Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2000–2001

27 743

Aanpassing van Boek 3 en Boek 6 van het Burgerlijk Wetboek, de Telecommunicatiewet en de Wet op de economische delicten inzake elektronische handtekeningen ter uitvoering van 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 L 13) (Wet elektronische handtekeningen)

Nr. 3

MEMORIE VAN TOELICHTING

ALGEMEEN

1. Inleiding

Eind 1999 is tot stand gekomen richtlijn nr. 99/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG L 13) (verder: richtlijn). Deze richtlijn beoogt het gebruik van elektronische handtekeningen te vergemakkelijken en tot de wettelijke erkenning ervan bij te dragen. Door het bieden van rechtszekerheid over de juridische status van de elektronische handtekening wordt het vertrouwen in dit middel gestimuleerd. Daarnaast gaat de richtlijn verschillen in wet- en regelgeving in de diverse lidstaten op dit terrein tegen. Uiteenlopende regels voor de wettelijke erkenning van elektronische handtekeningen en voor de accreditatie van certificatiedienstverleners kunnen immers belemmeringen opwerpen voor het vrije verkeer van diensten langs elektronische weg. De richtlijn dient voor 19 juli 2001 te zijn geïmplementeerd.
Het wetsvoorstel strekt tot uitvoering van de richtlijn. Het regelt daartoe de rechtsgevolgen van elektronische handtekeningen waaronder de gelijkstelling van elektronische handtekeningen aan handgeschreven handtekeningen op een papieren drager. Voorts bevat het wetsvoorstel een aansprakelijkheidsbepaling voor certificatiedienstverleners die gekwalificeerde certificaten uitgeven. Voor deze laatste certificatiedienstverleners is bovendien voorzien in een toezichtsysteem en de mogelijkheid tot het invoeren van een vrijwillige accreditatieregeling ter verbetering van certificatiedienstverlening.

KST53169
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2001

2. De richtlijn en de uitvoering

2.1 Verschillende soorten elektronische handtekeningen

De richtlijn maakt onderscheid tussen «gewone» elektronische handtekeningen en geavanceerde elektronische handtekeningen.
Onder een «gewone» elektronische handtekening wordt ingevolge artikel 2, eerste lid, van de richtlijn verstaan elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authentificatie. Hierbij valt bijvoorbeeld te denken aan een ingescande handtekening van een papieren drager. Afhankelijk van het doel waarvoor een elektronische handtekening wordt gebruikt, kunnen partijen gebruik maken van deze handtekening danwel van een elektronische handtekening die met meer waarborgen is omkleed: de geavanceerde elektronische handtekening. Van deze laatste handtekening is ingevolge artikel 2, tweede lid, van de richtlijn sprake indien de handtekening op unieke wijze aan de ondertekenaar is verbonden, zij het mogelijk maakt de ondertekenaar te identificeren, zij tot stand is gekomen met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden en zij op zodanige wijze aan de gegevens waarop zij betrekking heeft is verbonden, dat elke wijziging achteraf van gegevens kan worden opgespoord. In deze definitie wordt bewust geen melding gemaakt van een bepaalde techniek om elektronische handtekeningen aan te maken, om de voortschrijdende technologische ontwikkeling niet te belemmeren. Een geavanceerde elektronische handtekening kan derhalve met elke willekeurige techniek worden aangemaakt zolang aan de genoemde voorwaarden wordt voldaan.
Een op dit moment veel gebruikte techniek voor het aanmaken van een geavanceerde elektronische handtekening is de «digitale handtekening». Bij deze techniek wordt gebruik gemaakt van twee codes die onlosmakelijk met elkaar zijn verbonden: een publieke en een private sleutel. Deze sleutels zijn uniek voor een persoon. Welke publieke sleutel bij welke persoon hoort, wordt door een certificatiedienstverlener (onafhankelijke derde) vastgelegd in een digitaal certificaat. De betreffende persoon kan vervolgens een elektronisch bestand ondertekenen met zijn private sleutel. De ontvanger van dit bestand kan (alleen) met de bijbehorende publieke sleutel verifiëren of het bericht ongewijzigd is en afkomstig van de bezitter van de bijbehorende (geheime) private sleutel. De private sleutel is uniek voor een ondertekenaar en mag niet bekend raken bij anderen dan de ondertekenaar. Om deze private sleutel onder zijn uitsluitende controle te kunnen houden zijn er diverse (combinaties van) mogelijkheden. Alvorens een private sleutel te kunnen gebruiken voor het zetten van een handtekening kan er kennis (bijvoorbeeld een pincode), bezit (gebruikmaking van bijvoorbeeld een smartcard waar de private sleutel op staat) of een lichaamskenmerk van de ondertekenaar (bijvoorbeeld een vingerafdruk) worden geëist. Om tenslotte te voldoen aan de eis dat de ondertekenaar geïdentificeerd kan worden, moet de ontvanger weten welke publieke sleutel bij welke verzender hoort. Deze informatie staat op het certificaat dat door een certificatiedienstverlener voor de ondertekenaar is afgegeven. Het achterhalen van het certificaat kan op verschillende manieren. De ondertekenaar kan het digitale certificaat met daarop de publieke sleutel meesturen met zijn bericht. Mogelijk is ook dat hij aan de ontvanger doorgeeft bij welke certificatiedienstverlener hij zijn elektronische handtekening heeft aangevraagd. De ontvanger kan dan bijvoorbeeld de website van de betreffende certificatiedienstverlener raadplegen om de publieke sleutel van de verzender te achterhalen.

2.2 Verschillende soorten certificaten

Certificatiedienstverleners koppelen een unieke code aan een persoon en

leggen dit vast in een digitaal certificaat. De richtlijn maakt onderscheid tussen «gewone» certificaten en gekwalificeerde certificaten.
Een «gewoon» certificaat is een elektronische bevestiging die gegevens voor het verifiëren van een handtekening aan een bepaalde persoon verbindt en de identiteit van die persoon bevestigt. Daarnaast kan een certificaat nog meer gegevens bevatten die van belang zijn voor de ontvanger van de handtekening, zoals de geldigheidsduur van het certificaat, eventuele beperkingen betreffende het gebruik en de garantie van echtheid van het certificaat. Dit laatste aspect kan worden bereikt door het elektronisch ondertekenen van het certificaat door de afgevende certificatiedienstverlener.
Een gekwalificeerd certificaat is een certificaat dat met meer waarborgen is omgeven. Dit certificaat dient te voldoen aan de eisen van bijlage I van de richtlijn en dient te zijn afgegeven door een certificatiedienstverlener die voldoet aan de eisen van bijlage II van de richtlijn. Bijlage I vermeldt welke informatie in een certificaat moet worden opgenomen om het predikaat «gekwalificeerd» te krijgen. Een gekwalificeerd certificaat dient onder meer de volgende gegevens te bevatten: vermelding dat het certificaat als gekwalificeerd wordt uitgegeven, identificatie en het land van vestiging van de afgevende certificatiedienstverlener, de geldigheidsduur van het certificaat en de eventuele beperkingen betreffende het gebruik van het certificaat. Bijlage II bevat de eisen waaraan certificatiedienstverleners die gekwalificeerde certificaten afgeven dienen te voldoen. Deze bijlage bevat onder meer de plicht voor certificatiedienstverleners om aan te tonen dat zij voldoen aan de betrouwbaarheidseisen voor het aanbieden van certificatiediensten, de plicht om veilige en betrouwbare procedures, systemen en producten te gebruiken, een informatieplicht, een bewaarplicht alsmede organisatorische en financiële vereisten. Deze bijlage vereist bovendien dat een certificatiedienstverlener de identiteit van de persoon voor wie een gekwalificeerd certificaat wordt afgegeven controleert en het resultaat hiervan op verifieerbare wijze vastlegt.
Vermeld zij dat de bijlagen nu nog algemene doelstellingen bevatten maar dat de Europese Standaardisatie organisaties, European Telecommunication Standards Institute (ETSI) en Comité Européen de Normalisation (CEN) werken aan een precisering in technische normen.

2.3 Rechtsgevolgen van elektronische handtekeningen

De richtlijn bepaalt in artikel 5 lid 1 dat een geavanceerde elektronische handtekening die is gebaseerd op een gekwalificeerd certificaat, is aangemaakt met behulp van een veilig middel (zie § 2.8) en voldoet aan de wettelijke eisen die gelden voor handtekeningen, in gelijke mate rechtskracht heeft als een handgeschreven handtekening op een papieren drager in de gegeven omstandigheden zou hebben. Aan een elektronische handtekening die met genoemde waarborgen is omgeven dient derhalve dezelfde juridische status te worden toegekend als aan een handgeschreven handtekening op een papieren drager. De eisen waaraan de geavanceerde elektronische handtekening als bedoeld in artikel 5 lid 1 van de richtlijn moet voldoen, staan in artikel 2 leden 2, 6 en 10 van de richtlijn. Mede door de verwijzing naar de bijlagen I, II en III van de richtlijn gaat het in totaal om ongeveer dertig vereisten. Is daaraan voldaan, dan is de elektronische handtekening juridisch gelijkwaardig aan een handgeschreven handtekening en heeft deze derhalve dezelfde rechtsgevolgen. Al deze vereisten hebben ten doel een zeker veiligheids- en betrouwbaarheidsniveau te verzekeren, dat voor de meeste toepassingen in het rechtsverkeer volstaat.
Artikel 5 lid 2 van de richtlijn bepaalt dat aan een elektronische handtekening geen rechtsgeldigheid mag worden ontzegd en dat zij niet als bewijsmiddel in gerechtelijke procedures mag worden geweigerd louter op grond van het feit dat de handtekening in elektronische vorm is gesteld, of

niet is gebaseerd op een gekwalificeerd certificaat, of niet is gebaseerd op een door een geaccrediteerd certificatiedienstverlener afgegeven certificaat, of niet met een veilig middel is aangemaakt. Deze bepaling brengt derhalve tot uitdrukking dat de lidstaten ervoor moeten zorgen dat een elektronische handtekening niet (steeds) rechtens terzijde kan worden gesteld enkel en alleen op grond van het feit dat aan een of meer van de uit het eerste lid voortvloeiende vereisten niet is voldaan.
De richtlijn treedt niet in de contractsvrijheid van (private) partijen en dwingt hen niet tot het gebruik of het aanvaarden van elektronisch ondertekende gegevens. Het staat partijen vrij om onderling overeen te komen of zij elektronisch ondertekende gegevens zullen aanvaarden en, zo ja, onder welke voorwaarden, in de mate die door het nationale recht wordt toegestaan (rechtsoverweging 16, artikel 1 van de richtlijn). Partijen kunnen derhalve een hoger of een lager veiligheidsniveau overeenkomen dan in artikel 5 van de richtlijn is bepaald. De richtlijn brengt evenmin mee dat indien een elektronische handtekening aan een of meer van die vereisten van artikel 5 van de richtlijn niet voldoet, daarmee steeds (automatisch) vaststaat dat die niet een voldoende veiligheids- en betrouwbaarheidsniveau heeft. Ook dan kan uit de partijafspraak, de aard van de transactie, het doel waarvoor de elektronische gegevens werden verzonden of andere omstandigheden van het geval voortvloeien dat hetgeen elektronisch is verzonden in de gegeven omstandigheden dezelfde rechtsgevolgen heeft als een met de hand ondertekend schriftelijk stuk zou hebben.
Artikel 5 van de richtlijn veronderstelt in wezen het bestaan van een algemene norm, inhoudende dat een elektronische handtekening steeds dan als juridisch gelijkwaardig aan een handgeschreven handtekening dient te worden beschouwd indien deze, gelet op alle omstandigheden van het geval, met een voldoende mate van betrouwbaarheid dezelfde functies vervult als een handgeschreven handtekening. In het wetsvoorstel is in artikel 15a lid 1 BW dan ook een dergelijke algemene norm opgenomen. Een vergelijkbare bepaling is opgenomen in de Model Law on Electronic Commerce (1996) van de United Nations Commission on International Trade Law (UNCITRAL) en deze heeft dan ook model gestaan voor de in het onderhavige voorstel geformuleerde algemene norm. Deze bepaling biedt een grote mate van flexibiliteit voor de rechter die nodig is in verband met de veelheid aan situaties waarin elektronische handtekeningen in het maatschappelijk verkeer zullen worden gebruikt. Met deze bepaling wordt bovendien aangesloten bij de mondiale ontwikkelingen op dit gebied, aangezien inmiddels in vele geïndustrialiseerde landen buiten de Europese Unie wetgeving voor het elektronisch rechtsverkeer tot stand is gebracht die voortbouwt op deze Model Law.
Benadrukt zij dat het feit dat de elektronische handtekening als bewijs in gerechtelijke procedures dient te worden toegelaten nog niets zegt over de waardering van het bewijs. De richtlijn laat de beoordeling van de waarde van het bewijsmiddel door de rechter onverlet (rechtsoverweging 21), hetgeen overeenstemt met hetgeen reeds naar Nederlands recht geldt. Artikel 179 Wetboek van Burgerlijke Rechtsvordering kent een open bewijsstelsel, wat inhoudt dat tenzij de wet anders bepaalt, bewijs kan worden geleverd door alle middelen die zich daartoe lenen. De waardering van de bewijsmiddelen wordt echter, voor zover de wet niet anders bepaalt, overgelaten aan de rechter. Zo kan de rechter bij de waardering van het bewijsmiddel rekening houden met de mate van technische betrouwbaarheid van het toegepaste procédé of de gebruikte technologie, met de mogelijkheid van vervalsing van de weergave van het te bewijzen feit alsmede met de wijze waarop de afzender is geïdentificeerd en met de overige omstandigheden van het geval.
Van een elektronische handtekening kan onjuist danwel onbevoegd gebruik worden gemaakt. Afhankelijk van de omstandigheden van het geval en, indien gebruik is gemaakt van de diensten van een certificatie-

dienstverlener, in het bijzonder van de concrete inhoud van de desbetreffende contractuele relatie tussen gebruikers van elektronische handtekeningen en/of certificatiedienstverleners, kan hiertegen worden opgetreden. Nu het gebruik van een elektronische handtekening veelal mede plaats zal vinden in het kader van een contractuele relatie tussen de gebruiker van een elektronische handtekening en een certificatiedienstverlener, die voor beiden bepaalde rechten en verplichtingen zal meebrengen, dient de beoordeling van de vraag wat een gebruiker van een elektronische handtekening (zelfstandig) jegens derden zal kunnen ondernemen in het geval van bijvoorbeeld onrechtmatig gebruik van die elektronische handtekening, mede te worden bezien in het licht van deze contractuele relatie. Omgekeerd geldt eveneens dat bij het bepalen in hoeverre een certificatiedienstverlener (zelfstandig) jegens derden zal kunnen optreden ingeval hij op de hoogte raakt van onregelmatigheden in het gebruik van de elektronische handtekening, de contractuele relatie die hij met de gebruiker van die elektronische handtekening heeft een belangrijke rol zal spelen.
Een en ander brengt mee dat hierover in zijn algemeenheid, dat wil zeggen los van de omstandigheden van het geval, moeilijk uitspraken kunnen worden gedaan en dat een wettelijke regeling hiervan derhalve niet voor de hand ligt. De mogelijkheid voor gebruikers van elektronische handtekeningen en certificatiedienstverleners om in (algemene) contractsvoorwaarden gedragslijnen vast te leggen voor de in de praktijk het meest voor de hand liggende situaties, is derhalve van groot belang. Dit biedt hen een goede mogelijkheid voor het vinden van een evenwicht tussen enerzijds de wenselijkheid deze bepalingen toe te snijden op de individuele behoeften van gebruikers en certificatiedienstverleners en anderzijds die van rechtszekerheid voor betrokkenen. Het valt derhalve te verwachten dat in de praktijk tussen gebruikers van elektronische handtekeningen en certificatiedienstverleners – ten minste in grote lijnen – zal worden vastgelegd wat de mogelijkheden voor partijen in dit opzicht zijn en in welke gevallen, alsmede op welke wijze de gebruiker, respectievelijk de certificatiedienstverlener, in ieder geval gehouden zal zijn de andere partij bij het nemen van bepaalde stappen jegens derden te betrekken. Het is mogelijk dat daarbij wordt voorzien in toestemmingsvereisten, maar ook andere mechanismen die beogen te verzekeren dat de belangen van de andere betrokken partij bij het nemen van de hier bedoelde stappen niet worden veronachtzaamd, zijn denkbaar. Wat het strafrecht betreft kan worden opgemerkt dat het onbevoegd gebruik maken van een elektronische handtekening niet afzonderlijk is strafbaar gesteld. Onder omstandigheden is het echter denkbaar dat onbevoegd gebruik van een handtekening het delict valsheid in geschrifte op kan leveren. Zie de memorie van toelichting onder artikel 15c.

2.4 Aansprakelijkheid van certificatiedienstverleners

Een andere belangrijke bepaling in de richtlijn die omzetting behoeft, is die betreffende de aansprakelijkheid van certificatiedienstverleners die gekwalificeerde certificaten afgeven aan het publiek. Voor certificatiedienstverleners in het algemeen gelden de bepalingen van het toepasselijke nationale recht, in Nederland de aansprakelijkheidsregels zoals opgenomen in boek 6 van het Burgerlijk Wetboek (rechtsoverweging 22). Ingevolge artikel 6 van de richtlijn dient op certificatiedienstverleners die gekwalificeerde certificaten afgeven aan het publiek of publiekelijk instaan voor een dergelijk certificaat ten minste een (gekwalificeerde) schuldaansprakelijkheid met omgekeerde bewijslast te rusten. In die gevallen is de certificatiedienstverlener aansprakelijk voor schade die personen die in redelijkheid op dit certificaat vertrouwen, hebben ondervonden, met betrekking tot:
– de juistheid, op het tijdstip van afgifte, van alle gegevens in het gekwa-

lificeerde certificaat en de opneming in het gekwalificeerde certificaat van alle voor een dergelijk certificaat voorgeschreven gegevens;
– de opneming in het gekwalificeerde certificaat van alle voor een dergelijk certificaat voorgeschreven gegevens;
– de garantie dat de in het gekwalificeerd certificaat geïdentificeerde ondertekenaar, op het tijdstip van de afgifte van het certificaat, houder was van de gegevens voor het aanmaken van de elektronische handtekening en die met de in het certificaat gegeven of geïdentificeerde gegevens voor het verifiëren van een handtekening overeenstemmen;
– de garantie dat de gegevens voor het aanmaken van de elektronische handtekening en die voor het verifiëren van de elektronische handtekening, – indien zij beide door de certificatiedienstverlener werden gegenereerd –, complementair kunnen worden gebruikt.

Evenzeer zijn certificatiedienstverleners die gekwalificeerde certificaten afgeven aan het publiek of publiekelijk voor een dergelijk certificaat instaan op grond van artikel 6, tweede lid, van de richtlijn aansprakelijk voor de schade die is ontstaan doordat de intrekking van het certificaat niet werd geregistreerd. Ook hier kan de certificatiedienstverlener aan de op hem rustende aansprakelijkheid ontkomen door te bewijzen dat hij niet nalatig is geweest.

Artikel 6 lid 3 bepaalt dat deze certificatiedienstverleners niet aansprakelijk zijn voor schade die is ontstaan door het gebruik van een gekwalificeerd certificaat waarbij de op het certificaat aangegeven beperkingen zijn overschreden. Deze certificatiedienstverleners zijn evenmin aansprakelijk ingevolge artikel 6, vierde lid, van de richtlijn indien schade is ontstaan door overschrijding van de op het certificaat aangegeven grens voor de waarde van de transacties waarvoor het certificaat kan worden gebruikt mits die grens voor derden kenbaar is.

Artikel 6, vijfde lid, van de richtlijn besluit met de bepaling dat deze richtlijn complementair is aan richtlijn nr. 93/13/EEG van de Raad van 5 april 1993 betreffende oneerlijke bedingen. Deze richtlijn doet derhalve geen afbreuk aan het in de richtlijn betreffende oneerlijke bedingen bepaalde.

2.5 Erkenning van buiten de EG danwel een van de overige staten die partij zijn bij de Overeenkomst betreffende de Europese Economische Ruimte afgegeven gekwalificeerde certificaten

Artikel 7 van de richtlijn regelt de erkenning van gekwalificeerde certificaten afgegeven door certificatiedienstverleners gevestigd in landen buiten de Europese Gemeenschap (EG) danwel buiten een van de overige staten die partij zijn bij de Overeenkomst betreffende de Europese Economische Ruimte (EER). Deze certificaten worden gelijkgesteld aan gekwalificeerde certificaten die door een in de EG of EER gevestigde certificatiedienstverlener worden afgegeven indien de certificatiedienstverlener voldoet aan de eisen in de richtlijn en in het kader van een in een lidstaat van de EG of EER ingestelde vrijwillige-accreditatieregeling is geaccrediteerd, danwel een in de EG of EER gevestigde certificatiedienstverlener die voldoet aan de richtlijn in staat voor dit certificaat of het certificaat of de certificatiedienstverlener is erkend in het kader van een bilaterale of multilaterale overeenkomst tussen de EG of EER en derde landen of internationale organisaties. Dergelijke overeenkomsten kunnen de ontwikkeling van de internationale handel stimuleren (rechtsoverweging 23). Ingevolge artikel 7, tweede lid, van de richtlijn zal de Europese Commissie dan ook voorstellen doen om de effectieve uitvoering van normen en internationale overeenkomsten inzake certificatiediensten te bereiken. Het derde lid van artikel 7 van de richtlijn geeft de Europese Commissie de mogelijkheid om bij kennisneming van problemen van ondernemingen bij het betreden van markten van derde landen aan de Raad voorstellen te doen voor een passend mandaat voor onderhandelingen voor ondernemingen uit de EG in die derde landen.

2.6 Toezicht op certificatiedienstverleners die gekwalificeerde certificaten aan het publiek aanbieden of afgeven

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. Het verlenen van certificatiediensten mag ingevolge artikel 3, eerste lid, van de richtlijn niet afhankelijk van voorafgaande machtiging worden gesteld. Het uitgangspunt is dat certificatiedienstverleners hun diensten vrij, zonder voorafgaande machtiging, moeten kunnen aanbieden ter bevordering van het leveren via open netwerken van certificatiediensten in de gehele gemeenschap (rechtsoverweging 10). De zinsnede «zonder voorafgaande machtiging» wordt ruim geïnterpreteerd: hieronder wordt niet alleen elke vergunning verstaan waarvoor de certificatiedienstverlener een besluit van de nationale autoriteiten moet verkrijgen voordat hij zijn certificatiediensten mag aanbieden maar ook alle andere maatregelen met hetzelfde effect. Wel wordt erkend dat privaatrechtelijke organisaties die initiatieven nemen en regelingen toepassen die beogen de dienstverlening te verbeteren, aan certificatiedienstverleners een passend kader kunnen bieden om hun diensten verder te ontwikkelen en het door de markt verlangde niveau van vertrouwen, veiligheid en kwaliteit te bereiken. Van deze regelingen waarbij een door de overheid geautoriseerde instantie formeel erkent dat een certificatiedienstverlener voldoet aan bepaalde eisen, mag gebruik worden gemaakt mits het op vrijwillige basis geschiedt (rechtsoverweging 13). Lidstaten mogen ingevolge artikel 3, tweede lid, van de richtlijn dan ook zogenoemde vrijwillige accreditatieregelingen invoeren of handhaven mits de voorwaarden objectief, transparant, evenredig en niet-discriminerend zijn. Toezicht op certificatiedienstverleners wordt slechts gehouden om te waarborgen dat certificaten die als gekwalificeerde certificaten worden aangeboden of afgegeven aan de eisen voor deze certificaten voldoen, zijnde de eisen van bijlage I en II van de richtlijn.
Het door artikel 3 lid 3 van de richtlijn voorgeschreven passende systeem van toezicht op certificatiedienstverleners die gekwalificeerde certificaten uitgeven aan het publiek is opgenomen in de Telecommunicatiewet. Certificatiedienstverleners verrichten diensten die vaak gekoppeld zijn aan het gebruik van openbare telecommunicatienetwerken en -diensten als bedoeld in deze wet. In verband met deze verbondenheid en de uit de Telecommunicatiewet sprekende zorg voor een betrouwbaar telecommunicatienetwerk en een betrouwbare dienstverlening op dat netwerk, is het toezicht in die wet opgenomen. Bij de opzet van het toezichtsysteem is zoveel mogelijk aangesloten bij het toezichtsysteem van de Telecommunicatiewet dat geldt voor de aanbieders van telecommunicatienetwerken en -diensten.
De naleving van de regels door certificatiedienstverleners wordt zowel preventief als repressief gehandhaafd. De preventieve handhaving is zo ingevuld dat certificatiedienstverleners die gekwalificeerde certificaten aan het publiek aanbieden of afgeven en die een vestiging in Nederland hebben, geregistreerd moeten zijn bij de Onafhankelijke Post- en Telecommunicatieautoriteit (OPTA: verder het college). Het college registreert elke aanvraag van een certificatiedienstverlener waardoor geen belemmeringen optreden voor certificatiedienstverleners om hun dienstverlening te verrichten. Bij de aanvraag van hun registratie dienen de certificatiedienstverleners echter wel informatie over te leggen waaruit blijkt dat zij voldoen aan de eisen bij of krachtens algemene maatregel van bestuur gesteld, zijnde de eisen van bijlage I en II van de richtlijn. Na registratie beoordeelt het college of de bij de aanvraag voor registratie meegezonden informatie volledig is. Op deze manier verkrijgt het college de informatie die nodig is om in een voorkomend geval, nadat registratie

heeft plaatsgevonden, te kunnen controleren of aan de eisen van de algemene maatregel van bestuur is voldaan.
Een registratie bij het college geldt in beginsel voor onbepaalde tijd. Beëindiging of wijziging van de registratie zal naar verwachting in de meeste gevallen plaatsvinden op verzoek van de certificatiedienstverlener zelf.
Vrijwillige accreditatieregelingen zijn regelingen waarbij een geautoriseerde onafhankelijke instantie erkent dat een certificatiedienstverlener aan bepaalde eisen voldoet. Om deze erkenning te verkrijgen wordt een certificatiedienstverlener eerst getoetst aan het voldoen aan de eisen door het uitvoeren van een audit ter plaatse. Deze accreditatie is eveneens te kenmerken als een vorm van preventief toezicht. Men zie voor een meer uitgebreide toelichting van vrijwillige accreditatieregelingen in het artikelsgewijze deel van deze memorie, onder artikel 18.16.
Repressieve handhaving komt aan de orde als in strijd met de regels is gehandeld. De wet biedt hiervoor zowel bestuursrechtelijke als strafrechtelijke handhavingsinstrumenten. In de praktijk zal de nadruk liggen bij de bestuursrechtelijke handhaving. Voor de handhaving van de naleving van de registratieplicht voor certificatiedienstverleners die gekwalificeerde certificaten aanbieden of afgeven aan het publiek is de bestuursrechtelijke handhaving het aangewezen instrument. Dat geldt ook voor de handhaving van de verplichting van certificatiedienstverleners om aan de eisen van de bijlagen bij de richtlijn te voldoen. Het college is bevoegd om de registratie van een certificatiedienstverlener te beëindigen en kan van deze bevoegdheid gebruik maken indien de certificatiedienstverlener niet of niet geheel voldoet aan de bij algemene maatregelen van bestuur gestelde eisen. Om na te gaan of deze laatste situatie zich voordoet kan het college onderzoeken of een ingeschreven certificatiedienstverlener aan deze eisen voldoet. Hierbij kan het college gebruik maken van alle middelen die hoofdstuk 15 en artikel 18.7 van de Telecommunicatiewet bieden. Het uitoefenen van deze bevoegdheden zal in de praktijk beperkt blijven tot die gevallen waar een redelijk vermoeden bestaat dat een geregistreerde certificatiedienstverlener niet aan deze eisen voldoet. Indien uit een dergelijk onderzoek blijkt dat niet aan de gestelde eisen wordt voldaan, stelt het college de dienstverlener een termijn om alsnog hieraan te voldoen. Afhankelijk van de uitkomst van een onderzoek dat wordt verricht tegen het einde van of na de gestelde termijn kan het college de registratie beëindigen. Zo lang hij niet (opnieuw) is geregistreerd mag de certificatiedienstverlener geen gekwalificeerde certificaten aan het publiek (meer) afgeven. Indien van een certificatiedienstverlener, waarvoor het vermoeden van het niet voldoen aan de eisen bestaat, de overeenstemming met de wettelijke eisen is vastgesteld door een aangewezen instantie als bedoeld in artikel 18.16, vraagt het college met toepassing van artikel 18.7 eerste lid, eerst bij de aangewezen organisatie informatie over de certificatiedienstverlener en de wijze waarop deze organisatie deze certificatiedienstverlener heeft beoordeeld en op de naleving van de regeling toeziet. Indien het college daarna een onderzoek bij de certificatiedienstverlener noodzakelijk acht, kan hij daartoe het initiatief nemen. Voor het inwinnen van de inlichtingen bij organisaties die op grond van artikel 18.16 zijn aangewezen, kan artikel 18.7 worden toegepast. Het aanwijzen van een accreditatieorganisatie brengt met zich mee dat voor het toezicht op de geaccrediteerde certificatiedienstverleners, het college in eerste instantie zich zal richten tot de aangewezen organisatie die de overeenstemming van de certificatiedienstverlener met de wettelijke eisen heeft vastgesteld. In artikel 18.18 is een uitdrukkelijk verbod opgenomen voor de certificatiedienstverleners waarvan de registratie met toepassing van artikel 2.2, derde lid, onderdeel 3°, subonderdeel f is beëindigd. Hierdoor blijft het toepassen van bestuurlijke maatregelen tegen deze niet meer geregistreerde certificatiedienstverlener mogelijk. Dit is wenselijk met het oog op een ononderbroken toezicht op certificatiedienstverleners

die er niet in slagen aan de wettelijke eisen te voldoen, maar waarvan het vermoeden bestaat dat zij zich niet door een ontbrekende registratie zullen laten weerhouden van het aanbieden van als gekwalificeerd aangeduide certificaten. Met opzet is hiertegen ook strafrechtelijk optreden mogelijk gemaakt.
Strafrechtelijke handhaving is met name aan de orde als de bestuursrechtelijke middelen, zoals een onderzoek naar de niet-naleving van de registratieplicht, minder effectief blijken te zijn. In artikel III van het voorstel wordt overtreding van de artikelen 2.1, derde lid, eerste volzin, en 18.15, eerste en tweede lid strafbaar gesteld. Dit betekent ten eerste dat het strafbaar is om certificaten als gekwalificeerde certificaten aan het publiek aan te bieden of af te geven, als de certificatiedienstverlener of de certificaten die hij als zodanig aanbiedt niet aan de eisen voldoen, en ten tweede dat het strafbaar is als de certificatiedienstverlener die niet is geregistreerd bij het college, gekwalificeerde certificaten aan het publiek aanbiedt of afgeeft. Dat is vooral van belang bij de handhaving ten aanzien van certificatiedienstverleners die nog niet eerder zijn geregistreerd en waarvan het niet duidelijk is of zij gekwalificeerde certificaten aanbieden aan het publiek. Zij vallen in beginsel niet onder het toezicht van het college. Strafrechtelijke handhaving door het OM beperkt zich dan tot niet geregistreerde certificatiedienstverleners waarvan vermoed wordt dat zij gekwalificeerde certificaten uitgeven aan het publiek en waarvan onderzocht moet worden of ze dit daadwerkelijk doen.
Het college houdt kortom, door middel van aangewezen ambtenaren, toezicht op de naleving van de registratieplicht van certificatiedienstverleners die gekwalificeerde certificaten afgeven of aanbieden, en daarmee samenhangend, of de certificatiedienstverleners en de door hun afgegeven gekwalificeerde certificaten aan de bij of krachtens de Telecommunicatiewet gestelde eisen voldoen.
De Minister van Verkeer en Waterstaat kan instellingen aanwijzen die certificatiedienstverleners (voorafgaand aan de registratie door OPTA) op hun verzoek toetsen op de naleving van de bij of krachtens de Telecommunicatiewet gestelde eisen. De Minister houdt toezicht op de naleving van de voorwaarden voor aanwijzing. Het Openbaar Ministerie is belast met de opsporing van certificatiedienstverleners die niet zijn geregistreerd, maar die vermoedelijk certificaten als gekwalificeerd afgeven, hetgeen verboden is voor een niet geregistreerde certificatiedienstverlener.
De Minister van Verkeer en Waterstaat wijst instellingen aan die veilige middelen op de overeenstemming met de eisen van de richtlijn toetsen, en houdt toezicht op de naleving van de criteria voor aanwijzing. Het Openbaar Ministerie is belast met de opsporing van degenen die middelen om elektronische handtekeningen aan te maken als veilige middelen aanbieden of verhandelen, terwijl die middelen niet aan de eisen, gesteld bij of krachtens de Telecommunicatiewet voldoen.

2.7 De OPTA als toezichthouder op certificatiedienstverleners die gekwalificeerde certificaten aanbieden aan het publiek

In dit voorstel is de OPTA (het college) aangewezen als onafhankelijk toezichthouder op certificatiedienstverleners die gekwalificeerde certificaten aan het publiek aanbieden of afgeven. Aanvankelijk, voor het tot stand komen van de richtlijn, werd gedacht aan een, nog op te richten, TTP-Kamer als mogelijke toezichthouder op certificatiedienstverleners. De idee was dat deze TTP-Kamer zou toezien op certificatiedienstverleners die zich vrijwillig bij een, onder deze TTP-Kamer vallende, accreditatieregeling konden aansluiten. Van dit oorspronkelijke idee is echter door de komst van de richtlijn afgeweken. Reden is dat bevoegdheden die de toezichthouder in het licht van de richtlijn krijgt te kwalificeren zijn als de uitoefening van openbaar gezag, hetgeen niet voorzien was bij de

TTP-Kamer, en ten tweede het toezicht zich niet beperkt tot die certificatiedienstverleners die vallen onder een vrijwillige accreditatieregeling. De richtlijn verplicht namelijk toezicht te houden op alle in Nederland gevestigde certificatiedienstverleners die gekwalificeerde certificaten afgeven aan het publiek, onafhankelijk of zij onder een vrijwillige accreditatieregeling vallen of niet. Er is gezocht naar een alternatief dat ook op korte termijn operationeel kan zijn. Door te kiezen voor een bestaande toezichthouder wordt aan dit laatste punt tegemoet gekomen en wordt tevens voorkomen dat er weer een organisatie wordt toegevoegd aan de vele reeds bestaande toezichthouders. Een ander aspect dat meespeelde in de overweging is dat het nog onduidelijk is hoeveel inspanning het toezicht met zich meebrengt en of dit een aparte organisatie rechtvaardigt. Gezien de verankering van het toezicht in de Telecommunicatiewet is het college ook een logische keuze. Het college is immers al belast met het toezicht op andere onderdelen van de Telecommunicatiewet. Bovendien past de voorgestane wijze van toezicht, initieel alleen registratie, goed bij de huidige wijze van toezicht op telecommunicatiedienstverleners. De keuze voor het college sluit ook goed aan bij de keuze van toezichthouders door andere lidstaten van de EG. Meerdere lidstaten wijzen hun nationale telecommunicatietoezichthouder aan als toezichthouder op certificatiedienstverleners die gekwalificeerde certificaten aan het publiek aanbieden of afgeven.

2.8 Overeenstemming veilige middelen met bijlage III

Naast eisen die in bijlage I en II van de richtlijn worden gesteld aan certificatiedienstverleners die gekwalificeerde certificaten afgeven, worden in bijlage III van de richtlijn ook eisen gesteld aan middelen waarmee elektronische handtekeningen door een ondertekenaar worden aangemaakt. Deze middelen bestaan uit hardware of software. Indien deze hardware of software voldoen aan de eisen, die de richtlijn in bijlage III stelt, is sprake van veilige middelen voor het aanmaken van elektronische handtekeningen. De daadwerkelijke overeenstemming van die veilige middelen voor het aanmaken van elektronische handtekeningen met bedoelde eisen moet worden vastgesteld door onafhankelijke instellingen, die door de nationale overheden van de lidstaten worden aangewezen, ingevolge artikel 3, vierde lid, van de richtlijn. De Europese Commissie stelt de criteria vast aan de hand waarvan de lidstaten kunnen bepalen of een instantie voor aanwijzing geschikt is (zie § 2.11). De bevindingen van deze instanties met betrekking tot de overeenstemming met de eisen van bijlage III worden door alle lidstaten erkend. De richtlijn verplicht niet tot het aanwijzen van een dergelijke instelling; de afgegeven verklaring van overeenstemming door een door een lidstaat aangewezen instelling volstaat.
Veilige middelen die van buiten de Europese Unie en de Europese Economische Ruimte worden geïmporteerd en waarvan de overeenstemming met de eisen niet voorafgaande aan de invoer door een door een lidstaat aangewezen keuringsinstantie is vastgesteld, moeten na de invoer alsnog worden beoordeeld door een aangewezen keuringsinstantie, en van een verklaring van die instantie worden voorzien.
Het toezicht op de naleving van de regels voor veilige middelen voor het aanmaken van elektronische handtekeningen wordt niet aan het college opgedragen. Het toezicht op de naleving van deze producteisen door de fabrikanten en de keuringsinstanties past niet binnen de deskundigheid die het college heeft. In verband hiermee is in artikel 15.1, eerste lid, onderdeel g, van de Telecommunicatiewet, artikel 18.17 ingevoegd. Afhankelijk van de ontwikkeling van de markt, kan op grond van artikel 18.17 een instantie aangewezen worden.

2.9 Werking andere rechtsgebieden

De richtlijn gaat er blijkens rechtsoverweging 19 van uit dat elektronische diensten ook door de publieke sector zullen worden gebruikt, zowel binnen de ambtelijke diensten van de lidstaten en van de Gemeenschap, als bij de communicatie tussen deze diensten enerzijds en burgers en (andere) economische actoren anderzijds. Daartoe is in dit wetsvoorstel in 3:15c BW een schakelbepaling opgenomen die bepaalt dat buiten het vermogensrecht de bepalingen van de nieuwe afdeling 1A, van titel 1 van Boek 3 BW, overeenkomstige toepassing vinden, voor zover de aard van de rechtshandeling of van de rechtsbetrekking zich daartegen niet verzet. Voor deze schakelbepaling geldt in beginsel hetzelfde als voor de eerdere in Boek 3 opgenomen schakelbepalingen. Zij ziet derhalve primair op privaatrechtelijke verhoudingen buiten de sfeer van het vermogensrecht, maar toepassing op andere rechtsgebieden is niet uitgesloten. Wel ligt in zijn algemeenheid in de aard van een dergelijke bepaling, die beoogt de toepassing van een complex van wettelijke bepalingen mogelijk te maken op gebieden waarvoor deze naar de letter van de wet niet zijn geschreven, besloten dat deze toepassing minder voor de hand zal liggen, naarmate de materie verder afligt van de vermogensrechtelijke rechtsverhoudingen waarvoor de bepalingen zijn geschreven.
Zoals echter blijkt uit de hiervoor weergegeven rechtsoverweging 19 heeft de elektronische handtekening uiteraard een bredere strekking dan enkel de toepassing in het privaatrecht. Gelet daarop zal voor het bestuursrecht en het strafrecht afzonderlijk worden bekeken of en zo ja in welke gevallen rechtsverkeer tussen overheid en burger langs elektronische weg zou kunnen plaatsvinden en of daarvoor aanvullende eisen nodig zijn. Wat betreft het strafrecht is nog in studie in hoeverre wetswijziging of aanvulling nodig is. Derhalve ligt het niet voor de hand de schakelbepaling voor het strafrecht te gebruiken. Voor het bestuursrecht ligt dit anders nu hiervoor een wetsvoorstel wordt voorbereid – dat regelt dat in de Algemene wet bestuursrecht (Awb) wordt bepaald dat elektronische communicatie, voor zover het bestuursorgaan kenbaar heeft gemaakt dat het rechtsverkeer tussen overheid en burger langs elektronische weg kan plaatsvinden, tussen overheidsorganen onderling en tussen overheidsorganen en burgers in beginsel mogelijk is – dat voor wat betreft de elektronische handtekening de bepalingen van het BW van overeenkomstige toepassing verklaart. Derhalve valt niet te verwachten dat er bezwaar bestaat tegen toepassing van de schakelbepaling voor het bestuursrecht zolang de aanvulling van de Awb nog niet tot stand is gekomen.
Op grond van artikel 3, zevende lid, van de richtlijn kunnen lidstaten voor het gebruik van elektronische handtekeningen in de publieke sector echter aanvullende eisen stellen. Deze eisen dienen objectief, transparant, evenredig en niet-discriminerend te zijn en mogen slechts op de specifieke kenmerken van de betrokken toepassing betrekking hebben. Zij mogen evenmin een belemmering vormen voor grensoverschrijdende diensten. In de Algemene wet bestuursrecht zal een bepaling worden opgenomen die het mogelijk maakt bij specifieke wet aanvullende eisen op te nemen voor de publieke sector. Wat het strafrecht betreft zal bestudeerd worden wat de gevolgen zijn voor de strafrechtelijke handhaving in de elektronische omgeving. In de artikelsgewijze toelichting op artikel 15 c wordt nader ingegaan op de mogelijke gevolgen voor het strafrecht en de eventueel te nemen maatregelen.

2.10 Gegevensbescherming

Artikel 8 lid 1 van de richtlijn en rechtsoverweging 24 verplichten certificatiedienstverleners en de met accreditatie of toezicht belaste instanties de wetgeving inzake gegevensbescherming en bescherming van de persoonlijke levenssfeer na te leven om het vertrouwen van de gebruiker in elek-

tronische communicatie en elektronische handel te bevorderen. Artikel 8 lid 2 van de richtlijn bevat verder een zeer strikte regel voor certificatiedienstverleners die certificaten aan het publiek afgeven wat betreft het verkrijgen van persoonsgegevens en het verder verwerken van deze gegevens. Deze bepaling is strikter dan de in de Wet bescherming persoonsgegevens, die naar verwachting begin 2001 in werking zal treden, opgenomen bepalingen op dit punt. Dit artikel is dan ook geïmplementeerd in artikel 11.5a van de Telecommunicatiewet.
Voorts mogen de lidstaten volgens artikel 8 lid 3 van de richtlijn, onverminderd de rechtsgevolgen van pseudoniemen in het nationale recht, niet verhinderen dat certificatiedienstverleners op het certificaat een pseudoniem vermelden in plaats van de werkelijke naam van de ondertekenaar. Hierbij is van belang dat rechtsoverweging 25 expliciet aangeeft dat deze bepaling lidstaten niet belet op grond van communautaire of nationale wetgeving de identificatie van personen te eisen.

2.11 Taken van de Europese Commissie

De Europese Commissie wordt bijgestaan door een Comité voor elektronische handtekeningen (artikel 9 van de richtlijn). Dit comité heeft ingevolge artikel 10 van de richtlijn tot taak om de in de bijlagen opgenomen eisen toe te lichten. Daarnaast stelt het comité de in artikel 3, vierde lid, van de richtlijn bedoelde criteria (criteria aan de hand waarvan de lidstaten bepalen of een instantie geschikt is om aangewezen te worden, om te kunnen bepalen of veilige middelen voor het aanmaken van handtekeningen met de eisen van bijlage III overeenstemmen) alsmede de in artikel 3, vijfde lid, van de richtlijn bedoelde algemene erkende normen voor producten voor elektronische handtekeningen, vast. De Europese Commissie kan ingevolge artikel 3, vijfde lid, referentienummers van algemeen erkende normen voor producten voor elektronische handtekeningen vaststellen en via het Publicatieblad van de Europese Gemeenschappen bekendmaken. Wanneer een product voor elektronische handtekeningen aan dergelijke normen voldoet gaan de lidstaten er van uit dat het met de eisen van bijlage II, punt f, en bijlage III, van de richtlijn in overeenstemming is.
Om de Europese Commissie en het comité in staat te stellen hun taken op een goede manier uit te oefenen, legt artikel 11 van de richtlijn de lidstaten een informatieplicht op om de Europese Commissie en de andere lidstaten te voorzien van informatie. Het betreft informatie over nationale vrijwillige accreditatieregelingen, inclusief eventuele aanvullende eisen voor het gebruik van elektronische handtekeningen in de publieke sector. Voorts dienen de lidstaten de namen en adressen van de nationale instanties die belast zijn met accreditatie en toezicht alsmede de ingevolge artikel 3, vierde lid, van de richtlijn aangewezen instantie die de overeenstemming van veilige middelen voor het aanmaken van elektronische handtekeningen met de eisen van bijlage III vaststelt, mee te delen. Ook de namen en adressen van alle geaccrediteerde nationale certificatiedienstverleners dienen te worden verstrekt.
De Commissie en de lidstaten werken samen om de ontwikkeling en het gebruik van middelen voor het verifiëren van handtekeningen te bevorderen. Zij houden daarbij de in bijlage IV opgenomen aanbevelingen voor het veilig verifiëren van handtekeningen alsmede het belang van de consument voor ogen. Daarnaast zal de Commissie de richtlijn binnen twee jaar na inwerkingtreding evalueren om te waarborgen dat de vooruitgang van de techniek of wijzigingen in het juridische kader geen belemmeringen opwerpen voor de verwezenlijking van de in deze richtlijn vervatte doelstellingen. Van deze evaluatie wordt op grond van artikel 12 van de richtlijn voor 19 juli 2003 verslag uitgebracht aan het Europese Parlement en de Raad.

2.12 Adviezen

Het wetsvoorstel is in de uitvoerende fase voor advies voorgelegd aan de Registratiekamer, het Electronic Commerce Platform Nederland (ECP.NL), het openbaar ministerie (OM), de Nederlandse Vereniging voor Rechtspraak (NVvR), het Permanent Overlegorgaan Post- en Telecommunicatie (OPT) en de Onafhankelijke Post- en Telecommunicatieautoriteit (OPTA).
Het advies van ECP.NL en de uitkomst van de bedrijfseffectentoets luidde positief en gaf geen aanleiding tot aanpassing of wijziging. Naar aanleiding van het advies van de Registratiekamer is artikel 8 lid 2 van de richtlijn in het wetsvoorstel opgenomen.
De NVVR vraagt zich af of de strekking van de richtlijn en in navolging daarvan van dit wetsvoorstel is om een wettelijke basis te creëren voor de elektronische handtekening of dat de richtlijn en het wetsvoorstel ook op elektronische geschriften zien. Het antwoord hierop luidt dat zowel de richtlijn als het wetsvoorstel alleen een wettelijke basis beogen te creëren voor de elektronische handtekening. Dat deze wettelijke regeling ook gevolgen heeft voor elektronische geschriften en de rechtsgevolgen daarvan ligt voor de hand. Als zodanig komt dat onderwerp echter niet in de richtlijn en evenmin in het wetsvoorstel aan de orde.
De NVVR wijst op verschillen tussen artikel 5 van de richtlijn en artikel 3:15a BW dat dit artikel implementeert. Artikel 5 van de richtlijn bevat een tijdens de onderhandelingen moeizaam overeengekomen compromis. Dit artikel veronderstelt in wezen, zoals in § 2.3 van deze toelichting reeds is aangegeven, het bestaan van een algemene norm, inhoudende dat een elektronische handtekening steeds dan als juridisch gelijkwaardig aan een handgeschreven handtekening dient te worden beschouwd indien deze, gelet op alle omstandigheden van het geval, met een voldoende mate van betrouwbaarheid dezelfde functies vervult als een handgeschreven handtekening. Hoewel deze norm in de richtlijn niet expliciet is opgenomen maar impliciet wel wordt verondersteld, is deze algemene norm in artikel 3:15a lid 1 BW opgenomen. Hiermee wordt ook aangesloten bij de mondiale ontwikkelingen op dit gebied, zoals de Model Law on Electronic Commerce van 1996. Artikel 5 van de richtlijn kleurt deze algemene norm in. Ten eerste wordt in artikel 5 lid 1 bepaalt dat indien aan bepaalde voorwaarden is voldaan, een elektronische handtekening voldoet aan de eisen van een handgeschreven handtekening en als bewijsmiddel dient te worden toegelaten. Ten tweede worden in lid 2 criteria genoemd op grond waarvan aan een elektronische handtekening niet louter de rechtsgeldigheid mag worden ontzegd en evenmin op grond daarvan als bewijsmiddel mag worden geweigerd. Artikel 3:15a lid 3 BW is gelijk aan artikel 5 lid 2 van de richtlijn. Artikel 3:15a lid 2 BW is echter toegesneden op de in het eerste lid van dit artikel opgenomen algemene norm, in dier voege dat uitgegaan wordt van een vermoeden van rechtswege dat indien aan de in artikel 5 lid 1 van de richtlijn genoemde voorwaarden is voldaan, de methode die daarbij is gebruikt voor authentificatie voldoende betrouwbaar is.
Het OM adviseerde het wetsvoorstel aan te houden of in de memorie van toelichting dieper in te gaan op de vraag waarom de strafrechtelijke introductie van de elektronische handtekening nu nog niet aan de orde is. Vanwege de implementatie termijn kwam aanhouding niet aan de orde. Bovendien is het wetsvoorstel primair civielrechtelijk van aard. Dat neemt echter niet weg dat ook in het strafrecht wellicht wijzigingen nodig zijn. Deze behoeven evenwel niet gelijktijdig met dit wetsvoorstel tot stand te komen. Naar aanleiding van het advies van het OM is de artikelsgewijze toelichting op artikel 15c uitgebreid met een meer uitvoerige beschouwing over de mogelijke gevolgen voor het strafrecht en de eventueel te nemen maatregelen.
Op grond van artikel 5 van het Informatiestatuut Onafhankelijke Post- en Telecommunicatieautoriteit is bij brief van 27 juli 2000, kenmerk DGTP/00/

03760/EdV, het wetsvoorstel aan de OPTA (verder: het college) voorgelegd. Het college vraagt bij brief van 18 augustus 2000, kenmerk OPTA/N&R/2000/202373 aandacht voor een paar zaken.
Ten eerste acht het college het opnemen van een uitdrukkelijke verbodsbepaling gewenst die bepaalt dat certificatiedienstverleners waarvan de registratie door het college is ingetrokken niet langer gekwalificeerde certificaten mogen aanbieden. Naar het oordeel van het college wordt door de hem in het voorstel gegeven bevoegdheden het gedrag van een certificatiedienstverlener die niet aan de wettelijke eisen voldoet, niet wezenlijk beïnvloedt. Deze certificatiedienstverlener kan, na een nieuwe aanmelding, opnieuw gekwalificeerde certificaten aanbieden, hoewel hij nog steeds niet aan de eisen voldoet. Het college acht het gewenst deze mogelijke vicieuze cirkel te doorbreken door het opnemen van de bedoelde uitdrukkelijke verbodsbepaling. Deze zou met name betrekking moeten hebben op certificatiedienstverleners waarvan de registratie is beëindigd omdat zij niet binnen een gestelde termijn voldoen aan de wettelijke eisen, maar vervolgens certificatiediensten blijven aanbieden alsof zij wel aan de eisen zouden voldoen. Zoals in paragraaf 2.6 over toezicht is aangegeven, betekent opneming van 18.15 in artikel 1, onder 4°, van de Wet op de economische delicten dat strafrechtelijk kan worden opgetreden, niet alleen tegen certificatiedienstverleners die wel zijn geregistreerd maar die gekwalificeerde certificaten aan het publiek aanbieden of afgeven terwijl die niet aan de eisen van de richtlijn voldoen, maar ook tegen niet-geregistreerde certificatiedienstverleners die certificaten als gekwalificeerd aanbieden of afgeven aan het publiek hoewel zij niet aan de richtlijn voldoen.
Het opnemen van een verbodsbepaling is volgens het college naast de strafbepaling gewenst om OPTA in de gelegenheid te stellen een certificatiedienstverlener die geregistreerd is geweest, te blijven volgen. Deze aanbeveling van het college is overgenomen. In de toelichting op artikel 18.18 wordt nader ingegaan op de noodzaak van deze verbodsbepaling.
Ten tweede is het college van mening dat de hoogte van de aan de certificatiedienstverleners op te leggen tarieven voor registratie en toezicht een belemmering kan zijn voor aanbieders van gekwalificeerde certificaten om zich te laten registreren; het college refereert hierbij aan een soortgelijke belemmering die het heeft waargenomen bij de registratie van aanbieders van openbare telecommunicatienetwerken en -diensten. In dit wetsvoorstel wordt aangesloten bij het huidige systeem van tarifering zoals dat wordt gehanteerd voor registratie en toezicht in het kader van de Telecommunicatiewet. Aangezien toezicht op certificatiedienstverleners primair tot doel heeft een vertrouwensbasis te handhaven en in mindere mate tot doel heeft een marktordening te bewerkstelligen, zou op zeker moment een beleidsmatige heroverweging voor certificatiedienstverleners aan de orde kunnen zijn indien de voorziene kosten van toezicht inderdaad een ernstige belemmering zouden gaan vormen voor de toegang tot de markt.
Voorts acht het college het mogelijk dat er situaties zijn waarin het onredelijk zou zijn de registratie in te trekken indien de certificatiedienstverlener ook na het stellen van een termijn blijkt niet aan de eisen te voldoen. Het college beveelt aan dat het college de bevoegdheid krijgt om deze situaties te beoordelen. De suggestie van het college om de bevoegdheid te geven om te kunnen beoordelen of niet-naleving van de wettelijke eisen tot beëindiging van de registratie moet leiden of niet, wordt niet overgenomen. Het college gaat er van uit dat hij bij de ontvangst van de aanvraag van de registratie de daarbij gevoegde informatie, waarin de aanvrager aantoont dat hij aan de eisen voldoet, marginaal mag toetsen. Uit artikel 3 lid 1 van de richtlijn blijkt dat er geen voorafgaande vergunning of andere maatregelen mogen worden opgelegd, die de dienstverlening zou belemmeren. Het is derhalve niet de bedoeling om mogelijk te maken dat OPTA vooraf inhoudelijk beoordeelt of de certificatiedienstver-

lener aan alle vereisten voldoet, en de bevoegdheid zou hebben om de aanvraag te weigeren, om de reden dat OPTA niet is gebleken dat de aanvrager volledig aan de eisen voldoet. Wel moet OPTA een beeld hebben van de aanvrager, en in de overgelegde stukken geen contra-indicaties lezen. Indien dat wel het geval is zal OPTA nadere informatie kunnen inwinnen bij de aanvrager, alvorens tot registratie over te gaan.
Uit de door het college ten aanzien van geregistreerde certificatiedienst-verleners uitgevoerde periodieke routinematige onderzoeken, die in de meeste gevallen bestaan uit een verzoek om een schriftelijke vragenlijst in te vullen en te retourneren, zou moeten blijken of een door het college geregistreerde certificatiedienstverlener voldoet aan de wettelijke eisen of niet. Daarna kan het college handhavend optreden. Het college dient wel de gelegenheid te hebben om te beoordelen of het niet voldoen aan de wettelijke eisen zonder meer kan worden toegerekend aan de certificatie-dienstverlener. Indien dat niet het geval is kan het college besluiten de gestelde termijn waarbinnen de certificatiedienstverlener moet gaan voldoen aan de eisen, te verlengen. Indien daarna nog steeds niet aan de eisen wordt voldaan, behoort de registratie te worden beëindigd. Dit is overeenkomstig de geldende systematiek van artikel 2.2, derde lid van de Telecommunicatiewet. Er is geen aanleiding om van deze systematiek ten behoeve van de certificatiedienstverleners af te wijken.
Aan het OPT is advies gevraagd bij brief van 15 juni 2000, nr. DGTP/00/03297/EdV, met toepassing van artikel 11, tweede lid, onder a, van de Wet advies en overleg verkeer en waterstaat. Naar aanleiding van het advies zijn het wetsvoorstel en de memorie van toelichting op enkele punten aangepast.
Het OPT staat positief tegenover de – in artikel 18.16 geboden – mogelijkheid om door middel van zelfregulering, binnen de wettelijke kaders, uitvoering te geven aan de richtlijn, en binnen die kaders vorm te geven aan de ontwikkeling van de markt voor elektronische handtekeningen.
Het OPT is er een voorstander van dat door middel van accreditatie wordt voorzien in een eerstelijns toezicht, dat een preventief karakter heeft, en dat OPTA een tweedelijnstoezicht houdt, dat een repressief karakter heeft.
Het OPT ziet verder mogelijkheden om meer dan één accrediterende instelling aan te wijzen, en om accrediterende instellingen ook repressief te laten optreden.
Met het oog op de duidelijkheid is ervoor gekozen om, indien certificatie-dienstverleners worden geaccrediteerd, af te gaan op de verleende accreditatie, en dat OPTA, indien er een redelijk vermoeden is dat de certificatiedienstverlener niet aan de wettelijke eisen voldoet, eerst bij de accrediterende instelling inlichtingen gaat vragen over de door die instelling geaccrediteerde certificatiedienstverlener, zo nodig met het verzoek maatregelen te nemen. De bevoegdheid om informatie in te winnen bij de accrediterende instelling is gebaseerd op artikel 18.7 van de Telecommunicatiewet. Vooralsnog wordt ervan uitgegaan dat de accrediterende instellingen geen andere wettelijke toezichttaken opgedragen krijgen dan uit de aanwijzing voortvloeien; een goede samenwerking tussen de instellingen en OPTA is echter onontbeerlijk voor een goed toezicht.
Het OPT heeft voorts ervoor gewaarschuwd dat de registratie niet het karakter mag krijgen van een vergunning. In paragraaf 2.6 is hierop al ingegaan. Anders dan het OPT zijn de ondergetekenden van oordeel dat een registratie wel kan worden ingetrokken indien gebleken is dat de certificatiedienstverlener niet aan de eisen voldoet. Ook is het gewenst een registratieaanvraag van een certificatiedienstverlener waarvan de registratie onlangs is beëindigd omdat hij niet aan de eisen voldeed, te weigeren, indien niet kan worden aangetoond dat men inmiddels wel aan de eisen voldoet.

Dit wetsvoorstel regelt de rechtsgevolgen van elektronische handtekeningen waaronder de gelijkstelling van elektronische handtekeningen aan handgeschreven handtekeningen. Hiermee is één aspect van het elektronisch rechtsverkeer dat een belemmering voor het vrije verkeer van diensten van de informatiemaatschappij tussen EG-lidstaten zou kunnen vormen, geüniformeerd.
Richtlijn nr. 2000/31/EG van het Europees Parlement en de Raad van de Europese Unie van 8 juni 2000 betreffende bepaalde juridische aspecten van de diensten van de informatiemaatschappij, met name de elektronische handel in de interne markt (PbEG L 178, 17 juli 2000), beoogt nog een vijftal belemmeringen van het vrije verkeer van diensten op de informatiemaatschappij op te heffen, onder meer door regelingen betreffende het sluiten van contracten langs elektronische weg en de aansprakelijkheid van dienstverleners die als tussenpersoon optreden. Een wetsvoorstel ter uitvoering van die richtlijn is in voorbereiding en dient voor 17 januari 2002 gereed te zijn.
Verder is reeds in de Nota Wetgeving voor de elektronische snelweg (TK 1997–1998, 25 880) aangekondigd dat een wetsvoorstel zal worden ingediend inzake algemene vermogensrechtelijke bepalingen voor het elektronisch rechtsverkeer.
Een voorstel tot wijziging van de Algemene wet bestuursrecht, waarin wordt voorgesteld verkeer langs elektronische weg tussen burgers en bestuursorganen mogelijk te maken, is in voorbereiding (zie ook 2.9).

ARTIKELEN

ARTIKEL I

A

Artikel 15a

Dit artikel regelt de rechtsgevolgen van het gebruik van elektronische handtekeningen. Lid 4 bepaalt dat onder «elektronische handtekening» wordt verstaan de elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authentificatie. Met «logisch geassocieerd» wordt bedoeld dat de elektronische gegevens en de andere elektronische gegevens zodanige elektronische toegangskenmerken bevatten, dat de computer die deze kenmerken vergelijkt, vaststelt dat zij bij elkaar horen.
Op grond van het eerste lid van dit artikel geldt dat een elektronische handtekening dezelfde rechtsgevolgen heeft als een handgeschreven handtekening mits aan een aantal voorwaarden is voldaan. De methode van authentificatie dient voldoende betrouwbaar te zijn. De mate van betrouwbaarheid dient te worden beoordeeld aan de hand van het doel waarvoor de elektronische gegevens werden gebruikt en alle overige omstandigheden van het geval.
Voldoende betrouwbaarheid wordt op grond van het tweede lid, behoudens tegenbewijs, verondersteld indien gebruik is gemaakt van een geavanceerde elektronische handtekening gebaseerd op een gekwalificeerd certificaat en aangemaakt met een veilig middel.
Het derde lid geeft aan op welke grond een methode in elk geval niet als onvoldoende betrouwbaar kan worden aangemerkt. Gelet op de werking van het eerste lid zal het derde lid vooral consequenties kunnen hebben

voor de bewijslastverdeling in het kader van het eerste lid en voor de motiveringsplicht van de rechter.
Het vijfde lid van artikel 15a definieert het begrip «ondertekenaar». Dit is de persoon die een middel voor het aanmaken van elektronische handtekeningen als bedoeld in artikel 1.1, onderdeel ff Telecommunicatiewet gebruikt.
Uit dit systeem vloeit voort dat vele soorten elektronische handtekeningen gelijkwaardig aan een handgeschreven handtekening op een papieren drager kunnen zijn, mits de methode van authentificatie gelet op het doel waarvoor de elektronische gegevens werden gebruikt, voldoende betrouwbaar is. Het zesde lid brengt hierbij tot uitdrukking dat partijen bij overeenkomst een hoger of een lager betrouwbaarheidsniveau dan dat van lid 2 kunnen overeenkomen voor juridische gelijkstelling van een elektronische handtekening aan een handgeschreven handtekening. Dit is in lijn met hetgeen in het algemene deel van deze toelichting, onder § 2.3, ten aanzien van artikel 5 van de richtlijn is vermeld. In dat geval zal door uitleg van de overeenkomst, in het licht van het doel waarvoor de elektronische gegevens werden gebruikt, de aard van de transactie en alle overige omstandigheden van het geval bepaald moeten worden of de gebruikte methode van authentificatie voldoet aan hetgeen partijen hieromtrent zijn overeengekomen.

Artikel 15b

Dit artikel regelt de erkenning van gekwalificeerde certificaten die buiten de EG of de EER zijn uitgegeven. Op grond van het Besluit van het Gemengd Comité van de EER nr. 66/2000 van 2 augustus 2000 tot wijziging van bijlage XI (Telecommunicatiediensten) bij de EER-overeenkomst geldt de richtlijn ook voor de EER. De betreffende certificaten worden binnen de EG of EER erkend als een door een binnen de EG of EER gevestigde certificatiedienstverlener afgegeven gekwalificeerd certificaat indien aan een van de drie in dit artikel gegeven omstandigheden is voldaan:
– de certificatiedienstverlener voldoet aan de in richtlijn nr. 99/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG L 13) gestelde eisen en is binnen een EG- of EER-staat op vrijwillige basis geaccrediteerd, of
– een in de EG of EER gevestigde certificatiedienstverlener die voldoet aan de eisen van richtlijn nr. 99/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen (PbEG L 13), stelt zich borg voor dit certificaat, of
– het certificaat danwel de certificatiedienstverlener is erkend in het kader van een bilaterale of multilaterale overeenkomst tussen de EG of EER en derde landen of internationale organisaties.

Artikel 15 c

Door deze schakelbepaling gelden de bepalingen over de rechtsgevolgen van de elektronische handtekening, opgenomen in boek 3 van het BW onder een nieuwe afdeling 1A «Elektronisch vermogensrechtelijk rechtsverkeer» in beginsel ook voor andere rechtsgebieden voor zover de aard van de rechtsbetrekking zich daartegen niet verzet. Voor een nadere uitleg zij verwezen naar § 2.9 Algemeen deel van deze toelichting. Daar is ook aangegeven dat wat betreft het gebruik van elektronische handtekeningen in de publieke sector aanvullende eisen kunnen worden gesteld op grond van artikel 3 lid 7 van de richtlijn. In het in voorbereiding zijnde wetsvoorstel inzake de Algemene wet bestuursrecht waarin wordt geregeld dat elektronische communicatie – voor zover het bestuursorgaan kenbaar heeft gemaakt dat het rechtsverkeer tussen overheid en burger langs

elektronische weg kan plaatsvinden – tussen overheidsorganen onderling en tussen overheidsorganen en burgers in beginsel mogelijk is, wordt voorzien in een bepaling die het mogelijk maakt bij specifieke wet aanvullende eisen in de zin van de richtlijn op te nemen.
De Awb is in beginsel niet van toepassing op het rechtsverkeer van de burger in de sfeer van het strafrecht (artikel 1:6 Awb). Zoals aangegeven in § 2.9 wordt voor dat rechtsverkeer afzonderlijk bekeken of en zo ja in welke gevallen rechtsverkeer tussen overheid en burger langs elektronische weg zou kunnen plaatsvinden en of daarvoor aanvullende eisen nodig zijn. Zo zal worden bezien of het nodig is een wettelijke voorziening te treffen voor de gevallen waarin de verdachte of zijn raadsman langs elektronische weg een rechtsmiddel wil instellen. Voor wat betreft het opmaken van formele stukken in het kader van het strafrecht wordt afzonderlijk bekeken of het gewenst is dat een proces verbaal langs elektronische weg kan worden opgemaakt en ingezonden, welke eisen ter zake van betrouwbaarheid en vertrouwelijkheid daarbij gesteld moeten worden en welke praktische consequenties dit heeft voor bijvoorbeeld computerprogrammatuur en -apparatuur.
Nu wetgeving tot stand komt die tot doel heeft het vertrouwen in en de aanvaarding van de elektronische handtekening te bevorderen, vormt de vraag welke gevolgen deze wetgeving kan hebben voor de mogelijkheden voor strafrechtelijke handhaving in een elektronische omgeving een punt van aandacht. Voor de instanties die zijn belast met de opsporing van strafbare feiten is het van belang dat zij in bepaalde gevallen informatie kunnen verkrijgen over de persoon die aan een bepaalde elektronische handtekening verbonden is. Om die reden zal worden bezien of de bestaande bevoegdheden in het Wetboek van Strafvordering hiervoor een toereikende basis bieden.
Het openbaar ministerie werpt in zijn advies over het wetsvoorstel de vraag op of het wetsvoorstel aanleiding geeft tot een aanpassing van de artikelen 225 en 226 Sr betreffende valsheid in geschrifte. Ik ben van mening dat dit niet het geval is. De term «geschrift» leent zich voor moderne toepassingen (vgl. Noyon, Langemeijer, Remmelink, Het Wetboek van Strafrecht, artikel 113, aant. 5 en Th. de Roos, G. Schuijt en L. Wissing, Smaad, laster, discriminatie en porno op het Internet, Alphen aan den Rijn/Diegem 1996). In de memorie van toelichting bij het wetsvoorstel computercriminaliteit II is daarom geconcludeerd dat op dit punt de rechtsontwikkeling kan worden afgewacht (Kamerstukken II 1998/99, 26 671, nr. 3, blz. 7).
Gelet op de civielrechtelijke aard en de strekking van de richtlijn, kunnen eventuele aanpassingen van het bestuursrecht en het strafrecht afzonderlijk tot stand komen en behoeven deze niet noodzakelijkerwijs gelijktijdig met dit wetsvoorstel gerealiseerd te worden.

B

Artikel 196b

Dit artikel betreft de aansprakelijkheid van certificatiedienstverleners die gekwalificeerde certificaten uitgeven aan het publiek, of voor een zodanig certificaat instaan, voor schade die door personen die in redelijkheid op dit certificaat hebben vertrouwd, is geleden als gevolg van de in het artikel genoemde omstandigheden. Dit artikel legt derhalve een gekwalificeerde schuldaansprakelijkheid op de certificatiedienstverlener, met omgekeerde bewijslast. Indien de desbetreffende certificatiedienstverlener aan kan tonen dat hij niet nalatig heeft gehandeld, is hij van zijn aansprakelijkheid ontheven. De certificatiedienstverlener is aansprakelijk voor de volgende, in lid 1 en 2 opgesomde, omstandigheden:
– de juistheid, op het tijdstip van afgifte, van alle gegevens in het gekwa-

lificeerde certificaat en de opneming in het gekwalificeerde certificaat van alle voor een dergelijk certificaat voorgeschreven gegevens;
– de garantie dat de in het gekwalificeerd certificaat geïdentificeerde ondertekenaar, op het tijdstip van de afgifte van het certificaat, houder was van de gegevens voor het aanmaken van de handtekening, die met de in het certificaat gegeven of geïdentificeerde gegevens voor het verifiëren van een handtekening overeenstemmen;
– de garantie dat de gegevens voor het aanmaken van de handtekening en die voor het verifiëren van de handtekening, – ingeval zij beide door de certificatiedienstverlener werden gegenereerd –, complementair (private en publieke sleutel zijn op elkaar afgestemd) kunnen worden gebruikt;
– het niet registreren van de intrekking van het certificaat.

De leden 3 en 4 bepalen wanneer de certificatiedienstverlener in elk geval niet aansprakelijk is.
De functie van de woorden «aan het publiek» is de volgende. De ratio van dit artikel is gelegen in het wekken van het vertrouwen jegens personen dat op het uitgegeven certificaat kan worden vertrouwd en dat een deugdelijke aansprakelijkheid is geregeld als er iets mis mocht gaan. Dit laat onverlet dat partijen bij overeenkomst ten opzichte van elkaar hiervan af mogen wijken. Dit valt ook af te leiden uit rechtsoverweging 16 van de richtlijn waarin staat dat er geen behoefte bestaat aan een regelgevend kader voor elektronische handtekeningen die uitsluitend worden gebruikt in systemen die berusten op vrijwillige privaatrechtelijke overeenkomsten tussen een vastgesteld aantal deelnemers.
De beantwoording van de vraag of een certificaat is afgegeven aan het publiek, hangt niet alleen er van af of een certificaat is afgegeven aan een ondertekenaar die behoort tot een groep waarvan de omvang beperkt is, bijvoorbeeld door overeenkomsten met de certificatiedienstverlener voor andere dienstverlening. Het hangt ook af van het toepassingsgebied waarvoor het certificaat is afgegeven. Indien een certificaat is afgegeven binnen een besloten groep, maar ook buiten die groep kan worden gebruikt, moet het certificaat worden beschouwd als te zijn afgegeven aan het publiek omdat het toepassingsgebied niet beperkt is tot de besloten groep. Duidelijkheid omtrent het beoogde toepassingsgebied kan worden gegeven in het certificaat zelf. Uit de eisen waaraan gekwalificeerde certificaten moeten voldoen (bijlage I van de richtlijn) volgt dat op het certificaat moet worden aangegeven dat het om een gekwalificeerd certificaat gaat en of er eventuele beperkingen zijn betreffende het gebruik van het certificaat. Indien er geen beperkingen zijn aangebracht in het toepassingsbereik (waarmee niet bedoeld wordt de waarde) fungeert het certificaat als een aan het publiek afgegeven certificaat. Alleen certificaten die zijn afgegeven aan een contractueel of anderszins door de certificatiedienstverlener beperkte groep, en waarvan bovendien het toepassingsgebied (voor derden kenbaar) beperkt is tot die groep, kunnen als certificaten worden aangemerkt die niet aan het publiek zijn afgegeven.

ARTIKEL II

A

Artikel 1.1

In artikel 1.1 zijn de benodigde begripsomschrijvingen uit artikel 2 van de richtlijn betreffende elektronische handtekeningen opgenomen.
Een belangrijke omschrijving is die van «certificatiedienstverlener». Een certificatiedienstverlener wordt in de praktijk ook vaak aangeduid met het begrip «Trusted Third Party». Een certificatiedienstverlener geeft certificaten uit in verband met elektronische handtekeningen. Naast de afgifte

van certificaten kan een certificatiedienstverlener nog andere diensten leveren die in verband staan met elektronische handtekeningen. Deze andere diensten hebben onder meer betrekking op: het beheer van afgegeven certificaten; het genereren, opslaan, verstrekken, of het vernietigen van cryptografisch sleutelmateriaal (sleutelbeheer); het onweerlegbaar aantonen van verzending en ontvangst van elektronische berichten en het bewaren en tijdstempelen van elektronische berichten.
De begripsomschrijving van een veilig middel voor het aanmaken van handtekeningen alsmede de begripsomschrijving van een gekwalificeerd certificaat zijn nodig omdat deze begrippen zowel in de wet als in de op basis van de artikelen 18.15 en 18.17 op te stellen algemene maatregel van bestuur worden gebruikt.

B

Artikel 2.1

De richtlijn bepaalt dat de lidstaten dienen te zorgen voor een passend systeem voor toezicht op de op hun grondgebied gevestigde certificatiedienstverleners die gekwalificeerde certificaten aan het publiek afgeven. Om invulling aan het toezicht te geven is het noodzakelijk dat deze certificatiedienstverleners bij de toezichthouder (het college) bekend zijn. Bij het verzoek om registratie legt de certificatiedienstverlener informatie over waaruit blijkt dat wordt voldaan aan de richtlijneisen, die in de Nederlandse regelgeving bij of krachtens algemene maatregel van bestuur zijn vastgesteld. Het college beoordeelt de bij de aanvraag voor registratie meegezonden informatie op volledigheid en onderzoekt slechts of daadwerkelijk aan de aan de certificatiedienstverlener gestelde eisen is voldaan indien het college een redelijk vermoeden heeft dat het tegendeel het geval is. Dit vermoeden kan bij geregistreerde certificatiedienstverleners rijzen op basis van klachten van het publiek, of op basis van onduidelijkheden die ook na schriftelijke vragen door OPTA blijven bestaan. Als vastgesteld wordt dat de certificatiedienstverlener niet (meer) aan de eisen voldoet, kan het college een termijn stellen waarbinnen de certificatiedienstverlener in de gelegenheid wordt gesteld alsnog aan de eisen te voldoen.
Na het verlopen van een gestelde termijn, of indien daarvoor in het niet voldoen aan de eisen direct aanleiding wordt gevonden, wordt de registratie beëindigd. Zo lang hij niet is geregistreerd mag de certificatiedienstverlener geen gekwalificeerde certificaten (meer) aan het publiek afgeven.
Aan artikel 2.1 is een derde en vierde lid toegevoegd voor de registratie van certificatiedienstverleners omdat deze verschilt van de registratie van aanbieders van openbare telecommunicatienetwerken en -diensten. Certificatiedienstverleners voldoen namelijk niet in alle gevallen aan de definitie van aanbieders van telecommunicatienetwerken of -diensten. De Telecommunicatiewet geeft juist regels voor de geregistreerde aanbieders van telecommunicatienetwerken ofdiensten. De registratie van artikel 2.1, eerste lid van de Telecommunicatiewet is daardoor een andere dan die van de certificatiedienstverleners, en moet daarvan uitdrukkelijk worden onderscheiden. Het administratieve gedeelte van de registratie is echter in hoge mate gelijk aan de registratie van aanbieders van openbare telecommunicatienetwerken en -diensten. Bij de registratie wordt een vast bedrag in rekening gebracht; de variabele kosten van het daadwerkelijke toezicht (behandeling van klachten en in voorkomend geval beoordelen van certificatiedienstverleners op voldoen aan eisen; handhavend optreden) worden over de betrokken bedrijven die als certificatiedienstverleners staan geregistreerd omgeslagen. Gelet op de aard van de bedrijven, instellingen en beroepsbeoefenaars die gekwalificeerde certificaten aan het publiek (zullen gaan) aanbieden, zoals banken,

IT-dienstverleners, postbedrijven, notarissen en telecommunicatiedienstverleners, heeft de verwachte hoogte van de omgeslagen kosten, geschat enige tienduizenden guldens per jaar per certificatiedienstverlener, geen invloed op de concurrentiepositie van die bedrijven of op de mogelijkheden van andere bedrijven om tot de markt van certificatiedienstverlening toe te treden.
Het betreft een nieuwe activiteit die, doordat betrouwbare elektronische communicatie aan belang wint, een verschuiving in de communicatie van papier naar netwerk laat zien, met de daarmee gepaard gaande verschuiving van werkzaamheden. «Voor een meer uitgebreide toelichting op dit artikel zij verwezen naar paragraaf 2.6 «Toezicht op certificatiedienstverleners die gekwalificeerde certificaten aan het publiek afgeven».

C

Artikel 2.2

Artikel 2.2 is aangepast aan de registratie van certificatiediensten. Er is een nieuw onderdeel f aan het derde lid toegevoegd, waarin als beëindigingsgrond van de registratie wordt verwezen naar de situatie waarin een geregistreerde certificatiedienstverlener (ook na het stellen van een termijn) niet voldoet aan de bij algemene maatregel van bestuur gestelde eisen. Het stellen van een termijn wordt noodzakelijk geacht in verband met de mogelijke niet-naleving van bepaalde vereisten die de betrouwbaarheid van een gekwalificeerd certificaat niet direct in twijfel trekken. Het (tijdelijk of incidenteel) niet naleven van een dergelijke vereiste betekent niet zonder meer dat het certificaat tussen de partijen die het gebruiken onbetrouwbaar is geworden, noch dat de registratie van de certificatiedienstverlener die het gekwalificeerde certificaat heeft aangeboden of afgegeven zonder meer moet worden ingetrokken. Hiermee is ook de administratieve belasting gediend; als de tekortkoming binnen de door het college gestelde termijn wordt weggenomen, is er geen aanleiding om een nieuwe registratie te verlangen.

D

Artikel 11.5a

Dit artikel voert artikel 8 lid 2 van de richtlijn uit en bevat strikte voorschriften voor certificatiedienstverleners die certificaten aan het publiek afgeven voor het verkrijgen en verwerken van persoonsgegevens. Deze gegevens mogen enkel worden verkregen van de betrokkene zelf of met diens uitdrukkelijke toestemming en slechts voor zover de afgifte en het beheer van het certificaat dit vereisen. Verdere verwerking van deze gegevens, zoals het opmaken en versturen van nota's, is enkel toegestaan indien de betrokkene daarvoor uitdrukkelijk toestemming heeft gegeven. Implementatie van deze bepaling is nodig omdat het verder gaat dan de bepalingen over het verwerken en verkrijgen van persoonsgegevens in de Wet bescherming persoonsgegevens (Wbp), die naar verwachting begin 2001 in werking zal treden.
De regel dat uitdrukkelijke toestemming is vereist van de betrokkene lijdt alleen uitzondering indien het verwerken van de bij de certificatiedienstverlener bekende gegevens van deze betrokkene noodzakelijk is voor het opsporen van fraude, en in die gevallen dat de medewerking van de certificatiedienstverlener op grond van een bij of krachtens de wet gegeven bevoegdheid wordt gevorderd.

E

Artikel 15.1

Artikel 15.1 voorziet in de toedeling aan toezichthouders van onderwerpen benoemd in de Telecommunicatiewet. In het eerste lid vindt de aanwijzing plaats van de onder de Minister van Verkeer en Waterstaat ressorterende toezichtstaken. Het toezicht op de accreditatieorganisaties met betrekking tot de naleving van de aangewezen accreditatieregelingen is niet aan het college opgedragen.
Ook het toezicht op de naleving van de eisen voor veilige middelen wordt, zoals in het algemeen deel van de memorie, paragraaf 2.8, is aangegeven, niet aan het college opgedragen. In verband hiermee zijn de artikelen 18.16 en 18.17 opgenomen in artikel 15.1, eerste lid. De overige toezichtstaken genoemd in dit wetsvoorstel ressorteren, krachtens het bepaalde in artikel 15.1, derde lid, bij het college.

F

Artikel 18.15

In Hoofdstuk 18 is een viertal artikelen ingevoegd waarin onder andere de materiële eisen voor certificatiedienstverleners en veilige middelen zijn geregeld.
Daartoe wordt in artikel 18.15, eerste lid, bepaald dat certificatiedienstverleners die gekwalificeerde certificaten aan het publiek afgeven aan de bij of krachtens algemene maatregel van bestuur gestelde eisen moeten voldoen, zijnde de eisen van bijlage II van de richtlijn, en in het tweede lid dat gekwalificeerde certificaten aan de bij of krachtens algemene maatregel van bestuur moeten voldoen, zijnde de eisen van bijlage I van de richtlijn. De keuze voor implementatie in lagere regelgeving is ingegeven door de snelle technologische vooruitgang. Deze technologische ontwikkelingen vragen om regelgeving die gelijke tred hiermee kan houden. Nu de bijlagen vooral technische eisen bevatten, bestaat geen bezwaar om deze eisen in lagere regelgeving op te nemen. Voorts zal bij ministeriële regeling door ondergetekenden worden voorzien in de standaarden die worden gebruikt voor het bepalen van conformiteit aan de richtlijn.
Ingevolge de richtlijn moeten alle gekwalificeerde certificaten aan de eisen van bijlage I voldoen. De richtlijn schrijft echter voor dat er alleen toezicht wordt gehouden op certificatiedienstverleners die gekwalificeerde certificaten aan het publiek afgeven. De eisen die de richtlijn stelt aan gekwalificeerde certificaten zijn niet beperkt tot de gekwalificeerde certificaten die aan het publiek worden aangeboden of afgegeven door certificatiedienstverleners die geregistreerd zijn en aan de eisen van bijlage II van de richtlijn voldoen.
In artikel 18.15, derde lid, is een identificatieplicht opgenomen. Deze plicht is nodig voor de certificatiedienstverlener die gekwalificeerde certificaten afgeeft aan het publiek om te kunnen verifiëren of de persoon die een elektronische handtekening aanvraagt ook degene is, die hij beweert te zijn. Deze bepaling dient ter implementatie van de in bijlage II van de richtlijn opgenomen eis dat een certificatiedienstverlener de identiteit van de persoon aan wie een gekwalificeerd certificaat wordt afgegeven, natrekt.

Artikel 18.16

De richtlijn bepaalt dat lidstaten zogenoemde vrijwillige accreditatieregelingen kunnen invoeren of handhaven die op verbetering van de certificatiediensten zijn gericht. In feite worden hier certificatieregelingen bedoeld zoals omschreven in de Memorie van Toelichting op de Telecommuni-

catiewet, algemeen deel, paragraaf 9.1 (zie Kamerstukken II, 1996–1997, 25 533, nr. 3). In dit voorstel wordt echter aangesloten bij de terminologie van de richtlijn en wordt de term «accreditatie» gebruikt. Een accreditatieregeling bestaat minimaal uit de volgende componenten: normen en standaarden waaraan de certificatiedienstverlener moet voldoen om onder deze regeling geaccrediteerd te worden; eisen die worden gesteld aan de instanties die certificatiedienstverleners beoordelen en accrediteren; de algemene procedures die worden gevolgd om te komen tot een accreditatie, zoals de beslissing tot accreditatie, de periodieke controles en eventuele intrekking van een accreditatie. Het vrijwillige element is dat een certificatiedienstverlener die gekwalificeerde certificaten aan het publiek af wil geven zelf kan bepalen of hij zich onder een dergelijke regeling wil laten accrediteren. De voorwaarden van dergelijke accreditatieregelingen dienen objectief, transparant, evenredig en niet-discriminerend te zijn.
Vrijwillige accreditatieregelingen kunnen een belangrijke rol spelen om vertrouwen te krijgen in elektronische communicatie en elektronische handtekeningen. Zij zijn van oudsher privaatrechtelijke regelingen met een groot maatschappelijk draagvlak.
In dit voorstel wordt mogelijk gemaakt dat de Minister van Verkeer en Waterstaat een organisatie aanwijst, indien deze een accreditatieregeling toepast die voldoende waarborgen biedt dat de op basis van deze regeling geaccrediteerde certificatiedienstverleners voldoen aan de eisen die op grond van dit wetsvoorstel aan gekwalificeerde certificaten die aan het publiek worden afgegeven, worden gesteld. Door in het wetsvoorstel deze mogelijkheid te bieden, kan de overheid het afnemen van diensten van certificatiedienstverleners die zijn geaccrediteerd in het kader van die regeling, stimuleren. In een accreditatieregeling draagt een accrediterend instituut er zorg voor dat een certificatiedienstverlener steeds zal voldoen aan de voorwaarden die aanvankelijk aanleiding waren om tot accreditatie over te gaan. Hierdoor ontstaat er een keuzemogelijkheid in de markt voor certificatiedienstverleners die onder een dergelijke accreditatieregeling vooraf door een onafhankelijke derde, het certificerend instituut, zijn getoetst. De door de Minister aangewezen accreditatieorganisaties waarborgen dat de onder hun regeling geaccrediteerde certificatiedienstverleners aan de richtlijn en de eigen regels van de accreditatieregeling voldoen. Zij zijn echter niet te beschouwen als toezichthouder in de zin van de wet, maar kunnen door hun borgende rol wel een belangrijke functie vervullen bij de invulling van het toezicht.
Indien er klachten zouden zijn over het functioneren van een certificatiedienstverlener vallend onder een door de Minister aangewezen accreditatieregeling, ligt het voor de hand dat het college afstemt met de accreditatieorganisatie van die vrijwillige accreditatieregeling omtrent de afhandeling van een klacht en zoveel mogelijk handelt met inachtneming van de reeds binnen de accreditatieregeling aanwezige zelfreguleringsinstrumenten.

Artikel 18.17

Zoals in paragraaf 2.8 «Overeenstemming veilige middelen met bijlage III» al is aangeduid, wordt de overeenstemming van veilige middelen met de vereisten van bijlage III van de richtlijn vastgesteld door onafhankelijke instellingen. Deze instellingen moeten door Lidstaten worden aangewezen. Om te voorkomen dat er in een lidstaat geen instelling is die de overeenstemming van veiligheidsmiddelen met de vereisten kan vaststellen en om de handel tussen de lidstaten in veilige middelen niet te belemmeren, zijn de door de aangewezen onafhankelijke instellingen afgegeven verklaringen van overeenstemming geldig binnen de hele Gemeenschap. In verband hiermee is aan de Minister van Verkeer en Waterstaat de bevoegdheid gegeven om een onafhankelijke instelling aan

te wijzen, die vaststelt of het middel voor het aanmaken van elektronische handtekeningen, dat hardware of software of een combinatie daarvan kan zijn, voldoet aan de bij of krachtens algemene maatregel van bestuur gestelde eisen, zijnde de eisen van bijlage III van de richtlijn.
Degene die de veilige middelen op de markt brengt, is verantwoordelijk voor de naleving van de in artikel 18.17 bedoelde produkteisen. Hij mag, met andere woorden, de veilige middelen niet op de markt brengen, indien niet aan alle eisen van het eerste en het derde lid is voldaan.
Het vijfde lid voert de in artikel 3, vierde lid, tweede volzin, van de richtlijn opgenomen eis uit. De aangewezen instellingen dienen te voldoen aan de door de Europese Commissie, volgens de procedure van artikel 9 van de richtlijn, vastgestelde criteria. Deze criteria zijn neergelegd in de beschikking van de Europese Commissie van 6 november 2000, nr. C (2000) 3179 def. betreffende de minimumcriteria die de lidstaten in acht moeten nemen bij de aanwijzing van instanties overeenkomstig artikel 3, vierde lid, van de richtlijn.

Artikel 18.18

Niet-geregistreerde certificatiedienstverleners mogen geen gekwalificeerde certificaten aan het publiek aanbieden of afgeven op grond van artikel 2.1, derde lid, van de Telecommunicatiewet. Op de naleving van dit verbod door niet-geregistreerde certificatiedienstverleners ziet het college niet toe: het wordt strafrechtelijk gehandhaafd op grond van artikel 1, onder 2°, van de Wet op de economische delicten. Indien de registratie van een certificatiedienstverlener is beëindigd omdat hij, ook na een door het college gegeven periode, niet aan alle eisen van artikel 18.15 of artikel 18.17 van de Telecommunicatiewet voldoet, is de certificatiedienstverlener niet meer gerechtigd gekwalificeerde certificaten aan het publiek aan te bieden of af te geven. Ten behoeve van een efficiënte handhaving is het gewenst om het college te belasten met het toezicht op deze groep van niet meer geregistreerde certificatiedienstverleners. De naleving van het verbod dat in het eerste lid van artikel 18.18 is opgenomen, wordt ingevolge artikel 15.1, derde lid, van de Telecommunicatiewet door het college met bestuurlijke handhavinginstrumenten gehandhaafd. Hiermee wordt voorkomen, dat door problemen bij de dossieroverdracht of door het stellen van andere prioriteiten bij de onderscheiden diensten de kennis over de niet meer geregistreerde certificatiedienstverlener niet optimaal gebruikt wordt. Dit is van belang om onmiddellijk in actie te kunnen komen als deze certificatiedienstverlener toch gekwalificeerde certificaten aanbiedt of afgeeft. Maar ook als de certificatiedienstverlener opnieuw een aanvraag voor registratie bij het college zou willen indienen, is het van groot belang dat het college de bevoegdheid heeft om de certificatiedienstverlener in de periode na het beëindigen van de registratie te volgen. Artikel 18.18 wordt niet opgenomen in de Wet op de economische delicten, omdat zoals reeds aangegeven al strafrechtelijk kan worden opgetreden tegen certificatiedienstverleners die gekwalificeerde certificaten aanbieden of afgeven.

ARTIKEL III

Overeenkomstig de systematiek van de Telecommunicatiewet worden handelingen in strijd met de artikelen 2.1, derde lid, eerste volzin, 18.15, eerste en tweede lid en 18.17, eerste en derde lid, van de Telecommunicatiewet als economisch delict aangemerkt. Van de gelegenheid is gebruik gemaakt om de bestaande verwijzing naar artikel 2.1, eerste lid, te beperken tot de eerste volzin van dat eerste lid. Met een verwijzing naar

de eerste volzin kan voor het eerste lid van artikel 2.1 worden volstaan, omdat de tweede en derde volzin niet strafrechtelijk worden gehandhaafd.

De Minister van Justitie,
A. H. Korthals

De Staatssecretaris van Verkeer en Waterstaat,
J. M. de Vries

BIJLAGE

BIJ DE MEMORIE VAN TOELICHTING BEHORENDE BIJ HET VOORSTEL VAN WET HOUDENDE AANPASSING VAN BOEK 3 EN BOEK 6 VAN HET BURGERLIJK WETBOEK, DE TELECOMMUNICATIEWET EN DE WET OP DE ECONOMISCHE DELICTEN INZAKE ELEKTRONISCHE HANDTEKENINGEN TER UITVOERING VAN RICHTLIJN NR. 99/93/EG VAN HET EUROPEES PARLEMENT EN DE RAAD VAN DE EUROPESE UNIE VAN 13 DECEMBER 1999 BETREFFENDE EEN GEMEENSCHAPPELIJK KADER VOOR ELEKTRONISCHE HANDTEKENINGEN (PbEG L 13) (WET ELEKTRONISCHE HANDTEKENINGEN)

Transponeringstabel

Richtlijn betreffende een gemeenschappelijk kader voor elektronische handtekeningen

Artikel 1	Behoeft geen implementatie
Artikel 2	
lid 1: elektronische handtekening	Artikel 3:15a lid 4 van het Burgerlijk Wetboek
lid 2: geavanceerde elektronische handtekening	Artikel 3:15a lid 2 van het Burgerlijk Wetboek
lid 3: ondertekenaar	Artikel 3:15a lid 5 van het Burgerlijk Wetboek
lid 4: gegevens voor het aanmaken van handtekeningen	Behoeft geen implementatie
lid 5: middel voor het aanmaken van handtekeningen	Artikel 1.1, onderdeel ff, Telecommunicatiewet
lid 6: veilig middel voor het aanmaken van handtekeningen	Artikel 1.1, onderdeel gg, Telecommunicatiewet
lid 7: gegevens voor het verifiëren van een handtekening	Behoeft geen implementatie
lid 8: middel voor het verifiëren van een handtekening	Behoeft geen implementatie
lid 9: certificaat	Artikel 1.1, onderdeel cc, Telecommunicatiewet
lid 10: gekwalificeerd certificaat	Artikel 1.1, onderdeel dd, Telecommunicatiewet
lid 11: certificatiedienstverlener	Artikel 1.1, onderdeel ee, Telecommunicatiewet
lid 12: product voor elektronische handtekeningen	Behoeft geen implementatie
lid 13: vrijwillige accreditatie	Behoeft geen implementatie
Artikel 3	
lid 1	Behoeft geen implementatie
lid 2	Artikel 18.16 Telecommunicatiewet
lid 3	Artikel 2.1, derde en vierde lid en artikel 2.2, tweede lid Telecommunicatiewet
lid 4	Artikel 18.17, tweede en derde lid, Telecommunicatiewet
lid 5	Behoeft geen implementatie
lid 6	Behoeft geen implementatie
lid 7	In de Algemene wet bestuursrecht zal een bepaling worden opgenomen die het mogelijk maakt bij specifieke wet aanvullende eisen op te nemen in de zin van de richtlijn
Artikel 4	Behoeft geen implementatie
Artikel 5	Artikel 3:15a van het Burgerlijk Wetboek
Artikel 6	Artikel 6:196b van het Burgerlijk Wetboek
Artikel 7	Artikel 3:15 b van het Burgerlijk Wetboek
Artikel 8 lid 1	
Lid 1	Geïmplementeerd in de Wet bescherming persoonsgegevens, die naar verwachting begin 2001 in werking zal treden
Lid 2	Artikel 11.5a Telecommunicatiewet
Lid 3	Behoeft geen implementatie
Artikel 9	Behoeft geen implementatie

Artikel 10	Behoeft geen implementatie
Artikel 11	Behoeft geen implementatie
Artikel 12	Behoeft geen implementatie
Artikel 13	Behoeft geen implementatie
Artikel 14	Behoeft geen implementatie
Artikel 15	Behoeft geen implementatie
Bijlage I	AmvB
Bijlage II	AmvB
Bijlage III	AmvB
Bijlage IV	Behoeft geen implementatie