



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

CONCEPT FORUM STANDAARDISATIE 19 april 2017

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

Van:	Stuurgroep open standaarden
Aan:	Forum Standaardisatie
Bijlagen:	A. Forumadvies HTTPS & HSTS B. Forumadvies OAuth 2.0 C. Forumadvies ETSI 119 312 D. Rapport verduidelijking functionele toepassingsgebieden F. Reactie KOOP evaluatie OWMS PTOLU-lijst

Ter besluitvorming

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

- A. Forumadvies HTTPS en HSTS (*standaarden voor website en webserver beveiliging*) [Bijlage A]
- B. Forumadvies OAuth (*standaard voor API autorisatie*) [Bijlage B]
- C. Forumadvies ETSI 119 312 (*standaard voor elektronische handtekeningen*) [Bijlage C]
- D. Rapport verduidelijking functionele toepassingsgebieden. [Bijlage D]

Ter kennisname

- E. Reactie evaluatie OAI-PMH
- F. Reactie evaluatie OWMS [Bijlage F]

Ter besluitvorming

Ad A. Forumadvies beveiligingsstandaarden HTTPS en HSTS [Bijlage A]

Het Forum Standaardisatie wordt gevraagd om in te stemmen met:

Het Forum Standaardisatie adviseert het Nationaal Beraad Digitale Overheid om:

1. De status van HTTPS en HSTS te wijzigen van 'aanbevolen' naar 'pas toe of leg uit'.
2. In te stemmen met de additionele adviezen ten aanzien van de adoptie van de standaard zoals benoemd in bijgevoegd advies.

Over de standaarden

HTTPS, is een uitbreiding op het HTTP-protocol met als doel een veilige uitwisseling van gegevens met een website of webservice. Bij gebruik van HTTPS worden de gegevens versleuteld, waardoor het voor een buitenstaander, bijvoorbeeld iemand die afluistert, onmogelijk zou moeten zijn om te weten welke gegevens verstuurd worden. De standaarden staan op de lijst met standaarden van het Forum met als status aanbevolen. Terwijl de standaard TLS verplicht is conform 'pas toe of leg uit'. Gezien de raakvlakken tussen deze standaarden blijkt in de praktijk dat het verschil in status verwarrend is voor organisaties. Ook is er een toenemende roep om HTTPS te verplichten voor alle overheidswebsites. Vandaar dat het advies is om de standaarden HTTPS en HSTS te verplaatsen van aanbevolen naar verplicht ('pas toe of leg uit').

Betrokkenen en Proces

VKA, procedurebegeleider open standaarden in opdracht van het Bureau Forum Standaardisatie, heeft het onderzoek uitgevoerd. Hiertoe heeft een intakegesprek plaatsgevonden met het Bureau Forum Standaardisatie. Het expertadvies is opgesteld op basis van de intake en een aantal gesprekken met (potentiële) gebruikers en andere kennishebbers. Tijdens de openbare consultatie van het expertadvies van 24 februari – 25 maart 2017 zijn vijf reacties ontvangen. Het waren overwegend aanvullingen op het expertadvies en positief over de verplichting van HTTPS en HSTS. De reacties zijn in overleg met de betrokken partijen verwerkt in dit forumadvies.

Advies en gevraagd besluit

Geadviseerd wordt om HTTPS & HSTS te verplaatsen naar de 'pas toe of leg uit'-lijst. Gelet op het toepassingsgebied wordt ook geadviseerd om de standaard HTTP (versie 1.1 en 2) te verwijderen van de aanbevolen lijst omdat deze daarmee automatisch onderdeel is van de opname van HTTPS en HSTS. Dit om eventuele onduidelijkheid over http (aanbevolen) en HTTPS (verplicht) te vermijden. Meer informatie over het toepassingsgebied en de adoptieadviezen is te vinden in bijgevoegd advies. Aan het Forum wordt ook expliciet gevraagd of de oproep om implementatie voor eind 2018 uit de adoptie-impuls (zie additioneel advies 1 – pag 3) wel of niet vervroegd moet worden, zoals het CIBO vraagt (zie binnengekomen reacties – pag 9).

Ad B. Forumadvies autorisatiestandaard OAuth 2.0**[Bijlage B]****Het Forum Standaardisatie wordt gevraagd om in te stemmen met:**

Het Forum Standaardisatie adviseert het Nationaal Beraad Digitale Overheid om:

1. voor de overheid basis toepassingsprofiel voor OAuth 2.0 te ontwikkelen, en
2. de opname van OAuth 2.0 op de lijst voor 'pas toe of leg uit' aan te houden tot dit toepassingsprofiel voor OAuth 2.0 is opgesteld.

Over de standaard

Met OAuth 2.0 kunnen gebruikers of organisaties een programma of website toegang geven tot specifieke (privé)gegevens, die opgeslagen zijn op een ander systeem, zonder hun gebruikersnaam en wachtwoord uit handen te geven. OAuth 2.0 is een autorisatiestandaard voor met name webbased applicaties die gegevens uitwisselen met behulp van API's. Plaatsing op de lijst open standaarden met de status 'pas toe of leg uit' biedt overheden houvast en een duidelijk signaal dat OAuth 2.0 de te verkiezen standaard is. Het gebruik van OAuth 2.0 is groeiend, maar voor implementatie zijn er slechts enkele concrete plannen bekend. De adoptie van de standaard heeft daarom een extra stimulans nodig.

Betrokkenen en proces

Het Forum Standaardisatie heeft besloten de standaarden OAuth 2.0 en OpenID Connect in procedure te nemen voor opname op de 'pas toe of leg uit'-lijst. Aanleiding daartoe was de bespreking door het Forum van het Discussiedocument RESTful API's. Op basis van dit besluit is de expertgroep op 7 juli 2016 en 22 september 2016 bijeengekomen om de standaard, de aandachtspunten en openstaande vragen uit het voorbereidingsdossier te bespreken. Tijdens deze bijeenkomst is ook het advies ten aanzien van het functioneel toepassingsgebied vastgesteld. Het expertadvies is beschikbaar gesteld voor publieke consultatie. Dit heeft drie reacties opgeleverd.

Advies en gevraagd besluit

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, maar onder de voorwaarde dat er eerst een best practise of een soort van toepassingsprofiel voor de overheid is ontwikkeld. De expertgroep vindt het belangrijk om een gemeenschappelijk toepassingsprofiel te ontwikkelen zodat voorkomen wordt dat er verschillende implementaties ontstaan. Het advies is om in eerste instantie te starten met een basisprofiel met een algemeen karakter en algemene uitgangspunten. Omdat als zo'n profiel te diep uitgewerkt moet worden met dito beheer dan is het risico dat niemand daarvoor de verantwoordelijkheid neemt. Om te komen tot het toepassingsprofiel zou het Forum Standaardisatie hierbij in eerste instantie de rol van secretariaat op zich moeten nemen.

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

Ad C. Forumadvies elektronische handtekening standaard ETSI 119 312**[Bijlage C]****Het Forum Standaardisatie wordt gevraagd om in te stemmen met:**

Het Forum Standaardisatie adviseert het Nationaal Beraad Digitale Overheid om de aanbevolen standaard ETSI TS 102 176-1 v2.1.1 voor het waarborgen van elektronisch handtekeningen te vervangen voor een nieuwere versie van deze standaard: de ETSI TS 119 312.

Over de standaard

De standaard ETSI TS 102 176-1 v 2.1.1 uit 2011 is een standaard voor het waarborgen van de authenticiteit van een elektronische handtekening die aan een document is toegevoegd. De standaard staat op de lijst met standaarden van het Forum Standaardisatie met als status aanbevolen. Eind 2014 is deze standaard gewijzigd en vervangen voor een nieuwe versie, namelijk de ETSI TS 119 312 v1.1.1.

Betrokkenen en proces

Vanuit Logius (PKIoverheid) is het verzoek ingediend om op de lijst de 2011-versie te vervangen voor de meest recente versie van de standaard. Naar aanleiding daarvan is een expertadvies opgesteld op basis van de intake en analyse van de documentatie over de standaard van ETSI. Tijdens de openbare consultatie van het expertadvies van 24 februari tot 25 maart 2017 zijn twee reacties ontvangen vanuit de provincie Friesland, namens het CIBO en vanuit DICTU.

Advies en gevraagd besluit

Gevraagd wordt om de oude versie van de standaard ETSI TS 102 176 te vervangen door de meest recente versie van de standaard, ETSI TS 119 312. Ook wordt er nu gewerkt aan een nieuwe versie van de standaard, deze wordt medio 2018 gepubliceerd en sluit o.a. beter aan op de Ades Baseline Profiles. Het advies is om de 119 312 versie bij te werken naar de nieuwe versie zodra deze wordt gepubliceerd.

Ad D. Rapport verduidelijking functionele toepassingsgebieden**[Bijlage D]****Over het onderzoek**

Over de omschrijvingen van het functioneel toepassingsgebied van de standaarden op de lijst met open standaarden en het organisatorisch werkingsgebied is altijd de nodige discussie, omdat deze omschrijvingen bepalend zijn voor de vraag of een (overheids)organisatie een standaard wel of niet moet hanteren. Ook na de opname van een standaard op de lijst ontvangt het Bureau Forum Standaardisatie regelmatig vragen over het functioneel toepassingsgebied dat hierbij wordt vermeld. Onduidelijkheid hierover kan dan ook de adoptie van een standaard in de weg staan en vage beschrijvingen moeten daarom ook vermeden worden

Gebruikers van de lijst, zoals bestuurders, architecten en inkopers van ICT, hebben aangegeven behoefte te hebben aan omschrijvingen van functioneel toepassingsgebieden die:

- duidelijk maken wanneer een standaard moet worden toegepast;
- uniform zijn aan de omschrijving van andere functioneel toepassingsgebieden;
- consistent zijn met andere afspraken;

Verder is voor een selecte set van standaarden het functioneel toepassingsgebied ook daadwerkelijk verduidelijkt. Het gaat dan niet om een inhoudelijke aanpassing, maar om het aanscherpen ten behoeve van de leesbaarheid.

Aanpak

Hoofdstuk 2 bevat een analyse van de omschrijvingen van de toepassingsgebieden van alle (in behandeling zijnde) standaarden. Er wordt ingegaan op de elementen waaruit de huidige omschrijvingen zijn opgebouwd en aangegeven welke van deze elementen wel of niet moeten worden toegepast. Op basis hiervan wordt een ideaaltypische syntactische structuur voorgesteld, die helpt bij het vaststellen van een toepassingsgebied voor nu en in de toekomst.

Hoofdstuk 3 bevat voor enkele geselecteerde standaarden een voorstel voor een nieuwe omschrijving. Hierbij is gebruik gemaakt van de syntax en rekening gehouden met verplichtingen of beleidskaders die specifiek van toepassing zijn op de betreffende standaarden en die van invloed zijn op de beschrijving van het toepassingsgebied. Welke verplichting en kaders dit zijn, daarop wordt dieper op ingegaan.

Hoofdstuk 4, ten slotte, bevat de verschillende scenario's die mogelijk zijn voor de vaststelling van de nieuwe omschrijvingen en een beknopt projectvoorstel voor vaststelling van de nieuwe omschrijvingen en vervolgonderzoek naar enkele resterende standaarden.

Vervolg

Aan het Forum wordt gevraagd om het advies te bespreken en in te stemmen met de ideaaltypische syntactische structuur en de gevolgen hiervan voor gebruikers van de lijst (par. 2.4) en met de vervolgaanpak (hoofdstuk 4) om te starten met het daadwerkelijk aanscherpen van de toepassingsgebieden van de geselecteerde standaarden. Verder wordt vanwege haar rol in de toetsingsprocedure, aan het Forum Standaardisatie aangeraden om kennis te nemen van de elementen waaruit de omschrijvingen kunnen zijn opgebouwd (par. 2.2) en het advies om deze elementen al dan niet te gebruiken (par. 2.3).

Ter kennisname

Ad E. Reactie evaluatie metadatering standaard OAI-PMH

Achtergrond en evaluatieadvies

In de Forumvergadering van 14 december j.l. is de evaluatie van de standaard OAI-PMH besproken.¹ Deze standaard staat sinds 2010 op de lijst met open standaarden en er was weinig inzicht in het gebruik van de standaard. De uitkomst van de evaluatie is dat het veld rond metadatering van repositories om informatie/documenten/collecties op eenduidige wijze te ontsluiten in beweging is. Opname van de standaard op de lijst heeft zijn succes gehad tot het onderwijs en cultuur domein, daar wordt de standaard breed gebruikt. Daarbuiten echter niet tot nauwelijks. Het advies was om Kennisnet (de oorspronkelijke indiener) duidelijk te laten maken of plaatsing op de lijst nog nodig is en of het toepassingsgebied aangepast dient te worden. In het Forum van december is gevraagd om voor 1 april 2017 te komen met een reactie.

Reactie

Vanuit Kennisnet is zowel per mail als via een afspraak op bovenstaande vraag gereageerd. Kennisnet kan zich vinden in het advies om de standaard te verplaatsen van de 'pas toe of leg uit'-lijst naar de aanbevolen lijst. Kennisnet evalueert zelf toepassing van gebruikte standaarden die zijn aanbevolen binnen het onderwijsveld. Werk van het Forum i.h.k.v. de ptolu-lijst is wat dat betreft dubbel werk. Het stimuleren van adoptie, wat een andere functie van de lijst is, is voor het onderwijsveld niet meer nodig. Verplichten via de lijst heeft dat betreft geen toegevoegde waarde.

Op de vraag of Kennisnet een heldere en SMART businesscase rond OAI-PMH binnen het onderwijsdomein kan opstellen waardoor duidelijk is wat de standaard doet binnen dit domein. Wordt aangegeven dat Kennisnet op de websites van [Edustandaard](#) en [Edurep](#) toont hoe OAI-PMH wordt ingezet en welke meerwaarde het biedt voor de onderwijssector.

Tot slot als reactie op de opmerking of Kennisnet een meer expliciete rol kan krijgen bij het monitoren van het gebruik van de standaard, mocht het Forum Standaardisatie hier onvoldoende middelen voor hebben. Geeft Kennisnet aan dat een grotere rol voor Kennisnet in het beheer van OAI-PMH buiten de onderwijssector niet passend is. Dit mede gezien de missie: 'Kennisnet laat ict werken voor het onderwijs'. Bredere adoptie buiten het onderwijsveld is geen direct belang voor Kennisnet. Wel biedt Kennisnet handleidingen en verwijzingen voor implementatie en gebruik van OAI-PMH in het onderwijsveld en vervuld daarmee een actieve 'beheer-rol'.

Vervolgstappen

Op basis van de evaluatie en bovenstaande reactie wordt geadviseerd om te starten met de procedure voor het verplaatsen van de standaard OAI-PMH op de lijst naar de status "aanbevolen" en dan met name voor gebruik binnen onderwijs- en cultuurdomein. Aangezien er al een evaluatie is uitgevoerd kan hier volstaan worden met een verkorte procedure zonder expertgroep.

Wel zal er een openbare consultatie moeten plaatsvinden waarbij naast stakeholders in het onderwijs en erfgoed domein, ook organisaties als DEN, de metadata harvesting

¹ <https://www.forumstandaardisatie.nl/sites/default/files/FS/2016/1214/FS-20161214.03A-Evaluatie-advies-OAI-PMH.pdf>

community van de basisregistraties, de gemeente archiefcommissie, het CBS, Kadaster en Waternet om input wordt gevraagd.

Ad F. Reactie evaluatie metadatering standaard OWMS [Bijlage F]

Achtergrond en evaluatieadvies

In de Forumvergadering van 14 december j.l. is de evaluatie van de standaard OWMS besproken.² Deze standaard staat sinds 2011 op de lijst en er stonden enkele aanvullende adviezen open. Verder was er onduidelijkheid over het toepassingsgebied. De uitkomst van de evaluatie is dat technologische veranderingen op het gebied van zoekmachine technologie en de introductie van functioneel rijkere en meer dynamische standaarden zoals schema.org de adoptie van OWMS onder druk zetten. Er zijn inmiddels op verschillende niveaus en domeinen alternatieve standaarden in gebruik. Het verplicht stellen van de standaard via 'pas toe of leg uit' werkt vooralsnog onvoldoende. Hierdoor heeft OWMS aan belang ingeboet. Het advies was om KOOP (de oorspronkelijke indiener) duidelijk te laten maken of plaatsing op de lijst nog nodig is. In het Forum van december is gevraagd om voor april 2017 te komen met een reactie.

Reactie

KOOP heeft binnen de gestelde termijn geantwoord op de vraag van het Forum. In de reactie wijst KOOP op een aantal concrete voorbeelden van het gebruik van OWMS bij de overheid. KOOP onderkent het bestaan van andere standaarden zoals het NL profiel van DCAT en schema.org, maar beargumenteert dat deze niet ongenueanceerd als concurrent van OWMS moeten worden afgeschilderd. Volgens KOOP biedt OWMS in combinatie met deze standaarden nog altijd meerwaarde.

Verder geeft KOOP aan een nieuwe versie van OWMS te gaan ontwikkelen, versie 5.0. Deze zal de meerwaarde van de standaard vergroten met een betere URI strategie en door sterker in te zetten op waardelijsten. Als beheerder van OWMS voorziet KOOP de bouw van een nieuwe beheer- en publicatieomgeving van standaarden.overheid.nl waarmee ze een beter contact met de belanghebbenden kunnen onderhouden. Zo zou de 'community' voor OWMS ook zichtbaarder worden.

Vervolgstappen

Het antwoord van KOOP geeft voldoende vertrouwen in de meerwaarde en de adoptie van OWMS om de standaard op de 'pas toe of leg uit' lijst te laten staan. We nemen daarom vooralsnog geen vervolgstappen.

² <https://www.forumstandaardisatie.nl/sites/default/files/FS/2016/1214/FS-20161214.03B-Evaluatie-advies-OWMS.pdf>