



notitie

AdES Baseline Profiles-standaard en overzicht
reacties consultatieronde

FORUM STANDAARDISATIE

Forum Standaardisatie

www.forumstandaardisatie.nl

forumstandaardisatie@logius.nl

Bureau Forum**Standaardisatie**

gehuisvest bij Logius

Postadres

Postbus 96810

2509 JE Den Haag

Bezoekadres

Wilhelmina van Pruisenweg 52

2595 AN Den Haag

Bij bezoek aan Logius is

legitimatie verplicht

Agendapunt:	3A		
Betreft:	Expertadvies AdES Baseline Profiles-standaard en overzicht reacties consultatieronde		
Aan:	Forum Standaardisatie		
Van:	Stuurgroep Standaardisatie		
Datum:	6 oktober 2016	Versie	1.0

Aanleiding en achtergrond

Elektronische handtekeningen worden gebruikt voor het ondertekenen van digitale documenten. Een elektronische handtekening is voor de ontvanger het bewijs dat een elektronisch document inderdaad afkomstig is van de ondertekenaar en dat deze de inhoud ervan onderschrijft. Voor het ondertekenen van documenten die een hoge mate van betrouwbaarheid (integriteit), authenticiteit en onweerlegbaarheid vereisen, kunnen geavanceerde elektronische handtekeningen of gekwalificeerde elektronische handtekeningen worden gebruikt.

Ingediend zijn de AdES Baseline Profiles. Dit zijn standaarden die worden gebruikt voor het ondertekenen van XML-documenten (XAdES), PDF-documenten (PAdES), CMS-documenten (CAdES) en documentcontainers/ZIP (ASiC) met een geavanceerde/gekwalificeerde elektronische handtekening.

Een ondertekenaar is op dit moment vrij in de keuze van een standaard voor het zetten van een geavanceerde/gekwalificeerde elektronische handtekening. Het gevolg is dat een ondertekenaar een document kan tekenen op basis van een standaard die niet hetzelfde is als de standaard die de ontvanger ondersteunt. In de praktijk is de situatie dat een ontvanger niet van tevoren weet of én op welke manier de handtekening gevalideerd kan worden. Een handtekening kan dan onleesbaar blijken voor de ontvanger. Waardoor de betrouwbaarheid, authenticiteit en onweerlegbaarheid van de handtekening niet kan worden vastgesteld. Ook kan dit betekenen dat een derde partij, zoals een controlerende instantie, niet vooraf kan bepalen of deze de handtekening kan valideren.

Om zeker te stellen dat de ontvanger de handtekening van de ondertekenaar kan valideren is het noodzakelijk om een gemeenschappelijke set opties (een profiel) te selecteren. De AdES Baseline Profiles beschrijven dergelijke profielen. Door een standaard met vooraf vastgesteld profiel verplicht te stellen is het voor zowel de ondertekenaar als de ontvanger duidelijk met welke standaard een handtekening dient te worden gezet, welke informatie is opgenomen in de handtekening (profiel) en op welke manier de handtekening gevalideerd kan worden. De AdES Baseline profiles zorgen ervoor dat een handtekening uitgewisseld kan worden zonder dat er vooraf afspraken gemaakt hoeven te worden tussen ondertekenaar en ontvanger(s).

Opname op de lijst zou het gebruik van de standaarden moeten bevorderen.

Betrokkenen en proces

AdES Baseline Profiles is aangemeld door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Vervolgens heeft een intake en experttoets plaatsgevonden. Door de lage opkomst bij de expertbijeenkomst is er voor gekozen om een aantal experts schriftelijk input te laten leveren op het expertadvies. Het expertadvies vat de uitkomsten van de discussie en toetsing samen en is als zodanig in openbare consultatie geplaatst. Er zijn vier reacties ontvangen vanuit de openbare consultatie welke zijn verwerkt in dit Forumadvies. De reacties zijn overwegend positief en voornamelijk gericht op de praktische toepassing van de standaarden.

Consequenties en vervolgstappen

Op dit moment is het gebruik van geavanceerde/gekwalificeerde elektronische handtekeningen beperkt, het gebruik bevorderen via de lijst zorgt ervoor dat gelijk met juiste standaarden wordt gewerkt en legacy problemen voorkomen. Het verplicht stellen van de AdES Baseline Profiles draagt actief bij aan de interoperabiliteit tussen (semi) overheidsorganisaties, het bedrijfsleven en burgers.

Naar aanleiding van de expertbijeenkomst en openbare consultatie staan er nog teveel vragen open om nu al te kunnen besluiten over opname. De stuurgroep Open Standaarden stelt voor om eerst nog een aanvullend onderzoek uit te voeren voordat een besluit kan worden genomen. Naar verwachting volgen de uitkomsten hiervan in de Forumvergadering van december.

Gevraagd besluit

Naar aanleiding van de expertbijeenkomst en openbare consultatie staan er naar inzien van de stuurgroep Open Standaarden nog teveel vragen open om al te kunnen besluiten over opname. Gevraagd wordt om samen met de indiener deze nader uit te zoeken voordat wordt ingestemd met een eventuele opname, het gaat om de volgende vragen:

- *Hoe verder na opname: Op welke manier kan er een actieve community gevormd worden die de adoptie van de standaard ondersteunt en die fungeert als aanspreekpunt waar overheden terecht kunnen voor vragen over (toepassing van) de standaard? Dit sluit aan op criterium 2.6 van de toetscriteria.*
- *Meer inzicht in bestaande use cases (voor alle vier de profiles) en of deze gebruikt kunnen worden als praktijkvoorbeelden voor implementatie? Dit sluit aan op criterium 1.3 van de toetscriteria.*
- *Meer inzicht waar de standaarden ondersteunt worden (software / leveranciers en op welke manier overheden ondersteund worden bij de technische implementatie van de standaard? Dit sluit aan op criteria 3.1 van de toetscriteria.*

Ook wordt geadviseerd om op basis van bovenstaande vragen nogmaals kritisch te kijken naar het toepassingsgebied en of deze niet verduidelijkt kan worden.

Over het toepassingsgebied en werkingsgebied

Ad 1 Opname van AdES Baseline Profiles op de lijst met open standaarden

Er zijn verschillende overheidsorganisaties die geavanceerde/gekwalificeerde elektronische handtekeningen gebruiken (o.a. Kamer van Koophandel, Voedsel en Warenautoriteit, Autoriteit Consument & Markt en RDW) of willen gebruiken. Tevens zijn er bedrijven die diensten aanbieden voor geavanceerde/gekwalificeerde elektronische handtekeningen (o.a. QuoVadis, Evidos, Validata Group, KPN). Uit de expertbijeenkomst bleek dat overheidsorganisaties en bedrijven behoefte hebben aan een standaard die er voor zorgt dat handtekeningen zonder interoperabiliteitsproblemen uitgewisseld kunnen worden.

De AdES Baseline Profiles zijn volwassen standaarden die al een langere tijd bestaan. De standaarden beschrijven het gebruik van standaardprofielen voor geavanceerde/gekwalificeerde elektronische handtekeningen. Het verplicht stellen van de AdES Baseline Profiles draagt actief bij aan de interoperabiliteit tussen (semi-)overheidsorganisaties, het bedrijfsleven en burgers. Op praktisch vlak is er behoefte aan validatie van authenticiteit van digitale documenten.

Als functioneel toepassingsgebied voor AdES Baseline Profiles wordt geadviseerd: *De AdES Baseline Profiles zijn van toepassing op documenten in de vorm van een XML-, PDF-, CMS-, en ZIP-bestand dat is voorzien van een geavanceerde en/of gekwalificeerde elektronische handtekening of zegel (inclusief tijdstempels)*¹.

¹ Op grond van de gelijkgeschakeling in artikelen 27 ('Elektronische handtekeningen in openbare diensten') en 37 ('Elektronische zegels in openbare diensten') in verordening 910/2014, moet waar dit document spreekt over 'handtekening' steeds 'handtekening of zegel' gelezen worden.

Toelichting op het toepassingsgebied: De AdES Baseline Profiles richten zich op de ondertekening van documenten en niet op het de authenticiteit van berichtenverkeer.

Het betreft hier het toepassen van de standaard. Op grond van wettelijke regelingen zoals Besluit 2011/130/EU, Verordening 910/2014 van het Europees Parlement en de Raad en het Uitvoeringsbesluit 2015/2016 van de Europese Commissie dient de standaard al geaccepteerd te worden bij ontvangst.

Als organisatorisch werkingsgebied van AdES Baseline Profiles wordt geadviseerd: *Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.*

Ad 2 Additionele adviezen ten aanzien van de adoptie van de standaard

Ten aanzien van de adoptie van de standaard worden de volgende oproepen gedaan:

1. Het opnemen van een toelichting bij publicatie van de standaard op de website, waarbij het verschil en de overeenkomst tussen een gewone (ook wel natte) handtekening, een elektronische handtekening en een geavanceerde/gekwalificeerde elektronische handtekening wordt uitgelegd met een verwijzing naar artikel 15a Boek 3 van het Burgerlijk wetboek en de Richtlijn 1999/93/EG van het Europees Parlement.
2. Op basis van het aanvullend onderzoek met de stakeholders bepalen of er behoefte is aan een onderzoek naar aanvullende standaarden voor het beschrijven van tijdstempelautoriteiten.
3. PKI-overheid wordt opgeroepen om over te gaan tot onderzoek naar mogelijkheden voor aanpassing van de middelen om tijdstempels te ondersteunen bij het gebruik van een PKI certificaat.

Toelichting

1. Waar gaat het inhoudelijk over?

Elektronische handtekeningen worden gebruikt voor het ondertekenen van digitale berichten. Een elektronische handtekening is voor de ontvanger het bewijs dat een elektronisch bericht inderdaad afkomstig is van de ondertekenaar en dat deze de inhoud van het bericht onderschrijft. Voor het ondertekenen van berichten die een hoge mate van betrouwbaarheid (integriteit), authenticiteit en onweerlegbaarheid vereisen, kunnen geavanceerde elektronische handtekeningen of gekwalificeerde elektronische handtekeningen worden gebruikt.

Een organisatie dient zelf te bepalen welke mate van betrouwbaarheid, authenticiteit en onweerlegbaarheid vereist is voor ondertekening. Afhankelijk van het gewenste mate van betrouwbaarheid, authenticiteit en onweerlegbaarheid kan de organisatie er voor kiezen om te tekenen met een eenvoudige elektronische handtekening (bijvoorbeeld een ingescande handtekening of handtekening onder een e-mailbericht), een geavanceerde elektronische handtekening of een gekwalificeerde elektronische handtekening.

Een geavanceerde elektronische handtekening² voldoet aan vier eisen:

1. De handtekening is op unieke wijze aan de ondertekenaar verbonden;
2. De handtekening maakt het mogelijk de ondertekenaar te identificeren;
3. De handtekening komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
4. De handtekening is op zodanige wijze aan het elektronisch bestand waarop zij betrekking heeft verbonden, dat elke wijziging van de gegevens, na ondertekening, kan worden opgespoord.

Een gekwalificeerde handtekening is een geavanceerde handtekening gegenereerd met behulp van een veilig middel zoals een smartcard of token. Het certificaat moet door een erkende certificatieinstantie zijn uitgegeven. Deze certificatieinstantie moet door de toezichthouder (op dit moment Autoriteit Consument & Markt³) ingeschreven en erkend zijn.

De ingediende standaarden worden gebruikt voor het ondertekenen van XML-documenten (XAdES), PDF-documenten (PAdES), CMS-documenten (CAdES) en documentcontainers/ZIP (ASiC) met een geavanceerde/gekwalificeerde elektronische handtekening.

Door het toevoegen van een tijdstempel kan de authenticiteit en het bestaan van een document op een bepaald moment worden bevestigd. Voor het creëren van de tijdstempel kan gebruik gemaakt worden van een onafhankelijke tijdstempelautoriteit. Er zijn op dit moment nog geen kwaliteitseisen of openbare standaarden vastgesteld voor tijdstempelautoriteiten.

Juridisch kader

Het juridisch kader (waaronder Besluit 2011/130/EU, Verordening 910/2014 van het Europees Parlement en de Raad en het Uitvoeringsbesluit 2015/2016 van de Europese Commissie) verplicht op dit moment de ontvanger om een geavanceerde/gekwalificeerde elektronische handtekening op basis van de AdES-standaarden te accepteren. Voor het zetten van een geavanceerde/gekwalificeerde elektronische handtekening op basis van de AdES-standaarden is geen verplichting. Het verplicht stellen van het gebruik van de AdES-standaarden zorgt er voor dat zowel bij het ondertekenen als bij het ontvangen van geavanceerde/gekwalificeerde elektronische handtekeningen de AdES-standaarden verplicht zijn.

Type documenten

De documenten die ondertekend kunnen worden met de AdES-standaarden worden voor verschillende doeleinden gebruikt:

XML: Standaard voor een opmaaktaal waarmee gestructureerde gegevens in de vorm van platte tekst wordt opgeslagen. XML is zowel voor computers als mensen leesbaar. Onder andere Word- en ODF-documenten worden ondertekend als XML documenten.

PDF: Standaard voor de uitwisseling van elektronische documenten en formulieren waarbij de lettertypen, afbeeldingen en lay-out van het bronbestand behouden blijven.

CMS: Standaard voor cryptografische beschermde (versleutelde) digitale data.

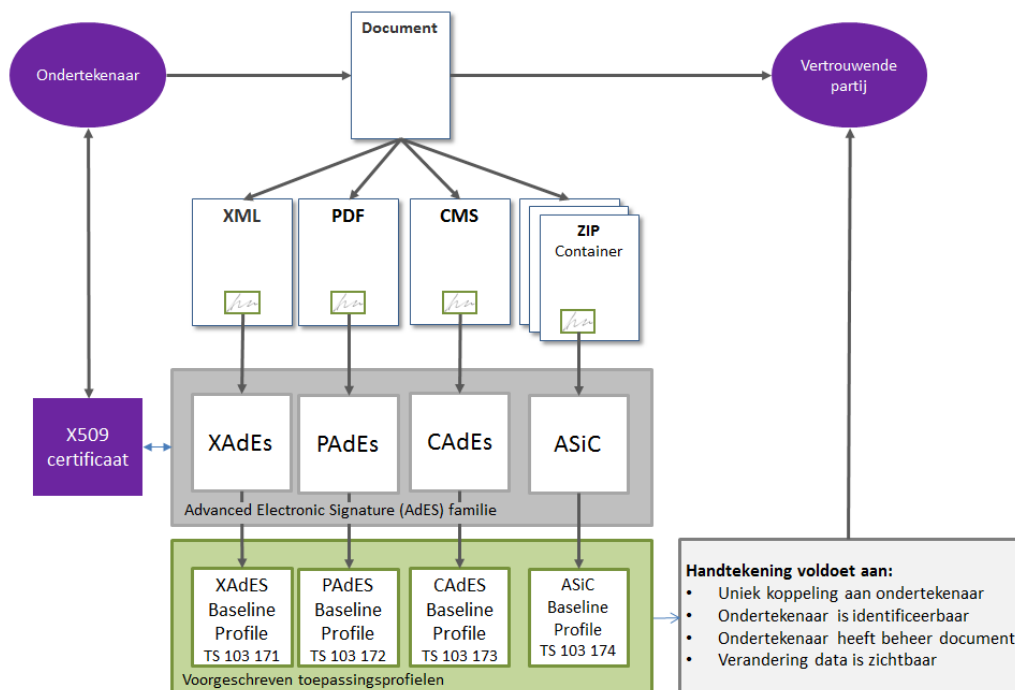
² Richtlijn 1999/93/EG van het Europees Parlement en de Raad, artikel 2 (<http://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:31999L0093&from=NL>)

³ Deze situatie verandert bij inwerkingtreding van wetsvoorstel 34 413 waarbij het toezicht belegd kan worden bij Agentschap Telecom (<https://zoek.officielebekendmakingen.nl/kst-34413-4.html>)

Documentcontainers/ZIP: Standaard voor een bestandstype waarbij objecten (o.a. teksten, spreadsheets en multimedia) gezamenlijk in een containerbestand worden opgeslagen.

Profielen AdES

De AdES-standaarden bevatten meerdere opties die in een handtekening kunnen worden gebruikt. Hierdoor zijn binnen deze standaarden meerdere variaties in de opmaak van dergelijke geavanceerde/gekwalificeerde elektronische handtekeningen mogelijk. Als een ondertekenaar een variatie gebruikt die niet door de ontvanger wordt ondersteund, is de handtekening niet zonder meer leesbaar voor de ontvanger. Om zeker te stellen dat de ontvanger de handtekening van de ondertekenaar kan valideren is het noodzakelijk om een gemeenschappelijke set opties te selecteren. Een dergelijke selectie wordt een profiel genoemd. In figuur 1 zijn de AdES-standaarden en bijbehorende profielen weergegeven.



Figuur 1: Schematische weergave AdES-standaarden en AdES Baseline Profiles

De AdES Baseline Profiles beschrijven dergelijke profielen. Per bestandstype is er door ETSI op verzoek van de Europese Commissie een Baseline Profile vastgesteld waarin staat welke informatie minimaal opgenomen moet zijn in een geavanceerde /gekwalificeerde elektronische handtekening.

Use case

Voorbeeld van een use case: Een overheidsorganisatie verstrekt een document, bijvoorbeeld een vergunning, in PDF-formaat aan burgers. Het document wordt gewaarmerkt met een digitale handtekening. Deze handtekening geeft de garantie dat de handtekening is gezet door de overheidsorganisatie en dat de informatie in het document door de overheidsorganisatie is bevestigd. Een derde partij, een controlerende instantie, heeft de taak het document van de burger te controleren.

Zonder AdES Baseline Profiles kan elke overheidsorganisatie ervoor kiezen om een eigen profiel te gebruiken voor de ondertekening van een digitale beschikking met een geavanceerde elektronische handtekening. Het is daardoor mogelijk dat de controlerende instantie de elektronische handtekening niet kan controleren. De burger heeft niet de mogelijkheid om het profiel van de handtekening aan te passen en zal dus op een andere manier de rechtmatigheid van het digitale document aan moeten tonen. Als de controlerende instantie alsnog het digitale document wil controleren dan moet de software aangepast worden of moeten er afspraken worden gemaakt tussen de controlerende instantie en de overheidsorganisatie.

In het geval dat de AdES Baseline Profiles verplicht zijn gesteld, is het voor alle betrokken partijen duidelijk welke standaard en welk profiel gebruikt moet worden voor een geavanceerde/gekwalificeerde elektronische handtekening. De AdES Baseline Profiles zullen in dat geval geaccepteerd worden in het PDF programma Adobe Reader. Hierdoor is het voor de burger direct mogelijk om te controleren of de handtekening klopt. De controlerende instantie weet welk profiel er gebruikt is om de elektronische handtekening te zetten en kan de handtekening direct valideren.

2. Hoe is het proces verlopen?

Om te komen tot dit Forumadvies zijn de volgende stappen doorlopen:

- Door de procedurebegeleider is een intakegesprek gevoerd met de indiener op 22 april 2016.
- Op basis van de intake is op 8 juni 2016 door het Forum besloten de aanmelding in procedure te nemen. Op basis van dit besluit is een expertgroep samengesteld en een voorzitter aangesteld.
- Op 30 juni 2016 is de expertgroep bijeengekomen om de bevindingen te bespreken. Tijdens deze bijeenkomst zijn ook het toepassings- en werkingsgebied vastgesteld.
- De uitkomsten van de expertgroep zijn door de begeleider verwerkt in dit adviesrapport. Een eerste conceptversie is aan de leden van de expertgroep gestuurd met het verzoek om een reactie. Tevens is de eerste conceptversie van het adviesrapport gedeeld met drie experts die niet aanwezig waren bij de expertbijeenkomst. Via telefonische afstemming hebben zij hun reactie kunnen geven op het document.
- Na verwerking van deze reacties is het rapport afgerond, nogmaals toegestuurd aan de experts en ingediend bij het Bureau Forum Standaardisatie ten behoeve van de publieke consultatieronde.
- Uit de publieke consultatie zijn 4 reacties ontvangen, welke zijn verwerkt in dit Forumadvies.

3. Hoe scoort de standaard op de toetsingscriteria?

Toegevoegde waarde

De expertgroep concludeert dat de standaarden voldoende toegevoegde waarde hebben binnen het geadviseerde functioneel toepassingsgebied en organisatorisch werkingsgebied.

De AdES Baseline Profiles zorgen ervoor dat een geavanceerde/gekwalificeerde elektronische handtekening voor de ondertekenaar en ontvanger uitwisselbaar is door eisen te stellen aan de minimale set aan informatie die wordt uitgewisseld.

Hierbij wordt er geen softwarepakket voorgeschreven, maar is het mogelijk om de handtekening te tekenen en te valideren met elk pakket dat AdES Baseline Profiles ondersteunt.

De standaarden dragen bij aan efficiëntie, vereenvoudiging en aan verlaging van de gehele productiekosten voor leveranciers en daarmee afname van de kosten voor afnemers. Tevens zorgen AdES Baseline Profiles voor de mogelijkheid van borging van authenticiteit bij langdurige archiefopslag. De kosten voor technische implementatie zijn niet hoger dan de implementatie van geavanceerde/gekwalificeerde elektronische handtekeningen gebaseerd op een ander profiel dat voldoet aan de eisen voor een geavanceerde/gekwalificeerde elektronische handtekening. De kosten van de implementatie bestaat uit de technische implementatie aanschaf van de software, opleiding van personeel en afname van diensten voor certificaten en tijdstempels. De kosten voor de certificaten zijn afhankelijk van het aantal gebruikers. De diensten voor tijdstempels worden aangeboden op basis van jaarlijkse abonnementen. Er zijn geen beveiligings- en privacyrisico's geïdentificeerd aan het implementeren en gebruiken van de standaarden.

Open standaardisatieproces

De expertgroep concludeert dat de ontwikkeling van de AdES Baseline Profiles voldoet aan alle kenmerken van een open standaardisatieproces. De standaard is ontwikkeld door ETSI, een Europese onafhankelijke partij. De Nederlandse overheid is lid van de ontwikkelorganisatie. De besluitvorming vindt plaats op een open en transparante wijze. De documentatie is drempelloos verkrijgbaar.

Draagvlak

De expertgroep concludeert dat het gebruik van de AdES Baseline Profiles voldoende draagvlak heeft. Er zijn positieve signalen over het toekomstig gebruik van de standaard. Op dit moment is de adoptie van de standaarden beperkt. Het verplichte karakter van de standaarden zal leiden tot een bredere adaptatie van de AdES-standaarden. Als zowel bij het ondertekenen als bij het ontvangen van geavanceerde/gekwalificeerde elektronische handtekeningen de AdES-standaarden verplicht zijn, is het eenvoudiger om geavanceerde/gekwalificeerde elektronische handtekeningen te hanteren. De AdES Baseline Profiles zijn vrij beschikbaar en vrij toe te passen. De standaarden zijn derhalve niet gekoppeld aan een beperkt aantal leveranciers.

De AdES-standaarden worden ondersteund door betaalde software en opensource software. Voorbeelden hiervan zijn de Digital Signature Service van de Europese Commissie, Microsoft Word (XAdES), OpenOffice (XAdES), Adobe Acrobat Reader (PAdES), SigningHub (PAdES), Aloaho Signer (CAdES), P7S Signer (CAdES), DigiDoc3 (ASiC). Daarnaast zijn er verschillende opensource projecten en ondertekendiensten waarbij onderteken- en validatiemogelijkheden worden ontwikkeld voor de AdES-standaarden.

CEF eSignatures ondersteunt overheden bij de implementatie van de AdES Baseline Profiles. Deze ondersteuning is voornamelijk gericht op de implementatie van de Digital Signature Services van de Europese Commissie. Er is in Nederland geen actieve community voor geavanceerde/gekwalificeerde elektronische handtekeningen op basis van de AdES Baseline Profiles.

Opname bevordert de adoptie

De expertgroep concludeert dat opname op de lijst een passend middel is om de adoptie van de standaarden binnen de (semi)overheid te bevorderen. Op dit moment is de adoptie beperkt en zal een verplicht karakter van de standaarden leiden tot een bredere adoptie. Uit de aanmelding van de standaarden en de bijeenkomst van de expertgroep blijkt dat verschillende partijen zoekende naar een standaard die gebruikt kan worden voor geavanceerde/gekwalificeerde elektronische handtekeningen. De AdES Baseline Profiles zijn volwassen standaarden die al een langere tijd bestaan. Het verplicht stellen van de AdES Baseline Profiles draagt actief bij aan de interoperabiliteit tussen (semi) overheidsorganisaties, het bedrijfsleven en burgers. Op praktisch vlak is er veel behoefte aan validatie van authenticiteit van digitale documenten.

*Toelichting eventuele risico's*4. Wat is de conclusie van de expertgroep en de consultatie?*Conclusie van de expertgroep*

De expertgroep adviseert het Forum Standaardisatie en het Nationaal Beraad Digitale Overheid om de AdES (Advanced Electronic Signature) Baseline Profiles op te nemen op de lijst met open standaarden, met 'pas toe of leg uit'-verplichting.

Eventuele aanvullingen vanuit de consultatie

Er zijn reacties ontvangen van Bureau Edustandaard, CIO Rijk, DigiKoppeling en Expertisecentrum Justid. Op basis van de reactie van DigiKoppeling is er een aanvulling gedaan op de adoptieadviezen. De reactie van het expertisecentrum Justid heeft invloed op formulering van het toepassingsgebied.

Bureau Edustandaard

Bureau Edustandaard geeft aan dat de standaarden geen (direct) impact heeft op het onderwijs en de onderwijsstandaarden.

Reactie:

De reactie van Bureau Edustandaard heeft geen effect op het forumadvies.

CIO Rijk

CIO Rijk geeft aan dat duidelijk moet zijn dat niet alle documenten elektronisch ondertekend zouden moeten worden.

Reactie:

Het CIO Rijk vraagt om een toelichting waarin het verschil en de overeenkomst tussen een gewone (ook wel natte) handtekening, een elektronische handtekening en een geavanceerde/gekwalificeerde elektronische handtekening wordt uitgelegd. Het Bureau Forum Standaardisatie is bezig met de ontwikkeling van een handreiking betrouwbaarheidsniveau waarin de toepassing van (elektronische) handtekeningen worden toegelicht. In de conceptversie van de handreiking is ook een toelichting opgenomen voor het praktisch gebruik van geavanceerde/gekwalificeerde handtekeningen opgenomen.

DigiKoppeling

Uit een gesprek met een van de experts bleek dat er een mogelijk overlap is tussen de AdES Baseline Profiles en Digikoppeling. Digikoppeling heeft een kort onderzoek gedaan naar de overlap en de resultaten verwerkt in een memo.

De standaarden Digikoppeling en AdES hebben naar de mening van Digikoppeling een ander organisatorisch werkingsgebied en kennen slechts in specifieke gevallen een overlap. Voor het begrip van niet-specialisten is het van belang dit organisatorisch werkingsgebied op z'n minst duidelijk wordt verwoord in beide standaarden. Hoofdstuk 2 van het expertadvies geeft volgens Digikoppeling onvoldoende invulling aan. Voor de verdere ontwikkeling van de standaarden en de praktische toepassing van beide standaarden is praktisch inhoudelijk onderzoek nodig. Op korte termijn kan dit leiden tot het opstellen van een best practice die beschrijft wanneer signing van het berichtenverkeer dan wel signing van documenten noodzakelijk is. Op de lange termijn is een visie gewenst op het gebruik van signing en encryptie binnen de overheid. Omdat AdES nauw verwant is met standaarden als Digikoppeling, PKIoverheid en ook eHerkenning (SAML-tokens gebruiken soortgelijke technologie) is het volgens Digikoppeling aan te raden om op korte termijn in een best practice aan te geven wanneer je (een van) beide standaarden kan en moet toepassen.

Reactie:

Volgens Digikoppeling hebben AdES Baseline Profiles en Digikoppeling een ander organisatorisch werkingsgebied en kennen slechts in specifieke gevallen een overlap. Dit heeft geen invloed op de opname van de AdES Baseline Profile op de lijst met open standaarden.

De aanvulling dat het functioneel toepassingsgebied en het organisatorische werkingsgebied volgens Digikoppeling onvoldoende invulling geeft, wordt geadresseerd door, zoals reeds opgenomen in het additionele adoptieadvies, een toelichting bij publicatie op te nemen waarbij het verschil en de overeenkomst tussen een gewone (ook wel natte) handtekening, een elektronische handtekening en een geavanceerde/gekwalificeerde elektronische handtekening wordt uitgelegd. Naar aanleiding van de reactie van Digikoppeling is de aanbeveling voor het opstellen van een best practice opgenomen als adoptieadvies.

Expertisecentrum Justid

Het Expertisecentrum Justid heeft haar reactie verwerkt in de PDF-versie van het Expertadvies AdES Baseline Profiles, versie 1.0. In de reactie komen een aantal onderwerpen aan bod:

- Het Expertisecentrum benoemt de Lange Termijn Validatie (LTV) van PDF. In de reactie wordt gesteld dat de LTV alleen mogelijk is door in het bestand ruimte te reserveren voor herhaalde validatie. Daarnaast worden de beperkingen genoemd van PDF/A-1 ten opzichte van de LTV-tijdstempel.
- In de reactie wordt gevraagd naar het mogelijke internationale draagvlak voor de standaard.
- De gebruikte applicatie moet volgens het Expertisecentrum ondersteuning bieden aan zowel het ondertekenen als het valideren. Tevens geeft het expertisecentrum aan dat er een courante lezer vereist is om te kunnen valideren en vraagt of dit kan worden opgelegd ondanks dat ze gratis zijn.
- Er wordt gevraagd of OCSP (Online Certificate Status Protocol) een mogelijk beveiligingsrisico is bij het adopteren van de standaard.

Reactie:

- De keuze om geavanceerde/gekwalificeerde handtekeningen toe te passen voor PDF/A-1 of PDF 1.7 is een keuze die elke organisatie zelf kan maken. Het toepassen van lange termijn validatie vereist een configuratieaanpassing in gangbare applicaties zoals Acrobat Reader en Microsoft Word. Deze aanpassing is nodig om de handtekening te verbinden aan het elektronisch bestand waarop zij betrekking heeft, zodat elke wijziging van de gegevens, na ondertekening, kan worden opgespoord zoals vereist is voor een geavanceerde/gekwalificeerde elektronische handtekening. De kosten die nodig zijn voor de configuratieaanpassing zijn per definitie nodig om de gratis applicaties te koppelen aan een tijdstempelservers.
- De standaarden die door ETSI worden ontwikkeld kunnen wereldwijd worden toegepast. Zoals ook in het expertadvies is aangegeven, zijn er geen alternatieve standaarden die een vergelijkbare basis bieden voor het gebruik van geavanceerde/gekwalificeerde elektronische handtekeningen.
- Er kunnen verschillende applicatie worden gebruikt voor het lezen en/of valideren van de geavanceerde/gekwalificeerde elektronische handtekening. Het gebruik en ondersteuning van de AdES Baseline Profiles zorgt er voor dat er kan worden uitgewisseld tussen programma die de standaard ondersteunen. Voor het valideren van de geavanceerde/gekwalificeerde elektronische is het inderdaad van belang dat er een courante lezer vereist wordt. Dit geldt voor alle praktische toepassingen van geavanceerde/gekwalificeerde elektronische handtekeningen. De toepassing van de AdES Baseline Profiles is niet applicatiegebonden, daarbij is het verplicht stellen van een specifieke applicatie dus niet nodig en zorgt een open standaard zelf voor een vrije keuze in applicaties.
- OSCP maakt onderdeel van de standaard die het x.509-certificaat beschrijft. Het risico dat OSCP geen encryptie ondersteund is een kwetsbaarheid van de standaard X.509. De standaard X.509 is opgenomen in de lijst van open standaarden (<https://www.forumstandaardisatie.nl/standaard/x509>). De kwetsbaarheid maakt het mogelijk dat een derde ongewenst informatie verkrijgt via zogenaamde 'man-in-the-middle'-aanval. De kwetsbaarheid is echter geen kwetsbaarheid van de AdES Baseline Profiles, maar van het protocol OSCP wat gebruikt wordt om een lijst met ingetrokken certificaten op te halen.

De AdES Baseline Profiles schrijft voor dat er gebruik wordt gemaakt van de gangbare protocollen om een ingetrokken certificaten te identificeren. Dit kan OSCP zijn, maar ook het protocol CRL (Certificate Revocation List). Het gebruik van de AdES Baseline Profiles introduceert dus geen nieuwe informatiebeveiligingsrisico's.

5. Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?

Naar aanleiding van de expertgroep zijn er bij opname op de lijst met open standaarden de volgende oproepen ten aanzien van de adoptie van de standaard te doen:

1. Een opname van een toelichting bij publicatie van de standaard op de website, waarbij het verschil en de overeenkomst tussen een gewone (ook wel natte) handtekening, een elektronische handtekening en een geavanceerde/gekwalificeerde elektronische handtekening wordt uitgelegd met een verwijzing naar artikel 15a Boek 3 van het Burgerlijk wetboek en de Richtlijn 1999/93/EG van het Europees Parlement.

2. Op basis van het aanvullend onderzoek met de stakeholders bepalen of er behoefte is aan een onderzoek naar aanvullende standaarden voor het beschrijven van tijdstempelautoriteiten.
3. PKIoverheid wordt opgeroepen om over te gaan tot onderzoek naar mogelijkheden voor aanpassing van de middelen om tijdstempels te ondersteunen bij het gebruik van een PKI certificaat.

De opgeroepen partijen worden gevraagd om één jaar na opname van de standaarden over de voortgang op deze punten te rapporteren aan het Forum Standaardisatie.

Bijlage

- Expertadvies AdES Baseline Profiles v1.0.
https://www.forumstandaardisatie.nl/sites/default/files/FS/2016/1019/Expert_advies-AdES-Baseline-Profiles-v1-0.pdf
- Overzicht reacties consultatieronde v1.0:
<https://www.forumstandaardisatie.nl/sites/default/files/FS/2016/1019/Reacties-uit-openbare-consultatie-AdES-Baseline-Profiles.pdf>