



notitie

Forum Standaardisatie

Wilhelmina v Pruisenweg 52
2595 AN Den Haag
Postbus 96810
2509 EJ Den Haag
www.forumstandaardisatie.nl

Forum Standaardisatie

Bijlagen:	A. Expertadvies adoptie-evaluatie SAML B. Notitie van eID over verwerking adviespunten C. Opzet monitor open standaarden-beleid 2014		
Aan:	Forum Standaardisatie		
Van:	Stuurgroep open standaarden		
Datum:	3 april 2014	Versie	1.0
Betreft:	Adoptie van open standaarden		

Doel

*U wordt gevraagd om **in te stemmen met:***

- 1) Adviespunten ter verdere bevordering adoptie SAML (authenticatie)

*U wordt gevraagd **kennis te nemen van:***

- 2) Documentatie eID en advisering door Forum
- 3) Opzet monitor open standaarden-beleid 2014
- 4) Adoptie-aanpak 2014 incl. actiepunten
- 5) Verantwoording in jaarverslagen, o.a. Logius
- 6) Phishing-mails in naam van overheid en DKIM (e-mailauthenticatie)
- 7) Voortgang adoptie (overig)
 - a. Opvolging advies ISO27001/2
 - b. Platform Internetstandaarden
 - c. Handreiking "Web of app?"
 - d. Taart voor inkoop-toppers
 - e. Activiteiten gericht op inkoopers

Ter Besluitvorming

Ad 1. Adviespunten ter verdere bevordering adoptie SAML (authenticatie) [bijlage A]

Het Forum Standaardisatie wordt gevraagd in te stemmen met de tien adviespunten die uit het expertonderzoek naar voren zijn gekomen (par. 5.2 bijlage A) om de interoperabiliteit en het implementatiegemak van SAML verder te vergroten.

Toelichting

Het Forum heeft in zijn vergadering van 29 oktober 2013 besloten om de adoptie van SAML versie 2.0 formeel te evalueren en te bezien of aanvullende adoptie-maatregelen nodig zijn. Deze standaard is sinds 2009 opgenomen op de lijst met open standaarden voor 'pas toe of leg uit' met als functioneel toepassingsgebied "federatieve (web)browser-based single-sign-on (SSO) en single-sign-off".

Het bijgaande adoptie-expertadvies geeft invulling aan het besluit van het Forum. Het advies is tot stand gekomen op basis van deskresearch en interviews met diverse experts.

Het advies bevat 10 adviespunten om de adoptie van SAML verder te bevorderen en met name om de interoperabiliteit en het implementatiegemak te vergroten. Daarin komt naar voren dat het belangrijk is dat de Nederlandse overheid stuurt op een uniforme implementatie van SAML die aansluit bij wat in de markt gangbaar is. De beoogde uniformiteit kan worden bereikt door sluitende afspraken te maken over één SAML deployment profiel voor dienstverleners in de Nederlandse (semi-)publieke sector te maken.

Het is cruciaal om bij de ontwikkeling van dit profiel uit te gaan van de SAML-standaard (incl. errata) en van industry best practices, met name het Kantara interoperabiliteitsprofiel. Bovendien is het van belang om stakeholders (leveranciers, overheidsorganisaties en standaardisatie-experts) actief te betrekken bij de ontwikkeling van het profiel. Om te leren en om eigen kennis in te brengen zou de Nederlandse overheid moeten participeren in de eGovernment Work Group bij Kantara Initiative en in standaardisatie-organisatie OASIS. Bij het oppakken van de adviespunten speelt het Nederlandse eID-project een belangrijke rol.

Ter informatie

Ad 2. Documentatie eID en advisering door Forum [bijlage B]

eID heeft een nieuwe versie van het document "Ontwerp op hoofdlijnen van de werking van het eID Stelsel NL" gepubliceerd. Daarin is het advies dat het Forum eerder heeft gegeven verwerkt.¹ In de bijlage komt terug hoe eID is omgegaan met de adviespunten van het Forum.

eID heeft ook eerste versies van de op SAML gebaseerde koppelvlakspecificaties gepubliceerd. Met eID is afgesproken dat deze specificaties in het voorjaar aan gerenommeerde (interationale) SAML-experts zullen worden voorgelegd.

¹ Zie Forum-notitie, <https://www.forumstandaardisatie.nl/sites/default/files/FS/2013/0903/FS-20130903.07C-20130822-Notitie-reactie-eID-v09.pdf>

Ad 3. Opzet monitor open standaarden-beleid 2014 [bijlage C]

In de bijlage zijn de hoofdlijnen voor de opzet van de monitor open standaarden-beleid over 2013 opgenomen. Ook dit jaar zal ICTU de monitor uitvoeren. De opzet is grotendeels gelijk aan die van vorig jaar. Over de opzet heeft afstemming plaatsgevonden met DGOBR/BZK. De rapportage zal in november 2014 in het College Standaardisatie aan bod komen. Daarnaast zal de rapportage door EZ worden gebruikt om aan de Tweede Kamer te rapporteren over de voortgang.

Ad 4. Adoptie-aanpak 2014 incl. actiepunt

In het werkplan 2014 komt de adoptie-aanpak voor 2014 terug. De komende Forum-vergadering zal een update worden gegeven over de voortgang. Daarbij zal ook aandacht zijn voor hoe wordt omgegaan met de adoptie-drempels ('bottlenecks') zoals die door Jaap Korpel (ICTU) tijdens de Forum-vergadering in december 2013 werden gepresenteerd.

Aan het College zal een korte update worden gegeven over de voortgang rondom adoptie. In samenwerking met ICCIO zal daartoe in ieder geval op een rij worden gezet wat de voortgang is ten aanzien van de afspraken die zijn gemaakt in de brief d.d. 18 juni 2013 over samenwerking tussen ICCIO en College Standaardisatie.²

Ad 5. Verantwoording in jaarverslagen, o.a. Logius

Van verschillende organisaties (o.a. de ministeries Fin, BZK en EZ) is bekend dat zij werken aan de verantwoording over open standaarden in het jaarverslag. BZK heeft aangegeven volgend jaar i.s.m. de Haagse Inkoop Samenwerking hier nog meer grip op krijgen.

Logius heeft in het onlangs gepubliceerde jaarverslag over 2013 een hoofdstuk over standaardisatie opgenomen. Het bevat ook de verantwoording over de toepassing van open standaarden binnen Logius-producten. Zie:

<http://publicaties.logius.nl/nl/magazine/6604/749529/standaardisatie.html>

Ad 6. Phishing-mails in naam van overheid en DKIM (e-mailauthenticatie)

De afgelopen periode zijn er door internetcriminelen diverse phishingmails verstuurd uit naam van de overheid. Het ging o.a. om mails waarbij de domeinnaam van de Belastingdienst en van het ministerie van Buitenlandse Zaken werden misbruikt. De 'pas toe of leg uit'-standaard DKIM helpt tegen dit soort misbruik doordat het een mail met een digitale handtekening koppelt aan een domeinnaam.

Met betrokkenen is hierover door Bureau Forum Standaardisatie contact gezocht. Bij het Bureau is bekend dat in ieder geval de Belastingdienst, MinV&J, DigiD en MijnOverheid ondertussen bezig om DKIM en aanverwante open standaarden voor e-mailauthenticatie (DMARC en SPF) te implementeren. Bovendien is MinAZ/Rijksoverheid.nl voor zijn nieuwsbrieven al vergevorderd qua implementatie.

² Zie bijlage bij Forum-notitie FS 44-05-04B ,
<https://www.forumstandaardisatie.nl/sites/default/files/FS/2013/0618/FS-20130618.04B-Notitie-voortgang-open-standaarden-+-brief-ICCIO.pdf>

Vanuit Bureau Forum Standaardisatie is daarnaast bijgedragen aan een artikel op ISPToday over het onderwerp met als titel "Nederlandse adoptie e-mailauthenticatie onvoldoende". Zie:

<http://www.isptoday.nl/nieuws/nederlandse-adoptie-e-mailauthenticatie-onvoldoende/>

Ad 7. Voortgang adoptie (overig)

a. Opvolging advies ISO27001/2

Van BZK is informatie ontvangen over de afkoopregeling die het Rijk heeft getroffen met NEN. Op basis hiervan zal de 'fact finding' worden afgerond en zal het gesprek met NEN worden aangegaan over overheidsbrede afkoop.

b. Platform Internetstandaarden

Op 20 februari heeft een eerste bijeenkomst plaatsgevonden over het op te richten Platform Internetstandaarden. Bij de bijeenkomst waren vertegenwoordigers van SIDN, ISOC, SURFnet, RIPE NCC, NLnet Labs en de Cyber Security Raad aanwezig. De organisatie was in handen van EZ en BFS. De uitkomst was dat samenwerking op het vlak van adoptie zeker kan lonen. Gezocht moet worden naar een samenwerkingsvorm die ertoe leidt dat partijen die geen insider zijn en wel impact kunnen hebben, aan de slag gaan met de nieuwe generatie internetstandaarden. SIDN, ISOC, EZ en BFS zullen een voorstel uitwerken voor de samenwerkingsvorm.

c. Handreiking "Web of app?"

Ondertussen heeft de onderzoeker verschillende gesprekken gevoerd o.a. met experts van de Belastingdienst, DUO, DICTU en Logius. Daarbij is duidelijk naar voren gekomen dat de handreiking in een behoefte gaat voorzien. Veel organisaties worstelen namelijk met de vraag wat de toegevoegde waarde is van een app in plaats van of naast een website. In het onderzoek wordt o.a. gekeken naar verschillen qua interoperabiliteit, toegankelijkheid en duurzaamheid. Eerste resultaten van het onderzoek zullen worden gepresenteerd tijdens een sessie op de aanstaande beurs "ICT & Overheid". Het definitieve rapport zal de eerstvolgende Forum-vergadering op de agenda staan.

d. Taart voor inkoop-toppers

In aansluiting op de monitor, die eind vorig jaar is behandeld in het College Standaardisatie, zijn onlangs felicitaties uitgedeeld aan verschillende ministeries, gemeenten en een provincie voor het uitvragen van relevante open standaarden in aanbestedingen. Aanbestedingen van de ministeries van Algemene Zaken en Veiligheid en Justitie, de provincie Gelderland, Bureau Inkoop en Aanbestedingen Zuid-Oost Brabant en de gemeenten Dordrecht en Steenwijkerland vielen in de prijzen met een ICT-aanbesteding waarin de relevante open standaarden werden uitgevraagd. De inkoopafdelingen van deze organisaties zijn beloond met een taart voor hun prima prestatie.

Naast bovengenoemde goede voorbeelden, komt in de monitor -zoals bekend voor het Forum- naar voren dat er ruimte is voor verbetering. In het nieuwsbericht hierover is hiervoor ook aandacht en wordt eveneens

gemeld dat Forum Standaardisatie in samenwerking met andere partijen (ICCIO, KING en PIANOo) werkt aan verbetering.

e. *Activiteiten gericht op inkopers*

- Op 14 april levert Bureau Forum Standaardisatie een bijdrage aan de workshop-cyclus 'Inkopen en aanbesteden ICT' van de Rijksacademie.
- Er is een eerste rondgang gemaakt met een voorproef van de bestekteksten. Daarbij is de gekozen aanpak om op basis van in de praktijk veelvoorkomende aanbestedingen te werken vooralsnog in goede aarde gevallen. Deze aanpak sluit eveneens goeddeels aan bij het category management zoals dat voor de Rijksoverheid is ingevoerd. De vervolgstappen zijn nu om de ontvangen terugkoppeling op de twee reeds uitgewerkte veelvoorkomende aanbestedingen (websites en webapplicaties) te verwerken en in een verificatiesessie met een groep experts bestaande uit zowel ICT-architecten als ICT-inkopers aan een laatste toets te onderwerpen. Op basis daarvan zullen de bestekteksten aan Forum en College Standaardisatie en het ICCIO worden voorgelegd.