



3 Oplegnotitie Open Standaarden, lijsten

Vergadering:	Forum Standaardisatie woensdag 7 december 2022
Agendapunt:	3
Documentnummer:	FS-20221207.3-Oplegnotitie-Open-Standaarden-Lijsten
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	Woensdag 7 december 2022
Versie:	1.1
Bijlage:	FS-20221207.3A-Forumadvies-Versiewijziging-VISI FS-20221207.3B-Intakeadvies-Versiewijziging-OAS FS-20221207.3C1-Evaluatierapport-Schoon-water-beschermde-bodem FS-20221207.3C2-Evaluatierapport-Veilig-internet
Opstellers:	Hans Laagland Han Zuidweg (3E. Acties voor doorontwikkeling van de lijst open standaarden)
Rechten:	CC0 publieke domein verklaring

Samenvatting

Ter besluitvorming

Vraag aan Forum Standaardisatie om in te stemmen met het volgende advies:

- de standaard **VISI** in de nieuwe versie (1.6) te blijven verplichten aan de overheid ([‘pas toe of leg uit’](#)-verplichting) (betere gegevensuitwisseling)
- toetsen of de standaard **OAS** in de nieuwe versie (3.1) geschikt is om te blijven verplichten aan de overheid ([‘pas toe of leg uit’](#)-verplichting) (betere gegevensuitwisseling)
- de geëvalueerde standaarden blijven verplichten aan de overheid ([‘pas toe of leg uit’](#)-verplichting) en opvolging geven aan de voorgestelde aanbevelingen per standaard

- (C1. Evaluatie **SIKB0101**, **SIKB0102**, **Aquo-standaard**, betere gegevensuitwisseling en C2. Evaluatie **STIX** en **TAXII**, veilig internet)
- D. evalueren van de standaarden **AdES Baseline Profiles** (betere gegevensuitwisseling), **WDO Datamodel** (betere gegevensuitwisseling) en **SKOS en aanpalende linked data standaarden** als cluster (meer openbaarheid en toegang) in 2023, voor waarborgen kwaliteit lijst verplichte standaarden

Ter toelichting

- E. Acties voor de doorontwikkeling van de lijst open standaarden
- F. Voortgang lopende procedures
1. Veiliger internet:
 - a. Nederlands profiel bij OpenID Connect 1.0 (authenticatie)
lopende procedure: verplichten aan de overheid ('pas toe of leg uit'-verplichting)
 - b. security.txt (security- en policy-contactinformatie)
lopende procedure: verplichten aan de overheid ('pas toe of leg uit'-verplichting)

Ter besluitvorming

Ad A. Forumadvies versiewijziging VISI (betere gegevensuitwisseling)

[Bijlage: FS-20221207.3A-Forumadvies-Versiewijziging-VISI]

Vraag aan Forum Standaardisatie om in te stemmen met het volgende advies:

de standaard **VISI** in de nieuwe versie (1.6) te blijven verplichten aan de overheid ('pas toe of leg uit'-verplichting), voor betere gegevensuitwisseling

Advies

De Stuurgroep Open Standaarden adviseert het Forum Standaardisatie om de standaard VISI in de nieuwe versie (1.6) te blijven verplichten aan de overheid ('pas toe of leg uit'-verplichting). VISI is een standaard voor procescommunicatie in de bouw.

Het blijven verplichten van VISI in de nieuwe versie (1.6) aan de overheid ('pas toe of leg uit'-verplichting) heeft toegevoegde waarde en vergroot de adoptie van de standaard. Versie 1.6 van de standaard zorgt voor betere gegevensuitwisseling: de uitbreiding in de functionaliteit voor meezenden van bijlagen is een meerwaarde in de ondersteuning van een bouwproject. De aanpassingen in de versiewijziging zijn beperkt en vergroten het gebruiksgemak van VISI voor eindgebruikers. Zowel overheden als marktpartijen ondersteunen deze versiewijziging, en de leveranciers hebben de versiewijziging geïmplementeerd in de softwarepakketten.

Het functioneel toepassingsgebied en het organisatorisch werkingsgebied blijven ongewijzigd. Het BIM Loket als nieuwe beheerorganisatie neemt het predicaat 'uitstekend beheer' niet over van de vorige beheerder CROW.

Belang van de standaard: betere gegevensuitwisseling

VISI draagt bij aan betere gegevensuitwisseling en leveranciersafhankelijkheid doordat VISI het eenvoudiger maakt om informatie over bouwprocessen uit te wisselen en daarmee transparantie en traceerbaarheid van het bouwproces vergroot. Dit draagt bij aan de kosten- en procesbeheersing van bouwprojecten.

Een aantal experts in [Evaluatie Bouwstandaarden](#) (2021) ziet als risico dat als VISI niet meer verplicht is, de kans groter is dat overheidsinstanties eigen software laten bouwen die niet onderling compatibel is en zodoende gegevensuitwisseling en interoperabiliteit beperkt.

Hoe is het proces verlopen?

Naar aanleiding van de Evaluatie Bouwstandaarden (2021) is vastgesteld dat de versie 1.4 van de standaard op de 'pas toe of leg uit'-lijst niet de gangbare versie is. Het BIM Loket heeft daarom op 15 oktober 2021 versie 1.6 aangemeld voor 'pas toe of leg uit'-lijst.

Op 9 maart 2022 besloot Forum Standaardisatie de versiewijziging in procedure te nemen en in de periode 8 april tot en met 9 juni 2022 heeft een schriftelijk expertonderzoek plaatsgevonden. Aan dit expertonderzoek namen vertegenwoordigers deel uit een brede coalitie van overheid, bedrijfsleven, en koepelorganisaties.

Het Expertadvies is van 1 oktober tot en met 30 oktober 2022 [ter openbare consultatie](#) gepubliceerd op internetconsultatie.nl. Op de consultatie zijn geen reacties binnengekomen. Op basis van het Intakeadvies en het Expertadvies is het Forumadvies samengesteld.

Over de standaard

VISI is een open standaard voor digitale communicatie tussen partijen in een bouwproject. Met behulp van VISI wordt bepaald wanneer (proces), wie (rol), wat (informatie), aan wie (rol) aanlevert. Denk hierbij aan het geven van opdrachten, het aanleveren van tijdschema's, het opleveren van resultaten en het melden van afwijkingen. Huidige gebruikers bevinden zich ook buiten de publieke sector, zoals (internationale) bouwgroepen die als opdrachtnemer ingehuurd worden door overheden.

De aanpassingen van VISI 1.6 ten opzichte van 1.4 zijn de volgende:

1. aantal rijen in een tabel kan nu in formulier worden vastgelegd;
2. het is nu mogelijk om bijlagen bij bepaalde berichten verplicht te stellen;
3. opbouw van tabellen is verbeterd en kent eenduidige afspraken;
4. er kunnen grotere bijlagen worden verstuurd.

De aanpassingen zijn beperkt en leveranciers passen de standaard toe in versie 1.6. Versie 1.6 versterkt de gegevensuitwisseling t.o.v. versie 1.4 in de ondersteuning van een bouwproject, met name vanwege het toenemende gebruikersgemak voor eindgebruikers.

Het beheer van VISI ligt sinds 2016 bij BIM Lokaal. Het Forum Standaardisatie heeft CROW nog als beheerder met het predicaat 'uitstekend beheer'. Dit predicaat is niet overgegaan naar het BIM Lokaal; daarom deze toetsingsprocedure voor de versiewijziging. Toetsing voor verkrijgen van predicaat 'uitstekend beheer' voor BIM Lokaal is geen onderdeel van deze procedure.

Ad B. Intakeadvies versiewijziging OAS (betere gegevensuitwisseling)

[Bijlage: FS-20221207.3B-Intakeadvies-Versiewijziging-OAS]

Vraag aan Forum Standaardisatie om in te stemmen met het volgende advies:

toetsen of de standaard **OAS** in de nieuwe versie (3.1) geschikt is om te blijven verplichten aan de overheid ('pas toe of leg uit'-verplichting), voor betere gegevensuitwisseling

Advies

De Stuurgroep Open Standaarden adviseert het Forum Standaardisatie om te toetsen of de standaard OpenAPI Specification (OAS) in de nieuwe versie (3.1) geschikt is om te blijven verplichten aan de overheid ('pas toe of leg uit'-verplichting). OAS is een standaard voor het beschrijven van REST API's; een Application Programming Interface (API) draagt bij aan het uitwisselen van informatie tussen applicaties.

De indiener Logius verzoekt om de versie van OAS te actualiseren op de 'pas toe of leg uit'-lijst vanuit het belang dat OAS wordt gebruikt in andere standaarden van Logius, waaronder Digikoppeling (in het bijzonder koppelvlakspecificatie REST-API). De huidige versie 3.0 op de 'pas toe of leg uit'-lijst is niet de gangbare versie. Versie 3.1 van OAS is niet backward compatible ten opzichte van versie 3.0.

Een beperkt expertonderzoek is aangewezen om de standaard in de nieuwe versie te toetsen aan de criteria voor opname op de lijst verplichte standaarden, met extra aandacht voor de punten die naar voren zijn gekomen tijdens het intakegesprek en tijdens de bespreking in de Stuurgroep Open Standaarden (o.a. draagvlak OAS 3.1).

Belang van de standaard: betere gegevensuitwisseling

OAS draagt bij aan betere gegevensuitwisseling tussen diverse partijen en betere toegankelijkheid van gegevens doordat OAS REST API's toegankelijker maakt door deze op een gestandaardiseerde manier te beschrijven. Een stabiele en eenduidige wijze van beschrijven van REST API's maakt het eenvoudiger om een API te documenteren. Dit bevordert weer het gebruik van API's.

Hoe is het proces verlopen?

Logius heeft op 10 augustus 2022 heeft de standaard OAS in de nieuwe versie 3.1 aangemeld bij het Bureau Forum Standaardisatie om te blijven verplichten aan de overheid ('pas toe of leg uit'-verplichting). Op 20 september 2022 heeft het intakegesprek plaatsgevonden.

Over de standaard

Een OpenAPI Specification (OAS) beschrijft de eigenschappen van de data die een REST-API als input accepteert en als output teruggeeft. Een API (Application Programming Interface) is een veel toegepaste en essentiële technologie om moderne applicaties (en databronnen) snel en effectief met elkaar te verbinden en om eenvoudig informatie uit te wisselen.

Representational State Transfer (REST) is een ontwerpprincipe dat wereldwijd veel gebruikt wordt voor het bouwen van programmeerinterfaces over het web (API's). REST is geen standaard maar een ontwerpprincipe, en laat nog veel vrijheid in het structureren van API's.

De aanpassingen van OAS 3.1 ten opzichte van OAS 3.0 zijn de volgende:

- toevoeging van beschrijvingen van webhooks. Webhooks zijn geautomatiseerde berichten die gegevens overbrengen tussen applicaties wanneer er een wijziging plaatsvindt in de bronapplicatie.
- mogelijkheid om Mutual TLS te specificeren als 'Security Schema'. Mutual TLS is een veelgebruikte methode waarbij authenticatie in twee richtingen plaatsvindt.

Mutual TLS is ook een vereiste bij de implementatie van de nieuwe versie van Digikoppeling koppelvlak REST API. Dit was voor Logius een belangrijke reden om deze versiewijziging in te dienen voor plaatsing op de 'pas toe of leg uit'-lijst.

Versie 3.1 van OAS is niet backward compatible ten opzichte van versie 3.0. De impact hiervan zal tijdens de expertbijeenkomst verder getoetst te worden.

Ad C1. Evaluatie SIKB0101, SIKB0102, Aquo-standaard (betere gegevensuitwisseling)

[Bijlage: FS-20221207.3C1-Evaluatierapport-Schoon-water-beschermde-bodem]

Vraag aan Forum Standaardisatie om in te stemmen met de volgende adviezen:

- a. standaarden **SIKB0101, SIKB0102, Aquo-standaard** blijven verplichten aan de overheid ('pas toe of leg uit'-verplichting) en opvolging geven aan de voorgestelde aanbevelingen per standaard
- b. (gecombineerde) procedures starten om het functioneel toepassingsgebied van SIKB0101, SIKB0102 en Aquo-standaard te actualiseren

Samenvatting en advies

De Stuurgroep Open Standaarden adviseert het Forum Standaardisatie om SIKB0101, SIKB0102, Aquo-standaard te blijven verplichten aan de overheid ('pas toe of leg uit'-verplichting) op basis van uitkomsten van de evaluatie van de standaarden. Ook adviseert de Stuurgroep Open Standaarden opvolging te geven aan de voorgestelde aanbevelingen per standaard, waaronder het actualiseren van het functioneel toepassingsgebied. De geëvalueerde standaarden SIKB0101 (bodeminformatie), SIKB0102 (archeologische informatie) en Aquo-standaard (watermanagementinformatie) bevorderen gegevensuitwisseling in het domein 'schoon water en beschermde bodem'.

Het Forum Standaardisatie evalueert jaarlijks een aantal standaarden op de 'Pas toe of leg uit'-lijst. Het doel van dit onderzoek is om de kwaliteit van de informatie op de lijst te waarborgen. Het onderzoek richt zich met name op de huidige relevantie van de standaard, het functioneel toepassingsgebied, het beheer en de stand van zaken rond de adoptie van de standaard.

Belang van de standaarden: betere gegevensuitwisseling

[SIKB0101](#) is een standaard voor de uitwisseling van gegevens voor de milieuhygiënische data inclusief geografische en administratieve gegevens. Op basis van deze gegevens kan worden vastgesteld of sprake is van schadelijke gevolgen voor de volksgezondheid en het milieu als gevolg van bodemvervuiling. SIKB0101 draagt zo bij aan het voorkomen van dergelijke schadelijke effecten en bevordert de bescherming voor de volksgezondheid en het milieu.

[SIKB0102](#) voorziet in optimalisering van digitale uitwisseling van archeologische gegevens tussen opgravende instanties, vondstendepots en/ of archeologische registers. SIKB0102 draagt zo bij aan een eenduidige uitwisseling van gegevens over archeologisch onderzoek en/of archeologische vondsten met overheidsinstanties zoals depots. Dit komt ten goede aan het vertrouwen in de kwaliteit van de beschikbare digitale documentaties.

[Aquo-standaard](#) maakt het mogelijk om op een uniforme manier gegevens uit te wisselen tussen partijen die betrokken zijn bij waterbeheer. Aquo-standaard draagt op deze manier bij

aan een kwaliteitsverbetering van het waterbeheer. Aquo-standaard is bedoeld voor iedereen die te maken heeft met het vastleggen en gebruiken van gegevens.

Aanbevelingen uit de evaluatie

Hieronder volgen de belangrijkste aanbevelingen per geëvalueerde standaard.

SIKB0101

1. Toepassingsgebied

Aan het Forum Standaardisatie om een procedure te starten om het toepassingsgebied dusdanig te formuleren dat deze breed genoeg is om nieuwe sectoren (bv. drinkwatersector) te adopteren binnen de standaard, zonder dat het toepassingsgebied bij iedere aanvullende sector opnieuw aangepast moet worden.

2. Draagvlak

Aan Forum Standaardisatie om aanvullend onderzoek te doen naar de adoptie onder gemeentes die geen gebruik maken van een Bodem Informatie Systeem (BIS) waarin SIKB0101 is geïmplementeerd.

3. Beheer

Aan het Forum Standaardisatie om een positie in te nemen rond het lidmaatschap van SIKB en de daaraan verbonden kosten die nodig zijn om organisaties te ontzorgen de standaard zo laagdrempelig mogelijk te implementeren.

4. Opname op de lijst

Aan het Forum Standaardisatie om SIKB0101 te blijven verplichten aan de overheid ('pas toe of leg uit'-verplichting)

5. Lopende ontwikkelingen

Aan het Forum Standaardisatie om vervolgonderzoek te doen naar de gevolgen van opname van (delen van) SIKB0101 in de Basisregistratie Ondergrond (BRO). Aan SIKB de aanbeveling om te blijven communiceren over de opname van (delen van) SIKB0101 in BRO en de impact hiervan.

SIKB0102

1. Toepassingsgebied

Aan het Forum Standaardisatie om een procedure te starten om het toepassingsgebied aan te passen zodat de gebruikte terminologie beter aansluit bij de doelgroep.

2. Toegevoegde waarde

Aan het SIKB om te onderzoeken of adoptie sneller vergroot kan worden en, waar mogelijk, initiatieven te ondersteunen die adoptie kunnen vergroten. Aan de vondstendepots om te

onderzoeken of hun implementatie van de standaard hen toegang geeft tot de volle breedte aan informatie die gedeeld kan worden middels de pakbon.

3. Beheer

Aan het SIKB om een versiebeheer of backward compatibility toe te passen op SIKB0102 en aanvullend te overwegen of het huidige wijzigingsregime van tweemaal per jaar aansluit bij het werkveld.

4. Opname op de lijst

Aan het Forum Standaardisatie om SIKB0102 te blijven verplichten aan de overheid ('pas toe of leg uit'-verplichting).

Aquo-standaard

1. Toepassingsgebied

Aan het Forum Standaardisatie om een procedure te starten om het toepassingsgebied aan te passen waarbij de [ideaaltypische formulering](#) meer gespecificeerd wordt. Aanpassing betreft het toevoegen van de tweede laag uit de ideaaltypische formulering (gebruikers van de ICT-dienst of -product).

2. Toegevoegde waarde

Aan het Informatiehuis Water (IHW) om het gesprek aan te gaan met oppervlaktewaterbeheerders om te onderzoeken wat er nodig is voor de Aquo-standaard zodat de Aquo-standaard meer wordt gebruikt voor oppervlaktewaterbeheer.

3. Beheer

Aan het IHW om softwareleveranciers en oppervlaktewaterbeheerders te betrekken bij de doorontwikkeling van de standaard. Aan het IHW om bij medewerkers te sturen op kennis van business, techniek en standaarden. Dit zal de ontwikkeling van de standaard ten goede komen.

4. Opname op de lijst

Aan het Forum Standaardisatie om Aquo-standaard te blijven verplichten aan de overheid ('pas toe of leg uit'-verplichting).

5. Lopende ontwikkelingen

Aan het Forum Standaardisatie om vervolgonderzoek te doen naar de gevolgen van opname van (delen van) de Aquo-standaard in Basisregistratie Ondergrond (BRO). Aan IHW om te blijven communiceren over de opname van (onderdelen van) de Aquo-standaard in de BRO en de impact hiervan op de standaard en haar gebruikers.

Conclusies en aanbevelingen over domein 'schoon water en beschermde bodem'

Het in samenhang evalueren van SIKB0101, SIKB0102 en Aquo-standaard biedt de mogelijkheid tot een aantal standaard-overstijgende conclusies en aanbevelingen:

1. Toepassingsgebied

Bij SIKB0101, SIKB0102, Aquo-standaard zijn opmerkingen gemaakt over het toepassingsgebied. Dit leidt tot de aanbeveling aan het Forum Standaardisatie om bij de actualisering van het toepassingsgebied van SIKB0101 en Aquo-standaard overlap in de toepassingsgebieden te voorkomen.

2. Opname op de lijst

Van alle standaarden wordt gezegd dat zij op de 'pas toe of leg uit'-lijst moeten blijven staan. Hoewel adoptie hoog is blijft het volgens zowel beheerders als gebruikers van belang om de specifieke standaard als 'pas toe of leg uit'-verplichting te hebben. Voor overheden is het met name van belang om het aanleverformaat te kunnen verplichten richting aanleverende partijen (dit kunnen zowel andere overheden zijn als commerciële partijen).

3. Lopende ontwikkelingen

Ontwikkelingen rond de Basisregistratie Ondergrond (BRO) moeten gevolgd worden voor SIKB0101 en de Aquo-standaard, met name ook ten aanzien van de impact op het blijven verplichten van deze standaarden.

Hoe is het proces verlopen

Het Forum Standaardisatie heeft op [8 december 2021](#) groen licht gegeven om SIKB0101, SIKB0102 en Aquo-standaard uit het domein 'schoon water en beschermde bodem' in samenhang te evalueren. Het doel van dit onderzoek is om de kwaliteit van de informatie op de lijst te waarborgen.

Onderzoeksbureau InnoValor is op 22 juni 2022 gestart met het onderzoek. InnoValor heeft in overleg met het Bureau Forum Standaardisatie per standaard een lijst met experts opgesteld. Na overleg met de beheerders van de standaard is de lijst met experts aangevuld. Focus lag op het betrekken van verschillende rollen die in aanraking komen met de standaard: de beheerder, de eindgebruiker en de softwareleverancier. Na presentatie van de eerste bevindingen is in samenspraak met Bureau Forum Standaardisatie besloten aanvullende interviews te houden.

De onderzoekers hebben aanbevelingen opgesteld op basis van analyse van de interviews. Uitkomsten van de interviews, de analyses en de aanbevelingen zijn opgetekend in één evaluatierapport. Op 14 november 2022 heeft InnoValor het evaluatierapport opgeleverd aan Bureau Forum Standaardisatie. De drie evaluaties zijn in één rapport samengebracht, dat is voorzien van een algemene inleiding en een overall conclusie.

Achtergrond

De beheerders van SIKB0101, SIKB0102 en Aquo-standaard hebben een geruime tijd het predicaat 'uitstekend beheer'. Nieuwe versies van deze standaarden worden twee keer per jaar vastgesteld door het Centraal College van Deskundigen Datastandaarden Bodem en

Water. Daardoor zijn deze standaarden niet tussentijds getoetst. Evaluatie is een geschikt middel de huidige versies te schouwen.

SIKB0101 staat sinds juni 2012 op de 'pas toe of leg uit'-lijst, SIBK0102 staat sinds februari 2016 op de 'pas toe of leg uit'-lijst en Aquo-standaard staat op de 'pas toe of leg uit'-lijst sinds november 2010.

Ad C2. Evaluatie STIX en TAXII (veilig internet)

[Bijlage: FS-20221207.3C2-Evaluatierapport-Veilig-internet]

Vraag aan Forum Standaardisatie om in te stemmen met de volgende adviezen:

- a. standaarden **STIX** en **TAXII** blijven verplichten aan de overheid ('pas toe of leg uit'-verplichting) en opvolging geven aan de voorgestelde aanbevelingen per standaard
- b. onderzoeken waar de regierol voor STIX en TAXII binnen de Nederlandse overheid het beste is te beleggen en hierover te adviseren

Samenvatting en advies

De Stuurgroep Open Standaarden adviseert het Forum Standaardisatie om STIX en TAXII te blijven verplichten aan de overheid ('pas toe of leg uit'-verplichting) op basis van uitkomsten van de evaluatie van de standaarden. Ook adviseert de Stuurgroep Open Standaarden opvolging te geven aan de voorgestelde aanbevelingen per standaard. De geëvalueerde standaarden STIX en TAXII (cyberdreigingsinformatie) dragen bij aan een veiliger internet doordat cyberdreigingsinformatie gemakkelijker en sneller wordt uitgewisseld.

In Nederland ontbreekt een regierol vanuit de Nederlandse overheid op STIX en TAXII. Evaluatierapport adviseert te onderzoeken waar de regierol voor STIX en TAXII binnen de Nederlandse overheid het beste is te beleggen en hierover te adviseren. Cybersecurity wordt in belangrijke mate vanuit het perspectief van de dreiging (en dus in termen van risico's) beleefd ([Nederlandse Cybersecuritystrategie 2022-2028](#)). Het is te verwachten dat de Nederlandse overheid een sturende rol (een regierol) wil hebben op standaarden over dreigingsinformatie. Deze regierol draagt bij aan het vergroten van de digitale weerbaarheid door grip te houden op het beheerproces en op de adoptie, en zorgt ervoor dat Nederland aansluit bij internationale ontwikkelingen rond STIX en TAXII.

Het Forum Standaardisatie evalueert jaarlijks een aantal standaarden op de 'Pas toe of leg uit'-lijst. Het doel van dit onderzoek is om de kwaliteit van de informatie op de lijst te waarborgen. Het onderzoek richt zich met name op de huidige relevantie van de standaard, het functioneel toepassingsgebied, het beheer en de stand van zaken rond de adoptie van de standaard.

Belang van de standaarden: veiliger internet

[STIX](#) draagt bij aan veilig internet doordat organisaties via STIX cyberdreigingsinformatie makkelijker en sneller kunnen uitwisselen. STIX maakt geautomatiseerde detectie van en reactie op cyberdreigingen mogelijk. STIX wordt gebruikt voor het consistent delen, opslaan en analyseren van cyberdreigingsinformatie doordat het een gestructureerde taal biedt om informatie over cyberdreigingen uit te wisselen.

[TAXII](#) draagt bij aan veilig internet doordat TAXII real-time uitwisselen van cyberdreigingsinformatie mogelijk maakt. Dit kan de reactietijd van organisaties op cyberdreigingen aanzienlijk versnellen. TAXII biedt een protocol voor de communicatie van cyberdreigingsinformatie op een eenvoudige en schaalbare manier. TAXII is specifiek

ontworpen voor de uitwisseling van cyberdreigingsinformatie in STIX-formaat, maar is niet beperkt tot STIX.

Aanbevelingen uit de evaluatie

Hieronder volgen de belangrijkste aanbevelingen.

STIX en TAXII

(aanbevelingen gelden voor STIX en voor TAXII)

1. In gesprek gaan met het NCSC over de regierol op STIX en TAXII gezien het NCSC de aanmelder van de standaarden op de 'pas toe of leg uit'-lijst is geweest.
2. In samenwerking met het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties afdeling Digitale Samenleving onderzoeken waar de regierol voor Nederland voor STIX en TAXII binnen de Nederlandse overheid het beste is belegd en hierover adviseren.
3. Tussen de twee en vier jaar de standaarden opnieuw te evalueren. De markt rondom cyberdreigingsinformatie groeit en is in beweging. De kans dat er op een middellange termijn ontwikkelingen zijn die de standaarden raken is groot.

Zodra de regierol voor STIX en TAXII voor Nederland belegd is binnen de Nederlandse overheid, zijn de volgende aanbevelingen gericht aan de partij die de regierol op zich neemt:

4. Contact leggen met partijen die actief zijn in STIX- en TAXII-committee bij de beheerorganisatie OASIS met als doel om zicht en grip te krijgen op het beheerproces en op internationale ontwikkelingen.
5. Opnieuw onderzoeken van het nut en de noodzaak van de adoptieadviezen. De experts geven geen signalen dat er behoefte is aan kennisdeling over de standaard. Daarentegen loopt de adoptie bij gemeenten en waterschappen achter en is de potentiële meerwaarde van de standaard niet helder voor alle organisaties.
6. Uitdragen en communiceren van toegevoegde waarde van STIX en TAXII.
7. Onderzoeken in hoeverre er sprake is bij STIX en TAXII van leveranciersafhankelijkheid door de sterke rol van leveranciers in de ontwikkeling en in het uitdragen van de standaard.

Conclusies en aanbevelingen over domein 'veilig internet'

Het in samenhang evalueren van STIX en TAXII biedt de mogelijkheid tot een aantal standaard-overstijgende conclusies en aanbevelingen:

De bevraagde experts geven aan dat STIX en TAXII duidelijk twee verschillende standaarden zijn, en dat ze ook zodanig behandeld dienen te worden. Tegelijkertijd geven ze aan dat de standaarden nauwelijks apart van elkaar gebruikt worden.

Het ontbreken van de regierol bij de Nederlandse overheid voor STIX en TAXII leidt tot de bevinding dat het van belang is om voor iedere standaard op de 'pas toe of leg uit'-lijst en voor nieuw aangemelde standaarden na te gaan of de regierol belegd is. Dit is van belang voor het houden van zicht en grip op het beheerproces, het aansluiten op internationale ontwikkelingen en het opvolgen van de adoptieadviezen.

Hoe is het proces verlopen

Het Forum Standaardisatie heeft op [8 december 2021](#) groen licht gegeven om STIX en TAXII standaarden uit het domein 'veilig internet' in samenhang te evalueren. Het doel van dit onderzoek is om de kwaliteit van de informatie op de lijst te waarborgen.

Onderzoeksbureau InnoValor is op 22 juni 2022 gestart met het onderzoek. InnoValor heeft in overleg met het Bureau Forum Standaardisatie per standaard een lijst met experts opgesteld. Focus lag op het betrekken van verschillende rollen die in aanraking komen met de standaard: de beheerder, de eindgebruiker en de softwareleverancier. Er is besloten om de interviews met experts in te steken op STIX en TAXII met daarin aandacht in het interview voor elke standaard afzonderlijk. Na presentatie van de eerste bevindingen is in samenspraak met Bureau Forum Standaardisatie besloten aanvullende interviews te houden.

De onderzoekers hebben aanbevelingen opgesteld op basis van analyse van de interviews. Uitkomsten van de interviews, de analyses en de aanbevelingen zijn opgetekend in één evaluatierapport. Op 10 november 2022 heeft InnoValor het evaluatierapport opgeleverd aan Bureau Forum Standaardisatie. De twee evaluaties zijn in één rapport samengebracht, dat is voorzien van een algemene inleiding en een overall conclusie.

Achtergrond

In het Forumadvies van 19 september 2017 heeft de expertgroep het Forum Standaardisatie geadviseerd om de adoptie van STIX 1.2.1 en TAXII 1.1.1 en de oproepen daaromtrent na twee jaar te evalueren. Daarnaast heeft het Forum Standaardisatie het advies gegeven aan meerdere partijen om kennis en ervaringen uit te wisselen. Vijf jaar na opname op de 'pas toe of leg uit'-lijst is het relevant om te bekijken in hoeverre dit is gelukt.

Op 10 juni 2021 is een nieuwe versie van TAXII (TAXII 2.1) goedgekeurd door de leden van OASIS (beheerorganisatie). Een nieuwe versie maakt het relevant om de standaard op de 'pas toe of leg uit'-lijst te evalueren. Het NCSC adviseert inmiddels STIX versie 2.1 bij aanschaf van nieuwe cybersecurity software.

Ad D. Selectie van standaarden ter evaluatie in 2023

Vraag aan Forum Standaardisatie om in te stemmen met het volgende advies:

evalueren van de standaarden **AdES Baseline Profiles** (betere gegevensuitwisseling), **WDO Datamodel** (betere gegevensuitwisseling) en **SKOS en aanpalende linked data standaarden** als cluster (meer openbaarheid en toegang) in 2023, voor waarborgen kwaliteit 'pas toe of leg uit'-lijst

Advies

De Stuurgroep Open Standaarden adviseert het Forum Standaardisatie om in 2023 de standaarden **AdES Baseline Profiles**, **WDO Datamodel** en **SKOS en aanpalende linked data standaarden** uit de Lijst Aanbevolen Standaarden als cluster te evalueren, voor waarborgen kwaliteit 'pas toe of leg uit'-lijst. AdES Baseline Profiles is een standaard voor geavanceerde en gekwalificeerde digitale handtekeningen (betere gegevensuitwisseling). WDO Datamodel is een standaard voor gegevensuitwisseling bij het oversteken van grenzen (betere gegevensuitwisseling). SKOS is een standaard voor duidelijke lijsten met termen en begrippen (meer openbaarheid en toegang); SKOS bouwt voort op aanpalende linked data standaarden uit de Lijst Aanbevolen Standaarden OWL, RDF, RDFa, RDFS en SHACL en zij worden in samenhang toegepast.

Het Forum Standaardisatie evalueert jaarlijks een aantal standaarden op de 'pas toe of leg uit'-lijst. Het doel van dit onderzoek is om de kwaliteit van de informatie op de lijst te waarborgen. Het onderzoek richt zich met name op de huidige relevantie van de standaard, het functioneel toepassingsgebied, het beheer en de stand van zaken rond de adoptie van de standaard.

Hoe is het proces verlopen?

De volgende criteria worden toegepast om standaarden te selecteren voor het onderzoek:

- a. Staat de standaard vier jaar of langer op de 'pas toe of leg uit'-lijst (i.e. 2018 of ouder) en is deze in de tussentijd niet getoetst (bijvoorbeeld voor een nieuwe versie)?
- b. Voldoet de standaard nog volledig aan de vier criteria voor opname op de 'pas toe of leg uit'-lijst?
- c. Zijn er signalen van gebruikers dat het draagvlak onder druk staat?
- d. Hebben er zich relevante (markt)ontwikkeling voorgedaan met betrekking tot de standaard of de toepassing ervan?
- e. Is het toepassingsgebied van de standaard nog relevant en duidelijk?

Op basis van selectiecriterium 'a' heeft het Bureau Forum Standaardisatie in oktober 2022 een long list samengesteld. Het Bureau heeft de standaarden op de long list beoordeeld op de overige vier criteria en heeft vervolgens standaarden gekandideerd voor evaluatie in 2023.

Over alle gekandideerde standaarden uit deze shortlist heeft een tweede selectieronde plaatsgevonden waarna onderstaande drie standaarden worden voorgedragen voor evaluatie.

Geselecteerde standaarden

Op basis van de bovengenoemde criteria zijn de onderstaande standaarden geselecteerd voor evaluatie in 2023:

Betere gegevensuitwisseling

- AdES Baseline Profiles (veilig internet)

Ministerie van Binnenlandse Zaken en Koninkrijksrelaties heeft in 2016 AdES Baseline Profiles aangemeld om de standaard te verplichten aan de overheid. Er is momenteel geen partij die zich ontfemt over deze standaard. Dit belemmert het stimuleren van adoptie en het verzamelen van gebruiksgegevens voor de Monitor Open Standaarden. Evaluatie onderzoekt de meerwaarde van de standaard op de 'pas toe of leg uit'-lijst.

[Advanced Electronic Signature](#) (AdES) voorziet in het digitaal tekenen van documenten met een geavanceerde of gekwalificeerde digitale handtekening. Bij gegevensuitwisseling tussen EU lidstaten is AdES Baseline Profiles verplicht. Een digitale handtekening geeft de ontvanger van een digitaal document of bericht zekerheid dat het afkomstig is van de ondertekenaar en dat deze de inhoud van het bericht onderschrijft.

- WDO Datamodel (economie en werk)

WDO Datamodel staat sinds 2014 op de 'pas toe of leg uit'-lijst. De registratie is aan een update toe. De beheerders zijn moeilijk te bereiken hetgeen van invloed is op de status van adoptie. Aandachtspunten bij evaluatie zijn: actualisatie van de registratie van WDO-Datamodel, status van de adoptieadviezen en de verplichtstelling.

[World Customs Organization Data Model](#) (WDO Datamodel) is in 1997 opgezet vanuit de G7 naar aanleiding van de wens van het bedrijfsleven om gegevensaanlevering van het bedrijfsleven naar de overheid op het gebied van grensoverschrijdend personen- en goederenverkeer meer te simplificeren en te harmoniseren.

Meer openbaarheid en toegang

- SKOS (openbaarheid en toegang) en aanpalende linked data standaarden uit de Lijst Aanbevolen Standaarden als cluster

Het gebruik van linked data bij overheden neemt toe. Binnen de overheid groeit (de wens naar) het aantal begrippenkaders, zowel vanuit informatievoorziening als vanuit semantische standaardisatie. Linked data draagt daarnaast bij aan interoperabiliteit zowel binnen organisaties als tussen organisaties. De linked data community ziet meerwaarde om linked data standaarden van de 'pas toe of leg uit'-lijst en van lijst aanbevolen standaarden te clusteren in één registratie (net zoals de GeoStandaarden), omdat linked data standaarden in samenhang worden toegepast. Evaluatie van SKOS en aanpalende linked data standaarden in samenhang borgt de kwaliteit van deze standaarden op de Lijst Open Standaarden nu de

vraag naar linked data toeneemt, en levert input voor een geclusterde registratie van linked data standaarden.

[Simple Knowledge Organization System](#) (SKOS) is een gegevensmodel om duidelijke lijsten met termen en begrippen op te stellen. Met deze termenlijsten kan informatie uit verschillende databases aan elkaar worden gekoppeld. SKOS maakt de relaties tussen begrippen inzichtelijk voor het vergelijken en interpreteren van data uit verschillende systemen. Zo krijgt informatie meer waarde.

Aanpalende linked data standaarden uit de Lijst Aanbevolen Standaarden zijn:

- [OWL](#) (Web Ontology Language): beschrijvingstaal semantisch web
- [RDF](#) (Resource Description Framework): publicatie gestructureerde gegevens
- [RDFa](#) (Resource Description Framework in Attributes): indexeren en verzamelen van geautomatiseerde content
- [RDFS](#) (Resource Description Framework Schema): standaardtaal voor structuur van gegevens in termen van klassen, eigenschappen en datatypen
- [SHACL](#) (Shapes Constraint Language): kwaliteitscriteria op linked data

Ter toelichting

Ad E. Acties voor de doorontwikkeling van de lijst open standaarden

[Bijlage: geen]

In de [vergadering van 20 april 2022](#) besprak het Forum Standaardisatie de acties die voortkwamen uit het onderzoek van Paul Dam over de [doorontwikkeling van de lijsten open standaarden](#). Hieronder volgt een overzicht van de voortgang.

Verwijderen van standaarden

Het Forum Standaardisatie (FS) vroeg het Bureau (BFS) in de vergadering van 20 april 2022 om de lijst aanbevolen standaarden relevanter te maken door standaarden te verwijderen die op de lijst geen duidelijke meerwaarde meer hebben. BFS heeft een concept-lijst gereed van standaarden die in aanmerking komen voor verwijdering van de lijst aanbevolen standaarden.

BFS verstuurt de concept-lijst na de Forumvergadering van 7 december 2022 met het verzoek aan het Forum Standaardisatie om via een schriftelijke review te reageren op deze concept-lijst van standaarden die in aanmerking komen voor verwijdering. Desgewenst kan het Forum Standaardisatie wijzigingen aanbrengen in de groep standaarden.

De verwachting is de concept-lijst met te verwijderen standaarden na de schriftelijke review als besluitpunt aan te bieden op de eerstvolgende vergadering van het Forum Standaardisatie. Daarna kan een gezamenlijke procedure van start ter verwijdering van deze standaarden van de lijst aanbevolen standaarden.

Opname 'andersoortige standaarden'

In de vergadering van 29 september 2022 stemde het Forum Standaardisatie ermee in om een 'andersoortige standaard' als *proof of concept* in procedure te nemen voor plaatsing op de lijst aanbevolen standaarden. Het doel van deze pilot procedure is om ervaring op te doen met het toetsen van 'andersoortige standaarden' zoals principes, baselines en richtlijnen, en om vast te stellen of de huidige toetsingsprocedure hiervoor geschikt is. [MANRS](#) en [NL Design System](#) zijn kandidaten om in de pilot procedure getoetst te worden.

BFS start deze procedure in 2023 omdat het contract met de procedurebegeleider (Lost Lemon) in 2022 afloopt. BFS is voornemens een Europese aanbesteding uit te zetten voor opvolging.

Gangbare standaarden minder op de voorgrond

In de vergadering van 20 april 2022 gaf het Forum Standaardisatie opdracht aan BFS om gangbare standaarden op de lijst aanbevolen standaarden minder op de voorgrond te laten treden. Om dit te realiseren moeten er twee dingen gebeuren:

1. De gangbare standaarden op de lijst aanbevolen standaarden moeten geïdentificeerd worden. BFS heeft een twintigtal standaarden in het vizier op de lijst aanbevolen standaarden die als gangbaar aangemerkt kunnen worden, waaronder HTML en CSS.
2. De informatiehuishouding (inclusief de website) moet worden aangepast om gangbare standaarden te onderscheiden en minder op de voorgrond te presenteren. BFS doet deze aanpassing als onderdeel van de bredere aanpak van professionalisering van de informatiehuishouding, waarbij gegevens van weergave worden gescheiden en semantisch worden verbonden met bijvoorbeeld gegevens van de NORA.

Met name het tweede punt vergt de nodige inzet en zorgvuldigheid, omdat BFS de informatiehuishouding in lijn wil brengen met geldende beleidskaders en richtlijnen van het Rijksprogramma voor Duurzaam Digitale Informatiehuishouding ([RDDI](#)). BFS verwacht hier voor de zomer van 2023 belangrijke voortgang mee gemaakt te hebben.

Indeling van de 'pas toe of leg uit'-lijst

In de vergadering van 20 april 2022 stemde het Forum Standaardisatie in met de herbenoeming van bestaande indeling van de 'pas toe of leg uit'-lijst volgens domeinen. De nieuwe benamingen richten zich op het doel van de standaard (bijvoorbeeld veilig internet) in plaats van het proces of de techniek (bijvoorbeeld stelselstandaarden of REST API).

Deze actualisatie van de bestaande indeling op domeinen wordt geleidelijk ingevoerd in de verschillende communicatie-uitingen van het Forum Standaardisatie.

Ad F. Voortgang lopende procedures

[Bijlage: geen]

Veiliger internet

Nederlands profiel bij OpenID Connect 1.0 (authenticatie): tweede expertbijeenkomst

Forum Standaardisatie toetst of de standaard van Logius [NL GOV Assurance Profile for OIDC 1.0](#) geschikt is om te verplichten aan de overheid via plaatsing op de 'pas toe of leg uit'-lijst. NL GOV Assurance Profile for OIDC 1.0 draagt bij aan veiliger internet doordat authenticatieservices (zoals DigiD) de identiteit van een eindgebruiker controleren op een gestandaardiseerde wijze.

Uit [expertadvies](#) (najaar 2021) en [reacties uit de openbare consultatie](#) (winter 2022) kwamen drie aandachtspunten naar voren, namelijk 'toegevoegde waarde (overlap met SAML)', 'draagvlak (marktondersteuning) (voorbeeldimplementatie)' en samenhang met het internationale iGOV-profiel voor OIDC. In overleg met de indiener Logius (7 april 2022) is besloten een tweede expertbijeenkomst te houden als aanloop naar een Forumadvies. De tweede expertbijeenkomst adresseert de genoemde aandachtspunten.

De tweede expertbijeenkomst heeft plaatsgevonden op 6 oktober. Tijdens de tweede expertbijeenkomst hebben de experts de oplossingsrichtingen uit het adviesrapport voor de criteria 'toegevoegde waarde' en 'draagvlak' besproken, alsook de resultaten uit de hackathon van 14 en 15 september van Logius op de toepasbaarheid van het OIDC-profiel. De uitkomsten van de tweede expertbijeenkomst worden verwerkt in een Forumadvies.

De toetsingsprocedure voor NL GOV Assurance Profile for OIDC 1.0 is de voortzetting van de aanmelding van de standaard door Logius op 15 oktober 2020 voor opname op de 'Pas toe of leg uit'-lijst. In de toetsingsprocedure is er aandacht voor opmerkingen die het Forum Standaardisatie heeft uitgesproken na het akkoord op het [Intakeadvies](#) van NL GOV Assurance Profile for Open ID Connect 1.0.

security.txt (security- en policy-contactinformatie)

Forum Standaardisatie toetst of de standaard security.txt geschikt is om te verplichten aan de overheid ('pas toe of leg uit'-verplichting). De standaard beschrijft op een uniforme wijze, hoe een kwetsbaarheid gemeld kan worden aan een organisatie met diensten/ systemen die verbonden zijn met het internet.

National Cyber Security Centrum (NCSC) en Digital Trust Center (DTC) hebben de standaard security.txt 2 juni 2022 aangemeld bij het Bureau Forum Standaardisatie. Het Forum Standaardisatie heeft op 28 september 2022 besloten om security.txt in procedure te nemen. De expertbijeenkomst is in voorbereiding.