De elektronische handtekening en de Dienstenrichtlijn

Deze factsheet behandelt de elektronische handtekening. Dit is een middel om te kunnen vertrouwen op elektronische berichten en transacties.

Op 28 december 2009 moet in alle EU-lidstaten de Dienstenrichtlijn zijn ingevoerd. Dankzij de richtlijn kunnen dienstverleners zoals cateraars, installatiebedrijven en horecaondernemers straks eenvoudiger aan de slag in de EU, wat de economische groei in deze sector kan stimuleren. Alle overheden leveren daaraan een bijdrage, waaronder gemeenten, provincies en waterschappen, centrale overheden zoals ministeries, PBO's, uitvoeringsorganisaties en toezichthouders. In het kader van de Dienstenrichtlijn komt er in alle lidstaten een centraal elektronisch loket waar dienstverleners al hun zaken met de overheid elektronisch kunnen regelen: het Dienstenloket. In Nederland wordt dit loket ondergebracht bij www.antwoordvoorbedrijven.nl.

De elektronische handtekening

Met het aansluiten op het elektronisch loket kunnen overheidsorganisaties via de berichtenbox elektronische aanvragen van ondernemers verwachten voor bijvoorbeeld vergunningen. Deze aanvragen zullen in sommige gevallen ondertekend zijn met een elektronische handtekening. Ook zal in voorkomend geval een verleende vergunning worden ondertekend namens het bevoegde bestuursorgaan met een elektronische handtekening. Een elektronische handtekening is een belangrijk middel waarmee ondertekenaars van elektronisch uitgewisselde documenten een wilsuiting bekrachtigen en zekerheid geven over de onweerlegbaarheid van het ondertekende document. Het laatste betekent dat u als bevoegde instantie ervan op aan kunt dat het bericht na ondertekening niet meer is gewijzigd.

Wat zegt een elektronische handtekening?

Een elektronische handtekening, de elektronische variant van een gewone handtekening, is voor de ontvanger het bewijs dat een elektronisch bericht inderdaad afkomstig is van de ondertekenaar en dat deze de inhoud van het bericht onderschrijft. Daarnaast garandeert de elektronische handtekening dat het bericht onderweg niet is gewijzigd. Dit met uitzondering van de ingescande handtekening die hiervoor geen enkele garantie biedt.

Wat zegt de elektronische handtekening niet?

Een geldige elektronische handtekening zegt niets over de daadwerkelijke betrouwbaarheid van degene die de handtekening zet. Een geldige elektronische handtekening zegt ook niets over de bevoegdheden of vakbekwaamheid van degene die de handtekening heeft gezet. Informatie over de betrouwbaarheid en vakbekwaamheid van een aanvrager/dienstverlener verkrijgt men desgewenst via het Interne Markt Informatiesysteem (IMI).

Verschillende elektronische handtekeningen

De ingescande (natte) handtekening

Elektronische handtekeningen zijn er in allerlei varianten. De meest eenvoudige is de met pen geplaatste handtekening op een papier dat wordt ingescand en als pdf-bestand wordt verzonden. Nadeel van deze handtekening is dat deze niet erg betrouwbaarheid is. Een ingescande handtekening is immers makkelijk te vervalsen.

De geavanceerde elektronische handtekening

Voor transacties die een hoger niveau van betrouwbaarheid vereisen, kunnen de zogeheten geavanceerde en gekwalificeerde elektronische handtekeningen worden gebruikt. De geavanceerde elektronische handtekening en de gekwalificeerde elektronische handtekening zijn in de context van de Dienstenrichtlijn het belangrijkst.

De geavanceerde elektronische handtekening moet volgens de Wet elektronische handtekeningen aan bepaalde eisen voldoen die meer zekerheid bieden dan de ingescande handtekening ten aanzien van de identiteit en wilsuiting van de ondertekenaar. Deze eisen zijn

a. zij is op unieke wijze aan de ondertekenaar is verbonden
b. zij maakt het mogelijk de ondertekenaar te identificeren
c. zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden en

d. zij is op een zodanige wijze aan het elektronische bestand waarop zij betrekking heeft verbonden, dat elke wijziging achteraf kan worden opgespoord

De geavanceerde elektronische handtekening kent meerdere varianten; een belangrijke variant is de geavanceerde elektronische handtekening gebaseerd op een gekwalificeerd certificaat. Een certificaat is conform de Wet elektronische handtekeningen een elektronische bevestiging die gegevens voor het verifiëren van een elektronische handtekening met een bepaalde persoon verbindt en de identiteit van die persoon bevestigt. Een gekwalificeerd certificaat is een certificaat dat onder strikte voorwaarden is uitgegeven aan de houder, zodanig dat er een grote zekerheid is over de koppeling met de houder. Gekwalificeerde certificaten zijn in verregaande mate gestandaardiseerd. Binnen het kader van de Europese Unie wordt de beoordeling van de betrouwbaarheid van gekwalificeerde certificaten vereenvoudigd door de beschikbaarheid van een zogenoemde Trusted List (zie ook controle elektronische handtekeningen).
Andere varianten van geavanceerde elektronische handtekeningen zijn veel minder scherp gedefinieerd en daardoor moeilijker op betrouwbaarheid te beoordelen.
De geavanceerde elektronische handtekening gebaseerd op een gekwalificeerd certificaat, voldoet aan bovenstaande eisen (a t/m d) en voldoet tevens aan de volgende aanvullende eis:
e. de elektronische handtekening is gebaseerd op een gekwalificeerd certificaat dat voldoet aan eisen zoals gesteld in de Telecommunicatiewet.

De gekwalificeerde elektronische handtekening
Het verschil tussen een geavanceerde handtekening en een gekwalificeerde handtekening is dat de gekwalificeerde handtekening naast bovengenoemde eisen (a t/m e) nog aan een extra eis moet voldoen, namelijk:
f. de elektronische handtekening is gegenereerd door een veilig middel.

Dit kan bijvoorbeeld door een smartcard, token of SIM-kaart met pincode. Doordat alleen de eigenaar over het ‘veilig’ middel kan beschikken heeft de gekwalificeerde handtekening een nog hoger betrouwbaarheidsniveau dan de geavanceerde handtekening.

Daarnaast is wettelijk bepaald dat aan een gekwalificeerde elektronische handtekening dezelfde rechtsgevolgen verbonden moeten worden als aan een handgeschreven handtekening.

Afweging
In het kader van de dienstenrichtlijn is het de ontvangende partij die dient te bepalen welke (elektronische) handtekening per procedure nodig is. Dat betekent concreet voor u, dat u een risicoanalyse dient uit te voeren voor ieder (type) elektronische transactie. Op basis daarvan bepaalt u welk niveau handtekening vereist wordt: eenvoudig waar het kan, geavanceerd of gekwalificeerd waar het moet. Daarbij kunt u als overheidspartij beslissen om voor de desbetreffende elektronische transactie andere elektronische handtekeningen dan de gekwalificeerde elektronische handtekening voldoende betrouwbaar te achten om de handgeschreven handtekening te vervangen.

Het handmatig controleren van een ontvangen elektronische handtekening
Elektronische handtekeningen zullen door u op echtheid beoordeeld moeten worden. Deze controle bestaat uit verschillende handmatige stappen:

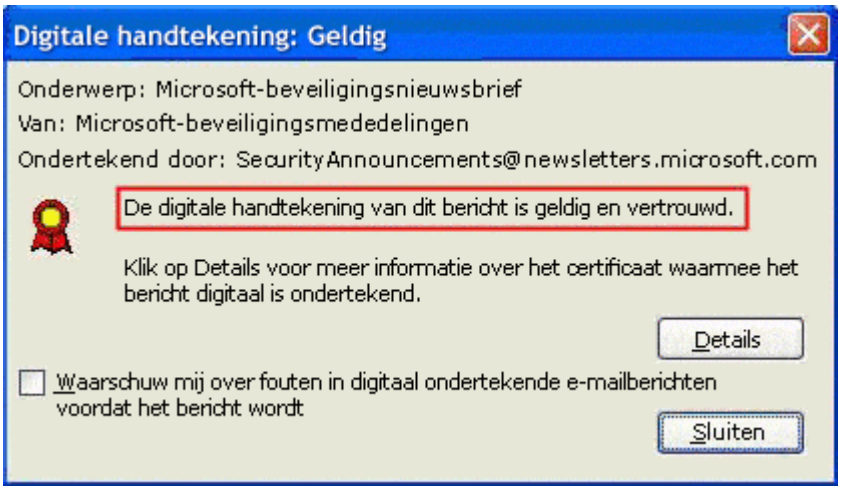
- Allereerst is het van belang dat de ontvangen elektronische handtekening ten minste overeenkomt met het gewenste niveau dat uit uw risicoanalyse is gekomen.

- Vervolgens dient er te worden vastgesteld of er sprake is van een betrouwbare uitgever van gekwalificeerde certificaten. Hiervoor kan de zogenaamde Trusted List gebruikt worden. Dit is een door de Europese Commissie beschikbaar gestelde lijst met links naar informatie over alle uitgevers van handtekeningen die aan de Europese regelgeving voldoen. De Trusted List is kosteloos raadpleegbaar.
  Het Nederlandse deel van de lijst wordt beheerd door de OPTA De Trusted List en een gedetailleerde beschrijving van de stappen die u moet doen om een elektronische

handtekening te controleren met behulp van deze Trusted List worden beschikbaar gesteld via www.dienstenrichtlijn.ez.nl.

- tijdens de technische controle van een elektronische handtekening door uw applicatie kunnen, ter illustratie, de volgende typen resultaten (of vergelijkbaar) zichtbaar zijn. Indien u een groen vinkje ziet (bv) of iets van vergelijkbare aard betekent dit dat de applicatie de elektronische handtekening met succes technisch heeft kunnen controleren. Dit zegt echter niets over de betrouwbaarheid van de handtekening. Indien de handtekening niet geldig is ziet u een rood kruis (bv) of iets van vergelijkbare aard.
  Verder geeft een pictogram als bv of aan dat de PDF op een certificaat is gebaseerd.

  Als u op het pictogram klikt dan kunt u de details van deze handtekening zien. Hieronder is een voorbeeld van deze weergave.



Het automatische controleren van een elektronische handtekening
Op dit moment is volledig geautomatiseerde controle van alle elektronische handtekeningen uit de EU nog niet mogelijk. Dit komt omdat de handtekeningen uit de lidstaten op technisch gebied van elkaar verschillen. Er zijn al wel oplossingen die handtekeningen uit enkele EU lidstaten automatisch kunnen controleren. De verwachting is dat automatische oplossingen binnen enkele jaren beschikbaar zullen zijn.

Verplichte acceptatie van elektronische handtekeningen
Een ontvangen elektronische handtekening kan niet geweigerd worden wanneer het gaat om een geavanceerde elektronische handtekening gebaseerd op een gekwalificeerd certificaat of een gekwalificeerde elektronische handtekening. Wanneer uw proces helemaal niet om een handtekening vraagt, kunt u een binnengekomen elektronische handtekening negeren. In de gevallen dat zekerheid over de wil en identiteit van de aanvrager naar uw oordeel niet nodig is, hoeft u de handtekening ook niet op echtheid te controleren.

Wanneer u echter op basis van een risicoanalyse heeft vastgesteld dat u voor een bepaalde transactie een geavanceerde elektronische handtekening gebaseerd op een gekwalificeerd certificaat nodig is, bent u ook verplicht om geavanceerde elektronische handtekeningen uit andere lidstaten te accepteren en om handtekeningen van een hoger betrouwbaarheidsniveau – de gekwalificeerde elektronische handtekening – te accepteren. Wanneer een overheidspartij ondertekening bijvoorbeeld een geavanceerde handtekening zonder gekwalificeerd certificaat vraagt dan moet deze overheidspartij ook de geavanceerde handtekening met gekwalificeerd certificaat of zelfs de gekwalificeerde handtekening accepteren. Door toepassing van het principe dat handtekeningen van een hoger niveau ook gebruikt kunnen worden voor processen waar een lager niveau volstaat, wordt voorkomen dat ondernemers voor ieder proces een verschillende handtekening moeten aanschaffen.

Het zetten van een elektronische handtekening
Berichten en documenten die door de overheid worden verstuurd, zijn vaak ondertekend door een bevoegde ambtenaar of bestuurder. Indien via uw Berichtenbox een bericht moet worden verzonden dat ondertekend is of waarbij een ondertekend besluit is gevoegd, kan de bevoegde instantie kiezen op welke wijze dit bericht of dit besluit ondertekend moet worden.

Een van de belangrijke vragen die hierbij spelen, is welke vormen van (elektronische) ondertekening rechtgeldig zijn. Een handgeschreven handtekening op een besluit, dat vervolgens wordt ingescand en elektronisch via de Berichtenbox wordt verzonden, is volgens het Nederlandse bestuursrecht in het beginsel rechtsgeldig voor zover deze vorm van ondertekening gelet op de aard, inhoud en het doel van deze vergunning voldoende betrouwbaar wordt geacht (artikel 2:16 Awb). Daarbij moet door de bevoegde instantie rekening houden met het feit dat aan een ingescande natte handtekening een laag betrouwbaarheidsniveau wordt toegekend.

Voor het zetten van geavanceerde en gekwalificeerde elektronische handtekeningen kunt u contact opnemen met een van de verschillende aanbieders van elektronische handtekeningen. Deze zullen u adviseren over de aanschaf van de benodigde middelen en infrastructuur om deze middelen te gebruiken.

Informatie
Meer informatie over de elektronische handtekening vindt u op; http://www.pkioverheid.nl/voor-eindgebruikers/brochures/, www.ecp.nl, www.afsprakenstelseleherkenning.nl, www.opta.nl

De belangrijkste elektronische handtekeningen kort samengevat.

Soort handtekening / ondertekening	**Juridische status**	**Acceptatie**	**Bijzonderheid**
Gekwalificeerde elektronische handtekening dwz. Elektronische handtekening gebaseerd op een gekwalificeerd certificaat en aangemaakt met een 'veilig' middel.	Gelijkgesteld met handgeschreven handtekening. Aan deze handtekening moeten dezelfde rechtsgevolgen worden verbonden als aan de handgeschreven handtekening.	Moet geaccepteerd worden zodra een bevoegde instantie dmv een risicoanalyse heeft aangetoond dat deze handtekening nodig is. Gekwalificeerde elektronische handtekeningen uit andere EU-landen moeten worden geaccepteerd.	Kan buiten beschouwing gelaten worden wanneer een bevoegde instantie voor een eenvoudige procedure genoegen neemt met een gescande handtekening of ondertekening met naam.
Geavanceerde elektronische handtekening met gekwalificeerd certificaat dwz Elektronische handtekening gebaseerd op een gekwalificeerd certificaat maar waarbij geen gebruik is gemaakt van een 'veilig' middel.	Niet gelijkgesteld aan handgeschreven handtekening. Aan deze handtekening hoeven niet dezelfde rechtsgevolgen verbonden te worden als aan de handgeschreven handtekening.	Moet geaccepteerd worden tenzij de bevoegde instantie dmv een risicoanalyse kan aantonen dat een gekwalificeerde elektronische handtekening noodzakelijk is. Geavanceerde elektronische handtekeningen met gekwalificeerd certificaat uit andere EU-landen moeten ook worden geaccepteerd.	Kan buiten beschouwing gelaten worden wanneer een bevoegde instantie voor een eenvoudige procedure genoegen neemt met een gescande handtekening of ondertekening met naam.
Geavanceerde elektronische handtekeningen/ vormen van authenticatie Dwz Elektronische handtekening zonder gekwalificeerd certificaat en waarbij geen gebruik is gemaakt van een 'veilig' middel.	Niet gelijkgesteld aan handgeschreven handtekening Aan deze handtekening hoeven niet dezelfde rechtsgevolgen verbonden te worden als aan de handgeschreven handtekening.	Bevoegde instantie bepaalt op basis van risicoanalyse of deze handtekening wordt geaccepteerd. Handtekening mag niet worden geweigerd vanwege het feit dat deze elektronisch is.	Echtheid van handtekening is moeilijk te controleren omdat deze niet voorkomt op de Trusted List.
Ingescande (natte) handtekening	Niet gelijkgesteld aan handgeschreven handtekening	Bevoegde instantie bepaalt dmv risicoanalyse geaccepteerd wordt. Verschilt per procedure	Wordt gebruikt voor eenvoudige procedures waar weinig zekerheid over de identiteit van de aanvrager is vereist.