



# | PKI overheid |

Is uw organisatie klaar voor de elektronische handtekening?

## Handreiking elektronische handtekening: Medewerker

### Voor wie is deze handreiking elektronische handtekening?

Als u kunt worden geconfronteerd met een elektronische handtekening is deze handreiking voor u van belang. U beoordeelt de waarde van ondertekende berichten en aanvragen en beslist hoe er wordt gereageerd.

### Wat is een elektronische handtekening?

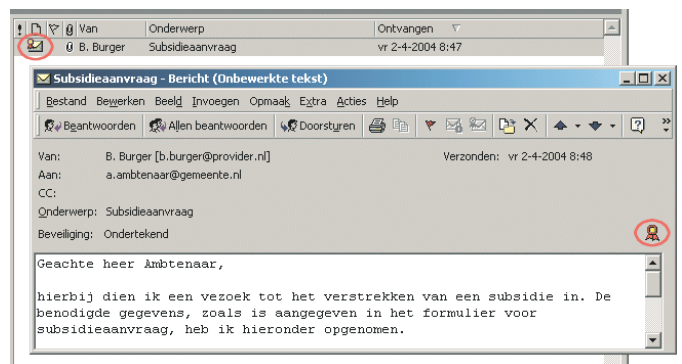
De elektronische handtekening is de elektronische tegenhanger van de handgeschreven handtekening. Waar een handgeschreven handtekening kan worden gebruikt om een brief te ondertekenen, kan een elektronische handtekening worden gebruikt om een e-mail te ondertekenen. Echter, ook elektronische documenten of formulieren kunnen worden gesigneerd. Bekende voorbeelden zijn de elektronische handtekening van de Belastingdienst voor het ondertekenen van de elektronische aangifte, de calculators die worden ingezet bij het internetbankieren en de elektronisch ondertekende uittreksels die door de Kamer van Koophandel worden uitgegeven.

Ambtenaren, burgers en vertegenwoordigers van bedrijven kunnen gebruikmaken van de elektronische handtekening. De techniek hiervoor is inmiddels beschikbaar. Dit betekent dat ook u hiermee kan worden geconfronteerd. Een burger zou u bijvoorbeeld een ondertekende e-mail kunnen sturen. In deze handreiking wordt uitleg gegeven over de elektronische handtekening en hoe u er mee kunt omgaan. Hierbij ligt de nadruk op het gebruik van ondertekende e-mail.

### Hoe herken ik een elektronische handtekening?

Technisch gezien is de elektronische handtekening niets meer dan een bestand dat u kunt meesturen met een bericht. In de praktijk merkt u hier niets van. Zo bieden de

meeste veelgebruikte e-mail-pakketten ondersteuning voor het lezen van ondertekende berichten. Dit betekent dat u als gebruiker gelijk kunt zien wanneer een e-mail is ondertekend. In Figuur 1 wordt een voorbeeld gegeven van een ondertekend bericht. Het rode zegel (rood omcirkeld) geeft aan dat de e-mail is ondertekend.



*Figuur 1 Voorbeeld van een getekende e-mail in Outlook. Ieder e-mailpakket gebruikt echter een eigen manier om weer te geven dat de e-mail getekend is*

### Hoe betrouwbaar is een elektronische handtekening?

Sommige elektronische handtekeningen bieden niet altijd voldoende garanties. Denk bijvoorbeeld aan de gescande handtekening, die eenvoudig kan worden gekopieerd. Andere handtekeningen waarbij bijvoorbeeld gebruik wordt gemaakt van een wachtwoord gekoppeld aan een gebruikersnaam bieden al meer betrouwbaarheid. Een techniek waarmee een hoge betrouwbaarheid kan worden bereikt is PKI (zie ook het kader). Een elektronische handtekening gebaseerd op PKI kan niet worden gekopieerd, wijzigingen in het bericht kunnen achteraf worden gedetecteerd en de afzender van het bericht is bekend. Het voorbeeld met het rode zegel in Figuur 1 toont het gebruik van een op PKI gebaseerde elektronische handtekening.

## Elektronische handtekeningen: hoe werkt dat?

Een elektronische handtekening is vergelijkbaar met een zegel, zoals die vroeger werden gebruikt voor het beveiligen van brieven. De verzender heeft een unieke stempel waarmee een zegel op een brief kan worden gezet. De ontvanger van de brief kan aan de hand van het zegel bepalen wie de brief heeft verzonden en zich er van overtuigen dat de inhoud onderweg niet is gewijzigd.

De elektronische handtekening die in deze handreiking wordt behandeld is gebaseerd op een public key infra-structure (PKI). Dit is een set van internationale standaarden over het uitgeven en beheren van onder meer elektronische handtekeningen. Bij het gebruik van PKI kan iemand alleen een handtekening onder een e-mail zetten als hij of zij beschikt over een digitaal certificaat. Deze certificaten worden uitgegeven door instanties en bedrijven. Elk certificaat is uniek en bevat de naam van de eigenaar. Met behulp van een dergelijk certificaat kan een persoon een elektronische handtekening zetten onder bijvoorbeeld een e-mail. De ontvanger kan vervolgens aan de hand van het certificaat zien wie de eigenaar is en daarmee wie de e-mail heeft ondertekend. Indien het bericht na ondertekening is gewijzigd, kan dit worden gedetecteerd.

Door het van kracht worden van de Wet elektronisch handtekeningen heeft de elektronische handtekening in Nederland sinds mei 2003 een juridische grondslag. Hierdoor hebben bepaalde elektronische handtekeningen dezelfde rechtsgeldigheid als de handgeschreven handtekening. Elektronische handtekeningen uitgegeven onder de PKI voor de overheid vallen binnen deze categorie. De PKI voor de overheid is een infrastructuur waarbinnen elektronische handtekeningen worden uitgegeven bedoeld voor betrouwbare communicatie met en binnen de overheid. Deze elektronische handtekeningen worden uitgegeven onder streng toezicht van de overheid en bieden daarmee een hoge betrouwbaarheid.

Als een e-mail is ondertekend met een elektronische handtekening gebaseerd op PKI, wil dit niet zeggen dat u het bericht per se kunt vertrouwen. In de tijd dat er nog stempels en zegels werden gebruikt, moest de ontvanger van de brief nagaan of de brief niet was opengemaakt en of het zegel wel echt was. Dit geldt ook voor de elektronische handtekening: u zult moeten nagaan of de handtekening betrouwbaar is.

## Hoe nu verder? Zeven stappen voor de medewerker...

Met het doorlopen van de onderstaande stappen kunt u nagaan in hoeverre een elektronische handtekening te vertrouwen is. Hierbij wordt met name aandacht besteed aan elektronisch getekende e-mail. Echter, de stappen zijn ook voor andere elektronische wegen van toepassing.

### In zeven stappen een elektronisch getekend bericht behandelen!

1. Ga na of de gevraagde dienst via elektronische weg toegankelijk is.
2. Bepaal of de handtekening relevant is.
3. Bepaal het soort handtekening.
4. Beoordeel de meldingen die worden gegeven door de software.
5. Controleer of de eigenaar van de handtekening degene is die het verzoek indient.
6. Ga na door welke instantie de elektronische handtekening is uitgereikt.
7. Bepaal de wettelijke status van de elektronische handtekening.

#### Stap 1: ga na of de gevraagde dienst via elektronische weg toegankelijk is

Aangezien in de meeste gevallen niet alle dienstverlening via elektronische weg toegankelijk kan worden gemaakt, zult u moeten nagaan of de gevraagde dienst via deze weg bereikbaar is. Zo wordt wellicht om een dienst gevraagd waarbij de aanvrager fysiek aanwezig moet zijn. Denk hierbij bijvoorbeeld aan het aanvragen van een nieuw paspoort bij een gemeente. Uw eigen organisatie moet bepalen welke diensten geschikt zijn om via elektronische weg open te stellen.

#### Stap 2: bepaal of de handtekening relevant is

U zult zich moeten afvragen of het verzoek wel een handtekening vereist. Wellicht wordt om openbare informatie gevraagd en kunt u deze gewoon verstrekken. Verdere controle van de handtekening is dan niet nodig.

#### Stap 3: bepaal het soort handtekening

U kunt nagaan welk soort elektronische handtekening wordt gebruikt. Een op PKI gebaseerde handtekening wordt in de meeste software weergegeven als een zegel. In het e-mailvoorbeeld zoals eerder beschreven wordt een rood zegel getoond. Stappen 4 tot en met 7 helpen u bij het valideren van een handtekening gebaseerd op PKI. Maar wellicht wordt gebruikgemaakt van een ander soort elektronische handtekening, bijvoor-

beeld gebaseerd op gebruikersnaam en wachtwoord. In dat geval moet uw organisatie aangeven of de toegepaste elektronische handtekening geschikt is voor de specifieke dienst en hoe deze dient te worden gecontroleerd.

#### Stap 4: beoordeel de meldingen die worden gegeven door de software

De software zoals het e-mailprogramma handelt automatisch een aantal controles voor u af. In Figuur 2 wordt een voorbeeld gegeven van de controle van een e-mail met een geldige handtekening. Dit venster verschijnt nadat op het rode zegel is geklikt (zie Figuur 1). Als de handtekening niet geldig is, wordt dit duidelijk aangegeven voordat de inhoud van het bericht kan worden bekeken.



Figuur 2 Controle van een (geldige) elektronische handtekening

De stappen die door de software worden afgehandeld staan hieronder beschreven.

- Is de integriteit van het bericht gewaarborgd, ofwel is het bericht na ondertekening niet gewijzigd? Indien de e-mail onderweg is gewijzigd zal dit worden opgemerkt door de software.
- Is het certificaat niet vroegtijdig ingetrokken? Uitgevers houden een 'zwarte' lijst bij van certificaten die niet meer geldig zijn. Deze kan via internet automatisch worden geraadpleegd.
- Is het certificaat nog geldig? Certificaten zijn geldig voor een bepaalde periode. Indien het certificaat is verlopen, mag de handtekening niet worden vertrouwd.
- Is het certificaat door een vertrouwde instantie uitgegeven? De software kan zo worden ingesteld dat elektronische handtekeningen die zijn uitgegeven door bepaalde instanties automatisch worden vertrouwd. In de stappen 6 en 7 wordt nader ingegaan op de wijze

waarop het vertrouwen in een instantie kan worden bepaald.

#### Stap 5: controleer of de eigenaar van de handtekening degene is die het verzoek indient

U kunt zien wie de eigenaar van het certificaat is en daarmee wie het bericht heeft ondertekend. In Figuur 2 wordt weergegeven wie het bericht heeft ondertekend, in dit geval B. Burger. Deze naam moet overeenkomen met de naam van degene die om de dienst vraagt. Het kan niet zo zijn dat meneer Jansen namens meneer Burger persoonlijke gegevens opvraagt.

#### Stap 6: ga na door welke instantie de elektronische handtekening is uitgereikt

Door het certificaat waarmee is ondertekend verder te bekijken, kan worden achterhaald welke de uitgevende instantie is. Klik hiervoor op het knopje Certificaat bekijken... Er verschijnt een venster zoals is weergegeven in Figuur 3. In dit geval wordt aangegeven dat deze e-mail is ondertekend door B. Burger, op basis van een certificaat dat is uitgegeven binnen de hiërarchie van de Staat der Nederlanden. Dit betekent dat het binnen de PKI voor de overheid is uitgegeven, waaruit geconcludeerd mag worden dat de handtekening is gelijkgesteld aan de handgeschreven handtekening. Deze handtekening kan dus worden vertrouwd.



Figuur 3 Certificaat binnen de hiërarchie van de Staat der Nederlanden

#### Stap 7: bepaal de wettelijke status van de elektronische handtekening

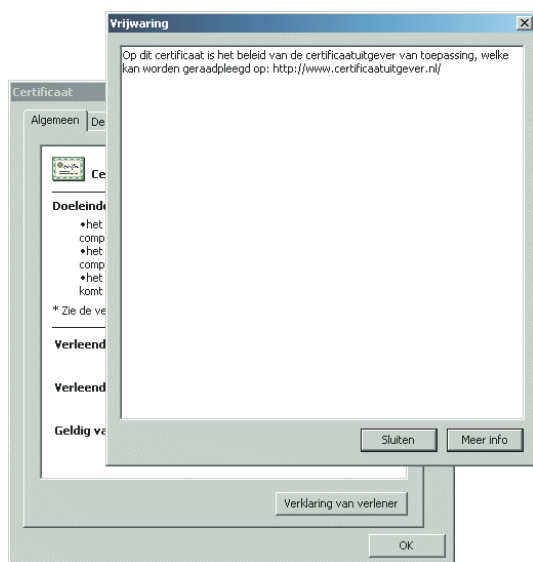
Het is natuurlijk mogelijk dat het certificaat buiten PKI voor de overheid is uitgegeven. Dit betekent geenszins dat deze handtekening onvoldoende betrouwbaarheid biedt. Wellicht heeft uw organisatie een lijst met vertrouwde uitgevers opgesteld, op basis waarvan u kunt bepalen of u de elektronische handtekening voor de specifieke dienst mag vertrouwen.

Als de uitgevende instantie niet op de lijst voorkomt of er is geen lijst beschikbaar, dan moet worden bepaald welk vertrouwen in deze uitgever mag worden gelegd.

Hiervoor moet echter een aantal zaken worden onderzocht. Het is dan ook aan te bevelen dit periodiek binnen uw organisatie te doen. De verantwoordelijkheid hiervoor ligt bij de leidinggevende of de proceseigenaar. In een andere handreiking binnen deze serie wordt specifiek ingegaan op het gebruik van de elektronische handtekening vanuit het perspectief van de leidinggevende en proceseigenaar.

Als er geen lijst beschikbaar is, kunt u zelf nagaan of het hier een handtekening betreft die wettelijk mag worden gelijkgesteld aan de handgeschreven handtekening. Dit wordt ook wel een gekwalificeerde elektronische handtekening genoemd. Zo kunt u de informatie uit het certificaat bekijken en daaruit opmaken of het hier een gekwalificeerd certificaat betreft. Een term als onweerlegbaarheid zoals ook wordt weergegeven in Figuur 3 duidt erop dat het hier een gekwalificeerde elektronische handtekening betreft. Soms wordt ook expliciet de term gekwalificeerd gebruikt.

Dit biedt echter geen volledige zekerheid: wellicht wordt wel een term als gekwalificeerd gebruikt, maar houdt de certificaatuitgever zich niet aan de wettelijke eisen. Als u meer zekerheid wilt kunt u informatie opvragen bij de certificaatuitgever op basis waarvan u kunt bepalen of de uitgever daadwerkelijke gekwalificeerde certificaten uitreikt. Aansluitend op het voorbeeld in Figuur 2 kunt u klikken op Certificaat bekijken... en vervolgens op Verklaring van verlener om deze informatie op te vragen. Dit wordt weergegeven in Figuur 4.



Figuur 4 Verklaring van de certificaatuitgever, met een verwijzing naar meer informatie

Naast het opvragen van deze informatie kunt u nagaan of de certificaatuitgever is geregistreerd bij de OPTA of bij een soortgelijke toezichthoudende instantie binnen

Europa. Deze registratie is namelijk verplicht voor uitgevers van gekwalificeerde certificaten. Indien u nog twijfelt over de betrouwbaarheid van de gebruikte elektronische handtekening, stap dan af op de leidinggevende of beveiligingsmanager.

### Hoe kan ik me verder voorbereiden op de komst van de elektronische handtekening?

Uw organisatie zal op beleidsniveau moeten bepalen in hoeverre het gebruik van de elektronische handtekening wordt toegestaan. Bij het vaststellen en invoeren van dit beleid spelen allerlei organisatorische en technische kwesties mee. Welke uitgevende instanties mogen worden vertrouwd en voor welke toepassingen? Is de technische infrastructuur aangepast op het gebruik van elektronische handtekeningen? En hoe moet worden omgegaan met de archivering van elektronisch getekende e-mails en documenten? Dit zijn enkele van de vragen die aandacht verdienen indien uw organisatie voorbereid wil zijn op de komst van de elektronische handtekening. De overige handreikingen in deze serie kunnen waardevolle informatie bieden bij deze voorbereiding.

### Andere handreikingen in deze serie

Naast deze Handreiking elektronische handtekening voor de Medewerker, zijn in deze serie tevens handreikingen beschikbaar voor de:

- Bestuurder
- Leidinggevende
- ICT-deskundige

### Meer informatie?

Heeft u behoefte aan advies, of bent u op zoek naar meer achtergrondinformatie over elektronische handtekeningen of specifieke hulpmiddelen? Neem dan contact op met het Informatiecentrum PKIoverheid. Het informatiecentrum heeft veel kennis, documenten en hulpmiddelen ter beschikking over de mogelijkheden en gevolgen van het invoeren en het gebruiken van elektronische handtekeningen.



| PKI overheid |

Informatiecentrum PKIoverheid  
Postbus 84011  
2508 AA Den Haag  
070-8887950  
info@pkioverheid.nl  
www.pkioverheid.nl