MEER *INFORMATIE*

De kosten van een elektronische handtekening

Voor een gekwalificeerd certificaat waarmee de elektronische handtekening gezet wordt betaalt u ongeveer € 35,- per jaar. Deze kosten zijn echter afhankelijk van het soort certificaat en de hoeveelheid documenten die u elektronisch ondertekent. U kunt het beste contact opnemen met een certificatiedienstverlener die u aan de hand van uw wensen precies kan vertellen wat een gekwalificeerd certificaat kost.

Publicatie 'eAuthenticatie voor managers' (ECP.NL, 2006).
Te downloaden via www.ecp.nl/downloads

Dossier elektronische handtekening op de website van ECP.NL:
www.ecp.nl/dossiers

DigiD
www.digid.nl

PKI Overheid
www.pkioverheid.nl

Diginotar B.V.
www.diginotar.nl

ESG de Electronische Signatuur BV.
www.de-electronische-signatuur.nl

Getronics Pinkroccade Nederland BV
www.pki.getronicspinkroccade.nl

Agentschap Centraal Informatiepunt Beroepen Gezondheidszorg
www.cibg.nl

OPTA
www.opta.nl

Colofon

Teksten:
ECP.NL, platform voor eNederland
GBO.Overheid, afdeling Beheer & Relatiemanagement

Eindredactie: ECP.NL
Illustraties: The Cartoonfactory
Druk: Efficiënta Offsetdrukkerij bv
Ontwerp: Dune Reclamebureau

Veilig en betrouwbaar elektronisch communiceren

Hoe weet u of degene die een bestelling bij u plaatst of u een opdracht geeft wel echt degene is voor wie hij zich uitgeeft? En hoe kunt u bewijzen dat u bent wie u aangeeft te zijn? Dit zijn twee van de belangrijkste vragen bij communicatie over het internet. Het afsluiten van overeenkomsten via het internet en het gebruik van toepassingen als e-mail, komen namelijk steeds vaker voor. Om te kunnen vertrouwen op deze elektronische transacties en overeenkomsten, waarbij bijvoorbeeld financiële of persoonlijke gegevens worden uitgewisseld, is het van belang dat u weet met wie u te maken heeft 'aan de andere kant van de lijn'. Ook belangrijk is dat uw berichten op de juiste plek terecht komen en onderweg niet ongemerkt veranderd kunnen worden. Door het gebruik van een elektronische handtekening zorgt u hiervoor. Hiermee kunt u ondertekenaars van elektronisch uitgewisselde overeenkomsten identificeren en de partij waarmee u elektronisch zaken doet laten weten dat u bent wie u zegt dat u bent. Dit maakt elektronisch zakendoen een stuk zekerder en ook efficiënter en makkelijker!

In deze brochure leest u wat een elektronische handtekening is, waarvoor u deze kunt gebruiken, welke bewijskracht deze heeft en waar u een elektronische handtekening kunt 'aanschaffen'.

De elektronische handtekening

Een elektronische handtekening, de elektronische variant van een gewone handtekening, is voor de ontvanger het bewijs dat een elektronisch bericht inderdaad verzonden is door de ondertekenaar en dat het onderweg niet gewijzigd is. De elektronische handtekening is dus een middel voor authenticatie. Dat wil zeggen dat daarmee de door de ondertekenaar geclaimde identiteit kan worden gecontroleerd.

Een elektronische handtekening kan gezet worden met behulp van (technische) middelen als gebruikersnaam en wachtwoord, een ingescande handtekening of een elektronisch certificaat (al dan niet beveiligd met PIN-codes of biometrie). Wat een elektronisch certificaat is en waarom dit de meeste zekerheid biedt, komt verderop in deze brochure aan bod.

Vanwege de snelle technologische ontwikkelingen worden door de wet geen specifieke technische eisen gesteld aan een elektronische handtekening. Dat betekent dat een elektronische handtekening met elke willekeurige techniek kan worden aangemaakt. Maar de betrouwbaarheid van de handtekening hangt natuurlijk wel af van de techniek die gebruikt wordt. Niet elke elektronische handtekening is waterdicht. U kunt zich voorstellen dat bijvoorbeeld voor het sluiten van contracten een ingescande handtekening niet betrouwbaar genoeg is. De verschillende soorten elektronische handtekeningen verschillen in betrouwbaarheid.

> "Een elektronische handtekening is een handtekening waarvan de elektronische gegevens zijn vastgehecht aan of logisch geassocieerd zijn met andere elektronische gegevens en die worden gebruikt als middel van authenticatie".
>
> Artikel 3:15a lid 4 Burgerlijk wetboek (Wet elektronische handtekeningen).

Soorten elektronische handtekeningen

'Gewone' elektronische handtekening
Een 'gewone' elektronische handtekening is een handtekening die gekoppeld is aan andere elektronische gegevens (bijvoorbeeld een document of een e-mail) en die wordt gebruikt als middel om de identiteit van de ondertekenaar vast te stellen. Een gewone elektronische handtekening is bijvoorbeeld een e-mailbericht waarin persoonsgegevens staan of een ingescande handtekening is gebruikt. Maar ook het intoetsen van een pincode of wachtwoord voor het bevestigen van een elektronische transactie is een gewone elektronische handtekening.

Geavanceerde elektronische handtekening
Een geavanceerde elektronische handtekening is daarentegen met meer waarborgen omkleed. Zij moet volgens de Wet elektronische handtekeningen aan eisen voldoen die meer zekerheid bieden ten aanzien van de identiteit en de wilsuiting van de ondertekenaar. Deze eisen zijn:

- zij is op een unieke wijze aan de ondertekenaar verbonden
- zij maakt het mogelijk de ondertekenaar te identificeren
- zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden en
- zij is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging van de gegevens achteraf kan worden opgespoord.

Door deze eisen is de geavanceerde elektronische handtekening betrouwbaarder dan de 'gewone'.

Daarnaast kent de Wet elektronische handtekeningen de volgende twee aanvullende eisen:

- de elektronische handtekening is gebaseerd op een gekwalificeerd certificaat dat voldoet aan eisen zoals gesteld in de Telecommunicatiewet en
- de elektronische handtekening is gegenereerd door een veilig middel voor het aanmaken van elektronische handtekeningen.

Een geavanceerde elektronische handtekening die ook aan deze laatste twee eisen voldoet, wordt ook wel aangeduid als een gekwalificeerde elektronische handtekening.

De keuze voor een bepaalde soort elektronische handtekening is sterk afhankelijk van het doel waar de elektronische handtekening voor wordt gebruikt. Het belang van de juistheid en de zekerheid moet afgewogen worden tegen de kosten en gemak. U moet zich daarbij steeds afvragen wie er baat bij heeft als er misbruik wordt gemaakt van de handtekening.
U bent van een hoop twijfel en onzekerheid af wanneer u gebruik maakt van een elektronische handtekening gebaseerd op een gekwalificeerd certificaat.

Hoe werkt een geavanceerde elektronische handtekening?

De techniek van een geavanceerde elektronische handtekening werkt op basis van 'a-symmetrische encryptie' (het coderen/versleutelen van gegevens zodat deze onleesbaar wordt voor onbevoegden) en gebruikt een publieke en een private sleutel, de elektronische identificatiegegevens. De private sleutel is alleen bekend bij de houder ervan en is uniek verbonden met de publieke sleutel. De private sleutel wordt gebruikt voor het zetten van de elektronische handtekening, het ontcijferen van een bericht of het elektronisch identificeren.

Een voorbeeld:

Alice ondertekent een elektronisch bestand met haar private sleutel. De ontvanger van dit bestand kan met de bijbehorende publieke sleutel (die op het meegestuurde digitale certificaat staat) verifiëren of het bericht ongewijzigd is en afkomstig van de bezitter van de bijbehorende private sleutel.

Dit lijkt wellicht ingewikkeld, maar na installatie van de juiste software is ondertekenen van het bericht meestal een kwestie van het aanklikken van een knop in uw e-mailprogramma!

De publieke sleutel is openbaar en wordt gebruikt voor het controleren op echtheid van de elektronische handtekening, het vercijferen van een bericht of het controleren van een elektronische identiteit.

Dat een bepaald sleutelpaar toebehoort een bepaald persoon of bedrijf, staat in een elektronisch certificaat dat door een certificatiedienstverlener (een onafhankelijke derde) is vastgelegd. Iedereen die dit wil, kan dit certificaat bij de certificatiedienstverlener controleren.

ALICE MET HAAR PRIVATE SLEUTEL

Juridische status van de elektronische handtekening

De eerdergenoemde Wet elektronische handtekening stelt de elektronische handtekening wettelijk gelijk aan de handgeschreven handtekening, mits een voldoende betrouwbaar middel is gebruikt om de handtekening te plaatsen. Dat betekent dat de elektronische handtekening die aan alle eisen in de wet voldoet (een gekwalificeerde elektronische handtekening) even betrouwbaar is en dus dezelfde rechtsgevolgen heeft als een handgeschreven handtekening. U heeft zekerheid over de juridische bewijskracht van de handtekening.

ELEKTRONISCHE HANDTEKENING RECHTSGELDIG

Dit wil overigens niet zeggen dat een handtekening die niet aan al die eisen voldoet, onbetrouwbaar is. Op basis van de afspraken die u gemaakt heeft met uw tegenpartij, de aard van de transactie, het doel waarvoor de gegevens zijn verzonden of andere omstandigheden, kan een rechter beslissen dat de gebruikte elektronische handtekening dezelfde rechtsgevolgen als een handgeschreven handtekening heeft.

Praktische gevolgen voor uw bedrijfsvoering

Een elektronische handtekening lijkt in eerste instantie complex, maar in de praktijk valt dat enorm mee. De handtekening kan heel eenvoudig toegevoegd worden aan de meest gangbare documenten als e-mailberichten, pdf's, webformulieren. Voordeel is dat u makkelijk op afstand overeenkomsten kunt sluiten én dat door het elektronisch afsluiten van overeenkomsten uw papieren administratie sterk slinkt. Wel is het van belang uw klanten/opdrachtgevers op de hoogte te stellen dat u een elektronische handtekening gebruikt en dit gebruik op te nemen in

de voorwaarden die u hanteert. Houd er ook rekening mee dat u de elektronische ondertekende documenten op een gedegen en veilige manier moet archiveren en bewaren. Uw netwerkbeveiliging moet dus ook op orde zijn. Ook uw medewerkers moeten ingelicht worden over hoe om te gaan met de elektronische handtekening. Kortom: houd ook rekening met organisatorische veranderingen bij invoering van de elektronische handtekening.

Een elektronische handtekening aanvragen

"Een certificatiedienstverlener is een natuurlijke persoon of rechtspersoon die certificaten afgeeft of andere diensten in verband met elektronische handtekeningen verleent". Artikel 1.1, sub tt Telecommunicatiewet 1998.

Om zeker te zijn dat de elektronische handtekening aan de voorwaarden voldoet die gesteld zijn in de Wet elektronische handtekeningen, is het belangrijk dat u een erkende certificatiedienstverlener (ook wel Certification Service Provider of CSP genoemd) inschakelt. Dit is een onafhankelijke, betrouwbare instelling die elektronische sleutels genereert en elektronische certificaten uitgeeft. In deze elektronische certificaten verklaart de certificatiedienstverlener dat een bepaalde elektronische sleutel toebehoort aan een bepaalde persoon of organisatie. Hiermee garandeert de certificatiedienstverlener dat een ondertekend bericht daadwerkelijk afkomstig is van een bepaalde organisatie of persoon, dat het bericht onderweg niet is gewijzigd en -als ook gebruik wordt gemaakt van versleuteling- dat niemand anders dan de ontvanger het bericht heeft kunnen lezen.

Het toezicht op Nederlandse certificatiedienstverleners die gekwalificeerde certificaten afgeven aan het publiek is neergelegd bij de Onafhankelijke Post en Telecommunicatie Autoriteit (OPTA). De certificatiedienstverleners zijn verplicht zich bij OPTA te registreren. Het register is openbaar toegankelijk op de website van OPTA.

In Nederland kunnen certificatiedienstverleners zich ook laten certificeren. Dat betekent dat zij zich vrijwillig kunnen laten toetsten op alle beveiligings- en kwaliteitseisen voor handtekeningdiensten. Voldoen zij aan alle eisen dan worden zij gecertificeerd. Een handtekening gezet met behulp van de diensten van een gecertificeerde certficiatiedienstverlener staat dus wettelijk gelijk aan de handgeschreven handtekening.

Nederlandse certificatiedienstverleners

U kunt een gekwalificeerde elektronische handtekening verkrijgen bij de volgende bij OPTA geregistreerde Nederlandse certificatiedienstverleners: Diginotar BV, Getronics Pinkroccade Nederland BV, Agentschap Centraal Informatiepunt Beroepen Gezondheidszorg en ESG de Electronische Signatuur BV.

Gecertificeerde certificatiedienstverleners.

Certificatiedienstverleners kunnen zich laten certificeren op basis van het TTP.NL Schema dat is opgesteld binnen het project TTP.NL (Thursted Third Party) van ECP.NL. Dit schema beschrijft de criteria voor het beoordelen en certificeren van elektronische handtekeningdiensten die worden geleverd door certificatiedienstverleners. Het TTP.NL-schema maakt gebruik van de technische specificaties die in Europees verband zijn gecreëerd door EESSI (European Electronic Signature Standardization Initiative) en sluit aan bij de Nederlandse Wet elektronische handtekening. Diginotar, PinkRoccade Infrastructure Services en CIBG (Centraal Informatiepunt Beroepen Gezondheidszorg) zijn gecertificeerde certificatiedienstverleners in Nederland.