Elektronische handtekening
powered by eaZySign ™ Zetes

ABSTRACT: Een elektronische handtekening is een geheel van elektronische gegevens die er voor zorgt dat een persoon de inhoud van een elektronische boodschap goedkeurt. De samenstelling van de elektronische handtekening wordt gereguleerd door verschillende internationale standaarden. Het wettelijk kader van de elektronische handtekening is afhankelijk van de wetgevende instantie.
Deze abstract biedt een antwoord op de manier waarop de elektronische handtekening in het eaZySign platform is gegenereerd en het wettelijk kader ervan binnen het Europees en meer specifiek het Belgisch grondgebied.

Geert Peeters
Project Manager Zetes
mailto:geert.peeters@be.zetes.com

Het begrip 'handtekening'

De techniek om een elektronische handtekening te genereren baseert zicht op bestaande cryptografische elementen. Binnen de cryptografie maakt men gebruik van publieke- en privésleutels om (elektronische) boodschappen te beveiligen.
In het geval van een elektronische handtekening wordt er gebruikt gemaakt van een privésleutel om de boodschap te versleutelen. Via de publieke sleutel kan dan weer gecontroleerd worden dat een boodschap op de juiste manier versleuteld werd. Aangezien de privésleutel enkel in handen is van de ondertekenaar en de publieke sleutel door iedereen kan geraadpleegd worden is het principe van de handtekening gegarandeerd. Enkel de ondertekenaar kan een 'getekende boodschap' maken, iedereen kan controleren dat de boodschap correct ondertekend werd door de ondertekenaar.
Wanneer men een elektronische handtekening wil plaatsen voor een document zal niet het gehele document versleuteld worden. Niet alleen zou de versleuteling tijdsrovend worden (zeker bij grotere documenten), maar tevens zou de inhoud van de inhoud van het document niet op eenvoudige manier (tenzij ontsleuteling) leesbaar blijven.
Daarom maakt de elektronische handtekening gebruik van een zogenaamde digest[1] van het document. Een digest (of checksum) is het resultaat van een cryptograpische hash-functie die beschouwd wordt als onomkeerbaar en representeert de inhoud van het document op een unieke manier. Door de onomkeerbaarheid kan de inhoud van het document niet terug samengesteld worden op basis van de digest. De uniciteit garandeert dan weer dat elke verandering aan het document tot een andere digest zal leiden.
Het plaatsen van een elektronische handtekening op een elektronisch document zorgt er dan ook voor dat volgende principes gegarandeerd worden:

[1] http://en.wikipedia.org/wiki/Message_digest

- Authenticiteit van het document. Door het plaatsen van de handtekening wordt er gegarandeerd dat het document authentiek is. Met ander woorden men is zeker dat het document afkomstig is van de ondertekenaar van het document.
- Integriteit van het document. Door het plaatsen van de handtekening is wordt er gegarandeerd dat de inhoud van het document niet gecompromitteerd werd. Met andere woorden men is zeker dat de inhoud van het document overeenstemt met de inhoud zoals aanwezig bij de ondertekening.
- Terugbrengbaarheid naar de ondertekenaar. Door het plaatsen van de handtekening kan de identiteit van de ondertekenaar op een onweerlegbare manier teruggebracht worden en kan men aantonen dat enkel de ondertekenaar deze handtekening heeft kunnen plaatsen.

PDF-documenten

Het plaatsen van een handtekening heeft op zich niets met de inhoud of formaat van de boodschap te maken. Ieder elektronisch document kan in principe ondertekend worden. Dat betekent eigenlijk dat de handtekening en het document op zich 2 elektronische dragers zijn die logisch geassocieerd worden. Bepaalde formaten van documenten bieden wel een inherent kader van de manier waarop de handtekening en het document geassocieerd worden. De meest bekende en binnen de markt commercieel onafhankelijke[2] formaten zijn PDF[3] en XML.
De manier waarop de associatie tussen de formaten en de elektronische handtekening moet geplaatst en gevalideerd worden is door ETSI vastgelegd in de respectievelijke PAdES[4] en XAdES[5] speficicaties. Deze specificaties werden opgesteld als kader voor het gebruik van de elektronische handtekening en in overeenkomst met de Europese richtlijn 1999/93/EG.

PDF wordt over het algemeen gebruikt als drager van tekst met inhoud, XML als drager van gegevens met een structuur.
Het eaZySign platform is bedoeld om documenten tussen 2 of meer partijen te laten ondertekenen, met als bijkomende eis dat het getekende document ook zonder het platform, offline en op langere termijn kan gevalideerd worden. Met die redenen in het achterhoofd ondersteunt eaZySign enkel het PDF formaat. eaZySign levert getekende documenten die volledig in lijn zijn met de PAdES specificaties en op die manier een breed draagvlak biedt voor het gebruik ervan.

---

[2] Microsoft Office 2007 and Office 2010 laten ook toe om digitale handtekening aan documentformaten zoals MS Word, MS Excell, enz. toe te voegen. De Office formaten zijn onder beheer en bezitsrecht van Microsoft.
[3] Adobe Systems ligt aan de basis van het PDF formaat, maar de PDF formaat werd vrijgegeven en als open standaard door ISO gepubliceerd op 1/7/2008. De standaard is gekend als de ISO32000:1 standaard en is vrij raadpleegbaar via www.iso.org
[4] http://en.wikipedia.org/wiki/PAdES
[5] http://en.wikipedia.org/wiki/XAdES

Wettelijk kader

Binnen de EU en in het Belgisch grondgebied bestaan er resp. verordeningen en Koninklijke Besluiten die het wettelijk kader van het gebruik van een elektronische handtekening vastleggen.
Deze zijn in chronologische volgorde:

- De Europese richtlijn 1999/93/EG die werd omgezet in het Wet van 9 juli 2001, de zogenaamde Wet op de Elektronische Handtekening.
- De Europese verordening 910/2014 van 23 juli 2014 betreffende elektronische identificatie en vertrouwensdiensten in de interne markt en tot intrekking van Richtlijn 1999/93/EG. Deze verordening zal vanaf 1 juli 2016 de Wet van 9 juli 2001 vervangen.

Volgens artikel 4 § 4 van de Wet van 9 juli 2001 geldt dat een geavanceerde handtekening op basis van een gekwalificeerd certificaat en aangemaakt met een veilig middel voor het aanmaken van de handtekening gelijkgesteld wordt met een handgeschreven handtekening. Dit principe wordt ook in de nieuwe verordening behouden.

De geavanceerde handtekening is een elektronische handtekening waarbij aan 4 vereisten moet voldaan worden, dit zijn:

1. Ze is op een unieke wijze aan de ondertekenaar verbonden zijn;
2. Ze maakt het mogelijk de ondertekenaar te identificeren;
3. Zij komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan gebruiken; en
4. Zij is op zodanige wijze verbonden aan de gegevens waarop zij betrekking heeft dat elke wijziging achteraf van de gegeven kan opgespoord worden.

Een gekwalificeerd certificaat is een middel dat de geavanceerde handtekening koppelt aan een identificeerbare persoon. Met behulp van dit certificaat kan de ontvanger de handtekening verifiëren en gebeurt aan de hand van de publieke sleutel van die gekoppeld wordt aan de plaatser van de handtekening. Om als gekwalificeerd te worden aanzien moet het certificaat voldoen aan een twintigtal vereisten.

Het gebruik van de Belgische eID voor het aanmaken van de elektronische handtekening voldoet aan alle eisen en kan onbetwistbaar[6] beschouwd worden bij het plaatsen van een elektronische handtekening.

Validatie

Om een handtekening door een derde partij te kunnen laten controleren moet alle elementen die de validatie van die handtekening mogelijk maken ingebakken worden in de handtekening. Eén van de elementen is de controle van de geldigheid van het gebruikte certificaat op het ogenblik van de handtekening.

[6] Jos Dumortier, Legally valid electronically signed PDF documents using the Belgian e-ID 2007, 19p. www.law.kuleuven.be/icri

Een certificaat kan immers vervallen (geldigheidstermijn verstreken) of een certificaat kan ook ingetrokken ('revoced') worden. Deze controle gebeuren bij de uitgever van het certificaat. Deze controles staat ook bekend als de intrekkingstatus van de handtekening (in concreto gebruikt men hiervoor de OCSP[7]- of CRL[8]-informatie).
Zodra een certificaat verloopt, is de instantie van afgifte niet langer verantwoordelijk voor het verstrekken van intrekkingsstatus op dat certificaat. Zonder conforme intrekkingsstatus, kan de handtekening niet worden gevalideerd.

Met langetermijnhantekeningvalidatie (LTV) kan men de geldigheid van een handtekening lang controleren nadat het document werd ondertekend. Zonder bepaalde extra informatie toe te voegen kan een elektronische handtekening immer gevalideerd worden voor een beperkte tijd. De vereiste elementen voor de vaststelling van de geldigheid van een handtekening zijn de volledige certificaatsketen, de intrekkingsstatus en een officiële tijdsstempel[9]. Zonder deze officiële tijdsstempel is het bijgevolg onmogelijk om de rechtsgeldigheid af te dwingen van een contract waarbij het moment van ondertekening een rol kan spelen. Als deze elementen aanwezig zijn kan de handtekening door derde partijen gevalideerd worden.

Volgens de PAdES standaard worden deze vereiste element ingebed in het ondertekende PDF. Het inbedden van deze elementen gebeurt wanneer het document wordt ondertekend of bij het aanmaken van de elektronische handtekeningen.

Een document dat door eaZySign wordt ondertekend voldoet aan de PAdES-LTV standaarden en kan dus voor langere termijn gevalideerd worden. Dit kan onder andere gebeuren door veel verspreide middelen zoals Acrobat Reader.

---

[7] OCSP staat voor Online Certificate Status Protocol. Zie ook http://*en.wikipedia.org/wiki/Online_Certificate_Status_Protocol* . Voor de Belgische eID is er een vrij raadpleegbare OCSP responder (ocsp.eid.belgium.be) ter beschikking die wordt beheerd door de Belgische overheid (Fedict).
[8] CRL staat voor Certificate Revocation List. Zie ook http://en.wikipedia.org/wiki/Revocation_list
[9] Een officiële tijdsstempel kan enkel worden verleend door een TSA (Time Stamp Authority). Een lokale tijdsaanduiding van een desktop of een server geldt niet als officiële tijdsstempel.