Het gevaar voor de rechtszekerheid op lange termijn als gevolg van de invoering van de elektronische akte.

Stefan de Groot

Scriptie Nederlands recht

Begeleider: Henri Martius

De Maccabae 2
7021 ZA Zelhem
834877903

Definitieve versie
23.01.10

Inhoud

1 Inleiding

Thans ligt wetsvoorstel 31 358 ter behandeling bij de Eerste Kamer. Het wetsvoorstel wijzigt enige bepalingen van het Wetboek van Burgerlijke Rechtsvordering en het Burgerlijk Wetboek om meer ruimte te bieden aan de ontwikkelingen van het elektronische verkeer. Het aannemen van dit voorstel zal onder andere tot gevolg hebben dat aktes ook in elektronische vorm opgemaakt mogen worden.

Deze wijzigingen, in combinatie met reeds bestaande wetgeving, brengt met zich mee dat onder omstandigheden - in ieder geval bij gebruik van een zogenaamde gekwalificeerde elektronische handtekening - een elektronische akte dwingend bewijs tussen partijen zal opleveren. Deze verstrekkende rechtsgevolgen van een elektronische akte werden door de Minister en de Tweede Kamer aanvaard omdat met gebruik van de gekwalificeerde elektronische handtekening nagenoeg zeker is dat de handtekening gezet is door de gebruiker en het ondertekende document naderhand niet is gewijzigd.

De nieuwe wetgeving sluit aan bij bestaande wetgeving omtrent de elektronische handtekening, waarbij vooral ook de Telecommunicatiewet en Het Besluit elektronische handtekeningen van belang zijn. In deze wetgeving wordt onder andere invulling gegeven aan het begrip gekwalificeerde elektronische handtekening. Hierbij valt op dat in de formulering van de waarborgeisen slechts rekening gehouden wordt met vervalsingtechnieken die beschikbaar zijn op het moment van het plaatsen van de handtekening.

Deze formulering is begrijpelijk, omdat het door de onvoorspelbare vooruitgang van de techniek onmogelijk is om thans een elektronische handtekening te creëren die ook in de toekomst niet te vervalsen zal zijn. Als het moment echter is aangebroken dat de op dit moment als veilig aanvaarde elektronische handtekening (eenvoudig) te vervalsen is, dan kan dit grote gevolgen hebben voor de rechtszekerheid.

Om dit te onderzoeken wil ik in dit stuk de vraag beantwoorden wat de gevolgen voor de rechtszekerheid op langere termijn zijn van het mogelijk maken van de elektronische akte, zoals geregeld in het genoemde wetsvoorstel.

Om deze vraag te kunnen beantwoorden geef ik eerst een overzicht van de huidige en toekomstige wetgeving en Europese regelgeving, voor zover deze van belang is. Ik zal daarbij de

verschillende soorten elektronische handtekeningen bespreken, waarbij ik vooral in ga op de waarborgen waarmee deze omkleed zijn.

Daarna ga ik in op de mogelijkheden om misbruik te maken van de elektronische handtekening, waarbij ik ook de nu al te verwachten toekomstige mogelijkheden betrek. Vervolgens maak ik een verkenning langs het geldende recht in het buitenland. Ik zal besluiten met enkele aanbevelingen om het gevaar voor de rechtszekerheid - want de conclusie zal zijn dat dit gevaar er is - tot aanvaardbare proporties terug te brengen.

2 Overzicht wetgeving

Zowel de huidige wetgeving als de voorgestelde nieuwe wetgeving behandelt een veel ruimer scala aan bepalingen dan nodig is om in dit onderzoek te betrekken. Ter wille van de eenvoud zal ik een groot aantal niet-relevante bepalingen niet bespreken. Toch zal ik meer bespreken dan strikt genomen noodzakelijk is, om zodoende voldoende context te bieden en mijn betoog meer begrijpelijk te maken.

Omdat in de Nederlandse wetgeving terminologie gebruikt wordt die voortkomt uit de Europese richtlijnen, zal ik eerst deze richtlijnen bespreken. Daarna zal ik bespreken hoe de verschillende soorten handtekeningen in de richtlijnen worden gedefinieerd om tenslotte de huidige Nederlandse wetgeving te behandelen.

2.1 Europees recht

2.1.1 Richtlijn 1999/93/EG

Richtlijn 1999/93/EG geeft een gemeenschappelijk kader voor de elektronische handtekening. De richtlijn is niet gericht op harmonisatie van het contractenrecht en geeft dan ook geen regels over wanneer een elektronische handtekening erkend moet worden, of wat de bewijskracht van een elektronische handtekening is[1]. Ook laat het de lidstaten vrij om te bepalen in welke rechtsgebieden elektronische handtekeningen en elektronische documenten kunnen worden gebruikt.

[1] Richtlijn nr. 99/93/EG (*PbEG* 2000, L13/13-14), overwegingen 17 en 21 en artikel 1.

De richtlijn geeft wel uitgebreide definities van de verschillende soorten elektronische handtekeningen die worden onderscheiden; deze zal ik in de volgende paragraaf bespreken. Verder worden de rechtsgevolgen van de elektronische handtekeningen beschreven. In de richtlijn is bepaald dat gekwalificeerde elektronische handtekeningen ten aanzien van elektronische documenten aan alle wettelijke vereisten voor een handtekening dienen te voldoen, net zo als dat geldt voor een gewone handtekening voor schriftelijke documenten[2].

Daarmee is niet gezegd dat alle overeenkomsten die schriftelijkheid als vormvoorschrift hebben, nu ook elektronisch tot stand kunnen komen, of dat een elektronische overeenkomst een even grote bewijskracht heeft dan een schriftelijke overeenkomst. Er wordt slechts voorgeschreven dat een gekwalificeerde elektronische handtekening dezelfde geldigheid heeft als een schriftelijke handtekening.

De gekwalificeerde elektronische handtekening dient ook zonder meer toegelaten te worden als bewijsmiddel in juridische procedures[3]. Ook hiermee is niets gezegd over de toe te kennen bewijskracht. Ook alle andere soorten elektronische handtekeningen zijn in beginsel geldig en toelaatbaar als bewijsmiddel, omdat wordt voorgeschreven dat het enkele feit dat een elektronische handtekening een element van een gekwalificeerde handtekening ontbeert, dit niet meebrengt dat daarmee de handtekening niet rechtsgeldig is of als bewijsmiddel toelaatbaar is[4]. Kennelijk kunnen er wel andere omstandigheden zijn die een niet-gekwalificeerde handtekening zijn geldigheid of bewijskracht ontzeggen.

Overweging 20 van de richtlijn bepaalt dat alleen gekwalificeerde elektronische handtekeningen als juridisch gelijkwaardig aan de schriftelijke handtekeningen kunnen worden beschouwd. Het is dus niet zo dat een gekwalificeerde elektronische handtekening met deze bepaling juridisch gelijkwaardig wordt aan de handgeschreven variant en dat een elektronische overeenkomst met een gekwalificeerde elektronische handtekening dus dezelfde (dwingende) bewijskracht heeft als een handgetekende akte. Feitelijk wordt in deze overweging alleen het omgekeerde gesteld: een niet-gekwalificeerde handtekening kan niet juridische gelijkwaardig zijn aan een handgeschreven handtekening.

[2] Richtlijn nr. 99/93/EG (*PbEG* 2000, L13/15), artikel 5 lid 1 sub a.
[3] Richtlijn nr. 99/93/EG (*PbEG* 2000, L13/15), artikel 5 lid 1 sub b.
[4] Richtlijn nr. 99/93/EG (*PbEG* 2000, L13/15), artikel 5 lid 2.

2.1.2 Richtlijn 2000/31/EG

Richtlijn 2000/31/EG bepaalt dat - op enkele uitzonderingen na - contracten via elektronische weg gesloten moeten kunnen worden[5]. De uitzonderingen betreffen onroerend goed transacties, overeenkomsten die alleen met tussenkomst van de rechtbank, of een publieke autoriteit of beroepsgroep gesloten kunnen worden, overeenkomsten waarin particulieren persoonlijke of zakelijke zekerheden verstrekken en overeenkomsten die onder het familie of erfrecht vallen. Ook hier wordt slechts de geldigheid voorgeschreven van elektronisch tot stand gekomen overeenkomsten. Over de bewijskracht van deze elektronische overeenkomsten ten opzichte van papieren overeenkomsten wordt niets aanvullends bepaald.

Geconcludeerd kan worden dat het Europese recht het de lidstaten verplicht om het op elektronische wijze van bepaalde soorten overeenkomsten mogelijk te maken en dat elektronische overeenkomsten in beginsel als bewijs toegelaten moeten worden. De lidstaten blijven vrij om de bewijsmiddelen door de rechter vrij te laten beoordelen. Het Europese recht schrijft dus geen dwingende bewijskracht voor ten aanzien van elektronisch gesloten overeenkomsten, noch schrijven de richtlijnen voor dat de bewijskracht van elektronische overeenkomsten gelijk zou moeten zijn aan de bewijskracht van schriftelijke overeenkomsten.

2.2 Verschillende soorten elektronische handtekeningen

2.2.1 De gewone elektronische handtekening

Richtlijn 1999/93/EG geeft feitelijk geen definitie van de gewone elektronische handtekening. Wel wordt een definitie gegeven van een "elektronische handtekening" en een geavanceerde elektronische handtekening". Een "gewone elektronische handtekening" is dus een elektronische handtekening die geen geavanceerde elektronische handtekening is. Minimaal moet deze handtekening voldoen aan de eisen die gesteld zijn in artikel 2 lid 1 van de richtlijn. Het moet gaan om elektronische gegevens die vastgehecht zijn of logisch geassocieerd zijn met andere elektronische gegevens en die gebruikt worden als middel voor authentificatie.

Het gaat hier om een zeer ruime definitie. Sommige auteurs menen dat zelfs een enkele bit aan deze definitie zou kunnen voldoen[6]. Of dat werkelijk zo is laat ik in het midden, maar het lijkt duidelijk dat een ingescande handtekening zeker aan deze definitie voldoet. Ook het

[5] Richtlijn nr. 2000/31/EG (*PbEG* 2000,L178/11), artikel 9 lid 1 en 2.
[6] Brazell, p. 133-135.

eenvoudigweg vermelden van de naam van de afzender onder een e-mailbericht, of zelfs de automatisch aan een e-mail toegevoegde afzendergegevens zijn voldoende om als elektronische handtekening door te gaan.

De Rechtbank in Maastricht neemt echter een ander standpunt in. De rechtbank heeft - ongemotiveerd - bepaald[7] dat een via Hotmail verstuurd e-mailbericht niet aan de vereisten van een elektronische handtekening voldoet. Of dit een juist oordeel is, is te betwijfelen. Het lijkt immers evident dat de naam van de afzender data is die gehecht is aan het e-mail bericht zelf. De vraag is of deze toegevoegde naam gebruikt kan worden als middel voor authentificatie.

Het antwoord op die vraag hangt af van wat in deze context onder authentificatie moet worden verstaan. Kennelijk gaat het niet om het met redelijke zekerheid kunnen vaststellen van de echtheid van de ondertekenaar - anders zou het onderscheid met een geavanceerde handtekening overbodig zijn. Waarschijnlijker is het dat de interpretatie aansluit bij de definitie die Unictral[8] aan de elektronische handtekening geeft, zodat we kunnen aannemen dat de handtekening toegevoegd moet zijn door de ondertekenaar om daarmee aan te geven dat hij het met de inhoud van de tekst eens is[9]. Als we deze uitleg aannemen, dan is bepalend welk doel de ondertekenaar had met het plaatsen van haar naam onder het e-mailbericht. Het valt goed te verdedigen dat zij haar naam onder het e-mail bericht heeft geplaatst om aan te geven dat zij het is die dit bericht heeft geschreven en daarmee de inhoud goedkeurt.

In Slovenië heeft een soortgelijke zaak gespeeld. Ook hier ging het om een beroepschrift van een student per e-mail, wat in eerste aanleg niet ontvankelijk is verklaard vanwege het feit dat de student een e-mail had gebruikt. In hoger beroep[10] is deze beslissing echter vernietigd.

Ook in Finland heeft een rechtbank in hoger beroep geoordeeld[11] dat een gewoon e-mail bericht in een zaak voldoende informatie bevatte omtrent de afzender, dat er geen reden is om aan de authenticiteit of de integriteit van het *bericht* te twijfelen.

Ondanks de uitspraak van de Maastrichtse rechtbank valt dus te verdedigen dat een eenvoudige e-mail waarbij voldoende informatie over de afzender in opgenomen is kan gelden als een bericht wat voorzien is van een elektronische handtekening. De informatie over de afzender, bijvoorbeeld

[7] Rechtbank Maastricht 2 mei 2006, *LJN* AW6886.
[8] UNICTRAL Model Law on Electronic Signatures 2001, art. 2a.
[9] Zie ook Brazell, p. 134.
[10] I Up 505/2003 - Engelse vertaling in Digital Evidence Journal, 2007, Volume 4, nr 2.
[11] Case 1486:2006 judgment 19.10.2006, besproken in Mason, p. 146.

de naam die onder een bericht wordt geplaatst, maar wellicht ook al de naam die in het e-mail adres van de afzender is opgenomen, kan dan als elektronische handtekening worden beschouwd. Het is voorlopig onduidelijk waar precies de grens ligt.

De rechtsgevolgen van een gewone elektronische handtekening worden geregeld in art 5 lid 2 van de richtlijn. Hieruit volgt dat een gewone elektronische handtekening in beginsel geldig is en toegelaten wordt als bewijs in een juridische procedure. Deze bepaling laat voldoende ruimte om omstandigheden aan te voeren waarin in een specifiek geval een gewone elektronische handtekening niet tot bewijs kan dienen.

2.2.2 De geavanceerde elektronische handtekening

Artikel 2 lid 2 van richtlijn 1999/93/EG geeft de definitie van een geavanceerde elektronische handtekening. Een geavanceerde elektronische handtekening voldoet aan vijf criteria. Het eerste criteria is in de vorige paragraaf besproken: het moet een elektronische handtekening zijn. Dan gelden de vier volgende aanvullende eisen:

1. De handtekening moet op unieke wijze aan de ondertekenaar verbonden zijn.

   Volgens sommige auteurs[12] levert dit een probleem op, omdat strikt genomen de handtekening nooit verbonden zal zijn met de ondertekenaar, maar met de encryptiesleutel die de ondertekenaar gebruikt om de handtekening aan te maken. Zelf ben ik van mening dat het begrip "uniek verbonden" ruimer geïnterpreteerd moet worden, waardoor ook de handtekening die gemaakt is met een encryptiesleutel die de ondertekenaar als enige beheert of zou moeten beheren uniek verbonden is met de ondertekenaar. De unieke verbondenheid volgt naar mijn al uit het feit dat de ondertekenaar in staat is het middel om de handtekening aan te maken in eigen beheer te houden.

2. De handtekening moet het mogelijk maken de ondertekenaar te identificeren.
3. De handtekening komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden.
4. De handtekening is op zodanige wijze aan de gegevens waar deze betrekking op heeft verbonden, dat elke wijziging achteraf van de gegevens opgespoord kan worden.

[12] Mason, p. 148.

De geldigheid en de bewijskracht van de geavanceerde elektronische handtekening is ook geregeld in artikel 5 lid 2. Strikt genomen is er geen verschil met de gewone elektronische handtekening. Vanwege de extra waarborgen die een geavanceerde elektronische handtekening ten opzichte van een gewone elektronische handtekening biedt, is het wel te verwachten dat er minder snel bezwaren tegen de bewijskracht van een geavanceerde elektronische handtekening op te voeren zijn, waardoor een geavanceerde handtekening in de praktijk een betere positie zal hebben als een gewone elektronische handtekening.

2.2.3 De gekwalificeerde elektronische handtekening

Ook dit type elektronische handtekening wordt niet als zodanig genoemd in de richtlijn. In de literatuur wordt een gekwalificeerde elektronische handtekening echter beschouwd als een geavanceerde elektronische handtekening die voldoet aan de twee extra voorwaarden die in artikel 5 lid 1 worden gesteld.

1. De handtekening is gebaseerd op een gekwalificeerd certificaat.

   Een gekwalificeerd certificaat is een elektronische bevestiging die de identiteit van een persoon bevestigt, die waarborgt dat aan deze persoon de controlesleutel gekoppeld is om de echtheid van de elektronische handtekening te controleren en dat afgegeven is door een dienstverlener die aan nader bepaalde eisen voldoet. Deze eisen staan in bijlage II van de richtlijn. Tevens dient het certificaat aan de eisen in bijlage I van de richtlijn te voldoen.

2. De handtekening moet door een veilig middel zijn aangemaakt.

   Een veilig middel wordt nader omschreven in bijlage III van de richtlijn. Het gaat om waarborgen zoals het niet kunnen wijzigen van de oorspronkelijke gegevens na het plaatsen van de handtekening en bescherming van de gegevens die gebruikt worden voor het maken van een elektronische handtekening. Te denken valt aan een smartcard en een cardreader.

De rechtsgevolgen van de gekwalificeerde elektronische handtekening worden geregeld in artikel 5 lid 1. Hier wordt bepaald dat dit type handtekening voldoet aan de wettelijke eisen van een handtekening en als bewijsmiddel in gerechtelijke procedures wordt toegelaten.

Om dit artikel juist te interpreteren is overweging 21 van belang. Hierin wordt bepaald dat deze richtlijn niet treed in de beoordeling van de bewijskracht door de rechter. Zodoende moet

geconcludeerd worden dat een gekwalificeerde elektronische handtekening weliswaar als bewijsmiddel geaccepteerd dient te worden, maar dat niet is voorgeschreven welke bewijskracht dit type handtekening heeft. Hierdoor wordt naar mijn mening de ruimte geschept om in sommige gevallen te kunnen bepalen dat een handgeschreven handtekening een grotere bewijskracht heeft dan een gekwalificeerde elektronische handtekening.

2.3 Huidig Nederlands recht

Nederland heeft de Europese richtlijnen 1999/93/EG[13] en 2000/31/EG[14] tamelijk minimalistisch geïmplementeerd. Voor het onderhavige onderwerp is vooral artikel 3:15 BW, 6:227a BW, de Telecommunicatiewet en het Besluit elektronische handtekeningen[15] van belang.

2.3.1 Art. 3:15BW

Art 3:15 BW regelt de geldigheid van de elektronische handtekening. Daarbij wordt analoog aan de Europese wetgeving een beschrijving van de verschillende soorten elektronische handtekeningen gegeven. Voor de beschrijving van een gekwalificeerd certificaat, een veilig middel voor het plaatsen van de handtekening en de certificatiedienstverlener wordt verwezen naar de Telecommunicatiewet.

Art 3:15 BW volgt bijna volledig de Europese richtlijnen. Artikel 3:15a lid 1 BW wijkt echter af[16], zonder overigens strijdig te zijn met de richtlijnen. In dit lid wordt in een open norm bepaald dat een elektronische handtekening alleen dezelfde rechtsgevolgen heeft als de handgeschreven handtekening, indien de methode die daarvoor gebruikt wordt voldoende betrouwbaar is gelet op het doel waarvoor deze wordt gebruikt en alle overige omstandigheden van het geval.

Deze - mijns inziens nodeloos vage beperking - geldt gelukkig niet voor gekwalificeerde elektronische handtekeningen, zo bepaalt lid 2 van dit artikel. Dit lid geeft het rechtsvermoeden dat gekwalificeerde elektronische handtekeningen aan de eisen van lid 1 voldoen.

Lid 3 van art 3:15a BW bepaalt voorts dat de betrouwbaarheid - en dus de geldigheid - van een handtekening niet mag worden ontzegd op de enkele grond dat de handtekening niet een

[13] *Kamerstukken II,* 27743.
[14] *Kamerstukken II,* 28197.
[15] *Stb.* 2003, 200.
[16] Zie ook Brazell P. 186.

gekwalificeerde handtekening is. Daarmee wordt de geavanceerde handtekening wat betreft geldigheid tussen de gewone en de gekwalificeerde elektronische handtekening geplaatst.

De hiërarchie wordt hierdoor zo, dat de gewone elektronische handtekening min of meer vogelvrij is. Deze is alleen geldig als deze aan de in lid 1 beschreven open normen voldoet. Daarna komt de geavanceerde elektronische handtekening. Deze handtekening geniet niet het privilege van het rechtsvermoeden van voldoende betrouwbaarheid, maar deze handtekening kan niet als ongeldig beschouwd worden vanwege het enkele feit dat het geen gekwalificeerde elektronische handtekening is. Het hoogst in de rangorde staat de gekwalificeerde elektronische handtekening. Hiervan wordt vermoed dat deze dezelfde rechtsgevolgen heeft als de handgeschreven variant.

2.3.2 Art 6:227a BW

Dit artikel is opgenomen ter implementatie van artikel 9 van richtlijn 2000/31/EG. Het artikel bepaalt dat overeenkomsten die volgens de wet alleen schriftelijk tot stand kunnen komen (zoals een huurkoopovereenkomst) ook rechtsgeldig via elektronische weg tot stand kunnen komen.

De uitzonderingen die de Europese richtlijn toelaat, worden onverkort door de Nederlandse wetgever overgenomen. Het gaat om overeenkomsten betreffende onroerend goed (behalve huur), persoonlijke zekerheden (niet uit hoofde van beroep of bedrijf), overeenkomsten betreffende het familierecht en erfrecht en overeenkomsten waar tussenkomst van een rechter, overheidsorgaan of beroepsbeoefenaar die een publieke taak uitoefent (de notaris) noodzakelijk is.

Lid 1 van artikel 6:227a BW omschrijft wel een aantal voorwaarden waar de elektronisch gesloten overeenkomst aan moet voldoen. Zo moet de overeenkomst raadpleegbaar zijn door partijen, moet de authenticiteit van de overeenkomst in "voldoende" mate zijn gewaarborgd, moet de tijd van totstandkoming met voldoende zekerheid kunnen worden vastgesteld en moet ook de identiteit van de partijen met voldoende zekerheid kunnen worden vastgesteld.

Ook deze eisen zijn niet in strijd met de richtlijn. De richtlijn eist immers slechts een situatie waarin geldigheid van de elektronisch gesloten overeenkomst niet wordt ontzegd louter omdat het om een elektronisch gesloten overeenkomst gaat.

2.3.3 De Telecommunicatiewet

In art 3.15a BW wordt naar de Telecommunicatiewet verwezen voor de invulling van de eisen waar de gekwalificeerde elektronische handtekening aan moet voldoen. Deze eisen worden echter

nauwelijks ingevuld in deze wet. Er wordt slechts een raamwerk opgezet, waarvan de technische invulling gedelegeerd wordt aan de minister. Hiermee is dan de juridische basis gelegd onder het Besluit elektronische handtekeningen.

2.3.4 Besluit elektronische handtekeningen

Dit besluit regelt gedetailleerd de eisen waar de uitgever van een gekwalificeerd certificaat aan moet voldoen. Ook de eisen waar een certificaat zelf en het veilige middel waarmee deze is aangemaakt aan moeten voldoen worden hier beschreven.

De certificatiedienstverlener moet aan strenge normen voldoen op het gebied van interne organisatie, deskundigheid van de medewerkers, financiële positie en continuïteit. Ook worden er eisen gesteld aan de beveiligingsprocessen en de encryptietechnieken. Dit moeten de beste technieken zijn die op het moment van het afgeven van het certificaat beschikbaar zijn (art. 2c).

Belangrijk ook is het voorschrift dat de certificatiedienstverlener de uitgegeven certificaten en alle gegevens die nodig zijn om de identiteit van de aanvrager van het certificaat te bewijzen tot zeven jaar na de geldigheidsduur van het certificaat moet bewaren. Deze bepaling zorgt voor een extra waarborg ten aanzien van de bewijskracht van een elektronische handtekening. Echter, deze waarborg is beperkt in tijd.

Artikel 5 lid b is voorts een erg belangrijke bepaling. De waarborg dat een elektronische handtekening of het document waar de elektronische handtekening onder gezet wordt niet vervalst kan worden, is vooral op dit artikel gebaseerd. Dit artikel is de zwakste schakel in de keten van waarborgen die gegeven zijn om te voorkomen dat een elektronisch document wat met een gekwalificeerde elektronische handtekening is ondertekend ongemerkt vervalst kan worden.

Dit artikel bepaalt dat een veilig middel waarmee een elektronische handtekening wordt aangemaakt beschermd is tegen vervalsingen met de op het tijdstip van het afgeven van de verklaring beschikbare technieken. Het gaat hier niet om de beschikbare technieken om te beschermen, maar om de beschikbare technieken om te vervalsen.

Een betere bescherming tegen vervalsing is feitelijk niet te geven. Een gebruiker van een gekwalificeerde elektronische handtekening (die per definitie is aangemaakt met een veilig middel) weet dus zeker dat deze handtekening niet is te vervalsen met een vervalsingstechniek die op dat moment bekend is.

De mogelijkheid dat er in de toekomst nieuwe vervalsingstechnieken ontdekt worden, wordt niet geregeld, maar kennelijk wel voorzien gezien de redactie. De keuze die hiermee gemaakt wordt is dat als een nieuwe vervalsingstechniek ontdekt wordt, de reeds geplaatste handtekening niet zijn privileges verliest, maar onverkort het rechtsvermoeden behoudt dat de handtekening dezelfde rechtsgevolgen heeft als de handgeschreven variant.

3 Wetsvoorstel 31 358

Op 25 februari 2008 is het wetsvoorstel waarin enige bepalingen van het Burgerlijk wetboek en burgerlijke rechtsvordering worden gewijzigd om ruimte te bieden aan ontwikkelingen op het gebied van elektronisch verkeer ter behandeling naar de Tweede Kamer gestuurd. In de Tweede Kamer is het voorstel op belangrijke punten geamendeerd. Op 2 december 2008 is het gewijzigde voorstel naar de Eerste Kamer gestuurd, alwaar het thans wordt behandeld.

3.1 Inhoud gewijzigde wetsvoorstel

Het wetsvoorstel regelt in grove lijnen vier wijzigingen, allen bedoeld om elektronische verkeer toe te staan daar waar dit voorheen alleen schriftelijk kon.

Zo wordt artikel 1:88 BW aangepast, dat toestemming van de echtgenoot voor bepaalde ingrijpende rechtshandelingen ook in elektronische vorm gegeven kan worden, daar waar dit eerst schriftelijk diende te gebeuren. In Boek 6 BW wordt artikel 234 zo gewijzigd, dat algemene voorwaarden met instemming van de contractspartij ook op elektronische wijze rechtsgeldig aan de contractspartij ter beschikking kunnen worden gesteld. En in titel 17 van boek 7 BW worden enkele bepalingen gewijzigd waardoor het onder omstandigheden mogelijk wordt om een elektronische polis af te sluiten en een verzekeringsovereenkomst elektronisch op te zeggen.

Al deze bepalingen zullen in dit stuk verder niet behandeld worden, geconcentreerd wordt op de vierde wijziging: het mogelijk maken van de elektronische akte.

3.2 Parlementaire behandeling

De parlementaire behandeling van het wetsvoorstel komt enigszins rommelig over.

Het initiatief voor het wetsvoorstel is door Frank Heemskerk gedaan, door een op 11 oktober 2005 aangenomen motie[17] die de strekking had het mogelijk te maken dat een verzekeringsovereenkomst elektronisch gesloten zou kunnen worden en dat rechtsgeldig een elektronische polis afgegeven kon worden. Frank Heemskerk is thans staatssecretaris van Economische zaken.

In weerwil van de mening van de minister dat een elektronische akte Nederland in een unieke positie zou brengen omdat geen enkel ander Europees land dit zo heeft geregeld[18], heeft deze motie geleid tot een wetsvoorstel wat een elektronische akte mogelijk maakt, behoudens akten die onder het personen of familierecht vallen of akten die persoonlijke of zakelijke zekerheden verstrekken, afgegeven door particulieren. Deze strekking is al zeer veer uitgebreider dan de strekking van motie Heemskerk. Tijdens de parlementaire behandeling zijn echter zelfs de bovengenoemde beperkingen geschrapt.

Tijdens de parlementaire behandeling is op geen enkel moment de vraag gerezen in hoeverre de rechtszekerheid op langere termijn gewaarborgd is als het wetsvoorstel aangenomen zou worden. Als het bekend is dat Nederland in ieder geval in Europa pionier is met dergelijke wetgeving en in de wetenschap dat informatietechniek snel wijzigt, zou dit naar mijn mening toch noodzakelijk zijn om tot een zorgvuldige afweging te komen.

Dat deze vraag niet naar boven gekomen is, komt wellicht vanwege het feit dat er geen parlementariërs zijn met een informatica opleiding. Enige relevante technische kennis is op dit punt onontbeerlijk om een zorgvuldig besluit te nemen in deze materie. Alleen de heer Biskop heeft een jaar informatiekunde gestudeerd, maar dit lid is niet betrokken geweest bij de behandeling van het wetsvoorstel. Het ware verstandig en zorgvuldig geweest - gezien het gebrek aan eigen relevante kennis van de Tweede Kamerleden - om zich door deskundigen te laten informeren. Uit de behandeling in de Tweede Kamer blijkt niet dat dit gebeurd is.

3.3 De elektronische akte

Als het wetsvoorstel wordt aangenomen, dan wordt in het Wetboek van Burgerlijke Rechtsvordering een artikel 156a ingevoegd. Dit artikel bepaalt dat onderhandse akten ook op een andere wijze dan schriftelijk kunnen worden opgemaakt, als dat gebeurt op een wijze waarop

[17] *Kamerstukken II* 2005/06, 30 137, nr. 17.
[18] *Handelingen II* 2005/06, 6, p. 292.

degene ten behoeve van wie de akte bewijs oplevert, de akte op kan slaan op een manier dat deze toegankelijk is gedurende een periode die is afgestemd op het doel waarvoor de akte is bestemd.

Het tweede lid van dit artikel bepaalt dat een akte alleen anders dan schriftelijk mag worden verstrekt, als degene aan wie de akte moet worden verstrekt hier uitdrukkelijk toestemming voor heeft gegeven.

Deze formulering is technologieneutraal gemaakt, maar op dit moment zal alleen een elektronische akte een zinvolle invulling kunnen geven aan dit artikel.

3.3.1 De functies van een akte

Artikel 156Rv en verder definiëren de akte en regelen de rechtsgevolgen van een akte.

Een akte is een ondertekend geschrift, bestemd om tot bewijs te dienen. De akte bestaat in twee gedaanten. De authentieke en de onderhandse akte. De authentieke akte is opgemaakt door de krachtens de wet daartoe bestemde ambtenaar, de notaris. Alle andere akten zijn onderhandse akten.

Omdat het onderhavige wetsvoorstel alleen betrekking heeft op de onderhandse akte, zal ik verder niet ingaan op de rechtsgevolgen van de authentieke akte.

De onderhandse akte heeft twee functies. Enerzijds wordt de onderhandse akte bij sommige benoemde overeenkomsten voorgeschreven om tot een geldige overeenkomst te komen. Het gaat dan bijvoorbeeld om de overeenkomst van huurkoop of pacht.

Anderzijds - en dat is de functie die in dit stuk het meeste aandacht zal krijgen - heeft de akte een geprivilegieerde positie in de hiërarchie van bewijsmiddelen.

Een onderhandse akte levert immers tussen de partijen die hun handtekening onder de akte hebben gezet, dwingend bewijs op van de waarheid van de inhoud van de akte. Dat betekent dat de rechter (art. 151Rv) verplicht is de inhoud als waar aan te nemen.

Tegenbewijs is mogelijk, maar moeilijk te leveren. Daarnaast is het zo dat als een handtekening onder een akte stellig wordt ontkend, de bewijskracht opgeschort wordt totdat bewezen is dat de handtekening authentiek is (art 159 lid 2 Rv). Deze nuanceringen doen echter nauwelijks af aan de kracht van het bewijs. Een stellige ontkenning is niet vrijblijvend[19]. Belangrijker: een schriftkundige

[19] Zie ook HR, 28 februari 1997, *NJ* 1997, 330.

is bijna altijd in staat om met zekerheid of met aan zekerheid grenzende waarschijnlijkheid een uitspraak te doen over de echtheid van een handtekening[20]. Kennelijk werkt het vooruitzicht om ontmaskerd te worden als valselijk wordt beweerd dat een handtekening niet authentiek is preventief, omdat het in de praktijk niet vaak voor komt dat de echtheid van een handtekening ten onrechte wordt ontkend[21].

Naast een totstandkomingsfunctie heeft de akte dan ook een zeer belangrijke bewijsfunctie.

3.3.2 Is een elektronische akte al mogelijk?

De vraag of een elektronische akte ook zonder dit wetsvoorstel mogelijk is, is naar mijn mening niet met zekerheid te beantwoorden. De minister van justitie heeft verschillende malen[22] verklaard dat thans al een elektronische akte mogelijk is. Diverse auteurs hebben dit als een belangrijke indicatie gezien dat de elektronische akte al bestaat. Andere auteurs hebben tegenstrijdigheden met deze verklaringen opgemerkt[23].

Deze conclusie wringt natuurlijk met het feit dat nu een wetsvoorstel voorligt waarin de elektronische akte nu mogelijk wordt gemaakt, waardoor nader onderzoek geboden is.

Overigens heeft dezelfde minister in 2005, ter gelegenheid van het stellig ontraden van een amendement van Heemskerk met de strekking polissen digitaal af te mogen geven, juist betoogt[24] dat een akte een *schriftelijk* ondertekend stuk is. Om een elektronische akte mogelijk te maken, zou volgens de minister een brede operatie nodig zijn.

Bij correcte - letterlijke - lezing van de wet moet geconcludeerd worden dat een elektronisch akte op dit moment niet mogelijk is. De akte vereist een handtekening en schriftelijkheid. Aan de eis van een handtekening kan een elektronische handtekening vanwege artikel 3:15a BW voldoen. Een elektronische handtekening krijgt met dit artikel immers dezelfde rechtgevolgen als een handgeschreven handtekening. Een totstandkomingseis kan als rechtsgevolg beschouwd worden, waardoor een elektronische handtekening niet in de weg hoeft te staan aan de totstandkoming van een akte.

---

[20] Bv. Rechtbank Zwolle 12 juli 2006, *LJN* AZ9727.
[21] Hidma en Rutgers, p. 91 en Franken e.a. p. 212.
[22] Bv. *Kamerstukken I* 2002/03, 27 743, nr. 35. p.10.
[23] Bv. Hendrikse, van Huizen en Rinkes, p. 153.
[24] *Handelingen II* 2005/06, 6, p. 292-293.

Daarmee is het stuk wat wij een akte willen noemen echter nog niet schriftelijk. Onze wet ontbeert tot op heden een bepaling wat een elektronisch stuk gelijk stelt aan een schriftelijk stuk. Wel bepaalt art 6:227a BW dat als uit de wet voortvloeit dat een overeenkomst alleen op schriftelijke wijze tot stand kan komen, dat aan deze eis ook is voldaan als de overeenkomst langs elektronische weg tot stand is gekomen en aan een aantal voorwaarden is voldaan.

Hij die de wet heel letterlijk neemt, zou kunnen betogen dat hiermee wel op elektronische wijze een pachtovereenkomst tot stand kan komen, maar dat huurkoop nog steeds slechts schriftelijkheid vereist. Immers, in de wet wordt bij pacht een schriftelijke overeenkomst geëist, maar bij huurkoop is een akte een vereiste. Als de wet op deze manier gehanteerd zou worden, dan zou de conclusie moeten volgen dat de Nederlandse wet thans in strijd is met artikel 9 van richtlijn 2000/31/EG, welke eist dat overeenkomsten zoals huurkoop in zijn algemeenheid op elektronische wijze gesloten dienen te kunnen worden.

Als we de wetgever de slordigheid en onduidelijkheid op dit punt niet tegenwerpen en er van uitgaan dat de wetgever met art 6:227a BW bedoeld heeft richtlijn 2000/31/EG volledig te implementeren, dan kunnen we nog steeds niet concluderen dat de elektronische akte thans reeds bestaat.

Immers, de richtlijn en art 6:277a BW hebben slechts betrekking op totstandkomingseisen van overeenkomsten. Over de bewijsfunctie wordt niet gerept, integendeel, de richtlijn gaat er juist vanuit dat deze niet ingrijpt in het nationale bewijsrecht.

Bij een niet al te rigide, maar ook niet al te losse interpretatie van de wet moet de stelling worden ingenomen dat een overeenkomst die een akte vereist weliswaar - onder omstandigheden - ook rechtsgeldig op elektronische wijze tot stand kan komen, maar daarmee is het elektronische document nog geen akte in de zin van art 156Rv en verder.

Mijn conclusie is dan ook dat een elektronische "akte" op dit moment alleen bestaat in zijn totstandkomingsfunctie, maar dat dit elektronische document niet het dwingend - maar slechts vrije - bewijskracht heeft van een schriftelijke akte.

Een volwaardige elektronische akte die net als een schriftelijke akte dwingend bewijskracht heeft, bestaat thans onder Nederlands recht dus niet.

4 Hoe werkt een elektronische handtekening?

In de wet wordt aan een gekwalificeerde elektronische handtekening de eis gesteld dat het document waar de handtekening aan gehecht is, niet ongemerkt gewijzigd kan worden met de huidige stand van de techniek. Er worden dus geen eisen gesteld aan de veiligheid van de akte in de toekomst. Omdat een akte dikwijls tot doel heeft om ook op langere termijn tot bewijs te dienen, zal voor het beantwoorden van de vraag of de elektronische akte de rechtszekerheid in gevaar brengt, onderzocht moeten worden of er een voorspelbare kans is dat op langere termijn de elektronisch ondertekende akte wél ongemerkt gewijzigd kan worden.

Rechtssubjecten die de wens hebben een elektronische akte te sluiten die over geruime tijd nog als bewijs kan dienen, hebben de mogelijkheid te kiezen voor de elektronische handtekening die met de meeste waarborgen omkleed wordt. Bezwaren op het gebied van de rechtszekerheid op de lange termijn die betrekking hebben op elektronische handtekeningen die niet een gekwalificeerde elektronische handtekening zijn kunnen eenvoudig gepareerd worden door te betogen dat de partijen dan maar een gekwalificeerde elektronische handtekening hadden moeten gebruiken. Daarom ga ik in het navolgende vooral uit van de gekwalificeerde elektronische handtekening en een elektronische akte die met een gekwalificeerde elektronische handtekening is ondertekend.

4.1 Samenvatten en versleutelen

De geavanceerde en dus ook de gekwalificeerde elektronische handtekening maakt gebruik van geavanceerde encryptie technieken. Meestal wordt gebruikt gemaakt van de RSA[25] versleutelingsmethode, in combinatie met de SHA[26]-1 of MD5[27] samenvattingsmethode. De samenvattingsmethode wordt gebruikt om de elektronische akte om te zetten in een (groot) getal. Dit getal wordt dan als basis voor de versleutelingsmethode gebruikt.

De digitale akte ondergaat dus eerst een rekenkundige bewerking, waar een samenvattingsgetal[28] uit volgt. Hier kom ik later over te spreken.

Dit samenvattingsgetal wordt vervolgens versleuteld met een geheime code, op zo'n manier, dat het oorspronkelijke samenvattingsgetal weer eenvoudig te berekenen is met behulp van een

[25] Naar de eerste letters van de namen van de uitvinders: Ron Rivest, Adi Shamir en Len Adleman.
[26] Secure Hash Algorithm.
[27] Message Digest Algorithm 5.
[28] Bij MD-5 gaat het om een getal van 39 cijfers.

openbare code. Het samenvattingsgetal en de openbare sleutel is het belangrijkste deel van de elektronische handtekening. Een ondertekende elektronische akte bestaat dus uit de elektronische akte, het samenvattingsgetal en de openbare code.

Als degene die de elektronische akte als bewijs inroept wil aantonen dat de akte niet gewijzigd is nadat hij een exemplaar ervan heeft ontvangen, dan moet hij laten zien dat als hij met dezelfde samenvattingsmethode opnieuw een samenvatting maakt van de akte waar hij een beroep op doet, hij hetzelfde getal verkrijgt als wanneer hij met de versleutelingsmethode de versleutelde code terugrekent met de openbare sleutel. Hij kan dat steeds doen, omdat de versleutelde code en de openbare sleutel feitelijk de elektronische handtekening is. Degene die zich op de bewijskracht inroept zal dit niet zelf met de rekenmachine in de hand bij de rechtbank demonstreren; de certificatiedienstverleners leveren hiervoor het bewijs.

Als alle methodes waterdicht zijn, dan is de bewijskracht ook heel sterk. Immers, als de akte na het ondertekenen gewijzigd zou zijn, dan wijzigt ook het samenvattingsgetal en komt dit niet meer overeen met het versleutelde samenvattingsgetal. Het is ook niet mogelijk om het versleutelde samenvattingsgetal te wijzigen als de akte gewijzigd is, omdat de beveiligingsmethode veronderstelt dat dit onmogelijk is zonder de geheime sleutel van de ondertekenaar. Deze geheime sleutel, samen met de openbare sleutel is overigens het belangrijkste kenmerk van het certificaat, het veilige middel om een gekwalificeerde elektronische handtekening te plaatsen.

4.2 Veiligheid van de samenvattingsmethode

De samenvattingsmethode moet dusdanig zijn, dat als een wijziging in de tekst wordt gemaakt, het praktisch onmogelijk is om, ook als er andere wijzigingen in de tekst gemaakt worden, tot het zelfde samenvattingsgetal te geraken. Immers, als dit wel zou kunnen, dan zou de tekst van de akte in een geheel andere tekst gewijzigd kunnen worden en zou deze wijziging onopgemerkt blijven, omdat het samenvattingsgetal van de twee akten precies hetzelfde is. De certificatiedienstverlener zal dan ten onrechte stellen dat de akte authentiek is, omdat het samenvattingsgetal uit de aangeboden akte overeenkomt met de ontcijferde sleutel uit de handtekening.

Het probleem met de samenvattingsmethode is dat er ook wiskundige methodes bestaan om verschillende teksten te genereren die hetzelfde samenvattingsgetal hebben als de oorspronkelijke tekst. De veiligheid van de samenvattingsmethode is gebaseerd op de veronderstelling dat de nu bekende wiskundige methodes zoveel computerkracht nodig hebben

om dit voor elkaar te spelen, dat hier tientallen jaren overheen zouden gaan. Daarom zijn de samenvattingsmethoden bij een bepaalde stand van de techniek in praktische zin veilig.

Echter, de computerkracht stijgt exponentieel en er worden steeds nieuwe wiskunde methodes bedacht waardoor er minder berekeningen nodig zijn om tot eenzelfde resultaat te komen.

In 2008 is ook feitelijk door wetenschappers aangetoond[29] dat de MD5 methode - wat tot 1996 als de veiligste methode gold - te omzeilen is. De wetenschappers hebben het voor elkaar gekregen om verschillende documenten te maken met hetzelfde samenvattingsgetal. Als deze techniek wordt toegepast op een elektronische akte, dan is het dus mogelijk om de akte aan te passen op zo'n wijze dat deze nog steeds – ten onrechte – als authentiek wordt erkend.

De Nederlandse overheid heeft in 2008 geconstateerd dat de MD5 methode nog steeds werd gebruikt en heeft opgeroepen om in plaats daarvan de momenteel meest veilige methode te gebruiken, het SHA-2[30] algoritme[31]. Maar ook van deze methode heeft de Nederlandse overheid voorspelt dat het "minimaal tien jaar" zal duren voordat deze methode gekraakt zal zijn.

4.3 Veiligheid van de versleutelingsmethode

De RSA versleutelingsmethode gaat uit van een geheime en een openbare sleutel. Met de geheime sleutel wordt het samenvattingsgetal versleuteld, wat alleen met de openbare sleutel weer ontcijferd kan worden. Als degene die een elektronische akte zou willen vervalsen of een valse akte zou willen opstellen de beschikking zou hebben over de geheime sleutel van een ander, dan zou hij in staat zijn om deze akte te ondertekenen met de elektronische handtekening van deze andere.

De versleutelingsmethode werkt zo, dat het met een relatief eenvoudige bewerking mogelijk is om van de geheime code en een samenvattingsgetal een code te maken, die weer eenvoudig met de openbare sleutel is te ontcijferen. Maar de methode brengt zich mee dat het theoretisch ook mogelijk is om aan de hand van de code en de publieke sleutel de geheime code te bepalen. Theoretisch is dit mogelijk, maar het vergt zoveel rekenkracht, dat het op dit moment in de praktijk niet mogelijk is. De snelste computers zouden er tientallen jaren voor nodig hebben.

---

[29] <http://events.ccc.de/congress/2008/>
[30] SHA-2(512) werkt met samenvattingsgetallen van 154 cijfers.
[31] *Factsheet FS-2009-01* versleutelingsmethode van het Nederlandse Computer Emergency Response Team, <http://www.govcert.nl/download.html?f=122>.

Maar ook hier geldt dat de computerkracht exponentieel toeneemt in de tijd en dat er steeds nieuwe methoden bedacht worden om hetzelfde probleem met minder berekeningen op te lossen. Zo is er bijvoorbeeld al een methode ontdekt die, zodra de kwantumcomputer op het toneel verschijnt, zeer snel in staat zal zijn om de geheime code uit een elektronische handtekening te herleiden[32].

Dus niet alleen de samenvattingsmethode, maar ook de encryptietechniek zal naar verwachting op termijn niet meer veilig zijn.

4.4 Veiligheid van de elektronische akte op lange termijn

De versleutelingstechnieken die gebruikt worden voor de elektronische handtekeningen die met de meeste waarborgen worden omkleed zijn in de praktijk veilig genoeg op korte termijn. Op langere termijn (vanaf tien jaar volgens bijvoorbeeld de Nederlandse overheid) moet echter aangenomen worden dat de huidige technieken door deskundigen te kraken zijn. Op nog langere termijn is het aannemelijk dat deze vervalsingstechnieken ook voor een breder publiek beschikbaar zijn. Laten wij aannemen dat dit over twintig jaar het geval zal zijn.

Als dat werkelijk het geval zal zijn, dan betekent dit dat het over twintig jaar voor een breed publiek mogelijk is om de inhoud van een elektronische akte die ondertekend is met een gekwalificeerde elektronische handtekening, ongemerkt te wijzigen. Ook betekent dit, dat over twintig jaar een breed publiek in staat geacht moet worden om de geheime code uit een gekwalificeerde elektronische handtekening te herleiden, waarmee dit publiek in staat is om nieuwe - valse - gekwalificeerde elektronische handtekeningen te plaatsen alsof deze van de oorspronkelijke ondertekenaar afkomstig zijn, zonder dat dit door onderzoek van alleen de handtekening zelf achteraf te ontdekken is.

Uiteraard zullen de technieken om een gekwalificeerde elektronische handtekening te plaatsen over twintig jaar zo ontwikkeld zijn dat op dat moment de techniek in praktische zin veilig zal zijn, maar als de vervalser over twintig jaar de techniek uit 2010 vervalst en pretendeert te beschikken over een akte die reeds in 2010 tot stand is gekomen, dan beschikt de vervalser, als het onderhavige wetsvoorstel wordt aangenomen, in 2030 over een akte die in beginsel tussen partijen dwingende bewijskracht heeft.

[32] Shor 1997.

4.5 De praktische bewijskracht van de akte op langere termijn

Zodra het mogelijk wordt om akten te vervalsen of in zijn geheel valselijk op te maken, zal dit vast door een bepaalde groep mensen in praktijk worden gebracht. Betoogt kan worden dat eerder een elektronische dan een handgeschreven handtekening vervalst zal worden. Immers, bij het vervalsen van een handgeschreven handtekening is een schriftdeskundige bijna altijd in staat de vervalsing te ontdekken; dit heeft een remmend effect. Over twintig jaar zal dit nog steeds het geval zijn, omdat de menselijke techniek om een handgeschreven handtekening te plaatsen niet aan technische inflatie onderhevig is. Er zal juist verwacht moeten worden dat de technieken om een vervalste handgeschreven handtekening te ontdekken juist verder verbeterd zullen worden.

Met een elektronische handtekening ligt dit anders, ook over twintig jaar zal niet op een technische wijze aan te tonen zijn dat een handtekening valselijk is geplaatst, of een elektronische akte is vervalst. De drempel om op deze wijze tot fraude over te gaan zal dus veel lager zijn.

Een doemscenario zou zijn dat over enige tijd vrijwel iedereen in staat zal zijn om een willekeurig gekozen wederpartij in rechte te confronteren met een naar believen gefingeerde opgestelde elektronische akte waarvan gesteld wordt dat deze in 2010 is opgesteld, waarbij de rechter steeds de dwingende bewijskracht van deze akte dient te accepteren. Dit zou een totale chaos en ontwrichting van de maatschappij tot gevolg kunnen hebben.

Artikel 159 lid 2 Rv zal ons voor dit scenario behoeden. Immers, een akte waarvan de ondertekening stellig wordt ontkend levert geen bewijs op zolang niet bewezen is van wie de ondertekening afkomstig is.

Iemand die geconfronteerd wordt met een valse akte, kan dus volstaan met stellig te ontkennen dat hij de akte heeft ondertekend, waardoor de vervalser zal moeten bewijzen dat de akte wel geldig ondertekend is. Dat bewijs zal niet geleverd kunnen worden, omdat op het moment dat vervalsingen eenvoudig mogelijk zijn, ook algemeen bekend zal zijn dat het eenvoudig is om akten te vervalsen, waardoor het enkele feit dat de elektronische akte is ondertekend met een gekwalificeerde elektronische handtekening onvoldoende zal zijn om dat bewijs te leveren.

Hiermee komt het werkelijke probleem op langere termijn duidelijk aan de oppervlakte. Het enkele feit dat een akte met een gekwalificeerde elektronische handtekening is ondertekend, zal over geruime tijd niet meer voldoende zijn om de echtheid van de akte aan te tonen, waardoor de akte over enige tijd geen bewijskracht heeft, als de elektronische handtekening wordt ontkend.

Hierdoor ontstaat de situatie dat iemand die over geruime tijd beschikt over een elektronische akte uit 2010, geen bewijskracht aan deze akte kan ontlenen, als de handtekening van zijn wederpartij stellig ontkent wordt door deze wederpartij.

Ter nuancering kan aangevoerd worden dat in de dagelijkse praktijk nauwelijks in rechte de echtheid van een handgeschreven handtekening wordt ontkend en dat het daarom aannemelijk is dat dit ook met een elektronische handtekening niet snel zal gebeuren. Daar kan tegenin gebracht worden dat bij het ontkennen van de echtheid van een handgeschreven handtekening een schriftkundige alsnog met redelijke zekerheid uitsluitsel kan geven over de echtheid van de handtekening, wat een remmend effect heeft op het ten onrechte betwisten van de echtheid van een handtekening. Bij een elektronische handtekening is dit anders; de vervalsing, maar dus ook de echtheid van een verouderde elektronische handtekening kan niet meer door een deskundige worden vastgesteld.

Gezien deze overwegingen ben ik van mening dat de praktijk zal zijn, dat partijen er in de toekomst niet meer op kunnen rekenen dat aan een akte die ondertekend is met een verouderde elektronische handtekening dwingend bewijskracht wordt toegekend.

Er moet ook geanticipeerd worden op het scenario dat iemand een beroep doet op een valse akte jegens een partij die niet meer in staat is om de echtheid van de elektronische handtekening te betwisten, bijvoorbeeld als gevolg van ernstige ziekte of overlijden. Ter voorkoming van dit soort excessen is het zeker niet uitgesloten dat in de toekomst een elektronische akte die is ondertekend met een verouderde elektronische handtekening zijn dwingend bewijskracht verliest.

4.6 Gevaar voor de rechtszekerheid op langere termijn

Nu reeds kan al antwoord gegeven worden op de vraag of de elektronische akte een gevaar met zich meebrengt voor de rechtszekerheid op lange termijn. Deze vraag moet bevestigend beantwoord worden.

Immers, nu reeds valt te voorzien dat er een moment komt dat een breed publiek in staat is elektronische documenten met een willekeurige inhoud te voorzien van een valse gekwalificeerde elektronische handtekening. Dat zal dan weliswaar gaan om een elektronische handtekening die op dat moment sterk verouderd is, maar dit maakt het probleem slechts een beetje kleiner. Een akte heeft nu eenmaal ook de functie om op langere termijn bewijs op te leveren en de mogelijkheid dat over twintig jaar valse akten, waarvan de valsheid niet door deskundigen

aangetoond kan worden, als bewijs worden overlegd in een juridische procedure, maakt al dat de rechtszekerheid op langere termijn in het geding is.

Als het - enigszins speculatieve - scenario wat in de vorige paragraaf is beschreven uitkomt en er een moment komt dat een akte slechts als bewijs wordt erkend als deze is ondertekend met een elektronische handtekening die niet in praktische zin vervalsbaar is op het moment dat het bewijs wordt ingeroepen, dan zal ook dat grote gevolgen hebben voor de rechtszekerheid op langere termijn.

Op dit moment is het zo dat de veiligheid van de gekwalificeerde elektronische handtekening zo groot geacht wordt, dat rechtssubjecten zich wellicht juist van de elektronische akte gaan bedienen als ze belangrijke zaken willen regelen en absoluut zeker willen zijn van de bewijskracht van de akte. Tegen de echtheid van een gekwalificeerde elektronische handtekening valt immers op dit moment niets in te brengen, een handgeschreven handtekening levert op dit moment minder waarborgen. Van de ernstige inbreuk op de bewijskracht van de elektronische akte op langere termijn zullen deze partijen zich - terecht - niet bewust zijn.

4.7 Ter nuancering?

Ter nuancering zou aangevoerd kunnen worden dat ook een handgeschreven handtekening geen volkomen waarborg biedt bij misbruik. Daarnaast wordt in juridische procedures in de praktijk nauwelijks gesteld dat een handgeschreven handtekening niet echt zou zijn. Waarom zou dat met elektronische handtekeningen anders zijn? Kortom, in de praktijk zal het allemaal wel meevallen.

Dit stelt mij echter niet gerust. Het doorslaggevende verschil tussen handgeschreven handtekeningen en elektronische handtekeningen is immers de rol die de factor tijd speelt in het ongemerkt kunnen vervalsen van een handtekening. De techniek van een handgeschreven handtekening zal in de tijd wijzigen met de snelheid van de evolutie van de mens en kunnen we derhalve verwaarlozen. De techniek om een vervalste handtekening te ontdekken, verbetert echter steeds door nieuwe vindingen en betere toepassing van bekende vindingen. Een handgeschreven handtekening zal dus, enigszins paradoxaal in dit digitale tijdperk, steeds veiliger worden, omdat steeds beter en steeds goedkoper en met steeds meer zekerheid vastgesteld kan worden of een handgeschreven handtekening van een bepaalde persoon afkomstig is.

Bij een elektronische handtekening doet zich het merkwaardige verschijnsel voor, dat zowel de techniek om een "veilige" elektronische handtekening te zetten als de techniek om een dergelijke

handtekening ongemerkt te vervalsen, in een zeer snel tempo verbeterd. De techniek om een veilig geachte elektronische handtekening ongemerkt te vervalsen loopt tien tot dertig jaar achter op de techniek om de handtekening te plaatsen.

Waar de factor tijd de betrouwbaarheid van de handgeschreven handtekening gunstig gezind is, is dit tegenovergesteld voor de elektronische handtekening. De mogelijkheid om op langere termijn onmerkbaar een elektronische handtekening te vervalsen, is dus belangrijk groter dan deze voor de handgeschreven handtekening is; dit verschil zal met het verstrijken van de tijd steeds groter worden.

Maar met de mogelijkheid om een elektronische handtekening te vervalsen is nog niet gegeven dat dit ook op een dusdanige schaal zal gebeuren dat dit werkelijk een probleem vormt. Met handgeschreven handtekeningen gebeurt dit immers ook zelden.

Ook hier manifesteert zich een belangrijk verschil tussen handgeschreven en elektronische handtekeningen. Bij het vervalsen van een handgeschreven handtekening is er zoals gezegd een grote kans dat de vervalser ontmaskerd wordt. De pakkans is hoog en de vervalser kan vooraf niet goed inschatten hoe groot de kans is dat zijn vervalsing onopgemerkt blijft. De wetenschap dat deze kans in ieder geval klein is en dat zijn positie problematisch wordt als ontdekt wordt dat hij als vervalser actief is, maakt dat het een verstandige afweging is om van vervalsing af te zien en om niet ten onrechte te beweren dat een handtekening vals is. Immers de subjectieve pakkans is een belangrijke factor die mensen er van weerhoudt deviant gedrag ten toon te spreiden[33].

Bij het vervalsen van een elektronische handtekening is dit anders. Dit lukt wel, of het lukt niet. Als het wel lukt, dan laat de vervalsing geen sporen na en is het niet mogelijk om aan de hand van uitsluitend de elektronische handtekening vast te stellen dat het om een vervalsing gaat. Dit is dus een wezenlijk verschil met de handgeschreven handtekening.

Het - tegen beter weten in - betwisten van de echtheid van een elektronische handtekening zal, in tegenstelling tot de handgeschreven elektronische handtekening, in zijn algemeenheid resultaat boeken in een tijdperk waarin het voor een breed publiek mogelijk is de elektronische handtekening waar een beroep op wordt gedaan te vervalsen. Het valt moeilijk in te zien hoe een gebruiker van een elektronische handtekening twintig jaar na het plaatsen van de ze handtekening nog kan aantonen dat de handtekening werkelijk geplaatst is, als de handtekening zelf hiervoor

[33] van Koppen, p. 955.

onvoldoende bewijs oplevert vanwege de mogelijkheid deze handtekening te vervalsen en de afwezigheid van de mogelijkheid om de echtheid van de handtekening te onderzoeken.

Vanwege de veel kleinere pakkans bij misbruik van een elektronische handtekening en het ten onrechte betwisten van de echtheid van een elektronische handtekening, valt te verwachten - de psyche van de mens indachtig - dat de elektronische handtekening belangrijk vaker dan een handgeschreven handtekening vervalst zal worden of ten onrechte zal worden betwist.

4.8 Voorlopige conclusie

Een voorlopige conclusie is dat het invoeren van de elektronische akte, op langere termijn - denk aan twintig tot dertig jaar - een gevaar voor de rechtszekerheid zal betekenen. Te beredeneren valt dat akten die kort na het invoeren van de elektronische akte tot stand zijn gekomen, op lange termijn niet meer de bewijskracht zullen hebben die de partijen redelijkerwijs mogen verwachten ten tijde van het sluiten van deze akte. Het is niet ondenkbaar dat een elektronische akte op langere termijn in de praktijk nog slechts een zeer geringe bewijskracht heeft.

5 Het buitenland

Het is zinvol om te onderzoeken hoe in het buitenland de bewijskracht van de elektronische handtekening is geregeld. Uit de verschillen in wetgeving kan wellicht voor de Nederlandse situatie lering getrokken worden.

5.1 Wat is de bewijskracht van de elektronische akten in het buitenland?

Een groot probleem bij het beantwoorden van deze vraag is dat een volledig antwoord het bestuderen van alle buitenlandse rechtsstelsels op dit punt vergt.

Brazell heeft overzicht gemaakt van de wetgeving op het gebied van de elektronische akte, van 59 landen en gebieden. In dit overzicht is de situatie in 2008 beschouwd.

Uit dit overzicht blijkt dat er veel landen zijn die de elektronische handtekening en een elektronische akte als bewijs in een gerechtelijke procedure toelaten, maar slechts weinig landen geven hieraan een dwingende bewijskracht zoals dat in Nederland beoogt wordt. Daar waar dit wel gebeurt, is de bewijskracht niet als dwingend beschreven, maar is het zo geregeld dat een gekwalificeerde elektronische handtekening het privilege heeft van een aantal rechtsvermoedens, waar tegenbewijs voor toegelaten is.

Wat bij het bestuderen van de regelingen van de verschillende landen opvalt is dat veel landen nagenoeg identieke wetgeving op dit punt hebben. Op de wetgeving van enkele landen wil ik iets nader ingaan. Uiteraard moet ik de keuze van de landen die ik bespreek beperken en elke keuze zal arbitraire trekken hebben. Ik heb geprobeerd landen te beschrijven met opvallende verschillen met de Nederlandse wetgeving.

5.1.1 India en Singapore

India verbindt van de door Brazell beschreven landen de meest verstrekkende gevolgen aan een elektronische handtekening.

Sinds oktober 2000 luidt artikel 85B van de Indian Evidence Act als volgt:

85B. Presumption as to electronic record and digital signatures

(1) In any proceedings involving a secure electronic record, the Court shall presume unless contrary is proved, that the secure electronic record has not been altered since the point of time to which the secure status relates.

(2) In any proceedings, involving secure digital signature, the Court shall presume unless the contrary is proved that-

> *(a) the secure digital signature is affixed by subscriber with the intention of signing or approving the electronic record;*
>
> *(b) except in the case of a secure electronic record or a secure digital signature, nothing in the section shall create any presumption relating to authenticity and integrity of the electronic record or any digital signature.*

Hier wordt een rechtsvermoeden geformuleerd dat een "secure electronic record", vergelijkbaar met een elektronische akte die ondertekend is met een gekwalificeerde elektronische handtekening[34], niet is gewijzigd na ondertekening en dat de ondertekenaar tot doel had de inhoud goed te keuren.

Deze formulering wijkt in die zin af van het Nederlandse wetsvoorstel, dat in Nederland de bewijskracht van de elektronische handtekening opgeschort wordt op het moment dat deze stellig ontkend wordt en dat het bewijs van echtheid dus door de ondertekenaar geleverd moet worden.

[34] *The Information Technology Act, 2000* Chapter V.

In India is dat andersom - degene die de echtheid van de handtekening betwist dient te bewijzen dat de handtekening niet echt is.

Indien de in het vorige hoofdstuk beschreven scenario werkelijkheid wordt, dan levert dit aan de ene kant meer en aan de andere kant minder problemen op.

Meer problemen zijn te verwachten doordat degene die geconfronteerd wordt met een valse handtekening of een valselijk gewijzigde akte, de bewijslast heeft om de vervalsing aan te tonen. Dit kan een moeilijke of onmogelijke opgave zijn. Daar staat tegenover dat degene die zich schuldig maakt aan de vervalsing een misdrijf begaat, waar in India tot twee jaar gevangenisstraf op staat[35].

Omtrent het verlies van bewijskracht van de elektronische akte zijn minder problemen te verwachten dan in Nederland. Omdat in India de gebruiker van een elektronische handtekening beschermd wordt door een rechtsvermoeden, is het niet eenvoudig mogelijk om de bewijskracht van een elektronische akte op te schorten of teniet te doen, ook niet in de situatie dat de elektronische handtekening eenvoudig na te maken zou zijn. De wederpartij kan niet - zoals in Nederland het geval kan zijn - de bewijskracht opschorten door eenvoudig te stellen dat de handtekening niet echt is, maar zal feitelijk dienen aan te tonen dat de handtekening niet gezet is of dat de inhoud van de elektronische akte is gewijzigd.

In Singapore geldt precies dezelfde regeling, voor zowel bewijskracht[36] van de gekwalificeerde elektronische akte als de strafbaarheid[37] van fraude op dit punt.

5.1.2 Canada

Ook in Canada geldt een gelijksoortige regeling als in Singapore en India, hoewel de regelgeving hier op een andere manier is geredigeerd. In beginsel heeft degene die zich beroept op een elektronische akte de bewijslast dat deze akte authentiek is[38]. De *Governor in Council* heeft de bevoegdheid nadere regels te stellen ontrent rechtsvermoedens betreffende de bewijskracht van een gekwalificeerde elektronische akte[39]. Hier is invulling aan gegeven, in die zin dat een gekwalificeerde elektronische handtekening het vermoeden met zich meebrengt dat de gegevens

[35] Art 493-495 *Indian Penal Code*.
[36] Art 18 *Electronic Transactions Act 1998.*
[37] Art 25 *Electronic Transactions Act 1998.*
[38] Art 31.1 *Canada Evidence Act.*
[39] Art 31.4 *Canada Evidence Act.*

in de elektronische akte ondertekend zijn door de persoon die via het certificaat van de handtekening geïdentificeerd kan worden[40]. Tegenbewijs is toegelaten, de enkele ontkenning van de echtheid van de handtekening schort de bewijskracht niet op.

5.1.3 Estland

Estland is een land waar bijzonder veel praktijkervaring is met het gebruik van elektronische handtekeningen. Dit komt omdat in Estland het identiteitsbewijs voorzien is van een chip en geschikt is als veilig middel om een elektronische handtekeningen te plaatsen. Eind 2009 waren er meer dan een miljoen van deze kaarten in omloop[41], waardoor verreweg de meeste Esten in staat zijn om een gekwalificeerde elektronische handtekening te plaatsen. Thans zijn er dan ook al meer dan 24 miljoen digitale handtekeningen geplaatst in Estland. De eerste Estse wetgeving is in 2000 aangenomen. Estland is pas in 2004 toegetreden tot de Europese Unie, waardoor Estland een originele – niet primair op de Europese richtlijnen gebaseerde – regelgeving op dit punt kent, waarmee uiteraard niet is gezegd dat de regelgeving in strijd zou zijn met de Europese richtlijnen.

De wetgeving in Estland op het terrein van elektronische handtekeningen is compacter en meer voorschrijvend dan de Nederlandse equivalent. In paragraaf 2 van de Digital Signature Act is de definitie van een elektronische handtekening gegeven. Hieruit blijkt dat er in Estland maar één soort elektronische handtekening is en dat is de gekwalificeerde. Immers, een digitale handtekening moet aangemaakt zijn met een veilig middel (art 2(2)).

Omdat praktisch iedereen in Estland de beschikking heeft over een middel om gekwalificeerde elektronische handtekeningen te zetten, is er ook geen behoefte aan regelgeving voor elektronische handtekeningen die minder waarborgen geven. Misschien is de vanzelfsprekendheid van de beschikbaarheid van de middelen om gekwalificeerde elektronische handtekeningen te zetten ook van invloed geweest op de eenvoud van de wetgeving.

In beginsel heeft in Estland de elektronische handtekening dezelfde bewijskracht als een handgeschreven handtekening[42]. Ook in Estland wordt de bewijskracht van de elektronische handtekening opgeschort als deze niet door de persoon gezet is die geassocieerd wordt met de handtekening[43]. In tegenstelling tot Nederland is niet het eenvoudig ontkennen van de

[40] Art 5 *Secure Electronic Signature Regulations* (SOR/2005-30).
[41] <www.id.ee>.
[42] Art 3(1) Digital Signature Act.
[43] Art 3(3) Digital Signature Act.

handtekening voldoende, maar moeten omstandigheden bewezen worden die misbruik van de handtekening aannemelijk maken[44]. Niet alleen deze bepaling is in mijn ogen evenwichtiger dan de situatie in Nederland. Ook de aanvullende bepaling dat de persoon die geassocieerd wordt met de vals geplaatste elektronische handtekening schadeplichtig is als de valse plaatsing het gevolg was van grove nalatigheid door de met de handtekening geassocieerde persoon, draagt bij aan de rechtszekerheid van de wederpartij.

In Estland bestaat weliswaar het voorschrift dat een handgeschreven handtekening verplicht is als de wet de schriftelijke vorm van een akte voorschrijft[45], maar ook hier is een elektronische handtekening geaccepteerd als de akte aan een aantal basale voorwaarden voldoet (zoals het bevatten van de namen van de partijen en reproduceerbaarheid) , de elektronische handtekening algemeen in gebruik is (wat het geval is in Estland) en de wederpartij geen handgeschreven handtekening verlangd.

In Estland levert een akte geen dwingend bewijs op[46].

5.2 Conclusies uit rechtsvergelijking

Gezien de beperktheid van het rechtsvergelijkend onderzoek is het niet mogelijk om harde conclusies hieraan te verbinden. Wel geeft de greep aan rechtstelsels die ik bestudeerd heb een duidelijk beeld.

Dit beeld is dat Nederland verder lijkt te gaan dan alle andere landen als het gaat om de bewijskracht van de elektronische akte. Dit komt vooral door de beoogde dwingende bewijskracht van de elektronische akte en het gebrek aan een evenwichtige regeling die ziet op misbuik van de elektronische akte.

Wat tevens opvalt, is dat ook andere landen in hun wetgeving geen rekening lijken te houden met de mogelijkheid dat de betrouwbare elektronische handtekening van deze tijd over enige tijd te vervalsen is. In andere rechtstelsels is dit gemis echter minder ernstig, omdat ofwel de elektronische akte op voorhand reeds geen dwingende bewijskracht had, ofwel er een betere regeling is omtrent vervalste handtekeningen.

[44] Art 3(4) Digital Signature Act.
[45] Art 78(1) General Part of the Civil Code Act.
[46] Art 95(2) Code of Civil Procedure.

Het lijkt er dus op dat Nederland, zoals de minister al bij het indienen van de motie van Heemskerk voorspelde, een buitenbeetje wordt met de beoogde wetgeving.

6 Aanbevelingen

De zorgen omtrent de rechtszekerheid na invoering van de elektronische akte culmineren in het feit dat een elektronische akte die momenteel als veilig wordt beschouwd, over enige tijd onmerkbaar te vervalsen is. Dit heeft als gevolg dat ten onrechte een beroep gedaan kan worden op een vervalste elektronische akte – en erger – dat de echtheid van een elektronische akte ten onrechte ontkent kan worden, zonder dat er aanvullende mogelijkheden zijn zoals schriftonderzoek om te oordelen over de authenticiteit van de elektronische handtekening. Omdat in Nederland een elektronische akte dwingende bewijskracht krijgt, is de rechtszekerheid in het geding, omdat een bewijsstuk wat voorheen dwingend bewijskracht had, devalueert tot een stuk wat alleen enige bewijskracht heeft als de wederpartij bereid is de echtheid van de handtekening niet te betwisten. Het ontkennen van de echtheid van de elektronische handtekening is op termijn nauwelijks als een valse ontkenning te ontmaskeren en op het valselijk ontkennen van de echtheid van een elektronische handtekening staat geen sanctie. Gevreesd moet worden dat het valselijk ontkennen van een elektronische handtekening in de toekomst veelvuldig zal voorkomen.

Aanbevelingen moeten tot gevolg hebben dat deze vrees wordt weggenomen.

6.1 Beperk de dwingende bewijskracht van elektronische handtekeningen in tijd

Dit is een even voor de hand liggende als effectieve maatregel. Feitelijk is het inconsequent dat de rechtskracht van een gekwalificeerde elektronische handtekening niet beperkt is in tijd. Immers, een elektronische handtekening kan alleen als gekwalificeerde elektronische handtekening gelden, als deze gezet is binnen de geldigheidsperiode van het certificaat waarop deze elektronische handtekening berust[47]. Een gekwalificeerd certificaat is maximaal vijf jaar geldig. Deze eis en beperking van de geldigheidsduur is juist ingevoerd vanwege het inzicht dat de techniek die met een gekwalificeerd certificaat geassocieerd is (bijvoorbeeld de sleutellengte en de encryptie en samenvattingstechniek) na enige tijd niet meer veilig is.

[47] Art 3 lid f Besluit elektronische handtekeningen juncto art 18.15 lid 2 Telecommunicatiewet.

Het zou consistent zijn – en mede daarom beveel ik dat ook aan – om slechts dwingende bewijskracht toe te kennen aan een elektronische akte die ondertekend is met een gekwalificeerde elektronische handtekening, binnen de geldigheidsperiode van het certificaat waar de elektronische handtekening op berust.

Het zou dan tevens mogelijk moeten zijn om de periode waarop een beroep op de dwingende bewijskracht gedaan kan worden, te verlengen door de elektronische akte binnen de geldigheidsduur van het certificaat, opnieuw te ondertekenen met een handtekening gebaseerd op een nieuw certificaat met een geldigheidsduur verder in de toekomst. Deze ondertekening hoeft slechts eenzijdig te geschieden door de persoon die een beroep wil doen op de echtheid van de akte. De medewerking van de wederpartij is hiervoor niet nodig. De hernieuwde ondertekening borgt de echtheid van het ondertekende stuk en kan gezien worden als de stuiting van de verjaring van de dwingende bewijskracht van de akte.

Dit is een eenvoudig in te voeren beperking, die de in dit stuk genoemde bezwaren voor een groot deel zou wegnemen, zonder dat deze beperking grote nadelen met zich meebrengt.

Deze aanbeveling gaat gepaard met het langer bewaren van de gegevens die gebruikt zijn voor het aanmaken van het certificaat door de dienstverlener. Nu hoeven deze gegevens slechts zeven jaar bewaard te worden, een termijn die goed is afgestemd op de geldigheid van het certificaat. Maar omdat deze aanbeveling ketens van geldige certificaten mogelijk maakt, kan het nodig zijn om ook duidelijkheid te krijgen over de certificaten die langer geleden zijn aangemaakt.

De bezwaren vervallen voor een groot deel met deze maatregelen, omdat het in praktische zin zeer onaannemelijk is dat een elektronische handtekening te vervalsen is binnen de geldigheidsduur van het geassocieerde certificaat. Indien de snelheid van de technische vorderingen op dit punt daar aanleiding toe zou geven kan ook de geldigheidsduur van certificaten bekort worden. Alle genoemde bezwaren zijn gebaseerd op een reële technische mogelijkheid om een elektronische handtekening te vervalsen of de inhoud van een ondertekend stuk ongemerkt te wijzigen.

Het enige nadeel van dit voorstel is dat een elektronische akte na enkele jaren opnieuw ondertekend moet worden om zijn dwingende bewijskracht te behouden. Dit is in het geheel geen nadeel voor de meerderheid van elektronische aktes die slechts bedoeld zijn om voor een korte periode als bewijs te gelden. Verreweg de meeste akten dienen slechts voor een korte periode als bewijs. Het vernieuwen van een elektronische handtekening is nauwelijks tijdrovend voor

rechtssubjecten die de beschikking hebben over een middel om gekwalificeerde elektronische handtekeningen te plaatsen.

Daarnaast pleit ik er niet voor om de bewijskracht van een elektronische akte waarvan het onderliggende certificaat is verlopen geheel te laten vervallen; slechts het dwingend karakter zou moeten vervallen.

Dat betekent dat een “verlopen” elektronische akte nog steeds vrij bewijs oplevert en de facto zelfs dwingend bewijs, zolang de techniek waarmee de elektronische handtekening is geplaatst niet is achterhaald. Immers, zolang de elektronische handtekening nog als veilig kan worden aangemerkt, zal de rechter naar verwachting veel waarde hechten aan de akte.

6.2 Koppel de dwingende bewijskracht aan registratie van de akte

Schriftelijke akten kunnen thans bij de belastingdienst geregistreerd worden. Daarmee kan naderhand bewezen worden dat op de datum van registratie de akte bestond. Elektronische akten kunnen echter niet geregistreerd worden.

Daarom is aan te bevelen ook een mogelijkheid te creëren om elektronische akten te registreren. Technisch gezien is dit eenvoudig. Feitelijk komt dit neer op het elektronische wijze versturen van de elektronische akte naar een instantie, waarbij de datum van versturen als registratiedatum zou kunnen gelden. Indien een betrouwbare partij (bijvoorbeeld de certificatiedienstverlening, de belastingdienst of een notaris) verklaart dat een elektronische akte op een bepaalde datum is geregistreerd, kan zodoende bewijs worden geleverd dat een elektronische akte met een gekwalificeerde handtekening op een moment dat het onderliggende certificaat geldig was bestond.

Thans zullen er zeker notarissen bereid gevonden kunnen worden om deze dienst te verlenen, maar de kosten hiervan zullen zo hoog zijn dat de drempel om van deze diensten gebruik te maken te hoog is. Het zou beter zijn een toegankelijke regeling hiervoor te maken, door bijvoorbeeld de certificatiedienstverleners te verplichten op eenvoudige en goedkope wijze de elektronische akte te laten registreren.

Het enkel laten registreren van een elektronische akte maakt dat iemand kan bewijzen dat de akte authentiek is. Als volstaan wordt met alleen de mogelijkheid om de akte te registreren, dan lost dit het probleem van de rechtsonzekerheid niet op. Immers, de vermeende dwingende bewijskracht

van niet geregistreerde akten is onverminderd problematisch en ook het op voorhand dwingend karakter van een vervalste niet geregistreerde akte is nog steeds aanwezig.

Daarom zal de introductie van een laagdrempelige mogelijkheid om elektronische akten te registreren gekoppeld moeten worden aan de bepaling dat alleen geregistreerde elektronische akten dwingend bewijskracht hebben.

6.4 Schaf de opschorting van de bewijskracht bij ontkenning van de handtekening af

Indien één of beide voorgaande aanbevelingen worden opgenomen, dan is het praktisch gezien nauwelijks mogelijk dat een elektronische akte die dwingend bewijskracht geniet niet echt is. Het is dan niet langer redelijk om de bewijslast van de authenticiteit van de handtekening bij de gebruiker van de handtekening te leggen. Het is veel evenwichtiger om een rechtsvermoeden te hanteren dat een akte die ondertekend is met een gekwalificeerde elektronische handtekening en die tevens voldoet aan één van de twee voorgaande aanbevelingen authentiek is. Tegenbewijs moet toegelaten worden, als is het maar omdat het mogelijk is dat een derde zich toegang heeft verschaft tot het middel om de elektronische handtekening te plaatsen en de bijbehorende codes heeft ontvreemd. Dit tegenbewijs - of het aannemelijk maken van omstandigheden die misbruik mogelijk zouden hebben gemaakt - zal dan echter door de degene die de handtekening geplaatst zou hebben moeten worden geleverd.

Hiermee is de rechtszekerheid gediend, omdat met deze regeling de gebruiker van een elektronische akte in beginsel kan vertrouwen op de dwingende bewijskracht van deze akte.

6.5 Maak de certificaathouder aansprakelijk voor schade door misbruik

Binnen de voorgestelde regelgeving is een scenario voorstelbaar dat een elektronische akte wordt ondertekend door een persoon die niet geassocieerd is met het veilige middel waarmee de handtekening gezet is, vanwege onzorgvuldigheid door deze persoon. Deze onzorgvuldigheid kan bestaan uit onvoldoende voorzorgsmaatregelen treffen om toegang voor derden tot het veilige middel en de codes om dit middel te bedienen af te schermen. Deze persoon is dan niet gebonden aan de akte omdat hij de handtekening zelf niet gezet heeft. Het is maar zeer de vraag of de schade die de wederpartij te goeder trouw zijn schade op basis van onrechtmatige daad kan verhalen.

Het lijkt mij voor de rechtszekerheid van belang dat een partij bij de elektronische akte de zekerheid heeft dat hij ofwel nakoming van de overeenkomsten beschreven in de akte kan vorderen, ofwel schadevergoeding kan verlangen.

In zijn algemeenheid is het zo dat de houder van een veilig middel om een elektronische handtekening te plaatsen steeds maatregelen kan nemen om te voorkomen dat dit middel in handen van derden valt. Gezien de verhouding in belangen en mogelijkheden om schade te voorkomen, wil ik zelfs verder gaan dan de regeling in Estland en een risicoaansprakelijkheid voorstellen die de houder van een veilig middel om een elektronische handtekening te zetten aansprakelijk maakt voor schade die ontstaat door het onbevoegd gebruik van dit middel.

Deze risicoaansprakelijkheid kan in zeldzame gevallen - zoals bij dwang - worden beperkt.

6.6 Maak het onterecht ontkennen van een elektronische akte strafbaar

Deze aanbeveling doe ik met enige aarzeling, omdat ik geen oordeel kan vellen over de haalbaarheid, wenselijkheid en handhaafbaarheid hiervan. Daarnaast levert deze “aanbeveling” slechts een beperkte bijdrage aan de oplossing van het onderhavige probleem.

Daarom wil ik mij beperken met de opmerking dat als het strafbaar zou zijn om ten onrechte in rechte te stellen dat een gekwalificeerde elektronische handtekening niet echt is, dit wellicht leidt tot preventie van deze onwenselijke situatie. Nu is het natuurlijk reeds mogelijk om partijgetuigen onder ede een verklaring te laten afleggen over de authenticiteit van de akte, maar dit is vanwege de kostbaarheid van een getuigenverhoor niet een economische optie. Daarnaast is het ook niet vanzelfsprekend om de partij die een beroep doet op de onechtheid van een akte als getuige te laten horen om juist de echtheid aan te tonen, waardoor het bestaan van deze optie niet hetzelfde effect zal hebben als de voorgestelde aanbeveling.

Deze aanbeveling zal echter alleen leiden tot minder onterechte beweringen dat een elektronische handtekening onecht zou zijn. Dat is behulpzaam, maar naar mijn mening niet afdoende.

7 Conclusie

Het is aannemelijk dat op middellange termijn, over ongeveer twintig jaar, de technieken die thans gebruikt worden voor het plaatsen van een elektronische handtekeningen die met de meeste waarborgen zijn omkleed, verouderd zijn. Dit heeft tot gevolg dat elektronische akten die met de

momenteel meest betrouwbare technieken worden opgesteld, over enige tijd kunnen worden gewijzigd zonder dat deze wijzigingen kunnen worden opgespoord en zonder dat een deskundige in staat zal zijn een betrouwbare uitspraak te doen over de authenticiteit van deze verouderde elektronische handtekening.

Een akte heeft in het Nederlandse recht dwingende bewijskracht. Partijen die met de voorgestelde wetswijziging indachtig een elektronische akte opstellen, zijn hiermee in de veronderstelling dat zij over een krachtig bewijsmiddel beschikken.

De dwingende bewijskracht van de (elektronische) akte wordt echter opgeschort als de echtheid van de handtekening (stellig) wordt betwist. Momenteel zal eenvoudig te bewijzen zijn dat een elektronische handtekening wel echt is, waardoor de bewijskracht gehandhaafd blijft.

Over geruime tijd zal het echter een feit van algemene kennis zijn dat verouderde elektronische akten met een gekwalificeerde elektronische handtekeningen eenvoudig te vervalsen zijn. Een partij die de echtheid van een elektronische handtekening betwist, hoeft nauwelijks te vrezen voor tegenbewijs. In tegenstelling tot een handgeschreven handtekening, is het immers niet mogelijk om aan te tonen dat een elektronische handtekening is vervalst, door onderzoek van alleen de elektronische handtekening.

Dit gegeven levert twee problemen op. Enerzijds wordt het over enige tijd eenvoudig om oude akten ongemerkt te wijzigen. Hierdoor lopen partijen het risico dat men geconfronteerd wordt met akten met een andere inhoud dan die ze feitelijk hebben ondertekend.

Op zichzelf is dit een negatief gevolg voor de rechtszekerheid. De gevolgen zullen echter beperkt blijven; de wederpartij zal met een andere versie van de akte kunnen aantonen dat in ieder geval één exemplaar niet authentiek is. Het vervalsen van een akte is daarnaast strafbaar, waardoor niet te verwachten is dat er op grote schaal akten zullen worden vervalst.

Ernstiger is de mogelijkheid om de authenticiteit van een elektronische handtekening te betwisten. De wederpartij die thans denkt over een bewijsstuk met dwingend bewijskracht te beschikken, staat dan met lege handen. Hij kan immers – zodra algemeen bekend is dat de betreffende handtekening te vervalsen is – niet door onderzoek van de handtekening zelf aantonen dat de handtekening echt is.

Het gevolg van de invoering van de elektronische handtekening is dat over enige tijd de bewijskracht van een oude elektronische akte alleen nog wordt gehandhaafd als de wederpartij

bereid is deze niet te betwisten. De functie van een akte is juist dat een wederpartij de bewijskracht altijd kan inroepen, ook als de wederpartij de inhoud betwist.

Om deze reden ben ik van mening dat door de invoering van de elektronische akte de rechtszekerheid op lange termijn ernstig wordt bedreigd.

De meest voor de hand liggende oplossing voor dit probleem is de dwingende bewijskracht van een elektronische akte te beperken in tijd, waarbij de bewijskracht te verlengen is (het verval van de bewijskracht wordt dan gestuit) door opnieuw een elektronische handtekening onder de akte te plaatsen.

Ter nuancering kan opgemerkt worden dat het partijen ook zonder aanpassing van de wet vrij staat om deze aanbeveling te volgen. Partijen zullen echter in het algemeen niet stil staan welke gevolgen de technische vooruitgang met zich mee kunnen brengen. Met het oog op de rechtszekerheid is het dan ook nuttig deze aanbeveling in de wet op te nemen.

Literatuur

Brazell 2008
L. Brazell, *Electronic signatures and identities, law & regulation*, London: Sweet & Maxell 2008.

Franken e.a. 2004
H. Franken, H.W.K. Kaspersen, J.P. Bergfeld en A.H. de Wild, *Recht en computer, vol 36*, Deventer: Kluwer 2004.

Hendrikse, van Huizen en Rinkes 2005
M.L. Hendrikse, Ph. H.J.G van Huizen en J. Rinkes, *Nieuw verzekeringsrecht praktisch belicht,* Deventer: Kluwer 2005.

Hidma en Rutgers 2004
T.R. Hidma en G.R. Rutgers, *Bewijs,* Deventer: Kluwer 2004.

van Koppen 2002
P.J. van Koppen, *Het recht van binnen: psychologie van het recht*, Deventer: Kluwer 2002.

Mason 2007
S. Mason, *Electronic signatures in law,* Haywards Heath: Tottel 2007.

Shor 1997
P.W. Shor, 'Polynominal-time algorithms for prime factorization and discrete logarithms on a quantum computer', *SIAM J. Computing* 1997-26 p. 1484-1509.