Een Gemeenschapsregime voor elektronische identificatie

Mr. H.W. Wefers Bettink en mr. drs. J. Theeven*

Elektronische transacties zijn niet meer weg te denken uit ons dagelijks leven. Het bestaande Europeesrechtelijke kader voor elektronische rechtshandelingen wordt onder meer gevormd door de Richtlijn elektronische handtekening[1] (hierna: de Richtlijn). Deze uit 1999 stammende richtlijn is echter niet toegesneden op de snelle ontwikkeling van nieuwe technologieën en toenemende mondialisering van het handelsverkeer die sindsdien hebben plaatsgevonden. Bovendien heeft de Richtlijn geleid tot uiteenlopende implementatie in de lidstaten. Dat was er volgens de Europese Commissie mede de oorzaak van dat er weinig groei zit in de markt voor grensoverschrijdende transacties binnen de EU. Ook het grensoverschrijdend gebruik van elektronische identificatie in het kader van overheidsdiensten viel de Commissie tegen. Op 4 juni 2012 heeft de Commissie haar voorstel voor een Verordening betreffende elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt toegezonden aan de Raad,[2] dat hierin moet voorzien.

Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende elektronisch identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (COM 2012/0238).

Richtlijn en de wet elektronische handtekeningen

Inleiding

Consumenten, bedrijven en overheden maken sinds de opkomst van het internet in steeds toenemende mate gebruik van de elektronische weg (internet, mobiele netwerken) voor het aanschaffen van goederen en diensten, het doen van betalingen en het indienen van belastingaangiften en vergunningaanvragen. Daarbij wordt gebruik gemaakt van elektronische identificatiemiddelen. Te denken valt aan de combinatie van bankpas, pincode en paslezer of SMS bij het elektronisch bankieren, DigiD bij het indienen van documenten bij de overheid, mobiele telefoon en logincode bij betaling van parkeergelden en het gebruik van een op naam gestelde OV-chipkaart bij reizen in het openbaar vervoer.

Al in 1999 is de Richtlijn elektronische handtekening ingevoerd (hierna: de Richtlijn) met als doel het in ontwikkeling zijnde elektronische handelsverkeer te bevorderen en daarvoor een interne markt te creëren door het gebruik van elektronische handtekeningen in lidstaten te vergemakkelijken en tot de wettelijke erkenning ervan bij te dragen. De Richtlijn was primair gericht op commerciële transacties, al was er geen beletsel om deze ook toe te passen op elektronisch rechtsverkeer met de overheid.

De Wet elektronische handtekening

In Nederland is de Richtlijn geïmplementeerd in de Wet elektronische handtekeningen, die heeft geleid tot invoering van de artikelen 3:15a-3:15c BW.[3] Deze wet is op 21 mei 2003 in werking getreden.[4] Op grond van artikel 2:16 Algemene wet bestuursrecht zijn de relevante bepalingen van overeenkomstige toepassing op de communicatie tussen burgers en overheden, tenzij de aard van het bericht zich daartegen verzet.[5]

Onder een elektronische handtekening wordt verstaan: elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authentificatie.[6] Voorbeelden van een elektronische handtekening

* Mr. H.W. Wefers Bettink is advocaat bij Houthoff Buruma. mr. drs. J. Theeven is bedrijfsjurist bij Sabic.

1. Richtlijn 1999/93/EG van 13 december 1999 betreffende een gemeenschappelijk kader voor elektronische handtekeningen.
2. Voorstel voor een Verordening van het Europees Parlement en de Raad betreffende elektronisch identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (COM 2012/0238).
3. De art. 3:15d-3:15f BW zijn later toegevoegd ter uitvoering van Richtlijn 2000/31/EG inzake de elektronische handel.
4. Wet van 8 mei 2003, *Stb.* 2003, 199 (Wet elektronische handtekeningen).
5. Wet van 29 april 2004, *Stb.* 2004, 214 (Wet elektronisch bestuurlijk verkeer).
6. Art. 2.1 Richtlijn (definities).

zijn de ondertekening van een e-mail en een ingescande handtekening.

Artikel 3:15a lid 1 BW bepaalt dat een elektronische handtekening dezelfde rechtsgevolgen heeft als een handgeschreven handtekening, indien de methode die daarbij gebruikt is voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische gegevens worden gebruikt en op alle overige omstandigheden van het geval. Het tweede lid bepaalt dat een dergelijke methode wordt vermoed voldoende betrouwbaar te zijn, indien een elektronische handtekening:

a. op unieke wijze aan de ondertekenaar is verbonden;
b. het mogelijk maakt de ondertekenaar te identificeren;
c. tot stand komt met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
d. op zodanige wijze is verbonden aan de gegevens waarop zij betrekking heeft, dat elke wijziging achteraf van de gegevens kan worden opgespoord;[7]
e. is gebaseerd op een gekwalificeerd certificaat;[8] en
f. is gegenereerd door een veilig 'middel';[9] hiermee wordt gedoeld op de software of hardware waarmee de handtekening is aangemaakt.

Deze elektronische handtekening wordt ook wel aangeduid als digitale handtekening of gekwalificeerde elektronische handtekening.

Belang van de elektronische handtekening

De gekwalificeerde elektronische handtekening is van belang in situaties waar de wet voor een geldige rechtshandeling een handtekening voorschrijft. Dat is bijvoorbeeld het geval wanneer een akte is vereist, hetgeen zowel schriftelijkheid als een handtekening impliceert. Dit geldt onder meer voor een koopakte voor een woning (art. 7:2 BW), de pachtovereenkomst (art. 7:317 BW), huurkoop (art. 7A:1576b BW). Een ander voorbeeld is de volmacht voor de aandeelhoudersvergadering (art. 2:117 BW en 2:227 BW). In 2010 is artikel 156a Rv ingevoerd, waarin de elektronische akte is gelijk gesteld met de schriftelijke akte van artikel 156 Rv.[10] In de praktijk wordt buiten de overheid weinig gebruik gemaakt van de gekwalificeerde elektronische handtekening. Het hiervoor benodigde systeem van afgifte door een onafhankelijke certificatiedienst (een '*trusted third party*'), waarvoor registratie en identificatie is vereist, lijkt in de meeste gevallen niet goed te passen bij de snelheid en het gemak waarmee consumenten online transacties willen doen. Het bedrijfsleven heeft eigen identificatiemiddelen ontwikkeld die voor een groot deel zijn gebaseerd op een combinatie van gebruikersnaam en wachtwoord, al dan niet in samenhang met een speciale logincode, waarbij op grond van de toepasselijke algemene voorwaarden de verantwoordelijkheid voor het gebruik (en misbruik) hiervan bij de gebruiker wordt gelegd. Die risicoverdeling wordt in de rechtspraak doorgaans erkend en dit systeem werkt in praktijk dan ook goed.[11] Voor bancaire transacties en voor identificatie tegenover de overheid zijn meer geavanceerde instrumenten ontwikkeld. Voor het internetbankieren hebben veel banken een eigen paslezer die – met bankpas en pincode – tijdens de verschillende stappen van het bancaire proces de benodigde codes berekent die op de website van de bank moeten worden ingevoerd. Hierbij is sprake van een geavanceerde elektronische handtekening, indien deze is gebaseerd op een gekwalificeerd certificaat. Dat is wel het geval bij de DigiD codes van de overheid die na een gedetailleerd registratieproces worden verstrekt door een *trusted third party*.

Totstandkoming Verordening

Het voorstel van de Europese Commissie voor een Verordening met betrekking tot elektronische identificatie en vertrouwensdiensten voor elektronische transacties in de interne markt (hierna: de Verordening) heeft ten doel een veilige en ongehinderde elektronische interactie tussen bedrijven, burgers en overheden mogelijk te maken om zo de effectiviteit van publieke en particuliere online diensten, e-business en elektronische handel in de EU te vergroten. Daartoe wordt een stelsel van wederzijdse erkenning van vertrouwensdiensten (zoals de elektronische handtekening en het web-certificaat) en van elektronische identificatiemiddelen geïntroduceerd. Wat de concrete obstakels zijn die de elektronische interactie op dit moment hinderen en hoe men denkt die met de Verordening te verwijderen wordt niet verduidelijkt in de toelichting op de Verordening en evenmin in de brief waarmee de Staatssecretaris van Buitenlandse Zaken de ontwerp-Verordening bij de Tweede Kamer introduceerde.[12] Het praktisch nut van de Verordening lijkt vooral te zijn gelegen in het faciliteren van grensoverschrijdend gebruik van overheidsdiensten, zoals het aanvragen van vergunningen en het doen van belastingaangifte in het buitenland waarvoor een uniform kader voor de erkenning van elektronische identificatiemiddelen onontbeerlijk is. Ook grensoverschrijdende deelname aan openbare aanbestedingsprocedure kan hierdoor worden gefaciliteerd.

Inmiddels heeft het Europees Economisch en Sociaal Comité (EESC) zijn advies uitgebracht.[13] Een van de voornaamste aanbevelingen is om één Europees eID te introduceren, in plaats van de erkenning en aanvaarding

7. Art. 2.2 Richtlijn. Deze eisen zijn minimumvereisten, lidstaten zijn vrij om strengere regels te stellen. Overweging 28 Richtlijn.
8. Art. 1.1 onderdeel ss Telecommunicatiewet (Tw).
9. Art. 1.1 onderdeel vv Tw.
10. Wet van 20 februari 2010, *Stb.* 2010, 222 (Wet ontwikkelingen elektronisch verkeer).
11. Zie reeds HR 19 november 1993, *NJ* 1994, 622 (*Cova*). Recentelijk: Gerechtshof Amsterdam 13 mei 2012, *JOR* 2012/182, m.nt. B.A. Schuijling (*Rahibi/Rabobank*); Rb. Zutphen 22 februari 2012, *RCR* 2012/38.
12. *Kamerstukken II* 2011/12, 22 112, nr. 1439, brief van de Staatssecretaris van Buitenlandse Zaken d.d. 13 juli 2012.
13. Zie voor actuele status: <http://parltrack.euwiki.org/dossier/2012/0146(COD)>.

van afzonderlijke nationale eID's.[14] Het voorstel voor de Verordening bevindt zich thans in de eerste leesfase bij het Europees Parlement. Aanname van het voorstel door het Europees Parlement en de Raad van Ministers is voorzien in 2014.

De Verordening vloeit voort uit de Digitale Agenda die door de Europese Commissie op 19 mei 2010 is gepresenteerd.[15] In de Digitale Agenda worden zeven doelstellingen benoemd die een uniforme digitale markt in de EU moeten realiseren. Een van de doelstellingen is de verwezenlijking van een interne markt,waarin online content en diensten vrij binnen en buiten de grenzen van de EU kunnen circuleren.

Een belangrijke constatering in de Digitale Agenda is dat er in het afgelopen decennium geen harmonisatie van wetgeving met betrekking tot de elektronische handtekening en transacties heeft plaatsgevonden. Daarin wordt de mening naar voren gebracht dat het ontbreken van deze harmonisatie een belangrijke oorzaak is voor het ontbreken van een interne markt op het gebied van e-commerce. Dat zou liggen aan de uiteenlopende implementatie van de Richtlijn elektronische handtekening in de lidstaten, die zou hebben geleid tot een versnippering van de markt, waardoor grensoverschrijdende online transacties zouden zijn beperkt. In dat verband wordt erop gewezen dat minder dan één op de tien online transacties een grensoverschrijdend karakter heeft en dat dergelijke transacties eerder met Amerikaanse bedrijven plaatsvinden dan met een bedrijf uit een ander Europees land.[16]

Omdat de Richtlijn niet heeft geleid tot de beoogde harmonisatie, heeft de Commissie besloten het zwaardere middel van een verordening in te zetten om de interne markt en de doelen uit de Digitale Agenda (en meer dan dat) te verwezenlijken. De Verordening is krachtens artikel 288 VWEU rechtstreeks van toepassing en zal, na inwerkingtreding, de Richtlijn en de implementatiewetgeving in de lidstaten vervangen. Het uniforme regime en de rechtstreekse werking van de Verordening zullen naar verwachting de betrouwbaarheid van de grensoverschrijdende dienstverlening en de rechtszekerheid vergroten. Dat moge zo zijn, het is echter de vraag of daarvan een groot effect zal uitgaan op de omvang van grensoverschrijdende transacties. De reden dat Amerikaanse bedrijven als Amazon.com in Europa zo populair zijn, lijkt vooral te maken te hebben met de service en de goede prijs/kwaliteitverhouding die zij leveren. Het ontbreken van een uniform regime voor de elektronische handtekening lijkt voor deze bedrijven geen obstakel om grensoverschrijdend te handelen.

14. Opinion of the EESC on the Proposal for a regulation of the European Parliament and of the Counsel on electronic identification and trust services for electronic transactions in the internal market, COM(2012) 238 final. Datum 18 september 2012.
15. Een digitale agenda voor Europa, herziene versie 26 augustus 2010, <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=COM:2010:0245:FIN:NL:PDF>.
16. Digitale agenda, par. 2.1.2, p. 11.

Inhoud Verordening

Waar de Richtlijn slechts ziet op de elektronische handtekening, heeft de Verordening betrekking op meerdere vormen van elektronische identificatie en op elektronische vertrouwensdiensten voor elektronische transacties.[17] Met elektronische identificatie wordt bedoeld het gebruik van persoonsidentificatiegegevens in elektronische vorm die op ondubbelzinnige wijze een natuurlijk persoon of rechtspersoon aanduiden.[18]

Onder elektronische vertrouwensdiensten wordt verstaan iedere elektronische dienst die bestaat uit het aanmaken, verifiëren, valideren, hanteren en bewaren van elektronische handtekeningen, elektronische zegels, elektronische tijdstempels, elektronische documenten, elektronische bezorgingdiensten, website authenticatie elektronische certificaten, met inbegrip van certificaten voor elektronische handtekeningen en voor elektronische zegels.[19] Onder de Richtlijn waren alleen de certificatie dienstverleners geregeld, die een certificaat afgeven waarmee de betrouwbaarheid van een website of een elektronische handtekening is geborgd.

Wederzijdse erkenning en aanvaarding eID's

De kern van de Verordening ligt in artikel 5 dat lidstaten verplicht tot wederzijdse erkenning van de systemen voor de uitgifte van elektronische identificatiemiddelen (eID's), die door een lidstaat zijn aangemeld bij de Commissie. Onder een elektronisch identificatiemiddel wordt verstaan een materiële of immateriële eenheid die gegevens bevat voor elektronische identificatie en die gebruikt wordt voor de online toegang tot een dienst. Een lidstaat kan een op zijn grondgebied toegelaten eID bij de Commissie aanmelden als erkende en aanvaarde identificatiedienst, mits die voldoet aan de daaraan gestelde eisen. De Commissie publiceert een lijst van aangemelde eID's, de zogenoemde vertrouwenslijst.[20] In een lidstaat toegelaten eID's die niet zijn aangemeld hoeven door andere lidstaten niet erkend en aanvaard te worden.

Op grond van artikel artikel 6 van de Verordening moeten elektronische identificatiemiddelen door, namens of onder verantwoordelijkheid van de aanmeldende lidstaat worden afgegeven[21] en moeten zij ten minste bruikbaar zijn voor toegang tot overheidsdiensten waarvoor elektronische identificatie in de lidstaat vereist is.[22] Dit bevestigt dat het primaire doel van de Verordening is om de grensoverschrijdende elektronische toegang tot overheidsdiensten te faciliteren. De aanmeldende lidstaat moet waarborgen dat de persoonsidentificatiegegevens op ondubbelzinnige wijze worden gekoppeld aan

17. Art. 1.1 Verordening.
18. Art. 3.1 Verordening.
19. Art. 3.12 Verordening.
20. Deze lijst wordt zes maanden na inwerkingtreding van de Verordening gepubliceerd (art. 7 lid 2 Verordening). Als de Commissie een aanmelding ontvangt nadat die periode verstreken is, wijzigt zij de lijst binnen drie maanden (art. 7 lid 3 Verordening).
21. Art. 6.1 onder a Verordening.
22. Art. 6.1 onder b Verordening.

de natuurlijke of rechtspersoon die wordt aangeduid.[23] De elektronische gegevens moeten dus steeds naar dezelfde persoon verwijzen zodat geen misverstand kan ontstaan over de identiteit van de persoon die gebruikmaakt van een vertrouwensdienst.

Om een goed werkend systeem te garanderen vereist artikel 6 voorts dat de lidstaat waarborgt dat de online authenticatiemogelijkheid ononderbroken beschikbaar en kosteloos is.[24] Zodoende kunnen partijen die gebruikmaken van eID's op ieder gewenst tijdstip door hen ontvangen elektronische persoonsidentificatiegegevens verifiëren

Wanneer een inbreuk plaatsvindt of de integriteit van een aangemeld systeem is geschonden, dient een lidstaat het aangemelde systeem of de authenticatiemogelijkheid meteen op te schorten of in te trekken. De betrokken lidstaat dient de andere lidstaten en de Commissie onverwijld van een dergelijke omstandigheid op de hoogte te stellen.[25]

Lidstaten dienen aansprakelijkheid te aanvaarden voor (1) de ondubbelzinnige koppeling van de persoonsidentificatiegegevens en (2) het in stand houden van een goed werkende online authenticatiemogelijkheid van door hen aangemelde systemen.[26]

Toezicht

De Verordening voorziet in een versterking van het toezicht op de vertrouwensdiensten. Gezien de problemen die in Nederland zijn ontstaan rond DigiNotar, dat certificaten voor veel overheidsdiensten en websites uitgaf, is dat niet overbodig.[27] Iedere lidstaat dient een toezichthoudend orgaan aan te wijzen of op te richten.[28] In Nederland zal deze rol worden vervuld door de OPTA en, zodra deze is opgericht, de Autoriteit Consument en Markt, waarin de OPTA in de loop van 2013 zal opgaan.[29]

De toezichthouder krijgt de bevoegdheid tot het geven van bindende aanwijzingen aan alle verleners van vertrouwensdiensten, die deze moeten opvolgen. In Nederland zal dat vermoedelijk geschieden in de vorm van een last onder dwangsom, een gebruikelijk handhavingsmiddel voor toezichthouders (zie art. 5:32Awb). Een belangrijke taak van de toezichthouder is de controle van de passende technische en organisatorische maatregelen die verleners van vertrouwensdiensten moeten nemen met het oog op de beveiliging van de door hen geleverde diensten. Daarnaast moet de toezichthouder toezien op de naleving van de meldplicht in geval van een veiligheidsinbreuk of integriteitverlies dat aanzienlijke gevolgen kan hebben voor de persoonsgegevens die daarmee worden beheerd.[30]

De toezichthouder heeft extra bevoegdheden ten opzichte van gekwalificeerde vertrouwensdiensten die voldoen aan de in artikel 19 van de Verordening opgenomen vereisten. Deze dienen te beschikken over voldoende gekwalificeerd personeel en voldoende financiële middelen of een toereikende aansprakelijkheidsverzekering om het risico van aansprakelijkheid voor schade te kunnen dragen. Zij moeten gebruik maken van betrouwbare systemen voor de opslag van de aan hen verstrekte gegevens en maatregelen nemen ter voorkoming van vervalsing en diefstal van gegevens. De gekwalificeerde verleners van vertrouwensdiensten moeten zorgen dat de persoonsgegevens door hen worden verwerkt in overeenstemming met de Privacyrichtlijn[31] en moeten alle relevante informatie met betrekking tot hun dienstverlening vastleggen en gedurende een bepaalde periode bewaren. Ook moeten zij beschikken over een geactualiseerd continuïteitsplan om de continuïteit van de dienstverlening te verzekeren. Een dergelijk continuïteitsplan is op grond van de Telecommunicatiewet reeds een vereiste voor aanbieders van elektronische communicatienetwerken en -diensten.[32]

Voor gekwalificeerde vertrouwensdiensten komt er voorts een verplichte jaarlijkse audit op naleving van hun verplichtingen uit de Verordening.[33] Deze wordt door een erkend onafhankelijk orgaan uitgevoerd. De uitkomsten van de audit worden aan de toezichthouder verstrekt. Niet-naleving van de aanwijzingen in het auditrapport kan leiden tot verwijdering van de gekwalificeerde vertrouwensdienst van de vertrouwenslijst.[34]

Elektronische handtekening

De Verordening vervangt de regeling van de elektronische handtekening in de Richtlijn en verduidelijkt de rechtsgevolgen van de elektronische handtekening en breidt deze uit ten opzichte van de Richtlijn.

Evenals bij de Richtlijn is het uitgangspunt dat de gekwalificeerde elektronische handtekening dezelfde rechtsgeldigheid heeft als de handgeschreven handtekening.[35] Gekwalificeerde elektronische handtekeningen moeten door alle lidstaten worden erkend en aanvaard.[36]

Voor grensoverschrijdende toegang tot een onlinedienst die door een openbare instantie wordt aangeboden, mag een lidstaat geen elektronische handtekening verlangen van een hoger veiligheidsniveau dan een

23. Art. 6.1 onder c Verordening.
24. Art. 6.1 onder d eerste zin Verordening.
25. Art. 6.1 onder d tweede zin Verordening.
26. Art. 6.1 onder e Verordening.
27. Zie de brief d.d. 12 november 2012 van minister Plasterk met een reactie op het onderzoeksrapport van de Onderzoeksraad voor de Veiligheid inzake 'Het Diginotar-incident, waarom digitale veiligheid de bestuurstafel te weinig bereikt.' Te vinden op: <www.rijksoverheid.nl/documenten-en-publicaties/brieven/2012/11/12/brief-met-reactie-op-rapport-het-diginotar-incident-waarom-digitale-veiligheid-de-bestuurstafel-te-weinig-bereikt.html>.
28. Dit is een verbetering ten opzichte van art. 3 lid 3 Richtlijn, dat lidstaten slechts gebiedt een passend systeem voor toezicht op te richten.
29. *Kamerstukken II* 2011/12, 22 112, nr. 1439, p. 3.
30. Art. 15 lid 1 en 2 Verordening.
31. Richtlijn 95/46/EG van het Europees Parlement en de Raad van 24 oktober 1995 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens, *Pb. EG* 1995, L 281/0031-0050. Te vinden op <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:nl:HTML>.
32. Besluit van 19 oktober 2012, *Stb.* 2012, 514 (Besluit continuïteit openbare elektronische communicatienetwerken en -diensten).
33. Art. 16 Verordening.
34. Art. 16 lid 4 Verordening.
35. Art. 20 lid 2 Verordening; zie art. 5 Richtlijn.
36. Art. 20 lid 3 Verordening.

gekwalificeerde elektronische handtekening.[37] Doel daarvan is te voorkomen dat het grensoverschrijdend rechtsverkeer wordt belemmerd door extra nationale eisen. Een gekwalificeerde elektronische handtekening wordt aangemaakt met een gekwalificeerd middel en is gebaseerd op een gekwalificeerd certificaat. Dat is een digitaal bestand dat aan het oorspronkelijke document is toegevoegd en is uitgegeven door een certificatiedienstverlener. In Bijlage I bij de Verordening zijn de eisen opgenomen waaraan deze certificaten moeten voldoen. Het certificaat voor Public Key Infrastructure (PKI) overheid, waarvan de Nederlandse overheid gebruikmaakt, wordt uitgegeven door Logius, dat onderdeel is van het Ministerie van BZK.[38] In Nederland controleert de OPTA op dit moment de certificatiedienstverleners. Ten opzichte van de Richtlijn bevat Bijlage I enkele aanvullende vereisten, onder meer dat ieder certificaat de locatie bevat waar het certificaat kosteloos beschikbaar is, alsmede het adres van de dienstverlener waar informatie kan worden opgevraagd over de geldigheidsstatus van het gecertificeerde certificaat. Dit dient extra bescherming aan de gebruikers te geven. Enkele bepalingen uit Bijlage I van de Richtlijn die in de praktijk niet werkten, zijn geschrapt, zoals de maximale waarde van de transactie waarvoor het certificaat kan worden gebruikt.

Overige vertrouwensdiensten

De Verordening bevat tevens regels voor het gebruik van de elektronische zegels (afd. 4), het elektronisch tijdsstempel (afd. 5), elektronische documenten (afd. 6), gekwalificeerde dienst voor elektronische bezorging (afd. 7) en authenticatie van websites (afd. 8). Voor deze vertrouwensdiensten geldt in grote lijnen hetzelfde regime als voor elektronische handtekeningen.

Het elektronisch zegel wordt gebruikt om de oorsprong en integriteit van de ermee verbonden gegevens te waarborgen. Het elektronisch tijdsstempel koppelt de tijd van verzending aan een document, waarvoor het wettelijk vermoeden geldt dat het aangeduide tijdstip en de integriteit van de gegevens die aan het tijdstip zijn gekoppeld zijn gewaarborgd.[39] Dat kan de rechtszekerheid en de onpartijdigheid vergroten bij procedures waar, zoals in het geval van aanbestedingen, deelnemers voor een bepaald tijdstip moeten inschrijven om voor een opdracht in aanmerking te komen. Artikel 34 van de Verordening bepaalt dat een elektronisch document[40] dat aan de gestelde eisen van authenticiteit en integriteit voldoet, wordt beschouwd als gelijkwaardig aan een papieren document en toelaatbaar is als bewijs in gerechtelijke procedures.

Een elektronisch document dat is ondertekend met een gekwalificeerde elektronische handtekening of dat een gekwalificeerd elektronisch zegel draagt, wordt vermoed authentiek en echt te zijn. Voorwaarde is dat het elektronisch document (achteraf) niet kan worden gewijzigd.[41] Worden gegevens verzonden met een elektronische bezorgingsdienst die voldoet aan de eisen van de Verordening, dan worden zij eveneens vermoed authentiek en echt te zijn.[42] Tot slot voorziet de Verordening in een waarborg voor de authenticiteit van websites en de eigenaars ervan. In bijlage IV worden eisen voor de authenticatie van websites vermeld. Gekwalificeerde certificaten voor authenticatie van websites die zijn afgegeven door een in een lidstaat erkende vertrouwensdienst, moeten worden erkend en aanvaard in alle lidstaten.[43]

Nederlands standpunt

Het Nederlandse kabinet heeft in de brief van 4 juli 2012 van staatssecretaris Knapen aangegeven dat het de Verordening verwelkomt.[44] De doelstellingen worden onderschreven, maar het kabinet plaatst enkele belangrijke kanttekeningen bij de in de Verordening gekozen benadering.[45] Zijn voornaamste zorg is dat gewaarborgd wordt dat eID's van andere lidstaten minimaal een gelijkwaardig betrouwbaarheidsniveau hebben als de Nederlandse varianten. De waarborg daarvoor is uitsluitend gelegen in het feit dat iedere lidstaat aansprakelijkheid aanvaardt voor de door hem erkende eID's. Dat biedt echter alleen de mogelijkheid achteraf schade te verhalen als blijkt dat een eID onbetrouwbaar is, maar biedt geen garantie vooraf dat in andere lidstaten erkende eID's een voldoende betrouwbaarheidsniveau hebben. Kennelijk is de regering beducht voor fraude met eID's die zijn afgegeven door lidstaten die lagere betrouwbaarheidseisen stellen.

Andere aandachtspunten zijn het vereiste dat een elektronisch identificatiemiddel wordt afgegeven door, namens of onder verantwoordelijkheid van de aanmeldende lidstaat en dat de lidstaten zich aansprakelijk stellen voor de ondubbelzinnige koppeling van de elektronische identiteit met (rechts-)persoonsidentificatiegegevens. Het kabinet is geen voorstander van het overnemen van verantwoordelijkheden door de overheid van het bedrijfsleven en heeft aangegeven daarover duidelijkheid te willen verkrijgen van de Europese Commissie.

37. Art. 20 lid 5 Verordening.
38. Zie: <www.rijksoverheid.nl/onderwerpen/digitale-overheid/vraag-en-antwoord/wat-is-een-elektronische-handtekening.html>.
39. Art. 32 lid 2 Verordening.
40. Onder 'elektronisch document' wordt verstaan ieder document in elektronische vorm (art. 3 lid 28 Verordening).
41. Art. 34 Verordening.
42. Art. 35 en 36 Verordening.
43. Art. 37 lid 2 Verordening.
44. *Kamerstukken II* 2011/12, 22 112, nr. 1439, p. 3.
45. *Kamerstukken II* 2011/12, 22 112, nr. 1439, p. 13.

Implicaties Verordening voor Nederland

Aanpassing wetgeving

De Verordening bevat bepalingen die het huidige regime voor elektronische handtekeningen in de Telecommunicatiewet, het Burgerlijk Wetboek en de Algemene Wet Bestuursrecht deels vervangen of wijzigen.[46] Vanwege de directe werking van de Verordening zal een aantal bepalingen moeten worden ingetrokken, dan wel aangepast. Voor de Telecommunicatiewet zullen specifieke regels met betrekking tot de taken van de toezichthouder (de OPTA) en de vertrouwenslijsten worden opgesteld. In de Verordening wordt bepaald dat deze twintig dagen na publicatie in werking treedt. Het kabinet vindt deze termijn, gezien het opstellen van de noodzakelijke uitvoerings- en aanpassingswetgeving, te kort en vindt een termijn van 24 maanden realistischer.[47]

Uitvoering en handhaving

De Nederlandse overheid overweegt om DigiD op grond van artikelen 5 en 7 van de Verordening als authenticatiemiddel aan te melden.[48] Hierdoor moet DigiD als vertrouwensdienst door andere lidstaten worden erkend en aanvaard. Dit zal betekenen dat Nederlanders hun DigiD voor buitenlandse overheidsdiensten kunnen gebruiken. Een lastige horde daarbij is dat DigiD bij authenticatie in grensoverschrijdende situaties het Burgerservicenummer (BSN) zou uitwisselen met de buitenlandse dienstenaanbieder. Op grond van artikel 1 sub d van de Wet Algemene Bepalingen Burgerservicenummer (Wabb), is gebruik van het BSN alleen toegestaan aan nationale overheidsorganisaties en niet aan ondernemingen (of buitenlandse overheidsinstanties). Om dit op te lossen, zou er bij grensoverschrijdend gebruik niet een BSN maar een pseudoniem moeten worden uitgewisseld met de buitenlandse aanbieder, of gebruik moeten worden gemaakt van een voorziening die de identiteit in het land van herkomst controleert. Daarvoor zal een omnummerfaciliteit en -autoriteit moeten worden ingericht, om zo nodig de relatie met de authentieke persoon te kunnen leggen.[49]

De Verordening: een verbetering?

De Verordening zal na inwerkingtreding de Richtlijn vervangen. Door de keuze voor het instrument van een verordening die na inwerkingtreding directe werking heeft in alle lidstaten, wordt een uniform stelsel geïntroduceerd dat gelijktijdig in alle lidstaten zal gelden. Dat bevordert de rechtszekerheid en zal ongetwijfeld het vertrouwen van handelspartijen en consumenten in de geldigheid van de door de Verordening gereguleerde vertrouwensdiensten en identificatiemiddelen vergroten. Of dit ook zal bijdragen aan een toename van grensoverschrijdende elektronische transacties, wat een van de doeleinden van de Verordening is, moet worden afgewacht. Zoals aangegeven spelen daarbij ook vooral aspecten als prijs, kwaliteit, service en gemak een rol. Het bereiken van een interne markt voor elektronische identificatiemiddelen en voor vertrouwensdiensten zal met name afhangen van de vraag of de lidstaten erin slagen eenzelfde niveau van betrouwbaarheid te hanteren bij toelating hiervan. Ook de effectiviteit van het toezicht zal daarbij een belangrijke rol spelen. Op papier dragen maatregelen als het aanstellen van toezichthouders en verplichte audits daar zeker aan bij, maar ook hier zal de praktische implementatie bepalend zijn voor het succes van de Verordening. Of de Verordening in deze vorm zal worden aangenomen hangt vooral af van de vraag of bij de lidstaten voldoende vertrouwen bestaat in de betrouwbaarheid van elkaars eID's. Na aanmelding bij de Commissie van een eID uit een willekeurige andere lidstaat, dient Nederland dat stelsel volledig en zonder voorbehoud te accepteren. De Nederlandse regering heeft aangegeven daartoe alleen bereid te zijn als de acceptatieplicht is beperkt tot buitenlandse eID's die minimaal het gelijkwaardige betrouwbaarheidsniveau hebben van de Nederlandse equivalenten daarvan.[50] De Commissie had dit probleem kunnen voorkomen door, zoals het EESC heeft geadviseerd, te kiezen voor een Europees eID dat voor alle lidstaten geldt. Het directe doel van de Verordening, het creëren van een uniform regime voor elektronische identificatiemiddelen, had daarmee wellicht beter verwezenlijkt kunnen worden, omdat er dan sprake zou zijn geweest van één voor iedereen bekend en betrouwbaar eID. In elk geval zal de afwezigheid van (te grote) verschillen tussen lidstaten een belangrijke factor zijn om de bovengenoemde doeleinden te bereiken.

46. Onder meer art. 3:15a-3:15c BW, art. 2:16 Awb, art. 1.1 onderdelen ss t/m yy, 2.1, 2.2, 11.5b en 18.5 t/m 18.18 Tw.
47. *Kamerstukken II* 2011/12, 22 112, nr. 1439, p. 9.
48. *Kamerstukken II* 2011/12, 22 112, nr. 1439, p. 10.
49. Zie voor deze problematiek: *Kamerstukken II* 2011/12, 22 112, nr. 1439, p. 10.
50. *Kamerstukken II* 2011/12, 22 112, nr. 1439, p. 13.