



DECOS ■ ELEKTRONISCHE HANDTEKENING

Mogelijkheden voor de private en de publieke sector

Regelgeving

De huidig geldende regelgeving voor elektronische handtekeningen is inmiddels tien jaar oud en begon bij de Richtlijn 1999/93/EG. Hiermee werd in Europees verband een richtlijn gegeven waaraan de elektronische handtekening moet voldoen. In mei 2003 werd in Nederlands de Wet elektronische handtekeningen van kracht. Dit was een wijzigingswet waarmee het concept van de elektronische handtekening werd geïntroduceerd in het Burgerlijk Wetboek en waarmee de eisen aan gekwalificeerde certificaten en certificatie-dienstverleners werden toegevoegd aan de Telecommunicatiewet. De formele juridische erkenning van de elektronische handtekening in het civiele recht is al vijf jaar een feit.

In juli 2004 werd ook de erkenning in het bestuursrecht formeel geregeld. Met de Wet elektronisch bestuurlijk verkeer werd elektronische communicatie tussen burger en bestuursorgaan onder voorwaarden erkend als geldige communicatiewijze voor bijvoorbeeld het aanvragen en verstrekken van beschikkingen. Deze wijzigingswet was een uitbreiding op de Algemene wet bestuursrecht en hiermee werd ook de elektronische handtekening erkend als geldige ondertekening in het bestuursrecht. Daardoor kan een aanvraag, bezwaarschrift of klaagschrift ook elektronisch worden ondertekend.

De volledige tekst van de regeling is terug te vinden in art. 3:15a BW, waar art. 2:16 AWB naar verwijst. Er is in het Nederlandse rechtssysteem dus één juridische regeling voor elektronische handtekeningen als implementatie van een Europese Richtlijn.

Constructie

De elektronische handtekening wordt in art. 3:15a lid 4 BW gedefinieerd als *'elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel voor authenticatie'*. Deze

gecompliceerde definitie probeert uit te drukken dat er sprake moet zijn van een elektronische authenticatie die ofwel los van het elektronische document bestaat ofwel daarvan deel uitmaakt. In het eerste geval moet er sprake zijn van een betrouwbare binding tussen de ondertekening en het document. De toelichting bij de Wet elektronische handtekeningen spreekt van *'zodanige toegangskennmerken dat de computer die deze kenmerken vergelijkt vaststelt dat zij [de ondertekening en het document] bij elkaar horen'*. Wie deze constructie goed analyseert realiseert zich dat er vele vormen van elektronische handtekening kunnen bestaan die aan deze definitie voldoen. Dat is expliciet de bedoeling van de Europese wetgever.

Deze elektronische ondertekening: *'heeft dezelfde rechtsgevolgen als een handgeschreven handtekening, indien de methode die daarbij is gebruikt voor authenticatie voldoende betrouwbaar is, gelet op het doel waarvoor de elektronische gegevens werden gebruikt en op alle overige omstandigheden van het geval'*. Opnieuw een lastige definitie. Als een elektronische handtekening wordt ingezet, in welke vorm dan ook, wordt de juridische erkenning daarvan gekoppeld aan de mate van betrouwbaarheid die gerelateerd is aan het doel van het document. Het belang en de context spelen dus een rol: een overeenkomst tot overdracht van aandelen van een BV zal anders worden beoordeeld dan een overeenkomst tot aankoop van een boek online. Hierin schuilt de kracht van deze constructie. Een aanvraag voor een parkeervergunning (die ondertekend moet zijn) zou met een eenvoudige vorm (een naam onder een e-mail bijvoorbeeld) kunnen worden ondertekend als dat binnen het vergunningsproces voldoende betrouwbaar is, gezien de lage risico's en omstandigheden. Die omstandigheden zouden bijvoorbeeld kunnen zijn dat de vergunning naar het GBA-adres van de burger wordt gestuurd, waardoor het zinloos is met een vals adres te werken.

De beoordeling van de erkenning is afhankelijk van het specifieke geval. Om meer zekerheden te bieden, worden zwaarder vormen beschreven die op voorhand als betrouwbaarder worden gezien. De hierboven beschreven definitie is die van de 'gewone' handtekening. Daarnaast bestaat de geavanceerde en de gekwalificeerde. Deze laatste is dermate zwaar dat het gebruik ervan wordt beloofd met een rechtsvermoeden: deze wordt vermoed voldoende betrouwbaar te zijn (behoudens tegenbewijs).

Vormen

Er zijn juridisch gezien drie vormen van elektronische handtekeningen, met verschillende niveaus van betrouwbaarheid. De gewone vorm bestaat uit een elektronische vorm van authenticatie, gekoppeld aan een elektronisch document. Bij gebruik van deze vorm zou uit de context moeten blijken dat de ondertekening als voldoende betrouwbaar moet worden gezien.

Daarnaast bestaat de geavanceerde vorm. Deze vorm voldoet ook aan de eisen die gesteld zijn in art. 3:15a lid 2 sub a t/m d. Zij is op unieke wijze aan de ondertekenaar verbonden, maakt het mogelijk de ondertekenaar te identificeren, komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden en is zodanig met het document verbonden dat wijziging achteraf kan worden gedetecteerd. Een voorbeeld van deze vorm is authenticatie met een PGP-key met een code van een RSA-token of dergelijke technische middelen. Er is hier sprake van een technisch hoogstaand middel waaruit de identificatie van de ondertekenaar nagenoeg onomstotelijk blijkt.

De derde en zwaarste vorm voegt eisen toe aan de geavanceerde handtekening. De gekwalificeerde elektronische handtekening heeft dezelfde kenmerken als de geavanceerde, maar maakt gebruik van een gekwalificeerd certificaat dat wordt uitgegeven door een certificatieinstantie. Zowel het certificaat als de certificatieinstantie (waarvoor de Engelse afkorting CSP wordt gebruikt) zijn aan zware eisen onderworpen, die kunnen worden teruggevonden in het Besluit elektronische handtekeningen. Alleen deze vorm krijgt het rechtsvermoeden uit art. 3:15a lid 2 BW.

Bewijsovereenkomst en 'betrouwbaarheidsbeding'

Partijen die in elektronische communicatie de onzekerheid over de betrouwbaarheid willen wegnemen, kunnen dat bij overeenkomst doen. Een overeenkomst (of de algemene voorwaarden die daarvan deel uitmaken) kan bijvoorbeeld een bepaling bevatten die stelt dat tussen partijen een bepaalde vorm van elektronische ondertekening als voldoende betrouwbaar moet worden gezien. Bijvoorbeeld iedereen die elektronisch bankiert, heeft

een algemene voorwaarde geaccepteerd waarin dit staat. Dit 'betrouwbaarheidsbeding' is mogelijk op grond van art. 3:15a lid 6 en is een speciale vorm van de algemene constructie van de bewijsovereenkomst. Hiermee kunnen partijen vastleggen dat een bepaald bewijs tussen partijen zal worden erkend (typisch is bijvoorbeeld dat de gegevens van de bank tussen bank en klant als bewijs zal gelden).

Bestuursrecht

De overheid kan op grond van art. 2:16 AWB werken met dezelfde constructie. In de AWB wordt voor de communicatie van burger naar overheid wel een ondertekening vereist (aanvraag, bezwaar- en klagschrift), maar niet voor communicatie van overheid naar burger (besluit). Dit betekent dat de vraag welke ondertekening de overheid van de burger accepteert net zo belangrijk is als de vraag welke ondertekening de overheid zelf gebruikt. In het bestuursrecht is er geen vorm gelijk aan de algemene voorwaarden die in het civiele recht de ideale plek bieden om hier afspraken over te maken. De overheid kan wel met de ondertekening aanhaken bij de spelregels voor elektronisch verkeer. Het is mogelijk om per proces vast te stellen dat het bestuursorgaan 'langs elektronische weg beschikbaar is'. Deze mogelijkheid moet aan de burger worden gecommuniceerd, zodat deze burger kan kiezen tussen traditionele en elektronische communicatie. In deze publicatie kan het bestuursorgaan meteen meenemen welke vorm van ondertekening als voldoende betrouwbaar zal worden erkend: vanzelfsprekend kan dit ook per proces verschillen (al naar gelang het betrokken belang). Zo kan een bestuursorgaan op een website bij de pagina over de parkeervergunning stellen dat elektronische aanvraag mogelijk is, waarbij alleen DigiD als authenticatie wordt geaccepteerd.

Technieken

In de drie verschillende juridische categorieën van elektronische handtekeningen bestaan vele technieken. In de laagste groep, de gewone handtekening, zijn de technische mogelijkheden eindeloos, aangezien letterlijk iedere vorm van authenticatie kan volstaan. Met de nadruk op *kan*. DigiD is binnen de overheid de bekendste in deze categorie, maar ook een naam onder een e-mail, een gescande handtekening of een username/password kan worden toegepast. Meer geavanceerde technieken zoals PGP-keys, RSA-tokens, smartcards en dergelijke leveren een hogere mate van betrouwbaarheid en zullen dus ook een hogere juridische waardering verdienen. In de topcategorie is eigenlijk PKI (met gekwalificeerde certificaten) de enig toegepaste techniek, waarbij op de Nederlandse markt slechts een handvol CSP's zijn betrokken.

Conclusie

De regelgeving laat expliciet ruimte voor een brede toepassing waarbij vele verschillende technieken kunnen worden toegepast. Bij de huidige stand van zaken wordt vooral de zwaarste categorie binnen de overheid als oplossing aangeboden, waarbij nog weinig organisaties daadwerkelijk de elektronische handtekening gebruiken. Vooralsnog schijnt daarbij niet zozeer de techniek of de juridische erkenning het probleem te zijn, maar de 'gewenning' door de organisatie. In de particuliere sector, vooral in de financiële hoek, is elektronische ondertekening veel gebruikelijker. Het betrouwbaarheidsbeding in de algemene voorwaarde biedt daarbij de gezochte zekerheid. Voor overheden valt van dat gebruik een hoop te leren.

© Copyright 2008 Decos Software Engineering B.V.,
ir. F.P.A. Dondorp BL, afd. Business Development.

Auteursrecht voorbehouden. Behoudens uitzonderingen door de wet gesteld mag zonder voorafgaande toestemming van Decos Software Engineering B.V. niets uit deze publicatie worden veelevoudigd, gepubliceerd of zonder bronvermelding worden hergebruikt. Voor aanvullende informatie en toestemming kunt u zich wenden tot de afdeling Business Development, tel. 071-3640700, info@decos.com.

