notitie

FORUM STANDAARDISATIE 10 oktober 2018
Agendapunt 3 Open Standaarden, lijsten

Nummer:	FS 181010.3
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	11 september 2018
Versie:	1.0
Bijlagen:	FS 181010.3A Forumadvies TLS 1.3 FS 181010.3C Forumadvies STARTTLS en DANE FS 181010.3D Forumadvies STOSAG 1.0 FS 181010.3F Forumadvies SHACL

Samenvatting

Ter besluitvorming

U wordt gevraagd om in te stemmen met de volgende adviezen.

Pas toe of leg uit:

A. Plaatsing van **TLS 1.3** (nieuwe versie van standaard voor de beveiliging van Internetverbindingen) op de pas-toe-of-leg-uit-lijst naast TLS 1.2 en verwijdering van **TLS 1.0** en **TLS 1.1** van de pas-toe-of-leg-uit-lijst.
B. Vervanging van versie 1.1.2 van **EN 301 549** door versie 2.1.2 (nieuwe versie Europese norm voor digitale toegankelijkheid) op de pas-toe-of-leg-uit-lijst; starten van een toetsingsprocedure ter verwijdering van EN 301 549 op 23 september 2019.
C. Uitbreiding van het functioneel toepassingsgebied van **STARTTLS** in combinatie met **DANE** (e-mailveiligheidstandaarden tegen het afluisteren of manipuleren van mailverkeer).
D. Verwijdering van **STOSAG 1.0** (standaard voor informatie-uitwisseling in de afvalverwerking) van de pas-toe-of-leg-uit-lijst.
E. Het starten van een procedure ter inperking van het functioneel toepassingsgebied van **COINS 2.0** (opslag- en uitwisselingsstandaard voor de bouw).

Lijst aanbevolen standaarden:

F. Plaatsing van **SHACL** (linked data standaard) op de lijst aanbevolen standaarden.
G. Plaatsing van **S/MIME** (standaard voor aanvullende e-mailbeveiliging) op de lijst aanbevolen standaarden voor uitsluitend digitale ondertekening, niet voor versleuteling van e-mail.

Ter kennisname

H. Aanvullend onderzoek voor plaatsing **PDF/UA** (documentstandaard die wettelijke toegankelijkheidseisen ondersteunt) op de pas-toe-of-leg-uit-lijst.

Ter besluitvorming

Ad A. TLS 1.3

[Bijlage A]

Het Forum Standaardisatie wordt gevraagd om in te stemmen met de volgende adviezen aan het OBDO:

1) Het plaatsen van TLS 1.3 op de pas-toe-of-leg-uit-lijst met behoud van TLS 1.2 als terugval-versie

2) Het verwijderen van TLS 1.1 en TLS 1.0 als terugval-versies van de pas-toe-of-leg-uit-lijst

Over de standaard

TLS is een standaard voor het opzetten van veilige verbindingen over het Internet. Een veilige https verbinding met een website (zichtbaar als het 'groene slotje' in de browser) maakt bijvoorbeeld gebruik van TLS. TLS 1.2 staat reeds op de pas-toe-of-leg-uit-lijst, waarbij TLS 1.1 en 1.0 ook nog worden toegelaten als een verbinding met TLS 1.2 niet mogelijk is. TLS 1.3 is een recent gepubliceerde nieuwe versie van het TLS-protocol dat efficiënter en veiliger werkt dan TLS 1.2.

Hoe is het proces verlopen?

NLnet Foundation (https://nlnet.nl/) heeft TLS 1.3 in april 2018 aangemeld voor plaatsing op de pas-toe-of-leg-uit-lijst. Op basis van het intake-advies heeft het Forum Standaardisatie in juni 2018 besloten om TLS 1.3 in procedure te nemen. In de zomer van 2018 heeft een expertonderzoek[1] plaatsgevonden waaraan experts van Logius, NCSC, DMarcian (private sector), VNG Realisatie, Enable-U (private sector), PowerDNS (private sector), Justid, Sonnection (private sector), MinBZK, Gemeente 's Hertogenbosch en UWV deelnamen. Het expertadvies is van 6 augustus tot en met 10 september 2018 ter openbare consultatie aangeboden. In de openbare consultatie zijn in totaal acht reacties ontvangen[2] van RINIS, Rechtspraak.nl, het Ministerie van Defensie, het Ministerie van Justitie en Veiligheid, de Sociale Verzekeringsbank (SVB), het Uitvoeringsinstituut Werknemersverzekeringen (UWV), de Kamer van Koophandel (KvK) en het Bureau Keteninformatisering Werk & Inkomen (BKWI).

Advies en gevraagd besluit

Een meerderheid van de organisaties die reageerden op de openbare consultatie steunt de opname van TLS 1.3 op de pas-toe-of-leg-uit-lijst met behoud van TLS 1.2 als 'terugval-optie'. Geen enkele organisatie twijfelt aan de meerwaarde van TLS 1.3 voor het realiseren van veilige verbindingen over het Internet. Drie organisaties vinden het echter te vroeg om TLS 1.3 op de pas-toe-of-leg-uit-lijst te plaatsen. Twee argumenten die daarbij worden genoemd zijn het ontbreken van marktondersteuning en de status van TLS 1.3 als 'proposed standard internet-draft'. Het Ministerie van Defensie vindt het functioneel toepassingsgebied van TLS 1.3 bovendien te breed en stelt dat er toepassingen zijn die sterkere encryptiemiddelen vereisen.

De experts geven de volgende reacties op deze kritiekpunten:

- Marktondersteuning: de meest gebruikte open source library openssl.org ondersteunt inmiddels TLS 1.3. De servers van de meeste commerciële leveranciers gebruiken openssl.org onder de motorkap. TLS 1.3 staat op de roadmap van de meeste leveranciers. Het (moeten) uitvragen van TLS 1.3 bij aanbestedingen zal verder druk zetten op de markt om vaart te maken met de implementatie van de standaard.
- Status van de standaard: IETF heeft RFC 8446 (TLS 1.3) in augustus 2018 formeel gepubliceerd als 'proposed standard'. Een 'proposed standard' heeft bij de IETF de status van een afgeronde, stabiele standaard. Vele bekende standaarden zoals http hebben deze status 'proposed standard'.
- Speciale applicaties: militair operationele applicaties zijn uitgesloten van de Instructie Rijk inzake de aanschaf van ICT producten en diensten (bijlage, artikel 3 lid 3)[3].

Het advies om TLS 1.3 op de pas-toe-of-leg-uit-lijst te plaatsen wordt daarom gehandhaafd.

Een meerderheid van experts en organisaties pleit voor het verwijderen van TLS 1.0 en TLS 1.1 van de pas-toe-of-leg-uit-lijst. Dit advies wordt overgenomen. TLS 1.0 en TLS 1.1 worden nog maar weinig gebruikt en het ligt in de verwachting dat het NCSC het gebruik van TLS 1.0 en TLS 1.1 binnen afzienbare tijd zal ontraden. Door het van de pas-toe-of-leg-uit-lijst verwijderen van TLS 1.0 en TLS 1.1 wordt het gebruik van deze versies niet meer aangemoedigd. Organisaties *mogen* deze versies echter nog wel blijven gebruiken om de compatibiliteit met oudere mobiele apparaten en browsers te waarborgen.

[1] https://www.forumstandaardisatie.nl/sites/bfs/files/20180803%20Expertadvies%20TLS%201.3.pdf

[2] https://www.forumstandaardisatie.nl/sites/bfs/files/Commentaar%20uit%20de%20openbare%20consultatie%20TLS%201.3.pdf

[3] http://wetten.overheid.nl/BWBR0024717/2008-11-23

Ad B. EN 301 549 v2.1.2 met WCAG 2.1

[Geen bijlage]

Het Forum Standaardisatie wordt gevraagd om in te stemmen met het volgende advies aan het OBDO:

1) Het vervangen van EN 301 549 versie 1.1.2 door versie 2.1.2 op de pas-toe-of-leg-uit lijst zodra het *Tijdelijk besluit toegankelijkheid digitale overheid* naar deze nieuwe versie verwijst.

2) Het starten van een toetsingsprocedure om te onderzoeken of EN 301 549 kan worden verwijderd van de pas-toe-of-leg-uit-lijst op 23 september 2019.

Over de standaard

De Europese norm (EN) 301 549 beschrijft richtlijnen waaraan online informatie (websites, documenten, webapplicaties) moet voldoen om digitaal toegankelijk te zijn voor iedereen, ook mensen met een functiebeperking. EN 301 549 versie 1.1.2 staat op de pas-toe-of-leg-uit-lijst van het Forum Standaardisatie. Deze specificatie verwijst normatief naar de toegankelijkheidsrichtlijnen WGAC 2.0 van het W3C. In augustus van dit jaar heeft ETSI een nieuwe versie 2.1.2 van EN 301 549[4] gepubliceerd die verwijst naar een nieuwe versie 2.1 van WCAG.

Hoe is het proces verlopen?

Vanaf 1 juli 2018 is het *Tijdelijk besluit toegankelijkheid digitale overheid*[5] van kracht, dat specificeert dat EN 301 549 vanaf 23 september 2019 wettelijk moet worden toegepast op *nieuwe*, en vanaf 23 september 2020 op *alle* websites en webapplicaties van de overheid. Wettelijke verplichting gaat boven pas-toe-of-leg-uit zoals vastgelegd in de *Instructie rijk inzake de aanschaf van ICT producten en ICT diensten*[6]. Met de wettelijke verplichting kan EN 301 549 van de pas-toe-of-leg-uit-lijst van het Forum Standaardisatie worden verwijderd.

In overleg met digitoegankelijk.nl (Logius) en het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties wordt geadviseerd om EN 301 549 tot 23 september 2019 op de pas-toe-of-leg-uit-lijst te laten staan. Dit voorkomt dat er tussen nu en 23 september 2019 een situatie ontstaat waarbij overheidsorganisaties EN 301 549 niet meer hoeven uit te vragen bij aanbestedingen en ook nog niet aan de toegankelijkheidseisen hoeven voldoen. Met andere woorden: de verplichting tot uitvragen moet blijven bestaan totdat overheidswebsites volgens de wet toegankelijk moeten zijn.

Advies en gevraagd besluit

Naar verwachting zal de nieuwe EU toegankelijkheidsrichtlijn 2102/2016 met daarin de verwijzing naar EN 301 549 versie 2.1.2 medio november 2018 gepubliceerd worden in het Official Journal[7] van de Europese Commissie. De lidstaten zijn verplicht om de nieuwe richtlijn direct toe te passen zonder overgangs- of implementatietermijn. Dit betekent dat het *Tijdelijk besluit toegankelijkheid digitale overheid* naar verwachting half november 2018 direct zal verwijzen naar versie 2.1.2 van EN 301 549 met verwijzing naar WCAG 2.1.

Om te voorkomen dat de pas-toe-of-leg-uit-lijst van het Forum Standaardisatie verwijst naar een oudere versie (1.1.2) van EN 301 549 dan het *Tijdelijk besluit toegankelijkheid digitale overheid* wordt geadviseerd om EN 301 549 versie 1.1.2 op de pas-toe-of-leg-uit-lijst te vervangen door EN 301 549 versie 1.2.1 op hetzelfde moment dat deze wijziging in het *Tijdelijk besluit toegankelijkheid digitale overheid* van kracht wordt.

Tevens wordt geadviseerd om een toetsingsprocedure te starten om te onderzoeken of EN 301 594 kan worden verwijderd van de pas-toe-of-leg-uit-lijst op 23 september 2019, wanneer websites van de overheid voor het eerst moeten voldoen aan de wettelijke toegankelijkheidseisen.

[4] http://www.etsi.org/deliver/etsi_en/301500_301599/301549/02.01.02_60/en_301549v020102p.pdf
[5] http://wetten.overheid.nl/BWBR0040936/2018-07-01
[6] http://wetten.overheid.nl/BWBR0024717/2008-11-23
[7] https://eur-lex.europa.eu/oj/direct-access.html

Ad C. STARTTLS en DANE

[Bijlage C]

Het Forum Standaardisatie wordt gevraagd om in te stemmen met het volgende advies aan het OBDO:

Het als volgt uitbreiden van het functioneel toepassingsgebied van STARTTLS in combinatie met DANE:
"STARTTLS en DANE moeten in combinatie worden toegepast op alle ontvangende en verzendende e-mailservers."

Over de standaarden

De standaarden STARTTLS en DANE worden in combinatie gebruikt om het afluisteren of manipuleren van mailverkeer tegen te gaan. STARTTLS zorgt ervoor dat e-mailservers hun onderlinge verbindingen met TLS[8] beveiligen. Met de complementaire standaard DANE kunnen e-mailservers het gebruik van TLS bovendien afdwingen zodat onveilige verbindingen worden geweigerd.

STARTTLS en DANE staan sinds september 2016 op de pas-toe-of-leg-uit-lijst. Het functioneel toepassingsgebied is thans beperkt tot inkomende mailstromen. In het Forum-advies werd destijds het volgende adoptieadvies opgenomen (punt 7 op pagina 4): "*Om een jaar na opname van de standaarden te toetsen (in samenspraak met de expertgroep) hoe het verloopt met de implementatie en of de standaard ook verplicht moet worden voor de uitgaande mailstromen.*"

Hoe is het proces verlopen?

Het Forum Standaardisatie heeft in juni 2018 besloten om de uitbreiding van het functioneel toepassingsgebied van STARTTLS en DANE voor uitgaande mailstromen in procedure te nemen. In de zomer van 2018 heeft een expertonderzoek plaatsgevonden[9] waaraan experts van Logius, NCSC, Dmarcian (private sector), NLnet Labs, VNG Realisatie, NInet en PowerDNS (private sector) deelnamen. Het expertadvies is van 6 augustus tot en met 10 september 2018 ter openbare consultatie aangeboden. In de openbare consultatie zijn in totaal zeven reacties ontvangen[10] van de heer Christian van Bruggen, RINIS, Rechtspraak.nl, de Nederlandse Zorgautoriteit, de Sociale Verzekeringsbank (SVB), het Uitvoeringsinstituut Werkgeversverzekeringen (UWV) en de Kamer van Koophandel (KvK).

Advies en gevraagd besluit

De meerderheid van de organisaties die reageerden op de openbare consultatie stemt in met het advies om het functioneel toepassingsgebied van STARTTLS en DANE uit te breiden met uitgaande e-mailservers. Een aantal organisaties deelt de volgende kritiekpunten:

- DANE laat het gebruik van *self-signed*[11] certificaten toe. Dit maakt DANE afhankelijk van DNSSEC en zou zelfs onveilig zijn.
- Er zou nog niet voldoende marktondersteuning zijn voor DANE. Met name Microsoft Exchange wordt genoemd als een product dat nog geen DANE-ondersteuning biedt voor uitgaande e-mail.
- Grotere e-mailproviders zoals Google en Microsoft ondersteunen de ontwikkeling van een alternatieve standaard, MTA STS[12].

In reactie op deze kritiekpunten laten de experts weten dat het gebruik van *self-signed* certificaten geen kwetsbaarheden introduceert. DNSSEC staat op de pas-toe-of-leg-uit-lijst en wordt door een aanzienlijk aantal domeinen in Nederland ondersteund. Er is open source software en er bestaan *add-ons* voor bestaande e-mailservers (waaronder Exchange) die DANE ondersteunen. MTA-STS is nog in ontwikkeling en heeft in het standaardontwikkelingsproces van IETF nog niet de status die DANE heeft. MTA-STS zal vooral voordelen bieden aan grote e-mai providers met uitgebreide infrastructuur, zoals Google en Microsoft. Kleinere e-mailproviders, maar ook gemeenten en overheidsorganisaties die hun eigen e-mailservers beheren, hebben juist meer baat bij DANE.

---

[8] **Transport Layer Security** (**TLS**) en diens voorganger **Secure Sockets Layer** (**SSL**), zijn encryptie-protocollen die de communicatie tussen computers (bijvoorbeeld op het internet) beveiligen.

[9] https://www.forumstandaardisatie.nl/sites/bfs/files/20180803%20Expertadvies%20STARTTLS%20en%20DANE%20uitbreiding%20functioneel%20toepassingsgebied.pdf

[10] https://www.forumstandaardisatie.nl/sites/bfs/files/Commentaar%20uit%20de%20openbare%20consultatie%20uitbreiding%20functioneel%20toepassingsgebied%20STARTTLS%20en%20DANE.pdf

[11] *Self-signed* certificaten zijn certificaten die niet zoals PKI certificaten uitgegeven zijn door een erkende autoriteit, en dus niet door een vertrouwde autoriteit geverifieerd kunnen worden. Als DNSSEC wordt gebruikt zijn *self-signed* certificaten voldoende en veel minder kostbaar dan PKI certificaten.

[12] https://datatracker.ietf.org/doc/draft-ietf-uta-mta-sts/

Gezien deze uitleg van de experts wordt geadviseerd om het functioneel toepassingsgebied van STARTTLS in combinatie met DANE uit te breiden met uitgaande e-mailservers.

Ad D. STOSAG 1.0

[Bijlage D]

Het Forum Standaardisatie wordt gevraagd om in te stemmen met het volgende advies aan het OBDO:

Verwijdering van STOSAG 1.0 van de pas-toe-of-leg-uit-lijst.

Over de standaard

STOSAG is een ICT-standaard voor digitaal container- en pasmanagement in de verwerking van afval en grondstoffen. De STOSAG-standaard beschrijft het proces van informatie-uitwisseling tussen chippas, gechipte containers, chiplezer en backoffice systemen. STOSAG 1.0 staat sinds 2011 op de pas-toe-of-leg-uit-lijst.

Hoe is het proces verlopen?

In het kader van regulier onderhoud op de pas-toe-of-leg-uit-lijst is STOSAG 1.0 in 2017 geëvalueerd door Innovalor[13]. Aanleiding voor de evaluatie was het feit dat de standaard meer dan vier jaar op de lijst staat en er vrijwel niets bekend was over de adoptiestatus van de standaard. Het evaluatierapport werd aan het Forum gepresenteerd in de vergadering van 14 maart 2018. Hierin wordt geadviseerd om STOSAG 1.0 van de pas-toe-of-leg-uit-lijst te verwijderen en te vervangen door STOSAG 2.1 als de beheerder daarom verzoekt.

Het Bureau Forum Standaardisatie heeft de Nederlandse Vereniging van Reinigingsdeskundigen (NVRD), beheerder van STOSAG, enkele maanden de gelegenheid gegeven om versie 2.1 van STOSAG aan te melden ter vervanging van STOSAG 1.0. Ondanks herhaalde contactpogingen heeft NVRD niet gereageerd. Op 13 juni 2018 stemde het Forum Standaardisatie in met het starten van de procedure ter verwijdering van STOSAG 1.0 van de pas-toe-of-leg-uit-lijst.

Het advies om STOSAG van de pas-toe-of-leg-uit lijst te verwijderen werd van 6 augustus tot en met 10 september 2018 ter openbare consultatie aangeboden. In de openbare consultatie werd een reactie ontvangen[14] van VConsyst (private partij).

Advies en gevraagd besluit

In de reactie op de openbare consultatie adviseert VConsyst om STOSAG 1.0 op de pas-toe-of-leg-uit lijst te vervangen door STOSAG 2.1. VConsyst verwacht dat NVRD, als beheerder van de standaard, deze aanmelding zelf doet. Innovalor gaf ditzelfde advies reeds in het evaluatierapport van 15 februari 2018.

NVRD reageerde niet op de openbare consultatie en heeft geen gehoor gegeven aan oproepen om STOSAG 2.1 aan te melden ter vervanging van STOSAG 1.0 op de pas-toe-of-leg-uit-lijst.

Het advies is daarom om STOSAG 1.0 van de pas-toe-of-leg-uit-lijst te verwijderen.

[13] https://www.forumstandaardisatie.nl/sites/bfs/files/FS%20180314.3A%20Evaluatie%20STOSAG%201.0.pdf

[14] https://www.forumstandaardisatie.nl/sites/bfs/files/Commentaar%20uit%20de%20openbare%20consultatie%20verwijdering%20STOSAG%201.0.pdf

Ad E. COINS

[Bijlage E]

Het Forum Standaardisatie wordt gevraagd om in te stemmen met het volgende advies aan het OBDO:

Het starten van een procedure voor beperking van het functioneel toepassingsgebied van COINS 2.0 tot alleen de grond-weg- en waterbouw.

Over de standaard

COINS is een standaard voor gegevensuitwisseling in bouwprojecten. COINS biedt een standaardformaat voor het uitwisselen van bouwinformatie die uit verschillende gerelateerde componenten bestaat. COINS wordt beheerd door het BIM Loket.

Hoe is het proces verlopen?

Het BIM Loket (https://www.bimloket.nl/) heeft COINS in april 2017 aangemeld voor de pas-toe-of-leg-uit-lijst. Er heeft een volledige toetsingsprocedure plaatsgevonden inclusief een expertbijeenkomst in september 2017 en openbare consultatie van 23februari tot en met 23 maart 2018. Aan het expertonderzoek namen Rijkswaterstaat, ProRail, de Gemeente Amsterdam, de gemeente Rotterdam, het BIM Loket en marktpartijen deel. Tijdens de openbare consultatie werd een reactie ontvangen van het ministerie van Infrastructuur en Waterstaat, maar deze bestond eerder uit vragen dan commentaar en gaven geen aanleiding tot wijziging van het expertadvies. Op basis van het expertadvies bracht het Forum Standaardisatie op 25 april 2018 een positief Forumadvies[15] uit aan het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) voor plaatsing van COINS 2.0 op de pas-toe-of-leg-uit-lijst. Het OBDO nam dit advies over in de vergadering van 25 mei 2018, waarmee COINS 2.0 op de pas-toe-of-leg-uit-lijst werd geplaatst.

Advies en gevraagd besluit

COINS 2.0 staat op de pas-toe-of-leg-uit-lijst met bouwprojecten in de gehele bouwsector als functioneel toepassingsgebied. In overleg met een aantal partijen uit de utiliteitsbouw is het BIM Loket tot inzicht gekomen dat dit functioneel toepassingsgebied te breed gedefinieerd is.

In de utiliteitsbouw zou de standaard nog moeilijk toe te passen zijn vanwege het gebrek aan marktondersteuning en expertise. Het Rijksvastgoedbedrijf diende daarom met steun van het BIM Loket en Schiphol een verzoek in om het functioneel toepassingsgebied van COINS 2.0 in te perken tot bouwprojecten in de grond, -weg- en waterbouw (GWW) waar de standaard voldoende draagvlak heeft.

Omdat het BIM Loket (de beheerder en originele aanmelder van COINS 2.0) achter dit verzoek staat, wordt geadviseerd om een procedure te starten voor aanpassing van het functioneel toepassingsgebied van COINS 2.0.

[15] https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS%20180425.3A%20Forum-advies%20COINS%202.0.pdf

Ad F. SHACL

[Bijlage F]

Het Forum Standaardisatie wordt gevraagd om in te stemmen met het volgende advies aan het OBDO:

Plaatsing van SHACL op de lijst aanbevolen standaarden.

Over de standaard

SHACL is een standaard waarmee relaties tussen en beperkingen op linked data sets kunnen worden beschreven op een voor machines leesbare manier. Je kan SHACL zien als een 'bijsluiter' op linked data die uitlegt hoe de data gestructureerd is, aan welke condities deze moet voldoen en wat er moet gebeuren als data niet aan de condities voldoet (bijvoorbeeld een foutmelding geven). SHACL biedt zo een kwaliteitscheck op linked data en helpt organisaties om elkaars linked data sets te begrijpen en integreren.

SHACL is een recent (juli 2017) gepubliceerde W3C standaard, gebaseerd op het Resource Description Framework (RDF) dat op de lijst aanbevolen standaarden staat.

Hoe is het proces verlopen?

Het Kadaster heeft SHACL aangemeld namens het Platform Linked Data Nederland (http://www.pilod.nl). Op basis van het intake-advies heeft het Forum Standaardisatie in juni 2018 besloten om SHACL in procedure te nemen. In de zomer van 2018 heeft een expertonderzoek plaatsgevonden[16] waaraan experts van het Kadaster, Kennisnet, CROW, Ordina (private sector), de Politie, Skemu (private sector), Netage (private sector) en Geonovum deelnamen. Het expertadvies is van 6 augustus tot en met 10 september 2018 ter openbare consultatie aangeboden. In de openbare consultatie zijn zes reacties ontvangen[17] van Dienst Uitvoering Onderwijs (DUO), het Kadaster, het Ministerie van Defensie, de Sociale Verzekeringsbank (SVB), het Uitvoeringsinstituut Werknemersverzekeringen (UWV) en de Kamer van Koophandel (KvK).

Advies en gevraagd besluit

Vrijwel alle reacties onderschrijven het positieve expertadvies en geven suggesties voor verdere verduidelijking of onderbouwing. Eén organisatie toont zich tegenstander van opname van SHACL op de lijst van aanbevolen standaarden. Deze organisatie stelt vraagtekens bij de toegevoegde waarde, het draagvlak, de beschrijving van het (niet verplichtende) toepassingsgebied en de mate waarin veiligheid en privacy onderzocht zijn. De reactie van deze organisatie gaat eraan voorbij dat de lijst aanbevolen standaarden niet alleen uit gangbare standaarden bestaat, maar ook beoogt om *opkomende* standaarden onder de aandacht te brengen. Het criterium 'draagvlak' (met daarin besloten 'ervaring' en 'marktondersteuning') heeft minder gewicht voor opkomende standaarden dan voor pas-toe-of-leg-uit of gangbare standaarden. Veiligheids- en privacyaspecten zijn relevant, maar verschillen in essentie niet van het publiceren van (meta)data op websites.

Gezien het positieve expertadvies en de positieve reacties van vijf van de zes overheidsorganisaties die reageerden in de openbare consultatie, alsmede het feit dat het hier niet gaat om een pas-toe-of-leg-uit verplichting, wordt er geen dwingende reden gezien om SHACL van de lijst aanbevolen standaarden te weren. Het advies is daarom om SHACL op de lijst aanbevolen standaarden te plaatsen.

[16] https://www.forumstandaardisatie.nl/sites/bfs/files/20180803%20Expertadvies%20SHACL.pdf

[17] https://www.forumstandaardisatie.nl/sites/bfs/files/Commentaar%20uit%20de%20openbare%20consultatie%20SHACL.pdf

Ad G. S/MIME

[Geen bijlage]

Het Forum Standaardisatie wordt gevraagd om in te stemmen met het volgende advies aan het OBDO:

Plaatsing van S/MIME op de lijst aanbevolen standaarden met als toepassing digitale ondertekening (maar niet de versleuteling) van e-mailberichten.

Over de standaard

S/MIME 3.2 is een standaard voor end-to-end-ondertekening en encryptie van e-mail. Daar waar extra beveiliging nodig is, kan S/MIME van toegevoegde waarde zijn in aanvulling op SPF, DKIM en DMARC. S/MIME waarborgt naast de betrouwbaarheid van de afzender namelijk ook de confidentialiteit (door encryptie) en integriteit (door digitale tekening) van de inhoud van de e-mail. S/MIME 3.2 wordt door de meeste mailapplicaties ondersteund.

Hoe is het proces verlopen?

In de vergadering van 25 april 2018 stemde het Forum Standaardisatie in met de plaatsing van S/MIME op de lijst aanbevolen standaarden. Voordat dit advies als hamerstuk kon worden voorgelegd aan het OBDO verscheen op 14 mei bericht in de media over een ernstig veiligheidsprobleem dat S/MIME raakt (zie https://efail.de/ voor details). S/MIME is daarom nog niet voorgelegd aan het OBDO.

Het gepubliceerde veiligheidsprobleem is besproken met de indiener van S/MIME (SIDN), de experts die betrokken waren bij de toetsing, en het NCSC. Deze adviseerden om S/MIME op de lijst aanbevolen standaarden te plaatsen met als toepassing digitale ondertekening van e-mail berichten, maar S/MIME niet aan te bevelen voor de versleuteling van berichten. Dit advies is ter openbare publicatie aangeboden van 6 augustus tot en met 10 september 2018. In de openbare consultatie werden in totaal vijf reacties ontvangen[18] van RINIS, het Ministerie van Defensie, de Sociale Verzekeringsbank (SVB), het Uitvoeringsinstituut Werknemersverzekeringen (UWV) en de Kamer van Koophandel (KvK).

Advies en gevraagd besluit

Drie van de vijf organisaties die reageerden op de openbare consultaties onderschrijven het advies. Twee organisaties gaven een kritische reactie, waarvan een zich uitsprak tegen het plaatsen van S/MIME op de lijst aanbevolen standaarden.

Eén organisatie is vooral bezorgd over de complexiteit en kosten van de adoptie van S/MIME en lijkt hierbij uit te gaan van een pas-toe-of-leg-uit-verplichting. Een verplichting is hier echter niet aan de orde. Het expertadvies erkent dat S/MIME kostbaar is. S/MIME wordt daarom alleen aanbevolen voor organisaties die zodanig hoge veiligheidseisen aan e-mail stellen, dat de e-mailstandaarden op de pas-toe-of-leg-uit-lijst (SPF, DKIM, DMARC, STARTTLS, DANE) onvoldoende bescherming bieden en de baten van S/MIME opwegen tegen de kosten.

Een andere organisatie verklaart alleen standaarden te willen ondersteunen die zowel *integriteit* als *vertrouwelijkheid* van e-mails waarborgen. Deze organisatie vreest ook dat de plaatsing van S/MIME op de lijst aanbevolen standaarden verkeerd geïnterpreteerd zal worden en S/MIME toch voor versleuteling van e-mail zal worden gebruikt. De organisatie zegt de voorkeur te geven aan oplossingen die zowel integriteit als vertrouwelijkheid van e-mail kunnen waarborgen, ook als deze niet op open standaarden gebaseerd zijn.

Het aanbevolen gebruik van S/MIME voor alleen digitale ondertekening van e-mail kan nadrukkelijk worden toegelicht op de website van het Forum Standaardisatie. Organisaties kunnen zelf beoordelen of S/MIME meerwaarde heeft voor digitaal ondertekenen van e-mails. Gelet op de reacties uit de expertgroep en de openbare consultatie ziet de meerderheid van de organisaties de meerwaarde van S/MIME voor digitale ondertekening van e-mail. Er geldt geen verplichting, dus geen enkele organisatie is gebonden aan het gebruik van S/MIME.

In een van de reacties op de openbare consultatie wordt gesignaleerd dat IETF binnen afzienbare tijd zal komen met een nieuwe versie van S/MIME die geen kwetsbaarheden heeft en ook (weer) voor versleuteling van e-mail geschikt is.

Geadviseerd wordt om S/MIME op de lijst aanbevolen standaarden te plaatsen voor digitale ondertekening van e-mail maar niet voor versleuteling van e-mail.

[18] https://www.forumstandaardisatie.nl/sites/bfs/files/Commentaar%20uit%20de%20openbare%20consultatie%20SMIME.pdf

Ter kennisname

Ad H. PDF/UA

[Geen bijlage]

Over de standaard

PDF/UA is een door NEN-ISO gestandaardiseerde versie van de documentindeling PDF, die voor zover mogelijk voldoet aan toegankelijkheidsrichtlijnen volgens WCAG 2.0 (de toegankelijkheidsrichtlijnen die ten grondslag liggen aan de Europese norm EN 301 549 en het *Tijdelijk besluit toegankelijkheid digitale overheid*, zie agendapunt B hierboven). Technisch gezien is PDF/UA een verzameling afspraken op het open standaardformat PDF 1.7 die het gebruik ervan zodanig inperken dat ze de digitale toegankelijkheid volgens WCAG 2.0 bevorderen.

Een andere standaard die uitgaat van PDF 1.7 is PDF/A-2 die op de pas-toe-of-leg-uit-lijst van het Forum Standaardisatie staat met duurzame toegankelijkheid (archivering) als toepassingsgebied. Eenzelfde document kan tegelijk aan de standaarden PDF 1.7, PDF/A-2 en PDF/UA voldoen en kan dus zowel duurzaam toegankelijk als digitaal toegankelijk zijn. Dit impliceert overigens niet dat PDF/UA en PDF/A-2 volledig compatibele specificaties zijn.

Hoe is het proces verlopen?

Het kenniscentrum Digitoegankelijk (https://www.digitoegankelijk.nl/) van Logius heeft PDF/UA in april 2018 aangemeld voor plaatsing op de pas-toe-of-leg-uit-lijst. Op basis van het intake-advies heeft het Forum Standaardisatie in juni 2018 besloten om PDF/UA in procedure te nemen. In de zomer van 2018 heeft een expertonderzoek plaatsgevonden[19] waaraan experts van de Gemeente Zeewolde, Justid, Tweede Kamer der Staten-Generaal, Firm Ground (private sector), VNG Realisatie, Logius, de Nederlandse Zorgautoriteit en het Nationaal Archief deelnamen.

Het expertadvies is van 6 augustus tot en met 10 september 2018 ter openbare consultatie aangeboden. In de openbare consultatie zijn in totaal dertien reacties ontvangen[20] van de heer van Hoytema, de Koninklijke Bibliotheek, de Belastingdienst, Adobe Systems Benelux, de Nederlandse Zorgautoriteit, het Ministerie van Defensie, het Ministerie van Infrastructuur en Waterstaat, de Rijksdienst voor het Wegverkeer, de Sociale Verzekeringsbank (SVB), het Uitvoeringsinstituut Werkgeversverzekeringen (UWV), de Autoriteit Consument en Markt (ACM), de Kamer van Koophandel (KvK) en de Justitiële Informatiedienst.

Reacties op de openbare consultatie en advies

De meeste organisaties die reageerden op de openbare consultatie spreken hun zorgen uit over plaatsing van PDF/UA op de pas-toe-of-leg-uit lijst. De meest genoemde argumenten tegen opname van PDF/UA op de pas-toe-of-leg-uit-lijst zijn de volgende:

- Er is nog te weinig marktondersteuning voor de creatie van PDF/UA documenten, met name in gangbare kantoorapplicaties. Overheidsorganisaties hebben nog vrijwel geen ervaring met PDF/UA. Een verplichting van PDF/UA zou daarom praktisch onuitvoerbaar zijn.
- PDF/UA is geen noodzakelijke PDF-standaard om aan de wettelijke toegankelijkheidseisen te voldoen. Andere PDF standaarden zoals PDF/A-1 (die al op de pas-toe-of-leg-uit-lijst staat) kunnen ook toegankelijk zijn.
- Er zou een technisch conflict bestaan tussen de PDF/A-2 en PDF/UA specificaties, die beiden inperkingen zijn van het PDF 1.7 open standaardformat. Dit betekent dat er PDF/UA documenten bestaan die technisch niet kunnen voldoen aan PDF/A-2. Dit levert een probleem op voor functionele toepassingsgebieden waarin zowel duurzame toegankelijkheid als digitale toegankelijkheid een eis zijn.

Deze punten zijn van dusdanige relevantie dat aanvullend onderzoek nodig is om te bepalen of PDF/UA voldoende toegevoegde waarden en draagvlak heeft voor plaatsing op de pas-toe-of-leg-uit-lijst. Bij het aanvullend onderzoek worden naast de experts ook de organisaties betrokken die kritisch reageerden op de openbare consultatie.

[19] https://www.forumstandaardisatie.nl/sites/bfs/files/20180803%20Expertadvies%20PDF-UA.pdf

[20] https://www.forumstandaardisatie.nl/sites/bfs/files/Commentaar%20uit%20de%20openbare%20consultatie%20PDF-UA.pdf