notitie

FORUM STANDAARDISATIE 22 april 2015
Agendapunt 2. Open standaarden, lijsten
Stuknummer 2. Oplegnotitie lijsten

Bijlagen:	A. Forumadvies DMARC en SPF B. Forumadvies SKOS C. Forumadvies nieuwe versie ISO27001/2
Aan:	Forum Standaardisatie
Van:	Stuurgroep open standaarden

*U wordt gevraagd **in de stemmen** met de volgende Forumadviezen:*

1. Advies over de opname van **DMARC en SPF**, standaarden voor e-mailbeveiliging.
2. Advies over de opname van **SKOS**, standaard voor het delen en linken van thesauri en begrippenwoordenboeken.
3. Advies over de opname van de nieuwe versie van **NEN-ISO/IEC 27001 en 27002**, een standaard voor informatiebeveiliging.

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

4. Voortgang van de procedure voor de nieuwe versie van **Digikoppeling** (een standaard voor berichtenuitwisseling).
5. **Nieuwe versie** van de toetsingscriteria.
6. Relatie tussen het dossier **internationaal en lijsten**. Zie hiervoor ook de stukken bij internationaal.
7. Nieuwe versie van de uitstekend beheer standaard **SIKB0101** (*bodemkwaliteit*)

Ter besluitvorming

Ad 1. Advies over de opname van DMARC en SPF
(Bijlage A. Forumadvies DMARC en SPF)

Het Forum Standaardisatie wordt gevraagd om in te stemmen met onderstaande advies.

Het Forum Standaardisatie adviseert het Nationaal Beraad Digitale Overheid om:

1. in te stemmen met de opname van DMARC op de 'pas toe of leg uit'-lijst onder voorwaarde dat het beheer van DMARC is geformaliseerd door IETF of een andere, gelijkwaardige, standaardisatieorganisatie.

2. in te stemmen met de opname van SPF op de 'pas toe of leg uit'-lijst.

   Voorwaarde voor het SPF advies is dat uit de controle op de toetsingscriteria geen aandachtspunten naar voren komen. Dit moet duidelijk zijn voor 29 april 2015 zodat het geen openstaand punt is op het moment dat het besluit voorligt in het Nationaal Beraad.

Zodra het Forum Standaardisatie vaststelt dat aan bovenstaande punten is voldaan kunnen de standaarden op de lijst worden opgenomen.

3. Verder wordt aan het Nationaal Beraad gevraagd in te stemmen met de Additionele adviezen ten aanzien van de adoptie van DMARC en SPF. Deze additionele adviezen zijn opgenomen in het bijgevoegde Forumadvies.

Over de standaarden
DMARC is een open standaard die het mogelijk maakt om beleid in te stellen over de manier waarop ontvangende e-mailproviders, die DMARC ondersteunen, om zouden moeten gaan met e-mail waarvan niet kan worden vastgesteld dat deze afkomstig is van het vermelde afzenderdomein. Het doel van DMARC is om, in combinatie met DKIM en/of SPF, misbruik van de domeinnaam middels e-mail te verminderen en/of te voorkomen. Daarnaast kan met DMARC worden voorkomen dat e-mailmailingen door ontvangende e-mailproviders onterecht voor spam worden aangezien.

DMARC maakt gebruik van SPF en DKIM. SPF controleert of de mailserver die een e-mail wil versturen namens het e-maildomein e-mail mag verzenden. DKIM koppelt een e-mail aan een domeinnaam met behulp van een digitale handtekening. DMARC gebruikt DKIM en SPF om de authenticiteit van een e-mail te verifiëren. Wanneer deze verificatie niet mogelijk is wordt het DMARC-beleid in werking gezet.

Geadviseerd wordt om zowel DMARC als SPF op te nemen zodat samen met DKIM de adoptie van een complete set van e-mailbeveiligingsstandaarden wordt bevorderd.

Betrokkenen en Proces
DMARC is ingediend door Measuremail met steun vanuit de gemeente Den Bosch en de gemeente Heerlen. Vervolgens hebben een intake en experttoetsing plaatsgevonden. De uitkomst van de expertgroep was om naast DMARC ook SPF op de lijst op te

nemen, onder voorwaarde dat de standaard voldoet aan de toetsingscriteria. Vervolgens heeft voor zowel DMARC als SPF een openbare consultatie plaatsgevonden.

Het expertadvies is gepubliceerd ten behoeve van de openbare consultatie. Tijdens de consultatie zijn er 11 reacties en vragen ontvangen. Het waren overwegend aanvullingen op het expertadvies en positief over opname van DMARC en SPF. Wel is het advies om voor SPF een aanvullende check uit te voeren op basis van de toetsingscriteria. De reacties zijn in overleg met de betrokken partijen verwerkt in dit forumadvies.

Consequenties en vervolgstappen
DMARC is nog niet in beheer genomen bij IETF. De standaard zelf is stabiel en de beheerprocedures zijn geheel afgestemd op IETF. De conclusie uit de expertgroep is om DMARC op te nemen op de 'pas toe of leg uit'-lijst onder voorwaarde dat DMARC minimaal een proposed standard is en wordt beheerd door IETF. Op dit moment is een werkgroep van IETF bezig om, conform de standaardisatieprocedure van IETF, de specificaties van DMARC op te stellen. De verwachting is dat deze specificaties in het derde kwartaal van 2015 definitief zijn en dat de standaard als gevolg hiervan in beheer wordt genomen door IETF.

SPF heeft een positief advies vanuit zowel de expertgroep als de openbare consultatie. SPF is niet vooraf apart getoetst aan de toetsingscriteria van het Forum omdat alleen DMARC is ingediend voor de toetsing. Om 'verrassingen' te voorkomen is een voorwaarde voor opname dat SPF nog apart getoetst wordt tegen de criteria van het Forum. Als SPF voldoet aan de criteria kan de standaard worden opgenomen op de 'pas toe of leg uit'-lijst. Deze toets vindt momenteel plaats en is eind april afgerond zodat het geen openstaand punt is op het moment dat het besluit voorligt in het Nationaal Beraad.

Tot slot kan het DMARC-beleid dat een organisatie kiest impact hebben het uitwisselen van privacy gevoelige gegevens. Het advies is om bij de invulling van DMARC-beleid een Privacy Impact Assessment (PIA) uit te voeren om te kunnen bepalen of er privacyrisico's zijn en of deze acceptabel zijn. Overheidsorganisaties kunnen hierbij gebruik maken van het Toetsmodel Privacy Impact Assessment (PIA) Rijksdienst .

Toepassingsgebied
Het advies is om de standaarden op te nemen voor het volgende toepassingsgebied:
DMARC: *Het instellen van beleid voor alle domeinnamen, waarvan de overheid de houder is, om betrouwbare e-mailcommunicatie met burgers, bedrijven en (semi)overheidsorganisaties te bevorderen, alsmede de bescherming van de overheid zelf tegen e-mail van ongeauthenticeerde afzenders te bevorderen.*

SPF: *Het controleren of een e-mailserver gerechtigd is om namens een domeinnaam e-mail te mogen verzenden.*

Ad 2. Advies over de opname van SKOS
(Bijlage B. Forumadvies SKOS)

Het Forum Standaardisatie wordt gevraagd om in te stemmen met onderstaande advies.

Het Forum Standaardisatie adviseert het Nationaal Beraad Digitale Overheid om SKOS, een standaard voor het online delen en linken van systemen voor kennisrepresentaties via het internet (zoals thesauri, begrippenwoordenboeken en classificatielijsten), op de lijst op te nemen 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 bijgevoegde Forumadvies.

Het publiceren van thesauri en taxonomieën (dit zijn begrippenlijsten of digitale gegevenswoordenboeken) door overheidsorganisaties gebeurt vaak in een vorm van documenten die niet bruikbaar zijn voor computerprogramma's. Thesauri of taxonomieën worden ook wel Knowledge Organization Systems (KOS) genoemd. SKOS zorgt ervoor dat een KOS bruikbaar is voor computerprogramma's (machine readable) en dat begrippen uitgewisseld kunnen worden tussen computerprogramma's onderling.

Hierbij kan in eerste instantie worden gedacht aan functionaliteiten in Content Management Systemen (CMS) en bibliotheeksystemen. Ook kan een SKOS gedeeld worden op het Web. Door het toepassen van de standaard worden de (familie)relaties tussen de verschillende definities van begrippen inzichtelijk en is data uit verschillende systemen beter te interpreteren en te vergelijken. Dit zorgt voor tijdswinst omdat relevante informatie sneller gevonden kan worden en geeft inzicht in de samenhang en (in)consistentie van begrippen (en bijbehorende definities). Daarmee kan de standaard meer waarde geven aan (overheids)informatie. SKOS is een van de linked data standaarden en vanuit de overheid (KOOP) wordt er ook een Linked Data adoptiestrategie ontwikkeld. Deze strategie is in lijn met het opname van SKOS op de 'pas toe of leg uit'-lijst.

Proces
De standaard is in eerste instantie aangemeld door het Platform Linked Data Nederland. Vervolgens heeft er een intakegesprek, experttoets en openbare consultatie plaatsgevonden. Naar aanleiding van de intake is besloten om SKOS in behandeling te nemen. Aan de experttoets hebben (toekomstige) eindgebruikers, leveranciers, adviseurs en andere kennishebbers deelgenomen. De conclusie uit de expertgroep is om SKOS met de status 'pas toe of leg uit' op te nemen op de lijst.

Het expertadvies is gepubliceerd ten behoeve van een openbare consultatie waarop 7 reacties zijn binnengekomen. Alle partijen hebben positief reageert op het expertadvies en onderschrijven het belang van het beter ontsluiten van Knowledge Organization Systems. Naar aanleiding van de openbare consultatie zijn nog wel een aantal aandachtspunten naar voren gekomen. Deze reacties zijn in overleg met de betrokken partijen verwerkt in het forumadvies.

Consequentie en vervolgstappen
Publieke organisaties die een KOS publiek beschikbaar stellen zullen deze KOS op basis van het 'pas toe of leg uit' principe ook moeten gaan aanbieden via SKOS. Verder zijn er geen specifieke beveiligingsrisico's of privacyrisico's. Tot slot zijn er enkele adviezen om de adoptie van de standaard te bevorderen, na opname van de standaard zal

hieraan uitvoering gegeven moeten worden.

Toepassingsgebied
Het advies is om SKOS op te nemen voor het volgende toepassingsgebied:

Het in een gestructureerde vorm op het Web publiek beschikbaar stellen van een 'niet geformaliseerd' Knowledge Organization System (KOS), met als doel kennis over de betekenissen en samenhang van de onderliggende begrippen te ordenen en toegankelijk te maken.

Ad 3. Advies over de opname nieuwe versies van NEN-ISO/IEC 27001 en 27002 (Bijlage C: Forumadvies NEN-ISO/IEC 27001 en 27002)

Het Forum Standaardisatie wordt gevraagd om in te stemmen met onderstaande advies.

Het Forum Standaardisatie adviseert het Nationaal Beraad Digitale Overheid om de huidige versies van de NEN-ISO/IEC 27001 en 27002 standaarden voor informatiebeveiliging op de 'pas toe of leg uit'-lijst te updaten naar de nieuwe 2013 versie.

Daarnaast is het advies om in te stemmen met de additionele adoptieadviezen zoals benoemd in bijgevoegde Forumadvies.

Vanuit de Stuurgroep open standaarden
De expertgroep geeft aan dat het beheer voor de standaard goed is geregeld en dat het predicaat 'uitstekend beheerproces' toegekend kan worden. Het advies vanuit de stuurgroep open standaarden is echter om deze status niet toe te kennen. Dit vanwege de kosten voor het aanschaffen van de standaard en de mogelijke impact van nieuwe versies voor overheden. Ook voor een eventuele nieuwe versie blijft nadere toetsing nodig en zal de gehele procedure doorlopen moeten worden.

Over de standaard
Op de lijst staan de normen voor informatiebeveiliging NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002. 27001 beschrijft de eisen aan het managementsysteem voor informatiebeveiliging. De bijbehorende 27002 standaard is een "best practice" van beveiligingsmaatregelen ('controls') om informatiebeveiligingsrisico's aan te pakken met betrekking tot vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening.

De versies die op de lijst staan dateren uit 2005 (NEN-ISO/IEC 27001) en 2007 (NEN-ISO/IEC 27002). Beide normen zijn in 2013 vernieuwd en zijn een vertaling van de internationale normen ISO/IEC 27001 en 27002. Ondanks dat de structuur van de nieuwe NEN-ISO/IEC 27001 aanzienlijk is veranderd en er een aantal nieuwe normen is toegevoegd, is de nieuwe 27001 standaard (2013) niet strijdig met de oude. De nieuwe NEN-ISO/IEC 27002 standaard omvat een aantal nieuwe normen en bestaande normen zijn geüpdate naar de huidige stand der techniek.

Betrokkenen en proces
Het Forum Standaardisatie heeft in samenwerking met de beheerders van de Baselines Informatiebeveiliging een verkennend onderzoek uitgevoerd naar de 2013 versie van de genoemde standaarden (zie FS 141216.5E Onderzoek NEN-ISO IEC 27001/ 27002). Dit onderzoek was aanleiding om het expertonderzoek uit te laten voeren. De

uitkomsten van het expertonderzoek zijn ter publieke consultatie aangeboden. Aan het expertonderzoek hebben (toekomstige) eindgebruikers, leveranciers, adviseurs en andere kennishebbers deelgenomen.

De conclusie is om de standaarden NEN-ISO/IEC 27001:2013 en 27002:2013 op te nemen op de 'pas toe of leg uit'-lijst, ter vervanging van de 2005 en 2007 versies van deze standaarden. Naar aanleiding van de openbare consultatie zijn een aantal aandachtspunten naar voren gekomen. Deze reacties zijn in overleg met de betrokken partijen verwerkt in het forumadvies.

Consequenties en vervolgstappen
De expertgroep concludeert dat er geen specifieke risico's verbonden zijn aan de keuze. Ook uit de openbare consultatie blijken geen specifieke risico's.
Verder zal op de lijst goed de verhouding tot de Baselines Informatiebeveiliging moeten worden weergegeven. De auditcertificaten op basis van de oude 27001 norm verlopen per 1 oktober 2015. Daarna zal een audit plaatsvinden op basis van de nieuwe normen. Tot slot zijn er enkele adviezen om de adoptie van de standaard te bevorderen, na opname van de standaard is het advies om hier uitvoering aan te geven.

Toepassingsgebied
Het advies is om de standaarden op te nemen voor het volgende toepassingsgebied:

NEN-ISO/IEC 27001:2013: *Voor het Specificeren van eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie.*

NEN-ISO/IEC 27002:2013: *Voor "best practices" op het gebied van het organiseren van informatiebeveiliging voor een organisatie, bestaande uit het beheer van bedrijfsmiddelen, veilig personeel, toegangsbeveiliging, cryptografie, fysieke beveiliging en beveiliging van de omgeving, beveiliging in de bedrijfsvoering, communicatiebeveiliging, leveranciersrelaties, beheer van informatiebeveiligingsincidenten, informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer, naleving en de acquisitie, ontwikkeling en het onderhoud van informatiesystemen.*

Ter Kennisname

Ad 4. Voortgang procedure nieuwe versie van Digikoppeling
Digikoppeling is een standaard voor berichtenuitwisseling en maakt het mogelijk om met en tussen overheden gestructureerd en gecontroleerd berichten uit te wisselen. Digikoppeling 2.0 staat op de 'pas toe of leg uit'-lijst. Op dit moment is versie 3.0 voor opname in behandeling.

Het expertadvies Digikoppeling 3.0 is voor openbare consultatie voorgelegd van 12 februari tot 12 maart jl. Tijdens de openbare consultatie zijn een aantal reacties ontvangen. Vragen vanuit onder andere het ministerie Economische Zaken, het ministerie van Veiligheid en Justitie en het Europese project e-SENS geven aanleiding om de procedure voor de nieuwe versie aan te houden en de vragen eerst nader uit te zoeken. De reacties hebben, kort gezegd, betrekking op het volgende:

1. De status van ebMS 3.0 en het profiel AS4, met name in Europees perspectief;
2. Het huidig gebruik van WS-RM;
3. Het nog niet beschikbaar zijn van een compliancyvoorziening voor het WS-RM-

profiel van Digikoppeling;
4. Uitzondering van de 'pas toe of leg uit'-verplichting voor de Linked Open Data-standaarden RDF en SKOS.

Het feiten onderzoek is erop gericht om na te gaan of bovenstaande punten in de weg staan om de nieuwe versie van Digikoppeling op de 'pas toe of leg uit'-lijst plaatsen en om nadere adoptieadviezen mee te geven. Het onderzoek zal worden afgestemd met de betrokken partijen (o.a. Ministerie van Economische Zaken, eSENS, Ministerie van Veiligheid en Justitie en Logius). Voor de vergadering van het Forum begin juni worden de uitkomsten verwacht.

Ad 5. Nieuwe versie van de toetsingscriteria

Er is een nieuwe versie van de toetsingscriteria. De huidige 1.3 versie is aangepast, naar de 1.4 versie. De nieuwe 1.4 versie van Toetsingsprocedure en criteria voor lijsten met open standaarden is te downloaden via de website van het Forum. (https://www.forumstandaardisatie.nl/sites/default/files/FS/2015/0422/Toetsingsprocedure-en-criteria-1-4.pdf) De grootste wijzigingen zijn:

1. In de Forumvergadering van 16 december was afgesproken om de toetsingcriteria uit te breiden met de vraag of er ook open source referentie-implementaties van een standaard beschikbaar zijn. Dit ter bevordering van de adoptie van een standaard. Deze vraag is toegevoegd.
2. In de oude criteria stonden nog verwijzingen naar het College Standaardisatie, dit is aangepast en geüpdate naar de nieuwe situatie.
3. De oude versie ging uit van aparte lijsten. Terwijl met het aanpassen van de site we nog maar 1 lijst hebben met verschillende statussen.
4. In de nieuwe versie spreken we over aanbevolen standaarden i.p.v. gangbare standaarden. Dit dekt de lading beter en geeft meer ruimte om standaarden op te nemen die nog niet gangbaar zijn, maar die je ook niet het verplichtende karakter van 'pas toe of leg uit' wilt geven.

Ad 6. Standaarden van de Europese MSP-lijst

De Europese Commissie identificeert via het Multi Stakeholder Platform standaarden voor het gebruik in openbare aanbestedingen. Dit gebeurt via een procedure vergelijkbaar met de Nederlandse. Het Forum heeft besloten om de internationale standaarden van de lijst die binnen scope zijn aan te melden bij de Europese Commissie.

Naast standaarden die op de Nederlandse lijsten staan melden ook andere lidstaten en de Europese Commissie zelf standaarden aan die niet op de Forum lijsten staan. In de "Notitie omgang met standaarden van het Europese Multistakeholder Platform on ICT Standardisation" wordt uitgelegd hoe om te gaan met deze standaarden. De notitie is besproken binnen de stuurgroep internationaal en staat op de Forumagenda onder agendapunt 7 (Internationaal).

Voor het dossier lijsten is de relatie dat Europese MSP standaard die binnen scope zijn, uiteindelijk ook worden voorgelegd in de stuurgroep open standaarden.

Ad 7. Nieuwe versie van de uitstekend beheer standaard SIKB0101

SIKB0101 is een open standaard die het mogelijk maakt om op een eenduidige wijze gegevens over de (milieu)kwaliteit van de bodem uit te wisselen binnen de keten van het bodembeheer. Schadelijke gevolgen door bodemvervuiling voor de volksgezondheid en het milieu kunnen hierdoor worden vastgesteld en voorkomen.

Op dit moment staat versie 11 op de 'pas toe of leg uit'-lijst en in oktober 2014 heeft de standaard het predicaat uitstekend beheer gekregen. De beheerorganisatie van

SIKB heeft doorgegeven dat er een nieuwe versie is gepubliceerd (versie 12). BFS zal een check uitvoeren of de procedure van deze nieuwe versie goed is doorlopen. Mocht dit geen vragen oproepen dan zal de versie op de lijst worden aangepast zonder aanvullende toetsing.