



ICTRECHT

Rechtsgeldigheid n-Digisign handtekeningen

Het product n-Digisign is een toevoeging op het n-Office pakket waarmee handtekeningen (en parafen) kunnen worden geplaatst onder Word-documenten. De vraag van n-tree is onder welke omstandigheden een dergelijke handtekening als juridisch equivalent aan een ‘papieren’ handtekening te zien is. ICTRecht heeft het n-Digisign pakket geanalyseerd.

Conclusie

De conclusie van ICTRecht is dat de handtekening die gezet wordt middels n-Digisign kan worden gekwalificeerd als een geavanceerde elektronische handtekening. Dit wil zeggen dat deze handtekening in beginsel net zo rechtsgeldig is als een “papieren” handtekening. Mocht een rechter deze interpretatie niet volgen, dan kan de handtekening altijd nog worden gekwalificeerd als een “gewone” elektronische handtekening.

Het is voor zowel de “gewone” als de “geavanceerde” elektronische handtekening belangrijk dat er zorgvuldige interne processen worden gedefinieerd voor invoering en beheersing van het n-Digisign traject. De softwaremodule biedt de organisatie ruime mogelijkheden voor een inrichting met de juiste autorisaties. De inrichting en deze processen zullen in belangrijke mate bijdragen aan de bepaling bij de rechter of de handtekeningen werkelijk dezelfde rechtsgevolgen hebben als een “papieren” elektronische handtekening.

Hieronder lichten wij dit nader toe.

1. Elektronische handtekening

De wet erkent een ‘elektronische’ handtekening onder omstandigheden als rechtsgeldig. Om de rechtsgeldigheid van een elektronische handtekening die gezet is met gebruikmaking van n-Digisign aan te tonen, wordt n-Digisign aan de hand van de Wet elektronische handtekeningen besproken. Allereerst wordt uitgelegd wat onder een elektronische handtekening wordt verstaan. Daarbij wordt gekeken naar de rechtsgevolgen. Vervolgens zal de elektronische handtekening worden gekwalificeerd.

1.1. Definitie van elektronische handtekening

De definitie van de elektronische handtekening is te vinden in 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 dient dus te gaan om elektronische gegevens die zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens. Dit kan in principe alles zijn. Zo zou een met een muis of pen/tablet gemaakte tekening van een handtekening, of een ingescande handtekening die met inkt is gezet onder deze definitie kunnen vallen. Wel is er vereist dat deze gegevens ‘vastgehecht of logisch geassocieerd’ zijn met andere gegevens, zoals een tekst of afbeelding. Een gescande handtekening (elektronische gegevens), die niet wordt gekoppeld aan andere elektronische gegevens (bijvoorbeeld een tekstdocument) kan nog niet worden aangemerkt als een elektronische handtekening.



ICTRECHT

1.2. Gewone elektronische handtekening

Een handtekening die alleen aan de definitie van een elektronische handtekening voldoet, wordt ook wel de “gewone” elektronische handtekening genoemd. Wanneer bij een elektronische handtekening gebruik wordt gemaakt van aanvullende technische middelen (zoals bijvoorbeeld smartcards en publieke/private sleutelparen) wordt gesproken van een “geavanceerde elektronische handtekening”. Dit komt overeen met wat in de beveiligingswereld als de “digitale handtekening” wordt aangeduid.

1.3. Geavanceerde elektronische handtekening

Van een “geavanceerde elektronische handtekening” is volgens lid 2 van artikel 3:15a BW sprake indien de handtekening op unieke wijze aan de ondertekenaar is verbonden, zij het mogelijk maakt de ondertekenaar te identificeren, zij tot stand is gekomen met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden en zij op zodanige wijze aan de gegevens waarop zij betrekking heeft is verbonden, dat elke wijziging achteraf van gegevens kan worden opgespoord. Men denkt hierbij in het bijzonder aan handtekeningen die met behulp van publiek/private sleutelparen en certificaten kunnen worden geplaatst, maar de definitie is daar niet toe beperkt.

2. Rechtsgevolgen

De rechtsgevolgen van de elektronische handtekening staan eveneens in artikel 3:15a, lid 1 BW:

“Een elektronische handtekening 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.”

De methode voor authenticatie moet voldoende betrouwbaar zijn. Dit slaat met name op het uitgifteproces. Een elektronische handtekening die je aan jezelf geeft is onbetrouwbaar. Een elektronische handtekening, die met behulp van n-Digisign wordt geplaatst, kan pas als methode voor authenticatie dienen als de gebruiker geen mogelijkheid heeft om zijn gescande handtekening toe te voegen. Dat dient de beheerder éénmalig te doen. Dat geldt tevens voor de gebruikersnaam en het wachtwoord, die vervolgens aan de gebruiker worden verstrekt om de handtekening daadwerkelijk te kunnen plaatsen.

Wanneer een systeem voor het plaatsen van geavanceerde elektronische handtekeningen wordt gebruikt, wordt krachtens lid 2 van artikel 3:15a BW deze handtekening vermoed voldoende betrouwbaar te zijn. Dat wil zeggen dat een persoon die betwist dat de handtekening frauduleus is gezet, zelf zal moeten aantonen dat niet aan de eisen uit leden 1 en 2 van artikel 3:15a BW wordt voldaan. Bij een gewone elektronische handtekening moet de plaatser van de handtekening aantonen dat het proces voldoende betrouwbaar is verlopen.

3. Kwalificatie van de n-Digisign handtekening

De n-Digisign handtekening gebruikt een plaatje van een “papieren” handtekening, hetgeen als “elektronische gegevens” aan te merken is in de zin van de wet. Omdat het pakket de handtekening invoegt in een Word-document, is deze daarmee “vastgehecht aan” of “logisch



ICTRECHT

geassocieerd met” het document. En als laatste wordt het plaatje gebruikt “als middel voor authenticatie”. Daarmee is aan alle eisen uit de wet voldaan zodat de n-Digisign handtekening een elektronische handtekening in de zin van lid 4 van artikel 3:15a BW is.

3.1. n-Digisign als gewone elektronische handtekening

De volgende vraag is dan of deze elektronische handtekening rechtsgeldig is. De n-Digisign handtekening is in ieder geval een ‘gewone’ elektronische handtekening. Deze is, zoals hierboven uiteen gezet, onder omstandigheden net zo rechtsgeldig als een gewone papieren handtekening. Het doel en de overige omstandigheden van het geval spelen daarbij een belangrijke rol.

Het doel van de handtekening is in principe iets dat de organisatie bepaalt die het n-Digisign pakket inzet. Hier valt dus moeilijk in het algemeen iets over te zeggen. In privaatrechtelijke verhoudingen, bijvoorbeeld bij het plaatsen van bestellingen of het ondertekenen van contracten, geldt echter geen algemene verplichting om een handtekening te zetten om ergens mee akkoord te gaan. De handtekening dient daar als doel om te bevestigen dat men nu écht akkoord is. Voor dat doel biedt het n-Digisign pakket voldoende zekerheid door de interne audit trail.

Dit audit trail en de andere borgen die in n-Digisign en het achterliggende n-Office pakket zijn ingebouwd vallen onder de “omstandigheden van het geval” zoals in dit wetsartikel bedoeld. Hierbij geldt wel dat veel af zal hangen van de implementatie die de gebruikersorganisatie kiest. Het moet bijvoorbeeld voorkomen worden dat iedereen handtekeningen voor willekeurige andere gebruikers in het systeem kan plaatsen of wijzigen. Ook het autoriseren (delegeren of machtigen) van andere personen moet streng worden gecontroleerd. Er is niets in n-Digisign dat hierin een hinderpaal vormt.

3.2. n-Digisign als geavanceerde elektronische handtekening

Voor meer rechtszekerheid zou het wenselijk zijn als de n-Digisign handtekening ook als geavanceerde elektronische handtekening kan worden gekwalificeerd. Hieronder analyseren wij kort de eisen uit het wetsartikel:

- *zij is op unieke wijze aan de ondertekenaar verbonden;*

De elektronische handtekening is op een unieke wijze aan de ondertekenaar verbonden, omdat deze door de ondertekenaar alleen met een gebruikersnaam en wachtwoord kan worden gezet.

- *zij maakt het mogelijk de ondertekenaar te identificeren;*

Bij het aanmaken van een nieuwe gebruiker zal de gebruiker eerst moeten worden geïdentificeerd door de beheerder. De beheerder verstrekt een gebruikersnaam en wachtwoord en koppelt de gescande handtekening aan de gebruiker. Tijdens het ondertekeningsproces moet de gebruiker een wachtwoord opgeven. Hiermee wordt de ondertekenaar geïdentificeerd. Daarnaast kan de ondertekenaar worden geïdentificeerd door middel van de gescande handtekening, die door n-Digisign in het document wordt geplaatst.



ICTRECHT

- *zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden; en*

De ondertekenaar (gebruiker) kan de elektronische handtekening onder zijn uitsluitende controle houden door het beheer- en het ondertekenaarwachtwoord geheim te houden.

- *zij is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf van de gegevens kan worden opgespoord*

De documenten die door middel van n-Digisign worden ondertekend, zijn beveiligd met door de software gegenereerd wachtwoord en bevatten op de achtergrond een “audittrail” waarin iedere actie is vastgelegd. Hierdoor is het mogelijk om wijziging van de gegevens achteraf op te sporen.

Aan alle eisen uit de wet wordt derhalve voldaan. Wel zal uit de analyse duidelijk zijn dat wederom veel afhangt van het proces waarmee n-Digisign wordt ingevoerd en handtekeningen worden beheerd. Men zal zorgvuldige interne processen moeten invoeren om de juiste handtekeningen in n-Digisign te importeren en om te zorgen dat alleen werkelijk geautoriseerde personen deze kunnen plaatsen. Een verkeerd geïmplementeerd proces kan de rechtsgeldigheid van handtekeningen aantasten.