



| PKI overheid |

Is uw organisatie klaar voor de elektronische handtekening?

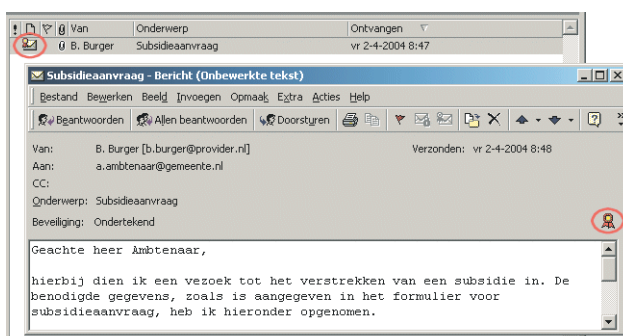
Handreiking elektronische handtekening: Leidinggevende

Voor wie is deze handreiking?

Indien u als leidinggevende en/of proceseigenaar binnen de overheid in aanraking komt met elektronische handtekeningen binnen uw afdeling of proces, dan is deze handreiking voor u interessant.

De elektronische handtekening komt eraan!

Stelt u zich eens voor. Eén van uw medewerkers ontvangt via de e-mail een bericht dat is ondertekend met een elektronische handtekening (zie Figuur 1). In de e-mail wordt een aanvraag gedaan die financiële gevolgen kan hebben voor uw organisatie. Denk bijvoorbeeld aan een subsidieaanvraag. Zijn uw medewerkers in dat geval op de hoogte van hoe zij met een dergelijke aanvraag kunnen omgaan? Kunnen uw medewerkers de elektronische handtekening eigenlijk wel herkennen? En zijn zij op de hoogte van de verschillende soorten elektronische handtekeningen en hoe zij deze mogen en kunnen accepteren?



Figuur 1 Een voorbeeld van een elektronisch ondertekende e-mail

In deze handreiking wordt ingegaan op de wijze waarop u met de elektronische handtekening kan worden geconfronteerd en de verschillende vormen waarin deze kunnen voorkomen. Tenslotte worden de stappen uitgelegd die u als leidinggevende en/of proceseigenaar

kunt nemen om te anticiperen op de ontvangst en het gebruik van een elektronische handtekening.

Elektronische handtekeningen

Bij het aanbieden van elektronische diensten over internet is het van belang om zorg te dragen voor voldoende beveiliging en vertrouwelijkheid. Het verzenden van berichten over het internet brengt immers risico's met zich mee. Hoe kan men weten dat de afzender van een bericht degene is die hij zegt te zijn? Hoe weet de ontvanger van een bericht dat deze onderweg niet is gewijzigd? En hoe weet de afzender dat onbevoegden geen kennis hebben kunnen nemen van de inhoud van het bericht na verzending? Het gebruik van papier biedt van nature een aantal waarborgen voor de betrouwbaarheid van een bericht die in de elektronische wereld ontbreken.

Bij het beveiligen van elektronische diensten speelt de elektronische handtekening een belangrijke rol. Elektronische handtekeningen worden in Nederland dan ook op steeds grotere schaal gebruikt. 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. Maar ook worden medewerkers binnen de overheid en het bedrijfsleven steeds vaker met een elektronische handtekening uitgerust. Deze elektronische handtekeningen worden bijvoorbeeld gebruikt om op het netwerk of applicaties te kunnen inloggen of elektronisch ondertekende berichten te kunnen versturen (het doen van een wilsuiting).

Soorten elektronische handtekeningen

De elektronische handtekening is de elektronische variant van de handgeschreven 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. Door het van kracht worden van de Wet elektronisch handtekeningen (Weh) heeft de elektronische handtekening in Nederland sinds mei 2003 een juridische grondslag gekregen. Hierdoor kan aan de elektronische handtekening, mits wordt voldaan aan een aantal voorwaarden, dezelfde rechtsgeldigheid worden toegekend als aan de handgeschreven handtekening.

Elektronische handtekeningen kunnen grofweg in twee categorieën worden ingedeeld. De eenvoudigste vorm is de *gewone elektronische handtekening*. Veruit de meeste elektronische handtekeningen die momenteel worden gebruikt vallen binnen deze categorie. Voorbeelden zijn een simpele gescande handtekening, het intoetsen van een pincode of wachtwoord voor het bevestigen van een transactie, maar ook het gebruikmaken van meer geavanceerde middelen zoals softwarecertificaten, SMS of beveiligingscalculators. Normale elektronische handtekeningen worden vanuit de wet niet zondermeer juridisch gelijkgesteld aan de handgeschreven handtekening. De bewijskracht zal afhangen van de specifieke context waarin de elektronische handtekening wordt gebruikt en zal bij een geschil door de rechter worden bepaald. Communicerende partijen kunnen de bewijskracht van een normale elektronische handtekening bijvoorbeeld kracht bijzetten door gebruik te maken van betrouwbare technologieën en toe te zien op de uitgifte van de elektronische handtekening. Daarnaast kunnen communicerende partijen met elkaar (contractueel) afspreken dat een bepaalde elektronische handtekening als bewijs wordt geaccepteerd. Deze oplossing wordt bijvoorbeeld door de banken gebruikt bij het internetbankieren. Nadeel hiervan is dat partijen hiervoor elkaar vooraf dienen 'te kennen'.

De tweede categorie elektronische handtekeningen is de *gekwalficeerde elektronische handtekening*. De gekwalficeerde elektronische handtekening wordt juridisch gelijkgesteld aan de handgeschreven handtekening, mits wordt voldaan aan alle wettelijke eisen. De elektronische handtekeningen die worden uitgegeven binnen de PKI voor de overheid vallen bijvoorbeeld binnen deze categorie. Daarnaast bestaan diverse andere partijen die dergelijke elektronische handtekeningen uitgeven. Praktisch gezien geldt dat voor dit type elektronische handtekening een smartcard moet worden gebruikt, in combinatie met een digitaal certificaat dat is uitgegeven binnen een public key infrastructure (PKI). Grote voordeel hiervan is dat partijen elkaar niet vooraf hoeven te kennen en geen afspraken hoeven te maken over de bewijskracht van de elektronische handtekening. Immers, deze handtekening heeft automatisch dezelfde rechtswaarde als de handgeschreven handtekening.

Hoe nu verder?

Acht te nemen stappen voor de leidinggevende...

Gezien de verdere gewenning aan elektronische dienstverlening en elektronische handtekeningen is de kans groot dat uw medewerkers vroeg of laat, al dan niet op eigen initiatief, worden geconfronteerd met elektronische handtekeningen. Om hierop te anticiperen kunt u als leidinggevende acht stappen doorlopen.

In acht stappen naar het gebruik van elektronische handtekeningen!

1. Identificeer (potentiële) kanalen en diensten.
2. Bepaal welke elektronische diensten hiervan in aanmerking komen voor elektronische afhandeling.
3. Bepaal welke typen elektronische handtekeningen worden ondersteund.
4. Stel richtlijnen op voor de omgang met de elektronische handtekening.
5. Maak aanpassingen in de technische infrastructuur.
6. Communiqueer de mogelijkheid tot het gebruik van de elektronische handtekening.
7. Evalueer periodiek de stand van zaken.
8. Zoek aansluiting bij andere overheidsinstellingen.

Stap 1: Identificeer (potentiële) kanalen en diensten

Bepaal langs welke communicatiekanalen uw afdeling of instelling nu reeds elektronisch bereikbaar is en welke diensten per kanaal (kunnen) worden aangeboden. Hierbij kan worden gedacht aan e-mail, een formulier op de website of een algemene postbus (info@gemeente.nl). De kans is immers groot dat uw medewerkers via één van deze communicatiekanalen worden benaderd met een elektronisch ondertekend bericht of een verzoek om een dienst.

Stap 2: Bepaal welke elektronische diensten hiervan in aanmerking komen voor elektronische afhandeling

Nadat de communicatiekanalen en diensten in kaart zijn gebracht, zult u moeten bepalen welke diensten via welke kanalen in aanmerking komen voor elektronische afhandeling. In het wetsvoorstel Elektronisch bestuurlijk verkeer (Webv) worden elektronische berichten zoals websites, e-mails en faxen gelijkgesteld aan 'schriftelijke' berichten. Behalve in die gevallen waar specifieke wetgeving vereist dat een dienst op de conventionele wijze dient plaats te vinden, kan deze dienstverlening dus elektronisch plaatsvinden. Gedurende deze stap zult u met name de potentiële baten voor uw organisatie en de klanten moeten adresseren. Tenslotte wordt aanbevolen aansluiting te zoeken bij sectorale en landelijke beleidsuitgangspunten voor elektronische dienstverlening. Zie voor meer informatie over de Webv de Handreiking voor Bestuurders.

Stap 3: Bepaal welke typen elektronische handtekeningen worden ondersteund

Omdat elektronische handtekeningen in vele soorten en maten voorkomen, zult u moeten bepalen welke typen elektronische handtekeningen moeten worden ondersteund en onder welke voorwaarden. In dit kader dienen de volgende aandachtspunten te worden geadresseerd:

- **Beveiligingsniveau elektronische handtekening**

Uitgangspunt moet zijn dat de afhandeling van een elektronisch bericht minimaal even betrouwbaar dient te zijn als in het conventionele verkeer. Aan het aanvragen van een subsidie via internet zullen bijvoorbeeld hogere beveiligingseisen moeten worden gesteld dan aan de verstrekking van algemene inlichtingen die ook langs andere kanalen verkrijgbaar zijn. Dit heeft gevolgen voor de beveiligingseisen die aan de elektronische handtekening worden gesteld. Allereerst dient bepaald te worden of er überhaupt van een handtekening gebruik moet worden gemaakt. Vervolgens moet worden bepaald of gewone elektronische handtekeningen, en zo ja, in welke vorm en door welke uitgevende partijen, als voldoende betrouwbaar wordt geacht of dat een gekwalificeerde elektronische handtekening wordt vereist. Deze keuze zal afhangen van de aard van de specifieke dienst en de mogelijkheden om aanvullende maatregelen te kunnen treffen zoals het afsluiten van een contract of het sturen van een bevestigingsbrief.

- **Technische gevolgen**

Het accepteren van elektronische handtekeningen kan gevolgen hebben voor de technische infrastructuur van uw organisatie. Als leidinggevende zult u deze gevolgen willen laten meewegen bij de keuze om een bepaald type elektronische handtekening te accepteren. Zo zullen (e-mail)applicaties in staat moeten zijn om de elektronische handtekening te herkennen en te valideren en mogen netwerkcomponenten elektronisch ondertekende berichten niet tegenhouden.

- **Organisatorische gevolgen**

Het verwerken van een elektronische handtekening brengt tevens een aantal organisatorische wijzigingen met zich mee. Uw medewerkers zullen richtlijnen moeten ontvangen met betrekking tot de afhandeling van elektronisch ondertekende berichten. Daarnaast zal in sommige gevallen naar een oplossing moeten worden gezocht voor de archivering van een elektronisch ondertekend bericht. Immers, een elektronische handtekening heeft alleen bewijskracht in elektronische vorm.

Stap 4: Stel richtlijnen op voor de omgang met de elektronische handtekening

Wanneer de voorwaarden zijn bepaald voor het accepteren van elektronische handtekeningen, zullen

deze moeten worden vastgelegd en aan alle betrokken medewerkers kenbaar worden gemaakt. Medewerkers dienen instructies te ontvangen over hoe zij met een elektronische handtekening moeten omgaan. In deze richtlijnen zullen onder meer de volgende zaken moeten worden geadresseerd:

- Welke elektronische diensten in aanmerking komen voor elektronische afhandeling door uw medewerkers;
- Op welke wijze medewerkers de elektronische handtekening kunnen herkennen;
- Op welke wijze de werknemer dient te bepalen dat de elektronische handtekening geldig is en door een betrouwbare partij is uitgegeven;
- Op welke wijze de elektronisch ondertekende berichten moeten worden verwerkt en gearchiveerd.

Stap 5: Maak aanpassingen in de technische infrastructuur

Systeembeheer zal opdracht moeten krijgen om de infrastructuur aan te passen zodat elektronische handtekeningen door de medewerkers kunnen worden ontvangen, gevalideerd en eventueel gebruikt. Om validatie mogelijk te maken zal systeembeheer onder meer de stamcertificaten van de verschillende vertrouwde uitgevers van elektronische handtekeningen (ook wel certificatie dienstverleners of CSP's genoemd) aan alle gebruikers beschikbaar moeten stellen. Hiervoor dient systeembeheer namens u periodiek een overzicht te ontvangen van welke certificaatuitgevers de elektronische handtekeningen (normale en gekwalificeerde) door uw organisatie worden vertrouwd. Het opstellen van deze lijst kan worden gedelegeerd aan bijvoorbeeld een beveiligings- of riskmanager. Om te bepalen in welke mate een elektronische handtekening van een certificaatuitgever kan worden vertrouwd, dienen onder meer de volgende zaken te worden gevalideerd:

- **Betrouwbaarheidsniveau elektronische handtekening**
Betreft het een gekwalificeerde elektronische handtekening of niet? Dit is bijvoorbeeld aangegeven in het certificaat zelf, en blijkt uit de informatie beschikbaar gesteld door de certificaatuitgever (certificate policy of certification practice statement).

- **Certificering certificaatuitgever**

Is de uitgever van de elektronische handtekening door een bevoegde instantie gecertificeerd tegen een bepaald kwaliteitsschema zoals het Programma van Eisen van PKIoverheid, ETSI, TTP.nl, Webtrust of ISO?

- **Registratie bij de OPTA**

Is de certificaatuitgever geregistreerd als uitgever van gekwalificeerde elektronische handtekeningen bij de OPTA of bij een soortgelijke toezichthoudende instantie binnen Europa?

Tenslotte zal systeembeheer opdracht moeten krijgen om de netwerkcomponenten zo te configureren dat elektronisch ondertekende berichten niet worden tegengehouden.

Stap 6: Communiceer de mogelijkheid tot het gebruik van de elektronische handtekening

U zult uw relaties kenbaar moeten maken onder welke voorwaarden zij gebruik kunnen maken van hun elektronische handtekening bij de elektronische communicatie met uw organisatie. Dit kan bijvoorbeeld via de website of via een mailing.

Stap 7: Evalueer periodiek de stand van zaken

Hoewel al op grote schaal gebruik wordt gemaakt van elektronische handtekeningen, is in het algemeen de verwachting dat de toepassing ervan de komende jaren sterk zal toenemen. Het landschap van de elektronische handtekening zal hierdoor dan ook veranderen. Met name wordt verwacht dat elektronische handtekeningen niet langer binnen slechts één specifieke dienst kunnen worden gebruikt, maar tevens voor andere doeleinden kunnen worden ingezet, zodat een digitale sleutelbos van elektronische handtekeningen wordt voorkomen. Het wordt daarom aanbevolen de gang van zaken op het gebied van elektronische handtekeningen aandachtig te blijven volgen en te evalueren.

Stap 8: Zoek aansluiting bij andere overheidsinstellingen

Veel overheidsinstellingen hebben reeds de eerste stappen gezet op weg naar elektronische dienstverlening. Er is dan ook inmiddels veel praktijkkennis en kunde voorhanden. Voor sommige vormen van het gebruik van elektronische handtekeningen hebben zich reeds best-practices gevormd. Denk bijvoorbeeld aan de WOZ-online toepassingen van een aantal gemeenten. Met enige regelmaat worden door het informatiecentrum PKIoverheid handreikingen gepubliceerd en rondetafelbijeenkomsten georganiseerd. Het wordt dan ook aanbevolen hierbij aansluiting te zoeken.

Andere handreikingen in deze serie

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

- Bestuurder
- Medewerker
- 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