notitie

FORUM STANDAARDISATIE 16 december 2015
Agendapunt 2. Open standaarden, lijsten
Stuknummer 2. Oplegnotitie lijsten

Bijlagen:	A. Intakeadvies FSS B. Intakeadvies Aquo Standaard C. Intakeadvies DANE / StartTLS D. Aanmeldformulier: Verzoek verwijdering NTA9040 E. Brief gemeente Den Haag: Verzoek verwijdering StUF
Aan:	Forum Standaardisatie
Van:	Stuurgroep open standaarden

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

Ter besluitvorming

1. Het niet in procedure nemen van het Framework Secure Software, een standaard voor het veilig ontwikkelen van software.
2. Het in procedure nemen van de nieuwe versie van de Aquo Standaard, een standaard voor watermanagement, en een toets op uitstekend beheer.
3. Het hertoetsen van DANE in combinatie met een toets op StartTLS, beide beveiligingsstandaarden.
4. Het verzoek om NTA9040 (ondernemersdossier) van de lijst te verwijderen in behandeling te nemen.

Ter bespreking: ingekomen brief van de Gemeente Den Haag

5A. Het verzoek om StUF van de lijst te verwijderen.
5B. Onderzoek naar overheidsbrede standaard voor uitwisseling basisgegevens.
5C. Governance (Forum naar het model van de gezondheidsraad).

Ter Kennisname

6. Ingetrokken aanmelding nieuwe versie van WDO Datamodel tezamen met de aanvraag uitstekend beheer.
7. Verkennend onderzoek naar de toenemende transitie naar REST API's als de te gebruiken koppelvlakken en de impact hiervan voor de lijst.
8. Stand van zaken update lijst met aanbevolen (gangbare) standaarden.

Ter besluitvorming

Ad 1. Het niet in procedure nemen van het Framework Secure Software.
(Bijlage A. Intakeadvies FSS)

Het Forum Standaardisatie wordt geadviseerd om het Framework Secure Software (hierna: FSS) niet in behandeling te nemen voor opname op de lijst. Het FSS is een kader voor het veilig ontwikkelen van software. Hoewel software ontwikkeling indirect een relatie kent met gegevensuitwisseling, is FSS niet specifiek toepasbaar voor elektronische gegevensuitwisseling. Daardoor voldoet de standaard niet aan de criteria voor inbehandelname.

Over de standaard
Software wordt veelal pas na oplevering getest op eventuele lekken en zwakheden door middel van code-reviews en penetratietesten. Het FSS is een framework om dit te voorkomen en geeft maatregelen en normen voor veilige softwareontwikkeling. FSS richt zich op alle belanghebbenden in de softwareketen die baat hebben bij duidelijke en objectief meetbare veiligheidskenmerken van software. Opdrachtgevers kunnen deze veiligheidskenmerken gebruiken als vereisten in de formulering van hun opdracht. Ontwerpers en ontwikkelaars kunnen er gebruik van maken bij het bouwen van applicaties, terwijl auditors aan de hand van diezelfde kenmerken de veiligheid van de geproduceerde software kunnen beoordelen. Hierdoor kan het aantal veiligheidsincidenten zoals het hacken van websites en software aanzienlijk worden verminderd.

Betrokkenen en Proces
Op 23 oktober 2015 is door de Secure Software Foundation het FSS als standaard aangemeld voor de lijst met open standaarden. Op 12 november 2015 heeft een intakegesprek plaatsgevonden met de aanmelder. In dit gesprek is de aanmelding besproken. Hierbij is gekeken of alle basisinformatie aanwezig is en of de standaard voldoet aan de criteria voor inbehandelname. Daarnaast is vooruitgeblikt op de procedure en zijn de uitkomsten van het intakeadvies afgestemd met de indiener.

Advies en Aandachtspunten
Het FSS is een kader voor het veilig ontwikkelen van software. Hoewel softwareontwikkeling indirect een relatie kent met gegevensuitwisseling is FSS niet specifiek toepasbaar voor elektronische gegevensuitwisseling. Bovendien is de kansrijkheid van een eventuele procedure onvoldoende doordat de beheerorganisatie nog in ontwikkeling is. Verder zijn de meerkosten voor softwareontwikkeling door het gebruik van het FSS nog niet duidelijk. Het is aannemelijk om te verwachten dat de kosten substantieel zullen zijn gezien de omvang van softwareontwikkeling binnen het organisatorisch werkingsgebied. Het advies is daarom ook om de standaard niet in behandeling te nemen voor opname op de lijst.

Ad 2. Het in procedure nemen van de nieuwe versie van de Aquo Standaard en een toets op uitstekend beheer. *(Bijlage B. Intakeadvies Aquo Standaard)*

Het Forum Standaardisatie wordt geadviseerd om de nieuwste versie van de standaard Aquo, 2015-12 tezamen met een aanvraag voor uitstekend beheer, in behandeling te nemen voor opname op de lijst met open standaarden.

Over de standaard
De Aquo-standaard maakt het mogelijk om op een uniforme manier geografische gegevens uit te wisselen tussen partijen die betrokken zijn bij het waterbeheer. Het vormt hiermee de digitale schakel tussen waterbeheerders: Rijkswaterstaat, provincies, waterschappen, gemeenten en drinkwaterbedrijven. Door de uniforme manier van uitwisselen zijn landelijke rapportages te maken ten behoeve van de waterkwaliteit en eenduidige conclusies te trekken over de waterkwaliteit.

Betrokkenen en Proces
Op dinsdag 20 oktober 2015 is door Informatiehuis Water (hierna: IHW) versie 2015-12 van de Aquo-standaard als standaard aangemeld voor de lijst met open standaarden. Dit is de meest actuele opvolger van de versie IMWA 2008, UM Aquo 2008, Aquo-domeintabellen, Aquo-lex v7 die nu op de lijst met open standaarden staat. Op donderdag 12 november 2015 heeft een intakegesprek plaatsgevonden. Hierbij is gekeken of alle basisinformatie aanwezig is en of de standaard voldoet aan de criteria voor inbehandelname. Daarnaast is vooruitgeblikt op de procedure en zijn de uitkomsten van het intakeadvies afgestemd met de indiener.

Advies en Aandachtspunten
Gezien de vele middelgrote en grote wijzigingen ten opzichte van de huidige versie van de standaard op de lijst is het advies om een 'uitgebreide toets' uit te voeren. In deze toets wordt een expertgroep samengesteld en zal er een expertbijeenkomst plaatsvinden. Onderdeel van de toets is of het beheerproces van de standaard voldoet aan de criteria van een 'uitstekend beheerproces'. Daarnaast is het advies om ook te kijken naar de huidige toepassing van de standaard in de praktijk, wat de relatie is tussen de Aquostandaard en IMWA-metingen en naast waterschappen ook meerdere provincies en Rijkswaterstaat te betrekken.

Ad 3. Het hertoetsen van DANE in combinatie met een toets op StartTLS. (*Bijlage C: Intakeadvies DANE en StartTLS)*

Het Forum Standaardisatie wordt geadviseerd om DNS-Based Authentication of Named Entities (DANE) en STARTTLS, standaarden voor de transportbeveiliging van e-mail, in behandeling te nemen voor opname op de lijst met standaarden.

Over de standaarden
DANE: Bij het maken van een veilige verbinding is een online controle op de authenticiteit van de verzendende partij en de eindbestemming wenselijk. Dit kan door middel van (gepubliceerde) certificaten die door certificaatautoriteiten (CA's) binnen het PKI-stelsel zijn uitgegeven. DANE maakt het voor de eigenaar van een domein mogelijk om via een met DNSSEC beveiligd DNS-record extra informatie bovenop de offline certificaten aan te reiken.

STARTTLS: E-mails worden door de mailserver van de verzendende mailprovider verstuurd naar de mailserver van de ontvangende partij. De verbinding tussen deze mailservers kan versleuteld worden door middel van TLS. De standaard STARTTLS upgrade een niet-versleutelde, en daarmee onbeveiligde, verbinding naar een versleutelde TLS-verbinding. Om STARTTLS in werking te laten treden is het noodzakelijk dat zowel de verzendende als de ontvangende mailserver STARTTLS ondersteunen.

Betrokkenen en proces
In 2013 is een toetsingsprocedure doorlopen voor DANE. Omdat DANE nog zeer beperkt werd toegepast en de marktondersteuning voor de toepassing van DANE onvoldoende was, heeft de expertgroep geadviseerd om de standaard niet op te nemen op de pas-toe-of-leg-uit-lijst. Onderdeel van het advies was om na een bepaalde periode en op aangeven van de indiener de adoptie van de standaard opnieuw te beoordelen.

DANE is opnieuw ingediend door NLnet. In het gesprek met de indiener is naar voren gekomen dat DANE in toenemende mate wordt toegepast met STARTTLS om een beveiligde verbinding tussen mailservers op te kunnen zetten. Daarom wordt op aangeven van de indiener geadviseerd om zowel DANE als STARTTLS in procedure te nemen, waarbij voor DANE aanvullend onderzoek wordt gedaan naar de adoptie van de standaard. De aanmelding van DANE en STARTTLS als open standaarden wordt ondersteund door het Nationaal Cyber Security Centrum (NCSC) en SURFnet.

Advies en Aandachtspunten
Het in procedure nemen van deze standaarden is van belang vanwege de risico's die via niet-versleutelde verbindingen kunnen ontstaan, zoals het 'afluisteren' en manipuleren van berichtenverkeer. DANE en STARTTLS zorgen ervoor dat elektronische gegevensuitwisseling (e-mail) tussen mailservers via een beveiligde verbinding wordt verstuurd. DANE en STARTTLS kennen een relatie met DNSSEC en TLS en de e-mailstandaarden DKIM, SPF en DMARC. Het is goed om tijdens de procedure deze relaties goed inzichtelijk te maken.

Geadviseerd wordt om tijdens de expertbijeenkomst stil te staan bij de adoptie van DANE binnen het organisatorisch werkingsgebied. Het is de vraag of DANE verplicht of aanbevolen moet worden gesteld. Daarnaast dient tijdens de expertbijeenkomst aandacht te worden besteed aan de implementatiekosten van STARTTLS en DANE.

Ad 4. Het verzoek om NTA9040 van de lijst te verwijderen (*Bijlage D: Aanmeldformulier NTA9040*)

Aan het Forum Standaardisatie wordt gevraagd om het verzoek om NTA9040 (standaard voor het ondernemersdossier) in behandeling te nemen voor verwijdering van de lijst.

Over de aanmelding
Na de deadline van het aanmelden van standaarden en net voor het opstellen van de stukken is er een verzoek van het programma Ondernemingsdossier van het ministerie van Economische Zaken (EZ), directie R&ICT binnengekomen om NTA9040 van de lijst te verwijderen. Het was echter niet meer mogelijk om een intake uit te voeren, maar om tot eind april te wachten met het in behandeling nemen is misschien ook niet nodig.

Het Forum wordt daarom verzocht om het verzoek in behandeling te nemen en te onderzoeken of de standaard van de lijst af kan. Het bijgevoegde aanmeldformulier dient daarbij als basis.

Over de standaard
NTA9040 is van toepassing voor overheden die expliciet met ondernemingen hebben afgesproken een Ondernemingsdossier in te zetten voor de informatie-uitwisseling met ondernemingen. Daarbij is de standaard van toepassing op het ondersteunen van ondernemingen bij het geautomatiseerd bepalen van de relevante voorschriften en bijbehorende maatregelen, het faciliteren van het digitaal indienen van aanvragen en meldingen vanuit een Ondernemingsdossier en het gebruik van een Ondernemingsdossier als bron van bedrijfsinformatie in het kader van het toezicht.

Betrokkenen en proces
De standaard wordt beheerd door het NEN in opdracht van het programma Ondernemingsdossier van het Ministerie van Economische Zaken. Er ligt nu een verzoek vanuit het Ministerie om de verplichting van de standaard via de pas-toe-of-leg-uit-lijst in te trekken. Omdat het aanmeldformulier pas net voor het opstellen van de stukken in binnengekomen, is de vervolgprocedure nog niet nader besproken met de indiener.

Consequenties en vervolgstappen
Mocht het verzoek in behandeling worden genomen, dan zal eerst met de indiener worden besproken wat de beste plan van aanpak is. Verder zal gekeken moeten worden wat de impact is van een mogelijke verwijdering voor stakeholders, welke alternatieve standaarden er zijn voor gebruikers om aan te sluiten op de voorziening het ondernemingsdossier en wat dit betekent voor het toekomstig beheer van de NTA9040. Deze uitkomsten zullen worden getoetst bij betrokkenen en leveranciers en tezamen met de andere procedures in openbare consultatie worden gebracht.

Ter bespreking

Ingekomen brief van de Gemeente Den Haag
In opdracht van de gemeente Den Haag heeft de Software Improvement Group (SIG) onderzocht of STuF op het gebied van interoperabiliteit, kostenreductie, marktwerking en innovatie voldoende ondersteuning biedt. De bevindingen zijn dat deze standaard hier onvoldoende aan bijdraagt. Naar aanleiding hiervan is er op 30 oktober jl. een bijeenkomst geweest waar de onderzoeksresultaten zijn besproken. Deze bijeenkomst was georganiseerd door de gemeente Den Haag in samenwerking met de SIG en het Kwaliteitsinstituut Nederlandse Gemeenten (KING).

Naar aanleiding van het rapport en de bijeenkomst heeft de Gemeente Den Haag bijgevoegde brief opgesteld gericht aan de Digicommissaris, het Forum Standaardisatie en de Directie Digitalisering en Informatisering Overheid van BZK. Deze brief is op 27 november ook besproken met KING, BZK, de Gemeente Den Haag en BFS. In deze brief worden drie voorstellen gedaan. Aan het Forum de vraag om deze voorstellen te bespreken.

Ad 5A. punt 1: het verzoek om de StUF-BG standaard in te trekken
Naar aanleiding van het rapport en de bijeenkomst verzoekt de Gemeente Den Haag om STuF van de lijst te halen. Er is geen apart aanmeldformulier ingediend en intake uitgevoerd. Aan het Forum de vraag om het verzoek in behandeling te nemen. Hierbij

is het belangrijk dat de reactie en de te nemen vervolgacties worden afgestemd met beheerorganisatie KING. Los van een eventuele procedure is het wel goed om te informatie op de lijst (in samenwerking met KING) te actualiseren zodat er een eenduidig beeld is over wat STuF wel en niet doet en wat de relatie is tot de sectorale STuF standaarden.

Ad 5B. punt 2. Onderzoek naar overheidsbrede standaard voor uitwisseling basisgegevens
In brief wordt opgeroepen tot een onderzoek naar de haalbaarheid van overheidsbrede standaarden voor het uitwisselen van basisgegevens en indien mogelijk het opstellen van een roadmap om te komen tot overheidsbrede standaarden in plaats van sectorale. Deze wens hangt ook sterk samen met de discussie rondom de vraag naar een stelsel van overheidsgegevens (rotondemodel). De vraag aan het Forum is welke rol het Forum moet innemen met betrekking tot een mogelijk onderzoek.

Ad 5C. punt 3. Governance (Forum naar het model van de gezondheidsraad)
Het laatste punt gaat over dat het proces van de besturing van ICT-standaarden beter moet, waarbij er voor gepleit wordt om het Forum Standaardisatie vorm te geven naar het model van de Gezondheidsraad. In dat model is gekozen voor een benadering waarbij onafhankelijke kwaliteitsbeoordeling centraal staat, ondersteund door kennisintensieve hoogwaardige instituten als het RIVM die dat borgen. Aan het Forum wordt gevraagd dit voorstel te bespreken.

Vervolgstap
De reactie (met daarin ook eventuele vervolgstappen) op de gehele brief zal worden afgestemd met de geadresseerden en KING. Op basis daarvan zal ook het gesprek gevoerd worden met de Gemeente Den Haag.

Ter kennisname

Ad 6. Ingetrokken aanmelding nieuwe versie van WDO Datamodel tezamen met de aanvraag uitstekend beheer

Ingediend was een nieuwe versie van het WDO Datamodel tezamen met de aanvraag uitstekend beheer. Na de intake is door de aanmelder (Logius) in overleg met de sponsor (de Douane) besloten om de procedure niet voort te zetten en de aanmelding in te trekken. De nieuwe versie van WDO Datamodel voldoet wel aan de criteria voor inbehandelname, maar naar verwachting zal niet worden voldaan aan de criteria voor uitstekend beheer. De aanmelder heeft aangegeven dat zij zich gaan richten op het verder uitwerken van het beheerproces alvorens opnieuw een aanmelding te doen waarmee ook toekenning van uitstekend beheer zal worden beoogd.

Ad 7. Verkennend onderzoek naar de toenemende transitie naar REST API's als standaard en de impact hiervan voor de lijst
Er is vaak discussie over de vraag of voor applicatie-naar-applicatie-communicatie en website-naar-applicatie-communicatie op REST gebaseerde standaarden voor API's (Application Programming Interface) gebruikt moeten worden. Dit in tegenstelling tot de meer 'traditionele' op SOAP gebaseerde standaarden voor API's. Deze leveren namelijk meer beheerlasten op, zijn minder flexibel en technisch 'zwaarder'. Wat de impact van deze verschuiving is voor de lijst en voor de standaarden op de lijst willen we laten uitzoeken. Als eerste zijn we nu echter bezig met een verkennend onderzoek om de discussie helder te krijgen en te bepalen welke vragen we moeten stellen.

Ad 8. Stand van zaken update lijst met aanbevolen (gangbare) standaarden
Er loopt een onderzoek of er standaarden toegevoegd moeten worden aan de lijst met aanbevolen standaarden of dat standaarden op deze lijst moeten worden bijgewerkt. Op dit moment is inzichtelijk welke standaarden op de lijst moet worden ge-update. Daarnaast hebben we een overzicht van standaarden die mogelijk kunnen worden toegevoegd aan de lijst met aanbevolen standaarden. Deze standaarden worden nu afgestemd met enkele experts. Naar verwachting gaan de uitkomsten van het onderzoek medio januari 2016 in openbare consultatie.