

## ELEKTRONISCHE ONDERTEKENING: HOE HAD U HET GEWENST?

Verslaglegging expertmeeting op UvA 6-6-2014; nabeschouwingen; drie kanttekeningen bij wetsvoorstel 34059/ KEI project <sup>1</sup>

### *1a. Aanleidingen en inleiding*

Onvaste terminologie leidt nogal eens tot onbestemde resultaten. Iets soortgelijks dreigt zich voor te doen bij de term elektronische hand- of ondertekening, dan wel gangbare terminologische equivalenten daarvan, zoals elektronische handtekening, digitale ondertekening of digitale handtekening.

De regelgeving hierover in art. 3:15a BW, ontleend aan Richtlijn 1999/93/EG, vertoont, zeker in terminologisch opzicht, een zwalkend geheel.

In lid 2 wordt de term gekoppeld aan reeds lang vertrouwde vereisten van waarborg en veiligheid, in lid 4 worden deze vereisten .. overboord gegooid; zoals hieronder zal blijken. De term elektronische/ digitale ondertekening dient derhalve steeds op een kontekstuele wijze te worden geduid of begrepen. Een frappant voorbeeld hiervan is te vinden onder nr. 12.3.3 van de Memorie van Toelichting van het op 24 oktober 2013 ingediende voorontwerp wetsvoorstel 34059/ project KEI, ofwel project Kwaliteit en Innovatie, ([www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2013/10/24/wetsvoorstel-vereenvoudiging-en-digitalisering-procesrecht.html](http://www.rijksoverheid.nl/documenten-en-publicaties/kamerstukken/2013/10/24/wetsvoorstel-vereenvoudiging-en-digitalisering-procesrecht.html).): " Als een document digitaal is ondertekend ... is van belang de integriteit van het document te waarborgen met middelen die het mogelijk maken het ongewijzigd blijven van het document aan te tonen." Overduidelijk duidt de hier gebezigde terminologie digitale ondertekening niet op art. 3:15a lid 4 BW.<sup>2</sup> Maar

---

<sup>1</sup> Met mijn hartelijke dank aan prof. dr. A.I.M. van Mierlo en drs. J. van Straalen voor hun bijdragen aan deze bijdrage. Mede aan de hand van onderstaande tekst verscheen in JBPr (Jurisprudentie Burgerlijk Procesrecht) 2014 aflevering 5, blz. 489-499, het openingsartikel onder het opschrift: Elektronisch ondertekenen volgens wetsvoorstel 34059 en volgens het vernieuwde arbitragerecht; in welk openingsartikel onder meer nog wat nader wordt ingegaan op het voorgestelde art. 30c Rv van wetsvoorstel 34059.

<sup>2</sup> De leden 1, 2 en 4 van art. 3:15a BW luiden als volgt.

Art. 15a-1. Een elektronische handtekening heeft dezelfde gevolgen als een handgeschreven handtekening, indien de methode die daarbij is gebruikt voor authenticatie voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische gegevens worden gebruikt en op alle overige omstandigheden van het geval.

-2. Een in lid 1 bedoelde methode wordt vermoed voldoende betrouwbaar te zijn, indien een elektronische handtekening voldoet aan de volgende eisen:

- a. zij is op unieke wijze aan de ondertekenaar verbonden;
- b. zij maakt het mogelijk de ondertekenaar te identificeren;
- c. zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden; en
- d. zij is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;
- e. zij is gebaseerd op een gekwalificeerd certificaat als bedoeld in artikel 1.1 onderdeel ss [lees:tt] van de Telecommunicatiewet;
- f. zij is gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen als bedoeld in artikel 1.1 onderdeel vv [lees:ww] van de Telecommunicatiewet.

-4. Onder elektronische handtekening wordt een handtekening verstaan die bestaat uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die

betekent dit dat art. 3:15a lid 2 BW onverkort over de hele linie heeft te gelden?

Het hier geschetste spanningsveld markeerde de op 6 juni 2014 gehouden expertmeeting over elektronische ondertekeningen aan de Universiteit van Amsterdam. Vragen die vaak op hun beloop worden gelaten, werden hier aan de orde gesteld en bediscussieerd, zoals bijvoorbeeld de vraag wanneer een elektronische ondertekening moet voldoen aan art. 3:15a lid 2 BW, of de vraag in welke mate wij, juristen, in een gedeeltelijk ICT-technische beoordeling moeten treden of een elektronische ondertekening voldoet aan art. 3:15a lid 2 BW.

Zoals gezegd, en wellicht engiszins blijkt uit voormeld citaat, worden dergelijke vragen dikwijls onder de pet gehouden, maar er zijn ook andere tekenen waarneembaar, zoals bleek tijdens de expertmeeting. Zo valt te wijzen op rechtspraak waarin nadere waarborg vereisten worden gesteld aan elektronische ondertekeningen. En ook de wetgever, zowel in Nederland als elders, heeft er in sommige situaties van blijk gegeven dat een elektronische ondertekening moet voldoen aan de waarborg vereisten van art. 3:15a lid 2 BW; zie bijvoorbeeld het in 2010 gewijzigde art. 7:932 lid 1 BW dat een elektronische verzekeringspolis mogelijk maakt mits deze is voorzien van een elektronische ondertekening die voldoet aan de waarborg vereisten van art. 3:15a lid 2 BW. Een recenter voorbeeld is de per 1 januari 2015 in werking tredende arbitrage wetgeving met het tijdens de expertmeeting besproken voorschrift van art. 1072b lid 3 Rv waarin is bepaald dat een elektronische ondertekening onder een arbitraal vonnis moet voldoen aan art. 3:15a lid 2 BW.

Volgens Martius, die eind 2007 promoveerde op de monografie Elektronisch handelsrecht <sup>3</sup>, heeft Duitsland een voorsprong op ons genomen met par. 126a BGB<sup>4</sup> waar is bepaald dat wanneer de wet een schriftelijke vorm voorschijft, aan dit voorschrift tevens op elektronische wijze kan worden voldaan 'mit einer qualifizierten elektronische Signatur', ofwel met een elektronische ondertekening die voldoet aan de waarborg vereisten zoals die van art. 3:15a lid 2 BW.

De deelnemers aan de expertmeeting waren afkomstig uit de advocatuur, rechterlijke macht, Raad voor de rechtspraak, Ministerie van Veiligheid en Justitie/ JustID, Notariaat, ICT bedrijven, Elektronische uitgeverij en universiteiten.

De dagvoorzitter was prof. dr. B.C.M. Waaijer (UvA; notaris bij Boekel De Neree), als inleiders traden op:

Mr. Ir. F.P.A. Dondorp (ICT bedrijf Decos, auteur van de monografie: Elektronische handtekeningen: juridische waarde en praktisch gebruik, SDU 2011, ISBN 9789012570534);

Prof. dr. A.I.M. van Mierlo (Erasmus Universiteit, partner Nauta Dutilh);

Prof. dr. G.J. Meijer (Erasmus Universiteit, partner Nauta Dutilh).

### *1b. Opbouw*

In nr. 2 volgen opmerkingen over de ambivalente regelgeving van art. 3:15a BW, in de nrs. 3-7 volgt een verslaglegging van de expertmeeting, in nr. 8 volgen enkele nabeschouwingen mede naar

---

worden gebruikt als middel voor authenticatie.

<sup>3</sup> Elektronisch handelsrecht De juridische aspecten van elektronische communicatie in het handelsrecht, Deel 8 NTHR-reeks, Zutphen 2008/ uitgeverij Paris, door mr. dr. H.P.A.J. Martius; nr. 5.4.2.

<sup>4</sup> par 126a BGB Elektronische Form

(1) Woll die gesetzlich vorgeschriebene schriftliche Form durch die elektronische Form ersetzt werden, so muss der Aussteller der Erklärung dieser seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronische Signatur nach dem Signaturgesetz versehen.

(2) Bei einem Vertrag müssen die Parteien jeweils ein gleichlautendes Dokument in der in Absatz 1 bezeichneten Weise elektronisch signieren.

aanleiding van opmerkingen van Martius en in nr. 9 gaat de aandacht uit naar de digitale ondertekening zoals die is opgenomen in wetsvoorstel 34059/ project KEI.

## **2. Ambivalente regelgeving in art. 3:15a BW**

Als het elektronische rechts- en processuele verkeer intensiever gaat worden, is duidelijkheid over de vereisten van de elektronische een voorwaarde. Die duidelijkheid is er nu niet of onvoldoende zoals blijkt uit het van Richtlijn 1999/93/EG afkomstige art. 3:15a BW dat, zoals werd opgemerkt, op twee gedachten hinkt.

In art. 3:15a lid 2 sub a/d BW worden voor een veilige en betrouwbare elektronische ondertekening waarborgen voorgeschreven die vrijwel samenvallen met die welke worden gerealiseerd door de traditionele schriftelijke ondertekening, waarbij voornamelijk - maar niet uitsluitend - valt te denken aan uniciteit en verifieerbaarheid. Lid 4 van art. 3:15a BW geeft daarentegen een ander uiterste te zien. Volgens lid 4 kwalificeert de enkele omstandigheid dat het ene bericht "vastgehecht aan of logisch geassocieerd" is met een ander bericht, dat dit ene bericht reeds als een elektronische ondertekening geldt; vanzelfsprekend zonder voormelde waarborgen.

Voormeld lid 4 van art. 3:15a lid 4 BW valt wat betreft het gebrek aan waarborgen als volgt met een voorbeeld te illustreren: wanneer A(lice) in een mail aan B(ob) zich bepaalt tot de mededeling dat ook C(harlie) akkoord gaat met een bepaalde transactie, dan geldt volgens de letterlijke tekst van voormeld lid 4 deze mededeling als een elektronische ondertekening van C(harlie) ten gunste van B(ob); van welke mededeling C(harlie) wellicht geheel onkundig is. Deze mededeling van A(lice) bevat immers "elektronische gegevens" gericht aan B(ob) terwijl deze gegevens "zijn vastgehecht aan of logisch geassocieerd met andere elektronische gegevens" - te weten de naam van C(harlie) - terwijl die andere elektronische gegevens "worden gebruikt als middel voor authenticatie" van C(harlie). Het mag duidelijk zijn dat een dergelijke "elektronische ondertekening" geen spoor, maar dan ook geen spoor, bevat van de waarborgen die vanouds en over de gehele linie worden geassocieerd met de term ondertekening of handtekening. Een onoverzienbare en overstelpende hoeveelheid elektronische berichten valt dus volgens dit lid 4 onder de term elektronische handtekening.

## **3. Uit en naar aanleiding van de inleiding van F.P.A. Dondorp**

### *3a. Elektronische ondertekening als bottleneck*

Met de digitalisering/ elektronisering van ons rechts- en maatschappelijk verkeer vlot het nog niet erg en de elektronische ondertekening vormt dikwijls een bottleneck. ICT-technische en -juridische oordelen ontmoeten elkaar nog niet optimaal en daardoor wacht men op elkaar; bijvoorbeeld op een vorige nog niet geheel afgeronde schakel of op verwachtingsdoeleinden van een volgende schakel. Vaak is voor elektronisch communiceren goedkeuring op papier nodig, maar verloopt deze communicatie tenslotte door het afdrukken op papier en vindt ook de archivering plaats op papier. Op den duur lijkt dit alles niet vol te houden en zou een laagdrempelig elektronisch alternatief voor de fysieke ondertekening, welk alternatief ook zeer gemakkelijk zou moeten zijn in het gebruik, uitkomst moeten bieden.

Wel moeten daarbij twee bindingen worden gewaarborgd: het elektronisch ondertekende bericht moet zijn te herleiden naar de ondertekenaar en mag niet na elektronische ondertekening ongemerkt kunnen worden gewijzigd.

### *3b. Gangbare PKI (Private/Public Key Infrastructure) systemen van elektronische ondertekening*

Bij een CSP (Certificate Service Provider), ook wel Certificate Authority (CA), eveneens wel Trusted Third Party (TTP), en hier verder aan te duiden als CSP, koopt A(lice) een sleutelpaar dat bestaat uit een privé en een publieke sleutel. Wat A(lice) kan versleutelen met haar privé sleutel, kan zij of B(ob) of een derde alleen ontsleutelen met haar publieke sleutel, die bekend, althans raadpleegbaar is voor

derden. Bovendien werkt dit vice versa: wat versleuteld is met de publieke sleutel van A(lice), kan alleen maar ontsleuteld worden - in beginsel door A(lice) - met haar privé sleutel.

A(lice) bepaalt een 'hashwaarde' van het door haar elektronisch te ondertekenen bericht. Die hashwaarde is een unieke samenvatting van het bericht met de bijzonderheid dat elke, zelfs uiterst minieme, wijziging van het bericht leidt tot een andere hashwaarde.<sup>5</sup> De hashwaarde wordt in het Engels aangeduid als message digest en wordt in bijgaande schema's wel afgekort als MD.

Het elementaire bestanddeel van de elektronische ondertekening van A(lice) is nu de hashwaarde van het bericht welke hashwaarde is versleuteld met haar privé sleutel; deze versleutelde hashwaarde wordt vaak apart verzonden.

Hiermee lijkt de cirkel rond: de publieke sleutel van A(lice) kan B(ob) opvragen, daarmee ontsleutelt hij de hashwaarde van het bericht. B(ob) kan daarnaast zelf de hashwaarde van het bericht bepalen en identiteit constateren. Het bericht is dus niet veranderd en afkomstig van A(lice).

### *3c. Heeft B(ob) hiervoor specifieke software of specifieke programma's nodig?*

B(ob) kan gebruik maken van het zeer wijd verspreide programma Adobe Reader. De sleutelbeheerder/ CSP vraagt bij de versleuteling of de elektronische ondertekening/ versleutelde hashwaarde is verzonden en geeft een bevestigend antwoord door aan Adobe Reader. Vervolgens wordt bij B(ob) in een blauwe balk aangegeven dat is ondertekend en verschaft het doorklikken nadere informatie omtrent die elektronische ondertekening.

### *3d. Een eerste bezwaar tegen PKI systemen van elektronische ondertekening: gebrek aan persoonsgebondenheid*

Hoewel A(lice) zich bij de aanschaf van het sleutelpaar vaak - niet altijd - moet legitimeren bij de CSP, geeft dit nog geen echte waarborg voor persoonsgebondenheid. De privé sleutel van A(lice) kan ook door anderen worden gebruikt en dit gebeurt in de praktijk ook waar bijvoorbeeld een (privé) sleutel aan een secretariaat ter beschikking wordt gesteld.

Een hierna aan de orde komende vraag is of aan het te constateren, dan wel geconstateerde, gebruik van de privé sleutel van A(lice) het (rechts)vermoeden kan worden ontleend dat het bericht inderdaad van A(lice) uitging.

Het is natuurlijk wel zo dat de vraag of A(lice) zelf getekend heeft of niet, geen louter technische is. In wezen gaat het tevens om het verzorgen van voldoende administratief organisatorische waarborgen.

Als die hoog genoeg zijn, zou ook eventueel van 'zwakkere' systemen van elektronische ondertekening gebruik gemaakt kunnen worden; zwaarder aangezet: de technici hebben zich gebogen over de technische waarborgen en nu valt te hopen dat de juristen de rijen sluiten over de vraag welke procedurele waarborgen in welk geval zijn vereist.

### *3e. Een tweede bezwaar tegen PKI systemen: de aanval van de Man in the Middle; zie ook schema 2*

Een technische zwakte van PKI systemen van elektronische ondertekening is dat het niet zeer moeilijk is voor een Man in the Middle, verder: C(harlie), om te interveniëren; zoals ook bij DigiNotar is gebeurd. C(harlie) ontsleutelt met de publieke sleutel van A(lice) het voor B(ob) bestemde bericht en hersleutelt het met zijn privé sleutel. In de communicatie waarin A(lice) aan B(ob) haar publieke sleutel mededeelt, vervangt C(harlie) die publieke sleutel door zijn eigen publieke sleutel. B(ob) denkt met A(lice) te communiceren, maar communiceert met C(harlie), die aldus wellicht vertrouwelijke gegevens van B(ob) verkrijgt.

---

<sup>5</sup> In de vakliteratuur wordt melding gemaakt van aanvallen op de betrouwbaarheid van hashwaarden. Zo af en toe sneuvelt een hashtechniek omdat er met botte rekenkracht toch een tweede bericht wordt gevonden waar de hash ook op past; zie Wikipedia (Engelse versie) onder hashcollisions.

### *3f. Vervanging en kosten van sleutelparen*

Als een gevolg van de voortdurend toenemende computerkracht geldt thans als richtsnoer dat sleutelparen na zeven jaar moeten worden vervangen. Zonder deze ingreep zouden de vaste sleutelparen niet meer geheim blijven. Later wordt nog terug gekomen op het mogelijke probleem dat dit kan vormen in verband met de duurzaamheid van de elektronische ondertekening. Een nieuw sleutelpaar kost minimaal EUR 100 per jaar.

### *3g. Vraag over procuratie*

De omstandigheid dat A(lice) haar sleutelpaar aan een secretariaat ter beschikking kan stellen, riep de vraag op of en hoe er bij PKI systemen van elektronische ondertekening iets is geregeld over procuratie. Die vraag kan ontkennend worden beantwoord evenals bij de fysieke ondertekening.

## **4. Uit en naar aanleiding van de inleiding van A.I.M. van Mierlo**

### *4a. Wat wordt gerealiseerd met de fysieke ondertekening?*

Aangezien wij geneigd zijn de elektronische ondertekening te bezien vanuit het perspectief van de fysieke ondertekening, wordt eerst aandacht gevraagd voor de fysieke ondertekening. Wat wordt daarmee gerealiseerd?

a) Dwingende bewijskracht, art. 157 Rv.

b) De heldere regel van bewijslastverdeling van art. 159 lid 2 Rv: wanneer de beweerde ondertekenaar de fysieke ondertekening stellig ontkent, dan draagt de wederpartij de bewijslast voor het tegendeel.

c) Wanneer een regelgeving een ondertekening als constitutief vereiste vergt, dan wordt met een fysieke ondertekening *altijd* aan dit vereiste voldaan.

*4b. HR 5-10-2012, ECLI:NL:HR:2012: BV6698, JBPr 2013/6 (H.W. Wiersma) en Rb. Amsterdam, 31-12-2013; ECLI:NL:RBAMS:2013:9381*

De Hoge Raad voorzag hier de rechtspraktijk van de welkome oplossing dat een geparafeerd geschrift kan gelden als een ondertekend geschrift "indien de paraaf de desbetreffende persoon in voldoende mate individualiseert."; rov. 3.4. Men zou hieruit kunnen afleiden dat het individualiserende vermogen van paraaf en ondertekening op één lijn staan.

In de zaak voor Rb. Amsterdam van 31-12-2013 ging het om een verstekvonnis dat niet was ondertekend terwijl de opposant hieruit de conclusie trok dat er dus geen vonnis was gewezen en de zaak op tegenspraak doorliep. Die vlieger ging niet op; de rechter gaf het, toch bij te vallen, oordeel dat het hier ging om een fout die zich, in de termen van art. 31 lid 1 Rv, voor eenvoudig herstel leent. Daarnaast speelt de vraag wat er gebeurt als een elektronische ondertekening niet voldoet. Valt dit eveneens onder het bereik van art. 31 Rv? In dat geval is de uitspraak relevant van de Raad van State van 11-12-2013.

*4c. Raad van State 11-12-2013, ECLI:NL:RVS:2013:2374: vereiste van ondertekening in art.6:5, aanhef, Awb ziet op een fysieke handtekening*

Een hogerberoepschrift van Gedeputeerde Staten is niet fysiek ondertekend maar bevat aan de voet de volgende tekst: "Gedeputeerde Staten van Zuid-Holland, voor dezen, mw. drs. J.A. Hilgersom, secretaris. Deze brief is digitaal vastgesteld, hierdoor staat er geen fysieke handtekening in de brief." De Raad van State achtte deze gang van zaken niet in overeenstemming met het vereiste van ondertekening in art.6:5, aanhef, Awb en bood, in overeenstemming met de wettelijke regeling, aan

Gedeputeerde Staten de mogelijkheid tot herstel. Van deze mogelijkheid werd gebruik gemaakt door het uitbrengen van een .. (vrijwel) identiek hogerberoepschrift.

Het laat zich raden dat Gedeputeerde Staten alsnog niet-ontvankelijk werden verklaard. Dit motiveert de Raad van State in rov. 1.5 als volgt:" Het in artikel 6:2, aanhef, van de Awb neergelegde vereiste dat het beroepschrift is ondertekend, ziet op een fysieke handtekening. Dit vereiste is gesteld opdat duidelijk is wie het beroep heeft ingesteld en of dit de daartoe bevoegde persoon of functionaris is. Dit geldt ingevolge artikel 6:24 ook voor het hogerberoepschrift."

#### *4d. Art. 3:15a lid 4 BW; van toevoegende waarde?*

Artikel 3:15a lid 4 BW:" Onder elektronische handtekening wordt een handtekening verstaan die bestaat uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authenticatie."

Het is de vraag of de wetgever, of beter de Europese regelgever, hier een gelukkige hand heeft gehad. Het kwam al in de uitnodiging tot deze bijeenkomst naar voren dat deze tekst zodanig ruim is uitgevallen dat daaronder ook berichten kunnen vallen die in de verste verte geen waarborg bevatten die men met de term hand- of ondertekening in verband brengt; zoals bijvoorbeeld een verklaring van A(lice) aan B(ob) omtrent hetgeen een derde zou hebben verklaard.

Dondorp heeft er in zijn inleiding op gewezen dat er talloze berichten in het elektronisch verkeer zijn die niet met dergelijke waarborgen omgeven hoeven te zijn. Maar dan is het de vraag of er nog wel van een hand- of ondertekening gesproken moet worden.

Wellicht zou men dit lid 4 beter met de volgende, gecuriveerde, toevoeging kunnen lezen:" Onder elektronische handtekening *kan onder omstandigheden* een handtekening worden verstaan die bestaat uit elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authenticatie."

#### *4e. De dubbel versleutelde PKI ondertekening*

Met behulp van de hashwaarde van het bericht en een asymmetrisch sleutelpaar wordt de elektronische ondertekening gerealiseerd.

De elektronische ondertekening bestaat derhalve uit de door A(lice) dubbel versleutelde hashwaarde van het bericht dat door B(ob) dubbel wordt ontsleuteld. B(ob) bepaalt aldus via ontsleuteling een hashwaarde en B(ob) bepaalt zelf de hashwaarde van het onversleutelde bericht en constateert - als het goed is - overeenstemming, ofwel match.

Dondorp merkt hierbij op dat dit zeker juist is, maar ook de eerder getoonde enkele versleuteling wordt aangemerkt als PKI ondertekening. Bij de dubbele versleuteling kan slechts de specifieke ontvanger het bericht openen, hetgeen vaak in het privaatrechtelijke berichtenverkeer is geboden. Maar het kan zich ook voordoen, zoals vaak in het bestuursrecht of bij een ondertekend besluit op een website, dat de ondertekening strekt ten behoeve van een veelheid van personen, in welk geval de enkele versleuteling gebruikt kan worden.

#### *4f. De inhouds- en waarborgvereisten van art. 3:15a lid 2 sub a/d BW*

- a. zij [de elektronische ondertekening] is op unieke wijze aan de ondertekenaar verbonden;
- b. zij maakt het mogelijk de ondertekenaar te identificeren;
- c. zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
- d. zij is op zodanige wijze aan het elektronische bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord;

In het verlengde van sub d zou men kunnen preciseren dat het door de elektronische ondertekening gegenereerde (bewijs)materiaal tot de verificatie in staat stelt.

#### *4g. De vijf essenties van ondertekening*

De vijf vereisten van een ondertekening zijn erop gericht dat de ondertekenaar aan het te ondertekenen bericht een bewijsbestemming geeft. Hieronder zijn die vereisten op een rij gezet met daarachter de corresponderende passages uit art. 3:15a lid 2 sub a/d BW. De ondertekenaar geeft de bewijsbestemming door:

- 1) ten behoeve van de geadresseerde*
- 2) een identificerende toevoeging aanbrengt, te weten een toevoeging (sub a en b)*
- 3) die slechts door de ondertekenaar bij dit bericht kan zijn aangebracht (sub c)*
- 4) en die in al deze opzichten door een niet bij de ondertekening betrokken derde (deskundige) kan worden geverifieerd (sub d)*
- 5) aan de hand van het ondertekende materiaal plus de ondertekening (sub d).*

#### *4h. Zwakte van PKI systemen wat betreft essenties 2 en 3, sub a, b en c*

A(lice) brengt geen identificerende toevoeging aan die slechts door A(lice) bij dit bericht kan zijn aangebracht, want velen kunnen een hashwaarde bepalen. Hier zien wij als het ware zich de twee valkuilen aftekenen van nabootsbaarheid en gebrek aan persoonsgebondenheid: een ander dan A(lice) kan het bericht hebben verzonden en een ander dan A(lice) kan de hashwaarde hebben bepaald. Het kwam bij de inleiding van Dondorp al aan de orde dat de privé sleutel van A(lice) zeer wel door een ander kan zijn gebruikt.

#### *4i. Zwakte van PKI systemen wat betreft de afwezigheid van bewijsmateriaal en de verificatie; essenties 4 en 5; sub d*

Wat een moeilijk te overkomen bezwaar lijkt van de PKI elektronische ondertekeningen is dat deze *geen bewijsmateriaal* genereren. De elektronische ondertekening is hier een enkel of dubbel versleutelde hashwaarde, maar na de ontsleuteling, onder meer ten behoeve van de match, blijft er .. niets aan bewijsmateriaal over. Dat 'bewijsmateriaal' bestaat immers louter uit een hashwaarde. Bij een conflict tussen A(lice) en B(ob) over de vraag welke versie van het ondertekende bericht de juiste is, kunnen A(lice) en B(ob) in beginsel met evenveel recht beweren dat de door de ander voorgehouden versie niet de juiste is. Een regel van bewijslastverdeling, laat staan een heldere regel zoals die van art. 159 lid 2 Rv, ontbreekt en kan zelfs niet anders dan ontbreken bij afwezigheid van door de ondertekening gegenereerd bewijsmateriaal. Men kan zeggen dat de PKI elektronische ondertekening als het ware verdampt doordat deze geen bewijsmateriaal genereert. Zou hier niet iets op moeten worden bedacht?

### **5. Uit en naar aanleiding van de inleiding van G.J. Meijer**

#### *5a. Modernisering van het arbitragerecht met onder meer voorzieningen voor elektronische communicatie*

Op 3 juni 2014 aanvaardde de Eerste Kamer het per 1 januari 2015 in werking te treden wetsvoorstel 33641 "tot modernisering van het Arbitragerecht". In dit wetsvoorstel is een aparte bepaling, art. 1072b Rv, opgenomen over elektronische communicatie. Artikel 1072b Rv beschrijft uitvoerig de mogelijke elektronische communicatie tijdens arbitrage. Het artikel geeft een goed beeld over de wijze van en de randvoorwaarden bij elektronische communicatie. In het kader van de expertmeeting ligt de nadruk op art. 1072b lid 3 Rv dat de vereisten van de elektronische ondertekening regelt.

#### *5b. Artikel 1072b leden 1 en 5 Rv; verzendtheorie*

Lid 1 beschrijft hoe omgegaan kan en moet worden met arbiters die niet elektronisch kunnen of willen communiceren. Daarnaast wordt bepaald gedurende welke tijdspanne de elektronische communicatie mag en kan plaatsvinden. Belangrijk is het verschil met art. 33 Rv, te weten dat de instemming met bereikbaarheid langs elektronische weg voor de duur van het geding niet eenzijdig kan worden ingetrokken, dit om te voorkomen dat een partij zich halverwege de procedure eenzijdig elektronische minder of niet meer beschikbaar kan maken.

Lid 5 behandelt het tijdstip waarop een verzending van een elektronisch bericht of stuk heeft plaatsgevonden. Uitgegaan wordt van het moment dat de ontvanger het bericht in zijn systeem heeft ontvangen, te weten "het tijdstip waarop het bericht een systeem voor gegevensverwerking heeft bereikt waarvoor de verzender geen verantwoordelijkheid draagt."

#### *5c. Bescheiden, met inbegrip van elektronische bescheiden, in art. 1072b lid 2 Rv; E-discovery*

Artikel 1072b lid 2 Rv: "Onder bescheiden als bedoeld in deze titel worden mede verstaan op een gegevensdrager aangebrachte gegevens, alsmede langs elektronische weg ingediende gegevens." Het nieuwe art. 1072b lid 2 Rv opent tevens de weg naar overeenkomstige elektronische toepassing van het inzage-recht van de art. 843a en 843b Rv in arbitrale gedingvoering; welke toepassingen ook dikwijls met de Engelse termen discovery en disclosure worden aangeduid. De wettekst zelf is hierover niet erg uitgeproken, maar de toelichting - 33611, nr. 3, 2012-2013, blz. 42 - verwijst uitdrukkelijk naar de art. 843a en 843b Rv.

Wat 'gegevensdragers' betreft worden daaronder in de toelichting tevens de elektronische opslag op tapes, floppy's, harddisks, audio- en videobanden verstaan en vallen hier tevens processtukken onder die bijvoorbeeld als word- of pdf-bestand per email worden verzonden.

#### *5d. Nieuw art. 1072b lid 4 Rv over E-Conferencing*

De in lid 4 geopende mogelijkheid om het arbitrale geding volledig elektronisch te doen plaatsvinden, bijvoorbeeld met behulp van videoconferenties of skype, is al gebruikelijk, realiseert al, zeker in internationale arbitrages, veel besparingen en deze tendens zal zich met de nieuwe wetgeving voortzetten.

Reactie A.I.M. van Mierlo: zou het niet aanbeveling verdienen deze elektronische mogelijkheden ook toe te passen op het getuigenverhoor bij de gewone rechter?

Riposte van de heer W. Waslander: in Limburg maakt men hiervan al gebruik.

#### *5e. Nieuw art. 1072b lid 3 Rv over de elektronische ondertekening van een arbitrale vonnis; gekwalificeerde elektronische ondertekening*

Nieuw art. 1072b lid 3 Rv: "Het vonnis als bedoeld in artikel 1057, tweede lid, kan ook in elektronische vorm worden opgemaakt door het te voorzien van een elektronische handtekening die voldoet aan het bepaalde in artikel 15a, eerste en tweede lid van Boek 3 van het Burgerlijk Wetboek." Een elektronische ondertekening die voldoet aan de in het voorgaande besproken waarborg- en inhoudelijke vereisten van art. 3:15a lid 2 sub a/d BW wordt aangemerkt als een geavanceerde elektronische ondertekening. Wordt daarbij tevens voldaan aan de op de Telecommunicatiewet gebaseerde (bedrijfs)organisatorische vereisten van art. 3:15a lid 2 sub e en f BW, dan is sprake van een gekwalificeerde elektronische ondertekening, zoals wordt vereist door art. 1072b lid 3 Rv. Aan deze vereisten sub e en f wordt hier verder voorbij gegaan.

#### *5f. Maatschappelijke behoefte aan een elektronische ondertekening onder een al dan niet elektronisch tot stand gekomen arbitraal vonnis*

Een elektronische ondertekening onder een al dan niet elektronisch tot stand gekomen arbitraal vonnis zou in een grote behoefte voorzien, vooral in internationale arbitrage, bijvoorbeeld met arbiters uit



Seoel, Madrid en Amsterdam. In de huidige praktijk moet het arbitrale vonnis naar deze drie steden worden gevlogen om een fysieke ondertekening aan te brengen, of wordt ook wel gewacht tot deze drie arbiters in elkaars fysieke nabijheid zijn. Een gekwalificeerde elektronische ondertekening zou hier derhalve een substantiële bijdrage kunnen leveren in de zin van snellere afhandeling en lagere kosten.

*5g. Komen gangbare PKI systemen in aanmerking voor de elektronische ondertekening van een arbitraal vonnis?*

Elektronische ondertekeningen volgens gangbare PKI procédés lijken niet in aanmerking te kunnen komen als elektronische ondertekening van een arbitraal vonnis.

In de inleiding van Van Mierlo kwam naar voren dat met de ontsluiting van het bericht dat de arbiters elektronische hebben ondertekend, het bewijsmateriaal hierover verdwijnt, verdampt. Een degelijke verdamping verdraagt zich niet met art. 1072b lid 3 Rv.

Daarnaast worden de PKI sleutels na zeven jaar vervangen. Dat verdraagt zich niet met het duurzaamheidsvereiste van 20 jaar van een rechterlijk of arbitraal vonnis, waarvan de bevoegdheid tot tenuitvoerlegging krachtens art. 3:324 lid 1 BW pas na 20 jaar verjaart.

Ten derde verdraagt de, hierna nog nader toe te lichten, ratio van het ondertekeningsvereiste van art. 1072b lid 3 Rv zich niet met het gegeven dat ook anderen dan de verzender A(lice) op betrekkelijk eenvoudige wijze, en zelfs gelijktijdig met A(lice), van de privé sleutel van A(lice) gebruik kunnen maken.

*5h. Ratio en belang van het vereiste van elektronische ondertekening van art. 1072b lid 3 Rv*

De belangrijkste door de ondertekening van het arbitrale vonnis veilig gestelde waarborg is om ervan verzekerd te zijn dat *alle* arbiters hebben geparticipeerd in de totstandkoming van het arbitrale vonnis. Zij geven met deze ondertekening *allen* te kennen dat zij voor hun rekening nemen dat het arbitrale vonnis van hen afkomstig is.

Mocht een ondertekening ontbreken dan is hier beslist geen sprake van een "andere kennelijke fout die zich voor eenvoudig herstel leent", zoals art. 31 lid 1 Rv onder woorden brengt, en die in de nieuwe versie van art. 1060 lid 1 Rv vatbaar zou zijn voor verbetering zoals dit door art. 1060 Rv wordt voorgeschreven. Bij ontstentenis van ondertekening van een arbitraal vonnis dat aan partijen is verzonden, zal het in dit opzicht niet ondertekende arbitrale vonnis om die reden onherstelbaar vernietigbaar zijn; zie (Güris/Bursa, HR 5 december 2008, ECLI:NL:HR:2008:BF3799, JBP 2009/2 (H.W. Wiersma)).

*5i. Het 'gewaarmerkte afschrift' van art. 1062 lid 2 Rv*

Het lijkt erop dat de (uitvoerings)wetgever nog aandacht moet besteden aan de elektronische realisering van het gewaarmerkt afschrift van de door de griffier op het arbitrale vonnis aangebrachte en ondertekende exequatur-verklaring krachtens art. 1062 lid 2 Rv. Op voorhand lijkt niet duidelijk hoe de gang van zaken is en de wetgever raadt aan om dan maar een printje te maken; zie TK 33611, nr. 6, 2013/2014, p. 13.

Bij een 'echte' elektronische ondertekening, dus die welke voldoet aan de waarborg- en inhoudelijke vereisten van art. 3:15a lid 2 sub a/d BW, zou dit printje niet nodig behoeven te zijn: de griffier mailt het naar hem gezonden elektronisch ondertekend arbitrale vonnis naar zichzelf, zendt dit door naar partijen, tekent in de begeleidende tekst aan dat dit exequatur-verlof is verleend en ondertekent met een 'echte' elektronische ondertekening dit verlof.

## **6. Discussie- en vraagpunten; bezwaren en oplossingsrichtingen of antwoordindicaties; twijfelpunten en stellingen**

Naar aanleiding van de inleidingen ontstaat een gesprek over de volgende onderwerpen:

- kan net als bij de fysieke ondertekening elektronisch met een stempel en bij volmacht worden

ondertekend?

- de veiligheidsvereisten bij een elektronische ondertekening;
- de duurzaamheid van de elektronische ondertekening en de ondertekende documenten met het oog op latere raadpleging en verificatie;
- de verdamping van het bewijsmateriaal bij het gebruik van PKI-sleutels.

#### *6a. Vragen over elektronisch ondertekenen per stempel en bij volmacht*

Wellicht zou ondertekenen met elektronische stempels mogelijk kunnen zijn met vaste sleutelparen. Maar dan moet wel duidelijk zijn dat diegeen namens wie wordt ondertekend, daarmee akkoord is. Indien de elektronische ondertekening moet voldoen aan de waarborg vereisten van art. 3:15a lid 2 BW, dan is een 'elektronische stempelondertekening' waarschijnlijk niet mogelijk door die vereisten zelf.

Een volmacht lijkt daarentegen bij elektronische ondertekeningen die voldoen aan de waarborg vereisten van art. 3:15a lid 2 BW, niet op problemen te hoeven stuiten. Aan de elektronische ondertekening door de gevolmachtigde namens de volmachtgever voegt de gevolmachtigde de elektronisch ondertekende volmachtverlening toe waardoor de wederpartij de beschikking krijgt over sluitend bewijsmateriaal van de volmachtverlening.

Bij de PKI systemen is dit niet mogelijk omdat de gevolmachtigde niet de beschikking krijgt over bewijsmateriaal en dit dus ook niet kan doorsturen.

#### *6b. Aanbevelingen over veiligheidsniveau*

Op dit moment blijkt er nog weinig inzicht te bestaan in de vereiste veiligheidsniveau's. Dondorp heeft in zijn inleiding aangegeven dat het veiligheidsniveau situationeel is gebonden. Het lijkt daarom van belang nader onderzoek hiernaar te doen. Het veiligheidsniveau kan soms ingegeven zijn door wetgeving, zoals nu bij arbitrage, door de aanwezigheid van ander bewijsmateriaal en het kan ook per rechtsgebied anders liggen. Een paar voorbeelden doken op.

- Soms in een elektronische ondertekening zo laagdrempelig dat die zich niet kan meten met een fysieke ondertekening; zoals bijvoorbeeld bij een pinbetaling.
- Het veiligheidsniveau wordt niet alleen door de techniek bepaald maar ook door organisatorische en procedurele randvoorwaarden; denk bijvoorbeeld aan secretariaten waar 'in opdracht' wordt getekend en die te achteloos met gegevens omgaan, of aan gebruikers die soms te gemakkelijk hun pincode of sleutels aan anderen ter beschikking stellen. Het is dan ook van belang vast te stellen dat bij een elektronische ondertekening die voldoet aan de waarborg vereisten van art. 3:15a lid 2 BW wat makkelijker een volmacht gegeven kan worden zonder dat dit tot generiek gebruik of misbruik kan leiden.
- Zou er bij bepaalde organisatorische en procedurele randvoorwaarden niet toch plaats kunnen zijn voor het rechtsvermoeden dat het gebruik van de sleutel van A(lice) op een activiteit van A(lice) duidt? Probleem bij deze vaststelling is natuurlijk de mate van slordigheid die in zo'n setting kan ontstaan.
- Een ander aspect van procedurele aard speelt in het privaatrecht waar bewijsovereenkomsten en algemene voorwaarden het veiligheidsniveau kunnen aangeven, terwijl dat in het bestuursrecht vaak weer anders ligt.

#### *6c. Duurzaamheid van raadpleging of verificatie bij vernieuwing van een bestandsformat*

Bij de opslag van elektronische documenten en elektronische ondertekening met PKI-sleutels zijn er twee vragen die inwerken op de duurzaamheid van het document en zijn elektronische ondertekening.

a) Hoe wordt omgegaan met de conversie van de inhoud van het document zelf?

b) En hoe wordt omgegaan met de verdamping van de elektronische ondertekening door: 1) vernieuwing van een bestandsformat?; zoals bijvoorbeeld viel te zien bij de omzetting van WP naar Word?; 2) vernieuwing van sleutels?

Dondorp doet een suggestie naar aanleiding van de Archiefwet 2009. Volgens deze wet kan worden vastgelegd wie de elektronische handtekening heeft gezet zonder de handtekening op te slaan. Daarvoor heeft de wet een procedure. Veel van de aanwezigen vinden dit ontoereikend omdat het genereren van bewijsmateriaal bij ondertekening de kern is. De oorspronkelijke ondertekening en de mogelijkheid om die te verifiëren maken daarvan onverbreekbaar deel uit. Voor de wijziging van het bestandsformat werden diverse technieken geopperd zoals: vertalen; emulatie; conversie; substitutie; dit alles door of althans ten overstaan van een derde/ deskundige wordt gedaan.

In het algemeen werd opgemerkt dat de technieken voor ICT en PKI zeer innovatief gericht zijn en daarmee op gespannen voet staan met begrippen als duurzame raadpleegbaarheid, duurzame archivering en duurzame verificatie.

Deze vragen en samenhangende problemen zijn nog zo nieuw dat er ook in Europees verband gestudeerd wordt op oplossingen.

#### *6d. Verdamping van bewijsmateriaal bij elektronische ondertekeningen volgens gangbare PKI procédés*

Als bij de elektronische ondertekening met PKI sleutels bewijsmateriaal voor de elektronische ondertekening van dat document door A(lice) ontbreekt, roept dat veel vragen op.

- A(lice) beschikt toch nog altijd over het *brondocument* als bewijsmateriaal?

Of hetgeen verzender A(lice) presenteert als brondocument, inderdaad het brondocument is, kan misschien wel circumstantieel worden vastgesteld maar wat hier als elektronische ondertekening geldt, te weten (dubbele) versleuteling van hahswaarde, leveret hiervoor geen bewijsmateriaal. Dat geldt niet alleen voor een origineel maar tevens voor een per abuis verkeerd opgestuurde en op deze wijze elektronisch ondertekende versie.

- B(ob) ging toch bij de opening van het ondertekende bericht, te weten bij de, enkele of dubbele, ontsleuteling van de hahswaarde van het bericht, akkoord met de inhoud? Hoe en waarom gaat B(ob) dan later dit bericht betwisten?

Wat voor A(lice) en B(ob) ook de overwegingen zijn om te betwisten wat er verstuurd dan wel ontvangen is, belangrijk is dat zij beiden weten dat geen (substantieel) bewijsmateriaal werd gegenereerd bij wat zij als elektronische ondertekening aanmerkten, waardoor zij de gelegenheid en ruimte hebben om hun 'eigen' versie als de juiste voor te houden.

-Is er niet vast te stellen wat het *origineel* verstuurd bericht is? Dat moet toch zijn te achterhalen? Het onderscheid tussen 'origineel' en 'kopie' bestaat, elektronisch bezien niet. Hoogstens is er sprake van 'versies'. Er valt geen origineel te traceren. Dat bemoeilijkt ook de verificatie.

## **7. Enkele bevindingen en eerste afsluiting**

### *7a. Enkele bevindingen*

\* De term elektronische/ digitale hand-/ ondertekening is ambivalent: duidt deze op de vertrouwde waarborgen van art. 3:15a lid 2 BW, laat men deze waarborgen met een beroep op lid 4 varen of koerst men 'ergens' in het midden?

\* De gangbare PKI systemen voldoen niet aan de waarborg vereisten van art. 3:15a lid 2 BW maar zitten zij niet 'ergens' in het midden en hoe valt dit nader te bepalen?

\* Een nader in kaart brengen lijkt gewenst van regelgeving waarin elektronische ondertekening als mogelijkheid open staat teneinde te bepalen of, dan wel in welke mate, moet worden vastgehouden aan de waarborg vereisten van art. 3:15a lid 2 BW.

\* Een systeem van elektronische ondertekening dat op gebruikersvriendelijke en redelijk goedkope wijze zou voldoen aan de waarborg vereisten van art. 3:15a lid 2 BW lijkt vooralsnog het meest aanbevelenswaardig.

#### *7b. Eerste afsluiting*

Het gegeven dat de gehele expertmeeting werd opgenomen, gaf de dagvoorzitter een speculatie in hoe later op deze bijeenkomst zou worden terug gekeken maar hij was er redelijk van overtuigd dat er in ieder geval met stevige inzet en kundigheid was gesproken, gedebatteerd en nagedacht; waarvoor hij de desbetreffenden gaarne dank zegde en hen graag uitnodigde voor een drankje en een hapje na afloop.

### **8. Enkele nabeschouwingen**

#### *8a. Het streven naar een technologie neutrale regelgeving*

Het contrast tussen de waarborg vereisten van art. 3:15a lid 2 BW en de volstrekte afwezigheid daarvan in lid 4 wordt enigszins verklaarbaar als men kijkt naar de totstandkoming van Richtlijn 1999/93/EG; welke totstandkoming helder uiteen wordt gezet de monografie van Lodder, Dumortier en Bol<sup>6</sup>.

Enerzijds wilde men voorkomen dat in de lidstaten onderling uiteenlopende regelingen zouden ontstaan over elektronisch berichtenverkeer en elektronische ondertekeningen, zoals al het geval was met de van 1997 daterende Italiaanse Legge Bassanini en de Duitse Signaturgesetz. Daarnaast kon men, met voorbijgaan aan eventuele verschillen in regelgevingen omtrent fysieke ondertekening, het goed eens worden over de in art. 3:15a lid 2 BW lid 2 geformuleerde waarborg vereisten die een dermate hoog beschermingsniveau garanderen dat aan alle eventueel in de lidstaten bestaande vereisten van fysieke ondertekening werd voldaan. Aldus kon in dit lid 2 worden afgekoerst op een pendant van de fysieke ondertekening.

Een bijkomend element in deze benadering was dat van de techniekonafhankelijke of technologie-neutrale regelgeving. De toepasselijkheid van de Richtlijn hangt, anders dan voormelde Italiaanse en Duitse wet uit 1997, niet af van de gebruikte technologie of methode van elektronische ondertekening. En daarmee werd tevens voorkomen dat een voorgeschreven technologie neutrale achterhaald zou raken.

Anderzijds kon en wilde men niet voorbijgaan aan de realiteit van de gangbare, niet aan de waarborg vereisten van art. 3:15a lid 2 BW tegemoetkomende, PKI systemen die ook wel werden en worden aangeduid als digitale ondertekeningen. Daarvoor werd dan de ruimte gevonden in lid 4. Nu kan men zich afvragen of deze ruimte zo royaal moest uitvallen als is gebeurd maar buiten twijfel staat in ieder geval dat de PKI systemen een zeker bestaansrecht hebben.

#### *8b Verificatie problemen bij de PKI systemen*

Dit bestaansrecht van de PKI systemen staat er evenwel niet aan in de weg dat zij op het gebied van verificatie tekortschieten; welk aspect niet erg bij de expertmeeting naar voren is gekomen. Bij, voortgezette, betwisting van een fysieke ondertekening plegen partijen een onafhankelijke externe deskundige, een grafoloog, in te schakelen. Deze externe deskundige was niet bij de ondertekening betrokken en kan zelf ook weer worden gecontroleerd met een contra expertise; hij pleegt dan ook te

---

<sup>6</sup> Het recht rond elektronische handtekeningen: Richtlijn 1999/03/EG en de omzetting in België en Nederland door Arno R. Lodder, Jos Dumortier en Stephanie H. Bol, Kluwer/ Deventer 2005; nr. 1.3.

worden geloofd door de rechter.<sup>7</sup>

Iets soortgelijks is niet mogelijk bij de PKI systemen. De sleutelbeheerder/ CSP staat als leverancier van sleutelparen in een klant-afnemer relatie tot A(lice) of B(ob) en beschikt evenmin als A(lice) of B(ob) over bewijsmateriaal. Het enige wat de CSP kan doen is op meer of minder plausibele wijze bevestigen of A(lice) inderdaad de rechthebbende van het gebruikte sleutelpaar is.

#### *8c. Gelijktelling elektronisch en fysiek ondertekend document; elektronische ingebrekestelling?*

Martius - a.w. (zie noot 3) bijvoorbeeld op p. 182 - verbindt aan de term technologie-neutraal de, mij aansprekende, lading dat het dan gaat om regelgeving "waarbij het uitgangspunt is dat dezelfde functies op een gelijkwaardige wijze langs schriftelijke en elektronische wijze vervuld kunnen worden." Het lijkt ongetwijfeld efficiency in algemene zin te bevorderen wanneer digitale en schriftelijke documenten als aan elkaar gelijkgesteld kunnen gelden. Maar dikwijls, niet altijd, is dan noodzakelijk dat de elektronische ondertekening voldoet aan de eisen van art. 3:15a lid 2 BW; zoals reeds in nr. 1 aan de orde kwam bij het attenderen op par. 126a BGB

Nochtans kleeft hieraan naar Duits recht wel de beperking dat deze bepaling niet geldt, en deze volledige gelijkstelling dus niet plaatsvindt, wanneer er geen expliciet wettelijk schriftelijkheidsvereiste is; zie Martius a.w. noot 623.

Iets soortgelijks geldt bij ons voor wat betreft de in art. 7:932 lid 1 BW geregelde elektronische polis. In dit lid 1 wordt immers uitdrukkelijk naar art. 156a Rv verwezen en volgens deze bepaling moet de wederpartij ten gunste van wie de 2 onderhandse akte is bestemd, uitdrukkelijk met de elektronische weg moet instemmen; welk instemmingsvereiste natuurlijk niet geldt voor de papieren weg.

Het voorgaande staat er verder niet aan in de weg dat Martius t.a.p. tot de algemene conclusie komt dat een elektronische ondertekening die voldoet aan de eisen van art. 3:15a lid 2 BW naar Duits recht ingevolge par. 371a ZPO vrijwel gelijkgesteld is aan een papieren akte.<sup>8</sup>

Tenslotte wil ik in deze nabeschouwingen nog enige aandacht besteden aan de in art. 6:82 BW geregelde ingebrekestelling. Sterke papieren heeft, naar ik vrees, de opvatting van Martius - a.w. p. 231 - dat de schriftelijk voorgeschreven ingebrekestelling niet langs elektronische weg mogelijk is. Men kan zeggen - Martius laat zich hierover overigens niet uit - dat de ingebrekestelling geheel buiten het bereik valt van art. 6: 227a BW dat slechts betrekking heeft op elektronisch tot stand gekomen overeenkomsten. En men zou ook kunnen zeggen dat de - papieren - ingebrekestelling geen akte is omdat de ondertekenaar hiermee geen bewijs *tegen* zichzelf schept.

Ik zou menen dat dit laatste te dogmatisch is gedacht. Wanneer de wet voorschrijft dat iemand ten gunste - althans mede ten gunste - van zichzelf een document moet opstellen en versturen, dan zou ik het ervoor willen houden dat een dergelijk document als het is ondertekend, door wetsduiding als een akte moet worden beschouwd die mede ten gunste van de ondertekenaar dwingende bewijskracht heeft. En daarmee valt dit document dan binnen het bereik van de elektronische onderhandse akte van art. 156a Rv en kan het dus, naar mijn mening: met inachtneming van de waarborg vereisten van art. 3:15a lid 2 BW, elektronisch tot stand komen.

### **9. Drie kanttekeningen bij KEI**

---

<sup>7</sup> In NJB 2010/ p.430 e.v. trekt Merkelbach de gereputeerdheid van de grafoloog ernstig in twijfel maar Merkelbach is in NJB 2010/ p. 2537 e.v., op m.i. overtuigende wijze, bestreden door Stoel, Berger, van den Heuvel en Fagel.

<sup>8</sup> Zie Martius nr. 5.4.2 die daarbij verwijst naar A. Rosznagel en S. Fischer-Dieskau, 'Elektronische Dokumente als Beweismittel - Neufassung der Beweisregelungen durch das Justizkommunikationsgesetz', NJW 2006/12, p.808.

De memorie van toelichting op wetsvoorstel 34059/ project KEI gaat onder nr. 12.3 in op de elektronische ondertekening met als opschrift: Integriteit, authenticiteit en het vereiste van ondertekening.

De kernbepaling hierover is art. 30c Rv waar de elektronische indiening van processtukken is geregeld en waar het begrip elektronische ondertekening aan de orde komt; bijgaande noot bevat de hier van belang zijnde passages van art. 30c.<sup>9</sup>

*9a. Kanttekening 1: waarom art. 3:15a BW niet tot model genomen?*

Om te beginnen vind ik het bevreemdend dat het model van het in 2003 in werking getreden art. 3:15a BW waarin Richtlijn 1999/93/EG werd geïmplementeerd, in KEI zo buiten beeld is gebleven. De inhoudsloze wettelijke omschrijving in art. 30c lid 3 van een elektronische ondertekening lijkt weliswaar als twee druppels water op het hierboven veelvuldig aan de orde gekomen art. 3:15a lid 4 BW maar er is toch verschil. Artikel 30c lid 3 is contextloos terwijl art. 3:15a lid 4 BW door het contrast met art. 3:15a lid 2 BW het duidelijke signaal afgeeft dat de waarborg vereisten van art. 3:15a lid 2 BW veruit de voorkeur verdienen; in Europa. Op een uitwerking hiervan hoop ik in een vervolg-publicatie spoedig terug te komen, maar ik kan niet nalaten te ventileren dat deze benadering niet Europa-breed het vertrouwen zal bevorderen dat Nederland met loyale naleving van de Europese richtlijnen zich inzet voor een optimum van efficiënte rechtspraak *en* met royale waarborgen omklede rechtspraak.

Wat zou erop tegen zijn geweest om art. 3:15a BW in zijn geheel op te nemen daarnaar te verwijzen?

*9b. Kanttekening 2: essenties van (elektronische) ondertekening volgens de memorie*

In het verlengde hiervan liggen mijn vraagtekens bij de volgens de memorie van toelichting in acht te nemen essenties, aldaar omschreven als: functies, van (elektronische) ondertekening. Ik citeer

---

<sup>9</sup> Artikel 30c

1. De eiser of verzoeker dient de procesinleiding langs elektronische weg in bij de rechter. Partijen dienen gedurende de procedure ook overige stukken langs elektronische weg in, tenzij de rechter anders bepaalt.

Anderen dan partijen, die bij de procedure worden betrokken, dienen stukken langs elektronische weg in, tenzij de wet of de rechter anders bepaalt.

2. Waar deze wet voorschrijft dat handelingen schriftelijk geschieden wordt hieraan langs elektronische weg voldaan, tenzij de wet of de rechter anders bepaalt.

3. Onder een elektronische handtekening wordt verstaan een handtekening die bestaat uit elektronische gegevens die gehecht zijn aan of logisch verbonden zijn met andere elektronische gegevens en die worden gebruikt door de ondertekenaar om te ondertekenen. Waar in deze wet ondertekening is voorgeschreven, is aan dit vereiste voldaan indien het stuk is ondertekend met een elektronische handtekening die voldoet aan bij of krachtens algemene maatregel van bestuur te stellen eisen. Een stuk dat langs elektronische weg is ingediend in het digitale systeem voor gegevensverwerking van de gerechten geldt als ondertekend.

(...)

7. In afwijking van het voorgaande lid kan de rechter bepalen dat de procedure wordt voortgezet volgens de regels die gelden voor stukkenwisseling op papier.

8. Niet-ontvankelijkverklaring wegens het ten onrechte indienen van een procesinleiding op papier of het buiten beschouwing laten van een stuk omdat het ten onrechte op papier of na afloop van een termijn is ingediend, blijft achterwege indien redelijkerwijs niet kan worden geoordeeld dat de indiener in verzuim is geweest.

tekstueel maar in andere opmaak: (1) de identificatie van de afzender; (2) de blijf van instemming met de inhoud van het bericht; (3) aanvaarding en/of begrip van de rechtsgevolgen; (4) bevestiging van de wilsuiting.

Tussen (2), (3) en (4) zie ik geen, laat staan substantiële, verschillen, maar wel schitteren door afwezigheid de volgende essenties die in het voorgaande aan de orde zijn gekomen:

(a) het element van identificatie van de afzender/ ondertekenaar door middel van een *identificerende toevoeging* aan het te ondertekenen bericht; (b) het element dat de koppeling van deze toevoeging, ofwel de (elektronische) ondertekening aan het te ondertekenen document, er uitsluit over geeft of het te ondertekenen document na (elektronische) ondertekening geen wijziging heeft ondergaan; (c) het element volgens hetwelk de (elektronische) ondertekening in staat zou moeten stellen tot het genereren van bewijsmateriaal, ofwel van verificatie, waardoor een derde (onafhankelijke) deskundige met redelijke zekerheid kan constateren/ verifiëren dat na (elektronische) ondertekening geen wijzigingen in het bericht zijn aangebracht.

*9c. Kanttekening 3: het digitale systeem voor gegevensverwerking van de gerechten als een soort - voorlopig (?) - elektronisch notariaat*

"De integriteit van een document moet vaststaan vanaf het moment dat het wordt ingediend bij de rechtbank."; aldus luidt het eind van de vijfde alinea van de memorie.

Maar er wordt niet gewerkt met het daartoe geëigende middel van een elektronische ondertekening die voldoet aan de waarborg vereisten van art. 3:15a lid 2 BW; hetgeen ook begrijpelijk is omdat een dergelijke elektronische ondertekening vooralsnog niet op grote schaal beschikbaar of gangbaar is.

In dit ontbreken wordt voorzien in art. 30c lid 3 Rv door:

in de eerste zin de omschrijving van art. 3:15a lid 4 BW over te nemen;

in de tweede zin te bepalen dat elektronische ondertekeningen zullen moeten voldoen aan 'bij of krachtens algemene maatregel van bestuur te stellen eisen'; en waarbij de memorie verderop aantekent dat rekening zal worden gehouden met aankomende Europese regelgeving;

in de laatste zin de fictie te hanteren dat wanneer een stuk langs elektronische weg is ingediend in het digitale systeem voor gegevensverwerking van de gerechten, dit stuk geldt als te zijn ondertekend.

Deze aanpak leidt ertoe dat dit digitale systeem voor gegevensverwerking van de gerechten tevens zal gaan functioneren als een soort notariaat dat erop toeziet dat de elektronische indiening en wisseling van stukken correct en regulier verloopt.

Ik zal bepaald niet beweren dat dit tot misstanden zal leiden, temeer waar ik ervan uitga dat de professionele rechtshulpverleners en het administratieve personeel van de gerechten nauwkeurig en consentieus tewerk zullen gaan. Maar op den duur en in zowel structureel als rechtsstatelijk opzicht lijkt mij dit minder gewenst omdat de burger in zijn toegang tot de rechter dan erg afhankelijk wordt van de, naar verwachting niet steeds even toegankelijke en controleerbare, wijze waarop de gerechten hun elektronische administratie inrichten.

Dr. H. W. Wiersma, voormalig senior onderzoeker Universiteit van Amsterdam; adviseur Hill & Ross advocaten; redacteur JBPr