechthebbende, zonder dat de rechthebbende daar weet van heeft.

5.6.2 Herstel en melden van beveiligingsrisico's (artikel 4.5)

Ook wanneer voorzorgsmaatregelen worden genomen kunnen zich beveiligingsincidenten voordoen. Deze regeling schrijft voor dat een houder van een erkenning dergelijke incidenten zo spoedig mogelijk moet oplossen. Verwacht wordt dus dat prioriteit wordt gesteld aan het oplossen van het incident.

Een beveiligingsincident moet binnen 24 uur na het bekend worden door de houder van een erkenning worden gemeld bij de minister van Binnenlandse Zaken en Koninkrijksrelaties.

Bij het ministerie van Binnenlandse Zaken en Koninkrijksrelaties zal vervolgens een onderzoek opgestart worden. Uit dit onderzoek zal blijken of de houder van de erkenning het incident op de juiste manier heeft afgehandeld of dat er nog vervolghandelingen moeten plaatsvinden. Deze vervolghandelingen kunnen zowel door de houder van de erkenning als door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties worden uitgevoerd. Voorbeelden van vervolghandelingen kunnen zijn: het melden van het incident bij AP, een aanscherping van eisen of regels voor houders van een erkenning, het informeren van gebruikers van de dienst van de houder van de erkenning over de gevolgen van een eventueel datalek.

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties zal alle gemelde beveiligingsincidenten bewaren, zodat deze informatie gebruikt kan worden bij het herkennen van eventuele trends. Indien een trend wordt herkend zal het ministerie van Binnenlandse Zaken en Koninkrijksrelaties alle houders van een erkenning informeren, zodat de houders van een erkenning op tijd voorzorgsmaatregelen kunnen nemen ter voorkoming van vergelijkbare veiligheidsincidenten.

5.6.3 Herstel van beschikbaarheidsincidenten (artikel 4.6)

Voor gebruikers is het van belang dat het middel dat zij gebruiken daadwerkelijk toegang geeft tot publieke dienstverlening. Zoals in paragraaf 5.3 is uitgelegd zijn erkende partijen verplicht te zorgen voor een beschikbaarheidsnorm van ten minste 99,5 procent.

Verder gelden voor deze partijen verplichtingen ten aanzien van het herstellen van beschikbaarheidsincidenten. Deze incidenten worden verdeeld in drie categorieën, waarvoor telkens een andere hersteltermijn geldt. Daarbij is de vereiste hersteltermijn afhankelijk van de hoeveelheid gebruikers die door het incident geen gebruik kunnen maken van elektroniche, publieke diensten. Deze regeling bevat verder regels over de wijze waarop de hersteltijd wordt berekend en over de frequentie en de wijze waarop over incidenten en hersteltijd daarvan wordt gerapporteerd. Een dergelijk rapport wordt maandelijks ingediend.

Wanneer een incident als gevolg van overmacht niet binnen de daarvoor geldende termijn kan worden opgelost mag daarvoor de tijd worden genomen die ten minste nodig is. In de maandelijkse rapportage moet in dat geval worden uitgelegd waarom sprake was van overmacht en binnen welke termijn het incident is opgelost.

5.6.4 Communicatie over onderbrekingen van de beschikbaarheid (artikel 4.7)

Wanneer een identificatiemiddel niet beschikbaar is moet daarover communicatie plaatsvinden aan gebruikers. In geval van geplande werkzaamheden moet, zoals in paragraaf 5.3 is aangegeven, daarover voorafgaand aan de werkzaamheden op de website worden gecommuniceerd. Over de andere gevallen waarin de beperkte beschikbaarheid niet werd gepland schrijft deze regeling voor dat op de website moet worden aangegeven welke problemen er zijn en binnen welke termijn toegang tot publieke dienstverlening waarschijnlijk weer mogelijk is. Wanneer het gaat om een onderbreking die naar waarschijnlijkheid niet langer dan 30 minuten zal duren is een mededeling daarover op de website niet nodig.

5.6.5 Bereikbaarheid voor gebruikers (artikel 4.8)

Een gebruiker moet voor vragen, instructies of meldingen terecht kunnen bij een helpdesk die daarover nuttige informatie kan verstrekken. In beginsel wordt ervan uitgegaan dat gebruikers niet kiezen voor een middel, wanneer de daarbij geleverde ondersteuning onvoldoende is. Niettemin moet worden voorkomen dat de serviceverlening op enig moment zodanig beperkt is dat de toegang tot publieke dienstverlening daardoor in gevaar komt. Daarom bevat deze regeling minimumregels over de bereikbaarheid van zo'n helpdesk.

Ten eerste schrijft de regeling voor dat een helpdesk ten minste 60 uur per week telefonisch bereikbaar moet zijn voor gebruikers. Daarmee wordt geborgd dat gebruikers voldoende mogelijkheden hebben om direct in contact te treden met de partij waarvan zij het identificatiemiddel afnemen.

5.6.6 Bereikbaarheid voor overleg met het ministerie (artikel 4.9)

Verder is het van belang dat overleg plaatsvindt tussen de private partijen en het stelsel dat beheerd wordt door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Dat overleg kan incidenteel plaatsvinden, bijvoorbeeld wanneer zich een incident heeft voorgedaan. Deze regeling schrijft voor dat de houder van een erkenning bereikbaar moet zijn voor overleg. In de aanvraag voor erkenning moet worden aangegeven op welke wijze de houder kan worden bereikt (artikel 3.1).

Verder is het wenselijk dat er periodiek overleg wordt gevoerd. Op grond van artikel 4.9 zijn toegelaten private partijen ook gehouden deel te nemen aan dat overleg. Minimaal 4 keer per jaar wordt van een houder van een erkenning verwacht dat ze deel zal nemen aan een stelseloverleg dat georganiseerd wordt door het ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Per overleg zal het ministerie van Binnenlandse Zaken en Koninkrijksrelaties een agenda opstellen en deze ruim op tijd delen met de houders van een erkenning. Van de houder van een erkenning wordt verwacht dat de deelnemer aan het stelseloverleg, die optreedt als afgevaardigde van de houder van de erkenning, over de juiste kennis en verantwoordelijkheid beschikt om de juiste bijdrage te leveren aan de onderwerpen op de agenda.

5.6.7 Herstel van fraude en misbruik

Van toegelaten partijen wordt geëist dat zij voorzieningen hebben die zijn gericht op het voorkomen van misbruik en op herstel van gevolgen van misbruik. In paragraaf 3.5 van deze toelichting is

ingegaan op de eisen met betrekking tot fraude en misbruik die in het toelatingsproces, dus voordat het middel wordt gebruik, worden getoetst. De artikelen 4.10 tot en met 4.16 bevatten eisen die gelden voor toegelaten partijen.

Logging en monitoring (artikel 4.12)

Deze regeling verplicht houders van een erkenning om bepaalde gegevens te registreren. Het doel is tweeledig. Ten eerste wordt daarmee de mogelijkheid gecreëerd om misbruik met gebruik van identificatiemiddelen te traceren en eventuele gevolgen daarvan te beperken of ongedaan te maken. Ten tweede wordt van houders van een erkenning gevraagd om op basis van die gegevens vermoedens van misbruik tijdig te herkennen. In het laatste geval moet het identificatiemiddel waarop het vermoeden ziet op grond van artikel 4.12 permanent of tijdelijk onbruikbaar worden gemaakt.

Schorsen en intrekken (artikel 4.13)

Wanneer is gebleken dat een middel gecompromitteerd is, of wanneer wordt vermoed dat daarvan sprake is, moet het middel zo snel mogelijk onbruikbaar worden gemaakt. Deze regeling kent daarvoor twee methoden. De eerste is schorsen, waarbij een middel onbruikbaar wordt gemaakt met de mogelijkheid om het gebruik ervan later weer mogelijk te maken. De tweede methode is intrekken, waarbij het middel permanent onbruikbaar wordt gemaakt. In het toelatingsproces wordt getoetst of ten minste een van deze opties wordt aangeboden aan gebruikers. Wanneer dat niet het geval is wordt een middel niet toegelaten. Dat regelt artikel 2.15.

Nadat middelen in gebruik zijn genomen gelden voor de houder van de erkenning verplichtingen met betrekking tot het schorsen of intrekken. Dat regelt artikel 4.13. Wanneer een gebruiker verzoekt het identificatiemiddel in te trekken of schorsen moet dat verzoek zo snel mogelijk worden uitgevoerd. Het middel moet dan in ieder geval binnen 24 uur ingetrokken zijn. Wanneer het verzoek wordt gedaan vanwege een vermoeden van fraude kan de identiteit van de gebruiker veelal niet wordt geauthentiseerd met gebruik van het identificatiemiddel. Dat is immers mogelijk gecompromitteerd. Het is aan de houder van de erkenning om een methode te kiezen om de identiteit van de verzoeker met voldoende mate van zekerheid vast te stellen. Deze regeling schrijft voor dat de te hanteren methode bestand moet zijn tegen aanvalspotentieel Basic of hoger. Een middel moet ook worden ingetrokken of geschorst wanneer daartoe door de minister een verzoek wordt gedaan. Een dergelijk verzoek moet binnen 24 uur worden uitgevoerd.

Op grond van artikel 4.11 moeten vermoedens van misbruik tijdig worden herkend. Wanneer zich een dergelijk vermoeden voordoet moet het desbetreffende identificatiemiddel zo spoedig mogelijk worden ingetrokken of geschorst. Het is denkbaar dat een houder van een erkenning systemen zodanig heeft ingericht dat meerdere middelen gekoppeld zijn aan eenzelfde gebruikersaccount, terwijl enkel het account kan worden geschorst of ingetrokken. Dit artikel staat daaraan niet in de weg. Wanneer een middel wordt geschorst moet de duur van het schorsen voldoende zijn om het vermoeden te kunnen onderzoeken.

Voor machtingsdiensten zijn geen eisen over dit onderwerp opgenomen. Voor die diensten geldt op grond van artikel 2.15 de verplichting om zorg te dragen voor deugdelijk beheer. Die verplichting omvat ook tijdig verwerken van wijzigingen in geregistreerde machtigingen.

Verstrekken van gegevens aan de minister (artikel 4.14 en 4.15)

Een houder van een erkenning wordt verplicht om bepaalde gegevens aan de minister te verstrekken. Dit maakt het mogelijk om partijoverstijgende functies binnen het stelsel toegang mogelijk te maken. Het gaat om de inzagemogelijkheden voor gebruikers en partijoverstijgende functies om misbruik en fraude te voorkomen of de gevolgen daarvan te herstellen.

In paragraaf 3.5.2 is ingegaan op de mogelijkheid die aan gebruikers moet worden geboden om inzage te krijgen in de middelen die op hun naam zijn verstrekt. Een dergelijke inzagefunctie is slechts effectief wanneer het voor gebruikers mogelijk is om alle binnen het stelsel aan die gebruiker uitgegeven middelen in te zien, en niet alleen de middelen die door de desbetreffende authenticatiedienst zijn verstrekt. Daarom wordt een centraal inzageregister ingericht, dat door de authenticatiediensten wordt ontsloten. Van erkende partijen wordt verwacht dat zij aan dit register een door dat doel aangemaakte authenticatiecode leveren van de gebruiker en een omschrijving van het identificatiemiddel, aan de hand waarvan de gebruiker kan vaststellen of dit een middel is dat hem of haar bekend is.

5.6.8 Eisen aan in te zetten personeel (artikel 4.16)

Verder schrijft de regeling voor dat het proces waarin de identiteit wordt vastgesteld en gecontroleerd door de erkende partij voorziet in kwaliteitsborging waaronder dat dit door opgeleide medewerkers geschiedt. Een bekende basis voor kwaliteitsborging bestaat uit een opzet van eerste en tweede lijn medewerkers. De tweede lijn beschikt over meer expertise en wordt aangeroepen als de eerste lijn zorgen heeft rond identiteitsvaststelling of -controle. Als nadere richtlijn voor kwaliteitsborging kunnen de handreikingen worden gehanteerd zoals die worden gepubliceerd op de website van de Nederlandse Vereniging voor Burgerzaken (NVVB) voor de afdelingen burgerzaken van gemeenten. Hierin worden ook richtlijnen gegeven voor de fysieke controle van identiteitsdocumenten en de databases die daarbij gebruikt kunnen worden, zoals het Europese PRADO (*Public Register of Authentic identity and travel Documents Online*). De NVVB verzorgt ook (opfris)opleidingen op mbo- en hbo-niveau rond het vaststellen en controleren van de identiteit van gebruikers waarvan de eindtermen als maatstaf voor het gewenste opleidingsniveau kunnen fungeren. Naast het volgen van een initiële opleiding is het ook van belang dat de opleiding regelmatig wordt geactualiseerd (*permanente educatie*) zodat ook nieuwe ontwikkelingen rond identiteitsfraude worden belicht.

5.6.9 Aansluiten op het stelsel (artikel 4.17)

Voorafgaand aan toelating wordt getoetst of de authenticatiedienst kan aansluiten op de voorzieningen die nodig zijn om het stelsel toegang te laten werken. Het gaat bijvoorbeeld om het BSN-koppelregister, maar ook om het inzageregister en het centrale fraude- en misbruikregister, waaraan bepaalde gegevens moeten worden verstrekt. Wanneer een erkenning is verleend worden houders van een erkenning verplicht ook daadwerkelijk op deze voorzieningen aan te sluiten.

5.7 Beëindigingsplan (artikel 4.19)

Verder moet een aanvrager aangeven op welke wijze op het moment dat de dienstverlening aan gebruikers wordt beëindigd, zorg wordt gedragen voor een ordentelijk beëindigingsproces waarbij de belangen van gebruikers zijn geborgd. Bij dit beëindigingsplan moet als gevolg van artikel 4.19, eerste lid, worden ingegaan op de volgende aspecten:

- De wijze waarop gegevens die voor authenticatie zijn verkregen worden vernietigd, bewaard of overgedragen (onderdeel a).
- De beschikbaarheid van gegevens die nodig kunnen zijn in verband met onderzoek naar misbruik (onderdeel b). Het herstelvermogen van het stelsel mag niet worden gehinderd wanneer een aanbiedende partij zijn activiteiten staakt. Daarom moet een aanvrager aangeven dat geen gegevens worden vernietigd die noodzakelijk zijn om oorzaak van misbruikgevallen te kunnen achterhalen of de schade daarvan te herstellen.
- Het informeren van gebruikers over de beëindiging (onderdeel c). De aanvrager geeft in het beëindigingsplan aan op welke wijze gebruikers worden geïnformeerd over beëindiging, waarna daarvan sprake is. Relevant is daarbij bijvoorbeeld de termijn waarbinnen gebruikers worden geïnformeerd en de informatie die wordt verstrekt over de mogelijkheden om gegevens te laten overdragen aan een andere toegelaten partij.

6. Regeldruk

[PM]

7. Uitvoering, handhaving en toezicht

[PM]

Artikelsgewijze toelichting

Artikel 1.1

Met dit artikel worden voor deze regeling relevant begrippen gedefinieerd. Daarbij wordt getracht zoveel mogelijk het woordgebruik in uitvoeringsverordening over te nemen of te gebruiken. In deze regeling worden ook de begrippen gehanteerd die zijn gedefinieerd in de wet en in de beide algemene maatregelen van bestuur.

Zo wordt “identificatiemiddel” gebruikt op de wijze waarop dat ook in de wet gebeurt, dus niet voor het aanduiden van een specifiek aan een gebruiker verstrekt middel, maar een type middel met een daarbij behorend authenticatiemechanisme. In artikelen die zien op een specifiek middel blijkt dat uit de tekst van het desbetreffende artikel of een begrip. Een voorbeeld is het “intrekken van een identificatiemiddel”, waarbij uit de tekst blijkt dat het gaat om het intrekken van een individueel, aan een gebruik verstrekt middel, en niet een type identificatiemiddel.

Authenticatiecodes en persoonlijke stelselcodes

In het stelsel toegang wordt gebruik gemaakt van pseudoniemen en versleutelde persoonsgegevens. Bij het registreren van een identificatiemiddel worden voor een gebruiker persoonlijke stelselcodes aangemaakt. Bij iedere inloghandeling worden deze persoonlijke stelselcodes omgezet in specifieke voor die handeling – en derhalve voor die specifieke dienstverlener – aangemaakte codes. Die codes worden in deze regeling authenticatiecodes genoemd. In de artikelen 2.8, 2.9, 2.18 en 4.2 wordt het gebruik van deze codes verplicht voor deelnemende partijen.

Authenticatiefraude en misbruik van een identificatiemiddel

Deze regeling bevat eisen die zijn gericht op het tegengaan van fraude en misbruik en het herstellen van de gevolgen daarvan. Onder authenticatiefraude wordt verstaan het authentiseren namens de gebruiker zonder diens toestemming. Het gaat dus om een geval waarin een ander dan de gebruiker inlogt in naam van de gebruiker, zonder dat de gebruiker daarmee instemt. Degene die de inloghandeling en daaropvolgende handelingen verricht is dus een ander dan degene wiens identiteit wordt gebruikt.

De term misbruik van een identificatiemiddel wordt in deze regeling gebruikt voor gevallen waarin met een identificatiemiddel onrechtmatig een voordeel wordt verkregen. Daarvan kan bijvoorbeeld sprake zijn bij gevallen van authenticatiefraude, dus zonder toestemming van de gebruiker, maar ook in gevallen waarin de gebruiker zelf inlogt en onrechtmatige handelingen verricht. In die laatste gevallen werkt het identificatiemiddel naar behoren, maar kan het toch nodig zijn om van de aanbieder van het identificatiemiddel gegevens te ontvangen en om te eisen dat bepaalde trends worden herkend in het inloggedrag van gebruikers. De term misbruik van identificatiemiddelen omvat dus de term authenticatiefraude.

Middelbeheerkwaliteit en middelkwaliteit

In het kader van de aanvraagprocedure moet met een rapportage worden onderbouwd dat de processen die de betrouwbaarheid van een identificatiemiddel bepalen voldoen aan de daaraan gestelde eisen. In deze regeling wordt een onderscheid gemaakt tussen middelkwaliteit en middelbeheerkwaliteit. Met middelkwaliteit wordt bedoeld de kwaliteit van het authenticatieproces, dus het proces waarmee bij het inloggen de identiteitsclaim van gebruiker wordt geverifieerd. De kwaliteit van de overige processen die voor de betrouwbaarheid van een identificatiemiddel van belang zijn worden aangeduid met het begrip middelbeheerkwaliteit.

Artikel 1.2 en 1.3

Deze regeling bevat eisen voor authenticatiediensten die identificatiemiddelen voor natuurlijke personen aanbieden, voor authenticatiediensten die bedrijfs- en organisatiemiddelen aanbieden en voor machtigingsdiensten. In artikel 1.2 en 1.3 is per type authenticatie- of machtigingsdienst bepaald welke eisen van toepassing zijn.

In artikel 1.2 zijn de eisen opgesomd voor authenticatiediensten die een identificatiemiddel aanbieden voor natuurlijke personen. Het gaat om nadere eisen gesteld op grond van artikel 7, eerste lid van het Besluit INP. Artikel 1.3 bevat twee leden. Het eerste lid duidt de eisen die van toepassing zijn op een authenticatiedienst voor bedrijfs- en organisatiemiddelen. Die eisen komen vrijwel geheel overeen met de eisen voor authenticatiediensten voor natuurlijke personen, met

uitzondering van de routering van de authenticatieverklaring. Een authenticatiedienst zendt een authenticatieverklaring aan een machtigingsdienst en niet rechtstreeks aan een publieke dienstverlener. Het tweede lid van artikel 1.3 bevat de eisen voor machtigingsdiensten.

Artikel 2.2

Dit artikel regelt de verplichting voor een aanvrager van een erkenning en eventuele onderaannemers om gecertificeerd te zijn overeenkomstig ISO 27001. Dat deze verplichting ook geldt voor onderaannemers komt tot uitdrukking doordat de verplichting geldt voor “alle processen waarop de aanvraag ziet”. Bij het beoordelen van een aanvraag wordt getoetst of aan deze eis wordt voldaan.

De algemene maatregelen van bestuur bepalen dat een houder van een erkenning ook moet blijven voldoen aan de eisen die bij de aanvraagprocedure worden getoetst nadat een erkenning is afgegeven. Voor deze eis betekent dat een houder van een erkenning moet beschikken over een ISO-certificaat dat is afgegeven op grond van ISO 27001. Wanneer een certificaat na afgifte wordt ingetrokken voldoet de houder van de erkenning niet langer aan deze eis.

Artikel 2.3

Wanneer een erkende partij wil stoppen met het aanbieden van de dienst waarvoor een erkenning is verleend moet daarvoor een procedure worden doorlopen. Tijdens die procedure moet de houder van de erkenning aantonen dat zorgvuldig wordt omgegaan met verwerkte gegevens en dat gebruikers tijdig over de beëindiging worden geïnformeerd. Dat regelen de artikelen 28 van het Besluit INP en artikel 17 van het Besluit BO. In artikel 2.3 van deze regeling is vastgelegd dat partijen tijdens de erkenningsperiode moeten aantonen dat er voorzieningen zijn om een beëindiging deugdelijk uit te voeren. Gedacht kan bijvoorbeeld worden aan een garantiefonds voor het afronden van werkzaamheden of een bankgarantie waarmee wordt gegarandeerd dat het afronden financieel mogelijk is.

Artikel 2.4

Dit artikel bevat de eis de processen waarop de aanvraag ziet bestand moeten zijn tegen aanvallen. Daarvoor wordt het begrip “aanvalspotentieel” gebruikt. Artikel 1.1 bevat een begripsbepaling voor “aanvalspotentieel”.

Artikel 2.5 en 2.6

Op deze artikelen over het gebruik van software met openbare broncode wordt uitgebreid ingegaan in de paragrafen 2.2.3 en 3.2.

Artikel 2.7

Met dit artikel wordt geregeld op welke wijze een authenticatiedienst een identificatiemiddel registreert in samenwerking met het BSN-koppelregister. Het eerste lid bevat de minimale gegevensset die voor registratie nodig is. Het gaat om de gegevens die nodig zijn om een controle via het BSN-koppelregister uit te kunnen voeren en om persoonlijke stelselcodes aan te maken. Dit

artikel bevat een verplichting om het proces met de voorgeschreven gegevens uit te voeren. De verwerkingsgrondslagen voor deze gegevens zijn opgenomen in het Besluit digitale overheid.

In het stelsel toegang wordt gewerkt met pseudoniemen in plaats van met een BSN van de gebruiker. Bij het registreren van een identificatiemiddel worden de gegevens over de identiteit van de gebruiker, waaronder het BSN, vervangen door een pseudoniem. Dit artikel regelt dat de gegevens over de gebruiker na ontvangst van een dergelijk pseudoniem moeten worden verwijderd.

Verder bevat dit artikel een verplichting om alternatief communicatiekanaal met de gebruiker vast te leggen. Gebruik van een kanaal, anders dan communicatie via het middel of het account van de gebruiker, is nodig wanneer bijvoorbeeld identiteitsfraude met het desbetreffende middel wordt vermoed.

Artikel 2.8

Dit artikel regelt de wijze waarop een identificatiemiddel kan worden geregistreerd met gebruik van een ander identificatiemiddel, de zogenaamde afgeleide verificatie. In paragraaf 3.3.1 wordt op de beleidsmatige achtergrond daarvan ingegaan.

Als gevolg van artikel 4.10 van deze regeling moet een erkenninghouder voldoende gegevens registreren om dispuutafhandeling over authenticatie mogelijk te maken. Wanneer gebruik wordt gemaakt van afgeleide verificatie moet het ook mogelijk zijn om te achterhalen van welk identificatiemiddel een ander identificatiemiddel is afgeleid.

Artikel 2.9

Bij het registreren van een identificatiemiddel wordt tussen de authenticatiedienst en de gebruiker een overeenkomst gesloten. In deze overeenkomst moet een aantal verplichtingen voor de gebruiker worden opgenomen, die nodig zijn in het belang van veilige toegang. Op grond van artikel 10 van het Besluit INP en artikel 12, tweede lid, onderdeel c, van het Besluit BO moet een concept voor een dergelijke overeenkomst worden overgelegd bij een erkenningsaanvraag.

Artikel 2.10

Dit artikel schrijft voor op welke wijze in het authenticatieproces moet worden omgegaan met persoonlijke stelselcodes en authenticatiecodes bij de authenticatie van natuurlijke personen. Bij een geslaagde authenticatie zet de authenticatiedienst de persoonlijke stelselcode om in een authenticatiecode die specifiek voor die inloghandeling wordt aangemaakt en die slechts kan worden ontsleuteld door de publieke dienstverlener waarop het authenticatieverzoek ziet. Voor het aanmaken van een dergelijke authenticatiecode moet gebruik worden gemaakt van een hardware security module. Wanneer een aanvrager niet in staat is dit proces uit te voeren wordt een aanvraag afgewezen. Op grond van artikel 3.1, tweede lid, onderdeel c, volgt dat dit met een rapportage moet worden aangetoond.

Zoals in paragraaf 2.2.4 van het algemene deel van deze toelichting uiteen is gezet gelden eisen die zijn gesteld aan private identificatiemiddelen in beginsel ook ten aanzien van publieke

identificatiemiddelen, tenzij de desbetreffende eis expliciet is uitgezonderd in artikel 2.28. Een dergelijke uitzondering geldt niet voor artikel 2.10, dus publieke identificatiemiddelen werken volgens het proces dat in dit artikel is beschreven.

Artikel 2.11

Wanneer authenticatie plaatsvindt voor het inloggen namens een onderneming of rechtspersoon werkt het proces anders dan bij het inloggen van natuurlijke personen. Een authenticatie verzendt een na positieve authenticatie verkregen authenticatiecode in dat geval namelijk niet rechtstreeks naar een publieke dienstverlener, maar naar een machtigingsdienst. Het authenticatieproces vindt ook plaats na een authenticatieverzoek van een machtigingsdienst en niet van een publieke dienstverleners. Die procedure regelt artikel 2.11. Technisch komt het proces van versleuteling wel overeen met het inlogproces namens een natuurlijke persoon.

Een authenticatiedienst verstrekt aan een machtigingsdienst meerdere authenticatiecodes. Eén van de codes wordt door de machtigingsdienst gebruikt om informatie die versleuteld is opgeslagen te raadplegen. De andere authenticatiecode wordt door de machtigingsdienst met de informatie over de machtiging doorgestuurd naar de publieke dienstverlener, die na versleuteling de identiteit van de gemachtigde kan vaststellen.

Artikel 2.11 en 2.12

Op de inhoud van de artikelen 2.11 en 2.12 wordt uitgebreid ingegaan in paragraaf 3.2.2. van het algemene deel van deze toelichting.

Artikel 2.13

Op dit artikel wordt ingegaan in paragraaf 3.3.2 van deze toelichting.

Artikel 2.15

Op de beleidsmatige achtergrond van dit artikel wordt ingegaan in paragraaf 3.5.2 van deze toelichting. In dit verband wordt nog vermeld dat de AVG al een inzageverplichting kent, maar dat in dit artikel is bepaald dat de genoemde gegevens elektronisch inzichtelijk moeten worden gemaakt. Dit artikel bevat geen juridische basis voor het verwerken van gegevens, maar slechts een verplichting om bepaalde verwerkte gegevens elektronisch te laten inzien.

Artikel 2.16 tot en met 2.20

Op deze artikelen wordt ingegaan in paragraaf 3.4 van het algemene deel van deze toelichting.

Artikel 2.21

Voor de veilige en betrouwbare werking van het stelsel is het van belang dat wijzigingen en veiligheidsrisico's zo spoedig mogelijk worden doorgegeven. Een machtigingsdienst sluit een overeenkomst met de onderneming of rechtspersoon namens welke het inloggen plaatsvindt. Dit artikel bevat een aantal afspraken die in ieder geval in een dergelijk overeenkomst moet worden opgenomen.

Artikel 2.26

Dit artikel regelt de aanwijzing van standaarden voor het uitwisselen van gegevens door de minister van Binnenlandse Zaken en Koninkrijksrelaties. Een dergelijke aanwijzing is geen algemeen verbindend voorschrift[9]. Daarom is de Bekendmakingswet op een degelijke aanwijzing niet van toepassing. Het tweede lid regelt de wijze waarop bekendmaking plaatsvindt.

Op de beleidsmatige aanleiding van dit artikel wordt in paragraaf 3.7 van het algemene deel van deze toelichting uitgebreid ingegaan.

Artikel 2.28

In paragraaf 3.8 van deze toelichting is ingegaan op de positie van publieke identificatiemiddelen binnen de systematiek van de toelatingseisen. In dat systeem gelden in beginsel alle eisen die voor private identificatiemiddelen gelden ook voor een publiek identificatiemiddel. In deze regeling worden enkele uitzondering gemaakt en worden enkele specifieke eisen opgelegd aan publieke identificatiemiddelen. In het hiernavolgende wordt ingegaan op de uitzonderingen en aanvullende eisen met een meer technisch karakter.

<u>Verzekeringsplicht (eerste lid, onderdeel a)</u>

Publieke identificatiemiddelen worden aangeboden door de Staat. Aan de Staat wordt geen verzekering verleend. Daarom is deze eis niet van toepassing op een publiek identificatiemiddel.

Verder wordt het publieke identificatiemiddel uitgezonderd van de certificeringsverplichting op grond van ISO 27001. Omdat de werking van dit middel voldoet aan de eisen van de Baseline informatiebeveiliging overheid, zou een dergelijke verplichting een doublure zijn.

<u>Te verwerken gegevens (eerste lid, onderdeel b)</u>

De minister van Binnenlandse Zaken en Koninkrijksrelaties kan, als beheerder van de publieke identificatiemiddelen, gebruik maken van de Basisregistratie persoonsgegevens. Vanuit het oogpunt van dataminimalisatie is het derhalve niet wenselijk om gegevens die in dat register zijn opgenomen nogmaals te registreren in het kader van het registratieproces voor een publiek identificatiemiddel. Om het registratie- en verificatieproces goed te laten verlopen zijn enkel het burgerservicenummer en de geboortedatum nodig. Artikel 2.7, eerste lid, van deze regeling bepaalt echter dat ook de voorletters of voornamen en de achternaam moeten worden verwerkt en gecontroleerd. In artikel

[9] Zie: HR 22 juni 2012, ECLI: NL: HR: 2012: BW0393 en ABRvS 2 februari 2011, JB 2011/65.

2.28, eerste lid, onderdeel b, worden publieke identificatiemiddelen van die verplichting uitgezonderd.

Hetzelfde geldt voor het vastleggen van een alternatieve wijze van communiceren met de gebruiker. Daarvoor worden in beginsel de adresgegevens uit de Basisregistratie persoonsgegevens gebruikt. Voor een publiek identificatiemiddel mág een andere wijze van communiceren worden gevraagd, maar dat is niet verplicht.

Inzage in de wijze waarop met gebruikers op alternatieve wijze wordt gecommuniceerd (tweede lid)

Op grond van artikel 2.15 moet inzage worden geboden in de verwerkte gegevens. Dat geldt ook voor het publieke identificatiemiddel. Hoewel het niet nodig is dat tijdens het registratieproces een alternatieve communicatiewijze wordt vastgelegd, is het wel wenselijk dat aan gebruikers wordt getoond op welke wijze contact met hen wordt opgenomen in gevallen waarin het wenselijk is om anders dan via de authenticatiedienst te communiceren. Artikel 2.28, tweede lid, regelt dat gebruikers daarover op de hoogte worden gesteld.

Artikel 3.1

Dit artikel regelt welke documenten bij een aanvraag voor een authenticatiedienst en het bijbehorende identificatiemiddel moeten worden gevoegd. Het betreft een aanvulling op de documenten die op grond van de beide algemene maatregelen van bestuur al moeten worden verstrekt. De documenten die in deze ministeriële regeling zijn opgenomen zien op de meer technische, procedurele of organisatorische werking van diensten en identificatiemiddelen waarop de aanvraag ziet.

Onderdeel a en b

Deze onderdelen schrijven voor dat de aanvrager een technische en een procesmatige beschrijving moet aanleveren van de werking van het identificatiemiddel en de bijbehorende authenticatiedienst. In het bijzonder moet worden ingegaan op de cryptografie die in deze processen wordt gebruikt. Een aanvrager moet verder onderbouwen dat deze processen voldoen aan de eisen die daarvoor gelden. Zo moet bijvoorbeeld worden onderbouwd dat een aanvrager systemen heeft ingericht om te voldoen aan de beschikbaarheidseisen, die zijn opgenomen in artikel 4.4, maar ook aan de eisen die zijn opgenomen in Uitvoeringsverordening (EU) 2015/1502.

Onderdeel c

Dit onderdeel bepaalt dat een aanvrager moet onderbouwen dat het identificatiemiddel en de authenticatiedienst voldoen aan de eisen voor middelkwaliteit en middelbeheerkwaliteit. Het gaat dus om de eisen aan de betrouwbaarheid van een authenticatie met het identificatiemiddel, op het betrouwbaarheidsniveau waarop de aanvraag ziet. Het tweede lid, onderdeel a, van artikel 3.1, in combinatie met artikel 3.2 schrijft voor dat aanvragers over deze onderbouwing een rapportage van een onafhankelijke derde partij moeten aanleveren.

Derde lid

Op grond van artikel 9, zesde lid, onderdeel b, en artikel 11, zesde lid, onderdeel b, moet een aanvrager aantonen dat het ontwerp van het identificatiemiddel waarop de aanvraag ziet voldoende voorziet in de bescherming van gegevens. Uit de memorie van toelichting bij deze onderdelen blijkt dat het gaat om een toets op de toepassing van het beginsel van privacy by design, zoals vervat in artikel 25 van de AVG. Aanvragers wordt gevraagd de conformiteit met dat beginsel te onderbouwen met een document en om de gegevensbeschermingseffectbeoordeling bij de aanvraag te voegen. Gelet op de aard van de gegevensverwerkingen die gepaard gaan met deelname aan het stelsel zal het opstellen van een dergelijke beoordeling verplicht zijn op grond van de AVG.

Artikel 3.4

Dit artikel regelt dat per authenticatiemechanisme een separate erkenning nodig is. Wanneer het bij een authenticatiedienst bijvoorbeeld zowel mogelijk is om een authenticatie uit te voeren via een smartcard als met gebruik van een identiteitsbewijs, zijn voor deze verschillende authenticatiemechanismen verschillende erkenningen nodig.

Artikel 3.5

De documenten die moeten worden aangeleverd bij een erkenningsaanvraag voor een machtigingsdienst komen voor een groot deel overeen met de documentatie bij een aanvraag voor een authenticatiedienst, die is opgenomen in artikel 3.1. Voor de leesbaarheid is gekozen voor een separaat artikel met een opsomming van de benodigde documenten, in plaats van een verwijzing naar specifieke onderdelen van artikel 3.1.

Met onderdeel b wordt een aanvrager, evenals bij een aanvraag voor een authenticatiedienst het geval is, verplicht te onderbouwen dat de processen die in de aanvraag zijn beschreven voldoen aan de eisen die op grond van de wet gelden. Voor de machtigingsdienst zij vermeld dat paragraaf 2.1.4 van de bijlage bij Uitvoeringsverordening (EU) 2015/1502 relevant is, omdat de eisen in die paragraaf zien op de werkzaamheden van een machtigingsdienst.

Artikel 4.9

Artikel 4.9, eerste en derde lid, bevatten verplichtingen voor erkende partijen om bereikbaar te zijn voor en deel te nemen aan incidenteel of periodiek overleg over zaken die het dagelijks beheer van het stelsel toegang betreffen. Gedacht kan worden aan het delen van ontwikkelingen die ook van andere stelseldeelnemers van belang kunnen zijn. Het gaat niet om een bevoegdheid om informatie of medewerking te vorderen, daarvoor bestaan de specifieke instrumenten van handhaving en toezicht.

Artikel 4.11

Dit artikel regelt de verplichting om voldoende gegevens te registreren om in geval van misbruik de oorzaak daarvan te kunnen traceren en om eventuele disputen af te kunnen handelen. In gevallen waarin een identificatiemiddel wordt geregistreerd op basis van een ander identificatiemiddel, de

zogenaamde afgeleide verificatie, houdt deze verplichting in dat ook moet kunnen worden getraceerd van welk identificatiemiddel het andere identificatiemiddel is afgeleid.

Het bewaren van deze gegevens geeft geen recht op het analyseren of op andere wijze gebruiken van die gegevens, tenzij deze regeling of andere regelgeving daartoe verplicht.

Artikel 4.13

In het zesde lid van dit artikel is geregeld dat bij het opheffen van een schorsing een authenticatie moet plaatsvinden op niveau Enhanced-basic of hoger. Erkende partijen kunnen er dus voor kiezen om voor deze procedure een hoger betrouwbaarheidsniveau te hanteren.

Artikel 4.20 en 4.21

Uit de beide algemene maatregelen van bestuur volgt dat een houder van een erkenning in bepaalde gevallen een melding moet doen bij de minister van Binnenlandse Zaken en Koninkrijksrelaties. Het gaat onder meer om het melden van wijzigingen in de processen of in de organisatie of de zeggenschap van de erkenninghouder. In artikel 4.20 is bepaald binnen welke termijn een dergelijke melding moet zijn gedaan en in artikel 4.21 op welke wijze de melding moet plaatsvinden.

Artikel 4.22

In artikel 4.22 wordt geregeld welke rapportages en documenten periodiek opnieuw moeten worden overgelegd. Het gaat om documenten die moeten worden vernieuwd of opnieuw worden afgegeven, zoals een ISO-certificaat. In onderdeel d is voorgeschreven dat iedere drie jaar een nieuwe gegevensbeschermingseffectbeoordeling moet worden verstrekt. De AVG bevat geen termijn voor het vernieuwen van een dergelijke beoordeling. Partijen moeten continu bezien of het document moet worden geactualiseerd op basis van nieuwe ontwikkelingen of aanpassingen in de dienstverlening. Wanneer een aanpassing zodanig ingrijpend is dat daarvoor een wijziging van de erkenning moet worden aangevraagd, wordt ook het verstrekken van een nieuwe gegevensbeschermingseffectbeoordeling vereist. In artikel 4.22, eerste lid, onderdeel d, is vastgelegd dat in andere gevallen ieder drie jaar een geactualiseerde beoordeling moet worden overgelegd.

Artikel 4.23

In dit artikel is geregeld welke eisen niet van toepassing zijn op het publieke identificatiemiddel, bedoeld in artikel 5, eerste lid, onderdeel a, van de wet. In het Besluit INP is geregeld dat eisen die van toepassing zijn op erkende private aanbieders van een identificatiemiddel ook van toepassing zijn op een publiek identificatiemiddel, tenzij bij ministeriële regeling anders is bepaald. In dit artikel zijn deze uitzonderingen vastgelegd.

Volledigheidshalve wordt vermeld dat procedurele eisen voor het verkrijgen van een erkenning of het intrekken daarvan niet van toepassing zijn op een publiek identificatiemiddel, omdat een dergelijk middel niet wordt erkend maar aangewezen.