notitie

FORUM STANDAARDISATIE 10 juni 2015
Agendapunt 2. Open standaarden, lijsten

Bijlagen:	A. Intakeadvies WPA2 Enterprise B. Intakeadvies SIKB0102 C. Intakeadvies Juriconnect BWB nieuwe versie D. Intakeadvies Kerberos E. Intakeadvies Revit F. Aanvullend onderzoek SPF
Aan:	Forum Standaardisatie
Van:	Stuurgroep open standaarden

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

1. Het is procedure nemen van **WPA2Enterprise,** een set van standaarden voor WIFI verbindingen.
2. Het in procedure nemen van **SIKB0102**, een standaard voor archeologische informatie.
3. Het in procedure nemen van de nieuwe versie van de **Juriconnect standaard BWB** (een standaard voor juridische verwijzingen) en de aanvraag voor uitstekend beheerproces.
4. Het is procedure nemen van de **Dutch Revit Standard,** een standaard voor bouwinformatie, voor op de lijst met aanbevolen standaarden.
5. Het niet in procedure nemen van de standaard **Kerberos**, een standaard voor Single Sign On.
6. Het niet in procedure nemen van de **Secure Software Development** (SSD) methode.

Ter Kennisname

1. Stand van zaken aanvullend onderzoek opname nieuwe versie **Digikoppeling**
2. Aanvullend onderzoek **SPF**, een standaard voor e-mailbeveiliging

Intakeadviezen algemeen
Na de aanmelding van een standaard houdt BFS een intakegesprek met de aanmelder. Tijdens dit gesprek wordt als eerst bepaald of de standaard binnen de scope van de lijsten valt. Aanvullend wordt besproken hoe kansrijk de toetsing van de standaard is. Hiervoor wordt bekeken hoe de standaard, volgens de aanmelder, scoort op de inhoudelijke toetsingscriteria. Op basis van de intake wordt een intakeadvies opgesteld, dat eerst met de stuurgroep Open Standaarden wordt besproken en vervolgens aan het Forum wordt voorgelegd[1].

Ter besluitvorming

Ad 1. Het in procedure nemen van WPA2 Enterprise (zie bijlage A)

Geadviseerd wordt om de standaard WPA2-Enterprise voor wifi-toegang in behandeling te nemen voor opname op de lijst met standaarden. In procedure nemen van deze standaard is van belang vanwege:

- Het uitsluitend door deze standaard geboden hoge beveiligingsniveau,
- De mogelijkheid om op veilige wijze met deze standaard voor gebruikers roaming (toegang tot wifi-netwerken door federatieve authenticatie) te bieden.

Over de standaard
WPA2-Enterprise bevat een set van vier standaarden (WPA2, RADIUS, EAP en 802.1X) die het mogelijk maakt om veilige wifi-netwerken op te zetten. Het zijn internationale open standaarden die worden beheerd door de standaardisatie-organisatie IEEE en IETF. Volgens de indieners komt het helaas nog te vaak voor dat niet de juist set van standaarden worden gebruikt bij het de implementatie van Wifi-netwerken. Opname van de standaarden op de lijst zorgt ervoor dat minder veilige oplossingen zoals een geheel open netwerk, of een gedeeld wachtwoord voor wifi-toegang, niet zonder duidelijke motivering worden geïmplementeerd. Het voorkomt daarmee onbewust onveilig gedrag. Verder is met WPA2-Enterprise ook veilige roaming mogelijk. De standaarden worden ondersteunt door bijvoorbeeld Rijk2Air, Eduroam (onderwijs) en Govroam.

proces
Door SURFnet en Stichting govroam Nederland zijn de standaarden WPA2, RADIUS, EAP, en IEEE 802.1X-2010 aangemeld voor de lijst met 'pas toe of leg uit' standaarden. Vervolgens heeft een intakegesprek plaatsgevonden en is gekeken of de standaarden voldoen aan de criteria voor inbehandelname. De standaarden hebben een duidelijke usecase binnen de (semi) publieke sector en er is sprake van heldere toegevoegde waarde ten aanzien van veiligheid en roaming.

Aangezien de specificatie WPA2-Enterprise het gebruik impliceert van de volledige set van aangemelde standaarden is het advies om WPA2-Enterprise in behandeling te nemen. Het vervolg is om met een expertgroep bijeen te komen en te bepalen of en hoe de standaard op de lijst opgenomen moet worden.

Aandachtspunten
Het is belangrijk om te kijken of het door de indiener geschetste probleem ook breed wordt ervaren en voor welke lijst (aanbevolen of 'pas toe of leg uit') de standaarden het

[1] *Zie voor meer informatie m.b.t. de procedure:*
https://www.forumstandaardisatie.nl/sites/default/files/FS/2013/0903/toetsingsprocedure-en-criteria.pdf

meest geschikt zijn. Daarnaast wordt geadviseerd om tijdens de expertsessie stil te staan bij een goede definiëring van het functioneel toepassingsgebied.

Ad 2. Het in procedure nemen van SIKB0102. (zie bijlage B)

Geadviseerd wordt om SIKB0102 versie 3.0, een standaard voor archeologische informatie, in behandeling te nemen voor opname op de lijst met standaarden. Daarnaast is het advies om te toetsen of het predicaat 'uitstekend beheer' van toepassing is voor Stichting Infrastructuur Kwaliteitsborging Bodembeheer (SIKB) voor het beheer van SIKB0102.

Op de lijst staat ook de standaard SIKB0101. Dit is een standaard voor het uitwisselen van bodemgegevens. SIKB0102 wordt beheerd door dezelfde organisatie, maar heeft een ander toepassingsgebied.

Over de standaard
De SIKB0102 standaard is voor de uitwisseling van archeologische informatie. Deze informatie wordt verzameld tijdens het uitvoeren van archeologisch onderzoek. Een vergunninghouder, een bedrijf of overheidsorganisatie, dat archeologisch onderzoek doet heeft een verplichting om na afronding van de opgraving de verzamelde informatie beschikbaar te stellen aan een aantal depots (landelijk, provinciaal en/of gemeentelijk). De structuur, het formaat en de waarden voor de uitwisseling van deze informatie wordt beschreven door SIKB0102.

Op dit moment vindt de uitwisseling van informatie veelal op niet-gestandaardiseerde wijze plaats. Depots hebben specifieke vereisten voor de aanlevering van informatie, leveranciers van informatiesystemen bieden een eigen koppelvlak. De werkwijze voor uitwisseling is daardoor niet efficiënt.

proces
Stichting Infrastructuur Kwaliteitsborging Bodembeheer heeft de standaard aangemeld voor opname op de lijst met de 'pas toe of leg uit' status. Het indienen van de standaard wordt ondersteund door de Rijksdienst voor het Culturele Erfgoed (RCE) en Data Archiving and Networking Services (DANS) en provinciale depothouders. Nadat de aanmelding was ontvangen heeft een intakegesprek plaatsgevonden. In dit gesprek is de aanmelding besproken en gekeken of de standaard voldoet aan de criteria voor inbehandelname. Hieraan voldoet de standaard.

Het vervolg is om met een expertgroep bijeen te komen en te bepalen of en hoe de standaard op de lijst opgenomen moet worden.

Aandachtspunten
Aandachtspunt bij de verdere behandeling is om ook te kijken naar het effect is van de 'pas toe of leg uit' status voor kleine partijen (gemeentelijke depots, vergunninghouders) met een lage graad van automatisering, laag volume van archeologische vondsten en beperkte (ICT-)budgetten. Andere aandachtspunten zijn de ervaringen met versie 3.0 van de standaard en de financiering van het beheer van de standaard.

Ad 3. Het in procedure nemen van de nieuwe versie van Juriconnect BWB en de aanvraag voor uitstekend beheerproces. (zie bijlage C)

Het Forum Standaardisatie wordt geadviseerd om de nieuwe versie 1.3.1 van Juriconnect-standaard BWB (een standaard voor juridische verwijzingen) in behandeling te nemen voor opname op de 'pas toe of leg uit'-lijst.

Gezien de beperkte wijzigingen t.o.v. de huidige versie op de lijst is het advies om een 'kleine' toets uit te voeren. In deze toets worden een aantal betrokkenen en belanghebbende schriftelijk bevraagd en zal er geen expertbijeenkomst plaatsvinden. Onderdeel van de toets is of het beheerproces voor de standaard voldoet aan de criteria van een "uitstekend beheerproces".

Over de standaard
De Juriconnect standaard BWB (Basis Wetten Bestand) biedt een eenduidige manier van verwijzen naar (onderdelen van) wet- en regelgeving. Hiermee wordt de interoperabiliteit van juridische documenten en systemen die veel verwijzingen kennen naar wet- en regelgeving bevorderd. Het citeren, vinden en verbinden van wet- en regelgeving wordt daardoor minder tijdrovend, minder foutgevoelig en minder ingewikkeld. Versie 1.3 van de Juriconnect standaard BWB kwam in 2013 op de 'pas toe of leg uit'-lijst.

De aangemelde nieuwe versie bevat uitbreidingen van de standaard die in de praktijk vereist zijn om in wet- en regelgeving te kunnen verwijzen naar: taalversies en onderdelen van internationale verdragen, wet- en regelgeving waarvan de indeling niet voldoet aan de gebruikelijke nummering van hoofdstukken en paragrafen, en ruimere begrippen zoals "enig artikel". De uitbreidingen op de standaard in versie 1.3.1 zijn beperkt en backwards compatible.

proces
Door Kennis- en Exploitatiecentrum Officiële Overheidspublicaties (KOOP), een dienstonderdeel van het ministerie van BZK, is versie 1.3.1 van BWB aangemeld voor de lijst met open standaarden. Deze nieuwe versie volgt versie 1.3 op, die nu op de 'pas toe of leg uit'-lijst staat. Er heeft een intakegesprek plaatsgevonden waar is gekeken of alle basisinformatie aanwezig is en of de standaard voldoet aan de criteria voor inbehandelname. Hieraan voldoet de standaard.

Aandachtspunten
Er zijn geen specifieke aandachtspunten. Gezien de beperkte wijzigingen t.o.v. van de huidige versie op de lijst richt het vervolgproces zich met name op de vraag de beheerorganisatie KOOP voldoet aan de criteria van een "uitstekend beheerproces" voor BWB.

Ad 4. Het is procedure nemen van de Dutch Revit Standard voor de lijst met aanbevolen standaarden. (zij bijlage D)

Het Forum Standaardisatie wordt geadviseerd om de Dutch Revit Standard (DRS), een bouwinformatie standaard, in behandeling te nemen voor opname op de lijst als aanbevolen standaard. In procedure nemen van deze standaard is van belang doordat deze standaard eenduidige afspraken vastlegt ten aanzien van de informatiestructuur van Bouw Informatie Model (BIM).

Over de Standaard
De overheid heeft als doelstelling het ontwerp en de uitvoering van alle bouwprojecten te

laten plaatsvinden middels de BIM (Bouw Informatie Model) werkmethode. De BIM-norm stelt eisen aan de oplevering van BIM-projecten. Deze norm beschrijft dat van op te leveren projecten zowel een extract in een Open Bestandsformaat moeten worden opgeleverd, als het originele BIM-model in de gebruikte modelleersoftware. In 60% tot 80% van de projecten is Autodesk Revit de gebruikte modelleersoftware. De standaard DRS verzorgt de uitwisseling van modellen die gemaakt zijn in Autodesk Revit. Naast de open standaard DRS zijn er alleen gesloten standaarden in omloop. DRS hangt samen met de IFC-standaard die al op de lijst staat. DRS zorgt voor consistentie bij de implementatie bij de IFC-standaard.

Proces
De Revit GebruikersGroep Nederland (RevitGG) heeft DRS aangemeld voor de lijst met aanbevolen open standaarden. De aanmelding van de standaard wordt ondersteund door de Bouw Informatie Raad (BIR), waar o.a. Rijkswaterstaat, het Rijksvastgoedbedrijf en de gemeente Rotterdam in deelnemen. Op basis van de aanmelding heeft een intake plaatsgevonden en is gekeken of de standaard voldoet aan de criteria voor inbehandelname voor de lijst met aanbevolen standaarden. De standaard voldoet hieraan.

Omdat de standaard is ingediend als aanbevolen standaard is het advies om niet de uitgebreide toets te doorlopen met expertbijeenkomsten, maar een kleinere experttoets met een aantal interviews.

Aandachtspunten
Van belang is dat DRS slechts betrekking heeft op gebruik binnen Autodesk Revit. Dit is een commercieel softwarepakket. Opname op de aanbevolen lijst moet niet opgevat worden als een aanbeveling om Autodesk Revit toe te passen (onverenigbaar met de rol van de overheid), maar opname op de lijst betekent slechts een aanbeveling om de DRS toe te passen voor zover Autodesk Revit wordt gebruikt binnen een BIM-project.

Ad 5. Het niet in procedure nemen van de standaard Kerberos, een standaard voor Single Sign On. (zie bijlage E)

Het Forum Standaardisatie wordt geadviseerd om Kerberos, een standaard voor Single Sign On, niet in behandeling te nemen voor opname op de lijst. Wel wordt geadviseerd om op de lijst bij het toepassingsgebied van SAML, ook een standaard voor Single Sign On, het verschil tussen de standaarden toe te lichting.

Over de Standaard
De standaard is een single-sign-on (SSO) authenticatieprotocol voor besloten netwerkomgevingen, oftewel binnen een organisatie. Met de standaard kunnen gebruikers zich eenmalig aanmelden, in plaats van meerdere keren, om binnen de netwerkomgeving toegang te krijgen tot verschillende client/server-applicaties.

Kerberos vindt geen toepassing bij gegevensuitwisseling tussen overheidsorganisaties en voldoet daarom niet aan de criteria voor inbehandelname, waarbij er sprake moet zijn van een organisatie overschrijdend interoperabiliteitsprobleem.

Proces
Greenvalley, een softwareontwikkelaar, heeft de standaard Kerberos aangemeld voor de lijst met open standaarden. Vervolgens heeft er een intakegesprek plaatsgevonden en is

de aanmelding besproken. Tijdens het gesprek ik gekeken of de standaard voldoet aan de criteria voor inbehandelname. Vervolgens is bij een aantal experts die betrokken waren bij de SAML experttoets getoetst of er in de praktijk een conflict was tussen SAML en Kerberos en of er sprake was van een interoperabiliteitsprobleem.

Aangezien er geen duidelijk interoperabiliteitsprobleem aanwezig is, is het advies de standaard niet verder in behandeling te nemen. Wel wordt aanbevolen om het verschil tussen Kerberos en SAML toe te lichten op de lijst met standaarden bij SAML.

Aandachtspunten
Er zijn geen specifieke aandachtspunten

Ad 6. Het niet in procedure nemen van de Secure Software Development (SSD) methode (geen bijlage)

Het Forum Standaardisatie wordt geadviseerd om de Secure Software Development Methode, een model voor software ontwikkeling, niet in behandeling te nemen voor opname op de lijst omdat de standaard niet voldoet aan de basiscriteria en kennis te nemen van de voorgestelde adoptieactiviteit

Over de methode
De Secure Software Development (SSD) is een methode met een aantal hanteerbare maatregelen en beveiligingseisen die beschrijven hoe op een veilige manier software te bouwen. Bij de beschrijving van de maatregelen wordt aangegeven wie in de keten van opdrachtgever – softwareontwikkelaar - hostingpartij wat moet doen. Door toepassing van de SSD beveiligingseisen/maatregelen is er een standaard niveau van beveiliging aanwezig in de software. Daardoor heeft ook de informatie-uitwisselingen tussen SSD beveiligde objecten een standaard niveau van beveiliging. Verschillende organisaties, zoals DICTU, RWS, UWV hebben ervaring met de methode en ook Logius is aan het onderzoek of SSD binnen Logius gebruik kan worden.

Proces
De methode is aangemeld door het Centrum Informatiebeveiliging en Privacy (CIP) en het UWV. Vervolgens is de methode ook toegelicht in het Forum Standaardisatie van 22 april 2015. Naar aanleiding van deze presentatie is afgesproken om nader in gesprek te gaan over de bijdrage die het Forum kan leveren om SSD onder de aandacht te brengen. Dit gesprek heeft op 26 mei plaatsgevonden. Opname van SSD op de lijst is echter niet het meest voor de hand liggende middel omdat het Forum normaliter geen methoden in behandeling neemt.

Vervolg
Het Forum Standaardisatie neemt over het algemeen geen methoden in behandeling voor opname op de lijst met standaarden. Ook is het geen methode voor informatie-uitwisseling, maar een methode voor het op een veilige manier bouwen van software, al komt dit impliciet de informatie-uitwisseling ten goede. Het advies is daarom om SSD niet in behandeling te nemen voor opname op de lijst.

Wel is in overleg met het CIP en naar aanleiding van de presentatie in het Forum een aantal acties besproken over hoe het Forum kan bijdragen aan adoptie van de methode.

1. Dit jaar zal een onderzoek uitgevoerd worden naar de samenhang tussen de verschillende beveiligingsstandaarden. Onderdeel van het onderzoek is om in

beeld te brengen welke verschillende kaders en methode er binnen de overheid zijn die bijdragen aan een betere informatiebeveiliging. Ook de rol van het SSD zal hierin worden meegenomen. Met het CIP zal in het kader van het onderzoek worden doorgepraat.

2. Een andere actie die is besproken om het beheermodel van SSD te toetsen aan de hand van BOMOS. Doel is om te kijken of er verbeterpunten zijn met betrekking tot het beheer van het model. Met het CIP zal bekeken worden of deze toets nodig is.

Ter Kennisname

Ad 7. Stand van zaken aanvullend onderzoek opname nieuwe versie Digikoppeling

Over de standaard
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 en versie 3.0 is ingediend voor opname.

Nieuw aan versie 3.0 is de toevoeging van de standaard WS-RM (Web Services Reliable Messaging) aan WUS. WUS WS-RM maakt het mogelijk om met de WUS-standaard (een onderdeel van Digikoppeling) meldingen te kunnen doen over bijvoorbeeld ontvangst van een bericht, voorheen was WUS alleen gericht op bevraging van systemen.

Proces
Naar aanleiding van de openbare consultatie en de experttoets stonden er een aantal vragen open die aanleiding gaven tot een aanvullend onderzoek. Dit waren:

1. Het huidig gebruik van WS-RM;
2. De status van ebMS 3.0 en het profiel AS4, met name in Europees perspectief;
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.

Deze vragen worden op dit moment uitgezocht, waarbij de uitkomsten onder andere worden afgestemd met de betrokken partijen (o.a. Ministerie van Economische Zaken, eSENS, Ministerie van Veiligheid en Justitie en Logius). Dit proces loopt nog en op basis van de uitkomst wordt het definitieve forumadvies opgesteld.

Voorlopige uitkomsten

- Toetsing van de criteria op gebruik van de standaard geeft aanleiding om Digikoppeling 3.0 pas op de lijst te plaatsen wanneer de beheerorganisatie succesvolle implementaties kan laten zien van het WS-RM profiel. Er moet dus al gebruik worden gemaakt van het WS-RM in Digikoppeling. Zodra aan deze voorwaarde is voldaan zal het besluit voor opname voor liggen in het Forum.
- Toetsing van de criteria in relatie tot ebMS 3.0/AS4 geeft geen aanleiding om de nieuwe versie niet op de lijst te plaatsen. Wel speelt dat de verplichting om Digikoppeling toe te passen ook betekent om het Digikoppeling profiel van de standaard ebMS 2.0 te gebruiken. Dit kan worden opgevat als een ontmoediging om te innoveren en ebMS 3.0/AS4 niet toe te passen. Beheerorganisatie Logius wordt dan ook opgeroepen om in afstemming met betrokkenen uit te zoeken of de onderliggende standaard ebMS3.0/AS4 in een nieuwe versie van Digikoppeling moet

terugkomen. De discussie of hier overigens behoefte aan moet niet liggen bij het Forum, maar verlopen via de Logius als beheerder van Digikoppeling.
- Een ‘pas toe of leg uit’-verplichting zou niet moeten worden opgevat als een ontmoediging om te innoveren. Hoe wordt omgegaan met nieuwere versies van een standaard daarover zal bij opname van de nieuwe versie aandacht aan moeten worden besteed
- Bij opname het toepassingsgebied zodanig te specificeren zodat duidelijk is wanneer ebMS2.0, wanneer WS-RM en wanneer WUS van belang is.
- Het functioneel toepassingsgebied in het expertadvies is te ruim omschreven en behoeft inperking tot gegevensuitwisseling waarbij tweezijdige authenticatie vereist is.

Ad 8. Aanvullende onderzoek SPF, een standaard voor e-mailbeveiliging

Tijdens de Forumvergadering van 22 april 2015, heeft het Forum het Nationaal Beraad geadviseerd om SPF op te nemen op de ‘pas toe of leg uit’-lijst. SPF is een standaard die controleert of een mailserver die een e-mail wil versturen namens het e-maildomein e-mail mag verzenden. Voorwaarde voor het opnameadvies was wel dat uit de toen nog lopende controle op de toetsingscriteria geen aandachtspunten naar voren zouden komen zodat er geen openstaande punten waren op het moment dat het besluit zou voorliggen in het Nationaal Beraad.

De controle is tijdig uitgevoerd en er zijn geen aandachtspunten naar voren gekomen. Daarmee voldoet SPF aan de criteria voor opname. In bijlage FS 150610.2G staan de uitkomsten van deze toets op de criteria.