



# | PKI overheid |

Is uw organisatie klaar voor de elektronische handtekening?

## Handreiking elektronische handtekening: ICT-deskundige

### Voor wie is deze handreiking?

Indien u voor een overheidsorganisatie werkt als ICT-deskundige en bent betrokken bij de inrichting en het beheer van de ICT-infrastructuur dan is deze handreiking voor u interessant.

### Wat is een elektronische handtekening?

De elektronische handtekening is de elektronische tegenhanger van de geschreven handtekening. Het plaatsen van een elektronische handtekening kan verschillende vormen aannemen, variërend van een eenvoudige pincode tot en met het gebruikmaken van een geavanceerde smartcard met kaartlezer. De elektronische handtekening heeft, mits wordt voldaan aan een aantal voorwaarden, dezelfde juridische bewijskracht als de geschreven handtekening.

Medewerkers binnen uw organisatie kunnen worden geconfronteerd met elektronische ondertekende berichten en documenten. Het is daarom van belang dat zij in staat zijn een elektronische handtekening te controleren. De ICT-infrastructuur speelt een belangrijke rol bij het ontvangen van dergelijke ondertekende berichten en bij het controleren ervan.

De elektronische handtekening die in deze handreiking wordt behandeld is gebaseerd op een public key infrastructuur (PKI). Dit is een set van internationale standaarden die het mogelijk maakt om digitale informatie te versleutelen of te voorzien van een handtekening. Een groot voordeel van PKI is dat het mogelijk wordt een hoge betrouwbaarheid te garanderen.

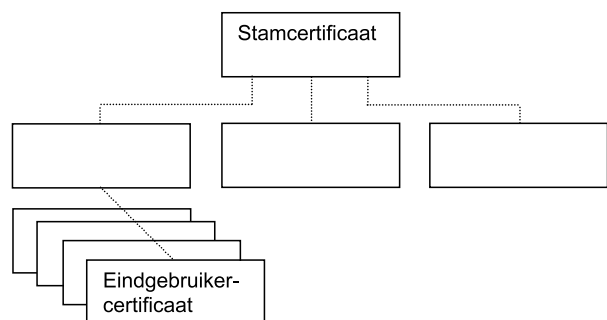
In deze handreiking ligt de nadruk op het gebruik van de elektronische handtekening binnen e-mailapplicaties. Echter, de informatie die wordt gegeven is veelal ook van

toepassing op andere applicaties waarbij PKI wordt toegepast.

### Wat zijn certificaten?

Een digitaal certificaat is uniek gekoppeld aan een persoon en gestructureerd volgens internationale PKI-standaarden. Iemand die een elektronische handtekening wil zetten op basis van PKI moet beschikken over een dergelijk certificaat. Dit certificaat bevat onder meer informatie over de eigenaar van het certificaat zoals de naam en de organisatie die wordt vertegenwoordigd door de eigenaar, de uitgever van het certificaat, de periode waarbinnen het certificaat geldig is en voor welke doeleinden het certificaat mag worden gebruikt. Zo kan een certificaat worden gebruikt voor versleuteling van gegevens, identificatie of het zetten van een elektronische handtekening.

Certificaten worden altijd in een hiërarchie geplaatst. Op het stamcertificaat na, zijn alle certificaten in de hiërarchie onbetwistbaar gekoppeld aan een hoger liggend certificaat. Dit maakt het mogelijk om een certificaat terug te leiden tot een stamcertificaat, de hoogste in de hiërarchie en daarmee het centrale punt van vertrouwen (zie Figuur 1).



Figuur 1 Certificaten hiërarchie

De Nederlandse overheid heeft een dergelijk stamcertificaat. Door vertrouwen te leggen in dit stamcertificaat, kunnen ook certificaten lager in de hiërarchie worden vertrouwd. Er zijn hoge eisen gesteld aan uitgevers van certificaten binnen de hiërarchie van de overheid, ofwel certificaten die binnen PKI voor de overheid vallen. Hierdoor hebben alle certificaten binnen deze hiërarchie een hoog betrouwbaarheidsgehalte.

### Welke software kan omgaan met elektronische handtekeningen?

Veel van de software die op een desktopomgeving wordt gebruikt is al geschikt voor het gebruik van PKI. Aparte software om een elektronische handtekening te kunnen controleren is dus veelal niet nodig. Zowel een aantal open source software pakketten als commerciële producten bieden ondersteuning voor PKI en het gebruik van certificaten. Kijk bijvoorbeeld bij Internet Explorer onder het menu: *Extra -> Internet opties... -> Inhoud -> Certificaten* om te zien welke certificaten zijn geïnstalleerd. Klik vervolgens op een certificaat om het te bekijken (zie Figuur 2). Ook veel gebruikte e-mailapplicaties bieden standaard de mogelijkheid om getekende e-mail te controleren of uitgaande e-mail te voorzien van een elektronische handtekening.



Figuur 2 Certificaat weergegeven in Microsoft Windows

Daarnaast zijn allerlei applicaties beschikbaar voor het ondertekenen van documenten en formulieren op basis van PKI. Ook kan PKI worden ingezet voor het versleutelen van informatie en het bieden van een beveiligde toegang tot het interne netwerk of het intranet.

### Hoe moet een elektronische handtekening worden gecontroleerd?

De meeste huidige e-mailsoftware kan controleren of een elektronische handtekening geldig is. Het volgende wordt door de software nagegaan:

- Hoort de handtekening bij de ondertekende e-mail? Indien de e-mail onderweg is gewijzigd zal dit worden opgemerkt door de software.
- Is het certificaat niet vroegtijdig ingetrokken? Certificaatuitgevers houden een 'zwarte' lijst bij van certificaten die niet meer geldig zijn, deze kan via internet automatisch worden geraadpleegd. Meer hierover volgt hieronder.
- Is het certificaat nog geldig? Certificaten zijn geldig voor een bepaalde periode. Indien het certificaat is verlopen, mag de handtekening niet worden vertrouwd.
- Valt het certificaat onder een hiërarchie, waarvan het stamcertificaat is opgenomen in het lokale systeem?

Wat betreft de 'zwarte' lijst van certificaten: certificaatuitgevers publiceren een lijst met vroegtijdig ingetrokken certificaten, welke niet meer mogen worden vertrouwd. Vaak biedt software de mogelijkheid om in te stellen of deze lijst (de certificate revocation list, CRL) moet worden geraadpleegd voordat een elektronische handtekening mag worden vertrouwd. Deze CRL wordt door de certificaatuitgever beschikbaar gesteld op het internet en periodiek ververs.

Indien een elektronische handtekening niet mag worden vertrouwd (omdat het bijvoorbeeld is verlopen), moet de software hiervan duidelijk melding maken aan de eindgebruiker. Een goede configuratie is echter van belang.

### Hoe nu verder? Zes stappen voor de ICT-deskundige..

Het is mogelijk om te anticiperen op de komst van de elektronische handtekening. Daarom staan hier zes stappen die de ICT-deskundige daarbij ondersteunen. Hierbij gaat het met name om het correct doorsturen van getekende e-mail en het controleren van de elektronische handtekening door de eindgebruiker.

#### Zes stappen ter voorbereiding op de komst van de elektronische handtekening!

1. Test of getekende e-mail goed wordt ontvangen.
2. Stem af met de leidinggevende binnen uw organisatie.
3. Achterhaal welke certificaatuitgevers mogen worden vertrouwd.
4. Pas de ICT-infrastructuur aan.

5. Zorg voor een goede configuratie van de e-mailserver.
6. Zorg voor een goede configuratie van de software bij de eindgebruiker.

### 1. Test of getekende e-mail goed wordt ontvangen

Het is nuttig om te testen in hoeverre ondertekende e-mails onbeschadigd de eindgebruiker bereiken. Uit een onderzoek gedaan door iPKIoverheid blijkt namelijk dat overheidsorganisaties vaak niet goed omgaan met ondertekende e-mail. De oorzaak ligt meestal in een verkeerde configuratie van de e-mailservers of virus-scanner. Om te testen is het handig om zelf te beschikken over certificaten. Er zijn bedrijven die certificaten uitgeven, al dan niet binnen de hiërarchie van PKI voor de overheid.

### 2. Stem af met de leidinggevende binnen uw organisatie

De leidinggevende zal keuzes moeten maken in welke diensten elektronisch beschikbaar moeten zijn. Op basis van deze keuzes kan de ICT-infrastructuur worden aangepast. Het betreft hier dus niet alleen e-mail, maar ook andere applicaties, zoals voor het ondertekenen en controleren van documenten en formulieren.

### 3. Achterhaal welke certificaatuitgevers mogen worden vertrouwd

Op basis van de stamcertificaten die beschikbaar zijn op een systeem wordt het vertrouwen in ondertekende berichten en documenten bepaald. Het is dus belangrijk om te weten welke certificaatuitgevers mogen worden vertrouwd. In samenspraak met de IT- of beveiligingsmanager moet worden vastgesteld welke certificaatuitgevers mogen worden vertrouwd. Vervolgens kan worden bepaald welke stamcertificaten moeten worden geïnstalleerd.

### 4. Pas de ICT-infrastructuur aan

Een aantal van de taken met betrekking tot het controleren van elektronisch getekende berichten en documenten kan automatisch worden afgehandeld. Het streven is dat de medewerker zo min mogelijk moet doen bij het controleren. Dit verhoogt zowel het gebruikersgemak, als het beveiligingsniveau.

De meeste besturingssystemen bieden ondersteuning voor het distribueren van stamcertificaten in het netwerk. Het is mogelijk om certificaten toe te voegen of deze te verwijderen voor alle computers in het netwerk. Zo zou het stamcertificaat van de overheid organisatiebreed vanuit de ICT-afdeling kunnen worden geïnstalleerd, zodat gebruikers dit niet zelf

hoeven te doen. Dit stamcertificaat is beschikbaar via <http://www.pkioverheid.nl>. Vermijd vervolgens ook dat medewerkers zelf certificaten van certificaatuitgevers kunnen toevoegen. Hiermee wordt voorkomen dat bepaalde certificaatuitgevers onterecht als vertrouwd worden gekenmerkt.

Zorg er ook voor dat de CRL's (de 'zwarte' lijst van certificaten), beschikbaar gesteld door certificaatuitgevers, toegankelijk zijn. Deze CRL's worden vaak op het internet gepubliceerd. Het is van belang dat applicaties hier toegang toe kunnen krijgen. Het is ook mogelijk deze CRL's te installeren op het systeem, min of meer gelijk aan de manier zoals dat voor certificaten kan. Het is dan van belang deze CRL's regelmatig te verversen.

### 5. Zorg voor een goede configuratie van de e-mailserver

Een ondertekend e-mailbericht lijkt erg veel op een e-mail met bijlage. Indien de mailserver dit type bijlage niet herkent, kan de e-mail worden geblokkeerd. De meeste mailservers bieden echter de mogelijkheid tot uitgebreide configuratie en dit maakt het mogelijk om ondertekende e-mails door te laten op basis van het type bijlage. Zo kunnen bestanden waar een virus in kan zitten worden gefilterd, terwijl ondertekende e-mails wel worden geaccepteerd. Het doorlaten van ondertekende e-mails hoeft dus geen extra risico's met zich mee te brengen.

### 6. Zorg voor een goede configuratie van de software bij de eindgebruiker

Bij het controleren van een elektronische handtekening speelt de configuratie van de software een belangrijke rol. Het is uiteindelijk aan de eindgebruiker om de betrouwbaarheid van een elektronische handtekening vast te stellen, de software biedt hier ondersteuning bij. Zo kan de software bijvoorbeeld controleren of het certificaat niet vroegtijdig is ingetrokken en of het certificaat is uitgereikt door een vertrouwde certificaatuitgever. De meeste software kan zodanig worden geconfigureerd dat al deze controles automatisch worden uitgevoerd.

## Andere handreikingen in deze serie

Naast deze Handreiking elektronische handtekening voor de ICT-deskundige, zijn in deze serie tevens handreikingen beschikbaar voor de:

- Bestuurder
- Leidinggevende
- Medewerker

## 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