Mr. S.A.K. d'Azevedo[1]

Elektronische handtekeningen in de praktijk

Bb 2020/14

1. Inleiding

Anno nu houden bedrijven zich meer dan ooit bezig met de digitalisering, optimalisatie en verduurzaming van bedrijfsprocessen. Het toenemende gebruik van elektronische handtekeningen past feilloos in deze tendens. De identiteit van een ondertekenaar wordt immers gewaarborgd terwijl tegelijkertijd blijk wordt gegeven van diens instemming met de inhoud van een document. Zo wordt op afstand bewerkstelligd wat hoofdzakelijk met het zetten van een schriftelijke handtekening wordt beoogd.[2] Verder wordt de tijd die met een transactie is gemoeid en de ecologische voetafdruk verkleind. Dit laatste is bijvoorbeeld het geval door het verminderde gebruik van papier en koeriersdiensten (maar uiteraard staat daar wel het verbruik van meer stroom tegenover).

Bedrijven die gebruik willen maken van elektronische handtekeningen lopen vaak tegen uiteenlopende vragen aan. Die hebben onder andere betrekking op de rechtsgevolgen van elektronische handtekeningen (par. 2), (juridische) aandachtspunten bij de selectie van een partij die het gebruik van elektronische handtekeningen mogelijk maakt (par. 3) en de validatie van elektronische handtekeningen (par. 4). In een poging om aan die informatiebehoefte tegemoet te komen, staat dit artikel achtereenvolgens bij deze onderwerpen stil.

2. Typen elektronische handtekeningen en hun rechtsgevolgen

De verschillende typen elektronische handtekeningen en hun rechtsgevolgen worden beschreven in Europese en nationale wetgeving. Beide licht ik hierna kernachtig toe.

2.1 *Europees recht: De eIDAS-verordening*

Op Europees niveau zijn regels over elektronische handtekeningen neergelegd in de eIDAS-verordening.[3] Hierin worden drie elektronische handtekeningen onderscheiden, namelijk (i) de elektronische handtekening, (ii) de geavanceerde elektronische handtekening en (iii) de gekwalificeerde elektronische handtekening.

De *elektronische handtekening* wordt ten behoeve van het onderscheid met de overige handtekeningen ook wel de 'gewone' elektronische handtekening genoemd. Juridisch kwalificeert een handtekening al als zodanig als gegevens in elektronische vorm gehecht zijn aan of logisch zijn verbonden met andere gegevens in elektronische vorm en die door de ondertekenaar gebruikt worden om te ondertekenen.[4] Voorbeelden hiervan zijn de scan van een papieren handtekening en de (getypte) handtekening onderaan een e-mail.

Aan de *geavanceerde elektronische handtekening* worden meer eisen gesteld. Zo moet een dergelijke handtekening (a) op unieke wijze aan de ondertekenaar verbonden zijn, (b) het mogelijk maken om de ondertekenaar te identificeren, (c) tot stand komen met gegevens voor het aanmaken van elektronische handtekeningen die de ondertekenaar, met een hoog vertrouwensniveau, onder zijn uitsluitende controle kan gebruiken en (d) op zodanige wijze aan de ondertekende gegevens verbonden zijn dat elke wijziging van de gegevens achteraf kan worden opgespoord.[5]

Voor de *gekwalificeerde elektronische handtekening* gelden de meeste eisen. In aanvulling op de eisen van de geavanceerde elektronische handtekening, moet dit type handtekening (i) aangemaakt zijn met een gekwalificeerd middel voor het aanmaken van elektronische handtekeningen en (ii) gebaseerd zijn op een gekwalificeerd certificaat voor elektronische handtekeningen.[6] Het gekwalificeerde certificaat moet voorts afgegeven zijn door een gekwalificeerde verlener van vertrouwensdiensten die voldoet aan de eisen van bijlage I van de eIDAS-verordening.[7] Wordt een handtekening gezet die aan al deze vereisten voldoet, dan heeft die handtekening dezelfde rechtsgevolgen als een handgeschreven handtekening en wordt die in alle lidstaten als zodanig erkend.[8]

Aldus is sprake van een drietrapsraket waarbij de gewone elektronische handtekening aan de minste eisen hoeft te voldoen, terwijl aan de gekwalificeerde elektronische handtekening de meeste eisen worden gesteld.

2.2 *Nederlands recht: Artikel 3:15a BW*

Hoewel de eIDAS-verordening op Europees niveau de rechtsgevolgen voor de gekwalificeerde elektronische handtekening dicteert, doet het dat niet voor de overige elektronische handtekeningen. De eIDAS-verordening bepaalt slechts dat het rechtsgevolg van een elektronische handtekening niet ontkend mag worden louter op grond van het feit dat die niet voldoet aan de eisen van een gekwalificeerde elektronische handtekening.[9] De lidstaten moesten daarom zelf invulling geven aan de rechtsgevolgen van de gewone en geavanceerde elektronische handtekening. Het gevolg daarvan is dat de wetgeving hierover per lidstaat verschilt. Met name bij grensoverschrijdende (Europese)

1 Samantha d'Azevedo is advocaat bij Kennedy Van der Laan te Amsterdam.

2 Vgl. R.E. van Esch, *De stellige ontkenning van een elektronische ondertekening*, *TCR* 2019/4, par. 2.

3 Verordening (EU) nr. 910/2014 van het Europees Parlement en de Raad van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt en tot intrekking van Richtlijn 1999/93/EG (hierna: eIDAS-verordening).

4 Artikel 3 lid 10 eIDAS-verordening.

5 Artikel 3 lid 11 jo. 26 eIDAS-verordening; Zie voor de (technische) totstandkoming van deze handtekening par. 3.3.

6 Artikel 3 lid 12, 3 lid 15, 23 en 28 tot en met 30 eIDAS-verordening; Zie voor de (technische) totstandkoming van deze handtekening par. 3.3.

7 Artikel 3 lid 15 eIDAS-verordening.

8 Artikel 25 lid 2 en 3 eIDAS-verordening. Op deze rechtsgevolgen wordt nader ingegaan in paragraaf 2.3.

9 Overweging 49 en artikel 25 lid 1 eIDAS-verordening.

transacties waarin gebruik wordt gemaakt van een gewone of geavanceerde elektronische handtekening moet dus altijd onderzocht worden welk recht van toepassing is en welke rechtsgevolgen dat rechtsstelsel aan het gebruik van deze elektronische handtekeningen toekent.
Naar Nederlands recht zijn de rechtsgevolgen van de gewone en geavanceerde elektronische handtekening geregeld in artikel 3:15a BW. Samengevat volgt daaruit dat deze elektronische handtekeningen dezelfde rechtsgevolgen hebben als een gekwalificeerde handtekening indien een methode voor ondertekening is gebruikt die voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische handtekening is gebruikt en alle overige omstandigheden van het geval. Het artikel noemt verder echter geen specifiek doel of specifieke omstandigheden waarin een elektronische handtekening in ieder geval voldoende betrouwbaar is. Ook is er weinig rechtspraak op dit punt. Er is dus sprake van een open norm die het lastig maakt om in algemene zin aan te geven wanneer aan de vereisten van artikel 3:15a BW is voldaan. Wel wordt aangenomen dat bij een eenvoudige transactie veelal een gewone elektronische handtekening zal volstaan, terwijl bij een meer complexe transactie die meer betrouwbaarheid en veiligheid vereist sneller een geavanceerde elektronische handtekening nodig zal zijn. Of een transactie eenvoudig of juist meer complex is, is evenmin in algemene zin te duiden, maar uit de parlementaire geschiedenis volgt dat onder meer de economische waarde en aard van de transactie daarin een rol spelen. Ter illustratie wordt bijvoorbeeld onderscheid gemaakt tussen de koop van een cd of boek op afstand als eenvoudige transactie en het geven van een (meer complex) juridisch of medisch advies.[10] In geval van discussie over de mate van betrouwbaarheid is het laatste woord hierover echter altijd aan de rechter.

2.3 *Bewijskracht van elektronische handtekeningen*

Het oordeel van de rechter over de betrouwbaarheid van een elektronische handtekening is van invloed op de bewijskracht van het ondertekende geschrift. Oordeelt een rechter namelijk dat een gewone of geavanceerde elektronische handtekening voldoende betrouwbaar is, dan heeft die handtekening – net als een gekwalificeerde elektronische handtekening – dezelfde rechtsgevolgen als een handgeschreven handtekening. Bewijsrechtelijk heeft dat tot gevolg dat het elektronisch ondertekende geschrift een onderhandse akte is en dwingende bewijskracht heeft.[11] Oordeelt een rechter dat een elektronische handtekening onvoldoende betrouwbaar is, dan heeft het elektronisch ondertekende geschrift slechts vrije bewijskracht.[12] De elektronische handtekening is dan dus niet ongeldig, maar er kan dan aanvullend bewijs nodig zijn om de authenticiteit van de elektronische handtekening aan te tonen.
Om deze potentiele bewijsproblematiek te omzeilen, kunnen contractspartijen een bewijsovereenkomst sluiten. Daarin dienen afspraken opgenomen te worden over het betrouwbaarheidsniveau van de gewone of geavanceerde elektronische handtekening. Het is echter niet ondenkbaar dat ook afspraken gemaakt worden over de rechtsgevolgen van de elektronische handtekening gebaseerd op de aard van de transactie en het doel van de elektronische handtekening in de gegeven omstandigheden.[13] Voor de rechtsgevolgen van een gekwalificeerde elektronische handtekening kan overigens geen bewijsovereenkomst gesloten worden nu de eIDAS-verordening de rechtsgevolgen hiervan dicteert.[14]

3. Overwegingen in het selectieproces van een leverancier van elektronische handtekeningen

Aan de keuze voor het type elektronische handtekening, gaat uiteraard de keuze voor een leverancier van elektronische handtekeningen vooraf.[15] Hierna volgen enkele praktische overwegingen waarmee een bedrijf rekening kan houden in het selectieproces.

3.1 *De voorfase*

Voordat een bedrijf een partij uitkiest die het gebruik van elektronische handtekeningen mogelijk maakt, zal het in kaart moeten brengen welke wensen het heeft. In dat kader zal een bedrijf zijn huidige werkwijze en de doelen die het met het gebruik van elektronische handtekeningen wil bewerkstelligen, moeten bestuderen.
Procesmatig zullen dan vragen aan de orde dienen te komen over de inrichting van het huidige ondertekeningsproces en de personen die momenteel aan dit proces uitvoering geven. Technisch is onder meer relevant hoe, waar en door wie de ondertekende documenten thans worden opgeslagen. Juridisch zal met name gekeken moeten worden naar de documenten die zijn en (in de toekomst) zullen worden ondertekend. Relevant is bijvoorbeeld of ondertekening van die documenten wettelijk is vereist, of elektronische ondertekening daarvan is toegestaan, of er sectorspecifieke wetgeving op van toepassing is en of er rekening gehouden moet worden met buitenlands recht.

3.2 *De selectiefase*

In deze fase staat hoofdzakelijk centraal welke functionaliteiten en commerciële opties een leverancier aanbiedt en in hoeverre die aansluiten op de wensen van het bedrijf. Omdat het aanbod van leveranciers zeer uiteenlopend is, volsta ik hierna met het noemen van enkele belangrijke aandachtspunten.
Procesmatig is allereerst van belang hoe een leverancier het ondertekeningsproces vormgeeft en in hoeverre dat aansluit of afwijkt van het proces zoals dat reeds wordt gehanteerd. Aan de hand hiervan kan worden bepaald wat voor impact een omschakeling naar elektronische ondertekening

10 *Kamerstukken II* 2001-2002, 27 743, nr. 6, p. 2.
11 Artikel 156a Rv.
12 Artikel 152 Rv.
13 *Kamerstukken II* 2000 – 2001, 27 743, nr. 3, p. 4 en 17; *Kamerstukken II* 2015 – 2016, 34 413, nr. 3, p. 63.
14 *Kamerstukken II* 2015 – 2016, 34 413, nr. 3, p. 63.
15 Enkele bekende leveranciers zijn bijvoorbeeld DocuSign, Adobe en SignRequest.

voor gebruikers zal hebben. Verder is interessant welke informatie uit het ondertekeningsproces precies wordt bijgehouden en opgeslagen. Is bijvoorbeeld alleen inzichtelijk dat een bepaalde stap uit het ondertekeningsproces is voltooid of is ook te achterhalen waar en wanneer een stap precies is voltooid? Dit kan relevante informatie zijn als een partij achteraf betwist dat hij of zij een elektronische handtekening heeft gezet. Tot slot kan het nuttig zijn navraag te doen naar de certificeringen en de resultaten van (onafhankelijke) audits bij de leverancier voor zover die beschikbaar zijn.

Technisch zijn met name de beveiligingsmaatregelen die een leverancier in acht neemt van belang. Een bedrijf zal in de regel namelijk alleen vertrouwen hebben in elektronische ondertekening als het product van een leverancier met voldoende waarborgen is omkleed. Denk bij de beveiligingsmaatregelen aan beveiligde verzending van documenten, de beveiliging van gebruikersaccounts en back-upvoorzieningen. Ook is relevant of elektronisch ondertekende geschriften door de leverancier worden opgeslagen en als dat het geval is, hoe(lang) en waar. Afhankelijk van de bedrijfsactiviteiten kan met name de 'waar' belangrijk zijn om te (blijven) voldoen aan eventuele verplichtingen uit (hoofdstuk V van) de Algemene Verordening Gegevensbescherming.[16]

Vanuit juridisch oogpunt is de belangrijkste vraag welke typen elektronische handtekeningen in de zin van de eIDAS-verordening een aanbieder faciliteert. Daarnaast is anticiperend op de mogelijke betwisting van de authenticiteit van een elektronische handtekening de wijze waarop een aanbieder een gebruiker identificeert relevant. Moeten gebruikers zich bijvoorbeeld identificeren met slechts een e-mailadres, een kopie van een identificatiemiddel of in persoon? Dit laatste is niet altijd wenselijk bijvoorbeeld als sprake is van een eenvoudige transactie waarbij een consument op afstand een product koopt. De wijze van identificatie moet dus in verhouding staan tot de aard van de transactie.

Commercieel zijn veelal de kosten die verbonden zijn aan het zetten van een elektronische handtekening doorslaggevend. Aanbieders hanteren verschillende prijsmodellen uiteenlopend van een vast bedrag per type elektronische handtekening, een vast bedrag per hoeveelheid elektronische handtekeningen en het afsluiten van een abonnement met een maandprijs. Een prijsvergelijking is niet te geven, maar in de regel geldt dat hoe complexer een elektronische handtekening (technisch) is, hoe hoger de prijs daarvan zal zijn.

3.3 *Post-selectie*

Als uit het brede scala van leveranciers een keuze is gemaakt, resteert de vraag welke 'klantenservice' die leverancier biedt. Daarmee doel ik niet (alleen) op hulp bij vragen over gebruik van het product, maar op assistentie bij de implementatie van het product in de bedrijfsvoering. Belangrijker is immers om te weten hoe een leverancier handelt als de geldigheid van een elektronische handtekening wordt betwist. In zo'n geval is het behulpzaam als de leverancier bereid is om bijvoorbeeld een garantie aan te bieden of (aanvullende) rechtshulp te verlenen. Het kan dus zeker geen kwaad om hier navraag naar te doen.

4. Elektronische ondertekening en validatie

Na de selectie van een leverancier en de implementatie van diens product, volgt de elektronische ondertekening. Voor begrip van het validatieproces dat na ondertekening volgt, is enig inzicht vereist in de techniek achter elektronische handtekeningen. Ik licht dat daarom eerst kort toe.

Voor het zetten van een geavanceerde elektronische handtekening is vereist dat de ondertekenaar met behulp van een algoritme een sleutelpaar genereert. Dit bestaat uit een geheime en publieke sleutel die cryptografisch onlosmakelijk met elkaar verbonden zijn; de geheime sleutel is bedoeld om te ondertekenen terwijl de publieke sleutel wordt gebruikt om te verifiëren of een elektronische handtekening geldig is. Met behulp van een ander algoritme, de geheime sleutel van de ondertekenaar en de te ondertekenen gegevens wordt vervolgens de elektronische handtekening gegenereerd.[17] Eventueel kan de elektronische handtekening gecertificeerd worden door een certificaatautoriteit. Dit is een betrouwbare derde die de identiteit van de ondertekenaar controleert, bijvoorbeeld met een kopie van een legitimatiebewijs of door legitimatie van de ondertekenaar in persoon. Bij succesvolle controle worden de identiteitsgegevens en de publieke sleutel van de ondertekenaar opgenomen in een digitaal certificaat dat wordt gekoppeld aan de elektronische handtekening. Als een certificaat wordt gebruikt van een gekwalificeerde verlener in de zin van de eIDAS-verordening, dan is sprake van een gekwalificeerde handtekening.

Na ondertekening zullen met name derden de elektronische handtekening willen valideren. Ook dit gebeurt met behulp van een algoritme. Die controleert dan of het document is ondertekend met de geheime sleutel van de ondertekenaar, of het document (binnen toegestane marges) is gewijzigd en of een eventueel certificaat afkomstig is van een betrouwbare certificaatautoriteit.[18] In de praktijk wordt deze verificatie, afhankelijk van de computerinstellingen, automatisch uitgevoerd. Zo zal bij een Pdf-bestand na een geslaagde

16 Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (hierna: Algemene Verordening Gegevensbescherming of AVG); De AVG schrijft voor de verwerking van persoonsgegevens van natuurlijke personen binnen de EU een bepaald beschermingsniveau voor. Eenzelfde beschermingsniveau moet op grond van de AVG ook gehanteerd worden bij de doorgifte van die persoonsgegevens naar landen buiten de EU (zie o.a. overweging 9, 10 en 101 AVG). Voor zover dat beschermingsniveau niet adequaat wordt gewaarborgd, kunnen er voor een leverancier zelfs aanvullende verplichtingen zijn. Het is uiteraard alleen mogelijk om te achterhalen of dit beschermingsniveau wordt gewaarborgd en of aan eventuele aanvullende verplichtingen wordt voldaan als kan worden achterhaald waar de persoonsgegevens zich precies zullen bevinden.

17 J. Linnemann, 'Juridische aspecten van blockchain', *Computerrecht* 2016/218, par. 2.2.

18 Ibidem.

validatie de melding 'Ondertekend en alle handtekeningen zijn geldig' verschijnen en is in het 'Handtekeningenvenster' extra informatie te vinden over de handtekening. Wat overigens niet wordt gecontroleerd is de geldigheid van een aan de elektronische handtekening gekoppeld certificaat. Het kan echter voorkomen dat een certificaat voor de vervaldatum door de certificaatautoriteit is ingetrokken, bijvoorbeeld omdat de ondertekenaar is overleden of omdat er identiteitsfraude is gepleegd. De intrekking van het certificaat zal in zo'n geval geregistreerd zijn in een *Certificate Revocation List* of in het *Online Certificate Status Protocol*. Bij validatie zullen dus ook die bronnen geraadpleegd moeten worden.

Een andere manier om een elektronische handtekening te valideren is met behulp van een validatietool. Eén daarvan is de *Digital Signature Service Demonstration WebApp*, een publieke tool van de Europese Unie.[19] Na het uploaden van een elektronisch ondertekend document krijgt de gebruiker onder meer informatie over het type elektronische handtekening (geavanceerd of gekwalificeerd), de leverancier van de elektronische handtekening en de datum en tijd van ondertekening. Een pluspunt van deze tool is dat certificaten ook meteen op geldigheid worden gecontroleerd.[20]

Gerelateerd aan deze tool, is de *Trusted List Browser* die de Europese Unie ingevolge artikel 22 lid 4 van de eIDAS-verordening aanbiedt.[21] Dit is overigens geen validatietool, maar een tool waarin zogenaamde vertrouwenslijsten van alle lidstaten zijn opgenomen met informatie over leveranciers van gekwalificeerde handtekeningen per lidstaat.[22] De informatie hieruit kan bijvoorbeeld nuttig zijn bij de selectie van een leverancier van elektronische handtekeningen. Zo zal een bedrijf dat regelmatig contracteert over grote, grensoverschrijdende (Europese) belangen, vermoedelijk zaken willen doen met een leverancier die (ook) het zetten van gekwalificeerde elektronische handtekeningen faciliteert.[23] Met behulp van de *Trusted List Browser* kan dan gemakkelijk een geschikte leverancier gevonden worden.

5. Tot slot

Hoewel veel bedrijven al gebruikmaken van elektronische handtekeningen, staan niet alle bedrijven daarom te popelen. De kosten voor het gebruik van gekwalificeerde elektronische handtekeningen liggen immers relatief hoog en op de overige elektronische handtekeningen is, althans in Nederland, een open norm van toepassing die rechtsonzekerheid schept over de bewijskracht. Omdat er daarnaast weinig rechtspraak is over dit onderwerp, is het soms lastig om vooraf in te schatten van welk type elektronische handtekening het beste gebruik gemaakt kan worden. Om twijfels weg te nemen en het gebruik van elektronische handtekeningen verder te doen toenemen zou de (Nederlandse) praktijk dus gebaat zijn bij meer illustratieve rechtspraak waarin invulling wordt gegeven aan het begrip 'voldoende betrouwbaar'. Het is te hopen dat die er in 2020 komt.

19 Zie https://ec.europa.eu/cefdigital/DSS/webapp-demo/validation.
20 Zie https://ec.europa.eu/cefdigital/DSS/webapp-demo/signature-standalone.
21 Zie https://webgate.ec.europa.eu/tl-browser/#/.
22 Zie https://ec.europa.eu/cefdigital/DSS/webapp-demo/tsl-info/nl.
23 Zie paragraaf 2.1 over de rechtsgevolgen van een gekwalificeerde elektronische handtekening.