notitie

FORUM STANDAARDISATIE 9 oktober 2019
Agendapunt 5 Open standaarden, adoptie

Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	9 okotober 2019
Versie:	1.0
Bijlagen:	B. Meting Informatieveiligheidsstandaarden medio 2019 C1. Brief SLM Rijk aan Microsoft inzake "Gebruik DANE en DNSSEC" C2. Brief Bureau Forum Standaardisatie aan Microsoft met aanvullende informatie inzake verplichting en achtergrond DANE en DNSSEC D. Overzicht agenderen Monitor en IV-meting door Forum-leden E. Overzicht Kamerstukken m.b.t. Forum Standaardisatie en open standaarden
Opsteller:	Bart Knubben
Meelezer(s):	Han Zuidweg

Samenvatting

Ter bespreking

A. Presentatie resultaten Monitor Open Standaarden door Jaap Korpel (ICTU)
B. Presentatie resultaten IV-meting medio 2019 door Robin Gelhard (BFS)
C. Brief aan Microsoft over support DNSSEC en DANE op Office365
D. Agenderen Monitor Open Standaarden en IV-meting door Forumleden

Ter kennisname

E. Kamerstukken m.b.t. Forum Standaardisatie en open standaarden
F. Consultatie “Besluit beveiligde verbinding met overheidswebsites en -webapplicaties”
G. API’s
H. Open documentstandaarden
    a. Best practices voor digitaal toegankelijk publiceren
    b. Webapplicatie voor validatie van digitale toegankelijkheid
    c. “Overheid, stop met PDF” - blog van de Open State Foundation in iBestuur
I. Moderne, betrouwbare internetstandaarden
    a. Ontwikkelingen Internet.nl
    b. Bijeenkomsten Platform Internetstandaarden en Betrouwbare OverheidsMail
    c. Presentaties
J. Overig nieuws en ontwikkelingen

Ter bespreking

Ad A. Presentatie Monitor Open Standaarden door Jaap Korpel (ICTU)

Ieder Forum-lid wordt gevraagd om:

kennis te nemen van en te reflecteren op de concept-resultaten van de monitor open standaarden. De ontvangen input zal worden gebruikt voor de afronding van de monitor-rapportage en voor de nadere analyse die zijn weerslag zal krijgen in de notitie "duiding en maatregelen".

Toelichting

De hoofdonderzoeker van de Monitor Open Standaarden geeft een presentatie van de eerste resultaten op hoofdlijnen. De presentatie is een preview. Het rapport is ten tijde van de oktobervergadering nog onder constructie en het eerste formele concept wordt behandeld in de decembervergadering ter besluitvorming, met de begeleidende notitie "duiding en maatregelen", die het standpunt van het Forum Standaardisatie hierop moet weergeven. Op 11 december 2019 wordt uw formele goedkeuring ter afronding van de onderzoeksopdracht gevraagd en uw goedkeuring en aanvullingen op het standpunt van het Forum die geformuleerd wordt in de notitie "duiding en maatregelen".

Daarnaast mag u in de decembervergadering een notitie verwachten over gesprekken die gevoerd zijn over raamovereenkomsten. Raamovereenkomsten zijn in de Monitor Open Standaarden gesignaleerd als problematisch als het gaat om het meten en beoordelen van het correct vragen naar de relevante open standaarden in aanbestedingen. Vaak gebeurt dit niet, of niet specifiek genoeg. Maar raamovereenkomsten bieden wellicht ook adoptiekansen. Meer hierover in december 2019.

Ad B. Presentatie meting informatieveiligheidsstandaarden medio 2019 door Robin Gelhard (BFS)

[bijlage B]

Ieder Forum-lid wordt gevraagd om:

kennis te nemen van en te reflecteren op de resultaten van de Meting Informatieveiligheidsstandaarden medio 2019. Op basis van de ontvangen input kunnen nadere acties worden bepaald om achterblijvende overheden, die de open standaarden waarvoor implementatieafapraken gelden nog niet in gebruik hebben, in beweging te krijgen.

Toelichting

Bijgevoegd vindt u de resultaten uit de Meting Informatieveiligheidsstandaarden van september 2019. Aan het Forum wordt gevraagd om kennis te nemen van de resultaten uit de meting en de resultaten in de achterban onder de aandacht brengen, met name bij de achterblijvers. Afstemming over de resultaten vind nog plaats via de koepelorganisaties, na afstemming zal het rapport definitief worden gemaakt en aan het OBDO worden verzonden.

De meting heeft betrekking op een aantal informatieveiligheidsstandaarden waarvoor, in aanvulling op 'pas toe of leg uit', overheidsbrede streefbeeldafspraken met uiterlijke implementatiedata zijn gemaakt door het Nationaal Beraad en door het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO).

Eind 2019 loopt de deadline van de derde overheidsbrede streefbeeldafspraak af. Deze streefbeeldafspraak gaat over het implementeren van STARTTS en DANE (om vertrouwelijkheid van mailverkeer te borgen) en het voldoende strikt configureren van SPF en DMARC (om mailspoofing

tegen te gaan). In het afgelopen half jaar is de adoptiegraad van deze standaarden met gemiddeld 5% gegroeid. Daarmee ligt het groeitempo iets lager dan dat van de vorige meting, waar we nog 7% groei zagen.

Specifiek ten aanzien van de derde streefbeeldafspraak is het gebruik van STARTTLS voor beveiligde mailverbindingen gegroeid met 3% naar 97%. Het gebruik van STARTTLS conform de NCSC richtlijnen is gegroeid met 9% naar 76%. Het gebruik van DANE voor het afdwingen van met STARTTLS beveiligde mailverbindingen bij het ontvangen van mail is gegroeid met 4% naar 45%. En tot slot is het toepassen van DMARC met strikte policy om mailspoofing tegen te gaan gegroeid met 12% naar 49%.

In algemene zin is gebruik van de informatieveiligheidstandaarden het afgelopen jaar wederom gegroeid. De webstandaarden worden gemiddeld beter toegepast dan de mailstandaarden (92% vs 77%). Waar de gemiddelde groei in gebruik van mailstandaarden in de vorige meting nog hoger was dan dat van de webstandaarden, is deze inmiddels gelijk met ongeveer 3% ten opzichte van een half jaar geleden.

Meest opvallende resultaten uit deze meting zijn de groei in gebruik van webstandaarden bij het Rijk, en de achteruitgang in toepassing van DNSSEC op mailservers.

Het Rijk heeft een flinke inhaalslag gemaakt met betrekking tot de standaarden voor het versleutelen van webverkeer (HTTPS en HSTS). Dit komt doordat een aantal doorverwijzende domeinen (redirects) van de ministeries recent voorzien zijn van HTTPS. Het gaat om domeinen die voornamelijk voor mail worden gebruikt, waar geen website op gehost wordt, maar die doorverwijzen naar een ander domein. Bijvoorbeeld minbzk.nl dat doorverwijst naar www.rijksoverheid.nl.

De oorzaak van de neerwaartse trend in toepassing van DNSSEC op mailservers (een randvoorwaarde voor DANE) is dat een aantal provincies en gemeenten de overstap naar Microsoft Office 365 Exchange Online heeft gemaakt. Dit product biedt vooralsnog geen ondersteuning voor DNSSEC en DANE. Dit is een duidelijk zorgpunt voor de vertrouwelijkheid van overheidsmail, omdat deze overheidsorganisaties niet altijd een versleuteld mailtransport kunnen afdwingen en tevens niet aan de streefbeeldafspraak omtrent het gebruik van DANE kunnen voldoen. Desondanks groeit het gebruik van DANE overheidsbreed nog steeds, en zien we bij het Rijk al een adoptiegraad van 75%.

Ad C. Brief aan Microsoft over support DNSSEC en DANE op Office365

[bijlagen C1 en C2]

Ieder Forum-lid wordt gevraagd om:

kennis te nemen van de correspondentie met Microsoft, en dit punt te bespreken in relatie tot agendapunt B.

Toelichting

Strategisch Leveranciersmanagement Microsoft Rijk (SLM Microsoft Rijk) heeft op 31 juli 2019 de brief "Gebruik DANE en DNSSEC" naar Microsoft gestuurd met daarin het formele verzoek voor ondersteuning van DNSSEC en DANE op Office365 Exchange Online. In aansluiting op dit gesprek heeft Bureau Forum Standaardisatie op verzoek van Microsoft aanvullende informatie aangeleverd over het beleid van de Nederlandse overheid m.b.t. DNSSEC en DANE (d.d. 30 August 2019 met als onderwerp "Information on Dutch government's position on DNSSEC and DANE (for secure mail transport)"). Microsoft heeft inmiddels laten weten dat ze begin oktober met een antwoord zullen komen waarin tijdslijn voor ondersteuning terugkomt.

SLM Microsoft Rijk voert namens het Rijk onderhandelingen met Microsoft ten aanzien van de voorwaarden, risico’s en kosten van de producten en diensten. SLM Rijk is belegd binnen het ministerie van Justitie en Veiligheid. Afgelopen jaar heeft SLM Rijk onder andere verschillende onderzoeken naar de privacy van Microsoft producten en diensten laten uitvoeren.

Zie: https://www.rijksoverheid.nl/documenten/publicaties/2018/11/12/strategisch-leveranciersmanagement-microsoft-rijk-slm-microsoft en https://www.rijksoverheid.nl/documenten/publicaties/2018/11/12/strategisch-leveranciersmanagement-microsoft-rijk-slm-microsoft

Ad D. Agenderen Monitor en IV-meting door Forum-leden

[bijlage D]

Ieder Forum-lid wordt gevraagd om:

een update te geven over het verspreiden en agenderen van de monitor Open Standaarden en IV-meting onder zijn/haar achterban.

Toelichting

1. De leden van het Forum Standaardisatie hebben afgesproken dat ieder Forum-lid de Monitor Open Standaarden 2018 en de laatste meting informatieveiligheidsstandaarden (hierna: IV-meting) actief onder de aandacht brengt bij zijn/haar eigen achterban.
2. Daarnaast hebben de leden van het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) op 12 februari ingestemd om de Monitor Open Standaarden en de IV-meting te agenderen in hun organisatie en hun achterban, inclusief verschillende gremia waar beleid wordt ontwikkeld met een sterke ICT-component. Daarnaast stemden zij in met het aansturen op het opnemen van eventuele 'leg uit' in het jaarverslag van hun organisatie dan wel de jaarverslagen van hun achterban.

De laatste digitale magazines over de Monitor Open Standaarden en de IV-meting vindt u op https://magazine.forumstandaardisatie.nl/.

In het voorliggende overzicht vindt u een overzicht van de huidige stand van zaken voor zover bekend en de gremia waarin de Monitor Open Standaarden en IV-meting (kunnen) worden besproken.

Ter kennisname

Ad E. Kamerstukken m.b.t. Forum Standaardisatie en open standaarden
[bijlage E]

Het Bureau Forum Standaardisatie heeft via Officiële Bekendmakingen een abonnement op de zoekvragen "Forum Standaardisatie" en "open standaarden". Op basis hiervan, krijgt het Forum Standaardisatie vier keer per jaar een overzicht.

De bijlage bevat het overzicht over de periode juni tot en met september 2019 (Q3)

Ad F. Consultatie besluit "Beveiligde verbinding met overheidswebsites en -webapplicaties"

Op 2 september is de internetconsultatie van het ontwerpbesluit "Beveiligde verbinding met overheidswebsites en –webapplicaties" van start gegaan (zie: https://www.internetconsultatie.nl/overheidswebsites/). Met dit besluit wordt de toepassing van de informatieveiligheidsstandaarden HTTPS en HSTS verplicht voorgeschreven voor publiek toegankelijke websites en webapplicaties van bestuursorganen.

Tegelijkertijd met de openbare consultatie is het ontwerpbesluit voor advies aangeboden aan de Autoriteit Persoonsgegevens en de commissie Regeldruk. De internetconsulatie loopt tot 20 oktober 2019. Daarna worden de consulatiereacties en ontvangen adviezen verwerkt.

Vervolgens zal het ontwerpbesluit worden aangeboden aan de Ministerraad en Raad van State. Daarvoor geldt dat eerst de onderliggende wet Digitale Overheid door de Tweede Kamer goedgekeurd dient te zijn.

Op het moment dat de wettelijke verplichting voor HTTPS en HSTS van kracht is, kunnen beide standaarden van de 'pas toe of leg uit'-lijst worden verwijderd. Forum Standaardisatie blijft het gebruik van de standaarden wel periodiek toetsen als onderdeel van de halfjaarlijkse IV-meting.

Ad G. API's

Op 15 juli 2019 heeft het Kennisplatform APIs de API Strategie voor de overheid formeel gepubliceerd. In deze versie zijn de reacties verwerkt die binnen kwamen tijdens de openbare consultatie van de API Strategie in februari en maart van dit jaar. Bureau Forum Standaardisatie heeft een substantiële bijdrage geleverd aan het hoofdstuk 2 over Communicatie een Beleid (zie: https://docs.geostandaarden.nl/api/API-Strategie/#communicatie-en-beleid). BFS stemt de bijdrage aan het Kennisplatform APIs af met de begeleidingsgroep APIs van minBZK en VNG Realisatie.

De API Strategie schrijft het gebruik voor van de open standaarden OAuth voor beveiliging en Open API Specification (OAS) voor documentatie van APIs. OAS staat op 'pas toe of leg uit'-lijst en voor OAuth wordt een overheidsprofiel verplicht (zie: https://docs.geostandaarden.nl/api/oauth/). Kennisplatform APIs heeft besloten om alle normatieve design principes van de API Strategie aan te melden voor de 'pas toe of leg uit'-lijst. Logius heeft toegezegd dit normatieve deel van de API Strategie in beheer te nemen en minBZK DIO heeft de financiering van het beheer voor minstens 3 jaar toegezegd.

In het najaar gaat ICTU in opdracht van Bureau Forum Standaardisatie een onderzoek uitvoeren naar het gebruik van Open API Specification (OAS) die nu ruim een jaar op de 'pas toe of leg uit'-lijst staat. Dit onderzoek levert een nulmeting op die een oriëntatie geeft voor de adoptieondersteuning van OAS en ook gebruikt zal worden voor de Monitor open standaarden.

Ad H. Opendocument-standaarden

a. Best practices voor digitaal toegankelijk publiceren
In de vergadering van juni 2019 besloot het Forum Standaardisatie meer te gaan inzetten op 'best practices' voor digitaal toegankelijk publiceren. In juli heeft het Bureau Forum Standaardisatie een begin gemaakt met de inventarisatie van zulke 'best pracices' door een informeel te organiseren met KOOP en het Nationaal Archief. In het najaar zal deze inventarisatie worden voortgezet, en zullen gesprekken plaatsvinden met organisaties als Platform Rijksoverheid Online (PRO), Koninklijke Bibliotheek, NVWA, RCE en de Tweede Kamer. Bob van Engelen, rijks-trainee bij BFS van september 2019 tot maart 2020, zal hieraan een belangrijke bijdrage leveren.

De intentie is om de meest bruikbare 'best practices' te presenteren in de jaarlijkse workshop over documentstandaarden en digitale toegankelijkheid die BFS in november organiseert.

b. Webapplicatie voor validatie van digitale toegankelijkheid
Bureau Forum Standaardisatie krijgt een substantiële bijdrage van het NL DIGIbeter Innovatiebudget om een open source webapplicatie te laten bouwen die de digitale toegankelijkheid van PDF bestanden valideert. Bij de overheid bestaat grote behoefte aan dit soort ondersteuning voor digitale toegankelijkheid, waar de markt nog niet serieus in gesprongen is. Door de software als open source te ontsluiten krijgt de markt een kans om de applicatie verder te ontwikkelen en te commercialiseren.

Op dit moment onderzoekt Bureau Forum Standaardisatie met de afdelingen Sourcing, Legal en Inkoop van Logius hoe dit project administratief en juridisch het beste kan worden opgezet. De verwachting is dat de uitvoering van het project in het najaar gestart kan worden.

c. "Overheid, stop met PDF" - blog van de Open State Foundation in iBestuur
In augustus publiceerde Tom Kunzler van de Open State Foundation een blog in iBestuur met de titel "Overheid, stop met PDF" (Zie: https://ibestuur.nl/weblog/overheid-stop-met-pdf-bestanden). In het artikel roept hij de Nederlandse overheid op om naar voorbeeld van het Verenigd Koninkrijk minder PDF te gebruiken voor het publiceren van informatie online. In zijn blog onderbouwt Tom waarom open bestandsformats zoals HTML en CSV vaak geschikter zijn voor online informatie.

Naar aanleiding van dit artikel heeft minBZK DIO met input van het Forum Standaardisatie een notitie opgesteld aan de Staatssecretaris waarin de achtergrond en mogelijke reactie worden beschreven. Op grond van dit advies heeft de Staatsecretaris Gé Linssen gevraagd om per e-mail direct te reageren naar de Open State Foundation. In het antwoord van Gé staat:

"Graag bericht ik dat de Staatssecretaris akkoord is met een verzoek aan het Forum Standaardisatie om een handreiking op te stellen met 'beste overwegingen' voor verschillende situaties van publiceren, zodat overheidsorganisaties aan de voorkant van hun publicatieproces daar 'by design' rekening kunnen houden. De rol en voordelen van HTML en CSV - en juist andere standaarden dan PDF - zouden daar goed voor het voetlicht kunnen komen. Het Forum Standaardisatie heeft deze zomer al een initiatief gestart met andere organisaties, zoals KOOP en het Nationaal Archief, om kennis over praktijken en ervaringen bij elkaar te brengen. De Staatssecretaris vraagt FS nu om daarbij gericht toe te werken naar een handreiking.

De vraag van de staatssecretaris aan het Forum zal één dezer dagen, met enige toelichting en motivatie, op https://www.digitaleoverheid.nl/ worden gemeld."

Deze lijn van actie komt overeen met wat in de vergadering van het Forum Standaardisatie in juni (agendapunt 5A) besproken is en wordt opgenomen in het werkplan van 2020. Bob van Engelen, Rijkstrainee bij het Bureau Forum Standaardisatie van september 2019 tot maart 2020, is reeds begonnen invulling te geven aan de genoemde handreiking.

Ad I. Moderne, betrouwbare internetstandaarden

a. Ontwikkelingen Internet.nl

- De volgende versie Internet.nl, die gepland staat voor het 4de kwartaal van 2019, zal gaan testen op basis van de nieuwe TLS-richtlijnen van NCSC (d.d. 23 april 2019). Dit betekent dat de test strenger gaat worden. Het gaat met name om de testcategorieen "HTTPS" in de websitetest en "STARTTLS en DANE" in de e-mailtest.

- Sinds kort is er een Internet.nl-dasboard beschikbaar waarmee eenvoudig webbased bulkmetingen voor meerdere domeinnamen kunnen worden uitgevoerd. Toegang staat momenteel open voor non-profits en overheden. Forum Standaardisatie gebruikt het dashboard ook voor de IV-metingen. Tijdens de Internet.nl-API-gebruikersbijeenkomst op 13 september kregen verschillende gebruikers hands-on training.

b. Bijeenkomst Platform Internetstandaarden en Betrouwbare OverheidsMail

- Op 12 september vond een bijeenkomst van Platform Internetstandaarden plaats. De bijeenkomst werd geopend door gastheer Ronald Roosdorp (MT-lid bij de directie Digitale Economie van ministerie van EZK). Op de agenda stonden o.a. twee gastsprekers, namelijk Carl Gahnberg van Internet Society over "Consolidation in the Internet Economy" (https://future.internetsociety.org/2019/) en Michel Verhagen van Digital Trust Center.
- Op 9 september vond een bijeenkomst plaats van het overleg Betrouwbare OverheidsMail (https://bom.pleio.nl/). Op de agenda stonden onder andere presetaties door de gemeente Amsterdam over hun aanpak en ervaringen met mailbeveiligingsstandaarden, en door Forum Standaardisatie over de laatste IV-meting.

c. Presentaties

- EuroDIG (20 jun), Larissa Zegveld en Gerben Klein Baltink over Nederlandse aanpak mbt adoptie van moderne internetstandaarden, https://www.eurodig.org/
- Webinar over DANE (2 sep) met Bart Knubben, https://www.onlineseminar.nl/sidn/webinar/27663/dane/
- OneConference (1-3 okt), https://one-conference.nl/
    - "How to Detect that Your Domains are Being Abused for Phishing by Using DNS" (Karl Lovink - Belastingdienst, Arnold Hölzel),
    - "Current State and Development of DNS Security and Privacy" (Gerben Klein Baltink, Marco Davids, Bert Hubert, Ralph Dolmans)
    - "The Pursuit of Better E-mail Security at de Tweede Kamer" (Robert Krenn, Bart Knubben)
- IPv6-bijeenkomst (4 okt) i.s.m. VNG en Logius: Larissa Zegveld en Gerben Klein Baltink
- 6Projects over Internet.nl / Platform Internetstandaarden, https://6projects.nl/
- Logius international seminar (19 nov) over 'Prevention by improving email security', https://www.logius.nl/logius-international-seminar-2019

Ad J. Overig nieuws en ontwikkelingen

- "Waar is de wet?", Marc van Opijnen, over (on-)herkenbaarheid van overheidsdomeinnamen: https://ibestuur.nl/weblog/waar-is-de-wet
- "De ICT-cliffhangers van minister Bruno Bruins", Jan Jacobs, over ICT-standaarden in de zorg: https://www.smarthealth.nl/2019/08/22/brief-ict-cliffhangers-bruno-bruins/
- Open Geodag | SDI.Next op 2 oktober: https://www.geonovum.nl/over-geonovum/agenda/open-geodag-sdinext
- Consultatie NEN 3610 Linked Data Profiel: https://www.geonovum.nl/over-geonovum/actueel/consultatie-nen-3610-linked-data-profiel
- "Extended validation certificates are really dead": https://www.troyhunt.com/extended-validation-certificates-are-really-really-dead/
  Toelichting: Vanaf versie 77 van Google Chrome browser (vanaf 10 september) en Firefox 70 (22 oktober) is het visuele onderscheid van een EV-certificaat niet meer te zien voor een gebruiker. In de Apple Safari browser was dit al niet het geval, en ook niet op mobiele browsers. Microsoft lijkt ook te volgen met haar Edge-browser. Concreet betekent dit dat de bedrijfsnaam van de eigenaar van het certificaat niet meer zichtbaar is in browsers, net als dat bij 'normale', niet EV-certificaten het geval is. Daarmee verdwijnt 1 van de redenen om een EV-certificaat te gebruiken: de communicatieve mogelijke meerwaarde van het zien van de bedrijfsnaam.