



notitie

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

FORUM STANDAARDISATIE 8 juni 2016 Agendapunt 3. Open standaarden, lijsten Stuknummer 3. Oplegnotitie lijsten

Van:	Stuurgroep open standaarden
Aan:	Forum Standaardisatie
Bijlagen:	A. Intakeadvies in procedure nemen Ades Standaarden B. Intakeadvies nieuwe versie SMEF C. Intakeadvies wijziging Webrichtlijnen D. Aanvullende Onderzoek SMTP STS E. Forumadvies opname STARTTLS i.c.m. DANE

Ter besluitvorming

U wordt gevraagd **in te stemmen** met de volgende Forum-adviezen:

1. Het in procedure nemen van standaarden voor elektronische handtekeningen (Xades, Pades, Cades en Asic). [Bijlage A]
2. Het in procedure nemen van een nieuwe versie van SMEF (standaard voor elektronisch factureren) en de aanvraag voor uitstekend beheer. [Bijlage B]
3. Het advies om de Webrichtlijnen (standaard voor web toegankelijkheid) te wijzigen en 'Principe Universeel' te verplaatsen. [Bijlage C]
4. Het aanvullend onderzoek naar SMTP STS (standaard voor e-mailbeveiliging). [Bijlage D]
5. Het opnemen van STARTTLS / DANE (Standaarden voor e-mailbeveiliging) op de lijst met standaarden. [Bijlage E]

Ter kennisname

6. Toets op de standaarden OAuth en OpenID Connect (authenticatie standaarden voor mobiele platformen).

Ter besluitvorming

Ad 1. Het in procedure nemen van standaarden voor elektronische handtekeningen. (*Bijlage A*)

Het Forum Standaardisatie wordt geadviseerd om de standaarden XAdES Baseline Profile, PAdES Baseline Profile, CAdES Baseline Profile en ASiC Baseline Profile in behandeling te nemen voor opname op de 'pas toe of leg uit'-lijst. In procedure nemen van deze standaarden is van belang om validatie van geavanceerde elektronische handtekeningen te kunnen garanderen.

Over de standaard

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).

Voorbeeld: Een gemeente verstrekt een beschikking van een omgevingsvergunning in PDF-formaat aan een burger. De vergunning kan worden gewaarmerkt met een digitale handtekening. Deze gemeente kan ervoor kiezen om een eigen profiel te gebruiken voor het ondertekenen van een digitale beschikking met een elektronische handtekening. Maar daardoor is het mogelijk dat de controlerende instantie de elektronische handtekening niet kan controleren. Het gevolg is dat software moet worden aangepast en/of er aparte afspraken gemaakt moeten worden. De open AdES Baseline Profiles is zo'n afspraak waardoor het mogelijk wordt om te controleren of de handtekening klopt zowel voor de burger als de controlerende instantie.

Betrokkenen en proces

Op 22 april 2016 zijn de standaarden ingediend door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties met steun van het Ministerie van Economische Zaken. Op donderdag 12 mei 2016 heeft een intakegesprek plaatsgevonden waarbij is gekeken of alle basisinformatie aanwezig is en of de standaard voldoet aan de criteria voor inbehandelname. Daarnaast is vooruitgeblikt op de procedure. Ook is besproken welke organisaties betrokken moeten worden tijdens de procedure en wat de mogelijke impact is voor deze organisaties. Dit is opgenomen in het intakeadvies.

Advies en aandachtspunten

Tijdens de intake is gebleken dat de standaarden voldoen aan de criteria voor inbehandelname en de kansrijkheid van de procedure wordt als voldoende geschat. Er is al ervaring met de standaarden bij overheidsorganisaties (RDW, KvK, DUO) en er is een duidelijke use case binnen de (semi) publieke sector. Ook is er op dit moment sprake van een interoperabiliteitsprobleem tussen de ondertekenaar van geavanceerde elektronische handtekeningen en de ontvanger van de handtekening. In bijgevoegde intakeadvies is dit nader toegelicht.

Aandachtspunten tijdens de procedure zijn:

- Inzicht geven in wat wel en niet wettelijk verplicht is van de 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 concurrerende standaarden vanuit leveranciers zoals de xDTM-standaard;
- De impact van implementatie van de standaard en de daarbij te maken kosten.

Ad 2. Het in procedure nemen van een nieuwe versie van SMEF, een standaard voor elektronisch factureren (*Bijlage B*)

Het Forum Standaardisatie wordt geadviseerd om de standaard SMeF 2.0 in behandeling te nemen voor opname op de lijst open standaarden met status 'pas toe of leg uit'. Op dit moment staat versie 1.3 op de lijst.

Aanvullend op het toetsen van de nieuwe versie zal getoetst worden of het beheer van de standaard voldoet aan de criteria voor 'uitstekend beheerproces'.

Over de standaard

Het Semantisch Model eFactuur (SMeF) is een standaard voor elektronisch factureren en verbindt (sector-)specifieke e-facturatie-oplossingen en -standaarden middels een gemeenschappelijk factuurmodel. Hierdoor worden verschillende formaten voor e-facturen uitwisselbaar. De standaard beschrijft welke informatie-elementen er in een elektronische factuur opgenomen dienen en kunnen worden, wat de samenhang is tussen deze elementen en wat de betekenis is van deze elementen.

Betrokkenen en proces

Op 21 april 2016 is door NEN een nieuwe versie van het Semantisch Factuurmodel (SMeF) aangemeld voor de lijst met standaarden. De aanmelder heeft als doel de standaard verplicht ('pas toe of leg uit') te stellen.

Op 9 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 en is gekeken welke organisaties betrokken moeten worden. Dit is opgenomen in het intakeadvies.

Advies en aandachtspunten

Het opnieuw in procedure nemen van deze standaard is van belang vanwege de aanmerkelijke wijzigingen die hebben plaatsgevonden in de standaard en het beheer van de standaard. Het gaat om wijzigingen waarmee SMeF 2.0 voorbereid is op invoering van het Europese eInvoicing model, wijzigingen op basis van wensen/eisen van gebruikers en de overdracht van het beheer van Logius aan TNO en NEN. Aangezien deze wijzigingen ook nadrukkelijk behandeld zijn bij het ontwikkelen van de nieuwe versie wordt het Forum geadviseerd een kleinere toets uit te voeren. Tijdens deze toets worden verschillende experts geraadpleegd, maar geen aparte expertbijeenkomst georganiseerd.

Aandachtspunten tijdens de procedure zijn:

- de inhoudelijke wijzigingen in de standaard vanwege de invoering van het Europese eInvoicing model (Richtlijn 2014/55/EU) zijn groot en zorgen ervoor dat SMEF 2.0 niet backwards compatibel is met voorgaande versies. Het effect op eindgebruikers lijkt beperkt, maar de impact voor implementatie in de praktijk zal expliciet worden meegenomen in de toets;
- begin 2015 is de beheerorganisatie van SMEF gewijzigd. Het beheer is van Logius overgedragen aan TNO en NEN. De ervaringen hiermee zullen worden getoetst alsmede of de huidige beheerstructuur voldoende is voor het predicaat 'uitstekend beheer'.

In de procedure zullen de volgende partijen middels interviews worden betrokken: beheerders van SMEF: NEN en TNO, beheerders van de standaarden OHNL, SETU, Simplerinvoicing, Energie eFactuur, Sales in de bouw en FrugiCom en enkele eindgebruikers/ beheerders van voorzieningen, zoals Logius (DigiInkoop), UWV en/of Randstad.

Ad 3. Intakeadvies wijzigingen Webrichtlijnen (*Bijlage C*)

Het Forum Standaardisatie wordt geadviseerd om:

1. De procedure te starten voor het verwijderen van de standaard Webrichtlijnen van de 'pas toe of leg uit'-lijst en deze te vervangen voor de Europese standaard voor toegankelijkheid van ICT producten en diensten EN 301 549;
2. De nationale standaard voor bouwkwaliteit, het Principe Universeel en op dit moment onderdeel van Webrichtlijnen 2.0, in procedure te nemen voor opname op de lijst met aanbevolen standaarden en daarmee te verwijderen van de 'pas toe of leg uit'-lijst.

Gegeven de maatschappelijke betrokkenheid rond dit onderwerp zal het ministerie van BZK de beleidslijn rond de verzochte aanpassing duidelijk en breed communiceren. De aanpassingen zullen in regiegroepen gepresenteerd worden aan overheden en in reguliere contacten met belangenorganisaties toegelicht worden. Belangenorganisaties hebben reeds eerder verzocht om de eisen op het gebied van bouwkwaliteit los te koppelen van de toegankelijkheidseisen, omdat dit de standaard volgens hen onnodig verzaamd; zij zullen naar verwachting instemmen met de nieuwe beleidslijn.

Over de standaarden

Voor de Europese richtlijn overheidsopdrachten (omgezet in de gewijzigde Aanbestedingswet) is een Europese standaard voor de toegankelijkheid van ICT-producten en -diensten ontwikkeld (EN 301 549). Deze standaard wordt verplicht gesteld in de aanstaande richtlijn toegankelijkheid overheidswebsites voor websites en apps van de overheid. Medio 2018 moet deze omgezet zijn in nationale wetgeving. Op termijn kunnen de Webrichtlijnen in huidige vorm niet meer toegepast worden. Om eenduidigheid te realiseren voor marktpartijen en overheden, is het advies om de procedure te starten om de Webrichtlijnen te verwijderen en te vervangen voor EN 301 549 op de 'pas toe of leg uit'-lijst, na toetsing op de criteria.

De Webrichtlijnen zoals deze op de lijst staat bestaat naast principes, beginselen en criteria voor toegankelijkheid, die zowel in Webrichtlijnen als in EN 301 549 identiek zijn aan de internationale standaard WCAG 2.0, ook uit de aanvullende specificatie 'Principe Universeel'. Principe Universeel ziet toe op bouwkwaliteit en is niet gebaseerd op een internationaal of Europees vastgestelde norm of standaard. De vermenging van

de Europese toegankelijkheidseisen met nationale eisen voor bouwkwaliteit zal door de Europese Commissie naar verwachting worden gezien als een onnodige en ontoelaatbare verzwaring van de eisen (EN 301 549) (verbod op 'goldplating').

Voor het onderdeel Principe Universeel betekent dit dat het de beste optie is om de standaard als een zelfstandige standaard te toetsen. Het wordt dus niet gekoppeld aan EN 301549, waar het nu wel gekoppeld is met Webrichtlijnen. Daarbij is het verzoek ingediend om het 'Principe Universeel' op te nemen met de status aanbevolen in plaats van 'pas toe of leg uit'. Het verminderen van de verplicht toe te passen richtlijnen en criteria, komt tegemoet aan de in de praktijk veel geuite klacht dat er 'zoveel criteria' moeten worden toegepast.

Betrokkenen en proces

Op 26 april 2016 is het verzoek om de Webrichtlijnen versie 2 te wijzigen aangemeld door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties (BZK). Op 11 mei 2016 heeft een intakegesprek plaatsgevonden en op 31 mei een nader informeren gesprek. Hierbij is gekeken of alle basisinformatie aanwezig is en welk scenario het best past bij de nieuwe ontwikkelingen. Daarnaast is vooruitgeblikt op de procedure en welke organisaties betrokken moeten worden. Dit is opgenomen in het intakeadvies.

Aandachtspunten voor de procedure

Geadviseerd wordt om in de procedure in ieder geval aandacht te geven aan de volgende punten:

- Te kijken of het 'functioneel toepassingsgebied' van Webrichtlijnen 2.0 als zodanig kan worden overgenomen voor de standaard EN 301 549 of dat deze moet worden aangepast;
- Hierin meenemen dat de toepassing van EN 301 549 breder is dan het huidige toepassingsgebied voor de Webrichtlijnen. Zo wordt o.a. het gebruik in Mobiele Applicatie en Intranetten verplicht. Het alvast toepassen van de standaard voor gebruik aldaar dient in ieder geval te worden aanbevolen, eventueel als aanvulling op het functioneel toepassingsgebied;
- Te kijken of het functioneel toepassingsgebied en het organisatorisch werkingsgebied voor het 'Principe Universeel' een op een kan worden overgenomen van het huidige toepassingsgebied voor Webrichtlijnen 2.0.
- Gegeven de maatschappelijke betrokkenheid rond dit onderwerp, zorgvuldig te communiceren en ervoor te zorgen dat de juiste organisatie betrokken zijn (aan het eind van dit advies is een overzicht van de te betrekken organisaties opgenomen). Daarnaast heeft de indiener aangegeven om de voorgenomen wijziging duidelijk en breed te communiceren.
- Wat de impact is van het implementeren van EN 301 549 en alvast vooruit te kijken hoe tot implementatie te komen van de Europese standaard EN301549.
- Verder zal goed gekeken moeten worden in hoeverre EN301 549 meer is dan een technische specificatie en hoe hiermee om te gaan in relatie tot een eventuele plaatsing op de lijst.

**Ad 4. Aanvullend onderzoek naar SMTP STS, standaard voor veilig mailen.
(Bijlage D)**

Het Forum Standaardisatie wordt gevraagd om:

1. kennis te nemen van de standaard SMTP STS;
2. kennis te nemen van de beoordeling van SMTP STS op de toetsingscriteria;
3. in te stemmen met het advies om de ontwikkelingen rondom SMTP STS in de gaten te houden en de besluitvorming omtrent de opname van STARTTLS en DANE voort te zetten.

Aanleiding en over de standaard

Ten tijde van de openbare consultatie van STARTTLS en DANE is een voorstel voor een nieuwe standaard (SMTP STS) ingediend bij de Internet Engineering Task Force (IETF), ondersteund door de grotere mailplatformen (Gmail, Yahoo, Microsoft). Het voorstel beschrijft een standaard voor de totstandkoming van versleutelde verbindingen tussen mailservers, waarbij het gebruik van DNSSEC niet noodzakelijk is.

Deze conceptstandaard kan gezien worden als potentiële concurrent van DANE en kan een impact hebben op de adoptie van STARTTLS en DANE, maar ook van DNSSEC. Het Forum Standaardisatie heeft zodoende de opdracht gegeven om aanvullend onderzoek te doen naar SMTP STS en de impact hiervan alvorens een besluit te nemen over de opname van de combinatie STARTTLS en DANE op de lijst met open standaarden.

Betrokkenen en proces

In bijgevoegde onderzoek is gekeken naar het voorstel voor de standaard SMTP STS, zoals eind maart ingediend bij IETF. Ook is het voorstel beoordeeld tegen de toetsingscriteria voor de lijst met open standaarden. De notitie geeft de uitkomsten van het onderzoek kort weer en sluit af met een advies aan het Forum Standaardisatie. Een eerste conceptversie van dit advies is aan de leden van de expertgroep STARTTLS en DANE en het Bureau Forum Standaardisatie gestuurd met het verzoek om een reactie op het advies. Na verwerking van deze reacties is het advies ingediend bij het Bureau Forum Standaardisatie.

Advies en vervolg

Naar aanleiding van het onderzoek kan geconcludeerd worden dat SMTP STS en de combinatie STARTTLS en DANE een overlappend toepassingsgebied hebben. Maar gezien de huidige premature status van het voorstel van SMTP STS is het voor de overheid niet wenselijk om een afwachtende houding aan te nemen. STARTTLS en DANE zijn beide ontwikkelde standaarden in beheer bij een gerenommeerde standaardisatieorganisatie en kunnen daadwerkelijk al geïmplementeerd worden.

Opname van STARTTLS in combinatie met DANE maakt het mogelijk om e-mailverkeer tussen overheden, tussen overheden en bedrijven en tussen overheden en burgers via een versleutelde verbinding mogelijk te maken. Ook is opname op de lijst een stimulans voor mailproviders om DANE en DNSSEC te ondersteunen.

Het Forum Standaardisatie wordt wel geadviseerd om de ontwikkelingen rondom SMTP STS in de gaten te houden en wanneer SMTP STS eenmaal een ontwikkelde standaard is deze opnieuw te duiden in relatie tot STARTTLS en DANE. Het advies is dan ook om deze ontwikkeling te volgen en waar mogelijk te participeren in de doorontwikkeling. De aangewezen partij hiervoor is het NCSC, conform haar Cyber Security strategie.

Ad 5. Het opnemen van STARTTLS / DANE (standaarden voor e-mail-beveiliging) op de lijst met standaarden (Bijlage E)

Het Forum Standaardisatie adviseert het Nationaal Beraad Digitale Overheid om:

1. STARTTLS i.c.m. DANE op te nemen als 'pas toe of leg uit'-standaard op de lijst met open standaarden voor het hieronder geformuleerde toepassings- en werkingsgebied.
2. In te stemmen met de additionele adviezen ten aanzien van de adoptie van STARTTLS i.c.m. DANE, zoals geformuleerd in bijgevoegde notitie.

Over de standaarden

STARTTLS en DANE zijn (e-mail)beveiligingsstandaarden die kunnen worden gebruikt om een beveiligde verbinding tussen mailservers op te zetten. STARTTLS zorgt er voor dat een niet-versleutelde, en daarmee onbeveiligde, SMTP-verbinding geüpgrade wordt naar een versleutelde TLS-verbinding.

De toepassing van DANE zorgt er voor dat een verbinding pas tot stand wordt gebracht wanneer het DNS-record van de ontvangende mailserver is gecontroleerd door de verzendende mailserver. Hierdoor is het voor aanvallers niet mogelijk om berichtenverkeer 'af te luisteren' of te manipuleren. Gebruikers van STARTTLS en DANE moeten de verbinding verbreken wanneer er geen beveiligde verbinding via STARTTLS opgezet kan worden, maar deze wel aanwezig is volgens het DNS-records. Geadviseerd wordt om STARTTLS en DANE in combinatie op te nemen op de lijst met open standaarden met de status 'pas toe of leg uit'.

Betrokkenen en proces

Tijdens de intake is besloten om DANE en STARTTLS als gecombineerde standaarden in behandeling te nemen om een beveiligde verbinding tussen mailservers op te kunnen zetten. Vervolgens heeft een expertbijeenkomst plaatsgevonden op 28 januari 2016. De conclusie van de expertgroep was om STARTTLS en DANE op te nemen op de lijst met open standaarden. Tijdens de openbare consultatie van het expertadvies van 16 februari tot 16 maart 2016 is één reactie ontvangen. Wel is tijdens de openbare consultatie een nieuwe soortgelijke standaard (SMTP STS) gepubliceerd, ondersteund door de grotere mail platformen (Gmail, Yahoo, Microsoft). In samenspraak met de experts en het Forum is toen besloten om hier een aanvullend onderzoek naar te doen. De uitkomsten van deze procedurestappen zijn opgenomen in bijgevoegde Forumadvies.

Consequenties en vervolgstappen

Het gebruik van de standaarden is binnen het geadviseerde organisatorische werkingsgebied beperkt, met name waar het DANE betreft. Wel zijn er verschillende overheidsorganisaties die de standaarden ondersteunen. Zo heeft het Nationaal Cyber Security Center (NCSC) de standaarden onlangs geïmplementeerd. Ook zijn er positieve signalen bij andere overheidspartijen die de standaarden op korte termijn in gebruik nemen. Daarnaast is het mogelijk om de implementatie van de standaarden te toetsen via Internet.nl. Aanbevolen wordt om dit nauw te blijven monitoren. Verder is de opname van STARTTLS en DANE een positieve impuls voor de adoptie van DNSSEC, omdat de standaarden verplicht gebruik maken van DNSSEC.

Gezien de recente ontwikkeling met betrekking tot SMTP STS is het belangrijk om zicht te houden op het gebruik van de standaarden bij de grote mailplatformen en de ontwikkeling rondom SMTP STS goed te volgen. Verder zijn er enkele adviezen om de

adoptie van de standaard te bevorderen. Deze staan in bijgevoegde advies.

Toepassingsgebied

Het advies is om STARTTLS i.c.m. DANE op te nemen voor de volgende toepassing:

Inkomende mailservers passen STARTTLS (SMTP over STARTTLS, oftewel ESMTPS) in combinatie met DANE toe, zodat verzendende mailservers daarmee een versleutelde verbinding over een onvertrouwd netwerk (zoals internet) kunnen opzetten. Dit voorkomt dat aanvallers het mailverkeer kunnen afluisteren (passieve aanvallers) en/of kunnen manipuleren (actieve aanvallers).¹



Figuur 1. Geadviseerd functioneel toepassingsgebied

Het toepassingsgebied geldt voor de mailverbindingen buiten de eigen (besloten) infrastructuur. Ook betreft de verplichting vooralsnog inkomende mail. De implementatie van STARTTLS in combinatie met DANE is voor uitgaande mailservers ingewikkelder en vraagt meer inzet in tijd en middelen. Ook is er onvoldoende ervaring binnen de overheid met de implementatie van de standaarden voor uitgaande mail. Zodra er meer ervaring is opgedaan met implementatie kan het toepassingsgebied worden uitgebreid met uitgaande mailstromen. Geadviseerd wordt om dit een jaar na opname van de standaarden te toetsen in samenspraak met de expertgroep.

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

Ter kennisname

Ad 6. Toets op de standaarden OAuth en OpenID Connect (authenticatiestandaarden voor mobiele platformen).

Tijdens de bespreking van het onderzoek naar RESTful APIs in de Forum-bijeenkomst van 15 maart is besloten om de standaarden OAuth en Odata te toetsen voor opname op de lijst met standaarden (aanbevolen of 'pas toe of leg uit'). Gezien de capaciteit en actualiteit is besloten is om eerst OAuth te toetsen. Deze standaard wordt veel gebruikt als authenticatie- en autorisatiestandaard binnen 'webbased' applicaties en mobiele applicaties. Met OAuth kunnen gebruikers een programma of website toegang geven tot hun privégegevens die opgeslagen zijn op een andere website zonder hun gebruikersnaam en wachtwoord uit handen te geven. Met name in een webomgeving waar je niet direct weet met welke partijen je communiceert, maar waarbij betrouwbaarheid wel belangrijk is, wordt de standaard gebruikt.

¹ Het gaat hier om IETF RFC 3207 (<https://tools.ietf.org/html/rfc3207>), RFC 3848 (<https://tools.ietf.org/html/rfc3848>) en IETF RFC 7672 (<https://tools.ietf.org/html/rfc7672>).

OpenID Connect is een veelgebruikt profiel gebaseerd op OAuth. Daarom is besloten om de twee standaarden gezamenlijk te toetsen. De expertbijeenkomst zal op 7 juli plaatsvinden, waarbij met name gekeken zal worden naar de ervaringen met de standaard binnen de overheid, waar de standaard met name ingezet wordt, wat de verhouding is tot SAML en voor welke status en toepassing de standaard in aanmerking komt. Aan de Forumleden de vraag om de mee te denken wie te betrekken en de bijeenkomst onder de aandacht te brengen.