



notitie

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:	FS 160608.3A		
Betreft:	Intake-advies voor Advanced Electronic Signature Baseline Profiles (AdES Baseline Profiles)		
Aan:	Stuurgroep open standaarden		
Van:	Bureau Forum Standaardisatie		
Datum:	24 mei 2016	Versie	1.0

Advies

Het Forum Standaardisatie wordt geadviseerd om de standaarden XAdES Baseline Profile, PAdES Baseline Profile, CAdES Baseline Profile en ASiC Baseline Profile in procedure te nemen. In procedure nemen van deze standaarden is van belang om validatie van geavanceerde elektronische handtekeningen te kunnen garanderen.

Over de standaarden

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 hoger niveau van betrouwbaarheid vereisen, kunnen geavanceerde elektronische handtekeningen of gekwalificeerde elektronische handtekeningen worden gebruikt.

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

Advies en aandachtspunten

Datum
24 mei 2016

De standaarden zijn ingediend door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties met steun van het Ministerie van Economische Zaken. Tijdens de intake is gebleken dat de standaarden voldoen aan de criteria voor inbehandelname als 'pas toe of leg uit'-standaarden en de kansrijkheid van de procedure wordt als voldoende geschat.

De AdES Baseline Profiles worden ondersteund door Ondernemersplein van EZ. De AdES-standaarden worden gebruikt door enkele overheidsorganisaties (zoals RDW, de Autoriteit Consument en Markt en SBR). Er is een duidelijke use case binnen de (semi)publieke sector. Ook is er sprake van een interoperabiliteitsprobleem tussen de ondertekenaar van geavanceerde elektronische handtekeningen en de ontvanger van de handtekening. In dit advies staat onder de toelichting meer informatie.

Aandachtspunten tijdens de procedure zijn:

- Inzicht geven in wat wel en niet wettelijk verplicht is van deze standaard;
- De vaststelling van het daadwerkelijke functioneel toepassingsgebied in relatie tot de bestaande (wettelijke) Europese verplichting vanuit o.a. de EiDAS-verordening;
- De mogelijke overlap met de xDTM-standaard;
- De impact van implementatie van de standaard en de daarbij te maken kosten.

De volgende organisaties worden betrokken/benaderd tijdens de procedure.

Doelgroep	Willers	Moeters
Vertegenwoordiging van (toekomstige) gebruikers	BZK, EZ (waaronder eHerkenning), RDW, Autoriteit Consument en Markt	Defensie, Financiën, IenM, OCW, SZW, VenJ (JustID), VWS, ICTU, VNG, KING, Belastingdienst, SSC-ICT, Logius (SBR), KvK, DUO. Privaat: Ontvanger digitale handtekeningen (CV Monitor)
Leveranciers (zowel kleinere als de grotere)	Adobe, Microsoft, DDS	Leveranciers handtekeningsoftware (waaronder KPN, D Soft)
Kennishebbers	ETSI (beheerder), W3C	xDTM Standard Association, adviescollege regeldruk Actal, ODF/PDF/XML/CMS experts, Europese ervaringsdeskundigen
Wetenschappers	Radboud Universiteit, Universiteit Leuven	

De lijst is opgesteld op basis van gegevens verstrekt door de indiener en experts uit het werkveld. De genodigdenlijst wordt afgestemd met Bureau Forum Standaardisatie voorafgaand aan het uitzenden van de uitnodiging.

Toelichting

Datum
24 mei 2016

1. Aanmelding, intakegesprek en toetsingsprocedure

Op vrijdag 22 april 2016 is door John Stienen, senior beleidsmedewerker bij Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, DG Overheidsorganisatie, directie Informatiesamenleving en Overheid, een viertal standaarden aangemeld: XAdES Baseline Profile, PAdES Baseline Profile, CAdES Baseline Profile en ASiC Baseline Profile (hierna tezamen 'AdES Baseline Profiles') voor de lijst met open standaarden. De aanmelder heeft als doel de standaard verplicht ('pas toe of leg uit') te stellen.

Op donderdag 12 mei 2016 heeft een intakegesprek plaatsgevonden met de aanmelder. In dit gesprek is de aanmelding besproken. Hierbij is gekeken of alle basisinformatie aanwezig is en of de standaard voldoet aan de criteria voor inbehandelname. Daarnaast is vooruitgeblikt op de procedure.

2. Korte beschrijving standaard

Waar gaan de AdES Baseline Profiles over?

Een elektronische handtekening wordt 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 hoger niveau van betrouwbaarheid vereisen, kunnen geavanceerde elektronische handtekeningen of gekwalificeerde elektronische handtekeningen worden gebruikt.

Een geavanceerde handtekening 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.

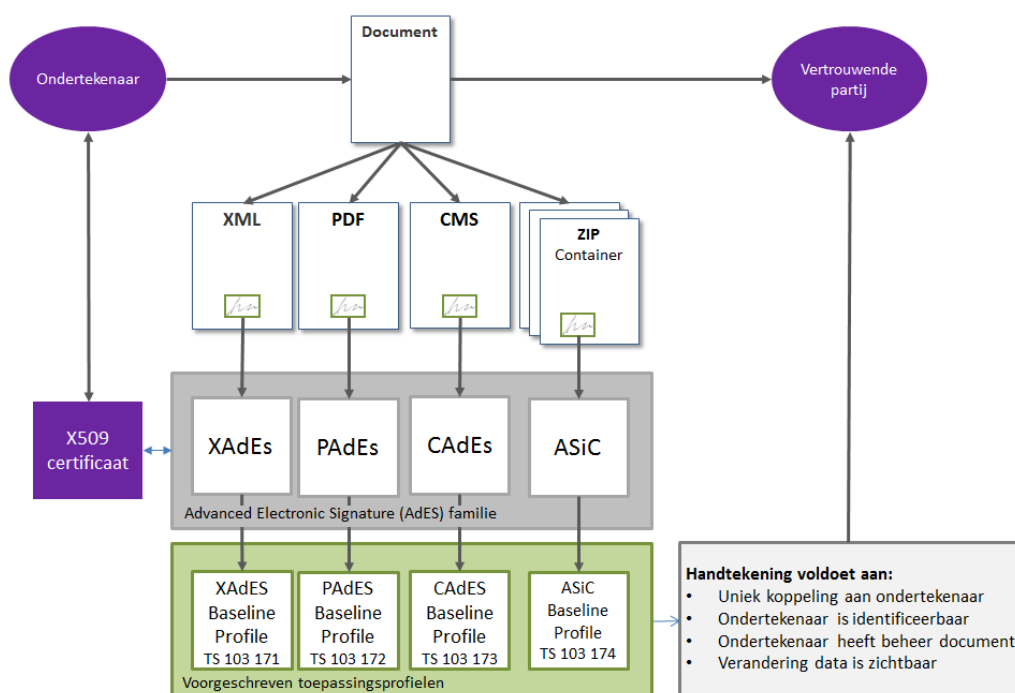
Een gekwalificeerde handtekening is een geavanceerde handtekening gegenereerd met behulp van een veilig middel zoals een smartcard of token.

De AdES-standaarden (Advanced Electronic Signature) zijn standaarden die het ondertekenen met geavanceerde elektronische handtekeningen beschrijven voor vier documenttypes: XML (XAdES), PDF (PAdES), CMS (CAdES) en ZIP (ASiC). Zie voor schematische weergave figuur 1.

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 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.

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 elektronische handtekening.

Door een AdES Baseline Profile te hanteren is het dus mogelijk om via een vastgesteld profiel een geavanceerde elektronische handtekening uit te wisselen, waarvan vooraf zeker is dat de ontvanger de handtekening kan lezen.



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

Welk probleem lost de standaard op?

In de huidige situatie is het verplicht om elektronische handtekeningen op basis van de AdES Baseline Profiles te accepteren als ontvanger bij Europese grensoverschrijdende uitwisselingen en in mindere mate bij uitwisselingen binnen Nederland.

Het is echter als ondertekenaar niet verplicht bij het ondertekenen met een geavanceerde elektronische handtekening gebruik te maken van een AdES Baseline Profile. Hierdoor kan het voorkomen dat een geavanceerde elektronische handtekening niet leesbaar blijkt voor de ontvanger. Dit kan gebeuren als de ondertekenaar gebruik maakt van een ander profiel dan het profiel wat de ontvanger accepteert.

Door vooraf vastgestelde AdES Baseline Profiles te hanteren is het voor een ondertekenaar duidelijk welk profiel er gebruikt moet worden voor ondertekening en is de handtekening altijd leesbaar voor de ontvanger.

Wie beheert de standaard?

De AdES-standaarden en AdES Baseline Profiles worden beheerd door het Europees Telecommunicatie en Standaardisatie Instituut (ETSI). ETSI is een formele Europese standaardisatieorganisatie.

Waarom is de standaard aangemeld voor pas toe of leg uit of aanbevolen?

Het beoogde doel van de aanmelding is het verplicht stellen van de AdES-Baseline Profiles. Door toepassing van de AdES Baseline Profiles is voor de ondertekenaar en ontvanger vooraf duidelijk aan welke minimale profieleisen een geavanceerde elektronische handtekening moet voldoen.

(zie ook: 8. Functionele use case)

3. Criteria voor inbehandelname

Om een standaard in behandeling te nemen moet de standaard vallen binnen de scope van de lijst. Hiervoor gelden drie criteria:

1. Is de standaard toepasbaar voor elektronische gegevensuitwisseling tussen (semi-)overheidsorganisaties en bedrijven, tussen (semi-)overheidsorganisaties en burgers of tussen (semi-)overheidsorganisaties onderling?

Ja, de AdES-standaarden zijn toepasbaar op elke elektronische gegevensuitwisseling van XML-, PDF-, CMS- of ZIP-bestanden die zijn ondertekend met een geavanceerde elektronische handtekening.

De standaard wordt ondersteund door diverse ontwikkelaars, waaronder een open source versie (http://ec.europa.eu/isa/actions/01-trusted-information-exchange/1-9action_en.htm) die in opdracht van de Europese Commissie wordt ontwikkeld. PAdES Baseline Profile wordt ondersteund door een groot aantal PDF readers. Het XAdES Baseline Profile wordt toegepast binnen tekstverwerkingspakketten zoals Microsoft Office en Open Office. De standaarden zijn direct op transparante wijze te gebruiken door de reguliere eindgebruiker doordat de AdES-standaarden in reguliere documentverwerkers reeds worden ondersteund.

2. Is het beoogde functioneel toepassingsgebied en het organisatorisch werkingsgebied van de standaard, voldoende breed om substantieel bij te dragen aan de interoperabiliteit van de (semi-)overheid?

Ja, de AdES Baseline Profiles zijn van toepassing op elk XML-, PDF-, CMS- en ZIP-bestand wat is ondertekend met een geavanceerde elektronische handtekening. Het beoogde organisatorisch werkingsgebied is alle (semi)overheidsorganisaties die in hun contact met elkaar, met burgers of met bedrijven gebruik maken van ondertekende documenten met geavanceerde elektronische handtekeningen.

In een aantal gevallen zijn er (semi)overheidsorganisaties waarvoor het gebruik van de AdES Baseline Profiles al wettelijk is verplicht voor de ondertekenaar en ontvanger. Voorbeelden hiervan zijn uitwisselingen in het kader van de aanbestedingsrichtlijnen en grensoverschrijdende uitwisselingen binnen de EU.

Datum
24 mei 2016

Het daadwerkelijke organisatorisch werkingsgebied moet nog worden vastgesteld door bestaande wetgeving en dwingende richtlijnen in kaart te brengen (zie onderstaande tabellen).

3. Is het zinvol de standaard op te nemen, gezien het feit dat deze niet al wettelijk verplicht is voor het beoogde functioneel toepassingsgebied en organisatorisch werkingsgebied?

Ja, de wettelijke verplichting tot gebruik van de AdES Baseline Profiles (XAdES, PAdES, CAdES en ASiC) beperkt zich tot verplichte acceptatie door de ontvanger (zie onderstaande tabellen). Er is, met uitzondering tot een aantal (semi-)overheidsorganisaties, geen wettelijke verplichting die bepaalt welk profiel wordt gebruikt bij het ondertekenen van documenten met geavanceerde elektronische handtekeningen.

Europese wet- en regelgeving

Naam	Heeft betrekking op	Gevolg
Besluit 2011/130/EU, <i>implementatie in Regeling elektronische handtekening bevoegde instanties</i>	Bevoegde autoriteiten (die documenten ondertekenen voor gebruik in andere lidstaten)	Erkenning van handtekeningen die voldoen aan PAdES-BES en PadES-EPES. Bij ondertekening met ander profiel moet de handtekening online, kosteloos, begrijpelijk te valideren zijn tenzij de informatie in de handtekening of documentdrager is opgenomen.
Uitvoeringsbesluit (EU) 2015/1506, <i>aangehaald in memorie van toelichting Telecommunicatiewet</i>	Openbare instantie die online dienst aanbiedt en een geavanceerde handtekening vereist	Lidstaten moet handtekeningen die voldoen aan AdES Baseline Profiles erkennen. Bij ondertekening met ander profiel moet de handtekening online, kosteloos, begrijpelijk te valideren zijn tenzij de informatie in de handtekening of documentdrager is opgenomen.
Verordening (EU) nr. 910/2014		Formulering van eisen aan geavanceerde elektronische handtekeningen bij transacties in de interne markt.
Richtlijn 2014/24/EU, Richtlijn 2014/25/EU	Aanbestedende diensten	Erkenning van geavanceerde elektronische handtekeningen zoals beschreven in Besluit 2011/130/EU.

Naam	Heeft betrekking op	Gevolg
Wetsvoorstel Algemene wet bestuursrecht 2:16	Bestuursorganen als vertrouwende partij	Elektronisch handtekeningen moeten voldoende betrouwbaar zijn. Verwijzing naar geavanceerde elektronische handtekeningen 910/2014.
Regeling vertrouwenslijst	Autoriteit Consument en Markt	Vertrouwenslijst moet worden ondertekend met XAdES/PADES-BES/PADES-EPES óf lijst moet worden verstrekt via website met TLS-verbinding

4. Draagt de standaard bij aan de oplossing van een bestaand, relevant (interoperabiliteits)probleem en het voorkomen van leveranciersafhankelijkheid?

Ja, in de AdES Baseline Profiles worden keuzes gemaakt uit de opties die de bovenliggende AdES-standaard biedt. Zo wordt het mogelijk om op basis van een bepaald profiel zekerheid te kunnen afgeven over de interoperabiliteit van de betreffende bovenliggende standaard in een bepaalde gebruikersgroep die allen hetzelfde profiel gebruiken.

De AdES Baseline Profiles zijn vrij beschikbaar en vrij toe te passen. De standaarden zijn derhalve niet gekoppeld aan een beperkt aantal leveranciers.

Conclusie

De standaard voldoet aan de criteria voor inbehandelname.

Het daadwerkelijke organisatorisch werkingsgebied moet nog worden vastgesteld tijdens het proces.

4. Toetsing kansrijkheid procedure

Het Forum Standaardisatie wil voorkomen dat er standaarden in procedure worden genomen, waarvan bij voorbaat al bekend is dat deze in de expertronde of consultatieronde zullen stranden op één van de inhoudelijke criteria. Daarom heeft de procedurebegeleider de beantwoording van de criteriavragen nagelopen, waar mogelijk zelf aangevuld en vervolgens besproken met de indiener.

1. Open standaardisatieproces

De ontwikkeling en het beheer van de standaard moeten op een open, onafhankelijke, toegankelijke, inzichtelijke, zorgvuldige en duurzame wijze zijn ingericht.

ETSI

Het ontwikkel- en beheerproces van de AdES-standaarden en AdES Baseline Profiles zijn ondergebracht bij ETSI. ETSI is officieel erkend door de Europese Unie als Europese standaardisatie organisatie (<http://www.etsi.org/about>). ETSI is een onafhankelijke not-for-profit-organisatie.

ETSI heeft meer dan 800 leden vanuit 66 landen, waaronder universiteiten, onderzoeksinstituten, publieke autoriteiten en industriële organisaties. Elke organisatie of bedrijf kan lid worden van ETSI (<http://www.etsi.org/membership>).

Het specificatiedocument en informatie over het ontwikkel- en beheerproces zijn drempelvrij beschikbaar via de website van ETSI (<https://www.etsi.org>).

Datum
24 mei 2016

Per AdES Baseline Profile is er een technische specificatie opgesteld:

- XAdES: http://www.etsi.org/deliver/etsi_ts/103100_103199/103171/02.01.01_60/ts_103171v020101p.pdf
- PAdES: http://www.etsi.org/deliver/etsi_ts/103100_103199/103172/02.01.01_60/ts_103172v020101p.pdf
- CAdES: http://www.etsi.org/deliver/etsi_ts/103100_103199/103173/02.02.01_60/ts_103173v020201p.pdf
- ASiC: http://www.etsi.org/deliver/etsi_ts/103100_103199/103174/02.01.01_60/ts_103174v020101p.pdf

ETSI geeft aan dat er geen intellectueel eigendomsclaims zijn op de AdES Baseline Profiles (<https://ipr.etsi.org/>).

De XAdES Baseline Profile, het profiel voor het ondertekenen van XML-bestanden, is ontwikkeld in samenwerking met de internationale standaardisatieorganisaties W3C. W3C is verantwoordelijk voor de ontwikkeling van de onderliggende standaard XML.

2. Toegevoegde waarde

De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de kosten, de risico's en nadelen. Voor elk van de te onderscheiden stakeholders (overheid, bedrijven en burgers) afzonderlijk zouden de baten voor de informatievoorziening en de bedrijfsvoering op moeten wegen tegen de kosten. Verder moeten de risico's aan overheidsbrede adoptie van de standaard (beveiliging, privacy) acceptabel zijn.

De AdES Baseline Profiles schrijven vooraf vastgestelde profielen voor. Hierdoor is het niet nodig om na implementatie van de AdES Baseline Profiles met de ontvangende partij af te stemmen over de specifieke invulling van de standaarden. De profielen zijn vrij te gebruiken en zijn opgenomen in de AdES Baseline Profiles.

De kosten voor de technische implementatie hangen af van de gebruikte software en onderliggende systemen. Voor PDF en XML zijn er meerdere softwarepakketten beschikbaar die de AdES Baseline Profiles ondersteunen. De kosten voor technische implementatie zijn derhalve niet hoger dan de implementatie van geavanceerde elektronische handtekeningen gebaseerd op een ander profiel

De organisatorische kosten zullen voornamelijk zijn gericht op de werkinstructies voor het ondertekenen en verifiëren van de handtekeningen. De AdES Baseline Profiles gaan uit van ondertekening op basis van het X.509-certificaat, een verplichte standaard die is opgenomen op de 'pas-toe-of-leg-uit' lijst. De kosten voor organisatorische implementatie zijn derhalve niet hoger dan de implementatie van geavanceerde elektronische handtekeningen gebaseerd op een ander profiel.

ETSI biedt de mogelijkheid om online gratis te controleren of de handtekening voldoet aan de eisen zoals gesteld in AdES Baseline Profiles. Dit controlemiddel is beschikbaar via <http://212.234.160.9/pub/index.shtml>.

3. Draagvlak

Aanbieders en gebruikers moeten voldoende ervaring hebben met de implementatie en het gebruik van de standaard.

Datum
24 mei 2016

De AdES Baseline Profiles worden op Europees niveau gebruikt voor grensoverschrijdende uitwisseling van geavanceerde elektronische handtekeningen bij (semi-)overheidsorganisaties.

De AdES standaarden worden gebruikt door enkele overheidsorganisaties (zoals RDW, de Autoriteit Consument en Markt en SBR) bij het ondertekenen met geavanceerde elektronische handtekeningen.

De Ades Baseline Profiles worden ondersteund in software zoals Word 2010, Open Office, Adobe Acrobat Reader en het Europese opensource pakket DDS.

Aandachtspunt is het bestaan van de standaard xDTM. De xDTM-standaard is in maart 2016 openbaar gemaakt door de xDTM Standard Association. De xDTM Standard Association is een not-for-profit organisatie gericht op online bedrijfsvoering.

De standaard omvat het digitale transactie management, waaronder elektronische handtekeningen. Onduidelijk is of de standaard, gelijk aan de XAdES Baseline Profielen, een technische implementatie van profielen voor geavanceerde elektronische handtekeningen behelst.

Het bestuur xDTM Standard Association bestaat uit organisaties die werkzaam zijn in de informatie technologie waaronder DocuSign, Microsoft, FedEx, Intel, Stanford, Visa en HP Enterprise. De xDTM Standard Association wordt uitgenodigd voor de expertbijeenkomst.

4. Opname bevordert adoptie

De opname op de lijst moet een geschikt middel zijn om de adoptie van de standaard te bevorderen.

Het verplichte karakter van de standaard zal leiden tot een bredere adaptatie van de AdES-standaarden. Als zowel bij het ondertekenen als bij het ontvangen van geavanceerde elektronische handtekeningen de AdES-standaarden verplicht zijn, is het eenvoudiger om geavanceerde elektronische handtekeningen te hanteren: het is vooraf duidelijk dat een ondertekend XML-, PDF-, CMS- of ZIP-bestand uitgewisseld kan worden tussen de ondertekende en de ontvangende partij.

De huidige beperking dat geavanceerde elektronische handtekeningen niet door de ontvanger gelezen kunnen worden vervalt bij het gebruik van de AdES Baseline Profiles.

Conclusie

De standaard voldoet aan de criteria voor inbehandelname.

Extra aandachtspunt tijdens de expertbijeenkomst is het bestaan van een mogelijke overlapping met de xDTM standaard.

5. Samenhang

Datum
24 mei 2016

Forum Standaardisatie wil weten of de aangemelde standaard samenhangt met standaarden die reeds op de lijst zijn opgenomen, of standaarden die voor toetsing in aanmerking komen. Uit de intake moet duidelijk worden of dit gevolgen heeft voor de toetsing en eventuele opname van de aangemelde standaard.

1. *Bestaat er samenhang tussen de aangemelde standaard en de verplichte ('pas-toe-of-leg-uit') standaarden die reeds op de lijst zijn opgenomen en wat betekent dit voor de toetsing en eventuele opname van de standaard?*

Er bestaat samenhang tussen de AdES Baseline Profiles en een aantal standaarden die reeds zijn opgenomen op de 'pas-toe-of-leg-uit' lijst:

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.
PDF/A-1/2	Bestandsformaat voor langdurige bescherming.
ODF 1.2	Uitwisseling van reviseerbare documenten.

De bestaande samenhang heeft geen gevolgen voor de toetsing en eventuele opname van de standaard.

2. *Bestaat er samenhang tussen de aangemelde standaard en de aanbevolen standaarden die reeds op de lijst zijn opgenomen en wat betekent dit voor de toetsing en eventuele opname van de standaard?*

Er bestaat samenhang tussen de XAdES Baseline Profile en een standaard die reeds op de lijst gangbare standaarden is opgenomen:

XML	Standaard voor de syntaxis van formele markuptalen. Hiermee kunnen gestructureerde gegevens worden gerepresenteerd in de vorm van tekst, die zowel door mensen als machines leesbaar is.
-----	--

De bestaande samenhang heeft geen gevolgen voor de toetsing en eventuele opname van de standaard.

3. *Bestaat er samenhang tussen de aangemelde standaard en standaarden die in aanmerking komen voor opname op de lijst en wat betekent dit voor de toetsing van de standaard(en)? (Denk bijvoorbeeld ook aan een gezamenlijke toetsing met (een deel van) deze aanvullende standaarden)*

De AdES Baseline Profiles kennen geen directe relatie met aanbevolen standaarden die in aanmerking komen voor opname op de lijst.

6. Sponsorschap

Datum
24 mei 2016

De aanmelding van standaarden voor de lijst van het Forum en het Nationaal Beraad dient ondersteund of gesponsord te worden door overheids- en/of (semi)publieke organisaties die de standaard reeds in gebruik hebben (of voornemens zijn dit te doen) en die de beoogde opname op de lijsten ondersteunen. Dit draagt bij aan het draagvlak voor de standaard, geeft zicht op de functionele use case voor de overheid en helpt bovendien om tijdens de toetsing de juiste experts te benaderen.

1. *Welke overheden en/of (semi) publieke organisaties ondersteunen de aanmelding van de standaard?*

De aanmelding van de AdES Baseline Profiles worden gesteund door John Stienen, namens het ministerie van Binnenlandse Zaken en Koninkrijksrelaties en Rob Brand, namens het ministerie van Economische Zaken.

2. *Hebben deze organisaties de standaard geïmplementeerd? (zie ook punt 8 voor een uitwerking)*

De AdES Baseline Profiles worden ondersteund door Ondernemersplein van EZ. De AdES standaarden worden gebruikt door enkele overheidsorganisaties (zoals RDW, de Autoriteit Consument en Markt en SBR) bij het ondertekenen met geavanceerde elektronische handtekeningen.

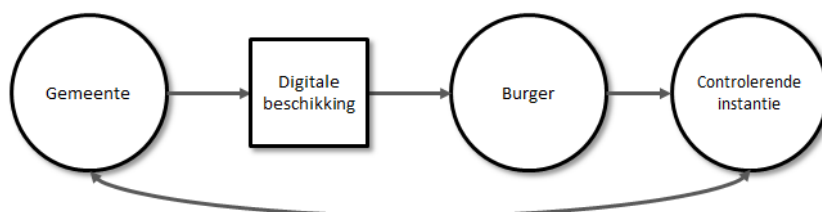
7. Functionele use case

Voor de standaard dient een duidelijke use case beschikbaar te zijn op basis waarvan overheden en/of instellingen uit de (semi) publieke sector kunnen bepalen of de aangemelde standaard voor hen relevant is en wie eventueel moet deelnemen aan de experttoetsing van de standaard.

Use case: Uitwisseling tussen gemeente en burger

Een gemeente verstrekt een beschikking van een omgevingsvergunning in PDF-formaat aan burgers. De vergunning wordt gewaarmerkt met een digitale handtekening. Deze handtekening geeft de garantie dat de handtekening is gezet door de gemeente en dat de informatie in het document door de gemeente is bevestigd.

Een derde partij, een controlerende instantie, heeft de taak om omgevingsvergunningen van burgers te controleren.



Controlerende instantie wilt weten of beschikking die burger heeft daadwerkelijk getekend is door gemeente.

Figuur 2: Use case Uitwisseling tussen gemeente en burger

Situatie zonder AdES Baseline Profiles

Elke gemeente kan 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 de digitale beschikking aan moeten tonen. Als de controlerende instantie alsnog de digitale beschikking wil controleren dan moet de software aangepast worden of moeten er afspraken worden gemaakt tussen de controlerende instantie en de gemeentes.

Datum
24 mei 2016

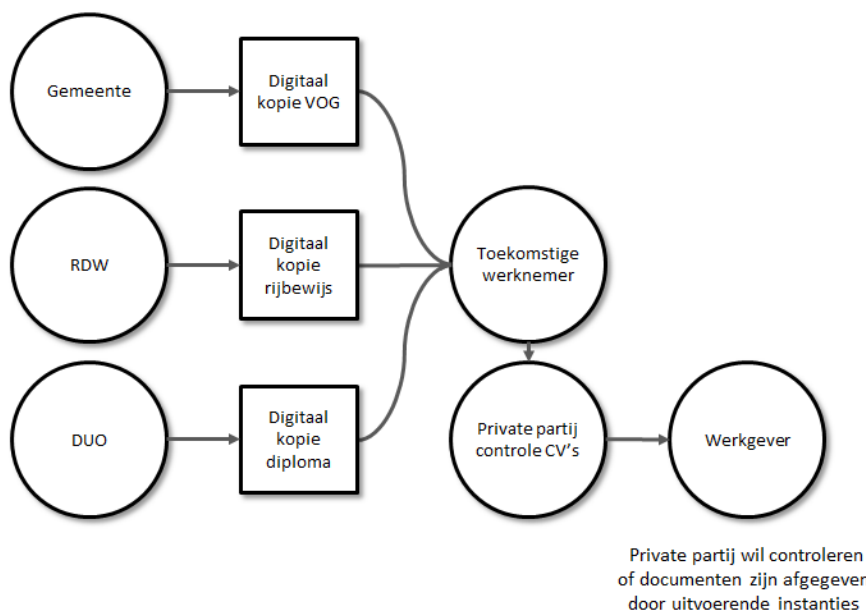
Situatie met gebruik van AdES Baseline Profiles

De AdES Baseline Profiles worden geaccepteerd 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 verifiëren.

Use case: Uitwisseling tussen overheidsinstanties, burger en private partij.

Een private organisatie biedt de mogelijkheid om namens werkgevers het CV van een toekomstige werknemer te controleren. Hiertoe controleert de private partij de digitale kopieën van diploma's, rijbewijs en Verklaring Omtrent Gedrag (VOG). De digitale kopieën zijn ondertekend met een geavanceerde elektronische handtekening om authenticiteit van de documenten te waarborgen.

De toekomstige medewerker deelt de digitale bewijzen via de website van de private organisatie. De private organisatie controleert de documentatie en handtekeningen op authenticiteit. Vervolgens meldt de organisatie naar de werkgever of de documenten van de toekomstige werknemer voldoen.



Figuur 3: Usecase 2 Uitwisseling tussen overheidsinstanties, burger en private partij.

Situatie zonder AdES Baseline Profiles

Bij gebruik van verschillende standaarden kan elke organisatie zelf beslissen met welk profiel van een geavanceerde elektronische handtekening de digitale kopie ondertekend kan worden. De private partij weet, zonder afstemming met de ondertekenaars, niet welke profielen hij kan verwachten.

Datum
24 mei 2016

Het is voor de private partij niet mogelijk om de handtekeningen te controleren als de ondertekenaar afwijkt van het profiel van de private partij. De private partij kan de handtekening niet lezen zonder het systeem aan te passen of af te wijken van het door hem gekozen profiel.

Situatie met gebruik van AdES Baseline Profiles

De toekomstige medewerker deelt de digitale bewijzen via de website van de private organisatie. Door gebruik van de AdES Baseline Profiles is voor de ondertekenaar duidelijk welk profiel hij moet gebruiken.

Doordat de ondertekenaar een AdES Baseline Profile gebruikt is het voor de private partij duidelijk welk profiel er gebruikt moet worden om de handtekening te verifiëren. Ook handtekeningen van eventuele nieuwe overheidsdiensten kunnen door de private partij direct beoordeeld worden zonder software aan te passen.