Staatsblad
van het Koninkrijk der Nederlanden

Jaargang 2003

200

Besluit van 8 mei 2003, houdende de vaststelling van eisen voor het verlenen van diensten voor elektronische handtekeningen (Besluit elektronische handtekeningen)

Wij Beatrix, bij de gratie Gods, Koningin der Nederlanden, Prinses van Oranje-Nassau, enz. enz. enz.

Op de voordracht van de Staatssecretaris van Economische Zaken van 13 november 2002, nr. DGTP/02/03931, Directie Wetgeving en Juridische Zaken;

Gelet op richtlijn nr. 1999/93/EG van het Europees Parlement en de Raad van de Europese Unie van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG 2000, L 13), alsmede op de artikelen 16.1, 18.15, eerste en tweede lid, en 18.17, eerste en vijfde lid, van de Telecommunicatiewet;

De Raad van State gehoord (advies van 12 december 2002, nr. W 10.02.0509/II);

Gezien het nader rapport van de Staatssecretaris van Economische Zaken van 7 mei 2003, nr. WJZ/03/00755;

Hebben goedgevonden en verstaan:

Artikel 1

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

a. wet:	Telecommunicatiewet;
b. certificatiediensten:	het afgeven, beheren en intrekken van gekwalificeerde certificaten door certificatiedienstverleners, alsmede andere diensten die samenhangen met het gebruik van elektronische handtekeningen;
c. sleutelbeheerdiensten:	het genereren, opslaan, verstrekken of vernietigen van cryptografisch sleutelmateriaal dat gebruikt wordt voor het aanmaken of het verifiëren van elektronische handtekeningen.

Artikel 2

1. Een certificatiedienstverlener als bedoeld in artikel 18.15, eerste lid, van de wet voldoet aan de volgende eisen:

a. hij beschikt over betrouwbare middelen en hanteert betrouwbare procedures voor het aanbieden van certificatiediensten aan het publiek;

b. hij past procedures en processen op het gebied van administratie en beheer toe overeenkomstig een beschreven kwaliteitssysteem dat in overeenstemming is met de laatste ontwikkelingen op het gebied van kwaliteitssystemen;

c. hij maakt uitsluitend gebruik van betrouwbare systemen en producten die procedureel of overeenkomstig de stand der techniek beveiligd zijn en die de technische en cryptografische veiligheid van de processen die zij ondersteunen garanderen;

d. hij neemt adequate maatregelen tegen het vervalsen van de gekwalificeerde certificaten die hij heeft uitgegeven en tegen het uitgeven van illegale gekwalificeerde certificaten en, indien hij gegevens voor het aanmaken van handtekeningen genereert, garandeert hij de vertrouwelijkheid van het proces waarmee dit gebeurt;

e. hij houdt voldoende financiële middelen ter beschikking om in overeenstemming met de eisen van de wet te kunnen functioneren;

f. hij heeft personeel in dienst dat deskundig is op het gebied van de aangeboden diensten, met name op het gebied van beheer, van de technologie voor elektronische handtekeningen, en van de beveiligingsprocedures die worden toegepast;

g. hij verifieert, alvorens een gekwalificeerd certificaat af te geven, de identiteit en eventuele specifieke attributen van de persoon die als ondertekenaar in dat certificaat wordt aangeduid door de geldigheid van de aangeboden documenten te controleren alsmede door de overeenstemming tussen de documenten en de kenmerken van de persoon te controleren door middel van visuele controle en zonodig met behulp van andere daartoe geschikte middelen;

h. hij stelt de datum en het tijdstip van afgifte en van intrekking van een gekwalificeerd certificaat vast met een nauwkeurigheid van één minuut of korter;

i. hij slaat tijdens de geldigheidsduur van het gekwalificeerde certificaat en gedurende een periode van ten minste zeven jaar na de datum waarop de geldigheid van het gekwalificeerde certificaat is verlopen alle relevante gegevens met betrekking tot dat gekwalificeerde certificaat op, met name de gegevens die benodigd zijn om in gerechtelijke procedures de certificatie te kunnen bewijzen, waaronder ten minste:

1°. het gekwalificeerde certificaat;

2°. alle gegevens waarmee de verificatie van de identiteit en van de attributen van de aanvrager bewezen kan worden, en

3°. alle historische gegevens over de afgifte en intrekking van het gekwalificeerde certificaat;

j. hij slaat ten behoeve van eigen gebruik en beheer certificaten zodanig op, in verifieerbare vorm en met gebruikmaking van betrouwbare systemen, dat:

1°. alleen bevoegde personen gegevens kunnen invoeren en wijzigen;

2°. de authenticiteit van de informatie kan worden gecontroleerd;

3°. de certificaten uitsluitend publiekelijk beschikbaar zijn in de gevallen waarvoor de ondertekenaar toestemming heeft gegeven, en

4°. elke technische wijziging die de genoemde beveiligingsvoorschriften in gevaar kan brengen, voor de gebruiker duidelijk is;

k. hij zorgt, met inachtneming van de door hem bekendgemaakte tijdsduur tussen verzoek tot intrekking en publicatie van die intrekking, voor een veilige en prompte intrekking van de door hem beheerde gekwalificeerde certificaten na ontvangst van een daartoe strekkend verzoek van de ondertekenaar of van een door hem aangewezen persoon of instantie, welk verzoek voldoet aan de door de certificatiedienstverlener bekendgemaakte procedure voor de intrekking van een gekwalificeerd certificaat;

l. hij publiceert, gedurende de geldigheid van het afgegeven gekwalifi-

ceerde certificaat, en tot ten minste zes maanden na het tijdstip waarop de geldigheid van het gekwalificeerde certificaat is verlopen of, indien dat tijdstip eerder valt, na het tijdstip waarop de geldigheid is beëindigd door intrekking, langs elektronische weg en zodanig dat die publicatie door alle gebruikers van de desbetreffende certificatiedienst alsmede door alle partijen die vertrouwen op de uitgegeven gekwalificeerde certificaten geraadpleegd kan worden:

1°. actuele en betrouwbare informatie over de status van de afgegeven gekwalificeerde certificaten, en

2°. afgegeven gekwalificeerde certificaten voor zover de ondertekenaar daarvoor toestemming heeft gegeven;

m. hij slaat de gegevens voor het aanmaken van elektronische handtekeningen van de personen aan wie hij sleutelbeheerdiensten heeft verleend niet op, en hij kopieert deze gegevens evenmin;

n. hij beschikt over beschreven klachtenafhandeling- en geschillenbeslechtingprocedures, en hanteert deze;

o. hij treft maatregelen om bij beëindiging van de dienstverlening de gegevens voor het aanmaken van de elektronische handtekening, waarmee de desbetreffende certificatiedienstverlener de uitgegeven gekwalificeerde certificaten tekent, te vernietigen op het vroegst mogelijke moment dat de publicatieverplichting, bedoeld in onderdeel l, dit mogelijk maakt;

p. hij treft zodanige voorzieningen dat bij beëindiging van de dienstverlening:

1°. de door hem afgegeven gekwalificeerde certificaten door een andere geregistreerde certificatiedienstverlener worden overgenomen en dat te dien aanzien voldaan wordt aan dit artikel, tenzij dit redelijkerwijze niet mogelijk is, alsmede de ondertekenaars daarvan in kennis worden gesteld;

2°. indien overneming als bedoeld in onderdeel 1° redelijkerwijze niet mogelijk is, de gekwalificeerde certificaten uiterlijk op het tijdstip waarop de dienstverlening wordt beëindigd worden ingetrokken, de ondertekenaars daarvan in kennis worden gesteld en voor het overige ten aanzien van de ingetrokken gekwalificeerde certificaten door een geregistreerde certificatiedienstverlener voldaan wordt aan de onderdelen i, j en q;

q. hij treft, ongeacht de reden en omstandigheden van beëindiging van de dienstverlening en voor zover de gekwalificeerde certificaten niet worden overgenomen door een andere certificatiedienstverlener, in ieder geval voorzieningen voor de voortzetting van de publicatie overeenkomstig onderdeel l, zulks op de tot dan gebruikelijke wijze en tot ten minste zes maanden na het tijdstip waarop de dienstverlening is beëindigd;

r. hij stelt schriftelijk, met behulp van een duurzaam communicatiemiddel en uit eigen beweging de persoon die een gekwalificeerd certificaat ter ondersteuning van zijn elektronische handtekening wenst en met wie hij een overeenkomst wil aangaan, en desgevraagd de derden, die op het gekwalificeerde certificaat vertrouwen, ten minste op de hoogte van:

1°. de exacte voorwaarden voor het gebruik van het gekwalificeerde certificaat met inbegrip van eventuele beperkingen inzake dit gebruik, alsmede van de wijzigingen van de voorwaarden;

2°. het bestaan van een vrijwillige accreditatie;

3°. de procedure voor intrekking van het gekwalificeerde certificaat zowel op verzoek van de gebruiker als door hem zelf, en

4°. de procedures voor klachtenbehandeling en geschillenbeslechting, en

s. hij toont door middel van een verklaring van een daartoe bevoegde instantie aan dat hij, ieder van de bestuurders van de onderneming, en de medewerkers die binnen zijn onderneming in het kader van het verlenen van certificatiediensten verantwoordelijk zijn voor de verwerking van

vertrouwelijke of gevoelige gegevens, niet binnen de laatste vier jaar wegens een misdrijf onherroepelijk zijn veroordeeld tot een onvoorwaardelijke vrijheidsstraf van meer dan zes maanden door een rechter in Nederland, de Nederlandse Antillen of Aruba.

2. Met een veroordeling als bedoeld in het eerste lid, onderdeel s, wordt gelijkgesteld een onherroepelijke veroordeling tot een onvoorwaardelijke vrijheidsstraf van meer dan zes maanden door een andere rechter wegens een misdrijf waarvoor naar Nederlands recht een bevel tot voorlopige hechtenis ingevolge artikel 67, eerste lid, van het Wetboek van Strafvordering is toegelaten;

3. Met een veroordeling tot een onvoorwaardelijke vrijheidsstraf als bedoeld in het tweede lid wordt gelijkgesteld een bevel tot tenuitvoerlegging van een zodanige onvoorwaardelijke vrijheidsstraf.

Artikel 3

Certificaten als bedoeld in artikel 18.15, tweede lid, van de wet bevatten ten minste:

a. de vermelding dat het certificaat als gekwalificeerd certificaat wordt afgegeven;

b. de identificatie en het land van vestiging van de afgevende certificatiedienstverlener;

c. de naam van de ondertekenaar of een als zodanig geïdentificeerd pseudoniem;

d. ruimte voor een specifiek attribuut van de ondertekenaar, dat indien nodig, afhankelijk van het doel van het gekwalificeerde certificaat, wordt vermeld;

e. gegevens voor het verifiëren van de handtekening die overeenstemmen met de gegevens voor het aanmaken van de handtekening die onder controle van de ondertekenaar staan;

f. vermelding van het tijdstippen van het begin en van het einde van de geldigheidsduur van het gekwalificeerde certificaat;

g. de identiteitscode van het gekwalificeerde certificaat;

h. de elektronische handtekening van de afgevende certificatiedienstverlener die voldoet aan de criteria van artikel 15a, tweede lid, onderdeel a tot en met d, van Boek 3 van het Burgerlijk Wetboek;

i. eventuele beperkingen betreffende het gebruik van het gekwalificeerde certificaat, en

j. eventuele grenzen met betrekking tot de waarde van de transacties waarvoor het gekwalificeerde certificaat kan worden gebruikt.

Artikel 4

1. De instelling die in aanmerking wenst te komen voor een aanwijzing als bedoeld in artikel 18.17, tweede lid, van de wet, dient daartoe een aanvraag in en voldoet aan de volgende eisen:

a. zij houdt zich niet bezig met activiteiten die een bedreiging kunnen vormen voor de onafhankelijkheid van haar oordeel en de integriteit bij de uitoefening van haar taak;

b. 1° zij is onafhankelijk van organisaties die betrokken zijn bij het ontwerpen, de fabricage, de verkoop en de levering, de installatie, het onderhoud of het beheer van veilige middelen, alsmede van certificatiedienstverleners en de gebruikers voor zover zij zich bedienen van veilige middelen voor het aanmaken van elektronische handtekeningen;

2°. zij is financieel onafhankelijk van de betrokken partijen;

3°. de directeur en het personeel dat met de beoordeling van de overeenstemming is belast, zijn geen ontwerper, fabrikant, leverancier of installateur van veilige middelen, noch certificatiedienstverlener, noch gemachtigden van een van die partijen;

4°. zij wordt niet rechtstreeks betrokken bij het ontwerp, de fabricage,

de verkoop of het onderhoud van veilige middelen, noch treedt zij op als gemachtigde van de hierbij betrokken partijen.

c. zij heeft personeel in dienst dat:

1°. voldoende bekwaamheid bezit om met een hoge mate van beroepsintegriteit de overeenstemming vast te stellen van de veilige middelen voor het aanmaken van elektronische handtekeningen met de eisen voor deze veilige middelen, bedoeld in artikel 5 van dit besluit, en

2°. betrouwbare procedures hanteert;

d. zij beoordeelt de overeenstemming op transparante wijze, stelt alle relevante informatie op schrift, zorgt ervoor dat alle geïnteresseerde partijen gebruik kunnen maken van haar diensten en past haar procedures zonder enige vorm van discriminatie toe;

e. zij beschikt over voldoende personeel en de nodige voorzieningen om de technische en administratieve werkzaamheden die uit haar taken voortvloeien, naar behoren en snel te kunnen verrichten;

f. het personeel dat belast is met de beoordeling van de overeenstemming van de veilige middelen met de eisen,

1°. heeft een adequate opleiding genoten, met name op het gebied van technologieën voor elektronische handtekeningen en de daaraan verbonden aspecten van de veiligheid van het gebruik van computers;

2°. bezit een behoorlijke kennis van voorschriften inzake de te verrichten overeenstemmingsbeoordelingen en heeft voldoende ervaring met dergelijke beoordelingen;

g. zij waarborgt de onpartijdigheid van het personeel, onder meer door de bezoldiging niet afhankelijk te stellen van het aantal uitgevoerde overeenstemmingbeoordelingen of van de resultaten van deze beoordelingen;

h. zij houdt voldoende financiële middelen ter beschikking om in overeenstemming met de eisen van de wet te kunnen functioneren;

i. zij behandelt de gegevens die haar ter kennis komen vertrouwelijk, en

j. zij staat in voor de overeengekomen activiteiten van de instellingen door welke zij een deel van de overeenstemmingbeoordeling laat uitvoeren en kan aantonen dat deze instelling in staat is de betrokken dienst te verlenen.

2. De instelling die deel uitmaakt van een organisatie die zich bezighoudt met andere activiteiten dan de beoordeling van de overeenstemming van veilige middelen voor het aanmaken van elektronische handtekeningen met de eisen van artikel 5, is binnen die organisatie herkenbaar als aangewezen instelling als bedoeld in artikel 18.17 van de wet, en scheidt haar werkzaamheden zodanig van de andere activiteiten, dat daardoor de correcte beoordeling van overeenstemming van veilige middelen is gewaarborgd.

Artikel 5

Een veilig middel voor het aanmaken van elektronische handtekeningen voldoet aan de volgende eisen:

a. het waarborgt dat de gegevens voor het aanmaken van elektronische handtekeningen in de praktijk slechts eenmaal kunnen voorkomen en de vertrouwelijkheid daarvan redelijkerwijs gegarandeerd is;

b. het waarborgt met redelijke zekerheid dat de gegevens voor het aanmaken van elektronische handtekeningen niet kunnen worden afgeleid en dat de elektronische handtekening beschermd is tegen vervalsing met de op het tijdstip van het afgeven van de verklaring beschikbare technieken;

c. het waarborgt dat de gegevens voor het aanmaken van elektronische handtekeningen door de legitieme ondertekenaar op betrouwbare wijze kunnen worden beschermd tegen gebruik door anderen;

d. het laat de te ondertekenen gegevens ongewijzigd en belet niet dat

die gegevens vóór de ondertekening aan de ondertekenaar worden voorgelegd.

Artikel 6

Bij ministeriële regeling kunnen nadere regels worden gesteld met betrekking tot de eisen genoemd in dit besluit.

Artikel 7

1. Aan artikel 4, eerste lid, van het Besluit vergoedingen Telecommunicatiewet[1] worden, onder vervanging van de punt achter onderdeel b door een komma, twee nieuwe onderdelen toegevoegd, luidende:

c. de aanwijzing van certificatie-organisaties als bedoeld in artikel 18.16, van de wet;

d. de aanwijzing van instellingen als bedoeld in artikel 18.17, tweede lid, van de wet.

2. Aan artikel 4, tweede lid, van het Besluit vergoedingen Telecommunicatiewet wordt, onder vervanging van de punt achter onderdeel h door een komma, een nieuw onderdeel i toegevoegd, luidende:

i. diensten van certificatiedienstverleners.

Artikel 8

Dit besluit treedt in werking op het tijdstip waarop de Wet elektronische handtekeningen in werking treedt.

[1] Stb. 1999, 130, gewijzigd bij besluit van 28 maart 2000, Stb. 143.

Het advies van de Raad van State wordt niet openbaar gemaakt op grond van artikel 25a, vijfde lid j° vierde lid onder b, van de Wet op de Raad van State, omdat het uitsluitend opmerkingen van redactionele aard bevat.

Artikel 9

Dit besluit wordt aangehaald als: Besluit elektronische handtekeningen.

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

's-Gravenhage, 8 mei 2003

Beatrix

De Staatssecretaris van Economische Zaken,
J. G. Wijn

Uitgegeven de *twintigste* mei 2003

De Minister van Justitie,
J. P. H. Donner

STB7760
ISSN 0920 - 2064
Sdu Uitgevers
's-Gravenhage 2003

NOTA VAN TOELICHTING

1. I. ALGEMEEN

1. Inleiding

Bij de Wet elektronische handtekeningen (Kamerstukken II, 2000–2001, 27 743) zijn Boek 3 en Boek 6 van het Burgerlijk Wetboek, de Telecommunicatiewet, alsmede de Wet op de economische delicten gewijzigd, ten behoeve van de regeling van respectievelijk de rechtsgevolgen van elektronische handtekeningen, de aansprakelijkheid van certificatiedienstverleners die gekwalificeerde certificaten aan het publiek afgeven en het toezicht op deze certificatiedienstverleners. Daarnaast zijn bepalingen opgenomen over vrijwillige accreditatie en over veilige middelen voor het aanmaken van elektronische handtekeningen. De Wet elektronische handtekeningen bevat de implementatie van de Richtlijn nr.1999/93/EG van het Europees Parlement en de Raad van de Europese Unie van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG 2000, L 13) (verder: de richtlijn), en de juridische basis voor de verdere implementatie van de eisen die in de bijlagen bij de richtlijn zijn opgenomen. Het onderhavige besluit strekt tot implementatie van deze bijlagen.

Ingevolge de ingevoegde artikelen 18.15, eerste en tweede lid, en 18.17, eerste lid, van de Telecommunicatiewet worden eisen gesteld aan achtereenvolgens:

– certificatiedienstverleners die gekwalificeerde certificaten aan het publiek afgeven;
– gekwalificeerde certificaten, en
– veilige middelen voor het aanmaken van elektronische handtekeningen.

Voorts zijn in artikel 4 van dit besluit de eisen opgenomen waaraan instellingen ingevolge artikel 18.17, vijfde lid, van de Telecommunicatiewet moeten voldoen om aangewezen te kunnen worden als een partij die verklaringen afgeeft, die de overeenstemming bevestigen met de eisen voor veilige middelen voor het aanmaken van elektronische handtekeningen, die zijn opgenomen in artikel 5 van het besluit.

De Wet elektronische handtekeningen en het onderhavige besluit geven samen invulling aan een belangrijke randvoorwaarde voor de ontwikkeling van elektronische handel en elektronisch openbaar bestuur («e-commerce» en «e-government») binnen Nederland en met de overige landen van de Europese Gemeenschap (EG) en de Europese Economische Ruimte (EER). Allerhande e-commerce en e-government toepassingen zullen profiteren van de harmonisering van de eisen voor elektronische handtekeningen en het gebruik ervan.

De keuze voor implementatie van de (technische) eisen van de richtlijnbijlagen in lagere regelgeving is ingegeven door de snelle technologische vooruitgang op het gebied van het elektronische berichtenverkeer. Deze technologische ontwikkelingen vragen om regelgeving die hiermee gelijke tred kan houden.

1.2. Verschillende soorten handtekeningen

De richtlijn maakt onderscheid tussen «gewone» elektronische handtekeningen en geavanceerde elektronische handtekeningen. Afhankelijk van het doel waarvoor een elektronische handtekening wordt gebruikt, kunnen partijen gebruik maken van een «gewone» elektronische handtekening dan wel van een elektronische handtekening die met meer waarborgen is omkleed.

Dit besluit bevat minimumnormen, zoals voor gekwalificeerde certificaten en veilige middelen om handtekeningen aan te maken, om

verschillende waarborgen te geven. Het gekwalificeerd certificaat maakt het mogelijk om een ondertekenaar te identificeren. Het gebruik van een veilig middel waarborgt dat de ondertekenaar zijn handtekening kan beschermen tegen gebruik door anderen. Als de ondertekenaar de elektronische handtekening baseert op een gekwalificeerd certificaat en de ondertekenaar voor het aanmaken van zijn handtekening gebruik maakt van een veilig middel, wordt ingevolge artikel 15a, eerste en tweede lid, van Afdeling 1A van Titel 1 van Boek 3 van het Burgerlijk Wetboek de methode van authentificatie van de ondertekenaar vermoed voldoende betrouwbaar te zijn en wordt aan de elektronische handtekening hetzelfde rechtsgevolg toegekend als aan een handgeschreven handtekening. De in dit besluit gestelde normen zijn derhalve te beschouwen als referentienormen voor de betrouwbaarheid van elektronische handtekeningen.

1.3. De eisen

1.3.1. De normstelling

De eisen genoemd in de bijlagen 1, 2 en 3 van de richtlijn, in dit besluit geïmplementeerd in respectievelijk de artikelen 3, 2 en 5, hebben het karakter van essentiële, technologie-onafhankelijke eisen. Dit technologie-onafhankelijke karakter en het bijbehorende abstractieniveau is in het onderhavige besluit zoveel mogelijk gehandhaafd. De ontwikkelingen staan echter niet stil.

De Europese standaardisatie organisaties, het European Telecommunications Standards Institute (ETSI) en het Comité Européen de Normalisation (CEN), hebben op initiatief van de Europese Commissie de eisen in het kader van het European Electronic Signature Standardization Initiative programma gepreciseerd in concretere technische specificaties en normen.

Verwacht wordt dat deze geconcretiseerde technische normen zullen worden gehanteerd door de Europese Commissie en door de Lidstaten van de Europese Unie om meer duidelijkheid en zekerheid te verschaffen aan certificatiedienstverleners, gebruikers en de toezichthouder dan mogelijk is op basis van uitsluitend de technologie-onafhankelijke eisen van de richtlijn.

In verband hiermee is in dit besluit reeds een uitwerking van sommige eisen gegeven.

De richtlijn geeft deze ruimte in overweging 14, waarbij als criterium wordt gesteld dat het van belang is om een evenwicht te vinden tussen de behoeften van de consumenten en die van het bedrijfsleven.

Niet alle in de bijlagen van de richtlijn geformuleerde eisen zijn zo duidelijk, dat de certificatiedienstverlener moet weten waaraan hij dient te voldoen en dat de toezichthouder weet waarop hij de certificatiedienstverlener kan controleren. Een open norm als bijvoorbeeld die in onderdeel i van bijlage II ten aanzien van de bewaartermijn voor alle relevante informatie met betrekking tot een gekwalificeerd certificaat dient daarom te worden ingevuld om binnen de nationale rechtsorde voldoende zekerheid te geven. Gedurende de geldigheid van het gekwalificeerde certificaat, en vervolgens gedurende een periode van tenminste zeven jaar moeten de in artikel 2, eerste lid, onderdeel i, genoemde gegevens worden opgeslagen.

Op een enkel punt is deze ruimte benut om aanvullende eisen te formuleren, die echter passen bij het karakter van de richtlijn, en die noodzakelijke uitwerkingen van de eisen van de richtlijn zijn voor het waarborgen van een goede en betrouwbare certificatiedienstverlening. Dit betreft met name de continuïteit van de dienstverlening als geheel en het bestaan van een in documenten neergelegde klachten- en geschillenafhandelingsprocedure. Deze twee zaken worden in de volgende twee subparagrafen apart toegelicht.

De totstandkoming van concretere technische normen is er de aanleiding voor dat in het besluit de bepaling is opgenomen dat bij ministeriële regeling een nadere invulling aan de essentiële eisen kan worden gegeven. Van deze mogelijkheid zal in ieder geval gebruik worden gemaakt voor een nadere concretisering van een aantal van de eisen, genoemd in de artikelen 2 en 5 van dit besluit, om zowel de certificatiedienstverleners als de toezichthouder een gestandaardiseerd handvat te geven voor het bereiken van het gewenste niveau van betrouwbaarheid, veiligheid en dienstverlening. De nadere invulling bij ministeriële regeling zal geschieden met inachtneming van hiervoor bedoelde technische normen, die door de instanties ETSI en CEN zijn gepubliceerd en de algemeen erkende normen voor producten voor elektronische handtekeningen die door de Europese Commissie worden gepubliceerd, ter uitvoering van artikel 3, vijfde lid, van de richtlijn.

Aan de certificatiedienstverleners worden geen verplichtingen opgelegd die het waarborgen van een goede en veilige dienstverlening te buiten gaan.

In artikel 5 van het besluit zijn de eisen opgenomen voor veilige middelen voor het aanmaken van elektronische handtekeningen. De wettelijke basis voor deze eisen is gelegen in de artikelen 1.1, onderdeel gg, en 18.17, eerste lid, van de Telecommunicatiewet.

De eisen, opgenomen in artikel 4 van dit besluit, waaraan instellingen ingevolge artikel 18.17, vijfde lid, van de Telecommunicatiewet moeten voldoen om aangewezen te kunnen worden als een partij die verklaringen afgeeft die de overeenstemming bevestigen van veilige middelen met de eisen van artikel 5 van het besluit, zijn gebaseerd op de beschikking van de Europese Commissie van 6 november 2000 (kennisgeving C(2000) 3179) betreffende de minimumcriteria die lidstaten in acht moeten nemen bij de aanwijzing van instanties (PbEG 2000, L 289). Deze zijn opgesteld overeenkomstig artikel 3, vierde lid, van de richtlijn. Het gaat hierbij om partijen die productcertificering kunnen uitvoeren op dit gebied. De onderliggende productevaluatie is specialistisch van aard en zal slechts door een beperkt aantal partijen uitgevoerd kunnen worden.

1.3.2 Continuïteit en beëindiging van de dienstverlening

De certificatiedienstverleners waarborgen door hun dienstverlening de mogelijkheden van het gebruik van de elektronische handtekeningen. De gebruikers zijn de houders van de gekwalificeerde certificaten (de ondertekenaars), en de partijen die op de juistheid van een gekwalificeerd certificaat vertrouwen: de ontvangers van een bericht met een elektronische handtekening. Het is belangrijk dat die gebruikers van elektronische handtekeningen vertrouwen hebben in de betrouwbaarheid van de certificatiedienstverlening.

De certificatiedienstverlening moet onder meer inhouden, dat gebruikers zo min mogelijk schade lijden door haperende dienstverlening als gevolg van vrijwillige of gedwongen bedrijfsbeëindiging. Dit laatste kan zich voordoen in het geval van faillissement, of bij beëindiging van de registratie als gevolg van het niet (meer) voldoen aan de wettelijke eisen.

De noodzaak om van overheidswege op continuïteit gerichte maatregelen te verlangen is eveneens in andere lidstaten en in Nederland, in een vroeger stadium van beleidsontwikkeling, in de notitie Nationaal TTP-project (kamerstukken II, 1998–1999, nr. 26 581), onderkend. Wil de dienstverlening over langere tijd gewaarborgd zijn op een voor de gebruikers aanvaardbaar niveau, dan moeten de certificatiedienstverleners een zekere continuïteit hebben. De beëindiging van de diensten van een certificatiedienstverlener zonder dat er voorzieningen zijn getroffen om de belangen van de betrokken partijen te behartigen, is een bedreiging voor de betrouwbaarheid van de certificatiedienstverlening en schaadt het vertrouwen in die dienstverlening. De partijen die niet meer

kunnen verifiëren wie de ondertekenaar is van een bericht, of die niet meer kunnen achterhalen dat de ondertekenaar die een pseudoniem gebruikt de persoon is die zij kennen, zullen terughoudender gebruikmaken van de mogelijkheden die het elektronische berichtenverkeer heeft.

Het onderhavige besluit stelt diverse eisen aan de certificatiedienstverleners die gekwalificeerde certificaten aan het publiek afgeven, die in meer of mindere mate betekenis voor de continuïteit van de dienstverlening hebben. Hierbij moet ten eerste gedacht worden aan de eis dat een certificatiedienstverlener voldoende financiële middelen ter beschikking houdt om eventuele gevolgen van aansprakelijkheid redelijkerwijs te kunnen dragen. In beginsel is de certificatiedienstverlener vrij om te kiezen hoe aan deze eis wordt voldaan. Dit kan door voldoende kasmiddelen te houden of door het afsluiten van een verzekering, of door een andere passende voorziening. Ten tweede wordt de eis gesteld dat een certificatiedienstverlener zodanige voorzieningen treft dat na beëindiging van de dienstverlening, ongeacht de reden van deze beëindiging, het beheer van de op het tijdstip van beëindiging nog geldige certificaten wordt overgedragen aan een andere bij de toezichthouder geregistreerde certificatiedienstverlener. Mocht deze overdracht echter redelijkerwijs niet mogelijk zijn, dan moet, met het oog op de rechtszekerheid, de certificatiedienstverlener bij beëindiging van zijn dienstverlening alle door hem uitgegeven en op dat tijdstip nog geldige gekwalificeerde certificaten intrekken.

Ongeacht of de certificaten worden overgedragen of niet, moet de certificatiedienstverlener voorzieningen treffen opdat:

– de status van de afgegeven gekwalificeerde certificaten onverminderd correct is en tenminste zes maanden na de datum van intrekking van het gekwalificeerde certificaat raadpleegbaar is voor gebruikers van elektronische handtekeningen;

– alle gegevens die de certificatie bewijzen en de historie van intrekking van certificaten gedurende de geldigheid van het gekwalificeerde certificaat en vervolgens zeven jaar na het tijdstip waarop het gekwalificeerde certificaat zijn geldigheid heeft verloren worden opgeslagen zodat zij toegankelijk blijven, met name ten behoeve van gerechtelijke procedures;

– de gegevens voor het aanmaken van de elektronische handtekening, waarmee de desbetreffende certificatiedienstverlener de uitgegeven certificaten tekent, worden vernietigd op het vroegst mogelijke moment dat de publicatieverplichting, bedoeld in artikel 2, eerste lid, onderdeel l, dit mogelijk maakt.

De eerste twee maatregelen betreffen derhalve de continuïteit van de dienstverlening door de toegankelijkheid van de gegevens te waarborgen gedurende een voor de soort gegevens vastgestelde periode, de derde genoemde maatregel is gericht tegen het misbruik van de software of andere gegevens, die door deze certificatiedienstverlener bij de ondertekening van de door hem afgegeven gekwalificeerde certificaten werden gebruikt.

Door de toezichthouder zal regelmatig worden gecontroleerd of de geregistreerde certificatiedienstverlener de hiervoor bedoelde voorzieningen in stand houdt. Indien de certificatiedienstverlener deze voorzieningen niet in stand houdt, waardoor de continuïteit van de dienstverlener in gevaar komt, treft de toezichthouder de nodige maatregelen om te zorgen dat deze certificatiedienstverlener de belangen van de ondertekenaars blijft behartigen. Hierbij kan gedacht worden aan het toepassen van artikel 2.2, derde lid, onderdeel f, van de Telecommunicatiewet door het stellen van een termijn, met de dreiging dat na verloop van die termijn de registratie wordt ingetrokken. In het belang van de ondertekenaars kan de toezichthouder ook besluiten tot gebruikmaking van artikel 15.2, tweede lid, van de Telecommunicatiewet, en bestuursdwang toepassen.

1.3.3 Klachten- en geschillenafhandelingsprocedure

De richtlijn stelt in bijlage II, onderdeel k, dat een certificatiedienstverlener de persoon, met wie hij een contractuele relatie aangaat in verband met de afgifte van een gekwalificeerd certificaat, op de hoogte moet brengen van onder meer de gehanteerde procedures voor klachtenbehandeling en geschillenbeslechting. Dit houdt geen directe verplichting in voor de certificatiedienstverlener om ook daadwerkelijk een beschreven klachtenafhandelings- en geschillenbeslechtingsprocedure te hanteren. Het is hierdoor mogelijk dat de certificatiedienstverlener kan volstaan met te melden geen procedure hiervoor te hebben. Echter, vanwege de hoge mate van vertrouwen die burgers, bedrijven en instellingen in de certificatiedienstverlening zullen (en moeten blijven) stellen, is een deugdelijke afhandeling van eventuele klachten gewenst. Dit is eveneens reeds onderkend in de notitie Nationaal TTP-project. Daarom is in artikel 2, eerste lid, onderdeel n, van het onderhavige besluit de verplichting opgenomen dat de certificatiedienstverlener beschikt over beschreven klachtenafhandeling- en geschillenbeslechtingprocedures, en deze hanteert.

1.4. Adviezen

Het ontwerp-besluit is voor advies voorgelegd aan het Permanent Overlegorgaan Post- en Telecommunicatie, de Onafhankelijke Post- en Telecommunicatieautoriteit (OPTA), het College Bescherming Persoonsgegevens (voorheen de Registratiekamer), de Taskforce PKI Overheid, en het Electronic Commerce Platform Nederland (ECP.NL). Op deze adviezen wordt hieronder ingegaan.

Het advies van het Permanent Overlegorgaan Post- en Telecommunicatie betreft niet zozeer de elementen die in het onderhavige besluit zijn verwoord, maar uitsluitend de keuze van de toezichthouder. Men vraagt zich af of de aanwijzing van de OPTA de meest voor de hand liggende is, met name omdat het toezicht slecht aan zou sluiten bij de overige activiteiten van de OPTA en omdat naar verwachting hiermee geen duurzame oplossing wordt gecreëerd.

In de memorie van toelichting bij de Wet elektronische handtekeningen (kamerstukken II, 2000–2001, 27 743, nr. 3) zijn de overwegingen gegeven om te kiezen voor OPTA. Deze overwegingen zijn nog steeds valide. Er is geen aanleiding een andere keuze te maken.

De Onafhankelijke Post- en Telecommunicatie Autoriteit (in deze paragraaf: het college of OPTA) vraagt in het belang van marktpartijen duidelijkheid op twee punten.

Ten eerste wijst het college op het belang voor de marktpartijen en voor het toezicht van een eenduidige norm of van eenduidige normen die gesteld worden aan de certificatiedienstverleners die gekwalificeerde certificaten aanbieden aan het publiek. Het college erkent dat het ontwerp-besluit eisen stelt, maar constateert dat een concrete verwijzing naar een specifieke norm ontbreekt, terwijl het besluit de ruimte creëert om dit middels een ministeriële regeling te doen.

In het onderhavige besluit is waar mogelijk een zowel voor de certificatiedienstverlener als voor de toezichthouder werkbare concretisering van de essentiële eisen opgenomen. In paragraaf 1.3.1 van deze toelichting is aangegeven voor welke artikelen van dit besluit middels een ministeriële regeling een specifieke norm wordt voorzien.

Ten tweede wijst het college op de mogelijke drempelwerking die de huidige tariefsystematiek voor de toerekening van toezichtkosten aan de marktpartijen met zich mee brengt.

Inderdaad kunnen, met name in de aanloopfase van deze markt, aanzienlijke kosten ontstaan vanwege de noodzakelijke opbouw en onderhoud van voldoende kennis en kunde binnen de OPTA in relatie tot

een gering aantal marktpartijen. Door een gerichte en tijdelijke bijdrage van het ministerie van Economische Zaken worden vooralsnog voor de eerste twee jaren na het tijdstip van inwerkingtreding van de Wet elektronische handtekeningen en van dit besluit de jaarlijks door de geregistreerde certificatiedienstverleners aan het college te betalen vergoedingen tot een aanvaardbaar niveau terug gebracht. Bij het besluit om deze bijdrage ter beschikking te stellen heeft het grote belang dat de overheid hecht aan het totstandkomen van een goede certificatiedienstverlening in Nederland een wezenlijke rol gespeeld.

Het college wijst daarnaast op een aantal punten waar nadere toelichting wenselijk is, hetgeen tot verduidelijking in het besluit en de nota van toelichting heeft geleid. Het betreft de volgende punten:

• De eis in artikel 2, eerste lid, onderdeel e, om voldoende financiële middelen ter beschikking te houden om in overeenstemming met de wet te kunnen functioneren. Hiermee wordt niet zozeer de financiële gezondheid van de certificatiedienstverlener bedoeld, maar veeleer het treffen van voorzieningen die het mogelijk maken om de betrouwbaarheid te garanderen en om de gevolgen te dragen van de aansprakelijkheid die samenhangt met de uitgifte van gekwalificeerde certificaten, zonder dat dit het voortbestaan van de certificatiedienstverlener bedreigt.

• De wijze van vaststelling van de identiteit van een persoon alvorens een gekwalificeerd certificaat uit te geven. Het wetsvoorstel geeft reeds aan dat dit aan de hand van een document zoals bedoeld in artikel 1 van de Wet op de identificatieplicht dient te geschieden, maar de wijze waarop dat moet gebeuren en welke gegevens ter latere verificatie door de certificatiedienstverlener dienen te worden vastgelegd, was echter niet bepaald. In de huidige tekst is als minimumeis in artikel 2, eerste lid, onderdeel g opgenomen dat de overeenkomst tussen de persoon en de door hem overgelegde identiteitsdocumenten door visuele controle geschiedt, en zo nodig door andere passende middelen. Het gebruik van andere controlemiddelen zou van belang kunnen zijn indien sprake is van twee personen met dezelfde naam, en in verband met de aanwezigheid van attributen.

Het College Bescherming Persoonsgegevens (CBP) vraagt in zijn advies aandacht voor de privacy-aspecten die verbonden zijn aan TTP-diensten en wijst hierbij op het rapport *Sleutels van vertrouwen* dat in 2001 is uitgebracht. Het CBP vraagt om een actieve behandeling van de in dat rapport geformuleerde aanbevelingen en benadrukt de wenselijkheid om Privacy Enhancing Technologies (PET) te ontwikkelen, een onderwerp waar de TTP-sector een belangrijke rol in zou kunnen spelen. De evaluatie van het nationaal TTP-beleid, welke gepland staat in 2003, acht zij in dit verband te laat.

In het algemeen is de certificatiedienstverlener gehouden slechts met toestemming van de betrokkene persoonsgegevens te verzamelen of te verwerken voor andere doeleinden dan nodig is voor de certificatiediensten. Dit voorschrift is in artikel 11.5a van de Telecommunicatiewet expliciet verwoord. Verwezen wordt naar de toelichting bij dat artikel. Ingevolge artikel 15.1 van de Telecommunicatiewet houdt OPTA toezicht op de naleving. Bij de beoordeling of aan genoemd artikel 11.5a wordt voldaan en of de middelen en processen die de certificatiedienstverlener hanteert voldoende betrouwbaar zijn in de zin dat persoonsgegevens adequaat worden beschermd, zal de toezichthouder onderzoeken of de bevragingen die door middel van de openbare directory kunnen worden gedaan in overeenstemming zijn met het doel van deze directory, en dat die gegevens alleen beschikbaar komen voor zover daarvoor toestemming is gegeven door de certificaathouder. Ook kan rekening gehouden worden met de aanwezigheid van alternatieven voor het gebruik van deze directory.

De Taskforce PKI Overheid (verder: de taskforce) stelt met name de volgende twee punten aan de orde.

Ten eerste stelt de taskforce de vraag in welke mate bij de bepaling van de in dit besluit geformuleerde eisen ook de eisen een rol hebben gespeeld zoals deze in andere lidstaten van de Europese Unie zijn verwoord en in welke mate men zich heeft gebaseerd op een (internationaal) geaccepteerde praktijk, zulks in het licht van de harmonisatiedoelstelling van de richtlijn.

De exacte formuleringen zoals andere lidstaten deze hanteren zijn, voor zover beschikbaar, vergeleken. Zoals in paragraaf 3 al is aangegeven, is de standaardisatie in CEN- en ETSI-verband als richtsnoer voor het formuleren van eisen gebruikt. De nadere normering die tot stand komt in deze internationale organisaties zullen als basis voor nadere invulling van de essentiële eisen uit dit besluit dienen.

Ten tweede constateert de taskforce bij de bepalingen omtrent de continuïteit van de dienstverlening van een certificatiedienstverlener, dat het de voorkeur heeft dat de certificatiedienstverleners als sector een systeem zouden moeten ontwikkelen om het beheer van nog geldige certificaten over te nemen, voor het geval dat een certificatiedienstverlener zijn dienstverlening beëindigt. De taskforce beveelt aan om in de toelichting voorbeelden aan te geven op welke wijze een dergelijk systeem kan worden ingericht, waarbij de taskforce tevens enkele mogelijke voorbeelden aanhaalt.

Mede naar aanleiding van dit advies zijn de onderdelen met betrekking tot de continuïteit van de dienstverlening geformuleerd.

Het Electronic Commerce Platform Nederland (ECP.NL) stelt de volgende zaken aan de orde:

• De certificatiedienstverlener is ingevolge artikel 196b van afdeling 4A van Titel 3 van Boek 6 van het Burgerlijk Wetboek aansprakelijk voor de schade die een persoon lijdt indien deze persoon handelt in redelijk vertrouwen op de juistheid van de gegevens van het door hem afgegeven gekwalificeerde certificaat, tenzij hij bewijst dat hij niet onzorgvuldig heeft gehandeld. Gegeven deze aansprakelijkheidspositie van de certificatiedienstverlener en de bewijslast is het wenselijk om meer duidelijkheid te verkrijgen over wat nodig is om te bewijzen dat een certificatiedienstverlener niet onzorgvuldig heeft gehandeld. Men beveelt aan om in het besluit meer aandacht te schenken aan de situaties rondom intrekking van certificaten en disputen over vermeende intrekking. In verband met deze opmerking is in artikel 2, eerste lid, onderdeel r, subonderdeel 3°, opgenomen dat de certificatiedienstverlener de gebruiker onder meer op de hoogte moet stellen van de procedures voor intrekking van een gekwalificeerd certificaat. Voor het overige handelt de certificatiedienstverlener in beginsel niet onzorgvuldig als hij gebruik maakt van betrouwbare processen en middelen en handelt overeenkomstig betrouwbare procedures.

• ECP.NL beveelt aan meer duidelijkheid te verschaffen over het antwoord op de vraag of gekwalificeerde certificaten nu wel of niet onafhankelijk kunnen worden uitgegeven van de veilige middelen voor het genereren van een elektronische handtekening en wat in dat geval de aansprakelijkheidspositie van de certificatiedienstverlener is. Op basis van de gehanteerde definities in de Telecommunicatiewet is duidelijk dat gekwalificeerde certificaten onafhankelijk van veilige middelen kunnen worden uitgegeven. De aansprakelijkheidspositie van de certificatiedienstverlener wordt ook in dit geval beheerst door het reeds aangehaalde artikel 196b van Boek 6 van het Burgerlijk Wetboek, waarin geen onderscheid wordt gemaakt naar situaties waarin de certificatiedienstverlener het veilige middel wel en waarin hij die niet verstrekt. Dit artikel is bovendien goed verenigbaar met situaties waarin het veilige middel door een andere partij dan de certificatiedienstverlener wordt aangeleverd. Wel moet de certificatiedienstverlener in alle gevallen zich ervan vergewissen dat de persoon voor wie het certificaat wordt aangevraagd beschikt over de corresponderende gegevens voor het aanmaken van de elektronische

handtekening (in de huidige technologie de private sleutel), ongeacht of de certificatiedienstverlener deze gegevens of het veilige middel waarmee deze gegevens worden gebruikt zelf verstrekt. Deze taak is in de praktijk eenvoudiger uit te voeren als de certificatiedienstverlener al deze gegevens zelf aanmaakt en op een veilig middel verstrekt.

1.5. Administratieve lasten

Elke lidstaat dient volgens artikel 3, derde lid, van de richtlijn te zorgen voor een passend systeem van toezicht op de op zijn grondgebied gevestigde certificatiedienstverleners die gekwalificeerde certificaten aan het publiek afgeven. Dit passend systeem van toezicht is opgenomen in de Telecommunicatiewet, en steunt op een informatieverplichting van de certificatiedienstverleners die gekwalificeerde certificaten aan het publiek aanbieden. De informatieverplichting bestaat er uit dat aan de toezichthouder OPTA eenmalig, bij registratie, een informatiedossier wordt overgelegd waaruit blijkt dat de certificatiedienstverlener voldoet aan de eisen, gesteld in de artikelen 2 en 3 van dit besluit. Voorts wordt jaarlijks door de toezichthouder gevraagd om wijzigingen van de gegevens in het informatiedossier aan te geven en enkele voorhanden documenten, zoals een overzicht van de algemene voorwaarden, toe te sturen. Overigens dient opgemerkt te worden dat certificatiedienstverleners, die een verklaring van overeenstemming overleggen zoals bedoeld in artikel 2.1, vierde lid, van de Telecommunicatiewet, geen volledig informatiedossier hoeven te overhandigen, maar kunnen volstaan met de verklaring van een door de minister van Economische Zaken, op grond van artikel 18.16 van de Telecommunicatiewet, aangewezen certificatieorganisatie waaruit blijkt dat zij aan de eisen voldoen. Het aantal certificatiedienstverleners in Nederland op wie de informatieverplichting de komende jaren komt te rusten wordt geschat op drie tot tien.

Op basis van de verkregen informatie beoordeelt de toezichthouder of de certificatiedienstverlener blijft voldoen aan de wettelijke eisen. Voor dit stelsel van toezicht is gekozen, omdat het aansluit bij het bestaande registratiemodel voor aanbieders van openbare telecommunicatiediensten en -netwerken, het de toetreding tot de markt voor certificatiediensten niet afhankelijk maakt van voorafgaande vergunningverlening, en het relatief weinig administratieve procedures of kosten met zich meebrengt. De hier gekozen vorm van overheidstoezicht is vrij licht van opzet, mede omdat een belangrijke rol wordt voorzien voor privaatrechtelijke borging van de wettelijke normen door vrijwillige accreditatiemechanismen. In de memorie van toelichting op artikel 18.16 van de Telecommunicatiewet wordt hierop ingegaan (Kamerstukken II, 27 743, nr. 3, p. 23). Enkele andere lidstaten zien duidelijk een sterkere rol voor hun overheidstoezichthouder in de zin dat deze in een vroegtijdig stadium bij een certificatiedienstverlener langsgaat om ter plekke te controleren of aan alle eisen wordt voldaan. Gelet op de belasting die dit voor een certificatiedienstverlener meebrengt, worden de administratieve lasten van een dergelijke invulling beduidend hoger ingeschat.

De kosten die samenhangen met het samenstellen van het (eenmalige) informatiedossier worden per certificatiedienstverlener geschat op ten hoogste € 5000. Dit is gebaseerd op het uitgangspunt dat certificatiedienstverleners de informatie reeds binnen de organisatie voorhanden hebben, inherent aan het feit dat zij deze dienst verlenen. De administratieve lasten worden gevormd door de kosten van de inzet van personeel om deze reeds aanwezige informatie samen te voegen en te bewerken tot het door de wetgever gewenste dossier. De jaarlijks terugkerende kosten bestaan uit het nalopen en doorgeven van eventuele wijzigingen in het informatiedossier en toezending van standaard documenten. Deze structurele kosten liggen in de orde van grootte van enkele honderden euro's. Indien tien certificatiedienstverleners zouden zijn geregistreerd

bedragen de met de registratie samenhangende administratieve lasten in totaal omstreeks € 55 000.

Naast de hiervoor beschreven informatieverwerking bij registratie is de toezichthouder, OPTA, bevoegd om ter plekke te onderzoeken of een certificatiedienstverlener aan de wettelijke eisen voldoet. Deze bevoegdheid zal in de praktijk beperkt blijven tot die gevallen waar een redelijk vermoeden bestaat dat de certificatiedienstverlener niet aan de eisen voldoet.

Onder administratieve lasten vallen ook de kosten van informatieverplichtingen aan derden indien zij worden voorgeschreven in wet- of regelgeving. In onderhavig besluit zijn een aantal door de richtlijn voorgeschreven verplichtingen overgenomen in artikel 2, eerste lid, onderdeel l en q. Zo wordt in artikel 2, eerste lid, onderdeel l, een publicatieverplichting opgelegd omtrent de status van afgegeven gekwalificeerde certificaten waarvan de kosten als administratieve lasten kunnen worden aangemerkt. Deze eis is echter niet zozeer opgenomen om de publicatieverplichting op zich. Immers, onderdeel van het verlenen van certificatiediensten is dat derden die op een elektronische handtekening vertrouwen, de geldigheid hiervan moeten kunnen verifiëren aan de hand van gekwalificeerde certificaten. Deze certificaten moeten dus benaderbaar zijn. Deze eis is juist opgenomen vanwege kwaliteitsaspecten die aan de publicatie worden gesteld, zoals actualiteit en betrouwbaarheid, en met de eis dat publicatie alleen maar is toegestaan voor zover de ondertekenaar daarvoor toestemming heeft gegeven.

In artikel 2, eerste lid, onderdeel r, is de verplichting opgenomen dat de certificatiedienstverlener degene met wie een certificatiedienstverlener een contractuele relatie aangaat, en desgevraagd derden die op een door de certificatiedienstverlener afgegeven certificaat vertrouwen, informeert over voorwaarden die aan het gebruik van certificaten zijn gesteld en enkele gehanteerde procedures die hiermee samenhangen. Dit betreft het versturen van standaard aanwezige documenten. De kosten die met deze verplichting zijn gemoeid, bestaan (bij het op papier versturen) uit het uitdraaien van desbetreffende informatie en het versturen per post. Afhankelijk van het aantal klanten dat men heeft zal dit op enkele duizenden mailings per jaar neerkomen.

Het totaalbedrag van de administratieve lasten op grond van deze verplichtingen is bij tien geregistreerde certificatiedienstverleners ongeveer € 10 000.

Het ontwerp-besluit is voorgelegd aan het Adviescollege toetsing administratieve lasten. Bij brief van 4 juli 2002 heeft dit College medegedeeld dat het onderhavige besluit niet geselecteerd is voor een Actaltoets op de gevolgen voor de administratieve lasten voor het bedrijfsleven.

1.6. Notificatie

Bij het formuleren van de eisen in de artikelen 2, 3 en 5 van het onderhavige besluit is uitgegaan van de eisen genoemd in de bijlagen 1, 2 en 3 van de richtlijn. Zoals in paragraaf 1.3.1 is uiteengezet, kan echter niet voor alle opgenomen eisen gezegd worden dat de certificatiedienstverlener weet waaraan hij moet voldoen en dat de toezichthouder weet aan de hand waarvan hij toezicht moet houden. Daarom is in het onderhavige besluit aan sommige eisen, ter verduidelijking, een uitwerking gegeven, waarbij, waar mogelijk, rekening is gehouden met de binnen ETSI en CEN ontwikkelde standaarden voor certificatiedienstverlening. Daarnaast zijn op enkele punten aanvullende eisen geformuleerd. Het betreft met name de continuïteit van de dienstverlening en het bestaan van een beschreven klachten- en geschillenafhandelingsprocedure. In de paragrafen 1.3.2. en 1.3.3. is op deze aspecten ingegaan.

In verband met de opneming van voorschriften in het besluit die niet uitdrukkelijk in de richtlijn zijn genoemd, maar de gevolgen ervan

reguleren, en die in overeenstemming zijn met Europese ontwikkelingen is het ontwerp-besluit op 16 oktober 2002 gemeld aan de Commissie van de Europese Gemeenschappen (notificatienummer 2002/0397/NL) ter voldoening aan artikel 8, eerste lid, van richtlijn 98/34/EG van het Europees Parlement en de Raad van de Europese Unie van 22 juni 1998 betreffende een informatieprocedure op het gebied van normen en technische voorschriften en regels betreffende diensten van de informatiemaatschappij (PbEG L 204), zoals gewijzigd bij richtlijn nr. 98/48/EG van 20 juli 1998 (PbEG L 217). Tijdens de zogenoemde stand-still-periode, die afliep op 17 januari 2003, zijn geen opmerkingen van de zijde van de Europese Commissie of van de andere lidstaten ontvangen.

II ARTIKELEN

Artikel 1

Onderdeel b

Certificatiediensten zijn diensten die door certificatiedienstverleners, zoals gedefinieerd in artikel 1.1, onderdeel ee, van de Telecommunicatiewet worden verricht. In die wet is geen beperking gegeven aan dit begrip. Een omschrijving ervan is echter wenselijk, omdat zowel bij de certificatiedienstverleners als bij de toezichthouders daarover hetzelfde beeld moet bestaan. Onder certificatiediensten wordt niet uitsluitend verstaan het afgeven van gekwalificeerde certificaten, en het registratieproces dat daaraan vooraf gaat. Het omvat andere diensten die in verband staan met elektronische handtekeningen zoals het beheer van afgegeven certificaten en het genereren, opslaan, verstrekken of het vernietigen van cryptografisch sleutelmateriaal (sleutelbeheer).

Sleutelbeheerdiensten vormen een aparte groep van certificatiediensten. De specifieke betekenis van deze term rechtvaardigt een afzonderlijke definitie.

Artikel 2 algemeen

Artikel 2 stelt de eisen vast aan welke certificatiedienstverleners moeten voldoen die gekwalificeerde certificaten aan het publiek aanbieden of afgeven en die in Nederland een vestiging hebben. Deze certificatiedienstverleners moeten ingevolge artikel 2.1, derde lid, van de Telecommunicatiewet ook zijn geregistreerd bij de Onafhankelijke Post- en Telecommunicatieautoriteit. Tezamen met deze registratie vormen de eisen van artikel 2 van dit besluit de basis voor het goed en betrouwbaar functioneren van certificatiedienstverleners en de basis voor het gebruik van elektronische handtekeningen die op een gekwalificeerd certificaat zijn gebaseerd.

Voor een toelichting op de relatie tussen registratie, het afgeven van gekwalificeerde certificaten aan het publiek en het voldoen aan de eisen wordt kortheidshalve verwezen naar onderdeel 2.6 van de memorie van toelichting bij de Wet elektronische handtekeningen. De certificatiedienstverlener is op grond van artikel 2.1, derde lid, van de Telecommunicatiewet verplicht reeds bij de aanvraag tot registratie aan te tonen dat hij aan de eisen voldoet.

Niet-geregistreerde certificatiedienstverleners moeten steeds nagaan of de certificaten die zij aanbieden of afgeven aangemerkt moeten worden als gekwalificeerde certificaten en of de klantenkring zodanig van samenstelling is dat de certificaten geacht worden aan het publiek te worden aangeboden of afgegeven. In de memorie van toelichting op de Wet elektronische handtekeningen (kamerstukken II, 2000–2001, 27 743,

nr.3, blz. 19) is beschreven wat verstaan wordt onder de woorden «aan het publiek».

Voor de goede werking van een stelsel waarin elektronische handtekeningen een rol van betekenis spelen, is het van belang dat de certificatiedienstverleners betrouwbaar zijn, hetgeen in onderdeel a van bijlage II bij de richtlijn met zoveel woorden is genoemd. Dit onderdeel moet als de vastlegging van een algemeen betrouwbaarheidsbeginsel worden beschouwd, waarvan aspecten in de daarna komende eisen worden uiteengezet. Het gaat om de betrouwbaarheid van de certificatiedienstverlener als organisatie (artikel 2, eerste lid, onderdelen f, s, tweede en derde lid) en om de betrouwbaarheid van de door de certificatiedienstverlener gehanteerde diensten, middelen en procedures (artikel 2, eerste lid, onderdelen a, b, c, d, g, h, i, j, k, l, m, n, en r. Betrouwbaarheid betekent ook dat de gebruiker op een minimumniveau van continuïteit kan rekenen.

De richtlijn regelt continuïteitsaspecten niet met zoveel woorden, maar stelt wel dat certificatiedienstverleners voldoende financiële middelen ter beschikking moeten hebben om in overeenstemming met de wet te kunnen functioneren (Bijlage II, onderdeel h, en artikel 2, eerste lid, onderdeel e). Hier wordt de schade onderkend die kan ontstaan bij het niet functioneren overeenkomstig de wettelijke eisen, welke schade eveneens kan ontstaan indien in het geheel geen certificatiediensten meer worden verleend. Die schade kan niet altijd worden gecompenseerd. De aanvullende continuïteitseisen van het besluit (artikel 2, eerste lid, onderdelen o, p en q) zijn er dan ook met name op gericht om maatregelen te laten nemen op het niveau van de certificatiedienstverlener, om het belang te dienen van de gebruiker van elektronische handtekeningen, indien de individuele certificatiedienstverlener zijn dienstverlening beëindigt. Dit komt het vertrouwen in de certificatiedienstverlening als geheel ten goede.

Verder heeft op een aantal plaatsen een nadere concretisering van het bepaalde in de richtlijn plaatsgevonden teneinde meer duidelijkheid te verschaffen. Hierbij is steeds het technologieonafhankelijke karakter van de richtlijn aangehouden.

De volgorde van bijlage II van de richtlijn is niet steeds gevolgd. In het onderhavige besluit zijn zoveel mogelijk de eisen geclusterd, die logischerwijze in het proces van dienstverlening bij elkaar horen.

Artikel 2, eerste lid

Onderdelen a en b

Deze onderdelen vloeien voort uit onderdeel a van bijlage II bij de richtlijn. Dat een middel een betrouwbaar middel is betekent dat het betrouwbaar is voor zover de stand der techniek en andere inzichten dat ondersteunen. De betrouwbaarheid van middelen en procedures moet voortdurend worden beoordeeld.

De betrouwbaarheid van procedures en processen, onder meer op het gebied van beheer en administratie als bedoeld in het laatste gedeelte van onderdeel e van bijlage II bij de richtlijn, kan het beste op peil worden gehouden door te werken overeenkomstig een beschreven kwaliteitssysteem, dat wordt aangepast aan de laatste ontwikkelingen. Dit maakt daarnaast de beoordeling van de betrouwbaarheid door de toezichthouder eenvoudiger.

Onderdeel c

Dit onderdeel is vrijwel geheel overgenomen uit de bijlage II, onderdeel f, bij de richtlijn. In de formulering is expliciet een verwijzing toegevoegd naar de stand der techniek. Indien het zeer eenvoudig is (geworden) om een bestaande beveiliging te omzeilen of te doorbreken, kan er niet meer

van worden gesproken dat de producten «beschermd zijn tegen wijziging», zoals de richtlijntekst zegt, of dat de «cryptografische veiligheid is gewaarborgd», indien de gebruikte versleutelingen eenvoudig kunnen worden ontcijferd. In die gevallen zullen de beveiligingen moeten worden verbeterd. Tevens is de eis met betrekking tot beveiliging breder genomen dan in de richtlijn, waar uitsluitend bescherming tegen wijziging is vereist. De toegepaste systemen moeten ook bescherming bieden tegen inbraak op computersystemen zonder te wijzigen (computervredebreuk).

De eis dat de veiligheid van de processen door de beveiligde systemen en procedures wordt gegarandeerd, is in beginsel een resultaatsverplichting. De toezichthouder kan, bij gebleken schending van de veiligheid, op grond van artikel 2.2 van de Telecomunicatiewet de registratie van de betrokken certificatiedienstverlener beëindigen. Indien de certificatiedienstverlener gebruik maakte van technische beveiligingen die aan de stand der techniek voldoen, en procedures heeft gehanteerd die onder de meeste omstandigheden een voldoende niveau van beveiliging geven, zal er aanleiding kunnen zijn artikel 2.2, derde lid, onderdeel f van de Telecommunicatiewet toe te passen en de certificatiedienstverlener in de gelegenheid te stellen om aanvullende maatregelen te nemen om herhaling te voorkomen.

Onderdeel d

Dit onderdeel is gebaseerd op onderdeel g van bijlage II bij de richtlijn. Enerzijds dienen zodanige maatregelen te worden getroffen dat uitgegeven gekwalificeerde certificaten niet kunnen worden vervalst. Dit betreft met name het niet kunnen wijzigen van de gegevens op het certificaat zonder dat deze wijziging kenbaar wordt aan de gebruiker van het certificaat. Anderzijds betreft het maatregelen tegen uitgifte van illegale certificaten. Hier gaat het met name om maatregelen die garanderen dat het ondertekenen en uitgeven van gekwalificeerde certificaten door de certificatiedienstverlener integer, zorgvuldig en met bescherming van de belangen van de certificaathouders en de certificatiedienstverlener geschiedt.

Onderdeel e

Dit onderdeel is gebaseerd op onderdeel h van bijlage II bij de richtlijn. In dit onderdeel wordt specifiek vereist dat de certificatiedienstverlener zodanige voorzieningen treft dat eventuele aansprakelijkheidsclaims het voortbestaan van de certificatiedienstverlener niet bedreigen. Voorts slaat dit onderdeel op het treffen van voorzieningen opdat gewaarborgd wordt dat bij beëindiging van de dienstverlening het gestelde in de onderdelen o, p en q daadwerkelijk wordt nagekomen. Aan de vorm van deze voorzieningen worden geen eisen gesteld. Naast financiële middelen zou kunnen worden gedacht aan het sluiten van verzekeringen of het instellen van een waarborgfonds.

Onderdeel f

Dit onderdeel is gebaseerd op onderdeel e (eerste gedeelte) van bijlage II bij de richtlijn.

De certificatiedienstverlener moet aantonen dat hij personeel in dienst heeft dat deskundig is om de aangeboden diensten te kunnen uitvoeren. Deze deskundigheid betreft met name het beheren van gekwalificeerde certificaten en de gegevens die daarvoor worden verzameld en verwerkt, en het genereren van elektronische handtekeningen met daarvoor geschikte technologie, die beveiligd is tegen inbreuken.

Onderdeel g

Dit onderdeel is gebaseerd op onderdeel d van bijlage II bij de richtlijn. De ondertekenaar moet met behulp van het (meestal met het ondertekende bericht meegestuurde) gekwalificeerde certificaat geïdentificeerd kunnen worden door de ontvanger van het ondertekende elektronisch bericht. Daarom moet het desbetreffende gekwalificeerde certificaat dusdanige gegevens bevatten dat de ondertekenaar daardoor binnen het domein van de certificatiedienstverlener uniek is geïdentificeerd. In de praktijk controleert de ontvanger de identiteit aan de hand van het gekwalificeerde certificaat van de ondertekenaar. Dat certificaat zal hiervoor een naam of een combinatie van naam en nummer bevatten die de ondertekenaar binnen het domein van de certificatiedienstverlener uniek identificeren. Ook indien er gebruik wordt gemaakt van een pseudoniem, hetgeen mogelijk is ingevolge artikel 3, onderdeel c, van dit besluit, zullen de gegevens in het certificaat uniek gekoppeld zijn aan één ondertekenaar in het domein van de certificatiedienstverlener.

Ingevolge artikel 18.15, derde lid, van de Telecommunicatiewet verifieert de certificatiedienstverlener de identiteit van de aanvrager van een gekwalificeerd certificaat. Bij eerste uitgifte aan een aanvrager moet worden gedacht aan een situatie waarbij de aanvrager fysiek verschijnt voor een medewerker van de certificatiedienstverlener en dan een identiteitbewijs overlegt. Door de verwijzing in de Telecommunicatiewet naar artikel 1 van de Wet op de identificatieplicht is bepaald welke documenten de aanvrager als bewijs kan overleggen. De desbetreffende medewerker van de certificatiedienstverlener dient dan te verifiëren dat het een geldig identiteitsbewijs betreft en dat de gegevens overeenstemmen met de fysiek aanwezige aanvrager. Hiertoe zal normaliter een visuele controle van het identiteitsbewijs volstaan. Zoals gesteld is het de verantwoordelijkheid van de certificatiedienstverlener de identiteit te verifiëren aan de hand van een geldig identiteitsbewijs. Ter extra zekerstelling, indien gerede twijfel bestaat over de geldigheid van een identiteitsbewijs, kan de certificatiedienstverlener daarbij gebruik maken van een controle bij het Verificatieregister. Het Verificatieregister is een deelregister van het Basisregister Reisdocumenten. De Minister van Binnenlandse Zaken en Koninkrijksrelaties is verantwoordelijk voor de verwerking van gegevens in dit register. De Minister van Binnenlandse Zaken en Koninkrijksrelaties kan ingevolge artikel 4a, zevende lid, van de Paspoortwet op verzoek organisaties autoriseren die een gerechtvaardigd belang hebben om het register te raadplegen om de geldigheid van een reisdocument te toetsen.

In het geval van verlengingen (van de dienstverlening door het afgeven van een nieuw certificaat) is het mogelijk het eerder afgegeven gekwalificeerde certificaat te gebruiken als identificatiedocument, zodat de identificatie op afstand kan plaatsvinden. Dit kan uiteraard alleen als het eerder afgegeven certificaat nog geldig is. Deze handelwijze voldoet aan de formulering «aan de hand van de .. aangewezen geldige documenten» van artikel 18.15, derde lid, van de Telecommunicatiewet, mits de eerste uitgifte plaats vindt aan de hand van een daadwerkelijke controle van die documenten en de in persoon ontvangen aanvrager.

De in dit onderdeel genoemde andere passende geschikte middelen hebben betrekking op de verificatie van de attributen.

Voor de (verplichte) controles op de juistheid van specifieke attributen kunnen in het algemeen geen concrete eisen worden gesteld, omdat naar verwachting deze controles per attribuut specifieke documenten en wellicht ook specifieke controlemethoden zullen vergen. Het is te verwachten dat er op dit punt per specifiek attribuut aanvullende eisen zullen worden afgesproken, die zo nodig in wettelijke voorschriften worden neergelegd.

Onderdeel h

Dit onderdeel is gebaseerd op onderdeel c van bijlage II bij de richtlijn, welk onderdeel nader in de tijdseenheid is gepreciseerd.

De certificatiedienstverlener moet de datum en het tijdstip van afgifte of intrekking van een gekwalificeerd certificaat ten minste vastleggen met een nauwkeurigheid van één minuut. Binnen het kader van de huidige en te verwachten toepassingen van elektronische handtekeningen waarvoor een gekwalificeerd certificaat wordt afgegeven wordt een nauwkeurigheid van een minuut voldoende geacht om de geldigheid van een certificaat op een bepaald tijdstip te verifiëren.

Onderdeel i

Dit onderdeel is gebaseerd op onderdeel i van bijlage II bij de richtlijn.

De richtlijn laat het aan de lidstaten over om tot een invulling te komen van de minimum bewaartermijn van alle gegevens die de certificatie bewijzen. Dit is een belangrijke bepaling omdat deze gegevens een essentiële rol als bewijsmateriaal kunnen vervullen in het geval een geschil ontstaat over een gerelateerde (geavanceerde) elektronische handtekening. Dit kan bijvoorbeeld een geschil zijn over de identiteit van de ondertekenaar of over de vraag of de handtekening wel correct is gebruikt in relatie tot de beperkingen die in het certificaat zijn aangegeven. De termijn waarbinnen zo'n geschil kan plaatsvinden is afhankelijk van de rechtshandeling waarin de elektronische handtekening een rol heeft gespeeld.

De certificatiedienstverlener moet de gegevens omtrent het gekwalificeerde certificaat en de uitgifte ervan bewaren op zodanige wijze dat de rechthebbenden op verzoek toegang tot die gegevens kunnen krijgen. De gegevens die een certificatiedienstverlener moet bewaren zijn de gegevens over de identiteit, zoals de naam en het adres van de ondertekenaar, en de wijze van identificatie van de ondertekenaar, zoals een paspoortnummer, een kopie uit het document waarmee de identiteit is aangetoond, alsmede de gegevens over het gekwalificeerde certificaat, zoals de precieze begin- en einddatum van de periode waarin het certificaat geldig was, en welke beperkingen golden voor de elektronische handtekening die op het certificaat was gebaseerd. Tevens dient de certificatiedienstverlener gegevens omtrent intrekking van dat certificaat bij te houden.

De bewaartermijn moet niet te kort worden genomen, omdat anders een beroep op de certificatie in een civielrechtelijke procedure gefrustreerd zou worden. Een te lange periode daarentegen zal onnodige kosten met zich mee brengen, en in strijd zijn met het uitgangspunt dat (persoons)gegevens niet langer worden opgeslagen of verwerkt dan voor het doel van de opslag en het verwerken noodzakelijk is.

De keuze van de minimum bewaartermijn wordt in de verschillende lidstaten in belangrijke mate bepaald door het soort gebruik dat men voorziet voor de gekwalificeerde certificaten en de regels die in de verschillende lidstaten met betrekking hiertoe bestaan. De invullingen zijn dus op meer dan één manier door de nationale context bepaald, en het blijkt dan ook dat de invullingen sterk verschillen per lidstaat, vanaf enkele jaren tot 30 jaar of meer. Waar lidstaten toepassingen zoals ten behoeve van het notariaat in gedachte hebben, wordt vaak gekozen voor zeer lange bewaartermijnen, terwijl toepassingen zoals ten behoeve van elektronische handel eerder zullen resulteren in de termijnen die overeenstemmen met de bewaartermijn die voor bedrijfsdocumenten aan de orde zijn.

In Nederland is, ter bepaling van de minimum bewaartermijn, een bedrijfsmatige toepassing van geavanceerde elektronische handtekeningen voor ogen gehouden. Zo wordt, ook in Europees verband, de

toepassing van geavanceerde elektronische handtekeningen voorzien voor elektronische facturen[1]. Dit heeft geleid tot een keuze voor de minimum bewaartermijn van zeven jaar, een termijn die in overeenstemming is met de termijn die geldt voor het bewaren van bedrijfsgegevens ingevolge artikel 24 van Boek 2 van het Burgerlijk Wetboek.

Bij onderdeel g van deze toelichting is beschreven dat voor een verlenging van de dienstverlening door het afgeven van een nieuw certificaat het mogelijk is het eerder afgegeven gekwalificeerde certificaat te gebruiken als identificatiedocument, zodat de identificatie als het ware «op afstand» kan plaatsvinden. In dit specifieke geval geldt de minimum bewaartermijn van 7 jaar vanaf de datum waarop de geldigheid van dit nieuwe certificaat is verlopen.

Voor sommige toepassingen zal de behoefte bestaan, bijvoorbeeld in verband met wettelijke vereisten, aan langere bewaartermijnen. Hier is ruimte gelaten aan de marktpartijen om langere bewaartermijnen overeen te komen.

Voor zover elektronische handtekeningen of gekwalificeerde certificaten zijn aan te merken als archiefbescheiden in de zin van de Archiefwet 1995, heeft het betrokken overheidsorgaan de verplichting om deze te bewaren, tenzij zij worden geplaatst op een selectielijst om te worden vernietigd. In beide gevallen is het niet nodig om de certificatiedienstverlener een wettelijke taak te geven bij de opslag van archiefbescheiden. De Archiefwet 1995 bevat al regels voor het geval archiefbescheiden zich niet bevinden bij een overheidsorgaan. Een certificatiedienstverlener kan niet als overheidsorgaan worden aangemerkt, tenzij zijn werkzaamheden rechtstreeks onder verantwoordelijkheid van een overheidsorgaan zouden vallen.

Het overheidsorgaan dat gebruikt maakt van certificatiediensten beschikt gewoonlijk over de elektronische handtekening en de sleutel die is gebruikt, en vaak ook over het gekwalificeerde certificaat, zodat het de bewaartermijn van deze bescheiden zelf kan vaststellen, alsmede de wijze van bewaren zelf kan regelen, zulks overeenkomstig de Regeling geordende en toegankelijke staat archiefbescheiden.

De gegevens over de verificatie van de identiteit en van de attributen van de certificaathouder en de historische gegevens over de afgifte en intrekking van het gekwalificeerde certificaat, die door de certificatiedienstverlener worden opgemaakt en bewaard, zijn in beginsel niet aan te merken als archiefbescheiden in de zin van de Archiefwet 1995. Indien deze gegevens worden gegenereerd door of uitgewisseld met een overheidsorgaan vallen zij in beginsel wel onder de Archiefwet 1995.

Onderdeel j

Dit onderdeel vloeit voort uit onderdeel l van bijlage II bij de richtlijn.

Onderdeel k

Dit onderdeel is gebaseerd op onderdeel b van bijlage II van de richtlijn, met betrekking tot de prompte en veilige intrekking.

Bij de intrekking van gekwalificeerde certificaten is de betrouwbaarheid van het verzoek tot intrekking en de termijn waarin een betrouwbaar verzoek tot publicatie van de intrekking van het gekwalificeerde certificaat moet leiden een potentiële bron van onenigheid. De richtlijn spreekt van een «prompte» en veilige intrekking. In de praktijk komt het er op neer dat de certificaathouder erop kan vertrouwen dat een door hem gegeven opdracht tot intrekking van het certificaat door de certificatiedienstverlener binnen de afgesproken termijn wordt uitgevoerd en dat de ingetrokken status van het gekwalificeerde certificaat direct daarna bekend wordt gemaakt aan de personen die de status van het certificaat opvragen.

[1] Richtlijn 2001/115/EG van het Europees Parlement en de Raad van 20 december 2001 betreffende vereenvoudiging, modernisering en harmonisering van de ter zake van de facturering geldende voorwaarden op het gebied van de belasting over de toegevoegde waarde (PbEG L15/24).

Daarbij is er voor gekozen om in dit besluit geen concrete termijn te noemen die voor alle certificatiedienstverleners geldt, maar slechts te eisen dat de certificatiedienstverlener de termijn waarbinnen hij deze diensten verricht bekendmaakt. Bij ministeriële regeling zal echter wel een maximum termijn worden gesteld waarbinnen, na ontvangst van het intrekkingverzoek, een certificaat moet zijn ingetrokken. Deze termijn zal in overeenstemming zijn met de termijn die in internationale afspraken wordt vastgelegd.

Onderdeel l

Dit onderdeel is gebaseerd op onderdeel b van bijlage II bij de richtlijn, voor zover betrekking hebbend op de publicatie van afgegeven gekwalificeerde certificaten en de status, waaronder wordt verstaan de geldigheid, van deze certificaten.

De partij die een document of bericht ontvangt, voorzien van een elektronische handtekening, zal deze handtekening willen controleren teneinde te kunnen vertrouwen op deze handtekening. Veelal wordt hiertoe het gekwalificeerde certificaat meegestuurd, zodat het mogelijk is de identiteit van de ondertekenaar te verifiëren. Soms zal echter slechts een verwijzing naar een gekwalificeerd certificaat worden meegestuurd en dient het eigenlijke certificaat in een voor het publiek toegankelijk bestand te worden opgezocht. In dit laatste geval is het noodzakelijk dat een gekwalificeerd certificaat in een voor het publiek toegankelijk bestand is opgeslagen. Tevens zal de ontvanger van de handtekening willen weten of het certificaat op het moment van ondertekening niet is ingetrokken.

De term directorydienst, die in de richtlijn wordt gebruikt, is in dit besluit niet gehanteerd om meer vrijheid te creëren voor de certificatiedienstverlener waar het de (technische) uitvoering van de publicatieverplichting betreft.

Onderdeel m

De gegevens voor het aanmaken van de elektronische handtekeningen mogen ingevolge bijlage II, onderdeel j van de richtlijn, ook als zij worden uitgegeven door de certificatiedienstverlener, niet door die certificatiedienstverlener worden behouden en niet gekopieerd.

In het geval van de elektronische handtekening is het nodig dat een zeer grote zekerheid wordt bereikt dat niemand anders dan de bedoelde ondertekenaar de elektronische handtekening kan aanmaken. Door het sleutelmateriaal niet te bewaren of te kopiëren na het aan de bedoelde ondertekenaar te hebben uitgegeven, wordt de hoogst mogelijke zekerheid bereikt voor die gevallen waarin de bedoelde ondertekenaar het sleutelmateriaal niet zelf aanmaakt.

Onderdeel n

Verwezen wordt naar hetgeen in paragraaf 1.3.3 van het algemene gedeelte van deze toelichting over de verplichting tot het hebben van een beschreven geschillenbeslechtings- en klachtenafhandelingsprocedure is gezegd.

Onderdelen o, p en q

Deze onderdelen hebben betrekking op de maatregelen die de certificatiedienstverlener moet nemen bij beëindiging van de dienstverlening.

Onderdeel o

Om zeker te stellen dat het niet mogelijk is dat er, na de beëindiging van de dienstverlening, opnieuw gekwalificeerde certificaten kunnen worden uitgegeven onder de naam van de certificatiedienstverlener waarvan de dienstverlening is beëindigd, moeten de hiervoor benodigde gegevens voor het aanmaken van de elektronische handtekening (sleutelmateriaal) waarmee de certificatiedienstverlener de uitgegeven gekwalificeerde certificaten tekent, ten tijde van de beëindiging worden vernietigd.

Het is gebruikelijk dat de certificatiedienstverlener voor het intrekken van certificaten hetzelfde sleutelmateriaal hanteert als voor het aanmaken van de elektronische handtekening waarmee hij de uitgegeven gekwalificeerde certificaten tekent.

Om niet in conflict te komen met de publicatieverplichting van onderdeel l en de behoefte om intrekkingsdiensten te blijven leveren na beëindiging van de reguliere dienstverlening, moet het moment van vernietiging van het sleutelmateriaal in dergelijke gevallen worden uitgesteld tot na het afronden van die intrekkingsdienst.

Onderdeel p

Dit onderdeel regelt de wijze waarop duidelijkheid blijft bestaan omtrent de status van uitgegeven gekwalificeerde certificaten, en dus de geldigheid van elektronische handtekeningen, indien een certificatiedienstverlener zijn dienstverlening beëindigt.

Hoofdregel is dat de certificatiedienstverlener ervoor zorgt dat, indien hij zijn eigen dienstverlening beëindigt, de gekwalificeerde certificaten die hij heeft afgegeven worden overgenomen en beheerd door een andere geregistreerde certificatiedienstverlener. Deze optie heeft de voorkeur omdat dit de continuïteit van het gebruik van de handtekening het beste garandeert. Indien het maken van afspraken over overneming niet mogelijk is of de nakoming van deze afspraken niet kan worden gewaarborgd, is het belangrijk dat de certificatiedienstverlener geen onduidelijkheid laat bestaan over de status van de gekwalificeerde certificaten en daarmee over de bruikbaarheid van de elektronische handtekeningen die daarop zijn gebaseerd. Daartoe dient hij alle nog geldige gekwalificeerde certificaten in te trekken. Hij moet dan nog wel maatregelen nemen om te voldoen aan de onderdelen i, j en q.

Onderdeel q

Om te voorkomen dat onduidelijkheid bestaat over de geldigheid van in omloop zijnde handtekeningen, is het gestelde in onderdeel l, dat de status van de gekwalificeerde certificaten nog tot zes maanden na de datum van intrekking van een certificaat opvraagbaar moet zijn, eveneens van belang als de dienstverlening is beëindigd.

Onderdeel r

Dit onderdeel is gebaseerd op de algemene informatieverplichting van onderdeel k van bijlage II bij de richtlijn.

De certificatiedienstverlener moet de aanvrager van de elektronische handtekening uit eigen beweging op de hoogte stellen van de in dit onderdeel genoemde voorwaarden. Aangezien het om de exacte voorwaarden gaat, houdt dit een verplichting in om eventuele wijzigingen in eerder bekendgemaakte voorwaarden uit eigen beweging aan de persoon aan wie een gekwalificeerd certificaat ter ondersteuning van zijn elektronische handtekening is afgegeven, en desgevraagd aan derden die op het gekwalificeerd certificaat vertrouwen, door te geven. Voor zover het om algemene voorwaarden gaat is de regeling die is opgenomen in

Boek 6, titel 5, afdeling 3 (artikelen 231 en volgende) van het Burgerlijk Wetboek van toepassing.

Onderdeel s, en het tweede en derde lid

Dit onderdeel is gebaseerd op onderdeel a van bijlage II bij de richtlijn. De certificatiedienstverlener identificeert binnen zijn organisatie de functies waar er sprake is van de verwerking van vertrouwelijke en gevoelige gegevens, bijvoorbeeld als onderdeel van de opstelling van het beveiligingsplan. Dat de bestuurders van de certificatiedienstverlener, en de medewerkers die de hiervoor bedoelde functies bekleden, niet in de afgelopen vier jaren zijn veroordeeld in verband met een misdrijf dat de vertrouwelijkheid en de betrouwbaarheid van de dienstverlening schade zou kunnen berokkenen, onder meer omdat deze medewerkers dan niet kwetsbaar zijn voor aantijgingen met betrekking tot een veroordeling, kan het publiek ervan overtuigen dat de certificatiedienstverlener serieus met de belangen van het publiek omgaat. De periode van vier jaren komt overeen met de huidige bewaartermijn voor deze gegevens.

In de praktische uitwerking kan er gewerkt worden met verklaringen omtrent gedrag als bedoeld in de Wet op de justitiële informatie en de verklaringen omtrent het gedrag van de medewerkers die deze functies uitoefenen.

Het tweede en derde lid bevatten nadere bepalingen over voor de toepassing van onderdeel s relevante veroordelingen

Artikel 3

Gekwalificeerde certificaten die als zodanig aan het publiek worden aangeboden of afgegeven moeten de gegevens bevatten die in dit artikel zijn opgesomd. De onderdelen d, i en j betreffen informatie die alleen moet worden opgenomen indien deze van toepassing is. In de laatste twee gevallen betekent het niet opnemen van deze velden ook dat de desbetreffende beperkingen in waarde of gebruik niet van toepassing zijn.

Uit het gekwalificeerde certificaat moet blijken dat het als zodanig is afgegeven (onderdeel a). Duidelijk moet zijn welke certificatiedienstverlener het gekwalificeerde certificaat heeft afgegeven (onderdeel b). De naam van de certificatiedienstverlener is de naam waaronder de certificatiedienstverlener in de markt optreedt en is geregistreerd bij de toezichthouder. Het betreft de certificatiedienstverlener die verantwoordelijk is voor het geheel van de dienstverlening. Het certificaat moet de naam van degene die het bericht elektronisch gaat ondertekenen vermelden of een als zodanig geïdentificeerd pseudoniem. Aangezien de aanvrager zich moet identificeren, moet bij de certificatiedienstverlener bekend zijn of een pseudoniem bij een ondertekenaar hoort, en zo ja welk pseudoniem.

Het gebruik van pseudoniemen leidt er, als uitvloeisel van artikel 2, eerste lid, onderdelen g en i, toe dat de certificatiedienstverlener, die gekwalificeerde certificaten met pseudoniemen uitgeeft, een registratie moet bijhouden met de koppeling tussen pseudoniemen en de bijbehorende werkelijke identiteiten. Bij situaties die zijn beschreven in de algemene voorwaarden of in andere situaties die bij of krachtens de wet zijn omschreven dient de certificatiedienstverlener de werkelijke identiteit prijs te geven die achter het pseudoniem gelegen is.

Uit het gekwalificeerde certificaat kan blijken of het «aan het publiek» is afgegeven (onderdeel i). Indien er geen beperkingen zijn aangebracht in het toepassingsbereik, fungeert het certificaat als een aan het publiek afgegeven certificaat; zie ook de memorie van toelichting op de Wet elektronische handtekeningen (Kamerstukken II, 2000–2001, 27 743, nr. 3, p. 19).

Artikelen 4 en 5

Elektronische handtekeningen worden door de ondertekenaar gegenereerd met behulp van een daartoe geschikt technisch middel. Veilige middelen voor het aanmaken van elektronische handtekeningen zijn technische producten, die aan de eisen van artikel 5 voldoen. De overeenstemmingsbeoordeling met die eisen moet worden opgedragen aan een instituut dat de technische kennis en kunde heeft om deze beoordeling te kunnen uitvoeren, in de praktijk betreft dit specialistisch werk.

Het ligt overigens niet voor de hand om OPTA met een dergelijke taak te belasten. Ten eerste zijn er binnen de Europese Unie voldoende instituten die de overeenstemmingsbeoordeling kunnen en willen uitvoeren. Deze instituten zijn bovendien ingericht om de technische ontwikkelingen te volgen, zodat de overeenstemmingsbeoordeling niet aan de ontwikkeling van nieuwe technieken in de weg staat. Ten tweede heeft de OPTA niet de deskundigheid noch de ambitie om deze technische taak te gaan uitvoeren en zou het opbouwen van de noodzakelijke deskundigheid grote investeringen vergen.

Een instelling die overeenstemmingsbeoordelingen gaat uitvoeren wordt daartoe aangewezen door de Minister, die bij de aanvraag en voorts regelmatig zal (laten) toetsen of de instelling voldoet aan de eisen van artikel 4, die zijn gebaseerd op de beschikking van de Europese Commissie van 6 november 2000 (kennisgeving C(2000) 3179) betreffende de minimumcriteria die lidstaten in acht moeten nemen bij de aanwijzing van instanties (PbEG 2000, L 289), welke beschikking op haar beurt is opgesteld overeenkomstig artikel 3, vierde lid, van de richtlijn.

De aangewezen instelling heeft een belangrijke taak bij de beoordeling van veilige middelen voor zij op de markt worden gebracht. Zij heeft geen bevoegdheid om te onderzoeken of de veilige middelen die reeds als zodanig op de markt zijn gebracht ook aan de eisen voldoen. Het is in het belang van de producenten en de gebruikers dat de veilige middelen ook die kwalificatie verdienen. Het is ook niet verboden om middelen om een elektronische handtekening aan te maken op de markt te brengen die niet aan de eisen voldoen. Zij mogen dan echter niet als «veilig middel» op de markt worden gebracht. Overtreding van dit verbod is op grond van artikel 18.17 van de Telecommunicatiewet en artikel 1, onder 4° van de Wet op de economische delicten strafbaar.

Bij het zetten van de elektronische handtekening zal de ondertekenaar op de een of andere wijze kenbaar maken of hij gebruik maakt van een veilig middel. De ontvanger van de elektronische handtekening zal zich op dergelijke informatie verlaten.

Er is geen aanleiding erop toe te zien dat alleen veilige middelen worden gebruikt voor het aanmaken van elektronische handtekeningen. Het is in het belang van de ondertekenaar dat hij zelf controleert of hij een veilig middel hanteert om de gewenste mate van betrouwbaarheid van zijn elektronische handtekening te bewerkstelligen.

Deze ondertekenaar zal zich op zijn beurt beroepen op een overeenstemmingsverklaring waarvan een afschrift bij het veilig middel gevoegd is. Indien de veilige middelen niet veilig blijken te zijn, moet hij de producent aanspreken.

De gestelde eisen beogen te waarborgen dat de instellingen betrouwbaar en deskundig zijn. De eis van de vertrouwelijke behandeling van gegevens kan alleen worden doorbroken indien de bevoegde autoriteiten op basis van een uitdrukkelijke wettelijke bepaling, zoals opgenomen in artikel 125i van het Wetboek van Strafvordering, de gegevens opeisen.

Artikel 6

Zoals in het algemene gedeelte van deze toelichting al is opgemerkt, kan in de praktijk blijken dat de eisen die in dit besluit zijn opgenomen, in een concreet geval onvoldoende aanknopingspunten bieden voor de gebruikers en de toezichthouder. In een ministeriële regeling kunnen in dat geval nadere concretiseringen worden opgenomen. Zoals eerder aangegeven zal dit voor een aantal eisen ook daadwerkelijk gebeuren, zulks op basis van in Europees verband tot stand gekomen normeringen.

Artikel 7

Ingevolge de huidige systematiek worden de kosten van het toezicht door de Onafhankelijke post- en telecommunicatieautoriteit omgeslagen over de bedrijven en instellingen waarop toezicht wordt gehouden in het kader van de Telecommunicatiewet. De hoogte van de vergoedingen wordt vastgesteld op basis van het Besluit vergoedingen Telecommunicatiewet. Dit besluit moet daarom een expliciete aanduiding bevatten van de certificatiedienstverleners teneinde een vergoeding te kunnen vaststellen.

Ook de vergoedingen die in rekening kunnen worden gebracht in verband met de werkzaamheden van de Minister van Economische Zaken voor het beoordelen van aanvragen om aanwijzing als accreditatieorganisatie, als bedoeld in artikel 18.16, eerste lid, van de Telecommunicatiewet, of als instelling die verklaringen afgeeft op het gebied van veilige middelen voor het aanmaken van elektronische handtekeningen, als bedoeld in artikel 18.17, tweede lid, van de Telecommunicatiewet worden op grond van het Besluit vergoedingen Telecommunicatiewet vastgesteld. Dit artikel brengt in het Besluit vergoedingen Telecommunicatiewet de juridische basis aan voor het in rekening brengen van de bedoelde vergoedingen.

De Staatssecretaris van Economische Zaken,
J. G. Wijn

Bijlage bij de nota van toelichting bij het Besluit elektronische handtekeningen

Transponeringstabel

Richtlijn	Besluit
Bijlage I	artikel 3
Onderdeel a	onderdelen a
Onderdeel b	onderdeel b
Onderdeel c	onderdeel c
Onderdeel d	onderdeel d
Onderdeel e	onderdeel e
Onderdeel f	onderdeel f
Onderdeel g	onderdeel g
Onderdeel h	onderdeel h
Onderdeel i	onderdeel i
Onderdeel j	onderdeel j
Bijlage II	artikel 2, eerste lid,
Onderdeel a	onderdelen a, b, s, en tweede en derde lid
Onderdeel b	onderdelen k, l
Onderdeel c	onderdeel h
Onderdeel d	onderdeel g
Onderdeel e	onderdelen b en f
Onderdeel f	onderdeel c
Onderdeel g	onderdeel d
Onderdeel h	onderdeel e
Onderdeel i	onderdeel i
Onderdeel j	onderdeel m
Onderdeel k	onderdelen n en r
Onderdeel l	onderdeel j
Bijlage III	artikel 5
Onderdeel 1	onderdelen a, b, c
Onderdeel 2	onderdeel d
Bijlage IV	behoeft geen implementatie