Eerste Kamer der Staten-Generaal

1

Vergaderjaar 2002–2003 Nr. 35b

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)

NADERE MEMORIE VAN ANTWOORD

Ontvangen 8 april 2003

Met belangstelling heb ik kennis genomen van de nadere vragen die de leden van de fracties van het CDA en de VVD nog hebben gesteld.
De leden van de CDA-fractie vragen hoe de leerstukken van de uitwendige, formele en materiële bewijskracht zich laten toepassen op met en zonder certificaat verstuurde documenten, voorzien van een elektronische handtekening, die rechtsgevolgen kunnen hebben en op die certificaten zelf. Hierbij ware te onderscheiden tussen elektronische handtekeningen met gekwalificeerd en gewoon certificaat.
Een akte is een ondertekend geschrift, bestemd om tot bewijs te dienen (artikel 156, eerste lid, Rv). Daarbij dient onderscheid te worden gemaakt tussen authentieke akten en onderhandse akten. Authentieke akten zijn ingevolge artikel 156, tweede lid, Wetboek van Burgerlijke Rechtsvordering (Rv), akten die door de daartoe bevoegde ambtenaar in de vereiste vorm zijn opgemaakt. Onderhandse akten zijn alle akten die niet authentiek zijn (artikel 156, derde lid, Rv). Bij akten kunnen verschillende soorten bewijskracht worden onderscheiden: de uitwendige bewijskracht (in hoeverre een stuk dat er uitziet als een akte tot op bewijs van het tegendeel voor een akte wordt gehouden), de formele bewijskracht (is door de ondertekenaar verklaard datgene wat in de akte staat?; is waar *dat* er verklaard is?) en de materiële bewijskracht (is waar *wat* de ondertekenaar in de akte heeft verklaard?). De Hoge Raad heeft bij arrest van 3 november 1951 (NJ 1953, 3) bepaald dat aan de vragen omtrent de formele en materiële bewijskracht de vraag vooraf gaat naar de echtheid van een handtekening (uitwendige bewijskracht). Pas indien de echtheid van de handtekening vaststaat, komt men toe aan de vragen over de formele en de materiële bewijskracht.
Hoe kan een elektronische handtekening op «echtheid» worden gecontroleerd? De algemene norm in artikel 3:15a BW maakt het mogelijk dat van verschillende soorten elektronische handtekeningen gebruik kan worden gemaakt. Daarbij kan onderscheid worden gemaakt tussen elektronische handtekeningen die zijn gebaseerd op een gekwalificeerd certificaat, elektronische handtekeningen die zijn gebaseerd op een gewoon

KST67470
ISSN 0921 - 7363
Sdu Uitgevers
's-Gravenhage 2003

certificaat en elektronische handtekeningen die niet zijn gebaseerd op een certificaat. In het algemene deel van de memorie van antwoord is per soort elektronische handtekening uitgebreid beschreven hoe de ontvanger van een bericht dat is ondertekend met een bepaald soort elektronische handtekening de betrouwbaarheid daarvan kan controleren. Kort samengevat kan de ontvanger van een bericht dat is ondertekend met een elektronische handtekening die is gebaseerd op een gewoon of een gekwalificeerd certificaat, de echtheid van de elektronische handtekening onderzoeken door het certificaat te raadplegen dat is meegestuurd of dat is te vinden op de website van de betreffende certificatiedienstverlener. De ontvanger van een bericht dat is ondertekend met een elektronische handtekening die niet is gebaseerd op een certificaat, heeft geen mogelijkheid om de handtekening te verifiëren door middel van een certificaat. Wellicht zijn er andere verificatiemiddelen, maar het merendeel van deze handtekeningen zal worden geaccepteerd enkel vanwege het vertrouwen dat aan het gebruik van een dergelijke handtekening ten grondslag ligt.

De echtheid van een elektronische handtekening kan derhalve worden betwist. Indien er een geschil ontstaat over de geldigheid van een elektronische handtekening gelden dezelfde bewijsregels als voor schriftelijke aktes. Indien bij een ontvangen onderhandse akte de handtekening wordt ontkend door degene wiens handtekening (ogenschijnlijk) onder de akte staat, zal de ontvanger van deze akte moeten bewijzen dat de handtekening «echt» is (artikel 159, tweede lid, Rv). Bij een onderhandse akte bestaat derhalve geen uitwendige bewijskracht. Pas wanneer de handtekening niet wordt betwist of de ontvanger er bij betwisting in slaagt de echtheid van de handtekening te bewijzen, komt men toe aan de formele en de materiële bewijskracht. Wat betreft de formele bewijskracht van een onderhandse akte geldt dat vaststaat dat de ondertekenaar heeft verklaard wat boven zijn handtekening staat. Wat betreft de materiële bewijskracht van een onderhandse akte geldt dat de inhoud van de verklaring voor waar geldt tegen hem die de verklaring heeft afgelegd en ten gunste van hem ten wiens behoeve zij is afgelegd. Ten laste van ieder ander en ten gunste van ieder ander heeft zij vrije bewijskracht.

Voor de uitwendige bewijskracht van een authentieke akte geldt dat het stuk dat er uitziet als een authentieke akte tegenover iedereen voor een authentieke akte wordt gehouden (artikel 159, eerste lid, Rv). De handtekening van de ambtenaar wordt voor echt gehouden. Wat betreft de formele bewijskracht geldt voor de authentieke akte dat partijen en de ambtenaar hebben verklaard wat boven hun handtekening staat. Wat betreft de materiële bewijskracht van een authentieke akte geldt voor hetgeen partijen hebben verklaard (artikel 157, tweede lid, Rv) dat de inhoud van de verklaring voor waar geldt tegen hem die de verklaring heeft afgelegd en ten gunste van hem ten wiens behoeve zij is afgelegd. Ten laste van ieder ander en ten gunste van ieder ander heeft zij vrije bewijskracht. Wat betreft de materiële bewijskracht van een authentieke akte geldt voor hetgeen de ambtenaar heeft verklaard dat de inhoud van de ambtenaarsverklaring tegenover een ieder voor waar geldt (artikel 157, eerste lid, Rv).

Zoals is geantwoord op een vraag van de leden van de fractie van de VVD in de memorie van antwoord zal binnen de grenzen van de artikelen 3:15a en 6:227a BW inderdaad kunnen worden voldaan aan de voor een akte gestelde eisen van ondertekening en schriftelijkheid (art. 156, eerste lid, Rv). In een dergelijk geval ligt gelijkstelling met een akte in de rede, met inbegrip van de daaraan toekomende – binnen de grenzen van artikel 157, tweede lid, Rv dwingende – bewijskracht.

De leden van de CDA-fractie vragen eveneens of een certificatiedienstverlener bij algemene voorwaarden zijn aansprakelijkheid voor het risico dat een website uit de lucht is, uit kan sluiten.

Zowel een certificatiedienstverlener die gewone certificaten uitgeeft als een certificatiedienstverlener die gekwalificeerde certificaten uitgeeft, zou zijn aansprakelijkheid voor het tijdelijk uit de lucht zijn van zijn website bij algemene voorwaarden kunnen uitsluiten ten aanzien van zijn wederpartij. Voor exoneraties in algemene voorwaarden die toepasselijk zijn op overeenkomsten met consumenten bestaat echter een hindernis voor een dergelijke uitsluiting in artikel 6:237 onder f BW. Uit dit artikel vloeit voort dat indien de certificatiedienstverlener een overeenkomst sluit met een natuurlijk persoon die niet handelt in de uitoefening van een beroep of bedrijf, een beding waarbij de certificatiedienstverlener of een derde zich geheel of ten dele bevrijdt van een wettelijke verplichting tot schadevergoeding, wordt vermoed onredelijk bezwarend te zijn. Ingevolge artikel 1.1 onder cc van de Telecommunicatiewet is een certificaat een elektronische bevestiging die gegevens voor het verifiëren van een elektronische handtekening met een bepaalde persoon verbindt en de identiteit van die persoon bevestigt. Het kunnen raadplegen van de website van de certificatiedienstverlener die het certificaat heeft afgegeven, is van cruciaal belang omdat de ontvanger op de website het certificaat kan raadplegen waarmee hij kan verifiëren van wie het bericht afkomstig is indien het certificaat niet reeds direct met het bericht is meegestuurd. Bovendien staan op deze site de statusgegevens van het certificaat waaruit blijkt of het betreffende certificaat nog geldig is. Het certificaat kan immers zijn ingetrokken vanwege diefstal van de bijbehorende smartcard. De website van de certificatiedienstverlener maakt door deze gegevens een dusdanig wezenlijk onderdeel van zijn dienstverlening uit dat hij er alles aan zal moeten doen om deze site in de lucht te houden. Dit is een sterke aanwijzing dat het uitsluiten van aansprakelijkheid voor het uitvallen van de website door certificatiedienstverleners bij overeenkomsten met consumenten inzake certificaten, ook daadwerkelijk onredelijk bezwarend is. Indien de certificatiedienstverlener dit niet kan weerleggen, is het beding waarbij de aansprakelijkheid wordt uitgesloten vernietigbaar op grond van artikel 6:233 onder a BW.
Indien de wederpartij van de certificatiedienstverlener een rechtspersoon is of een beroeps- of bedrijfsmatig handelende persoon geldt voor de uitsluiting van de aansprakelijkheid voor het tijdelijk uit de lucht zijn van een website het vermoeden van artikel 6:237 onder f BW niet. Wel zal in dit geval bij deze overeenkomsten het feit dat een beding bij een overeenkomst met een consument onredelijk bezwarend is, van invloed zijn op de toetsing aan de open norm van artikel 233 sub a BW, vooral in die gevallen waarin de wederpartij een met consumenten vergelijkbare positie inneemt.
De leden van de fractie van het CDA vragen een nadere uiteenzetting waarom aan de toegankelijkheid van de website van de certificatiedienstverlener straks hogere eisen worden gesteld dan aan de toegankelijkheid van het handelsregister, het Kadaster of het repertorium van de notaris. Vooropgesteld moet worden dat aan de website van certificatiedienstverleners die gekwalificeerde certificaten afgeven hogere eisen worden gesteld dan aan die van certificatiedienstverleners die gewone certificaten afgeven. De eerstgenoemde certificatiedienstverleners dienen in tegenstelling tot andere certificatiedienstverleners te voldoen aan de in de algemene maatregel van bestuur (AMvB) en de ministeriële regeling opgenomen eisen, waarvan de raadpleegbaarheid op elk tijdstip van statusgegevens van afgegeven certificaten er één is.
De gegevens die in de gekwalificeerde certificaten en in de certification revocation list (CRL) zijn opgenomen, moeten, om de waarde van de elektronische handtekening voor het internationale elektronische berichtenverkeer tot zijn recht te laten komen, dag en nacht opvraagbaar zijn. De identiteit van de ondertekenaar van een elektronische bevestiging van een handelsorder aan het buitenland, en met name naar landen buiten de Europese Unie, zal in veel gevallen geverifieerd worden op

tijdstippen die niet vallen binnen de reguliere kantooruren in Nederland. De website en de daardoor toegankelijke informatie moeten in verband hiermee voortdurend beschikbaar zijn. Met deze eis wordt aangesloten bij de desbetreffende eisen van de norm ETSI TS 101456, waarin staat dat de informatie 24 uur per dag en 7 dagen per week beschikbaar moet zijn. Bovendien is het voor de gelijkwaardigheid van elektronische en handgeschreven handtekeningen van belang dat zo min mogelijk verschillen tussen beide soorten handtekeningen bestaan. Indien een elektronische handtekening slechts tijdens werktijden geverifieerd zou kunnen worden, zou dat een onnodig verschil opleveren. Onnodig omdat de toegankelijkheid van een website niet in tijd beperkt behoeft te worden omdat er in beginsel geen werknemers nodig zijn om een website in de lucht te houden. Bovendien wezen de leden van de CDA-fractie er in het verslag op, dat zoveel mogelijk voorkomen moet worden dat een wederpartij er voor kiest om geen verificatie bij een certificatiedienstverlener te plegen omdat de website tijdelijk niet raadpleegbaar is. Dit probleem zou alleen nog maar worden vergroot indien de website enkel tijdens werktijden raadpleegbaar zou zijn. Een vergelijking tussen de eisen die worden gesteld aan de toegankelijkheid van de website van de certificatiedienstverlener en die van de toegankelijkheid van bijvoorbeeld het Kadaster is lastig te maken. Het doel van de bereikbaarheid van de website van een certificatiedienstverlener is immers een andere dan die van bijvoorbeeld het Kadaster, waar op dit moment alleen nog de bij wet ingestelde openbare registers en kadastrale kaarten voorzover zij in geautomatiseerde bestanden worden gehouden, kunnen worden geraadpleegd.

Ook vragen de leden van de CDA-fractie of de minister de opsomming van de elementen van de kern van de prestatie van de certificatiedienstverlener op pagina 7 zou willen voltooien.

Uit de definitie van artikel 6:231 onder a BW vloeit voort dat de in het BW opgenomen regeling voor de algemene voorwaarden niet van toepassing is op bedingen die de kern van de prestatie aangeven. Uit de memorie van antwoord zou onbedoeld afgeleid kunnen worden dat in algemene voorwaarden nooit kernbedingen opgenomen zouden mogen worden. Hoewel de kern van de prestatie in beginsel in de overeenkomst zelf zal worden opgenomen, is niet uitgesloten dat er kernbedingen in de algemene voorwaarden staan. Mocht dit laatste het geval zijn, dan zijn deze kernbedingen ingevolge artikel 6:231 onder a BW uitgezonderd van de toepassing van de regeling van de algemene voorwaarden. Bepalend voor de vraag of een beding tot de kern van de prestatie behoort, is of het naar objectieve maatstaven gaat om de kern van de overeengekomen verplichtingen. Uiteindelijk is de uitleg van het begrip «de kern van de prestaties» in artikel 6:231 onder a BW aan de rechter overgelaten. De kern van de prestatie bij de certificatiedienstverlener en zijn wederpartij valt dan ook in zijn algemeenheid niet in een limitatieve opsomming weer te geven omdat dit afhankelijk zal zijn van hetgeen partijen overeen willen komen. In de memorie van antwoord is getracht globaal aan te geven om welke afspraken het zou kunnen gaan. Duidelijk zal in elk geval moeten zijn om welke soort elektronische handtekening het gaat (wel of niet gebaseerd op een gekwalificeerd certificaat) en welke beperkingen aan het gebruik hiervan zijn verbonden. De aan het gebruik van een elektronische handtekening verbonden beperkingen kunnen zeer divers zijn, maar in de meeste gevallen zullen de beperkingen betrekking hebben op de geldigheidsduur (van het gekwalificeerde certificaat) en de soort en de waarde van de eventuele transactie waarvoor de elektronische handtekening mag worden gebruikt.

De leden van de fractie van de CDA vragen of de minister nog aan kan geven hoe de bij de Europese Commissie gemelde gegevens toegankelijk zullen zijn voor advocaten en gerechtsdeurwaarders en in welke talen.

De op grond van artikel 11 van de richtlijn bij de Europese Commissie

genotificeerde gegevens over onder meer de nationale vrijwillige accreditatieregelingen en welke nationale certificatiedienstverleners zijn geaccrediteerd, zijn raadpleegbaar via de volgende (Engelstalige) website van de Europese Commissie: *http://europa.eu.int/informationsociety/eeurope/action plan/safe/esignatures/indexen.htm*. Om de toegankelijkheid van deze site te vergemakkelijken zal op de website van de Onafhankelijke Post- en Telecommunicatieautoriteit (OPTA) en het ministerie van Economische Zaken een verwijzing hiernaar worden opgenomen. Op deze twee laatstgenoemde sites zal bovendien de door Nederland genotificeerde informatie in het Nederlands beschikbaar zijn.
Om te zien of een certificaat niet is ingetrokken zal een ontvanger steeds de Certification Revocation List (CRL) moeten raadplegen. De leden van het CDA geven aan dit niet gebruikersvriendelijk te vinden en vragen of die statusinformatie niet verplicht zou moeten worden meegeleverd bij het gekwalificeerde certificaat dat op het oog technisch eenvoudig te koppelen zou moeten zijn.
Een gekwalificeerd certificaat wordt door de certificatiedienstverlener afgegeven aan de persoon die als ondertekenaar in het certificaat wordt genoemd. In het certificaat zal onder meer de geldigheidsduur van het certificaat zijn opgenomen. De ondertekenaar gebruikt dit certificaat vervolgens, zonder tussenkomst van de certificatiedienstverlener, voor zijn elektronische communicatie. Mogelijk is nu dat de ondertekenaar tijdens de geldigheidsduur van het certificaat zijn private sleutel verliest of dat deze wordt gestolen. In dat geval zal het certificaat nog tijdens de geldigheidsduur moeten worden ingetrokken. Voor een ontvanger van een gekwalificeerd certificaat is het dan ook van groot belang om na te kunnen gaan of het certificaat dat hij heeft ontvangen en waarin een bepaalde geldigheidsduur is opgenomen nog steeds klopt. De ontvanger moet de status van het certificaat kunnen toetsen. Deze statusinformatie is te vinden in de CRL, die raadpleegbaar is via de website van de certificatiedienstverlener die het certificaat uit heeft gegeven. Het certificaat vermeldt welke certificatiedienstverlener het certificaat heeft uitgegeven. De veronderstelde gebruikersonvriendelijkheid zou er in zitten dat de ontvanger van het certificaat zelfstandig de extra handeling van het raadplegen van de site moet uitvoeren. Dit lijkt mij echter overkomelijk. Er is op dit moment geen goed realiseerbaar alternatief voor handen. Het opnemen van statusinformatie in het certificaat is niet wenselijk omdat deze informatie kan veranderen. Indien de statusinformatie zou zijn af te leiden uit het certificaat, zou dit betekenen dat ingeval van diefstal van het certificaat, dit certificaat nog steeds gebruikt kan worden. De ontvanger heeft dan immers geen mogelijkheid om na te gaan of de handtekening is gebruikt door de rechtmatige eigenaar of door de dief. Door de statusinformatie op de website van de certificatiedienstverlener op te nemen kan de ontvanger altijd controleren of het certificaat is ingetrokken. Om redenen van betrouwbaarheid is het daarom beter om statusinformatie te vermelden in een CRL die in beheer is bij een certificatiedienstverlener. Uitgaande van het nut van een CRL die wordt beheerd door een certificatiedienstverlener, blijft de vraag of de zelfstandige handeling van het raadplegen van deze lijst niet vervangen kan worden door een automatische koppeling met het certificaat. Dit zou betekenen dat de ontvanger van een certificaat de CRL niet meer hoeft op te zoeken door het intikken van een webadres of het aanklikken van een hyperlink in het certificaat, maar dat de status van het certificaat automatisch op het beeldscherm verschijnt na ontvangst van een gekwalificeerd certificaat. Om dit technisch mogelijk te maken, is ten eerste een aanpassing vereist in de internationale standaard die de inhoud van (gekwalificeerde) certificaten bepaalt. In deze standaard zal een verplichting moeten worden opgenomen om het webadres van de CRL altijd op een specifieke vaste plaats te vermelden. Ten tweede is een aanpassing vereist van de bestaande applicaties die certificaten gebruiken, waaronder e-mail-

programma's en browsers. De richtlijn verplicht hier niet toe en het is evenmin realistisch. Wel zal via internationale standaardisatiekanalen aandacht worden gevraagd voor de gebruikersvriendelijkheid van de toepassing van elektronische handtekeningen in het algemeen en het raadplegen van de status van een certificaat in het bijzonder.
De leden van de fractie van het CDA vragen een nadere uiteenzetting over waarom geen gebruik wordt gemaakt van artikel 6:110 BW dat de mogelijkheid bevat om de aansprakelijkheid van de certificatiedienstverlener te limiteren bij AMvB.
Zoals in de memorie van antwoord is aangegeven, wordt limitering van aansprakelijkheid in het algemeen slechts toegepast indien de schade dermate hoog kan oplopen dat deze in redelijkheid niet meer verzekerbaar is en evenmin kan worden gedragen door degene op wie de aansprakelijkheid rust. Het was de bedoeling van de wetgever om van artikel 6:110 BW slechts spaarzaam gebruik te maken en alleen wanneer sprake zou zijn van daadwerkelijk gebleken knelpunten. Naar mijn mening is van een dergelijk knelpunt nog geen sprake voor de in artikel 6:196b BW geregelde aansprakelijkheid voor gekwalificeerde schuldaansprakelijkheid met omgekeerde bewijslast voor certificatiedienstverleners die gekwalificeerde certificaten afgeven aan het publiek. De in dit artikel geregelde aansprakelijkheid geldt slechts indien zich een of meer van de in lid 1 onder a tot en met c genoemde gevallen hebben voorgedaan en deze gevallen aan de certificatiedienstverlener zijn toe te rekenen. De certificatiedienstverlener zal moeten bewijzen dat hij niet onzorgvuldig heeft gehandeld door aan te tonen dat hij aan de bij wet, de AMvB en de regeling gestelde eisen heeft voldaan. Deze bewijslast lijkt mij niet onuitvoerbaar. Daarnaast is van belang dat in bijlage II van de richtlijn onder h is bepaald dat de certificatiedienstverlener voldoende financiële middelen tot zijn beschikking moet houden om in overeenstemming met de eisen van de richtlijn te kunnen functioneren, met name met het oog op de gevolgen van aansprakelijkheid wegens schade, bijvoorbeeld door middel van een geëigende verzekering. Deze verplichting is geïmplementeerd in artikel 2, eerste lid, onder e, van het Besluit elektronische handtekeningen. In dat artikel is geen verzekeringsplicht opgelegd maar alleen de verplichting om voldoende financiële middelen ter beschikking te houden. Het is aan de certificatiedienstverlener om te bepalen of hij aan deze verplichting wil voldoen door een verzekering af te sluiten of op een andere manier. Bovendien kan de certificatiedienstverlener ingevolge artikel 6:196b lid 4 BW in het certificaat een grens aangeven voor de waarde van de transacties waarboven het certificaat niet mag worden gebruikt. Mits deze grens kenbaar is voor derden, is de certificatiedienstverlener niet aansprakelijk voor de schade die het gevolg is van een overschrijding van deze grens. Gezien het voorgaande blijft mijn voorkeur er naar uitgaan om alleen dan gebruik te maken van de mogelijkheid om de aansprakelijkheid te limiteren bij AMvB indien is gebleken dat dit noodzakelijk is. Mocht de huidige regeling in de praktijk tot grote problemen aanleiding geven, dan kan van artikel 6:109 BW gebruik worden gemaakt om de onaanvaardbare gevolgen van volledige schadevergoeding ongedaan te maken.
De leden van de fractie van het CDA vrezen dat een CSP alle voorwaarden die in de AMvB worden genoemd tegenover iedere chicane uitputtend zullen moeten kunnen aantonen. Zij vragen of het niet wenselijk zou zijn een standaardregeling op te stellen.
Voorop gesteld zij dat het Besluit elektronische handtekeningen (Besluit) strekt tot implementatie van de bij de richtlijn behorende bijlagen waarbij eisen worden gesteld aan certificatiedienstverleners die gekwalificeerde certificaten afgeven aan het publiek, aan gekwalificeerde certificaten en aan veilige middelen voor het aanmaken van elektronische handtekeningen. Deze eisen zijn, deels geconcretiseerd, in het Besluit opgenomen en dwingendrechtelijk voorgeschreven. In het voorgaande is al aangegeven dat een certificatiedienstverlener die gekwalificeerde certificaten wil

aanbieden of afgeven aan het publiek, verplicht is zich te laten registreren en daarbij aan te tonen dat hij aan de in het Besluit gestelde eisen voldoet. Dit is een publiekrechtelijk en dwingendrechtelijk voorgeschreven regel. Artikel 6:214 BW maakt het mogelijk om een regeling van aanvullend recht op te stellen voor bepaalde soorten overeenkomsten die in een bepaalde bedrijfstak of door een bepaalde groep beroepsbeoefenaren worden gesloten. Een dergelijke standaardregeling is een wet in materiële zin die van rechtswege van toepassing is op de aangewezen bedrijfstak, ook als het bedrijf niet is aangesloten bij een brancheorganisatie. De regeling kan uitsluitend worden gebruikt om rechten en verplichtingen te regelen in de contractuele sfeer. Het gebruik van een standaardregeling in aanvulling op het Besluit en de in artikel 2.1, derde lid, van de Telecommunicatiewet opgenomen registratieplicht is dan ook niet aan de orde omdat het hier geen contractuele sfeer betreft maar publiekrechtelijk en dwingendrechtelijk voorgeschreven verplichtingen. Overigens zou een Nederlandse standaardregeling ook niet wenselijk zijn omdat het Besluit en het wetsvoorstel dienen ter uitvoering van een Europese richtlijn. Het is uiteindelijk aan het Europese Hof van Justitie om te oordelen over de uitleg van de in het Besluit en het wetsvoorstel opgenomen eisen.
Voor wat betreft het kunnen aantonen door de certificatiedienstverlener dat hij voldoet aan de in het Besluit opgenomen eisen, kan nog het volgende worden opgemerkt. Een wettelijk verplichte toetsing voorafgaand aan de registratie zou in strijd zijn met de in artikel 3, eerste lid, van de richtlijn opgenomen bepaling dat het verlenen van certificatiediensten niet afhankelijk mag zijn van voorafgaande machtiging. De certificatiedienstverleners mogen zelf bepalen hoe wordt voldaan aan de in het Besluit gestelde eisen. De eisen die gesteld worden aan certificatiedienstverleners die actief zijn op de Nederlandse markt, zijn op deze wijze wel geharmoniseerd, maar niet gekoppeld aan een verplichte standaard. Een koppeling zou de toegang tot de Nederlandse markt voor certificatiediensten kunnen belemmeren voor buitenlandse certificatiedienstverleners, en omgekeerd de toegang tot de buitenlandse markten voor Nederlandse certificatiedienstverleners. Er zijn door Europese standaardisatie organisaties inmiddels wel standaarden ontwikkeld die certificatiedienstverleners kunnen hanteren om aan de eisen te voldoen. Certificatiedienstverleners kunnen zich vrijwillig laten toetsen op de overeenstemming met de essentiële eisen, door accreditatie-organisaties die daartoe door de Minister van Economische Zaken zijn aangewezen. Deze accreditatie-organisaties kunnen voor deze toetsing gebruik maken van de in Europa ontwikkelde standaarden en doen dat ook reeds. In zoverre zal vrijwillige standaardisering door de marktpartijen kunnen worden geïntroduceerd.
Voor de identiteitscontrole bij het gekwalificeerde certificaat zullen veel eisen worden gesteld. Dat betekent een ingewikkelde AMvB en een aantal ministeriële regelingen. Ware het niet wenselijk, dat de AMvB wordt voorgehangen? In het wetsvoorstel is bepaald dat ingevolge artikel 18.15, derde lid, van de Telecommunicatiewet een certificatiedienstverlener, alvorens een gekwalificeerd certificaat af te geven, de identiteit van de persoon die als ondertekenaar in dat gekwalificeerde certificaat wordt aangeduid, vaststelt aan de hand van de bij artikel 1 van de Wet op de identificatieplicht aangewezen geldige documenten. Bij artikel 2, eerste lid, onder g, van de AMvB is bepaald dat de identiteitscontrole ten behoeve van de afgifte van een gekwalificeerd certificaat geschiedt aan de hand van een visuele vergelijking, en zonodig met behulp van andere daartoe geschikte middelen, van de persoon met de gegevens van de bij artikel 1 van de Wet op de identificatieplicht aangewezen documenten. De certificatiedienstverlener moet alle gegevens waarmee de verificatie van de identiteit heeft plaatsgevonden gedurende een bepaalde periode opslaan om deze identificatiewijze op een later tijdstip aan te kunnen tonen (artikel 2, eerste lid, onder i, van de AMvB). Deze werkwijze, in

combinatie met voorschriften over de beveiliging van opgeslagen persoonsgegevens, vloeit voort uit de richtlijn en vereist geen ingewikkeld of van de normale identificatiepraktijk afwijkend regelgevingkader. Een noodzaak om de gedelegeerde regelgeving aan nadere voorwaarden te verbinden acht ik niet aanwezig.
Tot slot vroegen de leden van de CDA-fractie hoe het staat met de voorlichting, vooral omdat het wenselijk is, dat ook het MKB met gekwalificeerde handtekeningen zal gaan werken? Bij de Directie Voorlichting van het ministerie van Justitie is een factsheet te verkrijgen waarin wordt ingegaan op de feiten en achtergronden van dit wetsvoorstel. Deze factsheet is eveneens raadpleegbaar via de website van het ministerie van Justitie en binnenkort via die van het ministerie van Economische Zaken. Daarnaast is speciaal voor ondernemers een boekje samengesteld, getiteld: «Nederland Gaat Digitaal: Netjes volgens het boekje, de spelregels voor elektronisch zakendoen». Dit boekje beoogt een handleiding voor de praktijk te zijn door aan de hand van een vraag- en antwoordstructuur en vele praktijkvoorbeelden de relevante wet- en regelgeving die mogelijk van toepassing is bij het elektronisch handelsverkeer te behandelen. Aan de hand van een hierin opgenomen stroomschema kan een ondernemer snel bepalen wanneer welke regels wel of niet op zijn bedrijf van toepassing zijn. De elektronische handtekening is een van de aspecten die in dit boekje aan de orde komen. Zowel het ministerie van Economische Zaken als het ministerie van Justitie hebben aan de totstandkoming van dit boekje bijgedragen. Voor vragen over de in dit boekje behandelde onderwerpen kunnen ondernemers terecht bij een van de vijftien Syntensvestigingen voor gratis workshops en spreekuren. Daarnaast bestaat de mogelijkheid om via de website van ECP.NL juridische informatie te verkrijgen. Bovendien zal ook nog na de totstandkoming van dit wetsvoorstel en de daarop gebaseerde lagere regelgeving uitvoerig voorlichting worden gegeven. Duidelijk moge zijn dat het gebruik van elektronische handtekeningen die zijn gebaseerd op een gekwalificeerd certificaat voor iedereen openstaat. Naar verwachting zal het gebruik van deze elektronische handtekening ook voor het midden- en kleinbedrijf aantrekkelijk zijn. Voor specifieke voorlichting aan deze doelgroep wordt en zal gebruik worden gemaakt van daartoe geëigende kanalen, zoals brancheorganisaties en Syntens.
De leden van de VVD-fractie vragen om aan de hand van vier gegeven voorbeelden aan te geven wanneer er sprake is van certificaten die zijn afgegeven aan het publiek en er derhalve geen sprake is van een beperking van het toepassingsgebied tot een besloten groep.
De woorden «aan het publiek» zijn opgenomen omdat er in de richtlijn geen behoefte bestond (rechtsoverweging 16) om een regelgevend kader op te nemen voor elektronische handtekeningen die uitsluitend worden gebruikt in systemen die berusten op vrijwillige privaatrechtelijke overeenkomsten tussen een vastgesteld aantal deelnemers. Nu deze bewoordingen aan de richtlijn zijn ontleend, zal het uiteindelijk ook het Europese Hof van Justitie zijn om te oordelen of sprake is van certificaten die zijn afgegeven aan het publiek of niet. Bij de beantwoording van de vraag of een certificaat is afgegeven aan het publiek zal richtinggevend zijn of het certificaat is afgegeven aan een ondertekenaar die behoort tot een groep waarvan de omvang is beperkt alsmede of het toepassingsgebied waarvoor het certificaat is afgegeven, beperkt is. Indien het certificaat is bedoeld voor een onbeperkte groep ondertekenaars, ofwel het algemene publiek, en een onbeperkt toepassingsgebied zal sprake zijn van een certificaat dat is afgegeven aan het publiek. Beperkingen ten aanzien van de groep waarvoor het certificaat is bestemd, zullen moeten blijken uit de overeenkomst of anderszins. Duidelijkheid over het beoogde toepassingsgebied dient uit het certificaat zelf te blijken (artikel 3, onder i, van het Besluit). Voor de door de leden van de fractie van de VVD gegeven voorbeelden betekent dit het volgende.

Het eerste voorbeeld betreft een franchisegroep waarbij de franchisegever zelf certificaten uitgeeft. Deze certificaten kunnen worden gebruikt in het elektronische verkeer met alle zelfstandige ondernemingen die deel uitmaken van de franchisegroep. Indien de franchisegever aan de klanten van de franchisegroep gekwalificeerde certificaten verstrekt enkel voor het verrichten van transacties met ondernemingen die deel uitmaken van deze franchisegroep en deze certificaten niet kunnen worden gebruikt voor transacties daarbuiten, is geen sprake van gekwalificeerde certificaten die zijn afgegeven aan het publiek. Aan het criterium dat de groep in omvang onbeperkt is, is wel voldaan maar het toepassingsgebied is besloten omdat het is beperkt tot transacties met ondernemingen die deel uitmaken van de franchisegroep.
In het tweede voorbeeld geeft de moedermaatschappij van een financieel concern, bestaande uit een aantal banken, verzekeraars, lease-maatschappijen en effecteninstellingen, certificaten uit die kunnen worden gebruikt in het elektronische verkeer met alle onderdelen van het concern. Ook in dit voorbeeld geldt dat de moedermaatschappij van een financieel concern aan zijn klanten gekwalificeerde certificaten verstrekt enkel voor het verrichten van transacties met ondernemingen die deel uitmaken van dit concern en deze certificaten niet kunnen worden gebruikt voor transacties met ondernemingen daarbuiten. Ook hier is derhalve geen sprake van gekwalificeerde certificaten die zijn afgegeven aan het publiek. Aan het criterium dat de groep in omvang onbeperkt is, is wel voldaan maar het toepassingsgebied is besloten omdat het is beperkt tot transacties met ondernemingen die deel uitmaken van dit concern.
In het derde voorbeeld is sprake van een beheerder van een internet marktplaats die certificaten uitgeeft aan ondernemingen die een overeenkomst tot deelneming aan de marktplaats hebben gesloten met de beheerder. Deze certificaten kunnen worden gebruikt in het elektronische verkeer met alle ondernemingen die zijn aangesloten bij de marktplaats en via de marktplaats zaken met elkaar doen. In dit voorbeeld verstrekt de beheerder van de internet marktplaats aan elke onderneming die daartoe een overeenkomst met de beheerder sluit een gekwalificeerd certificaat. De certificaten kunnen worden gebruikt in het elektronische verkeer met de andere deelnemende ondernemingen. Indien het sluiten van de overeenkomst met de beheerder de enige voorwaarde is om in aanmerking te kunnen komen voor een certificaat dan is de omvang van de groep onbeperkt. Of ook het toepassingsgebied onbeperkt is, is lastig te bepalen zonder verdere gegevens. Indien de certificaten ook voor toepassingen buiten de internet marktplaats gebruikt zouden kunnen worden, zou sprake zijn van een onbeperkt toepassingsgebied. In dat geval zijn zowel de groep als het toepassingsgebied onbeperkt en zal sprake zijn van certificaten die zijn afgegeven aan het publiek. Indien de certificaten echter alleen gebruikt kunnen worden voor het elektronisch verkeer via deze marktplaats dan is het toepassingsgebied beperkt. In dat geval is geen sprake van certificaten die zijn afgegeven aan het publiek aangezien het toepassingsgebied beperkt is.
In het vierde voorbeeld heeft een onafhankelijke derde (TTP) een systeem opgezet dat beoogt ondernemingen een zekere mate van vertrouwen te geven bij het doen van zaken met hun onbekende ondernemingen in het buitenland. Aan het systeem kan worden deelgenomen indien men een daartoe strekkende overeenkomst heeft gesloten met de TTP. Deelnemende ondernemingen krijgen van de TTP een certificaat dat zij kunnen gebruiken in het elektronische verkeer met andere ondernemingen die deelnemen aan het systeem. Daarnaast verleent de TTP andere diensten aan de deelnemende ondernemingen, zoals het op verzoek verstrekken van een creditrating van de wederpartij. In dit voorbeeld verstrekt de TTP een gekwalificeerd certificaat aan elke onderneming die daartoe een overeenkomst met de TTP sluit. De certificaten kunnen worden gebruikt in het elektronische verkeer met de andere aan dit systeem deelnemende

ondernemingen. Indien het sluiten van de overeenkomst met de TTP de enige voorwaarde is om in aanmerking te kunnen komen voor een certificaat dan is de omvang van de groep onbeperkt. Het toepassingsgebied is eveneens onbeperkt omdat het gebruik van het certificaat blijkens het voorbeeld niet aan beperkingen is onderworpen en derhalve gebruikt kan worden voor al het elektronische verkeer. In dit geval is dus sprake van certificaten die zijn afgegeven aan het publiek.

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