Forum Standaardisatie

Wilhelmina van Pruisenweg 52
2595 AN Den Haag

Postbus 96810
2509 JE Den Haag

www.forumstandaardisatie.nl

notitie

Aan:	Forum Standaardisatie		
Van:	Bureau Forum Standaardisatie		
Datum:	22 september 2016	**Versie**	1.0
Betreft:	Overzicht reactie openbare consultatieronde AdES Baseline Profiles		
Bijlagen:	1. Reactie CIO Rijk 2. Reactie Kennisnet 3. Reactie Digikoppeling 4. Reactie Expertisecentrum Justid		

Datum
22 september 2016

1. Reactie CIO Rijk

Van: H. Wanders
Verzonden: vrijdag 9 september 2016 13:43
Aan: Forum standaardisatie
Onderwerp: Openbare consultatie Forum Standaardisatie

Bij ABP: belangrijk ervoor te zorgen dat Forum niet opnieuw misverstand creëert zoals bij DKIM.
Dus prima om standaard vast te stellen voor elektronische handtekeningen. Niet prima om te eisen dat alle documenten vanaf nu elektronisch getekend moeten worden.
Of ABP de goede standaard is kan ik niet beoordelen.

Groet,
Hans

2. Reactie Kennisnet

Datum
22 september 2016

Van: E. Lustenhouwer
Verzonden: maandag 12 september 2016 17:04
Aan: Forum standaardisatie
Onderwerp: Edustandaard

Beste Lancelot

Hartelijk dank voor de uitnodiging voor de openbare consultatie. De betreffende standaarden hebben geen (directe) impact op het onderwijs en de onderwijsstandaarden. Inhoudelijk hebben wij (Bureau Edustandaard) daarom nu niet iets toe te voegen.

Met vriendelijke groet,

Elise Lustenhouwer
Standaardisatie Expert

3. Reactie Digikoppeling

Datum
22 september 2016

Van: P.N. Hering
Verzonden: woensdag 14 september 2016 14:20
Aan: Forum standaardisatie
Onderwerp: AdES Baseline Profiles en overlap Digikoppeling

Beste Forum Standaardisatie,

Hierbij het resultaat van een kort onderzoek naar de overlap tussen Digikoppeling en de AdES standaarden.

Met vriendelijke groet,

Pieter Hering

Bijlage Digikoppeling

Datum
22 september 2016

Memo: Wat is de overlap tussen AdES en Digikoppeling

Datum: 13-09-2016 | Door: Martin van der Plas/Logius | Doelgroep: Expertgroep AdES standaard

Bron:
Op dit moment loopt de behandeling van plaatsing op de Pas-Toe-Leg-Uit lijst van de Advanced Electronic Signatures (AdES) Baseline Profiles. Deze standaarden zijn aangemeld door John Stienen van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.
De standaarden beschrijven het gebruik van profielen voor geavanceerde/gekwalificeerde elektronische handtekeningen op basis van de AdES standaarden.

Een van de geraadpleegde experts, de heer Gerald Groot Roessink, gaf aan dat er een mogelijke overlap bestaat met Digikoppeling.

Volgende week worden het expertadvies en het advies om de AdES Baseline Profiles op te nemen in de "Pas-toe-of-leg-uit Lijst" voorgelegd in een openbare consultatie.
Het voornemen is om de overlap met Digikoppeling op te nemen in het expertadvies.

Doel van dit memo:
Bepalen van de overlap tussen AdES en Digikoppeling

Aanpak:
Het expertadvies is gelezen en de overlap van AdES met Digikoppeling is intern bij Logius besproken.

Resultaat:
Beide standaarden beschrijven hoe Signing moet worden toegepast. Het verschil tussen Digikoppeling en de AdES standaarden zit met name in het organisatorische werkingsgebied:

- De Digikoppeling standaard is gericht op berichtuitwisseling tussen niet natuurlijke personen (Organisaties). Een envelop met handtekening ofwel een gesigned bericht zal dan ook altijd ondertekend zijn door een organisatie. Dit gebeurt met behulp van een PKIOverheid certificaat op een server die dit zonder menselijke interventie uitvoert. De Digikoppeling standaard heeft geen boodschap aan de boodschap. Indien signing wordt toegepast wordt ook de berichtpayload gesigned. De payload van een Digikoppeling bericht bestaat in principe echter altijd uit een xml container met optioneel bijlagen waarin alle bestandsformaten, dus bijvoorbeeld ook PNG of JPG, kunnen worden opgenomen.
- De AdES standaard is gericht op ondertekening van documenten door natuurlijke personen of niet natuurlijke personen (Mensen of Organisaties). Deze documenten bestaan altijd uit een XML, PDF, CMS of ZIP-bestand waaraan een handtekening is toegevoegd. De handtekening heeft niet alleen tot doel om het ontvangende systeem te laten weten wie de authentieke bron is van het document, ook de persoon die het document ontvangt kan de handtekening inzien en valideren. Verder kan de handtekening ook gebruikt worden als bestanden via andere media dan via de Digikoppeling standaard worden uitgewisseld. Denk hierbij aan een email, file shares, downloads of andere vormen van bestandsoverdracht.

Kortom Digikoppeling heeft een 'system to system' scope voor wat betreft signing, AdES heeft een 'person to person' scope en daarmee een breder werkingsgebied. Daarnaast functioneert de AdES standaard op het functionele berichtniveau en richt Digikoppeling zich op het transportniveau. Vergeleken met fysieke post komt AdES overeen met de handtekening op de brief en Digikoppeling komt overeen met aangetekende post (evt. met handtekening retour)

Het is in de praktijk aan te raden niet te veel standaarden te stapelen bij een oplossing. Wanneer AdES wordt toegepast en bestanden daarna met de Digikoppeling standaard worden uitgewisseld is het naar onze mening onverstandig om de berichten ook te signen indien hier niet een zwaarwegende reden voor is. De Digikoppeling standaard dwingt namelijk ook al TLS af dat naast versleuteling van de verbinding ook de partijen identificeert en authenticeert die data uitwisselen. Dat kunnen zelfs verschillende partijen zijn. Voor de onweerlegbaarheid is het cruciaal dat verschillende vormen en lagen van versleuteling, signing en identificatie elkaar niet tegenspreken of tegenwerken.

Conclusie:
De standaarden Digikoppeling en AdES hebben naar onze mening 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 hier nu 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.

Advies:
Omdat AdES nauw verwant is met standaarden als Digikoppeling, PKIOverheid en ook eHerkenning (SAML-tokens gebruiken soortgelijke technologie) is het aan te raden om op korte termijn in een best practice aan te geven wanneer je (een van) beide standaarden kan en moet toepassen. Op lange termijn raden we aan een visie op signing op te stellen en praktijkproeven te doen waarin de (in)compatibiliteit van de combinatie van oplossingen wordt geverifieerd in een werkend systeem.

4. Reactie Expertisecentrum Justid

Datum
22 september 2016

Van: A. Goedewaagen
Verzonden: donderdag 15 september 2016 11:50
Aan: Forum standaardisatie
Onderwerp: Openbare consultatie Ades Baseline Profiles

Geachte commissie,

Bijgaand onze opmerkingen over het advies over de Ades Baseline Profiles. Ons referentiekader is voornamelijk PDF zodat wij ons hier op heb toegelegd.
Zoals uit de opmerkingen blijkt zijn wij niet volledig ingewijd in dit domein. Wij zouden graag over meer achtergrondinformatie willen beschikken om een verantwoord advies te kunnen geven.
Wij wensen de commissie sterkte met de afwegingen.

Namens Expertisecentrum Justid

A. Goedewaagen
Adviseur digitale duurzaamheid

Bijlage Expertisecentrum Justid

Datum
22 september 2016

Het Expertisecentrum Justid heeft haar reacties verwerkt in de PDF versie van het Expertadvies AdES Baseline Profiles, versie 1.0. Om de omvang van dit document, het overzicht van de reacties op de openbare consultatie, te beperken zijn de reacties uit het Expertadvies gehaald en hieronder per pagina weergegeven.

Pagina 4 van Expertadvies AdES Baseline Profiles, versie 1.0

Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.

Dit geldt onverminderd de toepassing van de standaard op grond van andere verwijzingen dan die op basis van de pas-toe-of-leg-uit lijst, waaronder die op grond van wettelijke regelingen.

Wat wordt hiermee bedoeld?

gebruik van geavanceerde/gekwalificeerde elektronische handtekeningen.
De AdES Baseline Profiles zijn volwassen standaarden di[illegible] een langere tijd bestaan. De standaarden beschrijven het gebruik van standaardprofielen voor geavanceerde/gekwalificeerde el[illegible]

Graag meer juridische context voor het gebruik van een elektronische handtekening. Niet alleen burg wetboek maar ook eu regelgeving aanhalen

Pagina 5 van Expertadvies AdES Baseline Profiles, versie 1.0

Toegevoegde waarde
De expertgroep concludeert dat de toegevoegde waarde van de standaarden voldoende is.
De standaarden dragen bij aan efficientie, 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.
Er zijn geen beveiligings- en privacyrisico's geïdentificeerd aan het implementeren en gebruiken van de standaarden.

Is dit de zg lange termijn validatie (LTV)? Dat kan toch alleen als er in het bestand ruimte is gereserveerd voor herhaalde validatie? In dit advies moet mi duidelijk grenzen worden benoemd wat wel en niet kan

Pagina 12 van Expertadvies AdES Baseline Profiles, versie 1.0

Kan de standaard naast of in combinatie met reeds opgenomen standaarden worden toegepast (d.w.z. de standaard conflicteert niet met reeds opgenomen standaarden)?
Ja, er bestaat samenhang tussen de AdES Baseline Profiles en een aantal documentformaat-standaarden die reeds zijn opgenomen op de 'pas-toe-of-leg-uit' lijst: X.509, PDF 1.7, PDF/A-1/2, ODF 1.2. De standaarden zijn aanvullend op elkaar en conflicteren niet:

X.509	Systeem van certificaten met een beperkte levensduur en de wijze waarop de intrekking van deze certificaten geregeld wordt.
PDF 1.7	Bestandsformaat voor het weergeven van elektronische documenten.

Niet voor PDF/A-1.Heeft beperkingen tav timestamp LTV vindt plaats door revocationlist. (zeer groot)Dit moeten we niet willen.PADes is ontwikkeld voor 32000-1 resp PDF 1.7 en zijn evenknie PDF/A-2. LTV vindt plaats door het OCS protocol.

Pagina 14 van Expertadvies AdES Baseline Profiles, versie 1.0

De toepassing van een Europese standaard zorgt ervoor dat de handtekening ook op Europees niveau bijdraagt aan interoperabiliteit.

Pagina

Luratech

Hoe is het draagvlak buiten Europa?

Pagina 15 van Expertadvies AdES Baseline Profiles, versie 1.0

3.1.3.4 *Zijn de beveiligingsrisico's aan overheidsbrede adoptie van de standaard acceptabel?*
Ja, er zijn geen specifieke beveiligingsrisico's geïdentificeerd.

3.1.3.5 *Zijn de privacyrisico's aan overheidsbrede adoptie van de standaard acceptabel?*
Er zijn geen specifieke privacyrisico's geïdentificeerd. Het borgen van de bescherming van privacy is onderdeel van deze standaard.

3.1.4 *Conclusie criteria 'Toegevoegde waarde'*

De OCSP ondersteunt geen encryptie. Is het geen gevaar dat andere partijen deze informatie kunnen onderscheppen? de zg replay attack?

Pagina 20 van Expertadvies AdES Baseline Profiles, versie 1.0

aandacht vanwege technische kennis die mogelijk nodig is om de handtekeningen juist te valideren. Een situatie waarbij de burger zelf tekent met een geavanceerde/gekwalificeerde elektronische handtekening wordt niet verwacht op korte termijn.

Het is voor leveranciers mogelijk om ondersteuning te bieden voor het gebruik van de diensten die nodig zijn voor AdES Baseline Profiles

Burger moet wel kunnen valideren. Dit vereist een courante reader. Kan dat worden opgelegd ondanks dat ze gratis zijn?