Forum Standaardisatie

Expertadvies AdES (Advanced Electronic Signatures) Baseline Profiles

Datum 5 augustus 2016

Colofon

Projectnaam	Expertadvies AdES Baseline Profiles
Versienummer	1.0
Locatie	Den Haag
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag forumstandaardisatie@logius.nl
Auteur	David van Es
Onafhankelijk voorzitter	Marcel van Kooten

Inhoud

Forumadvies & Managementsamenvatting

Advies aan het Forum
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 'pas toe of leg uit'-lijst.

Als functioneel toepassingsgebied wordt geadviseerd:

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

Als organisatorisch werkingsgebied wordt geadviseerd:

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.

Waarom is opname belangrijk?
Op dit moment zijn verschillende (semi)overheidsorganisaties en bedrijven zoekende naar een standaard die gebruikt kan worden voor het gebruik van geavanceerde/gekwalificeerde elektronische handtekeningen. 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 veel behoefte aan validatie van authenticiteit[2] van digitale documenten.

Waar gaat het inhoudelijk over?
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 er van onderschrijft. Voor het ondertekenen van documenten die een hoger niveau van betrouwbaarheid vereisen, kunnen geavanceerde elektronische handtekeningen of gekwalificeerde elektronische handtekeningen worden gebruikt.

1 Op grond van de gelijkschakeling 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.
2 Authenticiteit betreft de mate van betrouwbaarheid van de originaliteit en herkomst van een document, een bericht, een gegeven of ander object.

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

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 (een profiel) te selecteren. De AdES Baseline Profiles beschrijven dergelijke profielen.

Hoe is het proces verlopen?
Om tot dit advies te komen is op 30 juni 2016 een groep experts bijeengekomen om over het toepassings- en werkingsgebied van de AdES Baseline Profiles te discussiëren en om de standaarden te toetsten tegen de toetsingscriteria. Dit expertadvies vat de uitkomsten van de discussie en toetsing samen.
Tevens is als onderdeel van deze expert-toets de voorliggende conceptversie van het adviesrapport via schriftelijke en telefonische afstemming van input voorzien door drie experts die niet aanwezig waren bij de expertbijeenkomst.

Vervolg
Dit expertadvies zal ten behoeve van een publieke consultatie openbaar worden gemaakt door het Bureau Forum Standaardisatie. Eenieder kan gedurende de consultatieperiode op dit expertadvies zijn/haar reactie geven. Het Bureau Forum Standaardisatie legt vervolgens de reacties voor aan de voorzitter en indien nodig aan de expertgroep.

Het Forum Standaardisatie zal op basis van het expertadvies en relevante inzichten uit de openbare consultatie een advies aan het Nationaal Beraad opstellen. Het Nationaal Beraad bepaalt uiteindelijk op basis van het advies van het Forum of de de standaard op de 'pas toe of leg uit'-lijst komt.

Hoe scoort de standaard op de toetsingscriteria?

<u>Toegevoegde waarde</u>
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.

Open standaardisatieproces
De ontwikkeling van de AdES Baseline Profiles voldoet aan alle kenmerken van een open standaardisatieproces. De standaard wordt ontwikkelt door 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 drempeloos verkrijgbaar.

Draagvlak
De expertgroep concludeert dat het gebruik van de AdES Baseline Profiles voldoende draagvlaak heeft. Er zijn voldoende positieve signalen over het toekomstig gebruik van de standaard. De adoptie van de standaarden wordt door de experts ondersteund.

Opname bevordert adoptie
De expertgroep concludeert dat de 'pas toe of leg uit'-lijst het passende middel is om de adoptie van de standaard binnen de (semi)overheid te bevorderen. Op dit moment is de adoptie beperkt en zal een verplicht karakter van de standaard leiden tot een bredere adaptatie.

Welke additionele adviezen zijn er ten aanzien van de adoptie van de standaard?
De expertgroep doet het Nationaal Beraad de aanbeveling om bij de opname op de lijst voor 'pas toe of leg uit' de volgende oproepen ten aanzien van de adoptie van AdES Baseline Profiles te doen:

- 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.
- Het Forum Standaardisatie wordt opgeroepen om te onderzoeken of er aanvullende standaard nodig is die de eisen omtrent tijdstempelautoriteiten beschrijft.
- De oproep aan PKI Overheid om over te gaan op onderzoek naar mogelijkheden voor aanpassing van de middelen om tijdstempels te ondersteunen bij het gebruik van een PKI certificaat.

1 Doelstelling expertadvies

1.1 Achtergrond

Het gebruik van open standaarden en het voorkomen van vendor lock-in is een van de doelstellingen van de Nederlandse overheid. Dit beleid wordt herbevestigd in actieplan "Open overheid", de digitale agenda 2011-2015, de digitale agenda 2017 en de kabinetsreactie op het rapport Elias. Deze plannen onderstrepen de noodzaak van het zoveel mogelijk meenemen van open standaarden bij het ontwerpen van informatiesystemen.

Een van de maatregelen om de adoptie van standaarden te bevorderen is het beheren van een lijst met open standaarden, die vallen onder het principe 'pas toe of leg uit' of 'aanbevolen'. Het Nationaal Beraad Digitale Overheid spreekt zich uit over de standaarden die op de lijst zullen worden opgenomen, onder andere op basis van een expertbeoordeling van de standaard. Het Nationaal Beraad wordt geadviseerd door het Forum Standaardisatie. Het Bureau Forum Standaardisatie ondersteunt beide instellingen.

1.2 Doelstelling expertadvies

Onderwerp van dit expertadvies zijn de AdES Baseline Profiles. De AdES Baseline Profiles zijn aangemeld voor opname op de lijst met open standaarden door John Stienen, senior beleidsmedewerker bij Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, DG Overheidsorganisatie, directie Informatiesamenleving en Overheid.

Doel van dit advies is om, aan de hand van de criteria, vast te stellen of de AdES Baseline Profiles moeten worden opgenomen op de lijst met open standaarden als 'pas toe of leg uit'-standaard, al dan niet onder bepaalde voorwaarden.

1.3 Doorlopen proces

Voor het opstellen van dit proces is de volgende procedure doorlopen:

- Door de procesbegeleider is een intakegesprek gevoerd met de indiener op 22 april 2016. Tijdens de intake is de standaard getoetst op uitsluitingscriteria ('criteria voor inbehandelname') en is een eerste inschatting gemaakt van de kansrijkheid van de procedure.
- 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 basis van de aanmelding en de intake is een voorbereidingsdossier opgesteld voor de leden van de expertgroep.
- De expertgroep heeft voorafgaand aan de expertbijeenkomst dit voorbereidingsdossier doorgenomen en aandachtspunten geïdentificeerd.
- Tot slot is de expertgroep op 30 juni 2016 bijeengekomen om de bevindingen in het algemeen en de geïdentificeerde aandachtspunten in het bijzonder 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 input kunnen geven op het hier voorliggende 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.

1.4 Vervolg

Dit expertadvies zal ten behoeve van een publieke consultatie openbaar worden gemaakt door het Bureau Forum Standaardisatie. De openbare consultatie vindt plaats van 1 augustus 2016 tot 15 september 2016. Eenieder kan gedurende de consultatieperiode op dit expertadvies een reactie geven. Het Bureau Forum Standaardisatie legt vervolgens de reacties voor aan de voorzitter en indien nodig aan de expertgroep.

Het Forum Standaardisatie zal op basis van het expertadvies en de relevante inzichten uit de openbare consultatie een advies aan het Nationaal Beraad opstellen. Het Nationaal Beraad bepaalt uiteindelijk op basis van het advies van het Forum of de de standaard op de 'pas toe of leg uit'-lijst komt.

1.5 Samenstelling expertgroep

Het Forum streeft naar een zo representatief mogelijke expertgroep, met een evenwichtige vertegenwoordiging van (toekomstige) gebruikers (zowel publiek als privaat), leveranciers, wetenschappers en andere kennishebbers. Daarnaast wordt een onafhankelijke voorzitter aangesteld om de expertgroep te leiden en als verantwoordelijke op te treden voor het uiteindelijke expertadvies.

Als voorzitter is opgetreden Marcel van Kooten, management consultant bij Verdonck, Klooster & Associates. David van Es, consultant bij Verdonck, Klooster & Associates, heeft de expertgroep in opdracht van het Bureau Forum Standaardisatie begeleid.

Aan de expertbijeenkomst hebben deelgenomen:
- Harm Voogt, Validata Group
- Douglas Skirving, PKI Overheid
- Patrick Beckman Lapré, QuoVadis
- Xander van der Linde, ICTU
- Kick Willemse, Evidos
- Arjen Haasnoot (namens indiener), Ministerie van Economische Zaken

Tevens zijn geraadpleegd als experts:
- Dominique Hermans, DO Consultancy
- Gerald Groot Roessink, DUO
- Geert Eenink, SURFmarket
- Rob Brand, DICTU

Lancelot Schellevis en Han Zuidweg van het Bureau Forum Standaardisatie was als toehoorder bij de expertbijeenkomst aanwezig.

1.6 Toelichting AdES Baseline Profiles

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.

Een geavanceerde handtekening voldoet aan vier eisen:

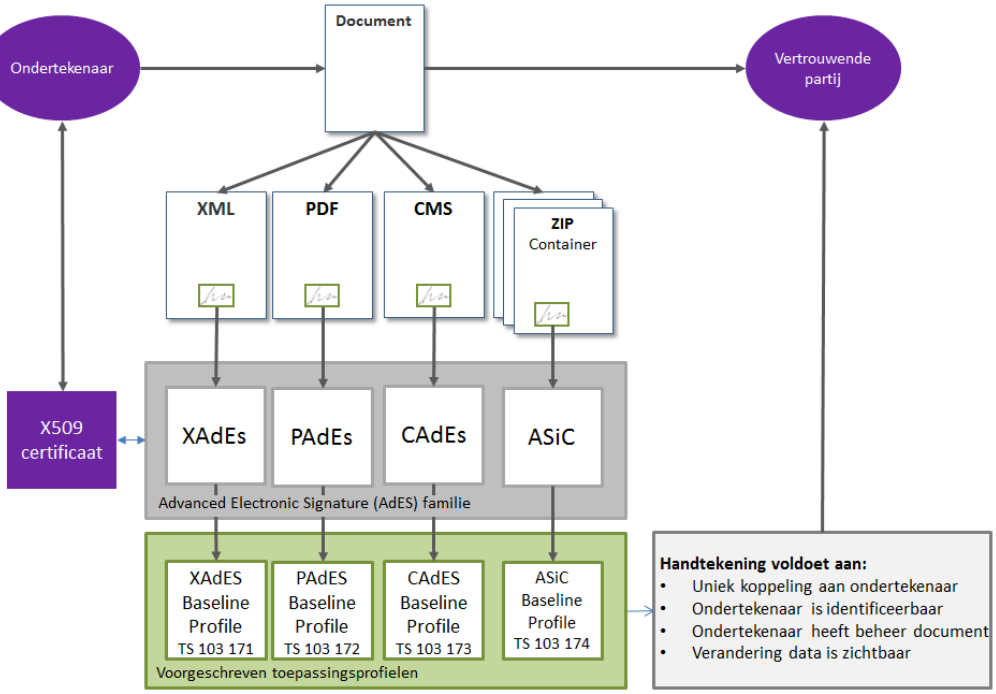
1. De handtekening is op unieke wijze aan de ondertekenaar verbonden;
2. De handtekening maakt het mogelijk de ondertekenaar te identificeren;
3. De handtekening komt tot stand met middelen die de ondertekenaar onder zijn uitsluitende controle kan houden;
4. De handtekening is op zodanige wijze aan het 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. Het certificaat moet door een erkende certificatiedienstverlener zijn uitgegeven. Deze certificatiedienstverlener moet door de toezichthouder (op dit moment Autoriteit Consument & Markt[3]) 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).

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 (figuur 1).

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



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.

Door het toevoegen van een tijdstempel kan de authenticiteit en het bestaan van een document op een bepaald moment worden bevestigd. Voor het creeren van de tijdstempel kan gebruikt gemaakt worden van een onafhankelijke tijdstempelautoriteit.

Relatie met andere standaarden
Er bestaat een nauwe samenhang met het gebruik van het X.509-certificaat. De X.509 standaard beschrijft een systeem van certificaten (op basis van gebruik van private en publieke sleutels) met een beperkte levensduur en de wijze waarop de intrekking van deze certificaten geregeld wordt.

1.7 Leeswijzer

In hoofdstuk 2 wordt beschreven in welke gevallen de standaard functioneel gezien gebruikt zou moet worden (functioneel toepassingsgebied) en door welke organisaties deze gebruikt zou moeten worden (organisatorisch werkingsgebied).

Om te bepalen of de standaard opgenomen moet worden op de lijst met standaarden voor ‘pas toe of leg uit’, is deze getoetst aan een viertal vastgestelde criteria. In hoofdstuk 3 staat het resultaat van deze toetsing.

2 Toepassings– en werkingsgebied

Van overheidsorganisaties wordt verwacht dat zij de lijst met open standaarden hanteren bij aanbestedingstrajecten volgens het 'pas toe of leg uit'-regime. Afhankelijk van de aan te schaffen functionaliteit zal bepaald moeten worden welke koppelvlakken geïmplementeerd moeten worden, en welke standaarden uit de lijst hiervoor ingezet dienen te worden. Om dit te kunnen doen heeft de expertgroep gekeken in welke gevallen de standaard functioneel gezien gebruikt zou moeten worden (functioneel toepassingsgebied), en door welke organisaties deze gebruikt zou moeten worden (organisatorisch werkingsgebied).

2.1 Functioneel toepassingsgebied

Als functioneel toepassingsgebied wordt voorgesteld:

De AdES Baseline Profiles zijn van toepassing op elk document in de vorm van een XML-, PDF-, CMS-, en ZIP-bestand dat is voorzien van een geavanceerde en/of gekwalificeerde elektronische handtekening (inclusief zegels/tijdstempels).

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

2.2 Organisatorisch werkingsgebied

De expertgroep adviseert om het organisatorisch werkingsgebied van de standaard overeen te laten komen met het werkingsgebied waarop het 'pas toe of leg uit' principe van toepassing is, te weten:

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 .

3 Toetsing van standaard aan criteria

Om te bepalen of de standaard opgenomen moet worden op de lijst met open standaarden is deze getoetst aan een aantal criteria. Er zijn vier hoofdcriteria:

1. Toegevoegde waarde
2. Open standaardisatieproces
3. Draagvlak
4. Opname bevordert adoptie

Deze criteria staan beschreven in het rapport, *"Toetsingprocedure en criteria voor indieners en experts"* en staan op de website www.forumstandaardisatie.nl/open-standaarden. Het resultaat van de toetsing zal in dit hoofdstuk per criterium beschreven worden. Voor de volledigheid is tevens de definitie van elk criterium opgenomen.

3.1 Toegevoegde waarde

De interoperabiliteitswinst en andere voordelen van adoptie van de standaard wegen overheidsbreed en maatschappelijk op tegen de risico's en nadelen.

3.1.1 Is het toepassings- en werkingsgebied van de aanmelding goed gedefinieerd?

3.1.1.1 Is het functioneel toepassingsgebied goed gedefinieerd?
Ja, zie paragraaf 2.1.

3.1.1.2 Is het organisatorisch werkingsgebied goed gedefinieerd?
Ja, zie paragraaf 2.2.

3.1.1.3 Is de standaard generiek toepasbaar (en niet alleen bedoeld voor gegevensuitwisseling met één of een beperkt aantal specifieke organisaties)? (toelichtende vraag)
Ja, de standaarden zijn generiek toepasbaar door alle partijen binnen het beschreven organisatorisch werkingsgebied.

3.1.2 Verhoudt de standaard zich goed tot andere standaarden?

3.1.2.1 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.

PDF/A-1/2[4]	Bestandsformaat voor langdurige opslag van van elektronische documenten.
ODF 1.2	Uitwisseling van reviseerbare documenten.
XML	Standaard voor de syntaxis van formele markuptalen.
ebMS	Standaard voor elektronisch berichtenverkeer (*meldingen tussen informatiesystemen*) tussen overheidsorganisaties.
WUS	Standaard voor elektronisch berichtenverkeer (*bevraging van informatiesystemen*) tussen overheidsorganisaties.
GB	Standaard voor elektronisch berichtenverkeer (*uitwisseling van grote berichten*) tussen overheidsorganisaties.

3.1.2.2 Biedt de aangemelde standaard meerwaarde boven reeds opgenomen standaarden met een overlappend functioneel toepassings- en organisatorisch werkingsgebied? (Dit kan ook om een nieuwe versie van dezelfde standaard gaan.)
Ja, er zijn geen standaarden met een overlappend functioneel toepassingsgebied gevonden die reeds zijn opgenomen.

Open standaarden voor berichtenverkeer, zoals XBRL en SOAP, richten zich op (de controle van) de authenticiteit van berichten. De standaarden beschrijven de elektronische uitwisselingen van berichten (respectievelijk financiële informatie en XML berichten). De AdES Baseline Profiles richten zich niet op het berichtenverkeer, maar op de ondertekening van documenten. Het functioneel toepassingsgebied van de AdES Baseline Profiles overlapt derhalve niet met dergelijke standaarden.

3.1.2.3 Biedt de aangemelde standaard meerwaarde boven bestaande concurrerende standaarden die in aanmerking zouden kunnen komen voor opname? (toelichtende vraag)
Ja, er zijn geen concurrerende standaarden die de leemte aan de kant van de ondertekenaar vult op het gebied van geavanceerde/gekwalificeerde elektronische handtekeningen.
De volwassenheid van de standaard blijkt uit de verankering binnen eIDAS. Ook in de OASIS DSS(core) standaard zijn de XAdES en XAdES standaarden geincorporeerd.

3.1.2.4 Is de standaard een internationale standaard of sluit de standaard aan bij relevante internationale standaarden? (toelichtende vraag)
Ja, de AdES Baseline Profiles zijn een internationale standaard, ontwikkeld door Europese standaardisatieorganisatie ETSI.

3.1.3 Wegen de kwantitatieve en kwalitatieve voordelen van adoptie van de standaard, voor de (semi-)overheid als geheel en voor de maatschappij, op tegen de nadelen?

3.1.3.1 Zijn de kosten van implementatie acceptabel en zijn deze kosten bekend en inzichtelijk?
Ja, voor de implementatie van een geavanceerde/gekwalificeerde elektronische handtekening wordt verwacht dat er geen extra kosten te verwachten zijn ten opzichte van de implementatie op basis van een ander profiel.
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.

4 Er bestaat een PDF A/3-standaard. De standaard beschrijft het inbedden van bestanden in een PDF-bestand. Deze standaard is niet opgenomen op de lijst open standaarden.

Er zijn geen kengetallen beschikbaar.

3.1.3.2 Is er een (kwalitatieve) businesscase van de standaard aanwezig?
Ja, het gebruik van de standaarden is voornamelijk van toegevoegde waarde voor de ontvangende kant: als het gebruikte software pakket aansluit op de standaard die gebruikt is voor het ondertekenen dan hoeven er geen aanpassingen te worden gemaakt aan het softwarepakket.

Een voorbeeld: als er door een accountant een uitreksel gevalideerd moet worden dan moet de accountant weten op welke standaard hij zijn validatie moet baseren. Datzelfde geldt voor een burger die datzelfde uitreksel wil controleren op authenticiteit. Als het software pakket wat de ontvanger gebruikt een andere standaard hanteert, dan moet er of een ander softwarepakket worden aangeschaft of een ander validatiemiddel worden gebruikt. Door een standaard te hanteren wordt het voor zowel overheden, bedrijven als burgers eenvoudiger om een keuze te maken voor een softwarepakket dat de handtekening met zekerheid kan valideren. Uit dit voorbeeld blijkt dat de voorliggende standaard ziet op de content van handtekeing en document, en niet op het transport van het bericht zoals bijvoorbeeld de SAML standaard.

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/gekwalificeerde elektronische handtekeningen gebaseerd op een ander profiel dat voldoet aan de eisen voor een geavanceerde/gekwalificeerde elektronische handtekening.

3.1.3.3 Is de meerwaarde van de standaard goed inzichtelijk te maken? Wat betekent de standaard voor de (bedrijfs)processen van een organisatie of keten en wat los je met de standaard op?
Ja, het verplichte karakter van de standaard zal leiden tot een bredere adoptie van de AdES-standaarden. Het juridisch kader (Uitvoeringsbesluit 2015/1506 van de Europese Commissie) verplicht op dit moment de ontvanger om een geavanceerde/gekwalificeerde elektronische handtekening op basis van standaarden te accepteren. Voor het zetten van een geavanceerde/gekwalificeerde elektronische handtekening op basis van een standaard is geen verplichting. Als zowel bij het ondertekenen als bij het ontvangen van geavanceerde/gekwalificeerde elektronische handtekeningen de AdES-standaarden verplicht zijn, dragen de standaarden bij aan legitimiteit. Positieve terugkoppeling van opname zal leiden tot verdere proliferatie.

De standaarden dragen bij aan efficientie, vereenvoudiging en verlaging van de gehele productiekosten voor leveranciers en daarmee afname van de kosten voor afnemers. Tevens zorgt het gebruik van de standaarden voor een borging van duurzame opslag van document. De authenticiteit wordt gewaarborgd bij langdurige archiefopslag.

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

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 expertgroep concludeert dat de toegevoegde waarde van de standaarden voldoende is.
De standaarden dragen bij aan efficientie, vereenvoudiging en 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[5].
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.

3.2 Open standaardisatieproces

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

3.2.1 Is de documentatie voor een ieder drempelvrij beschikbaar?

3.2.1.1 *Is het specificatiedocument beschikbaar zonder dat er sprake is van onacceptabele belemmeringen (zoals te hoge kosten en te hoge lidmaatschapseisen)?*
Ja, het specificatiedocument en informatie over het ontwikkel- en beheerproces zijn drempelvrij beschikbaar via de website van ETSI (https://www.etsi.org).

3.2.1.2 *Is de documentatie over het ontwikkel- en beheerproces (bijv. het voorlopige specificatiedocument, notulen en beschrijving van de besluitvormingsprocedure) beschikbaar zonder dat er sprake is van onacceptabele belemmeringen (zoals te hoge kosten en te hoge lidmaatschapseisen)?*
Ja, per AdES Baseline Profile is er een technische specificatie opgesteld welke gratis gedownload kunnen worden op de website van ETSI:
- 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

*5 Clausule 9 (='*Requirements for LTA-Level Conformance*') van de profielen is niet van toepassing op eIDAS (zie: http://eur-lex.europa.eu/legal-content/NL/TXT/HTML/?uri=CELEX:32015D1506&from=EN)*

- 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_103199/103174/02.02.01_60/ts_103174v020201p.pdf

3.2.2 Is het intellectuele eigendomsrecht voor eenieder beschikbaar, zodat de standaard vrij implementeerbaar en te gebruiken is?

3.2.2.1 Stelt de standaardisatieorganisatie het intellectueel eigendomsrecht op de standaard m.b.t. bijvoorbeeld eventuele patenten- onherroepelijk royalty-free voor eenieder beschikbaar?
Ja, het specificatiedocument en informatie over het ontwikkel- en beheerproces zijn drempelvrij beschikbaar via de website van ETSI (https://www.etsi.org). ETSI geeft aan dat er geen intellectueel eigendomsclaims zijn op de AdES Baseline Profiles (https://ipr.etsi.org/).

3.2.2.2 Garandeert de standaardisatieorganisatie dat partijen die bijdragen aan de ontwikkeling van de standaard hun intellectueel eigendomsrecht onherroepelijk royalty-free voor eenieder beschikbaar stellen?
Ja, de standaarden worden ontwikkeld door partijen die hun intellectueel eigendomsrecht onherroepelijk royalty-free voor eenieder beschikbaar stellen. Indien blijkt dat een standaard niet uitvoerbaar is zonder inbreuk te maken op een IPR dan heeft de ETSI IPR Policy tot doel om de rechten en belangen van rechthebbenden en de behoefte van de gebruikersvast te leggen onder FRAND voorwaarden.

3.2.3 Is de inspraak van eenieder in voldoende mate geborgd?

3.2.3.1 Is het besluitvormingsproces toegankelijk voor alle belanghebbenden (bijv. gebruikers, leveranciers, adviseurs, wetenschappers)?
Ja, ETSI heeft meer dan 800 leden vanuit 66 landen, waaronder universiteiten, onderzoeksinstellingen, publieke autoriteiten en industriële organisaties. Elke organisatie kan lid worden van ETSI (http://www.etsi.org/membership).

3.2.3.2 Vindt besluitvorming plaats op een wijze die zoveel mogelijk recht doet aan de verschillende belangen?
Ja, het ontwikkel- en beheerproces van de AdES-standaarden en AdES Baseline Profiles is officieel erkend door de Europese Unie (http://www.etsi.org/about). De werkwijze staat beschreven op http://www.etsi.org/standards/how-does-etsi-make-standards.

3.2.3.3 Kan een belanghebbende formeel bezwaar aantekenen tegen de gevolgde procedure?
Ja, dit is onderdeel van het beheer. Een lid heeft de mogelijkheid om formeel bezwaar aan te tekenen bij de General Assemby, de hoogste autoriteit voor besluitvorming binnen ETSI.

3.2.3.4 Organiseert de standaardisatieorganisatie regelmatig overleggen met belanghebbenden over doorontwikkeling en beheer van de standaard?
Ja, zowel overheid als bedrijfsleven en andere belanghebbenden kunnen kennisnemen van en interacteren in de doorontwikkeling en het beheer van de standaard door deel te nemen aan de werkgroep van ETSI.

3.2.3.5 *Organiseert de standaardisatieorganisatie een publieke consultatie voordat (een nieuwe versie van) de standaard wordt vastgesteld?*
Ja, de vorm van consultatie verschilt per type document. Alle standaarden worden ontwikkeld op basis van consensus (http://www.etsi.org/standards/how-does-etsi-make-standards/approval-processes).

3.2.4 Is de standaardisatieorganisatie onafhankelijk en duurzaam?

3.2.4.1 *Is de ontwikkeling en het beheer van de standaard belegd bij een onafhankelijke non-profit standaardisatieorganisatie?*
Ja, ETSI is een onafhankelijke not-for-profit-organisatie.

3.2.4.2 *Is de financiering van de ontwikkeling en het onderhoud van de standaard voor tenminste drie jaar gegarandeerd?*
Ja, ETSI is officieel erkend door de Europese Unie als Europese standaardisatie organisatie (http://www.etsi.org/about). De financiering van ETSI bestaat uit jaarlijkse lidgelden, financiering door de Europese Unie, inkomsten uit diensten aan externe organisaties en bijdragen van partnerorganisaties.

3.2.5 Is het (versie) beheer van de standaard goed geregeld?

3.2.5.1 *Heeft de standaardisatieorganisatie gepubliceerd beleid met betrekking tot (versie)beheer van de standaard? Bij voorkeur is dit beleid ook beschreven in een beheerplan (met o.a. aandacht voor migratie van gebruikers)*
Ja, het versiebeheer van de standaard vormt onderdeel van het beheermodel AdES Baseline Profiles.

3.2.5.2 *Is de beheerdocumentatie goed vindbaar en verkrijgbaar?*
Ja, per AdES Baseline Profile is er een technische specificatie opgesteld welke gratis gedownload kunnen worden op de website van ETSI.

3.2.5.3 *Is het belang van de Nederlandse overheid voldoende geborgd bij de ontwikkeling en het beheer van de standaard?*
Ja, de Nederlandse overheid is lid van de standaardisatieorganisatie ETSI.

3.2.5.4 *Is de vertegenwoordiging van belanghebbenden bij het beheer van de standaard een goede representatie van het werkingsgebied en functioneel toepassingsgebied van de standaard?*
Ja, de standaard wordt ontwikkeld door overheidsinstanties, fabrikanten, gebruikers, onderzoeksinstellingen en kennisinstituten.

3.2.5.5 *Is het standaardisatieproces van de standaardisatieorganisatie zodanig goed geregeld dat het Forum zich kan onthouden van aanvullende toetsing bij de aanmelding van een nieuwe versie van de standaard?*
Ja, het beheer van de standaard is zowel open met inbreng van alle belanghebbenden als bestuurlijk goed verankerd.

3.2.6 *Is er adoptieondersteuning voor de standaard?*
Ja, ETSI organiseert regelmatig Plugtest evenementen waarbij de adoptie en implementatie van de ETSI-standaarden rondom elektronische handtekeningen centraal staan.

3.2.6.1 *Is er een toegankelijk aanspreekpunt of organisatie waar meer informatie over de standaard is te vinden en op te vragen is?*
Ja, Sonia Compans is het aanspreekpunt als technical officer voor ETSI (https://portal.etsi.org/People/CommiteeSupportStaff.aspx/).

3.2.6.2 *Wordt er ondersteuning gegeven in de adoptie en de implementatie van de standaard?*
Ja, ETSI biedt op haar website een plug in test in de vorm van de ETSI Signature Conformance Checker (http://signatures-conformance-checker.etsi.org).

3.2.7 *Conclusie criteria 'Open standaardisatieproces'*
De ontwikkeling van de AdES Baseline Profiles voldoet aan alle kenmerken van een open standaardisatieproces. De standaard wordt ontwikkeld door 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 drempelvrij verkrijgbaar.

3.3 Draagvlak

Aanbieders en gebruikers moeten voldoende positieve ervaring met de standaard.

3.3.1 Bestaat er voldoende marktondersteuning voor de standaard?

3.3.1.1 *Bieden meerdere leveranciers ondersteuning voor de standaard?*
Ja, voor PDF en XML zijn er meerdere softwarepakketten bekend die de AdES Baseline Profiles ondersteunen.
De scope van de AdES Baseline Profiles betreft de toepassing van profielen en niet de keuze voor ondersteunende software.
De AdES Baseline Profiles zijn vrij beschikbaar en vrij toe te passen. De standaarden zijn derhalve niet gekoppeld aan een beperkt aantal leveranciers.

3.3.1.2 *Kan een gebruiker de conformiteit van de implementatie van de standaard (laten) toetsen?*
Ja, 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.

3.3.1.3 *Draagt de standaard voldoende bij aan interoperabiliteit zonder dat aanvullende standaardisatieafspraken (zoals lokale profielen) noodzakelijk zijn om de standaard te implementeren of te gebruiken?*
Ja. De standaard wordt in de praktijk toegepast in een keten van functionaliteit waar verdere standaardisatie van functionele componenten wenselijk zou zijn. Als voorbeelden worden genoemd: berichtuitwisseling, identificerende kenmerken, verificatie, betrouwbaarheid van processen, en opslag van "key materials". Dat laat onverlet dat de standaard op zichzelf staand kan worden toegeapst en in een dringende behoefte voorziet. De AdES Baseline Profiles bevatten de eisen aan de minimale vereiste profielen. Hierdoor is het niet noodzakelijk om aanvullende standaardisatieafspraken te maken omtrent de selectie van de specifieke profieleisen.

De standaard is een deel van een groter geheel van ketenafspraken. De standaard lost niet alle ketenvraagstukken op. Zo heeft de standaard geen betrekking op de betrouwbaarheid van het proces, de opslag van sleutels (keys) en de kwaliteit van een tijdstempel autoriteit.

3.3.1.4 Zijn er profielen of voorbeeldimplementaties van de standaard aanwezig en zijn deze vrij te gebruiken?
Ja, de profielen of voorbeeldimplementaties (in de vorm van voorbeelden van ondertekende documenten) zijn standaard aanwezig en vrijelijk te gebruiken.

3.3.2 Kan de standaard rekenen op voldoende draagvlak?

3.3.2.1 Staan de belangrijkste stakeholders vanuit de overheid voor deze standaard achter de adoptie van de standaard?
Ja, de aanmelding van AdES Baseline Profiles wordt ondersteund door Ondernemersplein van EZ. De AdES-standaarden worden gebruikt door enkele overheidsorganisaties (zoals KvK, RDW, de Autoriteit Consument en Markt en SBR).

3.3.2.2 Staan de overheidsorganisaties die daadwerkelijk worden geraakt door een mogelijke verplichting van de standaard achter het gebruik van de standaard?
Ja, zie paragraaf 3.3.2.1.

3.3.2.3 Wordt de aangemelde versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?
Ja, zie paragraaf 3.3.2.1.

3.3.2.4 Wordt een vorige versie van de standaard binnen het organisatorische werkingsgebied door meerdere Nederlandse overheidsorganisaties gebruikt?
Het is niet bekend of de vorige versie van de standaard gebruikt wordt.

3.3.2.5 Is de aangemelde versie backwards compatible met eerdere versies van de standaard?
Ja, oude implementaties zijn compliant met de meest recente versie.

3.3.2.6 Zijn er voldoende positieve signalen over toekomstige gebruik van de standaard door (semi-)overheidsorganisaties, het bedrijfsleven en burgers?
Ja, op dit moment zijn 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. Een belangrijke gebruiker bij het gebruik van geavanceerde/ gekwalificeerde elektronische handtekeningen is de burger. Redelijkerwijs is te verwachten dat er onder burgers voldoende draagvlak is voor een voorziening die validatie van de authenticatie van overheidstukken mogelijk maakt. Op dit moment is er beschikbare software (waaronder Acrobat Reader en Word). Het tekenen met elektronische geavanceerde/gekwalificeerde handtekeningen de burger behoeft extra

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.

3.3.3 Conclusie criteria 'Draagvlak'

De expertgroep concludeert dat het gebruik van de AdES Baseline Profiles voldoende draagvlaak heeft. Er zijn voldoende positieve signalen over het toekomstig gebruik van de standaard. De adoptie van de standaarden wordt door de experts ondersteund.

3.4 Opname bevordert adoptie

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

Met de lijst wil het Nationaal Beraad de adoptie van open standaarden bevorderen die voldoen aan de voorgaande criteria (toegevoegde waarde, standaardisatieproces en draagvlak).

- Met de "pas toe of leg uit"-status beoogt het Nationaal Beraad standaarden te verplichten als:
  a. hun huidige adoptie binnen de (semi-)overheid beperkt is;
  b. opname op de lijst bijdraagt aan de adoptie door te stimuleren (functie = stimuleren).
- Met de aanbevolen standaarden beoogt het Nationaal Beraad standaarden aan te bevelen als :
  a. hun huidige adoptie binnen de (semi-)overheid reeds hoog is;
  b. opname op de lijst bijdraagt aan de adoptie door te informeren en daarmee onbedoelde afwijkende keuzes te voorkomen (functie = informeren).

3.4.1 Is "pas toe of leg uit" het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Ja, 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/gekwalificeerde elektronische handtekeningen de AdES-standaarden verplicht zijn, is het eenvoudiger om geavanceerde/gekwalificeerde elektronische handtekeningen te hanteren.

3.4.2 Is de status "aanbevolen" het passende middel om de adoptie van de standaard binnen de (semi)overheid te bevorderen?

Nee, het gebruik van AdES Baseline Profiles heeft nog niet de omvang die nodig is om de standaard als gangbaar te kunnen beschouwen.

3.4.3 Conclusie criteria 'Opname bevordert adoptie'

De expertgroep concludeert dat de 'pas toe of leg uit'-lijst het passende middel is om de adoptie van de standaard binnen de (semi)overheid te bevorderen. Op dit moment is de adoptie beperkt en zal een verplicht karakter van de standaard leiden tot een bredere adaptatie.

3.5 Adoptieactiviteiten

Gebruik van de standaard is het einddoel van het Forum en Nationaal Beraad. Plaatsing op de lijst met open standaarden is hiervoor een goede stap, maar voor het daadwerkelijk adopteren (implementeren en gebruiken) van de standaard is vaak aanvullende actie benodigd. Aanvullend kan Forum Standaardisatie dan ook bijdragen aan adoptie van de standaard door het actief inzetten van adoptie-instrumenten of ondersteunende acties. Welke kansen zijn er om de adoptie te versnellen en welke drempels bestaan er die de adoptie van de standaard hinderen?

De expertgroep doet het Nationaal Beraad de aanbeveling om bij de opname op de lijst voor 'pas toe of leg uit' de volgende oproepen ten aanzien van de adoptie van AdES Baseline Profiles te doen:

- 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.
- Het Forum Standaardisatie wordt opgeroepen om te onderzoeken of er aanvullende standaard nodig is die de eisen omtrent tijdstempelautoriteiten beschrijft.
- De oproep aan PKI Overheid om over te gaan op onderzoek naar mogelijkheden voor aanpassing van de middelen om tijdstempels te ondersteunen bij het gebruik van een PKI certificaat.