De regulering van elektronische handtekeningen

SIMONE VAN DER HOF

De handgeschreven handtekening wordt in bepaalde – in verschillende rechtsstelsels overigens zeer uiteenlopende – gevallen over het algemeen in combinatie met een geschrift door de wet vereist. Voorbeelden van wettelijke vormvereisten in de Nederlandse wetgeving zijn artikel 8:412 BW (cognossement) en artikel 2 AW (overdracht auteursrechten). Ook wanneer de wet geen vormvoorschriften bevat, kunnen partijen er op grond van bewijsoverwegingen behoefte aan hebben om hun overeenkomst in een ondertekend geschrift vast te leggen.

Mr. S. van der Hof
is senior onderzoeker bij het Centrum voor Recht, Bestuur en Informatisering, Universiteit van Tilburg.
E-mail: svdrhof@uvt.nl

Met de opkomst van de elektronische handel zijn vragen ontstaan omtrent de rechtsgeldigheid van elektronische overeenkomsten en elektronische handtekeningen in het licht van wettelijke vormvoorschriften alsmede in het licht van het bewijsrecht. De behoefte aan rechtszekerheid bij elektronische communicatie en aan betrouwbare oplossingen voor het elektronisch ondertekenen daarvan – verder ook als elektronische authenticatie aangeduid – heeft wereldwijd tot een ware stortvloed aan wet- en regelgeving geleid.[1]
In het kielzog van de *1995 Utah Digital Signature Act*, de eerste wet op het gebied van elektronische authenticatie, hebben vele staten en landen al dan niet vergelijkbare wetgeving op dit gebied voorbereid of reeds afgekondigd. Vanuit Europese optiek is in dit verband relevant Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen. Deze richtlijn moest vóór 19 juli 2001 in de nationale wetgeving van de lidstaten zijn geïmplementeerd; een datum die door de Nederlandse wetgever ruimschoots is overschreden. In dit artikel zal worden ingegaan op het Nederlandse implementatievoorstel dat inmiddels bij de Eerste Kamer ligt en in najaar 2002 in werking zou moeten treden, alsmede op enkele implementatieverschillen in de elektronische handtekeningwetgeving van de lidstaten van de Europese Unie. Allereerst is het echter van belang enig inzicht te verschaffen in de terminologie met betrekking tot elektronische authenticatie en de verschillende benaderingen die bij de regulering van elektronische handtekeningen worden gehanteerd.

Terminologie | Voor een goed begrip van het onderwerp is het belangrijk om te onderscheiden tus-

sen het overkoepelende begrip 'elektronische handtekeningen' en het minder ruime begrip 'digitale handtekeningen'.
Onder 'elektronische handtekeningen' worden verstaan de informatietechnologische alternatieven voor een handmatige handtekening in algemene zin. Voorbeelden van elektronische handtekeningen zijn de pincode, de gescande handtekening en op biometrie of encryptie gebaseerde technologieën. Biometrie is een techniek, waarbij gebruik wordt gemaakt van persoonskenmerken, zoals fysieke of gedragskenmerken. Deze methode omvat onder meer handtekeningen door middel van de digitale pen, waarbij druk en snelheid tijdens het tekenen worden gemeten en getoetst aan de voor de betreffende persoon in een database opgeslagen waarden. Andere biometrische methoden zijn identificatie door middel van iris- of gezichtsherkenning. Een speciale vorm van de elektronische handtekening is het laatstgenoemde voorbeeld, namelijk de op encryptie gebaseerde methode. Deze methode wordt aangeduid met de term 'digitale handtekening'.
Encryptie is een proces, waarmee gegevens met behulp van een wiskundig algoritme en een – uit een reeks getallen bestaande – sleutel worden versleuteld, zodat deze voor onbevoegden onleesbaar worden. Op die manier kunnen partijen op vertrouwelijke wijze met elkaar communiceren. Met een specifieke vorm van encryptie – asymmetrische encryptie genoemd – kunnen partijen bovendien elektronische documenten digitaal tekenen. In dat geval wordt gesproken van een digitale handtekening.

E-paspoort alternatief voor papieren paspoort

Vooral voor laatstgenoemde techniek bestaat in de praktijk en daarmee tevens onder wetgevers grote belangstelling, omdat deze op basis van zijn eigenschappen het best in staat wordt geacht de handgeschreven handtekening te vervangen. Echter, ook biometrische methoden zijn momenteel sterk in opkomst. Veelal wordt zelfs een combinatie van beide technieken toegepast in elektronische authenticatiesystemen. Een dergelijke aanpak wordt bijvoorbeeld overwogen voor het project van de Nederlandse overheid dat ziet op de ontwikkeling van een elektronisch nationaal identiteitsbewijs. Het is de bedoeling dat dit e-paspoort het elektronische alternatief voor het papieren paspoort wordt.

Benaderingen in elektronische handtekeningregulering | In regulering op het gebied van elektronische authenticatie is in de loop der jaren een drietal benaderingen ontstaan:
1 digitale handtekeningbenadering;
2 hybride of tweesporenbenadering;
3 functionele benadering.[2]

Digitale handtekeningbenadering | De digitale handtekeningbenadering richt zich uitsluitend op regulering van de digitale handtekeningtechnologie en wordt daarmee beschouwd als technologie-afhankelijke regelgeving. Onder deze benadering kunnen drie verschijningsvormen worden geïdentificeerd. Ten eerste is er de technische variant, waarbij de digitale handtekening middels een juridisch instrument tot technische standaard wordt verheven. Wetgeving die in deze categorie valt, behandelt niet de juridische status van de digitale handtekening, ofschoon er mogelijk wel impliciete juridische consequenties aan een – volgens de eisen van een dergelijke wet – gebruikte digitale handtekening kunnen worden verbonden. Een voorbeeld van de benadering is het – inmiddels vervangen – Duitse *Signaturgesetz* 1997. Ten tweede bestaat er een juridische variant, waaronder wetgeving wordt begrepen die de digitale handtekening reguleert vanuit het oogpunt van juridische gelijkstelling met de handgeschreven handtekening. Het doel van dergelijke wetgeving is om aldus rechtszekerheid te verschaffen omtrent het gebruik van deze techniek ter vervulling van vormvoorschriften en/of in het licht van het bewijsrecht. Een voorbeeld van deze variant is de eerdergenoemde *Utah Digital Signature Act*. Ten derde kan een organisatorische variant worden onderscheiden die slechts aspecten rondom de voor het gebruik van digitale handtekeningen benodigde infrastructuur regelt. Een juridische gelijkstelling van handgeschreven handtekening en digitale handtekening vindt onder deze variant evenwel niet plaats. Een voorbeeld van deze variant is het Nederlandse TTP.NL-raamwerk dat door het Nationale TTP-project is opgesteld.[3]

Hybride benadering | Het inzicht dat wetgeving op basis van de digitale handtekeningbenadering mogelijk slechts een zeer beperkte levensduur heeft of op zijn minst nieuwe ontwikkelingen onvoldoende ondersteund, heeft een andere benadering ten aanzien van de regulering van de elektronische authenticatieproblematiek tot gevolg gehad. Hierdoor heeft de digitale handtekeningbenadering als zelfstandige benadering sterk of aan belang ingeboet. De hybride benadering is onder meer gevolgd door de Europese wetgever in Richtlijn 1999/93/EG betreffende elektronische handtekeningen.
Onder deze benadering heeft de wetgever de digitale handtekening als een bij uitstek geschikt middel voor elektronische authenticatie weliswaar niet los willen laten, maar tevens gekozen voor een meer open benadering die ruimte laat voor nieuwe ontwikkelingen. Voor zogeheten *advanced electronic signatures* wordt een uitgebreid eisenpakket in de wet neergelegd, op grond waarvan deze specifieke elektronische

handtekeningen vanuit juridisch oogpunt volledig worden gelijkgesteld met de handgeschreven handtekening. De definitie van deze elektronische handtekeningen verwijst in het bijzonder of onder de huidige stand van de technologie zelfs uitsluitend naar digitale handtekeningtechnieken. Dit deel van de wetgeving lijkt dan ook sterk op de manier waarop wetgeving onder de juridische variant van de digitale handtekeningbenadering is vormgegeven. Daarnaast wordt aan gewone elektronische handtekeningen eveneens, zij het geen absolute, juridische geldigheid toegekend. De juridische status van niet als *advanced* aangemerkte elektronische handtekeningen is in beginsel dus minder sterk en wordt overgelaten aan de rechterlijke waardering .

Juridische gelijkstelling elektronische en handgeschreven handtekening

Functionele benadering | De functionele benadering adresseert geen enkele specifieke techniek en is een vorm van volledig techniekneutrale wetgeving. Onder deze benadering wordt de aandacht gericht op de functies die een handtekening in een bepaalde situatie – bijvoorbeeld bij een concreet vormvoorschrift – dient te vervullen teneinde doelmatig te zijn. Dergelijke wet- of regelgeving schrijft niet een specifieke wijze voor waarop dat dient te gebeuren – bijvoorbeeld door toepassing van de digitale handtekeningtechniek – maar geeft meer algemeen aan dat de methode voldoende betrouwbaar moet zijn in het licht van het doel waarvoor het wordt gebruikt.
De in 1996 door de *UNCITRAL* aangenomen *Model Law on Electronic Commerce* is internationaal het meest bekende voorbeeld van de functionele benadering en heeft verschillende wetgevers reeds tot voorbeeld gediend. Een verschil met de eerdergenoemde voorbeelden is niet alleen gelegen in de gekozen benadering, maar tevens in het feit dat de *Model Law* niet enkel gaat over handtekeningen maar meer in het algemeen over vormvoorschriften. Dat is niet onbegrijpelijk, aangezien handtekening en geschrift in de fysieke wereld vrijwel onlosmakelijk met elkaar verbonden zijn en de functies die beide vervullen veelal onderling samenhangen.

Implementatie van Richtlijn 1999/93/EG in Nederland | In Nederland is het wetsvoorstel 27 743 dat voorziet in de implementatie van Richtlijn 1999/93/EG betreffende elektronische handtekeningen door de Tweede Kamer aangenomen. Inmiddels heeft de Vaste Commissie voor Justitie van de Eerste Kamer in mei 2002 naar aanleiding van een voorbereidend onderzoek van het wetsvoorstel enkele opmerkingen en vragen aan de betrokken ministers voorgelegd. Het wachten is thans op een behandeling van het wetsvoorstel door de Eerste Kamer. De belangrijkste wijzigingen waarin het wetsvoorstel voorziet, zijn die welke betrekking hebben op het Burgerlijk Wetboek en de Telecommunicatiewet.

Infrastructuur voor e-handtekeningen | De wijzigingen in de Telecommunicatiewet betreffen voornamelijk de infrastructuur die noodzakelijk is voor het gebruik van elektronische handtekeningen. Aangezien elektronische handtekeningen een individualiserend karakter ontberen, is het noodzakelijk om de elektronische handtekening door middel van digitale certificaten onlosmakelijk aan een bepaalde persoon te verbinden. Digitale certificaten worden verstrekt door zogeheten certificatiedienstverleners. In het wetsvoorstel wordt een onderscheid gemaakt tussen gewone en gekwalificeerde certificaten (ontwerpartikel 1.1 onder cc respectievelijk onder dd). Gekwalificeerde certificaten dienen – anders dan het gewone certificaat – aan strenge wettelijke organisatorische en technische vereisten te voldoen. De vereisten betreffen onder meer de betrouwbaarheid van de certificatiedienstverlener, de inhoud van het gekwalificeerde certificaat en veiligheid van de middelen (lees: soft- en hardware) voor het genereren van elektronische handtekeningen. Voorts voorziet het wetsontwerp in toezicht op certificatiedienstverleners die gekwalificeerde certificaten afgeven aan het publiek. Deze certificatiedienstverleners zullen zich moeten registreren bij de Onafhankelijke Post- en Telecommunicatieautoriteit (OPTA) en worden door deze instantie aan controle onderworpen (ontwerpartikel 2.1 lid 3). Voor registratie zullen certificatiedienstverleners moeten aantonen dat zij aan de gestelde wettelijke vereisten voldoen (ontwerpartikel 18.15). Dit kan gebeuren door het overleggen van de relevante informatie dan wel middels een verklaring van een door het Ministerie van Verkeer en Waterstaat aangewezen organisatie (ontwerpartikel 2.1 leden 3 en 4). De concrete eisen waaraan de certificatiedienstverleners alsmede de veilige middelen voor het aanmaken van elektronische handtekeningen moeten voldoen, zullen bij AMvB nader worden uitgewerkt.

Rechtsgeldigheid van e-handtekeningen | De aanpassingen in het Burgerlijk Wetboek betreffen de rechtsgeldigheid van de elektronische handtekeningen. In Boek 3 Titel 1 zullen daartoe in een nieuw in te voegen Afdeling 1A betreffende het elektronisch vermogensrechtelijk verkeer een aantal bepalingen worden geïntroduceerd. Ontwerpartikel 15a bepaalt onder welke voorwaarden een juridische gelijkstelling tussen handgeschreven en elektronische handtekening plaatsvindt. Het volgt daarin niet alleen Richtlijn 1999/93/EG, maar tevens de *UNCITRAL Model Law on Electronic Commerce* door in de bepaling een op

de functionele benadering gebaseerde open norm op te nemen (zie lid 1). Dit houdt in dat een elektronische handtekening dezelfde rechtsgevolgen heeft als een traditionele handtekening, indien de toegepaste methode voor elektronische authenticatie voldoende betrouwbaar is met het oog op het doel waarvoor deze werd gebruikt.

Verder onderscheidt de bepaling tussen de gewone en de geavanceerde elektronische handtekening. De gewone elektronische handtekening bestaat uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd met andere elektronische gegevens en die worden gebruikt als middel voor authenticatie (zie lid 4). De geavanceerde elektronische handtekening is een gewone handtekening, waaraan uitdrukkelijk enkele nadere vereisten worden gesteld:

1 zij is op unieke wijze aan de ondertekenaar verbonden;
2 zij maakt het mogelijk om de ondertekenaar te identificeren;
3 zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden; en
4 zij is op zodanige wijze aan het elektronische bestand verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord.

De eerste beide vereisten impliceren dat er sprake moet zijn van een digitaal certificaat. Het laatste vereiste leidt tot de veronderstelling dat bij de huidige stand van de techniek onder een geavanceerde elektronische handtekening in het bijzonder de digitale handtekening wordt verstaan.
De geavanceerde elektronische handtekening wordt vermoed voldoende betrouwbaar te zijn, indien – naast vervulling van voorgaande vereisten – sprake is van een gekwalificeerd certificaat en de elektronische handtekening is gegenereerd door een veilig middel; beide in de zin van de te wijzigen Telecommunicatiewet (zie lid 2). Overigens betekent het ontbreken van een gekwalificeerd certificaat en een veilig middel in voornoemde zin niet dat elektronische handtekening onvoldoende betrouwbaar is (lid 3). Bij een gewone elektronische handtekening wordt de waardering van deze handtekening als bewijs – als vanouds – aan de rechter overgelaten. Artikel 15a zal overigens regelend recht vormen, zodat partijen de vrijheid hebben zelf een methode van elektronisch ondertekenen overeen te komen en dienaangaande het gewenste betrouwbaarheidsniveau te bepalen (lid 6). Dit niveau kan bijvoorbeeld afhankelijk zijn van de (financiële) belangen die bij een transactie gepaard gaan. Bij *high-value* transacties bestaat naar verwachting een grotere behoefte aan veiligheid en betrouwbaarheid van de gebruikte methode dan bij *low-value* transacties.
Het daaropvolgende ontwerpartikel 15b gaat in op de geldigheid van in derdelanden – zijnde niet-EU-lidstaten – uitgegeven gekwalificeerde certificaten en bepaalt dat deze onder de in het artikel genoemde voorwaarden een gelijke status hebben met een in een lidstaat uitgegeven gekwalificeerd certificaat. Ontwerpartikel 15c bepaalt ten slotte dat de voorgaande bepalingen overeenkomstige toepassing vinden buiten het vermogensrecht, voorzover de aard van de rechtshandeling of van de rechtsbetrekking zich daartegen niet verzet.

Aansprakelijkheid van certificatiedienstverleners | Evenals in de Telecommunicatiewet zal ook in het Burgerlijk Wetboek onderscheid worden gemaakt tussen gewone en gekwalificeerde certificaten en wel voor wat betreft het aansprakelijkheidsregime. Voor certificatiedienstverleners in het algemeen geldt het algemene aansprakelijkheidsregime, terwijl voor certificatiedienstverleners die gekwalificeerde certificaten uitgeven aan het publiek voorts wordt voorzien in schuldaansprakelijkheid met omgekeerde bewijslast (ontwerpartikel 196b). Op grond van een nieuw in te voeren Afdeling 4A (aansprakelijkheid bij elektronisch rechtsverkeer) is deze certificatiedienstverlener – tenzij hij bewijst niet onzorgvuldig te hebben gehandeld – aansprakelijk voor schade van een persoon die in redelijk vertrouwen op grond van het certificaat heeft gehandeld. De schade moet betrekking hebben op:

1 de juistheid van alle in het certificaat opgenomen gegevens op het tijdstip van afgifte;
2 de opneming van alle voor dit certificaat voorgeschreven gegevens;
3 de garantie dat degene die in het certificaat als ondertekenaar is geïdentificeerd, op het tijdstip van afgifte van het certificaat, tevens de houder van de gegevens voor het aanmaken van een elektronische handtekening is en die gegevens overeenstemmen met de in het certificaat opgenomen gegevens voor het verifiëren van de elektronische handtekening; en

4 de garantie dat de gegevens voor het aanmaken van een elektronische handtekening en het verifiëren ervan – indien beide door de certificatiedienstverlener werden gegenereerd – complementair zijn (zie lid 1).

Tevens is de certificatiedienstverlener aansprakelijk voor schade ingevolge nalatigheid bij de registratie van ingetrokken – en dus niet langer geldige – gekwalificeerde certificaten (lid 2). De certificatiedienstverlener kan in het gekwalificeerde certificaat beperkingen aan het gebruik opnemen en is vervolgens niet aansprakelijk voor schade als gevolg van gebruik van het certificaat dat strijdig is met deze beperkingen (lid 3). Een voorbeeld van een mogelijke beperking is dat het certificaat alleen mag worden gebruikt bij transacties die een bepaalde geldelijke waarde niet overschrijden (zie ook lid 4).

Vormvoorschriften | Overigens zij opgemerkt dat daar waar Richtlijn 1999/93/EG slechts bewijsrechtelijk relevantie heeft,[4] de Nederlandse wetgever er uitdrukkelijk voor heeft gekozen om de juridische erkenning van elektronische handtekeningen breder te trekken door deze in Boek 3 van het BW (rechtshandelingen) te plaatsen en niet in het Wetboek van Burgerlijke Rechtsvordering. Tevens zal met de implementatie van Richtlijn 2000/31/EG betreffende de elektronische handel worden aangegeven op welke wijze langs elektronische weg aan een eventueel geschriftvereiste voor overeenkomsten kan worden voldaan (ontwerpartikel 6:227a BW).[5] Beide aspecten – de elektronische handtekening enerzijds en het elektronische geschrift anderzijds – worden in de behandelde wetsvoorstellen helaas niet met elkaar in verband gebracht. Hierdoor blijft bijvoorbeeld de vraag open of en, zo ja, onder welke voorwaarden sprake kan zijn van een elektronische akte in de zin van artikel 183 Rv.

Enkele implementatieverschillen tussen de EU-lidstaten | Richtlijn 1999/93/EG is inmiddels in de meeste lidstaten van de Europese Unie geïmplementeerd, zodat het mogelijk is om enkele verschillen tussen de geresulteerde wetgeving te kunnen aangeven. Ter wille van de afbakening zullen hier slechts enkele grove lijnen worden geschetst en volgt geen uitputtende vergelijking van de elektronische handtekeningwetgeving in de lidstaten van de Europese Unie.
Bij een vergelijking van de nationale elektronische handtekeningenwetgeving van de lidstaten is het allereerst van belang om te onderkennen dat de richtlijn middels een aparte handtekeningenwet kan zijn geïmplementeerd of door middel van (wijzigingen) in meerdere wetten. Het eerste is bijvoorbeeld het geval in België en Oostenrijk; het tweede onder meer in Duitsland en Nederland.
Voorts zijn er ook tal van inhoudelijke verschillen tussen de lidstaten. De definities die zijn gebruikt kunnen uiteenlopen. Zo kent Denemarken – anders dan andere lidstaten – een integriteitsvereiste voor (gewone) elektronische handtekeningen. Verder hebben sommige lidstaten – zoals Duitsland en Oostenrijk – gedetailleerdere en/of zwaardere vereisten voor certificatiedienstverleners of gekwalificeerde certificaten. Voor wat betreft Duitsland kan dit worden verklaard doordat het land reeds vóór Richtlijn 1999/93/EG een strenge handtekeningenwet kende die gericht was op de digitale handtekeningtechniek (digitale handtekeningbenadering). Ten tijde van de totstandkoming van de – aan de richtlijn – aangepaste nieuwe handtekeningenwetgeving had een aantal bedrijven reeds grote investeringen gedaan om onder de strenge criteria van de oude wet als certificatiedienstverlener te worden geaccrediteerd. Om deze bedrijven niet al te zeer te benadelen, zijn de vereisten – in vergelijking met andere lidstaten – aan de strenge kant gebleven. Een mogelijke andere of aanvullende verklaring is dat de Duitse wetgever – zo bleek reeds uit het oude *Signaturgesetz* – de lat voor het veiligheids- en betrouwbaarheidsniveau op het gebied van elektronische authenticatie hoger legt dan wetgevers in andere lidstaten.
Een verder verschil kan worden gevonden in de begrenzing van het onderwerp. Terwijl de Duitse wetgeving vormvoorschriften als geheel behandelt door de regulering van elektronische handtekeningen en elektronische documenten te combineren, ziet de wetgeving in andere lidstaten – zoals Nederland, Ierland en het Verenigd Koninkrijk – slechts op de regulering van elektronische handtekeningen. De Duitse wetgeving richt zich in dat geval overigens wel uitsluitend op de gekwalificeerde elektronische handtekening. In de andere voornoemde lidstaten vindt echter een juridische erkenning van de elektronische handtekening in het algemeen plaats, die in het Verenigd Koninkrijk overigens wel weer beperkt is tot het bewijsrecht. Eerder werd in dit verband reeds gerefereerd aan de ruime functionele benadering ten aanzien van elektronische handtekeningen die in de Nederlandse wetgeving zal worden ingevoerd. Overigens is door de Nederlandse overheid altijd al aangenomen dat elektronische handtekeningen ook zonder specifieke regelgeving – zoals noodzakelijk ten gevolge van de implementatieplicht ten aanzien van Richtlijn 1999/93/EG – onder het vrije bewijsstelsel door de rechter konden worden erkend. Dat is naar alle waarschijnlijkheid ook de reden dat er voorheen nooit Nederlandse wetgevingsinitiatieven op het gebied van de elektronische handtekening zijn ontplooid.[6]

Tot besluit | Richtlijn 1999/93/EG wordt in de lidstaten op verschillende wijzen geïmplementeerd. Hierdoor wordt een volledige harmonisatie in de regulering van elektronische handtekeningen niet

bereikt. Overigens behoeft dat vanuit de Europese wetgever bezien niet problematisch te zijn, indien de doelen van de richtlijn – juridische erkenning van de elektronische handtekening en vrij verkeer van elektronische handtekeningendiensten – in de Europese Unie worden gewaarborgd. Vooralsnog zijn er geen tekenen dat dit niet zo is. Voor bedrijven die zich als certificatiedienstverlener in de Europese Unie willen vestigen, kan het – vanwege de uiteenlopende nationale vereisten die aan deze vorm van dienstverlening worden gesteld – echter raadzaam zijn om een lidstaat met een 'gunstig' reguleringsklimaat te zoeken. Internationaal gezien kunnen de vrij strikte eisen die door de richtlijn aan geavanceerde elektronische handtekeningen worden gesteld belemmerend werken bij in het bijzonder de erkenning van buitenlandse digitale certificaten maar ook het internationaal elektronisch handelen meer in het algemeen. Voor buitenlandse certificatiedienstverleners gelden namelijk dezelfde vereisten als voor in de Europese Unie gevestigde certificatiedienstverleners en deze kunnen zeer wel als te streng (lees: te duur) worden ervaren. Voorts kan in een aantal landen, waaronder de Verenigde Staten, over de afgelopen jaren een tendens worden onderkend, waarbij de digitale handtekeningbenadering plaats heeft moeten maken voor de meer open functionele benadering. Dat betekent dat digitale certificaten een minder prominente betekenis krijgen bij de juridische gelijkstelling tussen de traditionele en de elektronische handtekening en het hoge niveau van de geavanceerde elektronische handtekening niet langer wordt vereist. Elektronische handtekeningen uit deze landen zullen in de Europese Unie naar verwachting veelal slechts de status van gewone elektronische handtekening hebben. Voor dergelijke landen kan deze status mogelijk te veel rechtsonzekerheid opleveren; zeker wanneer de betreffende lidstaat – zoals Duitsland – als weinig liberaal op het gebied van elektronische handtekeningen bekendstaat.

Links bij dit artikel vindt u op <http://www.javisite.nl>

Noten

1 Voor een uitgebreid overzicht van wet- en regelgeving betreffende elektronische handtekeningen alsmede ontwikkelingen daaromtrent wordt verwezen naar de *Digital Signature Law Survey*, die online beschikbaar is op: <http://rechten.uvt.nl/simone/ds-lawsu.htm>.

2 Zie uitgebreider Babette Aalberts & Simone van der Hof, *Digital Signature Blindness, Analysis of legislative approaches toward electronic authentication*, ITeR-serie nr. 32, Kluwer: Deventer 2000.

3 TTP staat voor *Trusted Third Party*. De hierna te behandelen certificatiedienstverlener is een soort TTP.

4 Zie in dit verband artikel 1 lid 2 Richtlijn 1999/93/EG dat als volgt luidt: 'Deze richtlijn heeft geen betrekking op aspecten die verband houden met de totstandkoming of geldigheid van contracten of andere wettelijke verbintenissen waarvoor het nationale of het Gemeenschapsrecht vormvereisten voorschrijven en laat de regels en beperkingen onverlet die het nationale of het Gemeenschapsrecht voorschrijven voor het gebruik van documenten'.

5 Zie TK 2001-2001, 28 197, nrs. 1-2.

6 Zie echter Nota Wetgeving voor de elektronische snelweg, Vergaderjaar 1997-1998, 25 880, nrs. 1-2, p. 5-6. Zie ook MDW-rapport Elektronisch verrichten van rechtshandelingen, Commissie Huls, maart 1998.