FS-20170308.02

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 08 maart 2017

Agendapunt 2. Open standaarden, lijsten
Stuknummer 2. Oplegnotitie lijsten

Van:	Stuurgroep open standaarden
Aan:	Forum Standaardisatie
Bijlagen:	A. Aanvullend onderzoek Ades Standaarden

Ter bespreking
*U wordt gevraagd **in te stemmen** met het volgende Forumadvies:*

A. Aanvullend onderzoek Ades Baseline Profiles *(standaarden voor elektronische handtekeningen)* [Bijlage A]
B. Verzoek voor het in trekken van de nu in procedure zijnde standaard Digikoppeling 3.0

Ter kennisname

C. Stand van zaken procedures
   1. HTTPS
   2. Oauth
   3. ODATA
   4. Dmarc
   5. ETSI TS 119 312

Ter bespreking

Ad A. Aanvullend onderzoek Ades Baseline Profiles
[Bijlage A]

Het Forum Standaardisatie wordt gevraagd om in te stemmen met:

Het Forum Standaardisatie adviseert het Nationaal Beraad Digitale Overheid om in te stemmen met het opnemen van standaard voor geavanceerde elektronisch handtekeningen (de Ades Baseline Profiles) op de lijst met open standaarden met de status 'pas toe of leg uit'.

Daarnaast wordt aan het Forum gevraagd om in te stemmen met de additionele adoptieadviezen zoals benoemd in bijgevoegd advies.

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

Een ondertekenaar is op dit moment vrij in de keuze van een standaard voor het zetten van een geavanceerde/gekwalificeerde elektronische handtekening. Het gevolg is dat een ondertekenaar een document kan tekenen op basis van een standaard die niet hetzelfde is als de standaard die de ontvanger ondersteunt. In de praktijk is de situatie dat een ontvanger niet van tevoren weet of én op welke manier de handtekening gevalideerd kan worden. Een handtekening kan dan onleesbaar blijken voor de ontvanger.

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

Over het aanvullend onderzoek
De AdES Baseline Profiles zijn aangemeld door het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Er heeft er een intake, experttoets en openbare consultatie plaatsgevonden. Naar aanleiding hiervan en de Forumvergadering van 19 oktober stonden er vragen open die eerst beantwoord moesten worden voordat besloten kon worden over opname op de 'pas toe of leg uit'-lijst. Deze vragen zijn:

1. Op welke manier kan er een actieve community gevormd worden die de adoptie van de standaard ondersteunt en die fungeert als aanspreekpunt waar overheden terecht kunnen voor vragen over (toepassing van) de standaard?
2. Zijn er bestaande use cases en kunnen deze gebruikt worden als praktijkvoorbeelden voor implementatie?
3. Waar worden de standaarden ondersteund (software / leveranciers) en op welke manier worden overheden ondersteund bij de technische implementatie van de

standaard?

In bijgevoegd advies zijn bovenstaande vragen uitgewerkt en wordt geadviseerd over het opnemen van de Ades Baseline Profiles op de 'pas toe of leg uit'-lijst.

Advies
De conclusie van het onderzoek is dat er geen beperkende factoren zijn om de standaard op te nemen op de 'pas toe of leg uit'-lijst op het moment dat documenten in de vorm van een XML-, PDF-, CMS-, en ZIP-bestand voorzien worden van een geavanceerde en/of gekwalificeerde elektronische handtekening of zegel.

Er zijn verschillende implementatie van de standaarden binnen de overheid bekend, met name voor Pades en Xades. Ook zijn er voldoende (open source) softwarepakketten in de markt aanwezig die gebruik en toepassing van de standaarden ondersteunen. Daarbij zijn er zowel grote als kleinere leveranciers die standaard gebruiken.

Wat wel binnen Nederland ontbreekt is een organisatie of aanspreekpunt waar gebruikers terecht kunnen voor implementatievragen, al is er een soortgelijk initiatief op Europees niveau. Dit kan potentieel de adoptie van de standaarden belemmeren en vertragen. Daarom wordt aan de indiener (Ministerie van BZK) meegegeven om een actieve rol aan te nemen m.b.t. het delen van kennis en ervaring. In lijn daarmee wordt geadviseerd om over twee jaar de stand van zaken en adoptiestatus van de standaard opnieuw te beoordelen.

Meer informatie over het toepassingsgebied en de adoptieadviezen is te vinden in bijgevoegd advies.

Ad B. Verzoek intrekken Digikoppeling 3.0

Over de lopende procedure
Ruim twee jaar geleden is een nieuwe versie van Digikoppeling ingediend voor opname op de lijst van standaarden (Digikoppeling 3.0), dit ter vervanging van de versie 2.0 die op de lijst staat. In de Forumvergadering van 28 oktober 2015 is vervolgens het volgende besloten[1]:

> *"Het beperkte gebruik van het WS-RM-profiel in Digikoppeling geeft aanleiding om Digikoppeling 3.0 nog niet op de lijst te plaatsen. Het plaatsen op de lijst kan pas wanneer de beheerorganisatie aantoont dat er meerdere succesvolle implementaties zijn van WS-RM conform het profiel dat in Digikoppeling is opgenomen. Dit is in lijn met het toetsingscriterium 'draagvlak'. Daarnaast moet de beheerorganisatie de compliance voorziening nog geschikt maken voor WS-RM.*

De Digikoppeling Compliance Voorziening mét WS-RM is wel in productie genomen er zijn echter geen organisaties die het WS-RM Digikoppeling koppelvlak gebruiken vandaar dat de beheerorganisatie besloten heeft het onderdeel WS-RM niet meer te ondersteunen en de aanmelding van versie 3.0 terug te trekken.

Het verzoek
Bij het Bureau Forum standaardisatie is het volgende verzoek binnengekomen:

" *Van: Hering, P.N. (Pieter) - Logius*

[1] *https://www.forumstandaardisatie.nl/sites/default/files/FS/2015/1028/FS-20151028.02-Oplegnotitie-Lijsten-open-standaarden.pdf*

Verzonden: woensdag 25 januari 2017 16:24
Aan: Forum standaardisatie
CC: Veen, M.A van der (Maarten) - Logius; Schellevis, H.L. (Lancelot) - Logius; Metz, O.M (Onno) - Logius; Damen, N. (Nicole) - Logius; Plas, M. van der (Martin) - Logius
Onderwerp: Intrekking verzoek tot plaatsing Digikoppeling 3.0 op de Pas-Toe-Leg-Uit lijst

Geachte Forum Standaardisatie, Beste Maarten en Lancelot

Hierbij wil ik namens Logius het verzoek voor het plaatsen van de Digikoppeling 3.0 standaard op de Pas-Toe-of-Leg-uit Lijst (PTOLU) intrekken.

Reden voor deze intrekking is dat uit het onderzoek van adviesbureau Deloitte is gebleken dat het WS-RM profiel bij overheden niet of nog niet gebruikt wordt. Minimaal twee werkende implementaties is een eis in de procedure van BFS voor opname op de PTOLU lijst. Verder bleek ook dat de geraadpleegde leveranciers van Digikoppeling adapters nauwelijks of geen ondersteuning bieden voor de WS-RM standaard. Het onderzoek liet overigens zien dat vanuit het bedrijfsleven wel belangstelling is voor WS-RM.

Bij de aanvraag tot plaatsing van Digikoppeling 3.0 op de PTOLU Lijst is tevens gevraagd om het predicaat Uitstekend Beheervoor de standaard. Daarnaast is tijdens de plaatsingsprocedure in een werkgroep onderzocht om het functioneel toepassingsgebied en het organisatorische werkingsgebied van de standaard aan te passen. Hoe we ook deze onderwerpen willen oppakken beschrijven we in de navolgende aanpak.

Plan van aanpak

Als beheerder van de standaard stellen we de volgende fasering voor om intrekking en aanpassing van het gebruik van de standaard te realiseren:

- *met het intrekken van de aanvraag voor plaatsing van Digikoppeling 3.0 blijft Digikoppeling 2.0 ongewijzigd op de PTOLU lijst staan;*
- *Logius gaat voorafgaand aan eventuele wijzigingen van het beheer en toepassing- en werkingsgebied eerst in 2017 een onderzoek doen naar een andere manier van versiebeheer van de standaard. Digikoppeling in nu een 'paraplustandaard' met een eigen versie (zoals 'Digikoppeling 2.0') waarin verschillende standaarden – ebMS, WUS en Grote Berichten- worden beschreven. Deze situatie is voor de versionering van de onderdelen en het (verplicht) gebruik niet transparant. Het onderzoek moet duidelijk maken of opsplitsen in delen, bijvoorbeeld synchroon, asynchroon en grote berichten de toepassing door gebruikers duidelijker maakt - te vergelijken met Geostandaarden en SETU;*
- *nadat dit onderzoek is afgerond zullen we een nieuw verzoek doen aan het Forum Standaardisatie voor plaatsing van de Digikoppeling standaard op de PTOLU lijst, met eventueel een ander vorm van versionering en opdeling in substandaarden;*
- *in dit verzoek zullen we ook de wijziging voor toepassings- en werkingsgebied en het verzoek voor uitstekend beheer opnemen;*

Reden voor deze fasering is dat we alle wijzigingen met de betrokkenen in het Digikoppeling Technisch Overleg kunnen bespreken, zodat we gestand doen aan de governance die in het Digikoppeling Beheermodel is beschreven.

Met vriendelijke groet,

Pieter Hering

Pieter Hering
Lead Architect Stelselvoorzieningen
.....
Logius
Ministerie van Binnenlandse Zaken en Koninkrijksrelaties
Wilhelmina van Pruisenweg 52 | 2595 AN | Den Haag
Postbus 96810 | 2509 JE | Den Haag"

Vervolgstappen
Het Bureau Forum Standaardisatie zal in overleg met de indiener de volgende acties ondernemen:

- Onderzoeken hoe Digikoppeling en de onderliggende standaarden het best op de lijst kunnen worden opgenomen. Daarbij wordt gekeken of het wel nodig is om een aparte versienummer voor Digikoppeling te hanteren of dat het duidelijker is om alleen de versies nummers van de onderliggende standaarden te benoemen;
- Toetsen of het nieuw voorgestelde toepassingsgebied uit de procedure op Digikoppeling versie 3 nog steeds klopt en op de lijst aangepast kan worden;
- Toetsen of het beheer op Digikoppeling voldoet aan het predicaat 'Uitstekend Beheer'. Dit was onderdeel van de toets op versie Digikoppeling versie 3 en gekeken zal of de resultaten uit deze toets nog steeds actueel zijn.

Bovenstaande vragen zullen ook worden afgestemd met de oorspronkelijk betrokken experts en organisaties. Naar verwachting kunnen we in de forumvergadering van 14 juni over de uitkomsten rapporteren

Ter kennisname

Ad C. Stand van zaken procedures
Op dit moment zijn er zeven standaarden, twee daarvan (Ades Baseline Profiles en Digikoppeling 3.0) zijn hierboven al besproken. Drie andere (Oauth, HTTPS en ETSI TS 119 312) zijn nu in openbare consultatie. Naar Odata wordt een klein onderzoek uitgevoerd en voor DMARC staat er nog één actiepunt open voordat deze opgenomen kan worden. Hieronder wordt de stand van zaken kort toegelicht.

1. HTTPS
Regelmatig komen er vragen over waarom de beveiligingsstandaard HTTPS op de aanbevolen lijst staat en waarom de beveiligingsstandaard TLS op de verplichte lijst staat. Want TLS is ook van toepassing op websites en dwingt HTTPS af indien deze wordt toegepast op een webserver. Onze lijst met standaarden zegt echter niet dat websites beveiligd moeten worden met de HTTPS standaard. Dit wordt nu aanbevolen.

Om meer duidelijkheid te geven over het verschil tussen HTTPS en TLS, of we nu geen tegenstrijdigheid propageren (aanbevolen vs verplicht) en of een aanvullende verplichting via 'pas toe of leg uit' van HTTPS nodig is loopt er een onderzoek naar de standaard. Deze uitkomsten zijn nu in openbare consultatie (van 24 februari tot 25 maart) en het voorlopige advies is om HTTPS (i.c.m. met HSTS) via 'pas toe of leg uit' te verplichten voor alle overheidswebsite. Dat dit onderzoek relevant is blijkt wel uit: http://www.nu.nl/internet/4399254/plasterk-wil-toch-beveiligde-verbinding-

verplichten-alle-overheidssites.html

2. Oauth
De standaard Oauth is nu in openbare consultatie waarbij het advies is om Oauth op te nemen voor applicaties waarbij gebruikers (resource owner) toestemming geven (impliciet of expliciet) aan een dienst (van een derde) om namens hem toegang te krijgen tot specifieke gegevens via een RESTful API. Voordat de standaard opgenomen wordt is het wel eerst nodig om aanvullende afspraken te maken over wat de beste manier is om de standaard binnen de overheid te implementeren zodat voorkomen wordt dat er verschillende soorten implementaties ontstaan.

3. Odata
Naar de standaard Odata wordt nu een onderzoek uitgevoerd in de vorm van een interview ronde. Odata is een standaard dat ervoor zorgt dat data op een uniforme wijze weergegeven kan worden zodat deze via APIs uitgewisseld kan worden. Het Forum heeft eerder besloten om deze standaard te toetsen. De voorlopige bevindingen zijn dat deze standaard waarschijnlijk niet in aanmerking komt voor opname op de 'pas toe of leg uit'-lijst, maar wel voor opname op de aanbevolen lijst.

4. Dmarc
De e-mailbeveiligingsstandaard Dmarc staat al sinds 18-05-2015 in het voorportaal van opname op de lijst met standaarden. Opname van de standaard is goedgekeurd door het Nationaal Beraad onder de voorwaarde dat de standaard officieel in beheer is genomen door de standaardisatieorganisatie IETF. Ondanks eerdere berichten dat dit zou gebeuren is dit tot op heden nog niet geëffectueerd. Mede met oog op het toenemend gebruik van de standaard en verplichtingen om de standaard te gebruiken is het wenselijk dat de standaard zijn status van 'in behandeling' inruilt voor de status 'opgenomen' op de lijst met standaarden. Vandaar dat we voor komende Forumvergadering uitzoeken wat de stand van zaken is en de daarbij horende acties.

5. ETSI TS 119 312
119 312 is een aanbevolen standaard voor het waarborgen van de authenticiteit van een document via het toevoegen van een elektronische handtekening, er is ook een nauwe relatie met de Ades Baseline Profiles. Eind 2015 is een nieuwe versie van de standaard gepubliceerd, deze versie is nu in openbare consultatie.