Nota van toelichting

1. Algemeen

Burgers en bedrijven communiceren steeds meer digitaal met de publieke en semipublieke organisaties. Hierbij kan bijvoorbeeld worden gedacht aan een burger die een vergunning aanvraagt of een ondernemer die een werknemer beter meldt na een periode van ziekte. Bij deze communicatiemomenten zal telkens op betrouwbare wijze de identiteit moeten worden vastgesteld van degene die communiceert terwijl de privacy en de gegevens van die persoon worden beschermd en beveiligd.

De Wet digitale overheid (hierna: de wet) regelt de manier waarop identificatie van burgers en ondernemingen bij publieke dienstverleners kan plaatsvinden. Artikel 9 van die wet bevat het regime voor identificatie van burgers en de artikelen 11 en verder bevatten het regime voor ondernemingen. Met dit besluit wordt uitvoering gegeven aan artikel 9. Dat artikel regelt dat identificatiemiddelen voor burgers door de Minister van Binnenlandse Zaken en Koninkrijksrelaties kunnen worden toegelaten door middel van een erkenning of aanwijzing als deze voldoen aan nader te stellen eisen. Een toelating van een middel leidt tot acceptatie van dat middel door organisaties in het publieke domein. Verder regelt artikel 9 van de wet dat een toegelaten middel gedurende de toelatingsperiode moet blijven voldoen aan bepaalde eisen. Zowel de eisen voor toetsing als de eisen waaraan een toegelaten middel moet voldoen worden met dit besluit en de onderliggende ministeriële regeling vastgelegd. Daarbij worden alle aspecten van het identificatieproces betrokken, zoals werking van de authenticatiedienst en de organisatie van de uitgever van het middel. Verder wordt in dit besluit geregeld op welke wijze een erkenning kan worden verkregen en in welke gevallen deze wordt geschorst of ingetrokken en aan welke eisen een door de overheid verschaft middel moet voldoen.

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

2. Juridische context: Betrouwbaarheidsniveaus en acceptatieplicht van toegelaten identificatiemiddelen

2.1 Betrouwbaarheidsniveaus

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

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

2.2 Gesloten systeem van geaccepteerde middelen

Op grond van artikel 7 van de wet mogen voor een dienst slechts identificatiemiddelen worden geaccepteerd waarvan is vastgesteld dat deze voldoen aan de eisen voor het betrouwbaarheidsniveau dat voor die dienst is vastgesteld. Dat zijn, volgens artikel 7, eerste lid, van de wet, identificatiemiddelen die behoren tot een stelsel dat in het kader van de eIDAS-verordening is aangemeld en goedgekeurd en middelen die in Nederland zijn toegelaten.
De artikelen 9 en 11 van de wet regelen de Nederlandse toelating van middelen voor burgers en bedrijven. Een middel kan worden toegelaten als het voldoet aan de eisen die voor het desbetreffende betrouwbaarheidsniveau zijn gesteld. De inhoud van die eisen en het proces van toelating worden in lagere regelgeving vastgelegd. Voor identificatiemiddelen voor burgers vindt invulling plaats met dit besluit en de ministeriële regeling die op dit besluit wordt gebaseerd.

2.3 Verhouding tot de eIDAS-verordening

Dit besluit regelt de toelating, en daarmee ook de acceptatie, van identificatiemiddelen in een nationale context. Wanneer een middel wordt toegelaten wordt het op grond van artikel 7, eerste lid, onderdeel a, van de wet geaccepteerd. De acceptatieplicht geldt verder ook voor middelen die behoren tot een stelsel dat in een Europese context is genotificeerd.

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

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

Dergelijke middelen kunnen niet zonder meer functioneren binnen het Nederlandse stelsel. Om de werking van die middelen mogelijk te maken is een voorziening gecreëerd, het eIDAS-knooppunt, waarop genotificeerde stelsels moeten aansluiten. Doordat via dit knooppunt wordt aangesloten op het Nederlandse stelsel wordt de feitelijke werking van deze middelen, en het beschermingsniveau daarvan gelijkwaardig.

3. Toelating van identificatiemiddelen

3.1 Beleidsmatige achtergrond

Het kabinet streeft naar een stelsel waarmee burgers "veilig, betrouwbaar, gebruiksvriendelijk kunnen inloggen zodat zij transacties kunnen verrichten in de digitale wereld". Tot het moment van inwerkingtreding van de wet en dit besluit kon identificatie door burgers slechts plaatsvinden met gebruik van het publieke identificatiemiddel DigiD en met middelen die in het kader van de Europese eIDAS-verordening zijn genotificeerd. Met de inwerkingtreding van de wet wordt het voor private partijen ook mogelijk om een identificatiemiddel voor burgers aan te bieden voor de toegang tot publieke dienstverlening. Met de keuze om naast het publieke middel ook private middelen toe te laten wordt beoogd de innovatieve kracht van de markt meer ruimte te bieden en te komen tot een systeem waarin gebruikers kunnen kiezen welk middel aansluit bij hun gebruikswensen. Daarnaast is een systeem met meerdere voor burgers beschikbare middelen minder kwetsbaar voor uitval, hetgeen de stabiliteit ten goede komt. Tegelijkertijd moet met deugdelijke randvoorwaarden worden geborgd dat private partijen zorgvuldig omgaan met gegevens van gebruikers. Private partijen kunnen dan een rol spelen bij identificatie van natuurlijke personen zonder dat gegevens van die gebruikers handelswaar worden in het verdienmodel van die partijen.

In het licht van het voorgaande moeten de eisen voor toelating van private identificatiemiddelen borgen dat toegelaten middelen voldoende veilig, betrouwbaar en gebruiksvriendelijk zijn, terwijl de privacy van gebruikers wordt geborgd. Uit de beleidswensen volgt tevens dat de eisen zodanig worden geformuleerd dat de mogelijkheden om te innoveren daarmee zo weinig mogelijk worden beperkt.

3.2 Doelvoorschriften gebaseerd op eIDAS-eisen en AVG

Daarom wordt zoveel mogelijk gekozen voor eisen die als doelvoorschrift zijn geformuleerd. Hiermee wordt bedoeld dat er eisen worden gesteld aan het resultaat, namelijk het bieden van waarborgen, maar zo weinig mogelijk aan de wijze waarop dit resultaat gehaald moet worden. Met name wordt beoogd zo weinig mogelijk technische aspecten vast te leggen in de regels voor toelating, zodat ruimte wordt gelaten voor innovatie. Als deze technische aspecten wel geregeld worden, wordt de noodzaak daarvan onderbouwd.
De eisen zijn gebaseerd op de eisen die in het kader van de eIDAS-verordening worden gesteld aan identificatiemiddelen, bijvoorbeeld over de onderliggende uitgifte-, activerings- en authenticatieprocessen en de betrouwbaarheidsniveaus waarop deze werken en op de Algemene verordening gegevensbescherming. Zoals in paragraaf 2.1 is aangegeven worden in dat verband

drie betrouwbaarheidsniveaus onderscheiden; Laag, Substantieel en Hoog. De eisen die worden gesteld aan middelen die op deze niveaus worden uitgegeven zijn opgenomen in Uitvoeringsverordening (EU) 2015/1502 van de Commissie van 8 september 2015 tot vaststelling van minimale technische specificaties en procedures betreffende het betrouwbaarheidsniveau voor elektronische identificatiemiddelen overeenkomstig artikel 8, lid 3, van Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (hierna: eIDAS-uitvoeringsverordening 1502). Daarin wordt voor niveau laag in veel gevallen gebruik gemaakt van "one-factor" authenticatie. Het gaat ruwweg om middelen met het betrouwbaarheidsniveau van DigiD basis, zoals dat op het moment van inwerkingtreding van dit besluit in werking was. De niveaus substantieel en hoog zijn beide gebaseerd op "two-factor" authenticatie. Daarbij heeft niveau Hoog een hogere weerstand tegen aanvallen dan Substantieel. De eIDAS-uitvoeringsverordening 1502 stelt per betrouwbaarheidsniveau nadere eisen ten aanzien van het juiste betrouwbaarheids- en veiligheidsniveau.

Deze eisen vormen de basis voor de eisen die in en op grond van dit besluit worden gesteld aan identificatiemiddelen. Verder wordt met de eisen waar nodig geborgd dat het middel werkt conform de AVG. De AVG is sinds 25 mei 2018 van kracht en daarin worden eisen gesteld aan de gegevensbescherming en het borgen van de privacy van data van eindgebruikers.

3.3 Aanvulling en invulling ter bescherming van de Nederlandse eindgebruikers
Aanvullend op de eisen die worden gesteld in de eIDAS-verordening en de AVG, biedt dit besluit ruimte om in het belang van gebruiksgemak, privacy en beveiliging nadere eisen te stellen aan identificatiemiddelen die worden toegelaten in Nederland. Waar de eIDAS-regelgeving bijvoorbeeld eisen bevat voor de mate waarin het authenticatiemechanisme bestand moet zijn tegen aanvallen daarop, ligt het voor de hand om deze eis ook voor de andere noodzakelijke processen, zoals het aanvraag- en registratieproces, te stellen. Een aanvaller zal immers het meest kwetsbare onderdeel van het proces aanvallen om een inbreuk te forceren.
Door de bredere implementatie en toepassing van elektronische overheidsdienstverlening binnen Nederland is Nederland aantrekkelijk is voor internetcriminelen. Op dit dynamische beleidsterrein, waarin ontwikkelingen elkaar spoedig opvolgen, moet sturing door de overheid snel kunnen inspelen op veranderende omstandigheden en technische ontwikkelingen. In het verleden is deze noodzaak bijvoorbeeld gebleken uit het DigiNotar incident in 2011 en de ervaringen rondom fraude in de e-commercedienstverlening. Om te voorkomen dat gegevens die bijvoorbeeld als gevolg van een datalek worden verkregen bruikbaar zijn voor andere partijen is in dit besluit opgenomen dat private aanbieders van identificatiemiddelen gegevens over gebruikers gescheiden moeten opslaan van gegevens over het gebruik. Op deze eis wordt nader ingegaan in paragraaf 4.1.3. Dit besluit maakt het ook mogelijk om regels te stellen die tegengaan dat gebruikers worden omgeleid naar een andere website dan waar zij denken in te loggen.
Ondanks regels met preventieve maatregelen en toezicht daarop kunnen misbruik of fraude plaatsvinden. Dit is nooit geheel uit te sluiten. Daarom is het noodzakelijk om ook het herstelvermogen van het stelsel te borgen. Dit besluit maakt het daarom tevens mogelijk om de

gevolgen van misbruik en fraude te herkennen en te herstellen. Een voorbeeld is de eis dat gebruikers inzicht moet hebben in het gebruik van de middelen die op hun naam zijn geregistreerd, waardoor problemen door de gebruiker zelf kunnen worden opgemerkt. Dat maakt het mogelijk dat gebruikers frauduleuze identificatiepogingen herkennen en maatregelen nemen om verder gevolgen daarvan te voorkomen. Daarnaast wordt op basis van dit besluit geregeld dat partijen binnen het stelsel zelf een verantwoordelijkheid hebben om misbruik te herkennen en te herstellen.
In het verleden is ook gebleken dat private partijen, bijvoorbeeld aanbieders van sociale media, de verkoop van gegevens over gebruikers en gebruik als verdienmodel hanteren. Het kabinet vindt dit bij identificatie in het publieke domein niet acceptabel. In dit besluit is daarom bepaald dat het niet is toegestaan om gegevens die zijn verkregen in verband met identificatie van gebruikers worden gebruikt voor andere doeleinden. Op deze zogenaamde doelbinding wordt ingegaan in paragraaf 6.1. In dit verband is ook de in het voorgaande genoemde verplichte scheiding van gegevens van gebruikers en gebruik van belang. Wanneer gegevens over het gebruik zonder nadere handelingen niet herleidbaar zijn tot de desbetreffende gebruikers kunnen deze niet worden gebruikt voor commerciële doeleinden. In de meer gedetailleerde eisen die bij ministeriële regeling worden gesteld kan vervolgens worden geregeld op welke wijze wordt vastgelegd of deze handelingen met de gegevens zijn uitgevoerd. Daarvoor biedt dit besluit een basis. Deze eisen zijn een verdere explicitering van de eisen die al zijn opgenomen in artikel 16 van de wet en in artikel 5b en 5e van het Besluit digitale overheid.
Op dit dynamische beleidsterrein, waarin ontwikkelingen elkaar spoedig opvolgen, moet sturing door de overheid snel kunnen inspelen op veranderende omstandigheden en technische ontwikkelingen. Dit besluit biedt daarom de nodige ruimte om bij ministeriële regeling aanvullende eisen te stellen waar ter borging van de beleidsdoelen. Op grond van dit besluit is het bijvoorbeeld mogelijk om aanbieders van een identificatiemiddel te verplichten om bereikbaar te zijn voor gebruikers en voor de overheid, zodat bijvoorbeeld bij incidenten zo efficiënt mogelijk kan worden gecommuniceerd. Deze aanvullende eisen gelden alleen voor identificatiemiddelen die, door het verlenen van een erkenning door de minister van BZK, worden toegelaten in het kader van artikel 9 van de Wet digitale overheid. Alleen die middelen worden getoetst aan de eisen die worden gesteld op grond van deze wet. Met middelen die in een andere EU-lidstaat zijn toegelaten en die behoren tot een stelsel dat genotificeerd is volgens de eIDAS-verordening, kan ook worden ingelogd bij dienstverleners in Nederland. In paragraaf 2.3 is hier nader op ingegaan.

3.4 Werking binnen de digitale overheidsinfrastructuur
Gebruik van een identificatiemiddel door een burger vindt plaats in het kader van de digitale infrastructuur van de overheid. Een publieke dienstverlener doet een authenticatieverzoek bij de aanbieder van het middel. De aanbieder beantwoordt met een authenticatierespons, waarbij gebruik wordt gemaakt van de uitgegeven middelen. Een publieke dienstverlener kan rechtstreeks interacteren met de aanbieder of via de zogenaamde routeringsvoorziening. In het laatste geval richt de publieke dienstverlener het authenticatieverzoek aan de routeringsvoorziening die dit doorzet naar de aanbieder; de routeringsvoorziening zet vervolgens de authenticatierespons ook weer door naar de publieke dienstverlener.

Bij deze opzet is het van essentieel belang dat de aanbieder hiervoor kan samenwerken met de technische standaarden en de delen van de generieke digitale infrastructuur (GDI) zoals die nu binnen de overheid worden gebruikt en zoals uiteengezet in het eerste lid artikel 5 van de wet. Te denken valt aan een door de overheid beheerde ontsluitende dienst of een machtigingenregister. Het middel zal derhalve moeten werken met de andere onderdelen, bijvoorbeeld onderdelen van de digitale infrastructuur of private routeringsdiensten, die nodig zijn om het middel naar behoren te laten functioneren. Een aanvrager van een erkenning moet in zijn aanvraag uiteenzetten dat en op welke wijze het middel werkt binnen die infrastructuur. Als op basis van een aanvraag een erkenning wordt verleend moet de houder van die erkenning er vervolgens zorg voor dragen dat het middel blijft werken binnen de infrastructuur, ook als daaraan technische aanpassingen worden gedaan. Als gevolg van deze feitelijke omstandigheden zal de Minister van BZK er zorg voor moeten dragen dat de technische specificaties voor aanvragers en houders van een erkenning niet verder gaan dan redelijkerwijs noodzakelijk is en dat de belangen van houders van een erkenning worden meegewogen in de beslissingen daaromtrent. Verder zullen de wijzigingen voldoende kenbaar worden gemaakt en dat wijzigingen daarin worden doorgevoerd met een voldoende tijdige aankondiging. Het ligt in de rede dat de specificaties bijvoorbeeld op een vaste website bekend worden gemaakt en dat ook aanpassingen daarvan op deze site worden aangekondigd.
Het is dus aan de aanvrager van een erkenning om in de aanvraag aan te tonen dat het middel waarvoor een erkenning wordt aangevraagd alle gewenste en vereiste functies heeft. Daarvoor zal de aanvrager in beginsel zelf moeten nagaan welke specificaties noodzakelijk zijn. Dit besluit voorziet met artikel 2.4, tweede lid, tevens in een mogelijkheid om regels te stellen met betrekking tot de interoperabiliteit. Dat artikel maakt het mogelijk om, bijvoorbeeld als dat in het kader van de rechtszekerheid gewenst is, specificaties voor te schrijven.

3.5 Delegatiesystematiek

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

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

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

deze dikwijls of met grote spoed moeten worden gewijzigd worden deze verder ingevuld bij ministeriële regeling. Dit besluit biedt daarvoor een basis.

3.6 Verhouding met de dienstenrichtlijn

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

4. Eisen aan een identificatiemiddel

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

Feitelijk kunnen in het proces van toelating van een privaat middel drie fasen worden onderscheiden. De eerste is de aanvraag van en erkenning en de besluitvorming daarover. In die fase wordt de conformiteit van het middel, dat op dat moment nog niet in werking is, getoetst aan de hand van door de aanvrager ingediende documenten. In deze fase kan de feitelijke werking van het middel slechts worden onderbouwd, maar kan deze niet worden getoetst.

Voldoet de aanvraag aan de gestelde eisen, dan wordt getoetst of het middel feitelijk werkt op de wijze die is aangegeven in de aanvraag. Dat is de tweede fase. Om deze toets uit te voeren moet het middel feitelijk in werking zijn en kunnen samenwerken met de noodzakelijke onderdelen van de digitale infrastructuur.

Als ook de tweede fase met positief resultaat wordt doorlopen, dan kan het middel worden gebruikt door burgers om te communiceren met publieke dienstverleners. Vanaf dat moment wordt toezicht gehouden op de conformiteit van het middel met de daaraan gestelde eisen. Dit is de derde fase van het proces.

Deze fasen worden als volgt juridisch vormgegeven. De eerste fase, die van het indienen van een aanvraag en de beoordeling daarvan, volgt het gebruikelijke bestuursrechtelijke proces van het behandelen van aanvragen. Nadat een aanvraag positief is beoordeeld wordt een erkenning verleend onder de opschortende voorwaarde dat binnen een bepaalde termijn na verlening ervan wordt aangetoond dat het middel werkt zoals in de aanvraag is aangegeven. Daarmee is de tweede fase geborgd. Als aan die opschortende voorwaarde wordt voldaan gaat de door de wet geregelde acceptatieverplichting in.

In het hiernavolgende wordt deze procedure verder uiteengezet.

4.1 Erkenning van private identificatiemiddelen

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

4.1.1 Eisen aan de aanvrager

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

Op grond van artikel 9, zesde en zevende lid, van de wet wordt een aanvraag verder afgewezen "in geval ernstig gevaar bestaat voor de cyberveiligheid of staatsveiligheid of in geval ernstig gevaar bestaat dat de erkenning mede zal worden gebruikt om strafbare feiten te plegen of uit strafbare feiten verkregen of te verkrijgen voordelen te benutten of anderszins de betrouwbaarheid en veiligheid van het Nederlandse stelsel voor elektronische dienstverlening in gevaar komt". Om invulling te geven aan deze afwijzingsgrond zal informatie over de aanvrager mede bepalend zijn.

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

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

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

De eisen die noodzakelijk zijn om deze verordening binnen de Nederlandse context vorm te geven zijn gedetailleerd van aard. De onderdelen a tot en met i van artikel 2.4 bieden derhalve een basis

voor het vaststellen van eisen over deze onderwerpen bij ministeriële regeling. Met deze onderdelen kunnen de eIDAS-gerelateerde eisen bij ministeriele regeling worden vastgesteld. Dit besluit biedt verder de mogelijkheid om over een aantal andere onderwerpen regels te stellen. Deze regels kunnen worden beschouwd als aanvullingen of invullingen die noodzakelijk zijn om uitvoering te geven aan de AVG of om de eIDAS-eisen in de Nederlandse context toe te passen. Artikel 2.4, eerste lid, biedt daarom een basis om bij ministeriële regeling bijvoorbeeld de volgende nadere eisen te stellen:

- Verplicht uit te voeren identiteitscontroles in de Basis Registratie Personen (BRP) aanvullend op de controles die de aanbieder zelf aanvoert (onderdeel a).
- Een verplichting om in de overeenkomst met gebruikers op te nemen dat de gebruiker geen anderen toegang geeft tot het gebruik van het middel (onderdeel j).
- Controles die, al dan niet periodiek, moeten worden uitgevoerd (onderdeel k). Gedacht kan worden aan een verplichting om periodiek na te gaan of een gebruiker nog in leven is. Een dergelijke verplichting kan misbruik van en fraude met identificatiemiddelen tegengaan.
- De verplichte toepassing van bepaalde technologie waarmee privacy van gebruikers beter wordt geborgd, bijvoorbeeld doordat het burgerservicenummer wordt beschermd (onderdeel l).
- Een verplichting dat een op gegevensverwerking gericht antecedentenonderzoek met positief resultaat moet zijn afgerond voor personeel en bestuurders die werken aan kritieke processen (onderdeel m).
- Het borgen van herstelvermogen in geval van fraude en misbruik, waaronder proactief melden van incidenten of misbruik (onderdeel n);
- Een bewaartermijn voor het bewaren van gegevens om herstelvermogen te waarborgen (onderdeel o).

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

4.1.3 Verplicht scheiden van gegevens van gebruiker en gebruik

Het Besluit digitale overheid bevat onder meer regels over de gegevens die door de verschillende onderdelen van de digitale infrastructuur mogen worden verwerkt en de wijze waarop dat gebeurt. Voor private identificatiemiddelen schrijft dat besluit voor dat gegevens over gebruikers op zodanige wijze moeten worden bewaard dat gegevens over gebruikers niet herleidbaar zijn tot gegevens over het gebruik van het middel door die gebruikers, in dit geval identificatie bij publieke dienstverleners. Een dergelijke scheiding zorgt ervoor dat bij een succesvolle inbreuk op een van de beide databases geen bruikbare gegevens worden verkregen. Verder kan een aanbieder van een identificatiemiddel zonder nadere handeling geen gegevens commercieel verhandelen. Voor een verdere uiteenzetting van de achtergrond bij dat voorschrift wordt in dit verband verwezen naar het Besluit digitale overheid en de toelichting bij artikel 5b.

In het kader van het toelaten van private identificatiemiddelen voor burgers wordt vooraf getoetst of aan deze eis wordt voldaan. Een aanvraag wordt derhalve afgewezen als daaruit blijkt dat gegevens over gebruikers niet gescheiden worden bewaard van gegevens over het gebruik van het middel.

4.1.4 Eisen aan de werking van het middel

Zoals in paragraaf 3.4 uiteen is gezet is een aanvrager of een houder van een erkenning in beginsel verantwoordelijk voor de interoperabiliteit van het middel binnen het systeem waarbinnen dat middel werkt. Als gevolg daarvan is het aan de aanvrager of de houder om na te gaan welke specificaties het middel moet hebben om als authenticatiemiddel te kunnen functioneren. In beginsel worden derhalve geen eisen gesteld waarin specifieke techniek wordt voorgeschreven waaraan wordt getoetst.
Dit besluit bevat in artikel 2.4, tweede lid, een grondslag voor stellen van nadere technische eisen bij ministeriële regeling. Deze eisen kunnen nodig zijn als de specifieke inrichting van de Nederlandse GDI daartoe noopt. Afhankelijk van de keuzes die worden gemaakt met betrekking tot het toelaten van private ontsluitende diensten kan het nodig zijn het gebruik van specifieke protocollen of standaarden voor te schrijven die beide private partijen in hun onderlinge processen moeten gebruiken.

4.2 Eisen aan een publiek identificatiemiddel

Met dit besluit worden tevens eisen gesteld aan het publieke identificatiemiddel. Deze eisen zijn gelijk aan de eisen die gelden voor private middelen, met dien verstande dat de eisen met betrekking tot de financiële positie van de aanbieder van het middel niet van toepassing zijn. Dat betekent dat ook bijvoorbeeld de eis met betrekking tot het scheiden van gegevens over de gebruiker van gegevens over het gebruik van een middel door die gebruiker van toepassing is een publiek identificatiemiddel voor natuurlijke personen. Op die eis wordt ingegaan in paragraaf 4.1.3 van deze toelichting. Op een aantal punten is het publieke middel wezenlijk anders dan een privaat middel. Een voorbeeld is de relatie met de gebruikers, waarmee geen overeenkomst wordt gesloten. Dit besluit maakt het mogelijk om recht te doen aan die verschillen, doordat kan worden bepaald dat specifieke eisen niet van toepassing zijn op het publieke middel. Een dergelijke uitzondering wordt uiteraard gemotiveerd gemaakt.
Voor een publiek middel geldt verder dat deze niet wordt erkend op basis van een aanvraag, maar dat daarvoor een ambtshalve aanwijzing plaatsvindt als het middel aan de eisen voldoet.

5. Aanvraagprocedure

Degene die een erkenning voor een privaat identificatiemiddel aanvraagt moet met de aanvraag onderbouwen dat aan alle gestelde eisen is voldaan. Dit besluit regelt welke documenten bij een aanvraag in ieder geval moeten worden aangeleverd. Als een van deze documenten ontbreekt kan een aanvraag buiten behandeling worden gelaten.
Artikel 9, vijfde lid, van de wet schrijft voor dat bij een aanvraag in ieder geval een verklaring wordt overgelegd van een geaccrediteerde certificerende instelling. Op grond van het negende lid

van dat artikel kunnen nadere regels worden gesteld over onder meer die verklaring. In dit hoofdstuk wordt nader ingegaan op de aanvraagprocedure.

5.1 Kring van aanvraaggerechtigden

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

5.2 Verklaring van een geaccrediteerde certificerende instelling

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

Een certificaat of conformiteitsverklaring is in het algemeen een zelfstandig document met eigen rechtsgevolg (keurmerk of toelating). In dit geval geeft de certificerende instelling een verklaring af, die echter niet meer is dan een vermoeden dat aan de geldende normen en eisen is voldaan. Het is in feite een advies aan de minister, die zelf op de aanvraag en continuering moet beslissen. Daarom toetst hij, zo volgt uit het zorgvuldigheidsbeginsel, of de (geaccrediteerde) certificerende instelling zorgvuldig onderzoek heeft verricht. De Minister van BZK is voornemens om het Agentschap Telecom in te schakelen voor deze toets, gelet op deskundigheid inzake (technisch-) inhoudelijke, procesmatige en juridische kennis en ervaring van die organisatie.

ISO- norm 27001 is de leidende norm rond informatiebeveiliging is. Het ligt voor de hand om, in de eisen die bij ministeriële regeling worden gesteld aan de aanvrager of houder van een erkenning, die eis op te nemen. De norm ISO 27006 is daarbij de gangbare norm waartegen certificerende instellingen worden geaccrediteerd die ISO 27001 certificeringen uitvoeren. Daarom wordt in dit besluit vereist dat een verklaring, die bij de aanvraag wordt gevoegd, is opgesteld door een instantie die is geaccrediteerd op grond van ISO 27006.

In de aanvraagprocedure voor een erkenning voor een bedrijfs- of organisatiemiddel is een vergelijkbare verklaring vereist. In dat verband wordt een verklaring gevraagd van een instantie die is geaccrediteerd conform ISO 17065. Dit besluit bepaalt dat een dergelijke verklaring ook bij een aanvraag voor een erkenning van een burgermiddel wordt geaccepteerd. Daarmee wordt het voor houders van een erkenning voor een bedrijfs- en organisatiemiddel mogelijk om voor dat middel zonder onnodige kosten een aanvraag in te dienen voor een erkenning van een burgermiddel. Omdat voor ISO 17065 geen specifiek certificeringsschema beschikbaar is, heeft de Minister van Binnenlandse Zaken en Koninkrijksrelaties hiervoor een schema vastgesteld. Dat schema, of een vergelijkbaar schema dat is vastgesteld in een andere EU-lidstaat, moet ook zijn gevolgd om aan de eisen van dit besluit te voldoen.

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

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

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

5.4 Verlening van een voorwaardelijke erkenning
Wanneer uit de beoordeling van een aanvraag blijkt dat aan de gestelde voorwaarden is voldaan, wordt een erkenning verleend. In deze fase zijn de werking, de veiligheid en de betrouwbaarheid van het middel enkel op papier beoordeeld. Het is vervolgens noodzakelijk dat de feitelijke werking van het middel wordt getoetst alvorens het door burgers wordt gebruikt. Alleen door een dergelijke toetsing uit te voeren kan worden geconcludeerd of het middel ook in de praktijk kan voldoen aan de gestelde eisen en of erop kan worden vertrouwd dat het middel in voldoende mate beschikbaar zal zijn voor gebruikers.

Om deze toetsing mogelijk te maken wordt een erkenning verleend onder de opschortende voorwaarde dat de houder ervan binnen een periode van 6 maanden aantoont dat het middel ook feitelijk kan functioneren zoals in de aanvraag is aangegeven.

6. Eisen aan de houder van een erkenning
Aan de houder van een erkenning worden ook gedurende de looptijd van de erkenning eisen gesteld om het belang van veilige, betrouwbare en gebruiksvriendelijke identificatie te borgen. Aan deze eisen vindt toetsing plaats door de toezichthouder. In het hiernavolgende wordt op een aantal van die eisen ingegaan. Bij overtreding daarvan kan worden overgegaan tot het opleggen van een bestuurlijke boete of het intrekken of opschorten van de erkenning.

6.1 Vertrouwelijk omgaan met gegevens

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

6.2 Eisen voor verlening blijven van toepassing

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

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

6.3 Acceptatieplicht

Burgers moeten in principe gebruik kunnen maken van alle erkende identificatiemiddelen. In principe geldt dan ook dat een houder van een erkenning geen potentiële gebruikers mag weigeren, behalve wanneer acceptatie van die gebruiker redelijkerwijs niet kan worden verwacht. Daarvan kan bijvoorbeeld sprake zijn indien een gebruiker een openstaande schuld heeft bij de houder van de erkenning.

6.4 Meldingsplicht

De digitale wereld en daarin gebruikte methoden en standaarden zijn voortdurend in beweging. Een houder van een erkenning zal het middel dan ook regelmatig moeten aanpassen om te zorgen dat het kan blijven werken. Buiten deze noodzakelijke aanpassingen kan de houder van een erkenning er ook eigenstandig voor kiezen om de werking van het middel of de processen die daarmee verband houden te wijzigen. Deze wijzigingen kunnen een wezenlijke invloed hebben op de veiligheid, de betrouwbaarheid en de gebruiksvriendelijkheid van het middel. Omdat de erkenning is verleend op basis van de aanvraag kan een wijziging ertoe leiden dat de erkenning

niet meer geldt voor het middel. Dat is het geval als de wijzigingen niet van ondergeschikte aard zijn. In dat geval is het aan de houder van een erkenning om een wijziging van die erkenning aan te vragen. Om te voorkomen dat de Minister van BZK en de aangewezen toezichthouder een informatieachterstand oplopen waardoor een situatie ontstaat die niet meer kan worden rechtgezet, moeten wijzigingen van enige omvang actief worden gemeld.

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

6.5 Regels met betrekking tot het tarief

Het is van belang dat burgers zo laagdrempelig mogelijk kunnen inloggen om toegang te krijgen tot publieke dienstverlening. Daarom ligt het voor de hand dat drempels voor die toegang zoveel als mogelijk worden weggenomen. Een mogelijke drempel is de prijs die een burger moet betalen voor authenticatie. Wanneer per authenticatie moet worden betaald kan dat voor burgers reden zijn om het middel minder te gebruiken. Daarom heeft het kabinet besloten dat de Rijksoverheid de kosten voor het gebruik betaalt voor zover het gebruik plaatsvindt in het publieke domein.

In beginsel zou een subsidie daarvoor de geëigende weg zijn. In dit geval zou een burger telkens een subsidie moeten aanvragen voor een bedrag van enkele eurocenten per authenticatie. Dat is onnodig inefficiënt. Het verschuldigde bedrag zal derhalve rechtstreeks aan de aanbieder van het middel worden betaald, door middel van een rechtstreekse subsidie of op basis van een overeenkomst. Het is onwenselijk dat naast deze betalingen voor het gebruik van het middel kosten in rekening worden gebracht aan burgers die het middel gebruiken. Daarom bepaalt dit besluit dat slechts voor het aanschaffen van het middel kosten in rekening mogen worden gebracht bij deze gebruikers. Op grond van dit besluit kunnen nadere regels worden gesteld over het tarief dat de houder van een erkenning in rekening brengt bij de gebruiker (voor aanschaf van het middel) of bij de Rijksoverheid (voor gebruik van het middel).

6.6 Nadere regels bij ministeriele regeling

Dit besluit biedt de mogelijkheid om bij ministeriële regeling nadere verplichtingen op te leggen aan de houder van een erkenning. Het gaat om verplichtingen die op een hoger detailniveau invulling geven aan het belang van veilige, betrouwbare en gebruiksvriendelijke identificatie door burgers. Aan een houder van een erkenning kunnen op grond van artikel 2.20, eerste lid, bijvoorbeeld de volgende aanvullende eisen worden gesteld:

- Het bereikbaar zijn voor gebruikers, waardoor deze terecht kunnen als het door hen gebruikte middel niet werkt (onderdeel a). Gelet op het belang van toegang is het nodig dat burgers met problemen worden geholpen bij het oplossen daarvan.
- Het treffen van organisatorische waarborgen ter bescherming van gegevens van gebruikers (onderdeel b). In paragraaf 6.5 is uiteengezet dat aan een houder van een erkenning eisen worden gesteld met betrekking tot de betrouwbare behandeling van gegevens. Bij ministeriële regeling kunnen aanvullende eisen worden gesteld.

- Een inzagemogelijkheid voor bepaalde gegevens (onderdeel c). Gegevens van gebruikers kunnen bijvoorbeeld noodzakelijk zijn in het kader van het afhandelen van geschillen.
- Een verplichting om gebruikers binnen een bepaalde termijn of op een specifieke wijze te informeren wanneer het middel door onderhoudswerkzaamheden niet beschikbaar zal zijn (onderdeel e).
- Een verplichting om bereikbaar te zijn voor medewerkers van dienstverleners of beheerders van de GDI (onderdeel f).
- Een verplichting om het middel een bepaald percentage van de tijd storingvrij en vrij van onderbrekingen aan te bieden (onderdeel g). Burgers moeten in voldoende mate toegang kunnen krijgen tot publieke digitale dienstverlening. Daarvoor is het identificatie met een identificatiemiddel onmisbaar. Wanneer een burger heeft gekozen voor een bepaald identificatiemiddel moet dat middel vervolgens in voldoende mate beschikbaar zijn. Het is derhalve niet acceptabel als een middel veelvuldig gedurende lange tijd niet beschikbaar is. Wanneer een dergelijke regel wordt gesteld is het op grond van de wettelijke systematiek mogelijk om op te treden, bijvoorbeeld door een erkenning in te trekken of een bestuurlijke boete op te leggen.

7. Wijziging, schorsing en intrekking

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

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

7.1 Wijzigen erkenning op verzoek, algemeen

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

7.2 Beëindiging erkenning op verzoek van de houder

Een houder van een erkenning is gehouden het middel daadwerkelijk aan te bieden en te borgen dat het middel beschikbaar is voor gebruikers. Op die verplichtingen is nader ingegaan in de paragrafen 6.2 en 6.6 van deze toelichting. Deze verplichtingen gelden zolang de erkenning geldt. Een houder van een erkenning die het middel niet langer wil blijven aanbieden zal daarom om beëindiging van de erkenning moeten verzoeken. Een dergelijke beëindiging heeft gevolgen voor gebruikers. Daarom wordt met dit besluit vastgelegd dat de beëindigingsprocedure de noodzakelijke waarborgen heeft om te zorgen dat burgers voldoende tijdig op de hoogte worden gebracht en dat hun gegevens waar nodig beschikbaar blijven zonder afbreuk te doen aan de veiligheidseisen die daarmee gepaard gaan.

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

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

8. Regeldruk en administratieve lasten

Kosten voor het indienen van een aanvraag en voor houders van een erkenning
Het indienen van een aanvraag vergt een investering, zowel in tijd als financieel. Voor zover de kosten voorvloeien uit dit besluit is gepoogd deze zo laag mogelijk te houden. De kosten die een private partij moet maken om erkend te worden bestaan in hoofdzaak uit kosten voor certificering. Het vereiste certificaat wordt op grond van een audit door een geaccrediteerde auditpartij afgegeven. Die auditpartij doet dit in opdracht en op kosten van de partij die zijn diensten wil laten erkennen. De kosten van een audit bestaan uit de kosten van de uitvoering van de audit en de kosten van de partij die erkend wil worden voor de voorbereiding van de audit. Deze voorbereidingskosten zijn voor de eerste keer dat de audit wordt uitgevoerd een factor 2 tot 4 hoger dan voor de jaarlijkse herhaalaudits omdat voor de eerste audit het bewijs dat aan de eisen wordt voldaan en het ophalen van de daarvoor benodigde informatie voor het eerst moet worden gestructureerd. Het ervaringsniveau van de te erkennen partij ten aanzien van het ondergaan van audits en de voorbereiding daarop is in dit kader bepalend voor de omvang van de benodigde voorbereiding.
Een aanvrager en een houder van een erkenning moet beschikken over een geldig certificaat. De inhoud van dat certificaat wordt bij ministeriële regeling vastgesteld. In dit besluit wordt enkel vastgelegd over welke accreditatie de certificerende instantie moet beschikken. Voor de aanvrager

of houder van een erkenning wordt gedacht aan ISO 27001 of de certificering die wordt gehanteerd voor een bedrijfs- en organisatiemiddel. Als gevolg hiervan zijn voldoende certificerende instellingen beschikbaar en is er sprake van marktwerking.
Tot slot zal een te erkennen aanbieder van een identificatiemiddel in het kader van de productie van bewijs, dat aan specifieke eisen moet worden voldaan, een technische beveiligingstest moeten uitvoeren en deze driejaarlijks moet herhalen. Deze audit vloeit voort uit de eisen van de Uitvoeringsverordening, die met dit besluit van toepassing worden verklaard. Deze audit wordt beschouwd als normale 'productiekosten' van een dienst, de kosten daarvan worden in dit kader niet beschouwd als 'additioneel' ten gevolge van deze regelgeving. Naar schatting zal een dergelijke test per identificatiemiddel en bijbehorend authenticatiemechanisme plusminus 25.000 euro bedragen al naar gelang de complexiteit van een middel en mechanisme. Hier geldt dat bij beperkte wijziging van een middel een herhaalde audit minder kosten met zich meebrengt dan bij een fundamentelere wijziging van middel en mechanisme.
Concluderend zijn de kosten van een erkenning afhankelijk van:

- De specifieke infrastructuur van de erkende of te erkennen dienst of diensten;
- Het al dan niet reeds in bezit zijn van een certificering zoals ISO/IEC 27001 en ETSI 319-411-2;
- Het aantal middelen dat moet worden erkend;
- De complexiteit van het middel en het bijbehorende authenticatiemechanisme;
- De aard, omvang en frequentie van wijzigingen die in de tijd worden aangebracht aan het middel en het authenticatiemechanisme.

9. Consultatie

[PM]

Artikelsgewijze toelichting

Artikel 2.3

In dit artikel is de eis vervat dat een middel moet kunnen functioneren met de onderdelen die nodig zijn voor het functioneren daarvan. Verder kan als gevolg van onderdeel b van dit artikel dat een aanvraag worden afgewezen indien de aanvrager niet kan aantonen dat de gegevens over de gebruiker worden bewaard op zodanige wijze dat deze niet zijn te herleiden tot de gegevens over het gebruik door die gebruiker.

Artikel 2.4

Artikel 2.4 biedt een basis om nadere eisen te stellen aan een middel en de aanbieder daarvan. De onderdelen a tot en met h van het eerste lid maken het mogelijk om eisen te stellen met betrekking tot de onderwerpen waarop het Europese eIDAS-regelgevingscomplex ziet. Daartoe zijn in deze onderdelen de onderwerpen gehanteerd uit de bijlage bij eIDAS-uitvoeringsverordening 1502. Een uitzondering is het begrip "intrekking" in onderdeel e, dat beter aansluit bij het woordgebruik in de praktijk dan het in de verordening gebruikte "herroeping".

Tweede lid

In de paragrafen 4.1.2 en 4.1.4 van het algemene deel van deze toelichting wordt ingegaan op de grondslagen in het voorgestelde artikel 2.4, tweede lid.

Artikel 2.6

Een aanvraag kan op grond van artikel 2.6 slechts worden ingediend door een rechtspersoon of andere onderneming naar Nederlands recht of naar het recht van een andere EU-lidstaat. Daarmee wordt voorkomen dat de integriteitstoetsing onmogelijk wordt. Als een aanvraag wordt ingediend door een natuurlijke persoon wordt deze op grond van artikel 4:5 van de Algemene wet bestuursrecht niet in behandeling genomen.

Artikel 2.7

Het tweede lid biedt onder meer een basis om het gebruik van een aanvraagformulier te verplichten.

Artikel 2.8

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

Eerste en tweede lid

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

Derde lid

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

Vierde lid

Accreditatie op grond van ISO 27006 ziet op algemene aspecten van gegevensbeveiliging. Daarom schrijft artikel 2.8, derde lid, van dit besluit specifiek voor dat een verklaring van een op grond van ISO 27006 gecertificeerde instelling moet zien op het identificatiemiddel.

Artikel 2.10

In paragraaf 3.6 is uiteengezet dat de erkenning waarop dit besluit ziet een vergunning is in de zin van de Dienstenrichtlijn. Op grond van artikel 28 van de Dienstenwet wordt een dergelijke vergunning na het verstrijken van de beslistermijn in beginsel verleend, tenzij bij wettelijk voorschrift anders is bepaald.

Deze regel zou zonder nadere regeling ook gelden voor de erkenning van een privaat identificatiemiddel voor burgers. Met het uitvoeren van een beoordeling van een identificatiemiddel voor burgers worden burgers beschermd. Met het van rechtswege verlenen van de erkenning, zonder die beoordeling, wordt het belang van burgers op onaanvaardbare wijze geschaad. Daarom wordt met artikel 2.10 bepaald dat de vergunning niet van rechtswege wordt verleend.

Artikel 2.12

Het eerste lid van artikel 2.12 bepaalt dat een erkenning voor onbepaalde tijd wordt verleend. Verlening voor onbepaalde tijd is het uitgangspunt in gevallen waarin geen sprake is van schaarste.

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

Artikel 2.17

Dit artikel regelt de meldingsplicht voor houders van een erkenning. Daarop wordt in paragraaf 6.3 van deze toelichting ingegaan. In dit verband wordt nog vermeld dat een houder van een erkenning op grond van het eerste lid, onderdeel c, gehouden is wijzigingen in de organisatie of de zeggenschap te melden. Dat maakt het mogelijk om ook na verlening van een erkenning een beoordeling te doen in het kader van de Wet bevordering integriteitsbeoordelingen door het openbaar bestuur. Op grond van artikel 9, zevende lid, van de wet kan een verleende erkenning worden geschorst of ingetrokken als is gebleken dat ernstig gevaar bestaat dat de erkenning wordt gebruikt voor het plegen van strafbare feiten.

Artikel 2.18

In het eerste lid van dit artikel is vastgelegd dat een houder van een erkenning bij de burger die het middel gebruikt geen bedrag in rekening brengt voor het gebruik daarvan. Op de beleidsmatige achtergrond van deze bepaling wordt ingegaan in paragraaf 6.4 van deze toelichting. Dit artikellid laat de houder van erkenning de keuze om een bedrag in rekening te brengen voor het aanschaffen van het middel.

Artikel 2.19

Met dit artikel wordt geregeld dat een houder van een erkenning ervoor moet zorgen dat alle gegevens die bij de houder ter kennis komen, vertrouwelijk behandelt. Een betrouwbare toegang van natuurlijke personen tot elektronische dienstverlening valt of staat immers met een organisatie die de haar ter beschikking staande gegevens van derden vertrouwelijk behandelt. Dit

houdt onder meer in dat toegang tot de gegevens beperkt is tot daartoe gerechtigde personen en dat er technische en organisatorische beveiligingsmaatregelen zijn genomen. Daarbij past tevens dat de houder beschikt over een loket waar betrokkenen in de toegang van elektronische dienstverlening aan ondernemingen en rechtspersonen terecht kunnen in geval van vragen of ontstane problemen in die toegang, bijvoorbeeld in het geval van security-meldingen. Die verplichting wordt uitgewerkt op grond van artikel 2.20, eerste lid, onderdeel a.
Onderdeel b regelt dat gegevens die door een houder van een erkenning worden verwerkt niet voor andere doeleinden mogen worden gebruikt dan voor authenticatie in het kader van de erkenning, dus bij de publieke dienstverleners waarop de wet ziet. Artikel 6, eerste lid, onderdeel a, van de Algemene verordening gegevensbescherming kan niet worden toegepast om de gegevens toch voor deze doeleinden te gebruiken als de gebruiker daarvoor toestemming heeft verleend.

Artikel 2.20
In paragraaf 6.6 wordt ingegaan op de noodzaak en de inhoud van dit artikel. Het betreft nadere eisen aan een houder van een erkenning, dus eisen waaraan een erkende private aanbieder van een identificatiemiddel moet voldoen. Het betreft eisen die naar hun aard en detailniveau vergelijkbaar zijn met de eisen, bedoeld in artikel 2.4. Daarom regelt dit besluit dat deze nadere eisen ook kunnen worden gesteld bij ministeriële regeling. De eisen die op grond van artikel 2.4 worden gesteld gelden ook voor de houder van een erkenning, door de koppelbepaling in artikel 2.13.
Onderdeel g van het eerste lid verdient in dit verband nadere duiding. Artikel 9, vierde lid, van de wet bepaalt dat aan de houder van een erkenning eisen worden gesteld, waaronder in ieder geval regels over een leveringsplicht. Met onderdeel g wordt deze de leveringsplicht uitgewerkt. Het gaat om de mate waarin het middel beschikbaar moet zijn voor gebruikers. Te denken valt aan een percentage van de tijd. Omdat er geen bestaande praktijk is met ervaring over het te hanteren percentage, wordt dat percentage bij ministeriële regeling vastgesteld. Het is denkbaar dat een onderscheid tussen verschillende soorten identificatiemiddelen wenselijk is. Het tweede lid van artikel 2.20 biedt daarvoor de ruimte.

Artikel 2.21
Een erkenning kan worden gewijzigd, bijvoorbeeld wanneer de houder van een erkenning ingrijpende wijzigingen wil doorvoeren in de werking van het middel waarop de erkenning ziet. In dat geval zou de erkenning niet meer zien op het gewijzigde middel. Dit artikel regelt dat een wijziging wordt beoordeeld op wijze waarop een eerste aanvraag ook wordt behandeld, met uitzondering van de eisen die in artikel 2.2 worden gesteld aan de aanvrager.
Het tweede lid regelt dat een erkenning niet kan overgaan naar een rechtspersoon buiten de Europese Unie of de Europese Economische Ruimte. Daarmee geldt hetzelfde voor het indienen van een eerste aanvraag.

Artikel 3.1

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