

# **De Digitale Handtekening**

Een digitale handtekening biedt de mogelijkheid om een document te ondertekenen zonder de fysieke aanwezigheid van de partijen.

De gebruiker kan na een veiligheidsprocedure e-mail verzenden waaraan zijn digitale handtekening wordt gekoppeld. Daarnaast kunnen elektronische mails worden versleuteld of geëncrypteerd.

Deze applicatie wordt al gebruikt voor de indiening van elektronische BTW aangiften. Ook de communicatie met het instituut kan uit deze applicatie haar voordeel putten. De jaarlijkse opgave van de permanente beroepsvervolmaking kan worden geautomatiseerd en ook de communicatie met de stagiaires kan sneller en efficiënter worden verricht. Dit alles met de zekerheid dat de afzender van het bericht inderdaad het instituut zelf, de accountant, de belastingconsulent, de stagemester of de stagiair is.

## **I. Benadering - problematiek**

De elektronische handtekening is een digitale ondertekening onder de vorm van een bijlage die aan een e-mail, een document of een elektronische handeling wordt bevestigd en die zekerheid geeft over de afzender van het bericht of de ondertekenaar ervan.

Een elektronische handtekening is daardoor veel belangrijker dan een "manuele" handtekening. Immers, het ondertekende document is zeker afkomstig van diegene waar de digitale handtekening aan toebehoort. Bij gewone elektronische handelingen (e-mail zonder digitale handtekening) is dat niet het geval! Als er elektronisch wordt gecommuniceerd, dan weet de ontvanger van het bericht niet zeker of de persoon die als afzender wordt opgegeven wel degelijk de persoon is die hij beweert te zijn. Hier zijn voldoende voorbeelden terug te vinden in de massa's SPAM MAIL die worden verzonden! Spam-mail kan ook worden teruggedrongen door van de afzender een digitale handtekening te eisen.

Digitale handtekeningen geven daarover definitief uitsluitel!

Ook op een site kan van een elektronische handtekening gebruik worden gemaakt. De persoon die zich aanmeldt wordt geverifieerd aan de hand van zijn digitaal certificaat. Daardoor kunnen hem bepaalde exclusieve rechten worden toegekend. Deze rechten kunnen verschillen volgens het profiel van de eigenaar van het digitale certificaat. Deze techniek maakt het mogelijk om erg vertrouwelijke informatie mee te delen of te ontvangen via de site: adreswijzigingen, gepersonaliseerde e-learning, enz

Daarenboven kunnen met digitale handtekeningen ook e-mails geëncrypteerd worden. De techniek gebruikt hiervoor 2 sleutels. De eerste sleutel is de publieke sleutel die door de afzender van het bericht op het Internet kan worden teruggevonden. De afzender moet zelf over een digitale handtekening beschikken van dezelfde provider als de bestemming en hij versleutelt in combinatie met zijn e-mail adres en zijn digitale handtekening en het e-mail adres en de publieke sleutel van de bestemming het bericht dat hij verzendt. De bestemming, en uitsluitend hij kan aan de hand van de private sleutel die zich op zijn computer moet bevinden het geëncrypteerde (versleuteld of gecodeerd) bericht ontcijferen. Bij deze uiterst veilige vorm van elektronische e-mail kan het bericht door niemand worden

ontsleuteld en kan er ook onderweg geen enkele wijziging aan het bericht worden aangebracht. De bestemming zal een corrupte e-mail ontvangen en die niet kunnen ontcijferen wanneer enige wijziging aan het bericht is aangebracht.

Deze veilige manier om elektronisch te communiceren dient tussen het IAB en haar leden, tussen de leden onderling en tussen de leden en derden te worden gepromoot. Tussen deze partijen vindt namelijk op een belangrijke wijze elektronische uitwisseling plaats van vertrouwelijke informatie.

#### Volgende problematiek kan worden onderkend:

- De authenticiteit
  - Het aangeven van de identiteit van de afzender
  - De integriteit: het bericht is zeker ongewijzigd tussen de afzender en de bestemming
  - De onweerlegbaarheid: de afzender heeft dit bericht wel degelijk verzonden
- De confidentialiteit of het vertrouwen tussen afzender en bestemming is gegarandeerd

#### Er wordt gebruik gemaakt van:

- een elektronische authenticiteit: token, pin codes, biometrie (fingerprint) of een digitale authenticiteit
- een certificaat
- PKI: Public Key Infrastructure: de private en de publieke sleutel

#### De behandeling van een digitale e-mail:

- de natuurlijke persoon koppelt zijn digitale handtekening aan een specifiek bericht dat hij wenst te verzenden
- deze persoon of afzender versleutelt (encrypteert) dit bericht met de publieke sleutel van de bestemming
- de e-mail wordt elektronisch verzonden
- de bestemming ontvangt een bericht en kan volgende verifiëren:
  - de afzender en de bestemming
  - de datum
  - de omschrijving
- om de inhoud te bekijken moet de bestemming het geëncrypteerde bericht ontsleutelen of decrypteren met zijn persoonlijke private sleutel
- daardoor is het bericht opnieuw leesbaar voor de bestemming

#### Voordelen

- enkel afzender en bestemming kunnen het bericht lezen
- eenvoudige behandeling in e-mail software (outlook, ...)
- snel
- efficiënt
- een corrupt bericht kan onmogelijk worden ontsleuteld.
- zekerheid aangaande de afzender

- zekerheid over de inhoud
- zekerheid over het afleveren en de datum

### Nadelen

- er moet beroep gedaan worden op een 3<sup>de</sup> partij: de certificatie autoriteit
- je moet sleutelen en ontsleutelen (encrypteren en decrypteren)

## **II. Hoe functioneert het praktisch?**

De procedure wordt opgestart op je eigen PC of computer. Je bezoekt de site van de certificaathouder die de digitale certificaten uitreikt, je vult de nodige informatie in en drukt een document af.

Een registratie autoriteit (aangesteld door de certificaathouder) controleert of verifieert fysisch de identiteit van de persoon die een digitale handtekening verlangt. Dit vindt plaats aan de hand van het genoemde document en de identiteitskaart.

Door deze registratie autoriteit wordt een bevestiging gezonden aan de certificaathouder dat de fysieke persoon effectief correspondeert met de persoon die is vermeld op het document.

Door de certificaathouder (provider van de digitale certificaten of handtekeningen) wordt aan de aanvrager een identificatie toegekend op de server en daar wordt een sleutelpaar aan gekoppeld: een private en een publieke sleutel.

De private sleutel hoort bij het e-mailadres van de aanvrager. De publieke sleutel staat voor iedereen ter beschikking op het Internet.

Om de procedure af te ronden moet de aanvrager, na ontvangst van een e-mail van de certificaathouder, zijn persoonlijke sleutel genereren. Dat gebeurt automatisch bij het heraanmelden op de site waar de procedure is opgestart.

Genoemde publieke sleutels kunnen vrij gevonden worden bij de registratie autoriteit.

## **III. Wat is het nut van een digitale handtekening?**

Accountants en belastingconsulenten kunnen digitale handtekeningen in hun dagelijkse praktijk uitgebreid gebruiken.

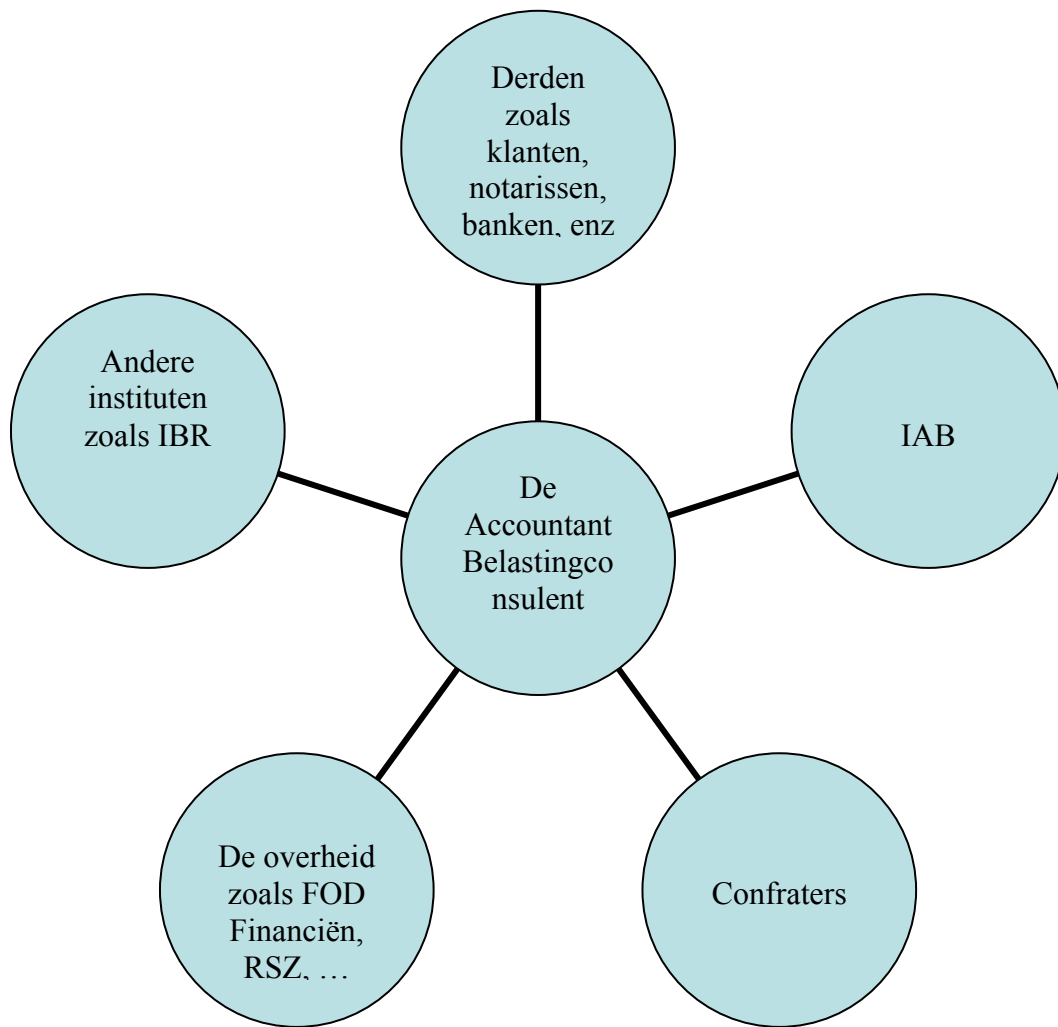
Volgende toepassingen zijn in dat opzicht belangrijk:

1. **Intervat:** het individueel indienen van een elektronische BTW aangifte kan enkel via het Intervat systeem plaatsvinden indien de indiener of de volmachthoudende accountant of belastingconsulent beschikt over een digitale handtekening van Globalsign, Certipost of Isabel.
2. **Vertrouwelijke communicatie:** ten einde op een veilige en zekere wijze elektronische post te verzenden kan dezelfde digitale handtekening gebruikt worden. Niet enkel de afzender wordt onlosmakelijk verbonden met de verzonden e-mail, er kan eveneens met encrypted mail (versleutelde berichten) gecommuniceerd worden.

Deze veilige communicatie kan worden gerealiseerd met een bestemming die eveneens over een digitale handtekening beschikt en is van toepassing op communicatie met:

- Het instituut: veilige gegevens uitwisseling met het IAB. Dit kan betrekking hebben op het overmaken van elektronische exemplaren van een accountantsverslag, het mededelen van het jaarlijks overzicht inzake permanente beroepsvervolmaking, wijziging van de gegevens van een lid, enz.
  - Confraters: onder elkaar kunnen accountants en belastingconsulenten veilig verslagen, balansen, rapporten of andere vertrouwelijke informatie overmaken. Niet enkel jaarrekeningen, ook fiscale aangiftes, e.d.
  - Klanten en derden: dit is zeker de meest aangewezen doelgroep om de digitale handtekening dagelijks te gebruiken! Op dit ogenblik wordt immers veel informatie via elektronische mail doorgezonden die volledig onbeschermd op het net kan worden onderschept en zowel de afzender als de bestemming is zich niet bewust van de onveilige wijze waarop de informatie ter beschikking wordt gesteld. Het overmaken van vertrouwelijke informatie zoals jaarrekeningen, winstberekeningen, tussentijdse resultaatberekeningen, verslagen van fiscale controles, enz zal veilig aan de klanten kunnen worden toegezonden.
3. **Toegang tot een intranet:** de toegang tot het afgeschermd deel van de site van het IAB kan veilig worden geregeld indien de leden van het IAB beschikken over een digitaal certificaat. De leden kunnen via het intranet tevens opgave doen van de verplichte rapportering inzake permanente beroepsvervolmaking, wijziging van de informatie van een lid, het neerleggen van een verslag, het mededelen van vertrouwelijke informatie aangaande tucht, commissie van beroep, e.d. Elke vorm van vertrouwelijke mededeling kan via het up-loaden van informatie veilig gebeuren.

#### **IV. Schematische voorstelling:**



## Welke relaties:

De relaties kunnen als volgt worden besproken:

### 1. Vanuit het standpunt van de Accountant & Belastingconsulent:

- In relatie tot het instituut:
  - Alle vertrouwelijke communicatie en correspondentie
  - Opgave van de gevolgde permanente beroepsvervolmaking
  - Aanpassen van de informatie van de leden in de ledenlijst
  - Neerleggen van verslagen waarvan de mededeling aan het IAB deontologisch wordt opgelegd
  - Neerleggen van documenten betreffende tucht, commissie van beroep, commissie van toezicht, enz
- In relatie tot klanten en derden
  - Alle vertrouwelijke communicatie
  - Afleveren van verslagen en rapporten
  - Bewijzen van lidmaatschap, van beroepsbekwaamheden, van kwalificaties, enz
  - Aangiften van diverse aard (fiscaal, sociaal, parafiscaal, enz) voor de beroepsbeoefenaar zelf of voor zijn klanten
- In relatie tot confraters
  - Alle vertrouwelijke communicatie
  - Het mededelen van kopijs van verslagen en rapporten
  - Elke confraternele mededeling
- In relatie tot de overheid
  - Alle vertrouwelijke communicatie
  - Ledenlijst (Rechtbanken: aanstellen van deskundigen)
  - Het indienen van aangiften met bijlage (Inkomstenbelasting, BTW, RSZ, provinciebelastingen, dimona, kruispuntbank voor ondernemingen, enz)
  - Antwoorden op berichten van wijziging
  - Fiscale akkoorden afsluiten
  - Indienen van bezwaarschriften
- In relatie tot andere instituten
  - Alle vertrouwelijke communicatie
  - Mededelen van kopijs van verslagen en rapporten
  - Bewijzen van lidmaatschap en of beroepsbekwaamheden
  - Ledeninformatie

## 2. Vanuit het standpunt van het IAB

- Vertrouwelijke mededelingen aan de leden, individueel en in groep zoals
  - Betreffende de organisatie van eigen seminaries door het IAB, permanente beroepsvervolmaking, enz
  - Betreffende tucht, commissie van beroep, commissie van toezicht, enz
  - Informatie aan de leden van diverse commissies (Tuchtraad, Commissie van Beroep, Commissie van Toezicht, enz)
- Ledenlijst, verzekering B.A.
- Lijst van de stagemesters en stagiairs
- Toegang tot het intranet
- Bijhouden van een elektronisch dossier met toegang voor het lid zelf:
  - Informatie over het lid (en aanpassing van de gegevens)
  - Informatie inzake jaarlijkse opgave permanente beroepsvervolmaking
  - Ingediende verslagen
  - Dossiers inzake tucht en beroep
  - Specifieke beroepsbekwaamheden
- Aangaande de stagiairs kan er verder uitgewerkt worden in de richting van:
  - Informatie over de stagiair (en aanpassing van de gegevens)
  - Lijst van de stagemesters en stagiairs
  - Gevolgde opleidingen die door het instituut worden georganiseerd
  - Het stageboek met elektronische aanvullingen door de stagemester
  - Eventueel ook e-learning en vervolmakingcursussen voor stagiairs
  - Elektronische verkiezing van de vertegenwoordigers van de stagiairs

## **V. Besluit**

De digitale handtekeningen of certificaten kunnen aangewend worden voor:

- Het digitaal ondertekenen van e-mail
- Het encrypteren van e-mail
- De vertrouwelijke toegang tot het Intranet
- De elektronische indiening van diverse aangiften

Doordat de papierenstromen kunnen vervangen worden door elektronische informatie uitwisseling met het gebruik van de digitale handtekeningen zal er minder papier nodig zijn en de implementatie van de digitale certificaten is dan ook onrechtstreeks milieu vriendelijk.

De informatiestroom vindt elektronisch veel sneller plaats en ze gaat gepaard met een grotere zekerheid en meer vertrouwelijkheid.

Al deze aspecten hebben een grote synergie met de praktijk van de accountant en de belastingconsulent en ze zullen het IAB en haar leden een groot voordeel opleveren betreffende:

- Tijd
- Zekerheid en veiligheid
- Milieu

Deze besparing in middelen en inspanningen die gepaard gaat met meer zekerheid en vertrouwelijkheid kan worden gerealiseerd door de implementatie van de digitale handtekening en de toename van de elektronische communicatie

Erwin VERCAMMEN  
Accountant-Belastingconsulent