Vinkje, krabbel of digitale handtekening?

Welke bewijskracht is voldoende voor mijn digitale proces?

Het antwoord op vier veelgestelde vragen:

1. Welk document vraagt welke bewijskracht?
2. Wat is rechtsgeldig?
3. Welke vormen van digitale handtekeningen kennen we?
4. Welke eisen worden daaraan gesteld?

Ondertekenen.nl

Aangezien de elektronische handtekening dezelfde juridische waarde heeft als de handgeschreven handtekening, staat een digitaal ondertekend document juridisch gelijk aan een schriftelijk ondertekend document. De elektronische handtekening moet dan wel voldoen aan de eisen die de wetgever stelt.

Inhoud

Inleiding

Steeds meer organisaties digitaliseren hun primaire processen. Ook de contracten, verklaringen, offertes en andere belangrijke documenten waar rechtszekerheid van belang is, gaan steeds meer digitaal. Maar hoe zit het eigenlijk met de rechtsgeldigheid en bewijskracht van deze documenten in digitale vorm?

De markt voor het plaatsen van digitale handtekeningen maakt momenteel een stormachtige ontwikkeling door. Steeds meer organisaties zijn in staat om de juiste afweging te maken tussen het risico van de transactie en de bewijskracht die noodzakelijk is in het digitale proces. De wet – en mogelijk ook de toezichthouder – stelt namelijk wel strikte eisen aan de digitale handtekening en voor ieder proces is het belangrijk om de juiste afwegingen te maken.

Welk document vraagt welke bewijskracht? Wat is rechtsgeldig, welke vormen van digitale handtekeningen kennen we, welke eisen worden daaraan gesteld en waarop moet worden gelet bij de selectie van een oplossing voor het plaatsen van digitale handtekeningen? Op deze vraagstukken gaan we in deze whitepaper dieper in.

Opmars digitale handtekening

Verschillende marktonderzoeksbureaus dichten de ‘digitale handtekening’ een gouden toekomst toe. Deze populariteit is eenvoudig te verklaren. Door de opkomst van het internet zijn brieven en papieren contracten vervangen door e-mail en digitale documenten, en die zijn lastig te ondertekenen met een fysieke handtekening.
De digitale of elektronische handtekening biedt daarnaast enkele andere voordelen ten opzichte van de traditionele variant:

- Een digitale handtekening is sneller te plaatsen; het is niet nodig om een document te printen, ondertekenen en per post terug te sturen naar de afzender.
- Een digitale handtekening zorgt voor een grote kostenbesparing. De kosten voor het printen, versturen, ondertekenen, terugsturen en inscannen van een papieren document lopen al snel op tot 3 euro. Met een digitale handtekening kan naar schatting zo’n 75 procent op de kosten worden bespaard.

  Het is bijvoorbeeld niet nodig om een envelop met daarin geprinte en ondertekende documenten te frankeren en het aantal administratieve handelingen wordt aanzienlijk teruggedrongen.
- Een digitale handtekening biedt een grotere controle over het proces.
  Het digitale document kan als het ware worden gevolgd.
- Een digitale handtekening voorkomt papierverspilling.

Is een vinkje goed genoeg?

Voor de rechtsgeldigheid van een overeenkomst is het lang niet altijd nodig om een digitale handtekening onder het document te plaatsen. Volgens de wet is een overeenkomst immers in beginsel 'vormvrij'. Dit houdt in dat partijen op iedere gewenste manier een overeenkomst kunnen sluiten, zelfs via gebarentaal of stilzwijgend. Ook een e-mail met daarin een omschrijving van de overeenkomst en een 'akkoord' voor de aanvaarding van de overeenkomst is volgens de wet rechtsgeldig, evenals een vinkje bij 'akkoord' in een webformulier. Op het moment dat een van beide partijen onder de overeenkomst uit wil, kunnen echter problemen ontstaan. Het is dan bijvoorbeeld lastig om te bewijzen dat een koper een e-mail met daarin 'akkoord' daadwerkelijk heeft verstuurd, of daadwerkelijk het vinkje heeft geplaatst.

Een elektronische handtekening kan dan uitkomst bieden. De ontvanger van de handtekening kan hiermee bewijzen dat een bericht of akkoord van de verzender afkomstig is. De bewijskracht hangt echter af van de manier waarop de elektronische handtekening is geplaatst.

Rechtsgeldige elektronische handtekeningen

De wet elektronische handtekening is al sinds 1999 actief op basis van de Europese Richtlijn. Sinds juli 2016 is deze Europese richtlijn opgegaan in de nieuwe Europese eIDAS-verordening. Hierbij is de richtlijn samengevoegd met de eisen voor digitale identiteiten in Europa en zijn er aanvullende trustdiensten gedefinieerd naast de digitale handtekening, zoals de digitale tijdstempel en aangetekend versturen van documenten.

> 'Volgens de wet kunnen alle overeenkomsten elektronisch tot stand worden gebracht'

Op basis van deze eIDAS-verordening zal ook de wet worden aangepast en meer worden verwezen naar de eIDAS-richtlijn. Feitelijk blijft de indeling voor de digitale handtekening in tact en kan een elektronische handtekening volgens de Wet Elektronische Handtekening (Burgerlijk Wetboek, artikel 15a) grofweg drie verschillende vormen aannemen:

1. **De gewone elektronische handtekening.** Dit is de eenvoudigste variant. Het gaat hier om iedere vorm van 'ondertekening' die de plaatser identificeert en iets zegt over de integriteit van het bericht. Een gewone elektronische handtekening is bijvoorbeeld een scan van een gewone handtekening die in het document wordt geplaatst, of een 'krabbel' gemaakt met de muis.

2. **De geavanceerde elektronische handtekening.** Bij de geavanceerde handtekening ligt de nadruk op de betrouwbaarheid van het proces.

   De volgende onderdelen spelen een rol bij het bepalen van de mate van betrouwbaarheid, bewijskracht:
   1. Zij is op unieke wijze aan de ondertekenaar verbonden;
   2. Zij maakt het mogelijk de ondertekenaar te identificeren;
   3. Zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden; en
   4. Zij is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden (Associatie), dat elke wijziging achteraf van de gegevens kan worden opgespoord.

   Hiervoor maakt de geavanceerde elektronische handtekening gebruik van wiskundige technieken voor het koppelen van een unieke code aan een bericht. Deze code wordt afgeleid uit het bericht zelf en uit de identiteit van de afzender. De associatie van het bericht en de code gaat met een digitale sleutel. Daarmee is de code niet bruikbaar bij een vervalst bericht.

3. **De gekwalificeerde elektronische handtekening.** Evenals bij de geavanceerde handtekening is ook bij de gekwalificeerde handtekening de betrouwbaarheid van het proces het uitgangspunt. Het verschil is dat bij een gekwalificeerde elektronische handtekening een gekwalificeerd certificaat wordt gebruikt voor het identificeren van de ondertekenaar. Daarnaast wordt het gekwalificeerde certificaat uitgegeven op een betrouwbaar middel, waarmee de ondertekenaar de associatie van zijn identiteit en het document met een persoonlijke sleutel kan doen in plaats van een algemene sleutel. Er zijn speciale instanties die certificaten uitgeven, de zogeheten certificatiedienstverleners. De Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA) controleert de certificatiedienstverleners.

Veel organisaties denken dat de digitale handtekening een gescande variant van je papieren handtekening is. Bij een digitale handtekening komt meer kijken dan het vervangen van de papieren handtekening door een gescande handtekening of een krabbel via touch of muis.
Zivko Lazarov, oprichter Evidos – Ondertekenen.nl

Betrouwbaarheid van het proces bepaalt de bewijskracht

Deze drie vormen zijn volgens de wet allemaal rechtsgeldig, maar vertegenwoordigen een andere bewijskracht.

Zo blijft het bij een gescande handtekening lastig om bij een meningsverschil te bewijzen dat de verzender de persoon is die daadwerkelijk de handtekening heeft geplaatst. Bij een 'geavanceerde elektronische handtekening' of een 'gekwalificeerde elektronische handtekening' is dit wel vast te stellen. In alle gevallen staat of valt de bewijskracht echter met de betrouwbaarheid van het onderliggende proces.

"Door de huidige manier van digitaal ondertekenen heeft Nationale Waarborg een nog beter controlemiddel via een transactiebon van de digitale ondertekening en daarmee de zekerheid dat de bankgarantie door de juiste personen daadwerkelijk ondertekend is."
Marjolein van Buuren van Nationale Waarborg.

De betrouwbaarheid van het proces en de bewijskracht wordt bepaald door de volgende onderdelen:

1. Hoe sterk zijn de identificerende kenmerken van de ondertekenaar en hoe goed heeft hij deze onder zijn eigen uitdrukkelijke controle?
2. Is duidelijk vastgelegd welke processtappen de gebruiker heeft doorlopen voor het ondertekenen?
3. Op welk tijdstip heeft de ondertekening plaatsgevonden en kan dit op een later moment ook worden aangetoond?
4. Voldoet het document aan het juiste formaat om duurzaam aan te tonen dat het document digitaal ondertekend is?
5. Hoe sterk is het mechanisme dat is gebruikt om de identificerende gegevens onlosmakelijk te verbinden met het document (Associatie), de sterkte van de cryptografie, zodat dit niet eenvoudig kan worden aangepast?

Sterke identificerende kenmerken

Voorbeelden van identificerende kenmerken op het Internet zijn bijvoorbeeld een email adres, ip adres, mobiel nummer, DigiD, iDIN, eHerkenning of een gekwalificeerd certificaat. Het is ook mogelijk om een aantal identificerende kenmerken te "stapelen", de combinatie zorgt voor een sterkere identificatie. Bij het ondertekenen van het bericht dient de ondertekenaar te kunnen beschikken over deze middelen, het is belangrijk om hier rekening mee te houden. Zo kan de bewijskracht van een gekwalificeerd certificaat wellicht hoger zijn, maar wanneer eindgebruikers hier niet over beschikken of het aanvraagproces enkele dagen in beslag neemt, dan zal de eindgebruiker niet kunnen ondertekenen.

Processtappen van het ondertekenproces

Voor het ondertekenproces is het belangrijk dat de ondertekenaar bewust is van het document hij gaat ondertekenen. Welke documenten zijn getoond en is er een expliciet moment dat de ondertekenaar bewust (wilsuiting) het document heeft ondertekend?

Tijdstip

Voor de betrouwbaarheid van het ondertekenproces en de bewijskracht is het belangrijk om ook het tijdstip van ondertekening op een onafhankelijke manier vast te stellen en op te nemen in de handtekening. Zo kan er geen dispuut ontstaan over het moment van ondertekenen, dan wel dat de ondertekening op een ander tijdstip is uitgevoerd.

‘Als het proces niet goed is afgedekt, dan is zelfs bij de gekwalificeerde elektronische handtekening de bewijskracht laag’’

Technische standaard PADES - XADES

In de standaarden van de digitale handtekening en vereisten van eIDAS wordt gesproken over het XADES of PADES formaat. Feitelijk is dit de technische standaard hoe in het document een juiste digitale handtekening in PDF of XML formaat kan worden gezet. Deze standaarden zorgen ervoor dat de digitale handtekeningen op een standaard manier kunnen worden gecontroleerd door diverse computer programma’s zoals bijvoorbeeld de Adobe PDF reader. Ook zorgt de standaard ervoor dat de digitale handtekeningen in de documenten ook in de toekomst nog altijd op een goede en betrouwbare manier kunnen worden gecontroleerd.

Vasthechten van identificerende kenmerken aan het document

Voor het vasthechten van de identificerende kenmerken aan het document wordt een PKI sleutel gebruikt. Het vasthechten wordt ook wel associatie genoemd. In het geval dat de gebruiker een gekwalificeerd certificaat op een betrouwbaar middel heeft, dan kan deze sleutel worden gebruikt voor de associatie. In andere gevallen kan de associatie gedaan worden met een algemene sleutel. Het is belangrijk dat deze sleutel op een hoogwaardige manier is afgeschermd, bijvoorbeeld op een elektronische chip in een smartcard, usb of hardware security module. Wanneer deze sleutel niet goed is afgeschermd kunnen onbevoegden ook de associatie hebben uitgevoerd. De lengte van de sleutel is ook belangrijk, door een eenvoudige sleutel kan de associatie en verzegeling eenvoudiger worden verbroken.

Alle elektronische handtekeningen kunnen een rechtsgeldigheid hebben en dienen als bewijsmiddel. Alleen het feit dat ze elektronisch zijn of niet voldoen aan de eisen voor gekwalificeerde elektronische handtekeningen, doet daar niets aan af. Als de betrouwbaarheid van het proces niet goed is afgedekt, dan bestaat zelfs bij het gebruik van het gekwalificeerde certificaat de mogelijkheid dat de bewijskracht laag is. Een goede vastlegging van de betrouwbaarheid van het proces van ondertekenen is belangrijk voor de toetsing door een onafhankelijke partij, zoals een rechter.

Hoe bepaal ik de juiste handtekening en bewijskracht voor mijn documenten?

Is een handtekening wel nodig?
Binnen organisaties zijn er verschillende bedrijfsprocessen waar documenten digitaal ondertekend kunnen worden. Enerzijds in ondersteunende processen zoals inkoop, HR en financiën. Anderzijds in het primaire proces van de dienstverlener zoals het uitzenden van personeel, verkoop of verhuur van huizen, leveren van verzekeringen of andere dienstverlening.

De belangrijkste vraag om mee te starten, is of een handtekening überhaupt noodzakelijk is. In sommige gevallen is de handtekening zoals die op papier wordt gezet meer een formaliteit of ceremonieel van aard. Hierdoor kan het zijn dat deze in het digitale proces niet relevant is, bijvoorbeeld omdat de papieren handtekening dient om de afkomst van een brief te duiden en dat dit digitaal via een met SSL beveiligd portaal van de organisatie kan gebeuren.

Ook is het belangrijk om te kijken of de digitale handtekening wordt gebruikt buiten de context van het bedrijf. Zo zouden documenten die nu binnen de organisatie ondertekend dienen te worden voor autorisatie door twee medewerkers, in een digitale variant prima via het lokale intranet en een inlogcode kunnen verlopen.

Daar waar de documenten buiten de context van het bedrijf komen en bewijskracht relevant is, kan de digitale handtekening vereist zijn.

Welke niveau digitale handtekening is relevant voor mijn documenten?
De risico's van een transactie, of bijvoorbeeld de eisen vanuit de toezichthouder, bepalen de eisen die worden gesteld aan de bewijskracht. De keuze voor een oplossing voor het plaatsen van elektronische handtekeningen hangt dus samen met de risicoafweging. Het is dus verstandig om betrouwbare elektronische handtekeningen te gebruiken als er grote belangen in het spel zijn. Zo zal bij het boeken van een campingplaats een vinkje al ruimschoots voldoende zijn, terwijl bij een huurovereenkomst voor een woning een geavanceerde elektronische handtekening meer voor de hand ligt.

> 'Bij de rechtsgeldigheid van een digitale transactie gaat het om de digitale bewijskracht'

De belangrijkste vragen op een rij om het niveau van bewijskracht en digitale handtekening te bepalen:

1. Zijn de documenten authentieke aktes en is er een wettelijke verplichting om gebruik te maken van een gekwalificeerde handtekening?
2. Welke eisen stellen de toezichthouders in mijn sector? Denk daarbij aan de Belastingdienst, NEN, AFM, brancheorganisaties en kredietvers?
3. Over welke middelen beschikken mijn ondertekenaars om überhaupt digitaal te kunnen ondertekenen?

Authentieke of onderhandse akte

In de afweging is het belangrijk om vast te stellen of het document een authentieke dan wel onderhandse akte is. Authentieke akten zijn akten in de vereiste vorm en bevoegdelijk opgemaakt door ambtenaren, zoals ambtenaren burgerlijke stand, notarissen en rechters. Onderhandse akten zijn alle akten die niet authentieke akten zijn. In de praktijk komt dit erop neer dat een onderhandse akte een schriftelijk stuk is dat niet is opgesteld door een notaris, maar dat wel is ondertekend. Authentieke aktes dienen op dit moment te worden voorzien van een gekwalificeerde elektronische handtekening. Dan gaat het om authentieke aktes waarin de gekwalificeerde handtekening benoemd staat, zoals de akte die de notaris opstelt voor het Kadaster.

95 procent van de documentstromen zijn onderhandse akten en kunnen met een geavanceerde digitale handtekening worden ondertekend, mits er geen aanvullende eisen worden gesteld door toezichthouders of de dienstverlener de strenge eis van een gekwalificeerde certificaat wenst om de ondertekenaar te identificeren.

“We hebben zo’n elf- à twaalfhonderd verhuringen per jaar. Het digitaal laten ondertekenen van huurcontracten scheelt ons vier à vijf uur per klant. We hoeven de documenten niet meer uit te printen, te scannen, op te sturen, et cetera.”

Henk Stoutjesdijk, teamleider ICT & Facilitair bij Stadlander

Toezichthouders en derde werking

Het is van belang om rekening te houden met de eisen die toezichthouders en andere betrokken partijen stellen aan de elektronische handtekening, of die zijn neergelegd in de geldende NEN-normen. De eisen van partijen zoals de Belastingdienst, branche-organisaties, auditors, accountants of verzekeraars hebben doorgaans betrekking op de betrouwbaarheid van de beoogde ondertekenoplossing. Wanneer documenten internationaal worden aangeboden dan is het goed om te kijken of er aanvullende eisen zijn in dit land. Op Europees niveau is de eIDAS verordening van toepassing.

Beschikbaarheid van identificerende kenmerken

DigiD, mobiel of iDIN zijn middelen die een grote dekking hebben. Nog maar weinig gebruikers beschikken over een gekwalificeerd certificaat. Wanneer een ondertekenaar een verzoek krijgt om digitaal te ondertekenen en hij beschikt niet over het juiste identificerende middel, dan zal hij alsnog het document per papier ondertekenen en retourneren. Wanneer een geavanceerde handtekening voldoet, kan ook gekozen worden voor de identificerende middelen waar de gebruiker over beschikt en de dekking al hoog is. Hoe sterk wil ik mijn ondertekenaar herkennen voor de bewijskracht van mijn transactie en betrouwbaarheid van het proces? Is een geverifieerd e-mailadres voldoende of wil ik op een hoogwaardigere manier de ondertekenaar herkennen voor mijn bewijskracht?

Bewijskracht en de onafhankelijke derde partij?

Een dienstverlener kan ervoor kiezen om het proces voor de digitale handtekening zelf in te richten, of om dit uit te besteden aan een externe ondertekendienst. Daarbij is het goed om te bedenken dat hier meer bij komt kijken dan het vervangen van de papieren handtekening door een gescande handtekening of een krabbel via touch of muis. Het op een juiste wijze inrichten van een gebruikersvriendelijk en rechtsgeldig ondertekenproces is een complexe, kennisintensieve en kostbare aangelegenheid. Ook zijn de ontwikkelingen nog in volle gang en zal dit niet een eenmalige statische inrichting zijn. Zo zal bijvoorbeeld het aanbod van digitale identiteiten om mee te ondertekenen de komende jaren zich steeds verder ontwikkelen. Er moet continu worden gekeken of de oplossing nog voldoet aan de laatste mogelijkheden, technische standaarden en juridische vereisten.
Belangrijker nog is het feit dat ondertekendiensten onder de eIDAS-richtlijn ook onder toezicht komen te staan en dus een maatschappelijke rol gaan vervullen. Hierbij is het ook relevant dat het voor een goede bewijskracht belangrijk is dat je als dienstverlener geen partij bent in de totstandkoming van de digitale handtekening. Uiteraard is het dan wel belangrijk dat de organisatie ook een cloudpolicy heeft om aan te sluiten op deze externe ondertekendienst.

Waar moet de ondertekenoplossing aan voldoen?

Wanneer de juiste keuze is gemaakt over het risico van de transactie en de benodigde handtekening, kan worden gekeken naar de eisen die worden gesteld aan de oplossing voor het digitaal ondertekenen.
Het is raadzaam om bij de selectie van een oplossing voor het plaatsen van elektronische handtekeningen in ieder geval de volgende vragen te beantwoorden:

- Voorziet de oplossing voor het plaatsen van elektronische handtekeningen in een ‘audittrail’? In dit transactiebewijs worden alle stappen van het ondertekenproces vastgelegd. Daarmee kunnen de betrokken partijen al voor een groot deel vaststellen of aan de voorwaarden voor rechtsgeldigheid is voldaan.
- Zijn zowel het document als de audittrail ‘verzegeld’ met behulp van PKI (Public Key Infrastructure)-encryptie?
  Die verzegeling biedt de betrokken partijen de zekerheid dat het document niet tussentijds is gewijzigd.
- Is de oplossing voor het plaatsen van elektronische handtekeningen gebaseerd op internationaal erkende handtekeningformaten zoals PAdES (PDF Advanced Electronic Signatures), XAdES (voor XML) en CAdES (voor CMS)? Deze standaarden bieden garantie dat documenten ook in de toekomst nog leesbaar zijn voor mensen of computers.
- Voegt de oplossing een ‘time stamp’ toe als bewijs dat het document op ‘moment X’ al bestond?

"Een machtiging voor de inzage in medische gegevens sturen we via 'www.ondertekenen.nl' naar de medewerker, en drie minuten later zit het document alweer ondertekend in de mailbox van de bedrijfsarts, die dan direct met het dossier aan de slag kan. De tijdwinst die we daarmee realiseren, is voor ons echt cruciaal. We willen geen tijd verliezen aan dingen die geen waarde toevoegen."
Marc Aelberts, Managing Partner van Richting

- Welke 'identificerende kenmerken' worden gebruikt? Een voorwaarde die is verbonden aan de totstandkoming van een elektronische overeenkomst, is dat de identiteit van de betrokkenen met zekerheid kan worden vastgesteld. De identiteit van een ondertekenaar kan op een groot aantal manieren worden vastgesteld, bijvoorbeeld aan de hand van gebruikersnaam en wachtwoord, DigiD, eHerkenning, iDIN, sms-code, een iDeal-betaling of een gekwalificeerd certificaat. Welk identificerende kenmerken de voorkeur hebben, is onder andere afhankelijk van de toepassing, de branche en de gebruikers. De geselecteerde oplossing voor het plaatsen van elektronische handtekeningen moet de beschikbare identificerende kenmerken zo breed mogelijk ondersteunen en de mogelijkheid bieden om een aantal identificerende kenmerken te 'stapelen' voor de juiste bewijskracht.
- Worden zowel de documenten als de transactiebewijzen volledig overgedragen aan de betrokken partijen? Mocht de geplaatste handtekening inzet worden van een rechtszaak, dan moet er geen afhankelijkheid zijn van de aanbieder van de ondertekenoplossing.
- Bij het plaatsen van een handtekening moet er duidelijk sprake zijn van een wilsuiting. Het gaat om een eenduidig ondertekenproces. De ondertekenaar moet dus duidelijk kunnen uiten akkoord te gaan.

Aanvullende wensen

Naast de aandachtspunten die helpen bij het selecteren van een ondertekenoplossing die voldoet aan de eisen die aan een elektronische overeenkomst worden gesteld, is het raadzaam om te letten op deze punten die meer te maken hebben met de gebruiksvriendelijkheid van de ondertekenoplossing:

- Is het mogelijk om het ondertekenen van een document aan iemand anders toe te wijzen, bijvoorbeeld aan een assistent of directiesecretaresse?
- Voorziet de oplossing in een duidelijke workflow als een verzoek tot het plaatsen van een handtekening wordt geweigerd?
- Voorziet de oplossing in een application programming interface (API) voor integratie met zakelijke applicaties, zodat bijvoorbeeld verzoeken voor het plaatsen van een handtekening kunnen worden afgehandeld via een IT-systeem dat binnen de organisatie al in gebruik is?
- Is de oplossing ook bruikbaar op mobiele apparaten?
- Is het systeem eenvoudig aan de eigen document-managementsystemen te koppelen?
- Is het mogelijk om documenten door meerdere ondertekenaars te laten ondertekenen?
- Is het mogelijk om meerdere documenten in één transactie te laten ondertekenen? Dus bijvoorbeeld een arbeidscontract, loonheffingsverklaring en de voorwaarden.
- Zijn de gegevens te allen tijde goed beveiligd en voldoet de ondertekendienst aan de juiste certificeringen zoals ISO 270001?

Conclusie

Steeds meer organisaties digitaliseren hun papieren processen. Ook de documenten met rechtsgevolgen verlopen steeds vaker digitaal. Het gebruik van de digitale handtekening groeit daardoor snel, maar het is belangrijk om op de juiste manier te bepalen of een digitale handtekening noodzakelijk is en aan welke vereisten deze moet voldoen.

‘De digitale handtekening is bewijsrechtelijk gezien gelijk aan de handgeschreven handtekening’

Aangezien de elektronische handtekening dezelfde juridische waarde heeft als de handgeschreven handtekening, staat een digitaal ondertekend document juridisch gelijk aan een schriftelijk ondertekend document. De elektronische handtekening moet dan wel voldoen aan de eisen die de wetgever stelt aan raadpleegbaarheid, authenticiteit, transparantie van het ondertekenproces en de mogelijkheid om de identiteit van de ondertekenaar vast te stellen.

Als dienstverlener is het belangrijk om te kijken naar de benodigde bewijskracht in het proces, wie de ondertekenaars zijn en de mogelijke vereisten die toezichthouders stellen. 95% van het documentenverkeer zijn onderhandse aktes en kunnen via een geavanceerde digitale handtekening worden ondertekend.

Bij de keuze voor een oplossing is het belangrijk om goed te kijken of op de juiste wijze kan worden voldaan aan de eisen voor een betrouwbaar proces en de juiste bewijskracht. Het inrichten een digitale ondertekenoplossing in de eigen organisatie is meer dan alleen het inbouwen van een gescande papieren handtekening of een digitale krabbel op basis van touch of met de muis.

Een ondertekendienst kan op eenvoudige wijze een oplossing bieden, waarbij het ook gaat om de onafhankelijke rol en toezicht. Een keuze voor cloud levert in de praktijk gebruiksgemak en lagere kosten op en een oplossing die altijd in overeenstemming is met de laatste wetgevingen en richtlijnen. Een voorbeeld van zo’n clouddienst is ‘Ondertekenen.nl’ waarmee gebruikers een document digitaal kunnen ondertekenen. Deze waarborgt de integriteit van het document. Voor de authenticatie zijn er verschillende middelen ter verificatie van de identiteit. De mate van identificatie verschilt per gebruikersgroep en varieert van persoonlijke identificatie tot online verificatiemiddelen.

Over Evidos

Evidos staat voor Evidence in Online Services, zeker zakendoen op Internet. Evidos is marktleider in het leveren van oplossingen voor digitale handtekening en digitale identiteit. Met onze oplossingen kunt u zeker zakendoen op Internet, kosten besparen en uw producten en diensten sneller en efficiënter leveren.

"Evidos is al meer dan tien jaar internationaal en nationaal expert op het gebied van digitale bewijskracht. Met de ondertekendienst van Evidos, Ondertekenen.nl, kijken wij altijd naar de juiste balans voor een dienstverlener tussen gebruikersgemak, kosten en rechtsgeldigheid."
Kick Willemse, oprichter Evidos – Ondertekenen.nl

Al meer dan 10 jaren zijn wij nationaal en internationaal actief betrokken bij de laatste standaarden, wetgeving en technieken voor de digitale handtekening en inloggen.
Op het Internet is het belangrijk om te weten met wie u zaken doet en een digitale transactie moet dezelfde juridische waarde hebben als op papier.

We zijn er trots op dat we in Nederland organisaties als TAF, Total, Kamer van Koophandel, PGGM, DTZ Zadelhof en ITstaffing als klant ondersteunen.
Ook het MKB maakt succesvol gebruik van onze oplossingen binnen de digitale dienstverlening.

Vanuit een bedrijfskundige visie en sterke technisch inhoudelijke kennis zijn wij een volwaardig gesprekspartner. Naast kwaliteit staat resultaatgericht werken voorop.

Contact

Neem contact met ons op om in een vrijblijvend persoonlijk gesprek uw behoefte of vraagstuk rondom digitale zekerheid te bespreken.

Evidos - Ondertekenen.nl
Kick Willemse
Telefoonnummer: +31(0)23 737 00 46
info@evidos.nl

www.evidos.nl
www.ondertekenen.nl

Blijf op de hoogte