Tweede Kamer der Staten-Generaal

2

Vergaderjaar 2001–2002

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 (PpbEG L 13) (Wet elektronische handtekeningen)

Nr. 6

## NOTA NAAR AANLEIDING VAN HET VERSLAG

Ontvangen 12 december 2001

### 1. Inleiding

Met waardering nam ik kennis van de opmerkingen van de fracties die in het verslag aan het woord komen. Het verheugt mij dat de fracties van de PvdA, VVD en D66 kunnen instemmen met de strekking van het wetsvoorstel. De fractie van de PvdA maakte ook een aantal kritische kanttekeningen. Daarop zal ik hieronder uitgebreid ingaan.

### 2. De richtlijn en de uitvoering

*2.1 Verschillende soorten elektronische handtekeningen*

De leden van de fractie van D66 vragen naar aanleiding van het onderscheid dat wordt gemaakt tussen «gewone» elektronische handtekeningen en «geavanceerde» elektronische handtekeningen om voorbeelden wanneer kan worden volstaan met een gewone elektronische handtekening en wanneer deze met meer waarborgen moet zijn omkleed. Bovendien vragen zij zich af wie de status bepaalt en of deze wordt vastgelegd in de contractuele relatie tussen partijen. Voor de gelijkstelling van een elektronische handtekening met een handgeschreven handtekening is ingevolge artikel 3:15a lid 1 van het Burgerlijk Wetboek voldoende dat de methode die daarbij is gebruikt voor authentificatie voldoende betrouwbaar is, gelet op het doel waarvoor de ondertekende elektronische gegevens werden gebruikt en op alle overige omstandigheden van het geval. Dit betekent dat in beginsel zowel een gewone als een geavanceerde elektronische handtekening gelijk kan worden gesteld aan een handgeschreven handtekening, maar dat de vraag of dat in een bepaald geval ten aanzien van een gewone elektronische handtekening daadwerkelijk het geval is, afhangt van de omstandigheden van dat geval. Partijen hebben de vrijheid om zelf te bepalen in welke situatie van welke elektronische handtekening gebruik zal worden gemaakt. Bij onenigheid over de vraag of een in een bepaald geval gebruikte elektronische handtekening in

KST58074
ISSN 0921 - 7371
Sdu Uitgevers
's-Gravenhage 2001

de gegeven omstandigheden voor gelijkstelling in aanmerking komt, zal uiteindelijk de rechter toetsen of de methode van authentificatie voldoende betrouwbaar is. Dit criterium is bewust «open» geformuleerd om de nodige flexibiliteit in het elektronisch rechtsverkeer mogelijk te maken en aldus aan partijen een grote mate van vrijheid te bieden om het voor de tussen hen te gebruiken elektronische handtekening gewenste veiligheids- en betrouwbaarheidsniveau zelf te bepalen.
Nu partijen zelf kunnen bepalen van welke elektronische handtekening gebruik kan worden gemaakt en de handtekening in de on-line wereld net als in de off-line wereld bij een veelheid van – naar aard en belang sterk uiteenlopende – rechtshandelingen gebruikt zal gaan worden, is het lastig om hier concrete voorbeelden te geven wanneer kan worden volstaan met een gewone elektronische handtekening en wanneer deze met meer waarborgen moet zijn omkleed. In algemene zin geldt uiteraard dat verwacht mag worden dat partijen voor eenvoudige transacties aan het gebruik van de meest eenvoudige – en dus goedkoopste – elektronische handtekening (de «gewone» elektronische handtekening) de voorkeur zullen geven, terwijl aan de andere kant het gebruik van een – duurdere – elektronische handtekening die met de meeste waarborgen is omgeven (een geavanceerde elektronische handtekening die is gebaseerd op een gekwalificeerd certificaat en is aangemaakt met een veilig middel) de voorkeur zal genieten voor transacties waarbij in de visie van partijen veiligheid en betrouwbaarheid voorop moeten staan. Tussen deze beide uiteinden bevindt zich een glijdende schaal, waarbij de elektronische handtekening met meer waarborgen zal moeten worden omgeven naarmate het belang van de rechtshandeling toeneemt. Bij de beoordeling van het belang van de rechtshandeling zullen partijen naar verwachting onder meer rekening houden met de hoogte van de economische waarde die met de rechtshandeling is gemoeid. Zo zal bij de koop van een boek of een cd langs elektronische weg doorgaans met het gebruik van een gewone elektronische handtekening kunnen worden volstaan. Bij grotere transacties als het kopen van een huis of een auto langs elektronische weg zal eerder gebruik worden gemaakt van een elektronische handtekening die met de meeste waarborgen is omgeven. Het belang van de transactie wordt in dit verband echter niet uitsluitend in economische termen bepaald. Zo zal het gebruik van een geavanceerde elektronische handtekening ook voor de hand liggen indien de aard van de transactie vereist dat zoveel mogelijk beveiligingsmaatregelen worden getroffen om de integriteit van het bericht te waarborgen, zoals in het geval van langs elektronische weg gegeven juridische of medische adviezen.
Zoals reeds aangegeven, kunnen partijen zelf bepalen welk soort elektronische handtekening zij bij welke rechtshandeling wenselijk achten. Partijen zullen een gemaakte keuze om bewijsredenen in de meeste gevallen in hun contractuele relatie vastleggen. Indien partijen een dergelijke keuze niet hebben gemaakt, zal in geval van een geschil de rechter toetsen of de in feite gebruikte handtekening, gelet op de aard van de transactie en alle overige omstandigheden van het geval, voldoende betrouwbaar is.

De leden van de fractie van D66 zijn met de Raad van State van mening dat een toereikende identiteitscontrole bij de toekenning van een elektronische handtekening van groot belang is. De Raad van State wijst erop dat de richtlijn wel algemene voorwaarden stelt maar geen waarborgen biedt voor de kwaliteit van een toekenningscontrole zoals die bijvoorbeeld kan worden bereikt met biometrische methoden. Hierbij wordt wel aangetekend dat dergelijke methoden vooral worden gebruikt als aan de ondertekening van bepaalde akten bijzondere eisen worden gesteld. De deugdelijkheid van de certificering is in belangrijke mate afhankelijk van de kwaliteit van de toekenningscontrole, die met daarop gerichte voorschriften kan worden bevorderd. Deze leden vragen dan ook of vermeld

zou kunnen worden of (op termijn), en zo ja hoe, zal worden voorzien in de bedoelde toekenningscontrole.
Met de leden van de D66-fractie en de Raad van State ben ik van mening dat de identiteitscontrole bij toekenning van een gekwalificeerd certificaat van groot belang is. Het wetsvoorstel voorziet dan ook, in navolging van de richtlijn alleen voor een geavanceerde elektronische handtekening die is gebaseerd op een gekwalificeerd certificaat, in een wettelijke identiteitscontrole. De certificatiedienstverlener die een dergelijk certificaat uitgeeft, dient ingevolge artikel 18.15, derde lid, van de Telecommunicatiewet de identiteit van de aanvrager vast te stellen aan de hand van de bij artikel 1 van de Wet op de identificatieplicht aangewezen geldige documenten (bijvoorbeeld een paspoort). De identiteitsvaststelling geschiedt derhalve op dezelfde wijze als in de off-line wereld. Dit laat onverlet dat certificatiedienstverleners daarenboven gebruik kunnen maken van biometrie. De waarborg voor de kwaliteit van de toekenning is niet primair gelegen in een extra mogelijkheid (biometrie) om de identiteit te controleren. De in artikel 1 van de Wet op de identificatieplicht voorgeschreven documenten bieden daarvoor, net als bij andere identiteitscontroles, (voorlopig) voldoende mogelijkheden. De waarborgen voor de kwaliteit liggen veel meer bij het toezicht door de Onafhankelijke Post- en Telecommunicatieautoriteit (verder OPTA) op de juiste uitvoering van deze voorgeschreven identiteitscontroles alsmede op de uitvoering van de overige eisen waaraan de certificatiedienstverlener op grond van artikel 18.15, eerste en tweede lid, van de Telecommunicatiewet dient te voldoen.
Uit het bovenstaande vloeit voort dat van biometrie nog geen gebruik kan worden gemaakt bij de identiteitscontrole in het kader van de toekenning van gekwalificeerde certificaten. Van biometrie kan wel gebruik worden gemaakt door een certificatiedienstverlener bij het koppelen van een elektronische handtekening aan een aanvrager (fingerprint, irisscan). Daarmee wordt de persoonsgebondenheid van de door hem uitgegeven elektronische handtekening verhoogd en kan derhalve beter worden voorkomen dat de elektronische handtekening door een derde wordt misbruikt.

*2.2 Verschillende soorten certificaten*

De leden van de VVD-fractie vragen waarom de richtlijn onderscheid maakt tussen gewone en gekwalificeerde certificaten. Het onderscheid tussen een gewoon en een gekwalificeerd certificaat vloeit voort uit het verschil in de richtlijn tussen een gewone en een geavanceerde elektronische handtekening. Bij beide elektronische handtekeningen kan gebruik worden gemaakt van een certificaat. Een 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. In de richtlijn wordt echter één soort elektronische handtekening, namelijk de geavanceerde elektronische handtekening die is gebaseerd op een gekwalificeerd certificaat en die is aangemaakt met een veilig middel, en die daardoor bijzondere waarborgen biedt op het punt van veiligheid en betrouwbaarheid, in elk geval volledig gelijkgesteld aan een handgeschreven handtekening. Het certificaat waarmee deze elektronische handtekening wordt aangemaakt is met meer waarborgen omkleed. Een dergelijk gekwalificeerd certificaat dient te voldoen aan de eisen die zijn opgenomen in bijlage I van de richtlijn en dient te zijn afgegeven door een certificatiedienstverlener die voldoet aan de vereisten van bijlage II van de richtlijn.
De leden van de VVD-fractie vragen voorts in hoeverre een gewoon certificaat met voldoende waarborgen is omkleed. Aan de vereisten van een gewoon certificaat is voldaan zolang het een elektronische bevestiging bevat die gegevens voor het verifiëren van een handtekening aan een bepaalde persoon verbindt en de identiteit van die persoon bevestigt. Of

een dergelijk certificaat met voldoende waarborgen is omkleed, zal afhangen van het doel waarvoor de elektronische gegevens werden gebruikt en alle overige omstandigheden van het geval. Indien partijen bijvoorbeeld zijn overeengekomen dat gebruik mag worden gemaakt van een elektronische handtekening gebaseerd op een gewoon certificaat zal in beginsel sprake zijn van voldoende waarborgen. Van elektronische handtekeningen gebaseerd op een gewoon certificaat zal naar verwachting gebruik worden gemaakt bij overeenkomsten die geen hoge economische waarde vertegenwoordigen, zoals het kopen van een boek of cd langs elektronische weg. Niet valt echter uit te sluiten dat van dergelijke elektronische handtekeningen ook gebruik zal worden gemaakt bij transacties die een hogere (economische) waarde vertegenwoordigen.

De leden van de VVD-fractie vragen of de precisering van de technische normen door ETSI en CEN verandering zal aanbrengen in de vrij algemene doelstellingen van de bij de richtlijn behorende bijlagen. De in de bijlagen opgenomen voorschriften zijn de essentiële vereisten. Deze technologieonafhankelijke algemene doelstellingen van de richtlijn zullen in Nederland worden omgezet in een algemene maatregel van bestuur. Meer technische standaarden zullen worden opgenomen in een ministeriële regeling waarbij rekening zal worden gehouden met de vanuit ETSI en CEN beschikbaar gekomen standaarden die een vrij gedetailleerde invulling geven van de in de bijlagen van de richtlijn opgenomen eisen. Deze invulling reflecteert een «best practice» voor certificatiediensten die in Europa breed wordt gedragen. Daarnaast zijn ook andere technische invullingen van de essentiële vereisten in de richtlijn denkbaar. Relevante standaarden zijn in dit verband:
– X.509, ETSI TS 101 862, en diverse Internet standaarden als nadere invulling voor bijlage I;
– ETSI TS 101 456, als nadere invulling voor bijlage II;
– CEN Workshop Agreements 14168 en 1469 voor de nadere invulling voor bijlage III.

In bijlage II, onder sub i, van de richtlijn is bepaald dat de certificatiedienstverlener gedurende een gepaste periode alle relevante informatie met betrekking tot een gekwalificeerd certificaat moet vastleggen, met name om ten behoeve van gerechtelijke procedures de certificatie te kunnen bewijzen. Dit vastleggen mag elektronisch plaatsvinden. De leden van de D66-fractie vragen zich af wat dient te worden verstaan onder «gepaste periode» en onder «alle relevante informatie». Gerelateerd hieraan is de vraag of dit per certificaat, per contract en per lidstaat kan verschillen. Op welke wijze worden de gegevens op verifieerbare wijze vastgelegd?
De eisen uit de bijlagen I tot en met III zullen worden uitgewerkt in een algemene maatregel van bestuur. Daarin zullen ook deze begrippen nader worden gespecificeerd. Hieronder zijn de huidige inzichten hierover weergegeven.
De noodzakelijke bewaarduur is in hoge mate afhankelijk van het gebruik en het beroep dat erop gedaan zal worden. Dit gebruik kan per certificaat verschillen omdat sommige certificaten slechts een zeer korte werkingsduur zullen hebben en de ondersteunde handelingen al spoedig zijn uitgewerkt. Alle gegevens die de certificatie bewijzen, dienen hierbij te worden opgeslagen. Bij de opgeslagen gegevens kan bijvoorbeeld worden gedacht aan een kopie van de identificerende pagina uit het paspoort. Daarnaast moeten al die gegevens worden opgeslagen die het mogelijk maken op een later tijdstip te kunnen controleren of een certificaat op een bepaald moment in het verleden geldig was. Hiertoe moet de gehele historische informatie met betrekking tot intrekkingen van certificaten worden bewaard. Gedacht wordt aan het verplicht stellen van een termijn van zeven jaar, gedurende welke de hiervoor bedoelde gegevens

tenminste moeten worden bewaard. Dit is, gelet op het verwachte gebruik van de elektronische handtekeningen die op een gekwalificeerd certificaat zijn gebaseerd, een redelijke termijn. Deze termijn stemt overeen met de normale bewaarduur van bedrijfsgegevens zoals vastgelegd in artikel 2:10 lid 3 BW, artikel 52 van de Algemene wet inzake rijksbelastingen en in artikel 8 lid 3 Douanewet. Partijen kunnen met de certificatiedienstverlener een langere bewaartermijn overeenkomen. Dit is bijvoorbeeld van belang indien in de elektronische communicatie tussen overheid en bedrijfsleven gebruik wordt gemaakt van de diensten van een commerciële certificatiedienstverlener. In de elektronische communicatie met particulieren zal de overheid gewoonlijk eenzijdig de voorwaarden voor certificering kunnen stellen. Hetzelfde geldt voor elektronische communicatie tussen overheden. Bij contracten met het bedrijfsleven kan het zijn dat de overheid op basis van de Archiefwet 1995 gehouden is documenten langer te bewaren dan zeven jaar, voor zover ze niet voor vernietiging in aanmerking komen. De overheid zal bij elektronische communicatie met derden op basis van een gekwalificeerd certificaat dat is afgegeven door een onafhankelijke certificatiedienstverlener bij de opdrachtverlening ervoor moeten zorgdragen dat de gegevens met betrekking tot identiteitscontrole, de certificatie en de geldigheid van het certificaat net zo lang worden bewaard als voor de betrokken verstuurde documenten ingevolge de Archiefwet 1995 noodzakelijk is. De staatssecretaris van Onderwijs, Cultuur en Wetenschappen bereidt thans nadere regelgeving voor met betrekking tot de wijze van bewaren van elektronische archiefbescheiden. Van belang is tenslotte dat ter uitvoering van artikel 8 van de richtlijn, artikel 11.5a van de Telecommunicatiewet bepaalt onder welke voorwaarden persoonsgegevens verkregen en verwerkt mogen worden.
Wat betreft de verschillen per certificaat, per contract en per lidstaat, kan het volgende worden opgemerkt. De richtlijn en de bijbehorende bijlagen gelden voor alle lidstaten van de Europese Unie alsmede voor de overige staten die partij zijn bij de Overeenkomst betreffende de Europese Economische Ruimte. Voor alle lidstaten geldt hetzelfde voorschrift, luidend dat «alle relevante gegevens» gedurende een «gepaste periode» moeten worden bewaard. Het is aan de lidstaten om hieraan invulling te geven. Duidelijk is al dat deze invulling, onder meer als gevolg van verschillen in de nationale wetgevingen over bewijsvoering en archivering, uiteen kan lopen. Sommige lidstaten nemen hierover geen bepalingen op terwijl andere lidstaten termijnen van 10 of 30 jaar of zelfs een onbeperkte termijn zullen opnemen.

De leden van de fractie van D66 vragen hoe de regering staat tegenover de zogenoemde «datapakhuizen». Deze «datapakhuizen» worden ook wel «informatiepakhuizen» of «datawarehouses» genoemd. Een informatiepakhuis wordt gedefinieerd als één grote elektronische databank met gegevens waarin gezocht kan worden naar zinvolle verbanden en kennis. Daarvan is echter geen sprake wanneer het gaat om het verwerken van persoonsgegevens ten behoeve van het verstrekken van gekwalificeerde certificaten. Bij het verstrekken van gekwalificeerde certificaten aan degenen die een elektronische handtekening aanvragen die is gebaseerd op een gekwalificeerd certificaat, is een wettelijke identiteitscontrole voorgeschreven. De gegevens die daarvoor dienen te worden verstrekt en noodzakelijkerwijs gedurende een gepaste periode dienen te worden vastgelegd, betreffen niet meer dan gegevens ter controle van de identiteit. Veel meer persoonsgegevens dan naam, adres en woonplaats, gekoppeld aan het nummer van het gebruikte document ter bevestiging van de geclaimde identiteit, alsmede eventueel de functie van de aanvrager en de naam en het adres van het betreffende bedrijf, zullen niet worden geregistreerd. Deze registratie is nodig om te kunnen bewijzen dat de afgifte van het certificaat op de juiste wijze is uitgevoerd. Artikel 11.5a van de Telecommunicatiewet bevat strikte regels voor het verkrijgen en het

verwerken van persoonsgegevens. Zo kunnen certificatiedienstverleners die certificaten aan het publiek afgeven, alleen persoonsgegevens verwerken die zij van de betrokkene zelf of met diens uitdrukkelijke toestemming hebben verkregen. Deze verkregen persoonsgegevens mogen niet voor andere doeleinden worden verzameld of verwerkt, tenzij de betrokkene daarvoor zijn uitdrukkelijke toestemming heeft gegeven. De gegevens worden derhalve met een grote mate van zorgvuldigheid verkregen en verwerkt.
De leden van de fractie van D66 vragen hoe de identiteit van een persoon voor wie een gekwalificeerd certificaat wordt afgegeven, wordt gecontroleerd en op verifieerbare wijze wordt vastgelegd en of daarbij de bescherming van de persoonsgegevens voldoende is gewaarborgd. Zoals vastgelegd in artikel 18.15, derde lid, van de Telecommunicatiewet, wordt de identiteit van een persoon voor wie een gekwalificeerd certificaat wordt afgegeven, gecontroleerd aan de hand van de bij artikel 1 van de Wet op de identificatieplicht aangewezen geldige documenten, te weten: een geldig reisdocument ingevolge de Paspoortwet; de documenten waarover een vreemdeling ingevolge de Vreemdelingenwet moet beschikken ter vaststelling van zijn identiteit, nationaliteit en verblijfsrechtelijke positie of andere door de minister van Justitie aangewezen documenten ter vaststelling van de identiteit van personen. De bescherming van de persoonsgegevens is voldoende gewaarborgd door artikel 11.5a van de Telecommunicatiewet, zoals hiervoor is aangegeven. In paragraaf 2.8 zal ik nog nader ingaan op de bescherming van persoonsgegevens.

*2.3 Rechtsgevolgen van elektronische handtekeningen*

De leden van de VVD-fractie vragen onder welke omstandigheden er bij onbevoegd gebruik van de elektronische handtekening sprake kan zijn van valsheid in geschrifte. Van valsheid in geschrift bij onbevoegd gebruik van de elektronische handtekening kan sprake zijn wanneer aan de bestanddelen van de delictsomschrijving van artikel 225 Wetboek van Strafrecht (Sr) is voldaan. Dit artikel stelt strafbaar hij die een geschrift dat bestemd is om tot bewijs van enig feit te dienen, valselijk opmaakt of vervalst, met het oogmerk om het als echt en onvervalst te gebruiken of door anderen te doen gebruiken. In de eerste plaats kan de term «geschrift» in artikel 225 Sr op grond van de jurisprudentie van de Hoge Raad ook een computerbestand betreffen (HR 15 januari 1991, NK 1991, 668). Van belang in het genoemde arrest was het feit dat het ging om met enige duurzaamheid vastgelegde gegevens die op tamelijk eenvoudige wijze leesbaar konden worden gemaakt. Daarnaast ligt het voor de hand aan te nemen dat onder het «valselijk opmaken» mede kan worden verstaan het onbevoegd toevoegen van een elektronische handtekening aan een elektronisch bestand, en onder het «vervalsen» het onbevoegd bewerken van een elektronische handtekening die bevoegd is geplaatst. Niet alleen degene die dit voor eigen gebruik doet, maar ook degene die dit ten behoeve van derden doet, kan onder de strafbaarstelling van artikel 225 Sr vallen. Het vereiste van «het oogmerk om het als echt en onvervalst te gebruiken of door anderen te doen gebruiken» ten slotte brengt mee dat voor toepassing van artikel 225 Sr bij het onbevoegd gebruik van de elektronische handtekening slechts plaats is indien dit geschiedt met kwade bedoelingen.

De leden van de fracties D66 en VVD vragen om een nadere toelichting op de vraag of de persoon die zich van de elektronische handtekening bedient in geval van onrechtmatig gebruik van zijn elektronische handtekening door een ander daartegen alleen of uitsluitend samen met de certificatiedienstverlener in rechte op kan treden. De leden van de D66-fractie vragen voorts waarom dit punt louter afhankelijk wordt gesteld van de contractuele relatie. Deze leden hebben een voorkeur voor

het alleen in rechte optreden door de gebruiker van de elektronische handtekening. In het nader rapport (onder punt 2) en de memorie van toelichting (in paragraaf 2.3) is uiteengezet dat het denkbaar is dat een certificatiedienstverlener een elektronische handtekening verstrekt waarop hijzelf rechten kan doen gelden. In dat geval kan zich de vraag voordoen of de persoon die zich van een dergelijke elektronische handtekening bedient in geval van onrechtmatig gebruik van zijn elektronische handtekening door een ander daartegen alleen of uitsluitend samen met de certificatiedienstverlener in rechte op kan treden. In zijn algemeenheid kunnen hierover moeilijk uitspraken worden gedaan omdat er vele manieren van onrechtmatig gebruik zijn en de omstandigheden van het geval zeer bepalend zullen zijn. In elk geval zal hetgeen in de contractuele relatie tussen de gebruiker van de elektronische handtekening en de certificatiedienstverlener die deze handtekening heeft verschaft, is afgesproken een belangrijke rol spelen omdat hiervoor geen specifieke wettelijke regeling geldt. De mogelijkheid in rechte op te treden is derhalve niet louter afhankelijk van de contractuele relatie. Het is in dit verband van belang om een onderscheid te maken tussen de positie van de gebruiker van een elektronische handtekening en die van de certificatiedienstverlener. De aard van de rechten die zij hebben is verschillend. Voor de gebruiker van een elektronische handtekening zal het onrechtmatig gebruik daarvan betekenen dat hij tegen zijn wil gebonden dreigt te worden aan de transactie die onbevoegd met gebruikmaking van «zijn» elektronische handtekening heeft plaatsgevonden. Tegen dat, uitsluitend hem regarderende, aspect van het onbevoegd gebruik zal de gebruiker zelfstandig kunnen optreden. De certificatiedienstverlener zal er in een dergelijk geval ook geen belang bij hebben om te voorkomen dat de gebruiker hiertegen geheel zelfstandig optreedt. Tegelijkertijd is echter denkbaar dat de certificatiedienstverlener op het aanmaken of het gebruik van bepaalde (typen van) elektronische handtekeningen een (exclusief) recht heeft, dat door een bepaalde vorm van onbevoegd gebruik (mede) wordt geschonden. Het ligt voor de hand dat de dienstverlener in een dergelijk geval zelfstandig in rechte zal kunnen optreden tegen dat, uitsluitend hem regarderende, aspect van het onbevoegd gebruik van de elektronische handtekening, ook al betreft het niet »zijn» elektronische handtekening, maar die van de gebruiker. Gelet op een en ander valt evenmin uit te sluiten dat zich in de praktijk gevallen zullen voordoen waarin het optreden in rechte tegen onbevoegd gebruik van een elektronische handtekening in de praktijk alleen mogelijk is of zinvol kan geschieden indien dit gezamenlijk door de gebruiker en de certificatiedienstverlener plaatsvindt. Te denken valt aan het geval dat de certificatiedienstverlener voor het effectueren van zijn recht gebruik wil of moet maken van een aan een bepaalde gebruiker uitgegeven elektronische handtekening. Een contractuele regeling met het oog op deze gevallen ligt dan ook voor de hand.

De leden van de D66-fractie vragen een nadere toelichting danwel uitwerking met betrekking tot de vraag over welke technische mogelijkheden en bevoegdheden de certificatiedienstverlener al dan niet in overleg met het Openbaar Ministerie zal beschikken om misbruik van elektronische handtekening te voorkomen en tegen te gaan indien hij in het kader van zijn dienstverlening op de hoogte raakt van onjuist of onbevoegd gebruik van een elektronische handtekening. Zo is bijvoorbeeld de vraag wanneer toestemmingsvereisten aan de orde zijn en aan welke andere mechanismen wordt gedacht. Indien een certificatiedienstverlener in het kader van zijn dienstverlening op de hoogte raakt van onjuist of onbevoegd gebruik van een elektronische handtekening die hij heeft verstrekt aan een bepaalde persoon zal veelal de contractuele relatie die hij met deze persoon heeft, meebrengen dat hij deze daarvan op de hoogte dient te stellen. Het zal dan vervolgens van de aard van het misbruik en de daardoor geschonden rechten afhangen wie daartegen, zo nodig in rechte, kan

optreden. Doorgaans zal dit de gebruiker van de elektronische handtekening zijn.

*2.4 Aansprakelijkheid van certificatiedienstverleners*

De leden van de D66-fractie merken op dat zij met de aansprakelijkheidsregels kunnen instemmen.

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

De leden van de fracties van PvdA, VVD en D66 vragen aandacht voor het wettelijk toezicht door de OPTA, met name in relatie tot de vrijwillige accreditatieregelingen. Het lijkt mij juist de positie van de OPTA hier uitgebreid uiteen te zetten.
Met ingang van 1997 zijn TTP's en overheid bezig ervoor te zorgen dat de marktpartijen zich aan een aantal minimum eisen conformeren. Het uitgangspunt is hierbij steeds zelfregulering geweest. Ik moge in dit verband verwijzen naar de TTP-beleidsnotitie (Kamerstukken II, 1998/99, nr. 26 581). De in deze notitie ontwikkelde visie op sectorale zelfregulering is uitgewerkt door de marktpartijen onder auspiciën van ECP.NL (het E-commerce Platform Nederland) binnen het zogenoemde TTP.NL project tot een systeem van certificatie en accreditatie. Marktpartijen kunnen zich hierbij laten toetsen door certificerende instanties (organisaties die EDP-audit diensten leveren) op het voldoen aan de wettelijke of andere eisen. Zelfverklaringen zijn hier niet aan de orde. Hierbij heeft men de van oorsprong zelf ontwikkelde eisen opgegeven ten faveure van de in internationaal verband samengestelde standaard ETSI TS 101 456, waaraan vanuit TTP.NL verband actief is bijgedragen. De certificerende instanties zelf worden op hun beurt geaccrediteerd door de Raad van Accreditatie in het concrete voorbeeld van het TTP.NL schema.
Dit systeem van certificatie en accreditatie levert door de toetsing vooraf en door herhalingsaudits een hoge mate van zekerheid op dat de marktpartijen ook werkelijk aan de wettelijke eisen voldoen. In het bijzonder betreft dit de eisen van bijlage II van de richtlijn. Vanwege deze hoge mate van zekerheid wordt het als wenselijk gezien dat alle marktpartijen zich onderwerpen aan deze accreditatie en certificatie. Ingevolge artikel 3, tweede lid, van de richtlijn mogen lidstaten dit soort accreditatie en certificatieregelingen invoeren of handhaven. Dit houdt een soort erkenning in, waarbij dergelijke erkende regelingen, alsmede de nationale instanties die zijn belast met accreditatie, moeten worden genotificeerd (artikel 11, eerste lid, onderdeel a, van de richtlijn). Deze erkenning is als een «aanwijzing van een instelling die beoordeelt dat de certificatiedienstverleners aan de wettelijke eisen voldoen» in artikel 18.16, eerste lid, van de Telecommunicatiewet geïmplementeerd. Na zo'n aanwijzing worden ook de voordelen daarvan ondervonden in de relatie met de toezichthouder OPTA. Aangenomen wordt dat de gecertificeerde certificatiedienstverlener inderdaad aan de eisen voldoet. Er behoeft geen inhoudelijke informatie meer te worden overlegd.
De richtlijn eist dat een dergelijk systeem van accreditatie en certificatie vrijwillig is. De markt kan dus betreden worden door alle certificatiedienstverleners, ook door diegenen die zich niet onderwerpen aan het systeem van accreditatie en certificatie. De richtlijn bepaalt verder in algemene zin dat de lidstaten toezicht moeten houden op de certificatiedienstverleners die gekwalificeerde certificaten uitgeven aan het publiek. De certificatiedienstverleners moeten voldoen aan de eisen van de bijlagen bij de richtlijn. De richtlijn verbiedt daarbij voorafgaande machtiging of andere maatregelen van gelijke werking die de toegang tot de markt voor certificatiediensten beperken; een stelsel van (voorafgaande) vergunningen is dus niet toegestaan. In verband hiermee is een inhoudelijk

onderzoek naar de juistheid van de gegevens met betrekking tot de overeenstemming van de certificatiedienstverlener met de wettelijke voorschriften, voorafgaand aan de registratie niet toegelaten, indien dit betekent dat de toegang tot de markt zou worden verhinderd zolang niet alle gegevens zijn geverifieerd. Hetzelfde geldt voor het verplicht stellen van een overeenstemmingsverklaring die is afgegeven door een aangewezen certificatie- en accreditatie-instelling. Om gekwalificeerde certificaten aan het publiek te mogen aanbieden, is in de wetgeving uitsluitend een registratieverplichting opgenomen. Daardoor is de toegang tot de markt zeer laagdrempelig. Wel moeten alle certificatiedienstverleners die gekwalificeerde certificaten aan het publiek afgeven bij registratie aannemelijk maken dat ze aan de wettelijke eisen voldoen. Een verklaring van overeenstemming afgegeven in het kader van een erkende certificatie en accreditatieregeling is hiervoor één mogelijkheid, een eigen verklaring met een ondersteunend informatiedossier is een andere mogelijkheid.
De toezichthouder OPTA zal slechts een marginale toets op dat informatiedossier uitvoeren, tenzij er redelijke vermoedens bestaan dat er feitelijk niet aan de eisen wordt voldaan. In dat laatste geval zal de certificatiedienstverlener meer bewijsmateriaal moeten overleggen om het voor de toezichthouder aannemelijk te maken dat er inderdaad aan de eisen wordt voldaan.
De achterliggende gedachte bij het onderscheid tussen registratie en toezicht op basis van informatiedossiers respectievelijk op basis van vrijwillige certificatie en accreditatie is dat afnemers van certificatiediensten zullen kunnen differentiëren tussen partijen die voorafgaand zijn getoetst als onderdeel van een vrijwillig systeem van accreditatie en certificatie en partijen die kiezen voor een zelfverklaring in plaats van een certificatie door een derde partij.
Overigens is duidelijk dat de toezichthouder OPTA en «erkende» vrijwillige accreditatie-instellingen goed met elkaar moeten samenwerken, om te zorgen dat zij dezelfde normen hanteren althans voor wat betreft de invulling van de wettelijke eisen. Concreet is de OPTA sinds dit voorjaar betrokken bij TTP.NL en bestaat de intentie dat beide dezelfde technische norm (ETSI TS 101 456) gaan hanteren. Op het moment dat zich een incident voordoet (bijvoorbeeld een klacht dat een certificatiedienstverlener niet aan de eisen voldoet), kan het onderzoek van de OPTA vereenvoudigd en bespoedigd worden door informatie van de instelling die de verklaring van overeenstemming heeft afgegeven. De OPTA kan deze informatie direct op basis van wettelijke bevoegdheden opvragen. In de praktijk is het wenselijk een nauwkeurige protocollering op te stellen om een ongewenste inbreuk in de vertrouwensrelatie tussen de certificatiedienstverlener en zijn beoordelende instelling te vermijden.
De leden van de PvdA fractie zijn van mening dat de rol van de toezichthouder met onvoldoende waarborgen is omkleed en vragen, samengevat, om een stevige controle vooraf van de certificatiedienstverleners, waarbij ook vergunningverlening is genoemd. Anders dan de leden van de PvdA fractie ben ik van mening dat het geschetste stelsel van vrijwillige certificatie en accreditatie, aangevuld met toezicht, voldoende waarborgen biedt. Ten eerste is het beleid er op gericht om partijen deel te laten uitmaken van het TTP.NL systeem, waarbinnen certificatie- en accreditatie instellingen worden aangewezen. Ten tweede heeft de OPTA, met het oog op de mogelijkheid dat partijen buiten het TTP.NL stelsel gaan opereren, aanzienlijke bevoegdheden om haar toezicht uit te oefenen. De richtlijn laat toetsing vooraf niet toe. Het wetsvoorstel biedt echter de mogelijkheid om naar aanleiding van het informatiedossier kort na de inschrijving een ingeschreven marktpartij te ondervragen en zonodig een nader onderzoek in te stellen.
De leden van de PvdA fractie willen tevens graag weten welke expertise er momenteel wordt ontwikkeld bij de politie en het Openbaar Ministerie om fraude met elektronische handtekeningen op te sporen en tegen te gaan,

zulks mede naar aanleiding van pilots (bijvoorbeeld bij een Haarlems notariskantoor). Ten aanzien van fraude met elektronische handtekeningen en de daaraan gerelateerde opsporing is er tot op heden geen significante praktische ervaring opgedaan. Wel zijn er veel theoretische beschouwingen die aanleiding zijn tot preventieve maatregelen, veelal in de technische sfeer. Sommige maatregelen zijn er op gericht om te voorkomen dat derden kunnen beschikken over de vertrouwelijke gegevens voor het genereren van de elektronische handtekening (het veilige middel speelt hierin een essentiële rol). Andere belangrijke maatregelen zijn er op gericht om zeker te stellen dat de elektronische handtekening uitsluitend wordt verbonden aan berichten die men ook wenst te ondertekenen (met de daaraan mogelijk verbonden rechtsgevolgen). Daarnaast wordt in algemene zin veel aandacht gegeven aan het ontwikkelen van expertise voor de handhaving in de elektronische omgeving. Bij brief van 15 augustus 2001 heb ik uw Kamer hierover geïnformeerd (Kamerstukken II, 2000–2001, 27 834, nr. 3). Omdat geen stelsel van preventieve maatregelen is te creëren dat volledige bescherming biedt op (onder meer) de bovenstaande punten, blijft er ruimte om het gebruik of de certificatie van een elektronische handtekening later te ontkennen. De praktische ruimte hiertoe moet zoveel mogelijk worden beperkt, omdat het niet goed mogelijk is om aanvullende zekerheden te verkrijgen uit de context waarin de elektronische handtekening wordt gezet. Een juiste vorm van forensisch onderzoek zou wellicht kunnen uitwijzen of iemand terecht of juist onterecht zijn handtekening ontkent, maar vooralsnog is er weinig ervaring op dit gebied.
De leden van de PvdA fractie vragen tevens hoe gebruik wordt gemaakt van de ervaringen van de Belastingdienst. In het algemeen worden ervaringen met pilots binnen de Rijksoverheid op dit gebied (Taskforce PKI Overheid, TTP) goed gedeeld. De Taskforce PKI Overheid vervult in deze de rol van overlegplatform. Diverse op dit gebied actieve partijen (de ministeries van Economische Zaken, van Justitie en van Verkeer en Waterstaat, alsmede de Belastingdienst) binnen de Rijksoverheid zijn binnen deze taskforce en de daaraan verbonden stuurgroep betrokken, zodat inbreng vanuit de verschillende ervaringen is geborgd.

De leden van de VVD-fractie zien graag verduidelijkt waarom de minister instellingen kan aanwijzen om certificatiedienstverleners te toetsen. Biedt zelfregulering hier geen uitkomst? Het gaat hier om het aanwijzen van instellingen binnen een vrijwillige certificatie- en accreditatieregeling, zoals concreet beoogd met het TTP.NL systeem (hoewel er in beginsel meerdere systemen naast elkaar kunnen bestaan). In het kader van het TTP.NL project zijn de bestaande Nederlandse marktpartijen in gezamenlijk overleg op het mechanisme uitgekomen dat in de praktijk een audit wordt uitgevoerd door een aangewezen instelling. Overigens bestaat er naast het voorgestelde systeem van vrijwillige certificatie en accreditatie in combinatie met toezicht de mogelijkheid voor certificatiedienstverleners om zelf een verklaring op te stellen dat zij aan de eisen voldoen, een claim die men bij registratie dient te ondersteunen met een informatiedossier. Hierdoor wordt ruimte geschapen voor zelfregulering. Volledige zelfregulering zonder toezicht is niet toegestaan.

De leden van de D66 fractie vragen zich af of de voorgestane wijze van toezicht, initieel alleen registratie, niet wat mager is. Zoals in de uiteenzetting aan het begin van deze paragraaf is aangegeven, mogen op grond van artikel 3, eerste lid, van de richtlijn, certificatiediensten niet afhankelijk worden gesteld van voorafgaande machtiging. Het wetsvoorstel schrijft voor dat certificatiedienstverleners die gekwalificeerde certificaten aan het publiek afgeven zich moeten laten registreren; daarbij moeten zij echter informatie overleggen waaruit blijkt dat zij aan de gestelde eisen voldoen. Dit kan bijvoorbeeld aan de hand van een informatiedossier, dat in het

algemeen marginaal, met name op volledigheid, zal worden getoetst. De beperkingen van het toezicht rond het moment van registratie volgen derhalve direct uit de beperkingen van de richtlijn. De OPTA heeft echter zoals geschetst ruimschoots voldoende bevoegdheden om daarna adequaat inhoudelijk toezicht uit te oefenen.
De leden van de D66 fractie willen graag een nadere uitleg over de wijze waarop met name de preventieve handhaving gestalte krijgt. Hoe controleert de OPTA of certificatiedienstverleners daadwerkelijk aan de eisen voldoen? Deze eerste fase van het toezicht is er vooral op gericht om vast te stellen dat het aannemelijk is dat er door de certificatiedienstverlener aan de eisen wordt voldaan. Zoals het toezichtmodel hiervoor is geschetst, zal met het toezicht (marginale toetsing rondom de registratie, later onderzoek op basis van redelijk vermoeden) ook in de latere fasen, wellicht niet dezelfde mate van zekerheid worden bereikt als in het geval van vrijwillige certificatie en accreditatie. Er is immers in het algemeen slechts sprake van een marginale controle, die waarschijnlijk zal zijn gebaseerd op de inspectie van de beantwoording van een vragenlijst (die op zijn beurt zal zijn gebaseerd op de standaard ETSI TS 101 456). Het naast elkaar bestaan van deze vormen van toetsing of aan de eisen wordt voldaan, zal in de praktijk weinig problemen geven, omdat de markt in staat mag worden geacht te differentiëren tussen aanbieders die grote zekerheid bieden op dit punt en aanbieders die op dit punt minder zekerheid bieden. Verder wordt opgemerkt dat de bevoegdheden van de OPTA om geregistreerde certificatiedienstverleners te laten bewijzen dat ze aan de wettelijke eisen voldoen, alsmede de mogelijkheden tot onderzoek waarover de OPTA beschikt, voldoende ruim zijn om adequaat op te treden.
De leden van de D66 fractie vragen naar de rol van de accreditatieorganisaties in de vrijwillige stelsels (schema's) van certificatie en accreditatie en de wijze waarop deze zelf verantwoording afleggen. Ter beantwoording geef ik een enigszins vereenvoudigde beschrijving van zo'n stelsel:

- Certificatiedienstverleners leveren (al dan niet gekwalificeerde) certificaten en hieraan gerelateerde dienstverlening aan afnemers.
- Certificerende instellingen controleren door middel van audits de certificatiedienstverleners en geven conformiteitsverklaringen af. Dit betreft dus het voldoen aan de eisen van de betreffende certificatie- en accreditatie-regeling. Een certificatie – en accreditatieregeling moet, om voor aanwijzing in het kader van deze wet in aanmerking te komen, eisen stellen die in overeenstemming zijn met de wettelijke eisen of die eisen overtreffen.
- Accrediterende instellingen (veelal landelijke instellingen, zoals de raad voor de Accreditatie) controleren of de certificerende instellingen zelf voldoen aan de eisen die nodig zijn om goede audits af te kunnen leveren. Te denken valt aan vakbekwaamheidseisen en het bestaan van goede procedures.
- Accrediterende instellingen visiteren en controleren elkaar (bijvoorbeeld in het verband van Europese accreditatie-instellingen).
- De OPTA houdt toezicht op de certificatiedienstverleners, maar heeft geen rechtstreekse betrokkenheid bij de werking van het stelsel van vrijwillige accreditatie- en certificatieregelingen.

De leden van de D66 fractie vragen naar de handelwijze van de OPTA in het geval van repressieve handhaving en stellen vragen bij de wijze waarop de OPTA controles moet uitvoeren. In het algemeen is beoogd de OPTA bevoegdheden te geven om effectief toezicht uit te kunnen oefenen, waarbij de OPTA voldoende discretionaire vrijheid wordt geboden om – binnen het kader van de wettelijke mogelijkheden – tot een invulling van dit toezicht te komen. In dit kader moet ook de mogelijkheid worden gezien die de OPTA heeft om nader onderzoek te verrichten of een certificatiedienstverlener aan de eisen voldoet; er is bewust geen verplichting

aan de OPTA opgelegd. Het is in deze sector van dienstverlening vooraf niet aan te geven onder welke voorwaarden de OPTA in actie zou moeten komen. De ruimte die de richtlijn biedt voor inhoudelijke controle is om, volgend op registratie, verdergaande bewijzen te eisen van de certificatiedienstverlener (dat men aan de eisen voldoet) dan thans het geval is. De weg van verplichte controle door een certificerende instelling is echter zeer bewust niet bewandeld omdat dit in strijd is met de richtlijn en bovendien niet in lijn is met het ingezette beleid van zelfregulering, waarbij deze zaken worden overgelaten aan de sector en de overheid (inclusief de toezichthouder) een bescheiden rol speelt.
De leden van de D66 fractie vragen hoe een goede samenwerking tussen de OPTA en vrijwillige certificatie – en accreditatieregelingen wordt bewerkstelligd. In Nederland gaat het vooralsnog vooral om samenwerking tussen de OPTA en TTP.NL. Allereerst zullen zij zich baseren op dezelfde standaarden. Ten tweede onderhoudt de OPTA nauwe kontakten met TTP.NL en het aan de regeling verbonden College van Deskundigen teneinde verschillende interpretaties van eisen te voorkomen. Ten derde wordt samenwerking bevorderd door het uitwisselen van informatie over de situatie op de markt alsmede door het uitwisselen van informatie tussen de certificerende instelling en de OPTA in de gevallen waarin een vermoeden ontstaat dat een op basis van het schema van TTP.NL goedgekeurde certificatiedienstverlener wellicht toch niet aan de eisen voldoet (door bijvoorbeeld klachten). Zulks zal in beginsel conform een voorafgaande protocollering verlopen.

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

De leden van de fracties van VVD en D66 stellen vragen over de OPTA als toezichthouder op certificatiedienstverleners die gekwalificeerde certificaten aanbieden aan het publiek en de wijze waarop het toezicht op de geregistreerde certificatiedienstverleners is vormgegeven. Op deze vragen kan in het algemeen het volgende worden geantwoord.
Er is momenteel geen toezichthouder waaraan het toezicht op de certificatiedienstverleners en hun dienstverlening logischerwijze en zonder noemenswaardige aanpassing van werkwijze of expertise kan worden opgedragen. Dat was ten tijde van het totstandkomen van de richtlijn eveneens het geval. Vooralsnog moet afgewacht worden of het nodig zal zijn gespecialiseerde toezichthoudende instanties in het leven te roepen om belast te worden met toezicht op certificatiedienstverleners. Hoewel er in het begin van de werkzaamheden veel geïnvesteerd zal moeten worden in specifieke kennisopbouw, biedt de OPTA de beste kansen om goed toezicht op certificatiedienstverleners te bewerkstelligen. De OPTA is reeds vertrouwd met het houden van toezicht op basis van registratie. Onder paragraaf 2.9 wordt op de kosten van registratie en toezicht ingegaan.

Met artikel 18.18 van de Telecommunicatiewet heeft de OPTA een instrument om toezicht te houden op de certificatiedienstverleners waarvan de registratie is beëindigd omdat zij niet aan de wettelijke eisen voldoen. Deze certificatiedienstverleners kunnen wel certificaten aan het publiek afgeven, maar mogen geen gekwalificeerde certificaten aanbieden of afgeven omdat daarvoor registratie verplicht is. De OPTA heeft daardoor een instrument om onderzoek te doen naar de mate waarin een niet (meer) geregistreerde certificatiedienstverlener aan de wettelijke eisen voldoet. Indien een certificatiedienstverlener zich, wellicht zelfs onder een andere naam, opnieuw zou willen laten registreren bij de OPTA, dan is de OPTA voldoende op de hoogte van de specifieke situatie om het instellen van een nader onderzoek naar de zwakke punten van deze aspirant-certificatiedienstverlener te kunnen rechtvaardigen alvorens opnieuw tot

registratie over te gaan. Als dan blijkt dat (nog steeds) niet aan de wettelijke eisen wordt voldaan, wordt registratie geweigerd.
Op de vraag van de VVD-fractie waarom de bevoegdheden van de toezichthouder zijn te kwalificeren als de uitoefening van openbaar gezag kan worden geantwoord dat de OPTA een zelfstandig bestuursorgaan is dat als toezichthouder bekleed is met openbaar gezag.
De leden van de VVD-fractie vragen zich voorts af of de OPTA kwalitatief en kwantitatief voldoende is toegesneden op deze nieuwe toezichttaak. Deze nieuwe taak impliceert de opbouw van nieuwe expertise binnen de OPTA. Expertise die voldoende in de organisatie is geborgd. Dit impliceert een minimale kritische massa; een belangrijke reden om de inspanning voor dit toezicht op ca. 1,5 taak (FTE) te begroten. Deze opbouw van kennis en netwerk is overigens inmiddels binnen de OPTA in gang gezet. In kwantitatieve termen worden geen problemen verwacht.
Op de vraag van de D66 fractie, welke mogelijkheden de OPTA heeft om herregistratie te weigeren van een partij waarvan de registratie recent is geschrapt vanwege het (persistent) niet voldoen aan de wettelijke eisen is hierboven reeds ingegaan.

*2.7 Overeenstemming veilige middelen met bijlage III*

De leden van de D66-fractie vragen of het al bekend is aan welke instantie wordt gedacht voor toezicht op de naleving van de regels voor veilige middelen voor het aanmaken van elektronische handtekeningen. Veilige middelen voor het aanmaken van elektronische handtekeningen zijn technische producten die aan de eisen van bijlage III van de richtlijn voldoen. De overeenstemmingsbeoordeling met die eisen (en de nadere uitwerking hiervan in standaarden) moet worden uitgevoerd door een technisch instituut dat de kennis en kunde heeft om deze beoordeling te kunnen uitvoeren. Aangezien er binnen de Europese Unie voldoende technische instituten zijn die zo'n overeenstemmingsbeoordeling kunnen en willen uitvoeren is er geen aanleiding om de OPTA met deze nieuwe en zeer specialistische taak te belasten.
Verder dient de partij die veilige middelen op de markt brengt, deze te voorzien van een (afschrift van een) dergelijke overeenstemmingsverklaring. De klant kan op basis hiervan beoordelen of het hier inderdaad een veilig middel is conform de richtlijn (bijlage III) en derhalve of dit middel kan worden gebruikt om de gewenste elektronische handtekening te zetten.
Er is geen partij voorzien die actief toezicht houdt op de markt voor veilige middelen. Men zal bij klachten over het product bij de leverancier moeten aankloppen. Bij klachten over aanbieders die producten als veilig middel conform de richtlijn op de markt brengen zonder de bijbehorende overeenstemmingsverklaring, is ingrijpen mogelijk op basis van de Wet op de economische delicten.

*2.8 Gegevensbescherming*

De leden van de VVD-fractie willen weten waarom is gekozen voor een striktere bepaling omtrent het verkrijgen en het verder verwerken van persoonsgegevens dan in de Wet bescherming persoonsgegevens het geval is. In lijn hiermee wil deze fractie graag weten of de regering het niet met de leden van de VVD-fractie eens is dat het adagium off-line=on-line ook hier zou moeten gelden.
Deze striktere bepaling omtrent het verkrijgen en verwerken van persoonsgegevens dan in de Wet bescherming persoonsgegevens vloeit voort uit artikel 8, tweede lid, van de richtlijn. Hierdoor is het niet mogelijk in dit geval het adagium off-line = on-line te volgen.

De leden van de D66-fractie zijn zeer verheugd met het overnemen van het advies van de Registratiekamer waardoor via artikel 8, tweede lid, van de richtlijn extra waarborgen zijn ingebouwd met betrekking tot de door deze leden zeer gewenste voldoende bescherming van persoonsgegevens. Wel vragen zij verheldering omtrent de uitzondering die wordt gemaakt op het punt van de fraudebestrijding. Zij vragen zich af in welke gevallen opsporingsinstanties informatie kunnen krijgen over de persoon die aan een bepaalde elektronische handtekening is verbonden. Alsmede hoe deze informatie wordt verkregen en om wat voor fraude het dan gaat. Ten behoeve van de opsporing van strafbare feiten kan het van belang zijn dat opsporingsinstanties informatie over personen achter de elektronische handtekening kunnen krijgen. Het kan gaan om fraude, maar ook om andere strafbare feiten, bijvoorbeeld handel in verboden goederen, waarbij van elektronische documenten gebruik wordt gemaakt. De informatie kan in dringende gevallen worden verkregen op grond van artikel 43 Wet bescherming persoonsgegevens. Afhankelijk van de omstandigheden kan ook artikel 125i Wetboek van Strafvordering van toepassing zijn. Verder is van belang dat overwogen wordt meer algemene bevoegdheden tot het vorderen van gegevens in het Wetboek van Strafvordering op te nemen, zoals deze zijn voorgesteld door de Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij.

*2.9 Adviezen*

De VVD-fractie vraagt om het voorziene tariferingssysteem toe te lichten en de mogelijke knelpunten die hierbij zijn te verwachten. Hieraan is de vraag gerelateerd die onder paragraaf 2.6 door de D66-fractie is gesteld, boven welk bedrag per aanbieder er marktbelemmeringen kunnen ontstaan. De markt voor certificatiediensten staat nog in zijn kinderschoenen. De meeste toepassingen worden thans gevonden in betrouwbare communicatie in besloten gebruikersgroepen. Veel partijen vragen zich af hoe groot de markt voor elektronische handtekeningen die aan de handgeschreven handtekening zijn gelijkgeschakeld nu werkelijk is en hoe snel deze zich zal ontwikkelen. Voor grote bedrijven die de certificatiedienstverlening als een nieuw speerpunt van dienstverlening zien, vormt een jaarlijks omgeslagen kostenbedrag minder snel een belemmering om in de markt actief te zijn of te blijven dan voor een kleine dienstverlener. Precieze bedragen zijn hierbij niet te noemen. Naarmate het aantal certificatiedienstverleners stijgt, vermindert in beginsel het per dienstverlener omgeslagen bedrag. De kosten van registratie door de OPTA zullen gebaseerd worden op de werkelijke kosten van de activiteiten ten tijde van en na de registratie, bijvoorbeeld informatiediensten ten behoeve van gebruikers. Verwacht wordt dat hier geen belemmeringen om tot de markt toe te treden, zullen ontstaan. De kosten van het toezicht door de OPTA, althans in de beginfase, waarin expertise wordt opgebouwd en de markt zich gaat vormen, zijn door de OPTA in de uitvoeringstoets van 18 augustus 2000 geschat op 368 000 gulden per jaar. Dit bedrag is dezerzijds steeds als leidraad gebruikt bij de gedachtevorming over een passend stelsel van toezicht op de relatief kleine groep van geregistreerde certificatiedienstverleners. De omvang van deze groep zal naar de huidige inzichten geleidelijk groeien van 3 aanbieders in 2002 tot circa 8 binnen enkele jaren. In de concept-begroting voor 2002 heeft de OPTA deze schatting inmiddels naar boven bijgesteld op basis van nadere inzichten. De conceptbegroting is binnenkort onderwerp van overleg tussen de OPTA en het Ministerie van Verkeer en Waterstaat. In verband hiermee is de precieze wijze van financiering momenteel nog niet vastgesteld, en kunnen nog geen uitspraken worden gedaan over de hoogte van het bedrag dat over de geregistreerde certificatiedienstverleners wordt omgeslagen.

## ARTIKELEN

### ARTIKEL I

A

*Artikel 15c*

De leden van de fractie van de VVD vragen met betrekking tot de mogelijkheden voor de strafrechtelijke handhaving, welke voorwaarden worden meegenomen en welke stappen precies worden verwacht en hoe deze zich verhouden tot het onderhavige wetsvoorstel, bij het onderzoek naar de vraag of de bestaande in het Wetboek van Strafvordering neergelegde bevoegdheden een toereikende basis bieden. Zij vragen voorts hoe deze nadere beschouwing zich verhoudt tot hetgeen is gesteld in artikel 11.5, derde lid, van de Telecommunicatiewet en hoe – meer in het algemeen – de risico's worden ingeschat zonder dat duidelijk is wat de strafrechtelijke handhaafbaarheid van een en ander is.
De Commissie Strafvorderlijke gegevensvergaring in de informatiemaatschappij heeft onderzocht of de bestaande bevoegdheden in het Wetboek van Strafvordering nog toereikend zijn in de informatiemaatschappij. Deze commissie heeft voorgesteld enkele nieuwe bevoegdheden tot het vorderen van gegevens in het Wetboek van Strafvordering op te nemen. Dit spoort met artikel 11.5a, derde lid, van de Telecommunicatiewet. Artikel 11.5a, derde lid, is de spiegelbepaling van de bevoegdheden van de opsporing. Deze bepaling maakt duidelijk dat het beperkte regime voor de verwerking van gegevens doorbroken kan worden ten behoeve van de opsporing.

### ARTIKEL II

A

*Artikel 1.1*

De D66-fractie vraagt welke privacywaarborgen van toepassing zijn op diensten, zoals sleutelbeheer, die gerelateerd zijn aan de basis-certificatiediensten. Op de verwerking van persoonsgegevens door aanbieders van certificatiediensten is de Wet bescherming persoonsgegevens van toepassing. Dat geldt voor alle diensten die een certificatiedienstverlener aanbiedt. Zoals onder paragraaf 2.8 is aangegeven, geldt er voor de verwerking van persoonsgegevens door certificatiedienstverleners die gekwalificeerde certificaten aan het publiek afgeven, op grond van artikel 8, tweede lid, van de richtlijn en artikel 11.5a van de Telecommunicatiewet een strenger regime. Op de naleving van dit strengere regime houdt de OPTA toezicht.

B

*Artikel 2.1*

De leden van de D66-fractie lijkt het wenselijk dat de OPTA niet slechts bij een redelijk vermoeden van niet- naleving toetst of de certificatiedienstverlener voldoet aan de wettelijke eisen. Zoals hiervoor onder paragraaf 2.5 is aangegeven, biedt het systeem van registratie op basis van een globale toetsing van het bij de aanvraag overgelegde informatiedossier, waarin de aanvrager zelf verklaart en aantoont aan de gestelde eisen te voldoen, in combinatie met de periodieke onderzoeken van de

OPTA voldoende zekerheid dat de dienstverlening in overeenstemming is met de wettelijke eisen. Het is daarnaast de verwachting dat zelfregulerende organisaties een aantal certificatiedienstverleners voorafgaand aan de aanvraag voor de registratie zullen hebben getoetst aan de wettelijke eisen. Aangezien het om diensten gaat die juist betrouwbaarheid en integriteit van het elektronische berichtenverkeer beogen te vergroten, is het aannemelijk dat inbreuken op de betrouwbaarheid en de integriteit als gevolg van het optreden van een certificatiedienstverlener niet onopgemerkt blijven en tot claims zullen leiden. Een onderzoek ter plekke van de certificatiedienstverlener is voor zowel de OPTA als de dienstverlener in financiële en in administratieve zin belastend, en dient slechts te worden uitgevoerd indien er aanwijzingen zijn dat de wettelijke regels niet worden nageleefd.

E

*Artikel 15.1*

De leden van de VVD-fractie vragen een nadere toelichting op de wijze waarop het toezicht op accreditatieorganisaties plaatsvindt. Klachten over afzonderlijke certificatiedienstverleners zullen in hoofdzaak bij de OPTA worden neergelegd. Indien een certificatiedienstverlener behoort tot een certificatie- en accreditatieorganisatie heeft hij bij zijn verzoek om registratie aan de OPTA een verklaring van overeenstemming met de wettelijke eisen overgelegd. Deze verklaring van overeenstemming is afgegeven op basis van een onderzoek en een reglement, op grond waarvan de minister van Verkeer en Waterstaat de betrokken accreditatieorganisatie heeft aangewezen. Indien de certificatiedienstverlener inderdaad niet aan de wettelijke eisen blijkt te voldoen, ligt de verantwoordelijkheid daarvoor primair bij hemzelf, maar wellicht ook bij de certificatie- en accreditatieorganisatie, indien die onjuiste informatie heeft gegeven over de wettelijke regels, of indien die bij het overeenstemmingsonderzoek bepaalde aspecten niet heeft onderzocht of juist over het hoofd heeft gezien. Er is aanleiding om bij de accreditatieorganisatie na te vragen op welke wijze is onderzocht of de betrokken certificatiedienstverlener aan het aspect voldeed, ten aanzien waarvan hij in de praktijk steken blijkt te laten vallen. Enerzijds wordt de accreditatieorganisatie erop gewezen dat een aangesloten certificatiedienstverlener niet aan de wettelijke eisen voldoet, hoewel er een verklaring van overeenstemming is afgegeven, zodat de organisatie interne maatregelen kan nemen; anderzijds wordt duidelijk of de aanwijzing van deze accreditatieorganisatie moet worden ingetrokken, op de grond dat zij zich niet aan de eigen reglementen houdt.

F

*Artikel 18.17*

De VVD-fractie vraagt aan welke instanties het toezicht wordt opgedragen inzake de veilige middelen. Veilige middelen voor het aanmaken van elektronische handtekeningen zijn technische producten, die aan de technische eisen van bijlage III van de richtlijn voldoen. De overeenstemmingsbeoordeling met die technische normen moet worden opgedragen aan een technisch instituut dat de kennis en kunde heeft om deze beoordeling te kunnen uitvoeren. De OPTA heeft daarvoor niet de deskundigheid om deze technische taak te gaan uitvoeren. Aangezien er binnen de Europese Unie voldoende technische instituten zijn die de overeenstemmingsbeoordeling kunnen en willen uitvoeren is er geen aanleiding de OPTA met deze nieuwe taak te belasten.
De VVD-fractie vraagt tevens hoe een dergelijke instantie zich verhoudt tot de opmerkingen in de memorie van toelichting onder paragraaf 2.1 dat in

de definitie van de elektronische handtekening bewust geen melding wordt gemaakt van een bepaalde techniek om de voortschrijdende technologische ontwikkeling niet te remmen. Een geavanceerde elektronische handtekening waarvan de definitie is opgenomen in artikel 2, tweede lid, van de richtlijn, kan worden aangemaakt door elke willekeurige techniek zolang aan de in de definitie genoemde voorwaarden wordt voldaan. Daarbij kan gebruik worden gemaakt van een veilig middel. Aan veilige middelen worden in bijlage III van de richtlijn eisen gesteld. Ingevolge artikel 3, vierde lid, van de richtlijn, wordt de daadwerkelijke overeenstemming van veilige middelen voor het aanmaken van elektronische handtekeningen met de eisen van bijlage III vastgesteld door een onafhankelijke instelling, waarop hiervoor is ingegaan.

De fractie van D66 vraagt naar de wijze van toezicht op de instellingen die overeenstemmingsverklaringen afgeven en op bedrijven die middelen ten onrechte als veilig middel op de markt brengen. Dat er bij het zetten van elektronische handtekeningen gebruik is gemaakt van veilige middelen zal moeten blijken doordat al of niet door middel van een overeenstemmingsverklaring van de bedoelde aangewezen instelling de overeenstemming wordt aangetoond. Er is geen aanleiding om erop toe te zien dat alleen veilige middelen worden gebruikt voor het aanmaken van elektronische handtekeningen. Het is in het belang van de gebruiker dat hij zelf erop toeziet dat hij een veilig middel hanteert om de gewenste status van zijn elektronische handtekening te bewerkstelligen.
De instelling wordt aangewezen door de minister, die bij de aanvraag en na de registratie regelmatig zal (laten) toetsen of de instelling aan de richtlijneisen voldoet. De aangewezen instelling heeft geen bevoegdheid om actief te beoordelen of de veilige middelen die als zodanig op de markt worden gebracht ook aan de eisen voldoen. Het is in het belang van de producenten en de gebruikers dat de veilige middelen ook die kwalificatie verdienen. Het is strafbaar ingevolge de Wet op de economische delicten om middelen die niet aan de eisen voldoen als «veilig middel» op de markt te brengen.

De Minister van Justitie,
A. H. Korthals