FS-20140617.04

notitie

Forum Standaardisatie

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

FORUM STANDAARDISATIE

Bijlagen:	A. Praktische handreiking open standaarden bij inkoop B. Review "ICT-beveiligingsrichtlijnen voor webapplicaties" van NCSC		
Aan:	Forum Standaardisatie		
Van:	Stuurgroep open standaarden		
Datum:	4 juni 2014	**Versie**	1.0
Betreft:	Adoptie van open standaarden		

Bijlage
A
Praktische handreiking open standaarden bij inkoop

B
Review "ICT-beveiligingsrichtlijnen voor webapplicaties" van NCSC

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

1. Praktische handreiking open standaarden bij inkoop (ook wel: specifieke bestekteksten) [bijlage A].

*U wordt gevraagd om **te bespreken:***

2. Opvolging onderzoek bottlenecks en best practices;
3. Betekenis adoptie-advies SAML voor voorzieningen buiten eID [Erwin Bleumink].

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

4. Review van concept nieuwe versie "ICT-beveiligingsrichtlijnen voor webapplicaties" van NCSC [bijlage B];
5. IPv6 Nummerplan Nederlandse Overheid [Guus Bronkhorst];
6. Voortgang samenwerking adoptie ICCIO en College Standaardisatie [Wim Sijstermans];
7. Voortgang adoptie (overig):
    a. Status afkoop ISO27001/27002;
    b. Onderzoek naar adoptie&samenhang eFactuur-standaarden;
    c. Adoptie DKIM (phishing-preventie);
    d. Handreiking “Web of app?”.

Korte toelichting per punt

Ad 1. Praktische handreiking open standaarden bij inkoop (ook wel: specifieke bestekteksten) [bijlage A]

Het Forum Standaardisatie wordt gevraagd in te stemmen met:
1. de "Praktische handreiking open standaarden bij inkoop" te laten vaststellen door College Standaardisatie onder voorbehoud van een positieve juridische toets door de interdepartementale Commissie Bedrijfsjuridisch Advies (CBA);
2. het verzoek aan het Rijk (ICCIO en ICCIA), Manifestgroep, IPO, UvW en KING om de handreiking vervolgens i.s.m. BFS onder de aandacht te brengen van hun achterban en ervaringen terug te geven aan het Forum Standaardisatie;
3. het ingaan op het aanbod van PIANOo en NORA om de handreiking onder de aandacht te brengen van respectievelijk inkopers en architecten.

Naar aanleiding van de resultaten van de monitor over 2011 en 2012 heeft er in het vierde kwartaal van 2013 een rondgang plaatsgevonden langs een aantal actoren in het inkoopveld. Op basis daarvan zijn de reeds eerder door het Forum Standaardisatie vastgestelde "Generieke bestekteksten voor verplichte ICT-standaarden" toegepast op een aantal veelvoorkomende aanbestedingen.

Als resultaat hiervan is de "Praktische handreiking open standaarden bij inkoop" ontstaan. Daarin zijn voor een aantal veelvoorkomende aanbestedingen voorbeeld-bestekteksten opgenomen. In de huidige versie is met name aandacht voor websites en webapplicaties.

Dit document is in een aantal revisieslagen met een steeds bredere kring van inkopers, IT-architecten en aanbestedingsjuristen gedeeld. Hiervoor zijn bijdragen geleverd vanuit DUO, V+J, PIANOo, BZK/DGOBR, BZK/BPR, ICTU, AZ/DPC, KING, Logius en de HIS. In de versie zoals bijgevoegd is de terugkoppeling op eerdere versies zoals ontvangen vanuit de diverse disciplines verwerkt.

Net als de generieke bestekteksten is het voorstel om het document te laten vaststellen door het College Standaardisatie. Vanuit juridische hoek is gesignaleerd dat het wenselijk is om dit stuk in ieder geval aan de interdepartementale Commissie Bedrijfsjuridisch Advies (CBA) voor te leggen voor een juridische toets.

Het is van belang dat inkopers het stuk kennen. Het voorstel is om het stuk, na vaststelling door College en toetsing door CBA, via de koepels en de Manifestgroep verder te verspreiden.

PIANOo heeft reeds aangegeven bij te dragen aan de verdere communicatie onder inkopers, bijvoorbeeld via een symposium en/of opname in het programma van het eerstvolgende PIANOo-congres. Vanuit de beheerders van de NORA is aangegeven dat men delen van de inhoud in de NORA wenst op te nemen en onder architecten wil verspreiden.

Ad 2. Opvolging onderzoek bottlenecks en best practices

Het Forum wordt gevraagd van de status kennis te nemen, de lopende acties te onderschrijven en om eventuele aanvullende suggesties te geven.

In december 2013 presenteerde Jaap Korpel van ICTU in het Forum Standaardisatie over bottlenecks en best practices bij de adoptie van open standaarden. Zijn bevindingen waren gebaseerd op het door hem uitgevoerde monitor-onderzoek en een aantal aanvullende interviewgesprekken met belanghebbenden. Zijn presentatie eindigde met een aantal mogelijke acties.

Daarin kwam naar voren dat draagvlak voor het openstandaarden-beleid en bekendheid van de 'pas toe of leg uit'-lijst niet het probleem zijn. Onder andere de complexe werkelijkheid (o.a. legacy, migratiepaden), onduidelijke verantwoordelijkheidsverdeling en moeite met inschatting relevantie van een standaard kwamen als drempels naar voren. De presentatie eindigde met een aantal concrete suggesties die in de interviewgesprekken naar voren kwamen. BFS heeft deze opgepakt, al dan niet in samenwerking met andere partijen. Hieronder volgt een korte status-update.

#	Suggestie	Status
1	V&J heeft een model aanbestedings-document, met verwijzing naar de lijst op de BFS-website.	BFS heeft nu specifieke bestekteksten ontwikkeld in aanvulling op de bestaande generieke bestekteksten. I.s.m. de koepels en PIANOo moeten deze de inkopers bereiken.
2	Borgen via interne processen, instructies, sjablonen e.d.	BZK/DGOBR laat in verschillende basisdocumenten zoals PSA ook open standaarden terugkomen. Met DGOBR, CIO-office BZK en HIS is een gesprek gevoerd over het proces binnen het BZK-domein en zijn afspraken gemaakt. Gesprekken met andere ministeries volgen.
3	Als er een semantische wiki over de open standaarden zou zijn, dan kan die worden gekoppeld aan de NORA-wiki.	Met NORA loopt hierover contact. Bij de aanstaande herziening van de Forum-website wordt hiermee rekening gehouden.
4	Organiseer bij elk departement een sessie met inkopers en ICT-specialisten, met experts van ICCIO en BFS. We kunnen dan naderhand een nota opstellen hoe om te gaan met open standaarden.	Met BZK/DGOBR is afgesproken om een aantal resultaten van de monitor van dit jaar te bespreken met individuele ministeries.

5	Logius: compliance van voorzieningen op website.	Logius heeft dit jaar opnieuw een uitgebreid overzicht gegeven van de standaarden in zijn voorzieningen. Deze best practice is gedeeld met verschillende andere partijen, zoals DGOBR en ICTU.
6	Ik zou aanbestedingen wel willen laten toetsen door BFS (als dat snel kan). En/of vooraf DGOBR laten adviseren.	Regelmatig ontvangt BFS adviesvragen via de mailbox. BFS heeft bij een aantal grote trajecten advies gegeven (zoals ON2013, eID). Met Logius zijn afspraken gemaakt over advisering. Daarnaast zijn i.s.m. DGOBR afspraken gemaakt over advisering in aanbestedingstrajecten met CIO-office BZK en HIS. Bereikbaarheidsgegevens van BFS (mail en telefoon) zullen o.a. via koepels breder bekend worden gemaakt.

Ad 3. Betekenis adoptie-advies SAML voor voorzieningen buiten eID [Erwin Bleumink]

Het Forum wordt gevraagd kennis te nemen van de onderstaande vervolgacties en daar eventueel aanvullende suggesties voor te doen.

1. BFS, SURFnet en Logius (DigiD en eHerkenning) gaan gezamenlijk na wat de betekenis is van de bevindingen uit het adoptie-advies voor SAML voor (bestaande) voorzieningen buiten het eID Stelsel.
2. Het resultaat hiervan zal in de vorm van een aantal additionele adviespunten worden voorgelegd aan het Forum Standaardisatie.

Afgelopen vergadering heeft het Forum Standaardisatie het adoptie-advies voor SAML aangenomen, in het bijzijn van Hans-Rob de Reus van het programma eID. Daarbij maakte Erwin Bleumink (Algemeen directeur SURFnet, Forum-lid) de kanttekening dat de bevindingen weliswaar duidelijk en herkenbaar zijn, maar dat de (op zichzelf terechte) adviezen erg gericht zijn op het eID Stelsel. De SAML-standaard wordt ook buiten het eID Stelsel gebruikt, bijv. in het onderwijsdomein en in organisatie-interne voorzieningen, en dat zal zo blijven. Bovendien is het eID Stelsel weliswaar een belangrijke veelbelovende ontwikkeling, maar nog niet werkend in de praktijk.

Om op korte termijn ook adoptiewinst voor SAML te behalen is het van belang om de betekenis van de bevindingen te duiden voor bestaande voorzieningen (zoals SURFconext, DigiD en eHerkenning) en ook te bekijken hoe de barrières aan de leverancierszijde kunnen worden doorbroken. Zoals afgesproken, heeft BFS hierover nader contact gehad met Erwin Bleumink. Dat heeft geresulteerd in het bovenstaande voorstel voor vervolgacties.

Ad 4. Review van concept nieuwe versie "ICT-beveiligingsrichtlijnen voor webapplicaties" van NCSC [bijlage B]
Het Nationaal Cyber Security Centrum (NCSC) heeft aan het Bureau Forum Standaardisatie (BFS) gevraagd om een review uit te voeren van de nieuwe concept-versie van de "Beveiligingsrichtlijnen voor Webapplicaties" (hierna: "NCSC-richtlijnen"). Een gedeelte van de huidige versie van de richtlijnen wordt gebruikt voor de DigiD-beveiligingsassessments.

De scope van de reactie omvat het werkdomein van Forum Standaardisatie, namelijk standaarden en interoperabiliteit. Aan deze notitie hebben Marco Davids (SIDN), Lancelot Schellevis en Bart Knubben (BFS) bijgedragen. De notitie bevat het resultaat van de review.

Hoofdpunten uit de review zijn:

- De richtlijnen zijn nuttig, lezen plezierig maar zijn wel omvangrijk. Praktische toepasbaarheid is een aandachtspunt;
- De richtlijnen hebben zelf niet het karakter van een standaard en komen daarmee niet in aanmerking voor opname op de 'pas toe of leg uit'-lijst. Wel zouden Forum/College wellicht op andere wijze status kunnen verlenen aan de richtlijnen;
- In de richtlijnen wordt gewezen op het belang van standaarden voor informatiebeveiliging;
- De relatie tot ISO27001/27002 komt wel aan bod, maar de relatie met de Baselines Informatiebeveiliging van de overheid niet;
- Verschillende maar niet alle relevante 'pas toe of leg uit'- en gangbare standaarden worden in de handreiking genoemd. Voor de ontbrekende standaarden zou ook aandacht moeten zijn.

De review is inmiddels gedeeld met NCSC. Zij verwachten de nieuwe versie in oktober 2014 te publiceren.

Ad 5. IPv6 Nummerplan Nederlandse Overheid [Guus Bronkhorst]
De afgelopen weken is met verschillende partners gewerkt aan een nadere uitwerking van het onderzoeksplan IPv6 Nummerplan Nederlandse Overheid. De hoofdvraag is in hoeverre en onder welke voorwaarden een IPv6 Nummerplan Nederlandse Overheid kan leiden tot meer control, meer autonomie van overheden en kansen voor leveranciersonafhankelijkheid, informatieveiligheid en financieel voordeel, rekeninghoudend met het organisatorische en bestuurlijke landschap. Een begeleidings- en leescommissie bestaande uit vertegenwoordigers van onder andere de koepelorganisaties en overheden en experts zullen toezien op een goede uitvoering van het onderzoek.

De notitie IPv6 Nummerplan Nederlandse Overheid waar het onderzoek in wordt aangekondigd wordt op 11 juni in het DB-BRG besproken en op 25 juni in de BRG. Dit betreft een principeakkoord waarmee de weg wordt vrijmaakt om op basis van een gedegen analyse definitieve besluitvorming te laten plaatsvinden.

Ad 6. Voortgang samenwerking adoptie ICCIO en College Standaardisatie [Wim Sijstermans]
Binnen ICCIO-verband wordt gewerkt aan een notitie over de voortgang ten aanzien van de afspraken die zijn gemaakt in de brief d.d. 18 juni 2013 tussen ICCIO en College Standaardisatie.[1] Deze afspraken zijn er op gericht om de adoptie van open standaarden binnen het Rijk te bevorderen.

[1] *Zie bijlage bij Forum-notitie , https://www.forumstandaardisatie.nl/sites/default/files/FS/2013/0618/FS-20130618.04B-Notitie-voortgang-open-standaarden-+-brief-ICCIO.pdf*

De voortgangsnotitie van ICCIO zal op 4 september op de agenda van het College staan. Deze zal ook aan bod komen in een volgende Forum-vergadering.

Ad 7. Voortgang adoptie (overig)

a. Status afkoop ISO27001/27002

Met BZK/BenI en EZ is het te voeren gesprek met NEN voorbesproken. BFS zet een en ander op een rij en gaat hierover met NEN het gesprek aan.

b. Onderzoek naar adoptie&samenhang eFactuur-standaarden

Het onderzoek gaat binnenkort met lichte vertraging van start. Oorzaak van vertraging is dat binnen de mantel geen geschikte partij is gevonden en de offerte-aanvraag vervolgens aan andere partijen verstuurd.

c. Adoptie DKIM (phishing-preventie)

Achtereenvolgens hebben de Rijksoverheid.nl, Belastingdienst, MijnOverheid, gemeente Den Bosch en Pleio deze standaard van de 'pas toe of leg uit'-lijst geïmplementeerd. Naar aanleiding van een recente phishing-incident is ook CJIB er mee bezig. De standaard staat ook op de ontwikkelkalender van DigiD.

d. Handreiking "Web of app?"

De oplevering van de handreiking heeft lichte vertraging opgelopen. Met name doordat er meer partijen zijn geïnterviewd en meer documentatie is gebruikt, dan aanvankelijk was voorzien. Ook willen we omwille van de kwaliteit en gedragenheid een consultatie doen van het concept. De handreiking zal nu de volgende Forum-vergadering op de agenda staan.