De elektronische handtekening: rechten en plichten van de certificatiedienstverlener, de certificaathouder en de vertrouwende derde

Veerle VANDENABEELE[1]

Samenvatting

De Wet van 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten introduceert de noties "certificaat" en "certificatiedienstverlener".

In haar bijdrage ontleedt de auteur de rechten en verplichtingen van de partijen die bij de uitgifte en het gebruik van een certificaat komen kijken.

Résumé

La loi du 9 juillet 2001 fixant certaines règles relatives au cadre juridique pour les signatures électroniques et les services de certification introduit les notions de 'certificat' et de 'prestataire de service de certification'.

Dans sa contribution l'auteur analyse les droits et obligations des parties impliquées dans l'émission et l'utilisation d'un certificat.

1. Inleiding

De recente Wetten van 20 oktober 2000 en 9 juli 2001 hebben de elektronische handtekening en het bijhorende certificaat een vaste plaats gegeven in ons Belgisch recht. De Wet van 20 oktober 2000[2] voert het gebruik van de moderne telecommunicatiemiddelen en de elektronische handtekening in de gerechtelijke en buitengerechtelijke procedure in. De Wet van 9 juli 2001[3], die de Europese Richtlijn 1999/93/EC[4] in het Belgisch recht implementeert ("de Richtlijn"), introduceert de noties "certificaat" en "certificatiedienstverlener".

Dit artikel heeft als doel een schets te maken van de rechten en verplichtingen van de partijen die bij de uitgifte en het gebruik van een certificaat komen kijken, nl. de certificatiedienstverlener, de certificaathouder en de ontvanger van het ondertekende bericht (de "vertrouwende derde" of "relying party").

De Wet van 9 juli 2001 bevat immers geen rechten of verplichtingen van de certificatiedienstverlener, de certificaathouder of de vertrouwende derde in verband met "gewone" elektronische handtekeningen en "gewone" certificaten, behoudens de mogelijke gelijkschakeling van dergelijke elektronische handtekening met een handgeschreven handtekening. Bijgevolg zullen deze rechten en verplichtingen geregeld worden door het gemeen recht: contractueel voor de verhouding tussen certificatiedienstverlener en certificaathouder, extracontractueel tussen de certificatiedienstverlener, de certificaathouder en de vertrouwende derde.

Hoofdstuk V van de Wet van 9 juli 2001 legt bepaalde verplichtingen op aan de certificatiedienstverleners die gekwalificeerde certificaten afgeven en hoofdstuk VI van dezelfde wet regelt de verplichtingen van de certificaathouders. De wet legt aan de vertrouwende derde geen verplichtingen op, maar deze geniet van een aantal rechten die voortvloeien uit de aansprakelijkheid van de certificatiedienstverlener. De verhouding tussen de drie partijen is echter verre van volledig geregeld door de wet, en in verband met de uitgifte en het gebruik van niet-gekwalificeerde certificaten is zelfs helemaal niets geregeld.

Daarom hebben de verschillende belanghebbende partijen in het Public Key Infrastructure of PKI- en e-commercegebeuren (dienstverleners, gebruikers, fabrikanten, onderzoekers, ...) het initiatief genomen om naast de technische standaarden die zij opstellen in het kader van verenigingen zoals EEMA[5] ("The European Forum for Electronic Business"), EESSI ("European Electronic Signature Standardisation Initiative")[6] en ETSI ("European Telecommunications Standards Institute")[7], ook de rechten en verplichtingen van partijen bij het afgeven en gebruiken van certificaten vast te leggen. De meest gebruikte standaard is heden ETSI TS 101 456 genaamd "Policy requirements for certification authorities issuing qualified certificates" en diens opvolger TS102 042, die de standaarden uitbreidt naar genormaliseerde certificaten.[8]

2. Korte beschrijving van de elektronische handtekening, het certificaat en de certificatiedienstverlener

Teneinde de rechten en plichten van de certificatiedienstverlener, de certificaathouder en de vertrouwende derde te kunnen schetsen, is een basisbegrip van de concepten elektronische handtekening, certificaat en certificatiedienstverlener, gedefinieerd in de Wet van 9 juli 2001, noodzakelijk. Hierna volgt een korte schets van deze begrippen, zonder de

1. Bedrijfsjurist.
2. Wet 20 oktober 2000 tot invoering van het gebruik van telecommunicatiemiddelen en van de elektronische handtekening in de gerechtelijke en de buitengerechtelijke procedure, *B.S.* 22 december 2000.
3. Wet 9 juli 2001 houdende vaststelling van bepaalde regels in verband met het juridisch kader voor elektronische handtekeningen en certificatiediensten, *B.S.* 29 september 2001.
4. Richtlijn 1999/93/EG van het Europees Parlement en de Raad van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen, *PB. L.* 13/12 van 19 januari 2000.
5. www.eema.org.
6. www.ict.etsi.org/eessi/EESSI-homepage.
7. www.etsi.org.
8. Genormaliseerde certificaten zijn certificaten met dezelfde veiligheidsgraad als gekwalificeerde, maar uitgegeven voor andere doeleinden dan de handtekening en daarom niet onderworpen aan de Richtlijn of de Wet van 9 juli 2001.

intentie te hebben hierover zo exhaustief te zijn zoals vele auteurs dit reeds in het verleden hebben gedaan.[9]

2.1. De elektronische handtekening

Er bestaat verwarring tussen de termen "elektronische" en "digitale" handtekening. Het verschil tussen beide is nochtans belangrijk, zowel juridisch als technisch.

2.1.1. Algemeen aanvaarde definitie van de elektronische handtekening[10]

De term "elektronische handtekening" is een algemene term die gebruikt wordt om eender welke digitale markering aan te duiden die aanwijst dat een partij door een document gebonden is of die de authenticiteit van een document vastlegt. Het is derhalve een zeer algemene term die zowel kan verwijzen naar een scan van een "papieren" handtekening als naar de getypte vermelding aan het einde van een elektronisch document "getekend: X".

De term verwijst m.a.w. geenszins naar een bepaalde zekerheid of meerwaarde die door de handtekening aan het document zou worden verleend.

2.1.2. Algemeen aanvaarde definitie van de digitale handtekening

De digitale handtekening is een bepaalde soort elektronische handtekening, gebaseerd op asymmetrische encryptie en met bepaalde eigen kenmerken.

2.1.2.1. ASYMMETRISCHE ENCRYPTIE

Asymmetrische encryptie betekent dat twee verschillende sleutels gebruikt worden om veilige verrichtingen te verzekeren: een privé-sleutel (enkel gekend door de eigenaar) en een publieke sleutel (voor iedereen toegankelijk gemaakt door de certificatiedienstverlener). Beide sleutels zijn wiskundig complementair via een "hashfunctie" of algoritme dat een digitale weergave creëert van het bericht. Iedere wijziging van het bericht resulteert in een andere digitale weergave van het bericht bij gebruik van dezelfde hashfunctie.

De verzender van het bericht (de certificaathouder) ondertekent het bericht met zijn private sleutel. De ontvanger van het bericht (de vertrouwende derde) vindt de publieke sleutel van de verzender in diens certificaat dat door de certificatiedienstverlener publiek gemaakt werd, doorgaans op diens website, en gebruikt deze sleutel om de handtekening te verifiëren.

Deze soort encryptie/decryptie wordt asymmetrisch genoemd wanneer het technisch onmogelijk is de private sleutel af te leiden uit de publieke.

Eén bepaalde digitale handtekening, gebaseerd op dergelijke asymmetrische encryptie, heeft automatisch dezelfde kracht als een handgeschreven handtekening (zie verder: de geavanceerde handtekening gebaseerd op een gekwalificeerd certificaat en gecreëerd met een veilig middel voor het aanmaken van handtekeningen).

2.1.2.2. KENMERKEN VAN DE DIGITALE HANDTEKENING

Vier kenmerken karakteriseren de digitale handtekening: authentificatie van de ondertekenaar, authentificatie van het bericht, onmogelijkheid tot ontkenning, en integriteit. De onmogelijkheid tot ontkenning en de authentificatie van de ondertekenaar hebben betrekking op de persoon die de handtekening plaatst. De authentificatie van het bericht, en de integriteit hebben betrekking op het ondertekende bericht op zich. Het gebruik van asymmetrische cryptografie kan ook de vertrouwelijkheid van het bericht garanderen.

– *Onmogelijkheid tot ontkenning:* het feit dat een bericht enkel kan getekend worden met gebruik van de private sleutel van de ondertekenaar bewijst de oorsprong van de gegevens. Het beschermt de ontvanger tegen de eventuele ontkenning door de verzender/ondertekenaar dat hij de gegevens gestuurd heeft. De private sleutel bevindt zich immers op een drager waartoe enkel de ondertekenaar geacht wordt toegang te hebben. Daarenboven maakt het feit dat de ondertekenaar zijn private sleutel dient te gebruiken hem bewust van het feit dat hij een handeling stelt die juridische gevolgen kan hebben.
– *Authentificatie van ondertekenaar en bericht:* het proces van aanmaken en verifiëren van een digitale handtekening verleent een grote zekerheid dat de handtekening wel degelijk deze is van de ondertekenaar. In vergelijking met de papieren wereld is de echtheid van de digitale handtekening zeer gemakkelijk na te gaan en veel beter gegarandeerd. De digitale handtekening kan bovendien niet worden vervalst, tenzij ingeval de ondertekenaar de controle over de private sleutel verliest. De handtekening toont aan wie een document of bericht getekend heeft en is moeilijk na te maken. Dit

9. Zie o.m.: D. GOBERT en E. MONTERO, "La signature dans les contrats et les paiements électroniques: l'approche fonctionnelle", *DAOR* 2000, n° 53, 17-39; M. ANTOINE en D. GOBERT, "La Directive Européenne sur la signature électronique. Vers la sécurisation des transactions sur l'Internet?", *J.T. dr. eur.* 2000, n° 68, 73-78; M. ANTOINE en D. GOBERT, "Pistes de réflexion pour une législation relative à la signature digitale et au régime des autorités de certification", *R.G.D.C.* 1998, 285-310; E. WÉRY, "La Belgique achève le cadre légal de la signature électronique et des services de certification", http://www.droit-technologie.org; E. WÉRY, "La signature électronique fait dorénavant partie du droit belge!", http://www.droit-technologie.org; J. DUMORTIER en S. VAN DEN EYNDE, "De juridische erkenning van de elektronische handtekening in België", *Computerrecht* 2001, 185-195; M.E. STORME, "De invoering van de elektronische handtekening in ons bewijsrecht – Een inkadering van en commentaar bij de nieuwe wetsbepalingen", *R.W.* 2000-01, 1505-1525.
10. www.reallegal.com.

verzekert de authentificatie van de verzender/ondertekenaar, maar ook van het bericht zelf: de digitale handtekening identifiëert het ondertekende bericht of document op een manier die het onmogelijk maakt het ondertekende bericht te wijzigen.
– *Integriteit:* er kan worden nagegaan of het bericht niet gewijzigd of vervangen werd tijdens het versturen, en dit met een veel hogere zekerheidsgraad dan ingeval van een papieren document. Bij verificatie zal immers de minste wijziging van het bericht aan het licht komen, aangezien de vergelijking van de hashresultaten (één bij verzending en één bij ontvangst) zal aantonen of het bericht al dan niet intact is gebleven.

De normale digitale handtekening waarborgt niet de vertrouwelijkheid van de verzending. Het systeem van de PKI laat echter toe om met het gebruik van een tweede sleutelpaar het bericht te encrypteren en aldus de vertrouwelijkheid ervan te garanderen.

2.1.3. De elektronische handtekening en haar bewijswaarde

De Wet van 9 juli 2001 voerde de volgende definitie in het Belgische recht in:

Artikel 2.2°: *"Elektronische handtekening: gegevens in elektronische vorm, vastgehecht aan of logisch geassocieerd met andere elektronische gegevens, die worden gebruikt als middel voor authentificatie"*.

Deze definitie sluit duidelijk aan bij de hoger vermelde algemeen aanvaarde definitie van elektronische handtekening, en toont aan dat de wetgever een technologisch neutraal wettelijk kader wenst te creëren.

De bewijswaarde van de elektronische handtekening is niet automatisch en wordt negatief gedefinieerd in artikel 4 § 5 van de Wet van 9 juli 2001:

"Een elektronische handtekening kan geen rechtsgeldigheid worden ontzegd en niet als bewijsmiddel in gerechtelijke procedures worden geweigerd louter op grond van het feit dat:
– *de handtekening in elektronische vorm is gesteld; of*
– *niet gebaseerd is op een gekwalificeerd certificaat; of*
– *niet gebaseerd is op een door een geaccrediteerd certificatiedienstverlener afgegeven certificaat; of*
– *niet met een veilig middel is aangemaakt"*.

Artikel 2 van de Wet van 20 oktober 2000 voegt hieraan toe:

Artikel 2: *"Artikel 1322 van het Burgerlijk Wetboek wordt aangevuld met het volgende lid: 'Kan, voor de toepassing van dit artikel, voldoen aan de vereiste van een handtekening, een geheel van elektronische gegevens dat aan een bepaalde persoon kan worden toegerekend en het behoud van de integriteit van de inhoud van de akte aantoont'"*.

Of met andere woorden: de elektronische handtekening kan, geval per geval, door de rechter gelijkgeschakeld worden met een handgeschreven handtekening of niet.

2.1.4. De geavanceerde elektronische handtekening en haar bewijswaarde

De geavanceerde elektronische handtekening wordt in artikel 8, 2° van de Wet van 9 juli 2001 als volgt gedefinieerd:

"Elektronische gegevens vastgehecht aan of logisch geassocieerd met andere elektronische gegevens, die worden gebruikt als middel voor authentificatie en aan de volgende eisen voldoet:
a) zij is op unieke wijze aan de ondertekenaar verbonden;
b) zij maakt het mogelijk de ondertekenaar te identificeren;
c) zij wordt aangemaakt met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
d) zij is op zodanige wijze aan de gegevens waarop zij betrekking heeft verbonden, dat elke latere wijziging van de gegevens kan worden opgespoord".

Het betreft met andere woorden een elektronische handtekening die voldoet aan de vereisten om als digitale handtekening bestempeld te worden.

Artikel 4 § 4 van de Wet van 9 juli 2001 stelt dan ook de geavanceerde elektronische handtekening gelijk met een handgeschreven handtekening, op voorwaarde dat zij (i) gebaseerd is op een gekwalificeerd certificaat en (ii) aangemaakt is met een veilig middel voor het aanmaken van een handtekening, algemeen in technische teksten *"secure signature creation device"* genoemd en afgekort als SSCD.

De SSCD kan een smartcard zijn of een "token", speciaal ontworpen voor het genereren en behouden van de private sleutel van de ondertekenaar. Zij dienen in overeenstemming te zijn met de vereisten van Bijlage III van de Wet van 9 juli 2001 en kunnen goedgekeurd worden door bevoegde instanties. Heden is nog geen enkele SSCD officieel goedgekeurd.

2.2. Het certificaat

2.2.1. Het certificaat

Het certificaat wordt door de Wet van 9 juli 2001 als volgt gedefinieerd:

Artikel 2, 3°: *"Een elektronische bevestiging die de gegevens voor het verifiëren van de handtekening*[11] *koppelt aan een natuurlijke persoon of een rechtspersoon en de identiteit van die persoon bevestigt"*.

11. Met "gegevens voor het aanmaken van een handtekening" wordt in de Wet van 9 juli 2001 de private sleutel aangeduid, en met "gegevens voor het verifiëren van een handtekening" de publieke.

Het certificaat is dus een elektronisch document dat met de ondertekende boodschap wordt meegestuurd en dat de gegevens vermeldt waarvan de ondertekenaar/certificaathouder de certificatie wenst.

2.2.2. Het gekwalifieerde certificaat

Het gekwalifieerde certificaat is een certificaat dat voldoet aan de vereisten van Bijlage I van de Wet van 9 juli 2001 en uitgegeven wordt door een certificatiedienstverlener die voldoet aan de vereisten van Bijlage II van dezelfde wet[12] (zie art. 2, 4°).

De vereisten van Bijlage I hebben betrekking op de inhoud van het certificaat en dienen om de identificatie van de certificaathouder te verzekeren en de grenzen (zoals bijvoorbeeld geldigheidsduur, grenzen met betrekking tot de waarde van de transacties waarvoor het certificaat kan worden gebruikt, ...) van het certificaat aan te duiden. Het bevat onder meer de naam van de certificatiedienstverlener en de publieke sleutel van de certificaathouder.

Het certificaat is geldig zolang het niet herroepen is. De certificatiedienstverlener zal het certificaat herroepen wanneer bijvoorbeeld (i) de geldigheidsduur verstreken is, (ii) de gegevens voor het aanmaken van de handtekening gecompromitteerd zijn[13], (iii) de gegevens in het certificaat niet meer geldig zijn[14], naar gelang van het geval op eigen initiatief of op initiatief van de certificaathouder. Het is ook mogelijk het certificaat tijdelijk op te schorten. De status van het certificaat kan worden nagegaan in een elektronisch register dat de certificatiedienstverlener bijhoudt ("Certificate Revocation List" of "CRL").

2.3. De certificatiedienstverlener

De Wet van 9 juli 2001 definieert de certificatiedienstverlener als volgt:

Artikel 2, 10°: *"Elke natuurlijke persoon of rechtspersoon die certificaten afgeeft en beheert of andere diensten in verband met elektronische handtekeningen verleent"*.

Het betreft dus een "trusted third party" of "TTP" die de gegevens certificeert waarvan de certificaathouder de certificatie vraagt, en waarop de ontvanger van een getekend bericht vertrouwt bij het verifiëren van de handtekening.

Enkel certificatiedienstverleners die voldoen aan de vereisten van Bijlage II van de Wet van 9 juli 2001 mogen gekwalificeerde certificaten uitgeven. Deze vereisten hebben betrekking op de betrouwbaarheid en de manier van werken van de certificatiedienstverlener. Volgens artikel 4 § 2 van dezelfde wet dienen deze certificatiedienstverleners zich te melden bij het bevoegde bestuur als gedefinieerd in de wet.

Tot de commerciële certificatiedienstverleners die actief zijn op de Belgische markt en certificaten aan het publiek afgeven behoren Globalsign, Isabel en Belgacom E-Trust.[15]

3. De verhouding tussen de certificatiedienstverlener en de houder van het certificaat

3.1. Wettelijke verplichtingen van de certificatiedienstverlener ten opzichte van de certificaathouder: hoofdstuk V van de Wet van 9 juli 2001

Zoals hoger reeds vermeld, gelden de verplichtingen van de Wet van 9 juli 2001 enkel voor de certificatiedienstverleners die gekwalificeerde certificaten uitreiken. Het staat de andere certificatiedienstverleners vrij contractueel andere rechten en plichten met hun klanten af te spreken.

De certificatiedienstverlener, als TTP, certificeert in het certificaat de gegevens waarvan de kandidaat-certificaathouder de certificatie verzoekt. Daarom legt artikel 8 van de Wet van 9 juli 2001 hem bepaalde plichten op in verband met het uitreiken van een certificaat.

Zo is de certificatiedienstverlener gehouden om de complementariteit van de gegevens voor het aanmaken en verifiëren van de handtekening (private en publieke sleutel) na te gaan vooraleer een certificaat af te leveren. Hij is eveneens gehouden de gegevens waarvan de certificatie verzocht wordt, zoals onder meer de identiteit van de kandidaat-certificaathouder, te verifiëren.

De certificatiedienstverlener moet op eenvoudig verzoek van de certificaathouder diens certificaat herroepen. In de gevallen waarin de certificatiedienstverlener gemachtigd is op eigen initiatief het certificaat te herroepen, dient hij de certificaathouder hiervan gemotiveerd op de hoogte te brengen. Wanneer hij het certificaat herroept omdat het vervalt, dient hij de houder hiervan minstens één maand op voorhand in te lichten.

Bij stopzetting van zijn activiteiten dient de certificatiedienstverlener die gekwalificeerde certificaten afgeeft de nodige maatregelen voor continuïteit te treffen (art. 15): ofwel laat hij zijn activiteit overnemen door een andere certificatiedienstverlener die een zelfde kwaliteits- en veiligheidsniveau waarborgt, ofwel herroept hij de certificaten twee maanden na de houders ervan te hebben ingelicht.

12. Zie hieronder, onder 2.3.
13. B.v. ingeval van verlies van het token.
14. B.v. ingeval van een certificaathouder wiens functie gewijzigd werd.
15. Te bereiken via respectievelijk: nl.globalsign.net, www.isabel.be en www.e-trust.be.

3.2. Wettelijke verplichtingen van de certificaathouder ten opzichte van de certificatiedienstverlener: hoofdstuk VI van de Wet van 9 juli 2001

De wettelijke verplichtingen van de certificaathouder bestaan zowel ten voordele van de certificatiedienstverlener als van de vertrouwende derde.

De certificaathouder is verantwoordelijk voor de vertrouwelijkheid van de private sleutel. Eens deze niet meer gegarandeerd is, dient hij onmiddellijk aan de certificatiedienstverlener te vragen het certificaat te herroepen. Hij moet dit ook vragen wanneer de in het certificaat opgenomen gegevens niet meer met de werkelijkheid overeenstemmen. Met andere woorden heeft de certificaathouder de plicht de certificatiedienstverlener te verwittigen wanneer de informatie die hij certificeert onjuist zou worden of indien de vertrouwelijkheid van de private sleutel niet meer gegarandeerd zou zijn. Het onmiddellijk intrekken van het certificaat valt onder de verantwoordelijkheid van de certificatiedienstverlener.

Eens het certificaat vervallen of herroepen – en dus niet meer geldig –, mag de voormalige certificaathouder de bijbehorende sleutels niet meer gebruiken in verband met een ander certificaat.

4. De verhouding tussen de certificatiedienstverlener en de vertrouwende derde

4.1. Wettelijke verplichtingen van de certificatiedienstverlener ten opzichte van de vertrouwende derde (art. 14 van de Wet van 9 juli 2001)

Hier ligt de belangrijkste en zwaarste verantwoordelijkheid van de certificatiedienstverlener. De wetgever heeft echter een bijkomende beperking ingelast: artikel 14 geldt enkel voor certificatiedienstverleners die gekwalificeerde certificaten afgeven *aan het publiek*. Prestaties in het kader van gesloten gebruikersgroepen zijn derhalve uitgesloten.

Artikel 14 § 1 stelt de certificatiedienstverlener aansprakelijk voor de schade die hij toebrengt aan elke vertrouwende derde die, als goede huisvader, redelijkerwijze vertrouwen stelt in het certificaat, voor wat betreft:

– de juistheid van alle gegevens die in het gekwalificeerd certificaat zijn opgenomen op de datum dat het werd afgegeven en de vermelding, in dit certificaat, van alle voorgeschreven gegevens voor een gekwalificeerd certificaat;
– de garantie dat de in het gekwalificeerde certificaat geïdentificeerde ondertekenaar op het tijdstip van de afgifte van het certificaat de gegevens bevat voor het aanmaken van de handtekening overeenstemmend met de in het certificaat vermelde of geïdentificeerde gegevens voor het verifiëren van de handtekening;
– de garantie dat de gegevens voor het aanmaken en die voor het verifiëren van een handtekening complementair kunnen gebruikt worden, ingeval de certificatiedienstverlener beide soorten gegevens genereert;

tenzij de certificatiedienstverlener bewijst dat er van geen enkele nalatigheid sprake is.

Eerst en vooral dient de certificatiedienstverlener derhalve de gegevens waarvan hem de certificatie wordt gevraagd, na te gaan. Hij mag de kandidaat-certificaathouder niet op diens woord geloven, maar dient deze gegevens voor zover het in zijn macht ligt, te verifiëren. Zo kan de identiteit en geboortedatum en -plaats bijvoorbeeld m.i. voldoende geverifieerd worden door de kandidaat-certificaathouder in persoon zijn aanvraag te laten doen en hem daarbij een kopie van zijn identiteitskaart te laten afgeven. De certificatiedienstverlener is eveneens aansprakelijk voor het vermelden van alle gegevens voor een gekwalificeerd certificaat en derhalve voor de overeenstemming met Bijlage I van de Wet van 9 juli 2001.

De certificatiedienstverlener dient eveneens, bij afgifte van het certificaat, na te gaan of de publieke sleutel wel bij de private sleutel past en of zij voldoen aan de vereisten voor compatibiliteit met een gekwalificeerd certificaat. Net zoals bij de verplichting in verband met de juistheid van de gecertificeerde gegevens, geldt deze verplichting enkel op het ogenblik van afgifte van het certificaat, en is de certificaathouder daarna verplicht om de herroeping van het certificaat aan te vragen van zodra deze gegevens zouden wijzigen.

Ingeval de certificatiedienstverlener de sleutels zelf aanmaakt, is hij bovendien aansprakelijk voor hun onderlinge complementariteit.

Artikel 14 § 2 stelt dezelfde certificatiedienstverlener aansprakelijk voor de schade die hij toebrengt aan elke vertrouwende derde die, als goede huisvader, redelijkerwijze vertrouwen stelt in het certificaat wanneer hij heeft nagelaten de herroeping van het certificaat te laten registreren, tenzij de certificatiedienstverlener bewijst dat er van geen enkele nalatigheid sprake is.

Zodra de certificatiedienstverlener vanwege de certificaathouder een aanvraag tot herroeping ontvangen heeft (art. 12 § 1) of het certificaat moet herroepen om één van de redenen beschreven in artikel 12 § 2 moet hij dat onmiddellijk doen. De notie "onmiddellijk" is niet gedefinieerd en zal m.i. geval per geval geïnterpreteerd worden in functie van de mogelijkheden van de door de certificatiedienstverlener gebruikte infrastructuur en software en van de verificatietaken die hij moet uitvoeren alvorens het certificaat te kunnen herroepen. De certificatiedienstverlener deelt in zijn Certification Practice Statement ("CPS", zie verder) aan het publiek mee op welke wijze hij het certificaat intrekt en hoe hij het begrip "onmiddellijk" invult.

Een kort voorbeeld kan dit verduidelijken: wanneer certificaathouder A vreest dat zijn private sleutel niet meer ver-

trouwelijk is, is het A's verantwoordelijkheid zijn certificatiedienstverlener te vragen dit certificaat te herroepen. Doet hij dit niet en blijft hij het certificaat gebruiken, is de certificatiedienstverlener niet verantwoordelijk voor de schade die aangericht wordt wanneer bijvoorbeeld B de private sleutel gebruikt. Doet hij dit wel zal de certificatiedienstverlener zoals in de CPS beschreven nagaan of het verzoek wel van de certificaathouder komt (b.v. door het gebruikte paswoord na te gaan) en het certificaat intrekken. De certificatiedienstverlener zal ten opzichte van iedere vertrouwende derde aansprakelijk zijn voor alle schade aangericht door het gebruik van het certificaat na de aanvraag tot herroeping.

Volgens *artikel 14 § 3* is de certificatiedienstverlener niet aansprakelijk voor de schade die voortvloeit uit het overschrijden van de aangegeven gebruiksbeperkingen wanneer deze beperkingen in het certificaat aangegeven zijn en voor derden herkenbaar. Hetzelfde geldt voor schade die voortvloeit uit het overschrijden van de aangegeven maximumwaarde van de transacties waarvoor het certificaat gebruikt kan worden (art. 14 § 4).

Wanneer bijvoorbeeld certificaathouder C een certificaat bezit waarin duidelijk vermeld wordt dat hij zijn werkgever slechts tot een bepaald bedrag kan verbinden, zal de certificatiedienstverlener niet aansprakelijk zijn voor de schade die een vertrouwende derde zou lijden ingeval C deze limiet overschrijdt. De certificatiedienstverlener zal wel aansprakelijk zijn indien deze limiet niet duidelijk in het certificaat was vermeld.

4.2. Wettelijke verplichtingen van de vertrouwende derde ten opzichte van de certificatiedienstverlener

De wet legt geen verplichtingen op aan de vertrouwende derde. Men dient daarom terug te vallen op de algemene regels betreffende buitencontractuele aansprakelijkheid, aangevuld met het feit dat de vertrouwende derde, door op het certificaat te vertrouwen, de rechten en verplichtingen die hem in het Certification Practice Statement van de certificatiedienstverlener worden toegekend, heeft aanvaard (zie verder onder punt 6.4.).

5. De verhouding tussen de houder van het certificaat en de vertrouwende derde

5.1. Wettelijke verplichtingen van de certificaathouder ten opzichte van de vertrouwende derde (hoofdstuk VI van de Wet van 9 juli 2001)

De verplichtingen van de certificaathouder hoger beschreven onder 3.2. zijn even zoveel verplichtingen ten opzichte van de vertrouwende derde, aangezien ook hij beschermd dient te worden tegen het vertrouwen op gegevens die niet correct meer zijn of waarvan de herkomst niet meer gegarandeerd kan worden.

5.2. Wettelijke verplichtingen van de vertrouwende derde ten opzichte van de certificaathouder

De wet legt geen verplichtingen op aan de vertrouwende derde.

6. In de praktijk: de contractuele documenten

Teneinde de door de wet geregelde rechten en verplichtingen te verduidelijken en aan te vullen (voor wat gekwalificeerde certificaten betreft) of teneinde duidelijke afspraken, vaak geïnspireerd op de Wet van 9 juli 2001, vast te leggen i.v.m. niet-gekwalificeerde certificaten, hebben de verschillende spelers op de markt (certificatiedienstverleners, gebruikers, softwareproducenten, gebruikers, onderzoekers, ...) op Europees vlak bepaalde standaarden gecreëerd. Het document ETSI TS 101 456 genaamd "Policy requirements for certification authorities issuing qualified certificates" stelt standaarden voor voor het opstellen van Certificate Policies ("CP") en Certification Practice Statements ("CPS"). Teneinde de zaken praktisch overzichtelijk te maken voor zichzelf en zijn klant/certificaathouder zal de certificatiedienstverlener hieraan doorgaans nog een bestelbon en algemene voorwaarden toevoegen.

6.1. De bestelbon

Net zoals voor ieder ander product, zal de kandidaat-certificaathouder zijn certificaat bij de certificatiedienstverlener bestellen door middel van een bestelbon. Dit document heeft echter i.v.m. certificaten een bijkomend belang, aangezien het alle gegevens bevat waarvan de kandidaat-certificaathouder de certificatie verzoekt. Wanneer deze gegevens betwist worden, zal de bestelbon derhalve een belangrijk contractueel hulpmiddel zijn om aan te tonen welke opdracht door de kandidaat-certificaathouder aan de certificatiedienstverlener gegeven werd.

De wijze waarop de certificatiedienstverlener deze gegevens nagaat, wordt doorgaans uiteengezet in de bestelbon, de CP en de CPS. Dit is uitermate belangrijk in het kader van bijvoorbeeld de aansprakelijkheid die de certificatiedienstverlener heeft ten opzichte van iedere vertrouwende derde i.v.m. de juistheid van de in een gekwalificeerd certificaat gecertificeerde gegevens op het ogenblik van uitgifte ervan. Aan de hand van de beschreven procedures (bewijs van identiteit door voorlegging van een getekende kopie van de identiteitskaart van een individu, bewijs van vertegenwoordigingsbevoegdheid van een orgaan door voorlegging van een recente kopie van de statuten, ...) zal de certificatiedienstverlener ingeval van een schadeclaim kunnen aantonen dat hij niet nalatig heeft gehandeld bij de uitgifte van het certificaat.

6.2. De algemene voorwaarden

De algemene voorwaarden zullen, naast de voorwaarden die ook voor de eventuele andere producten van de certifi-

catiedienstverlener zoals betalings- en leveringstermijnen, ook specifieke gegevens vermelden in verband met het uitgeven van certificaten. Het is echter geen belangrijk contractueel document, aangezien de meeste specifieke voorwaarden zullen voorkomen in de respectieve CP's.

6.3. De Certificate Policy ("CP")

Volgens de huidige standaard ETSI TS 101 456 is een CP een *"named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements"* of vrij vertaald een benoemde set regels die de toepasselijkheid van een certificaat of een bepaalde gemeenschap en/of toepassingsklasse met gemeenschappelijke veiligheidsvereisten aanduidt.

De CP is met andere woorden een document dat de procedure uiteenzet die de certificatiedienstverlener volgt bij het uitgeven, instandhouden en herroepen van het specifieke certificaat waarop de CP betrekking heeft. Het schetst de vereisten die aan het specifieke certificaat gesteld worden.

Zo zal men in de CP bijvoorbeeld onder meer de volgende informatie terugvinden:
- of het certificaat als gekwalificeerd beschouwd wordt of niet;
- welke gegevens d.m.v. het certificaat gecertificeerd (kunnen) worden;
- wijze van aanvragen van het certificaat (op afstand of in persoon);
- enz.

Tussen de certificatiedienstverlener en de certificaathouder maakt de CP deel uit van de contractuele documenten en is dus bindend. De CP heeft echter ook een impact op de vertrouwende derde. Ieder certificaat verwijst naar de toepasselijke CP d.m.v. een identificatiecode. De vertrouwende derde kan dus bij ontvangst van een gecertificeerd bericht nagaan in welke mate hij de certificatiedienstverlener van de verzender van het bericht vertrouwt door de CP te lezen. De certificatiedienstverlener houdt de CP's doorgaans ter beschikking van het publiek op zijn website. Zo heeft de vertrouwende derde de mogelijkheid om het certificaat met kennis van zaken te vertrouwen (of niet), maar zijn ook de certificatiedienstverlener en de certificaathouder beschermd tegen eventuele schade die zou kunnen veroorzaakt worden door onwetendheid of verkeerde informatie in hoofde van de vertrouwende derde.

6.4. Het Certification Practice Statement ("CPS")

De CPS wordt door de standaard ETSI TS 101 456 als volgt gedefinieerd: *"statement of the practices which a certification authority employs in issuing certificates"* of vrij vertaald "verklaring over de wijze waarop een certificatiedienstverlener certificaten uitgeeft". Waar de CP eerder een document is over WAT de certificatiedienstverlener verklaart na te leven, is de CPS een document over HOE hij dit doet. De CPS gaat veel verder dan het uiteenzetten van rechten en plichten van partijen, maar is veeleer een algemene verklaring over hoe de certificatiedienstverlener zich organiseert om certificaten uit te geven, zowel op technisch als op bedrijfsorganisatorisch vlak.

Zo legt ETSI TS 101 456 de verplichting op aan een certificatiedienstverlener van gekwalificeerde certificaten te beschikken over een Policy Authority Management Board, een orgaan dat beslist over de wijze van uitgifte van certificaten en zijn werkwijze en vergaderingsdocumenten ter beschikking houdt van auditeurs.

Ook de CPS is voor het publiek toegankelijk, doorgaans via de website van de certificatiedienstverlener.

7. Besluit

De Wet van 9 juli 2001 implementeert de Europese Richtlijn 1999/93/EC in het Belgisch recht. Hierbij worden nuttige begrippen zoals elektronische handtekening, certificaat en certificatiedienstverlener in ons recht geïntroduceerd en verkrijgt de elektronische handtekening een wettelijke waarde.

Men dient echter degelijk te beseffen dat de meeste bepalingen in de Wet van 9 juli 2001 over de rechten en verplichtingen van de certificatiedienstverlener, certificaathouder en vertrouwende derde enkel betrekking hebben op de uitgifte en het gebruik van gekwalificeerde certificaten, en derhalve slechts een klein deel van de bestaande certificaten betreffen.

Aangezien de elektronische handtekening die automatisch het equivalent is van een "handgeschreven" of "papieren" handtekening die geplaatst wordt middels een gekwalificeerd certificaat, zijn op deze manier de belangrijkste rechtsverhoudingen bij het gebruik van dergelijke handtekening geregeld. De Wet van 9 juli 2001 regelt echter niets in verband met de andere soorten certificaten.

Daarom is het belangrijk dat verenigingen zoals ETSI standaarden opstellen, die internationaal door de verschillende partijen bij de certificaatuitgifte erkend en gevolgd worden. Zij creëren een bijkomende zekerheid bij het gebruik van de nieuwe communicatiemiddelen.