Met EEN *elektronische handtekening koop* JE *nog* GEEN *veiligheid*

mr. F.W. (Friso) de Jong

mr. F.W. (Friso) de Jong is directeur van Silverback B.V. Silverback houdt zich onder meer bezig digitale handtekeningen, digitaal factureren en juridische diensten op het gebied van beveiliging en privacy. Voor meer informatie jong@silver-back.nl

"Zelfs al zijn alle deskundigen het met elkaar eens, dan hoeven ze nog geen gelijk te hebben", aldus Bertrand Russell, een bekende Engelse filosoof. Hij wilde hiermee duidelijk maken dat er een verschil bestaat tussen wat theoretisch en praktisch gezien de beste oplossing voor een probleem is.

Dat gaat op dit moment ook op voor digitale handtekeningen (zie kader). In theorie is de digitale handtekening op basis van een gekwalificeerd certificaat (hierna: de gekwalificeerde handtekening) de beste oplossing. Dit komt onder meer door het grote aantal waarborgen dat verbonden is aan dit type handtekening. De schaduwzijde van deze waarborgen is dat dergelijke handtekeningen erg duur zijn. In sommige gevallen worden zelfs enkele honderden euro's in rekening gebracht. Daarmee is wat in theorie de beste oplossing is, in de praktijk niet meer dan een duur alternatief, vergeleken met de veel minder dure technisch geavanceerde digitale handtekening (hierna: geavanceerde handtekening). Maar wanneer moet je welke handtekening gebruiken?

Voor het antwoord op die vraag biedt de wet, waarin de digitale handtekeningen worden geregeld en die op 21 mei 2003 in werking is getreden, een goed beoordelingskader. Een bepaling in die wet zegt dat het van een aantal punten afhangt of een elektronische handtekening dezelfde geldigheid heeft als een geschreven handtekening.

Allereerst hangt het af van de methode voor authenticatie. Die zal waarschijnlijk voldoende betrouwbaar te zijn als de elektronische handtekening aan een zestal eisen voldoet (zie kader). Maar, als er geen sprake is van een gekwalificeerd certificaat of gecertificeerde dienstverlener of van een veilig middel dan is een digitale handtekening niet meteen onvoldoende betrouwbaar.
Het hangt dan af van het doel waarvoor de elektronisch te verzenden gegevens worden gebruikt en van alle overige omstandigheden van het geval, aldus de wettelijke bepaling.

Deze bepaling is erg belangrijk; het bepaalt dat een elektronische handtekening niet steeds ongeldig kan worden verklaard, alleen maar omdat aan een of meer van de zes voorwaarden niet is voldaan en er dus geen sprake is van een gekwalificeerde handtekening. Met ander woorden: de wet rammelt aan de poorten van iedereen die juist op basis van diezelfde wet –probeert te- beweren, dat alleen een gekwalificeerde handtekening zorgt voor betrouwbaarheid en zekerheid. Voorbeelden daarvan zijn de overheid. Terwijl diezelfde overheid – de belastingdienst- nog gewoon een gebruikersnaam en een wachtwoord verlangt bij je online belastingaangifte.

Welke omstandigheden spelen dan een rol om een handtekening, niet zijnde een gekwalificeerde handtekening, als voldoende betrouwbaar aan te merken? Allereerst is dat de contractsvrijheid van partijen. De toelichting bij de wet maakt duidelijk dat het partijen vrij staat om onderling overeen te komen of zij elektronisch ondertekende gegevens zullen aanvaarden en, zo ja, onder welke voorwaarden. Zo kunnen partijen in contract vastleggen dat zij gebruik maken van de minder dure geavanceerde handtekening. Uiteraard moet dit wel in toegestaan zijn in het geldende nationale recht, zeker als de partijen uit verschillende EU-lidstaten komen. De afspraak tussen partijen kan dus meebrengen dat, hoewel geen gebruik is gemaakt van een gekwalificeerde handtekening, er toch sprake is van voldoende betrouwbaarheid en veiligheid en dus dat de gebruikte handtekening dezelfde geldigheid heeft als een geschreven handtekening. Een gekwalificeerde handtekening is dan zeker niet nodig.

Op de tweede plaats: de aard van de te verzenden gegevens. Heel vaak zal men betogen dat, vanwege de aard van de gegevens, alleen een gekwalificeerde handtekening de betrouwbaarheid voldoende waarborgt. Maar het is nog steeds zo dat de zwakste schakel de kracht van ketting bepaalt. En als de organisatorische, juridische en overige technische aspecten binnen de organisatie van de gebruiker niet goed zijn geregeld, dan kan de gekwalificeerde handtekening nog met zoveel waarborgen zijn omgeven, het dan is dat zeker geen waarborg voor voldoende betrouwbaarheid. Met een gekwalificeerde handtekening koop je geen betrouwbaarheid, daarvoor is meer nodig.

Verder speelt het doel waarvoor de elektronische gegevens

Digitale en elektronische handtekeningen volgens wetgeving

Centraal in de wet staat de bepaling die de voorwaarden beschrijft wanneer een elektronische handtekening net zo betrouwbaar is als een normale handtekening. De wet maakt onderscheid tussen een 'gewone' elektronische handtekeningen en een geavanceerde elektronische handtekening. Een ingescande handtekening is een voorbeeld van een gewone elektronische handtekening. De digitale handtekening is een van de meest gangbare vormen van een geavanceerde elektronische handtekening.

Bij digitale handtekeningen spreken we over een standaard digitale handtekening, over een technisch geavanceerde digitale handtekening (de geavanceerde handtekening) en over een digitale handtekening gebaseerd op een gekwalificeerd certificaat (de gekwalificeerde handtekening). Bij alle typen digitale handtekeningen wordt gebruik gemaakt van twee sleutels, een publieke en een private sleutel, die onlosmakelijk met elkaar zijn verbonden en die uniek zijn voor een (rechts)persoon. Welke publieke sleutel bij welke (rechts)persoon hoort, wordt door degene die de sleutel aanmaakt, vastgelegd in een digitaal certificaat.

De standaard digitale handtekening vormt de basis en voldoet aan de voorwaarde dat er gebruik wordt gemaakt van een publieke en private sleutel. Een geavanceerde handtekening en de gekwalificeerde handtekening moeten aan meer voorwaarden voldoen. Een gekwalificeerde handtekening moet aan zes voorwaarden voldoen, die in de wet staan vermeld:

- het is op unieke wijze aan de ondertekenaar verbonden;
- het maakt het mogelijk de ondertekenaar te identificeren;
- het komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
- het is zodanig verbonden aan het bestand waarop het betrekking heeft dat elke wijziging achteraf kan worden opgespoord;
- het is gebaseerd op een gekwalificeerd certificaat;
- het is gegenereerd door een veilig middel.

De laatste twee voorwaarden vormen de basis voor twee bijlagen, waarin nog eens dertig extra waarborgen zijn opgenomen. De geavanceerde handtekening hoeft "alleen maar" te voldoen aan de eerste vier voorwaarden.

worden verzonden een rol. Stel dat het doel is het verzenden van een digitale factuur, dan volstaat een geavanceerde handtekening, volgens de Minister van Financiën. Maar gaat het om het afgeven van beschikkingen door een gemeente aan een burger (bijvoorbeeld een visvergunning), dan wordt het een ander verhaal. Het afgeven van een beschikking heeft juridische gevolgen voor degene aan wie de beschikking is gericht. Voor die gevallen is een gekwalificeerde handtekening noodzakelijk, aldus de wetgever. Het uitgangspunt zou voorlopig moeten zijn dat wanneer een wetgever een gekwalificeerde handtekening niet verplicht heeft gesteld, een geavanceerde handtekening volstaat. Het aantal keren dat de wetgever dit heeft vastgelegd is tot nu toe op de vingers van een hand te tellen.

Tot slot is er het vangnet van "de omstandigheden van het geval". Zo kan het zijn dat het netwerk waarover wordt gecommuniceerd, al zo veilig is dat een gekwalificeerde handtekening niet nodig is. Denk daarbij aan het C2000 netwerk van de hulpdiensten in Nederland. Een ander voorbeeld is het gebruik van een extreem lange sleutellengte bij het zetten van digitale handtekening, of een zware vorm van EDI. De duur en de aard van de communicatie kan ook een dergelijke omstandigheid vormen. Wat als er maar een keer een berichtje wordt verzonden? Moet er dan toch een gekwalificeerde handtekening aan te pas komen? Het lijkt mij van niet.

Er bestaat dus een algemene norm in de wet, die bepaalt dat een elektronische handtekening gelijk staat aan een handgeschreven handtekening, als die elektronische handtekening, gelet op de punten hierboven, voldoende betrouwbaar dezelfde functies kan vervullen als een handgeschreven handtekening. Deze norm is heel ruim, waardoor het in een juridisch conflict een rechter of arbiter veel een flexibiliteit en vrijheid biedt. En dat is precies wat nodig is om conflicten te beoordelen waarin communicatie, voorzien van een elektronische handtekening, een rol speelt.

De rechter of arbiter gaat daarbij overigens uit van het 'open bewijsstelsel'. Dit betekent dat bewijs kan worden geleverd door alle middelen die zich daarvoor lenen. De waardering van de diverse bewijsmiddelen is vervolgens overgelaten aan de rechter. Een rechter kan dan tot de slotsom komen dat zelfs een gekwalificeerde handtekening onvoldoende bewijs biedt. Niet vanwege de handtekening zelf, maar vanwege het proces waarin de handtekening is gebruikt.

Ondanks de nadruk op de gekwalificeerde handtekening, is het verstandig om op basis van bovenstaande punten na te gaan welk type handtekening volstaat voor de bescherming van de behoeften en belangen. Deze uitgangspunten zijn dezelfde als die de rechter zal gebruiken in geval van een conflict. In de meeste gevallen zal een geavanceerde digitale handtekening volstaan en is een gekwalificeerde handtekening nog niet nodig.