



notitie

FORUM STANDAARDISATIE 6 mei 2020

Agendapunt 4 Open standaarden, adoptie

Nummer: FS20200506.4

Aan: Forum Standaardisatie

Van: Stuurgroep Open Standaarden

Datum: 6 mei 2020

Versie: 1.0

Bijlagen: A. IV-meting onder leden Forum
B. Agendering IV-meting en Monitor en sponsoring door Forum-leden + aanwezigheid
C. Recente voorbeelden spoofing
D1. Analyse van de Monitor Open Standaarden 2019
D2. Notitie n.a.v. de gesprekken met betrokkenen bij onderzochte aanbestedingen en voorzieningen
G. Brief van SLM Rijk en Forum Standaardisatie aan Microsoft d.d. 20-03-2020

Opsteller: Bart Knubben (met dank aan Annemieke Toersen, Désirée Castillo Gosker, Han Zuidweg en Robin Gelhard)

Meelezer: Han Zuidweg

Samenvatting

Ter besluitvorming en bespreking

- A. IV-meting onder leden Forum (voorbeeldfunctie)
- B. Agendering IV-meting en Monitor, sponsorschap door Forum-leden, en aanwezigheid
- C. Recente voorbeelden spoofing

Ter kennisname

- D. Monitor open standaarden
- E. Documentstandaarden
- F. API's
- G. Internet- en beveiligingstandaarden
- H. Standaarden voor e-facturatie en administratie
- I. Overig

Ter besluitvorming en bespreking

Ad A. IV-meting onder leden Forum (voorbeeldfunctie)

[bijlage A]

Aan ieder Forum-lid wordt gevraagd om:

- de eigen organisatie aan te sporen om de verplichte moderne internetstandaarden te implementeren;
- aan te geven wat eventuele knelpunten zijn voor adoptie binnen de eigen organisatie.

Toelichting

Forum Standaardisatie stimuleert de toepassing van moderne internetstandaarden om zo onder meer cybercriminaliteit te voorkomen. Het Forum Standaardisatie en de Forumleden zelf dienen bij de toepassing van de verplichte standaarden het goede voorbeeld te geven.

Bijlage A toont in hoeverre belangrijke e-maildomeinen en webdomeinen van de organisaties waar Forumleden werkzaam zijn, of vanuit e-mailen, voldoen aan internetstandaarden van de lijst verplichte standaarden. Peildatum is 16 april 2020.

De meting toont aan dat het mogelijk is om een 100% score te halen op zowel de web- als de e-mailtest. De geaggregeerde resultaten zijn vergelijkbaar met die van de meest recente overheidsmeting; de uitdaging ligt met name bij de e-mailstandaarden, en meer specifiek bij een voldoende strikt DMARC beleid om spoofing te voorkomen, en het toepassen van DANE voor e-mailversleuteling.

Ad B. Agendering IV-meting en Monitor, sponsorschap door Forum-leden, en aanwezigheid

[bijlage B]

Ieder Forum-lid wordt gevraagd om:

1. een update te geven over het verspreiden en agenderen van de monitor Open Standaarden en IV-meting onder zijn/haar achterban;
2. een update te geven over hun sponsorschap;
3. kennis te nemen van het overzicht van de aanwezigheid.

Toelichting

1. In de bijlage treft u een overzicht aan van de huidige stand van zaken (voor zover bekend) met betrekking tot de verspreiding en agendering van de Monitor Open Standaarden en laatste meting informatieveiligheidsstandaarden (hierna: IV-meting).
 - a. De leden van het Forum Standaardisatie hebben afgesproken dat ieder Forum-lid de Monitor Open Standaarden en IV-meting actief onder de aandacht brengt bij zijn/haar eigen achterban. De laatste digitale magazines over de Monitor Open Standaarden en de IV-meting vindt u op <https://magazine.forumstandaardisatie.nl/>.
 - b. Daarnaast hebben de leden van het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) op 18 maart 2020 herbevestigd 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. Tevens herbevestigden zij aan te sturen op het opnemen van eventuele 'leg uit' in het jaarverslag van hun organisatie dan wel de jaarverslagen van hun achterban.
2. De Forum-leden zijn ook sponsor van een of meerdere Forum-onderwerpen, eveneens weergegeven in bijgaand overzicht.
3. Tevens wordt een overzicht gegeven van de aanwezigheid van de Forum-leden sinds 13 juni 2018.

Ad C. Recente voorbeelden spoofing

[bijlage C]

Aan het Forum wordt gevraagd om:

- kennis te nemen van recente incidenten en nieuws m.b.t. e-mailspoofing;
- te bespreken hoe meer urgentie kan worden gegeven aan het proactief toepassen van anti-spoofingstandaarden (voordat incidenten plaatsvinden);
- te bespreken hoe de herkenbaarheid van de overheid online kan worden vergroot zodat burgers phishing kunnen doorzien.

Toelichting

Twee manieren om schade door phishing te voorkomen zijn:

- 1) door als organisatie anti-spoofingstandaarden toe te passen om te voorkomen dat de eigen domeinen worden misbruikt, en
- 2) door bewustwording te creëren onder gebruikers hoe zij phishing kunnen herkennen.

Forum Standaardisatie rapporteert al enkele jaren halfjaarlijks middels de Meting Informatieveiligheidsstandaarden welke belangrijke overheidsdomeinen niet voldoen aan standaarden die e-mailspoofing voorkomen (DMARC, DKIM en SPF). Ook wijst het bureau Forum Standaardisatie organisaties individueel op het niet toepassen van standaarden. In april kwamen het RIVM en Rijksoverheid.nl in het [nieuws](#) omdat zij geen strikte DMARC policy toepasten. Binnen enkele uren na melding door de journalist was een strikt DMARC policy toegepast. Media-aandacht lijkt in bepaalde gevallen meer urgentie te creëren dan de signaleringen door Forum Standaardisatie.

Om phishing te kunnen herkennen moet impliciet herkenbaar zijn wat wél authentiek is. De overheid maakt herkenbaarheid zelf lastiger door internetdomeinen schijnbaar als wegwerpartikelen te zien. Door onvoldoende regie is een wildgroei aan internetdomeinen ontstaan. Zo heeft alleen de rijksoverheid (voor zover bekend) al meer dan 8000 internetdomeinen. De overheid lijkt onvoldoende oog te hebben voor de risico's die daarmee ontstaan.

Onduidelijkheid over de authenticiteit van internetdomeinen ondermijnt tevens het vertrouwen van burgers in echte overheidswebsites/-mails. Eén van de uitgangspunten van overheidscommunicatie is dat de overheid, ongeacht het kanaal of medium, herkenbaar is als afzender. Er ligt dus een uitdaging om verstandiger om te gaan met internetdomeinen om zo de herkenbaarheid van de overheid te vergroten.

Bijlage C legt de relatie tussen herkenbaarheid van de overheid op internet en de spoofingproblematiek, en illustreert deze met recente voorbeelden van spoofing van de overheid.

Ter kennisname

Ad D. Monitor open standaarden

[bijlage D1 en D2]

1. Analyse van de Monitor Open Standaarden 2019:
Het gaat hier om een analyse van de onderzoeksresultaten van de Monitor Open Standaarden 2019 met betrekking tot een aantal grote overheidsorganisaties. Deze analyse zal in het Magazine van de Monitor Open Standaarden terugkomen.
2. Gespreksnotities ICTU n.a.v. onderzochte aanbestedingen en voorzieningen:
Notitie over de gesprekken die gevoerd zijn naar aanleiding van de Monitor Open Standaarden van 2018 en 2019 met betrokkenen bij de onderzochte aanbestedingen en beheerders van de onderzochte voorzieningen. In deze notitie heeft Jaap Korpel, hoofdonderzoeker bij ICTU thematisch een aantal interessante uitspraken verzameld. Deze notitie zal gebruikt worden als input voor het onderzoek "Knelpunten voor adoptie" dat nog voor de zomer van 2020 verwacht wordt te zijn afgerond.

Ad E. Documentstandaarden

- Het onderzoek naar praktijkcases voor digitaal toegankelijk publiceren is eind februari afgerond. Tussen september en december vorig jaar heeft rijkstrainee Bob van Engelen 17 overheidsorganisaties geïnterviewd over hun aanpak van digitale toegankelijkheid. BFS heeft daar vijf organisaties uitgelicht die verschillen in taken en omvang, en digitale toegankelijkheid op hun eigen manier met variërend succes benaderen. Het [online rapport](#) laat zien welke lessen er geleerd kunnen worden van de Inspectie van het Onderwijs, DUO, de Algemene Rekenkamer, de gemeente Tilburg en Geonovum. Dit rapport is bedoeld voor brede verspreiding en er zal ook een opgemaakte en gedrukte versie van gemaakt worden.
- Bureau Forum Standaardisatie geeft de OpenState Foundation opdracht een richtlijn te produceren die overheden helpt het meest passende bestandsformaat te gebruiken afhankelijk van het doel en de doelgroep van de gepubliceerde informatie. De richtlijn moet organisaties helpen bepalen welke bestandsformaten in verschillende situaties het meest aangewezen zijn om informatie vindbaar, open, digitaal toegankelijk en herbruikbaar te publiceren. Hierin wordt ook 'nevenschikking' besproken: het aanbieden van informatie in meer dan één format voor verschillende doelen. Ook wordt aan de hand van een aantal voorbeelden uit de praktijk beschreven hoe het niet moet en hoe het wel moet.
- De Pleio community-website die BFS beheert voor digitaal toegankelijk publiceren heet voortaan digitaaltoegankelijk.pleio.nl. De oude naam opendocumentstandaarden.pleio.nl paste eigenlijk niet omdat deze site zich vooral richt op het publiceren van digitaal toegankelijke informatie van de overheden. De oude URL <https://opendocumentstandaarden.pleio.nl> blijft voorlopig nog wel werken, maar we raden aan om de nieuwe URL <https://digitaaltoegankelijk.pleio.nl> met uw contacten te delen. Verder hebben we de community-website zelf wat vereenvoudigd. Pleio heeft de digitale toegankelijkheid van het platform inmiddels sterk verbeterd, maar er blijven nog enkele aanpassingen nodig. BFS helpt de Stichting Pleio om de laatste puntjes op de 'i' te zetten en het platform honderd procent digitaal toegankelijk te maken.
- Larissa Zegveld zou op 14 april voor een RADIO een webinar geven over digitale toegankelijkheid, met medewerking van Raph de Rooij (beleidsverantwoordelijke digitale toegankelijkheid bij minBZK) en Han Zuidweg (dossierhouder en expert digitale toegankelijkheid bij BFS). Door de situatie rondom COVID-19 is dit webinar uitgesteld, maar de intentie is om dit nog voor de zomer te laten doorgaan als de situatie het toelaat.

Ad F. API's

- Op 4 maart 2020 organiseerde het Kennisplatform APIs in samenwerking met Forum Standaardisatie en andere organisaties een bijeenkomst over APIs. De bijeenkomst had een recordaantal van rond de 160 inschrijvingen. Na de publicatie van de API Strategie voor de overheid en de API Design Rules in 2019 hebben de werkgroepen zich gereorganiseerd naar de behoeften voor 2020. In de bijeenkomst van 4 maart 2020 presenteerden de nieuwe werkgroepen zich, en was er ruimte voor discussie over het werk dat nog aan de API Strategie

moet gebeuren. Han Zuidweg van Bureau Forum Standaardisatie is voorzitter van de werkgroep API Strategie en Beleid. De resultaten van de discussies uit deze werkgroep zijn openbaar gedocumenteerd op Github.

- Gino Laan van minBZK organiseerde op 3 maart 2020 een bijeenkomst over 'knowledge graphs' en API's, waarbij vertegenwoordiging van Logius, Geonovum, ICTU, NORA, VNG en minBZK (zowel architecten als beleidsadviseurs) aanwezig was. Ervaring van Geonovum en TNO laat zien dat klassieke berichtenstandaarden effectief kunnen worden vervangen door API's te combineren met knowledge graphs (linked data) die het informatiemodel en de achterliggende semantiek vastleggen. De hoge opkomst liet zien dat er veel belangstelling is voor dit onderwerp. Verrassend ontstond niet zozeer een discussie over technologie maar een (zeer relevante) discussie over business case die nog moet worden gerealiseerd om een gemeenschappelijk API beleid van de grond te krijgen bij de overheid. Hierbij hielden enkele aanwezigen een pleidooi dat de overheid APIs professioneler moet ontwikkelen en aanbieden met SLA's, waarbij het gebruik ook doorberekend kan worden.
- ICTU voert een gebruiksmeting uit voor de standaard Open API Specification 3.0. De resultaten van deze meting worden voor de zomer verwacht en kunnen gebruikt worden in de Monitor 2020.

Ad G. Internet- en beveiligingstandaarden

[bijlage G]

- Microsoft heeft aangekondigd per eind 2021 volledige ondersteuning te bieden voor [DANE op Office 365 Exchange Online](#). DANE voorkomt dat aanvallers mailverkeer kunnen 'afluisteren' of aanpassen. Strategisch Leveranciersmanagement Rijk heeft hier samen met Forum Standaardisatie op aangedrongen (zie ook bijgaande brief). Forum Standaardisatie adviseert overheidsorganisaties die willen overstappen op Office 365 Exchange Online in ieder geval te wachten tot Microsoft de standaard daadwerkelijk heeft geïmplementeerd.
- Rijksambtenaren die mobiel internet van Vodafone gebruiken, zijn nu beschermd tegen gemanipuleerde vertaling van ondertekende domeinnamen naar kwaadaardige IP-adressen. Vodafone [controleert](#) namelijk sinds 8 april op domein-handtekeningen (DNSSEC).
- Alle overheidswebsites en -maildomeinen moeten voor het einde van 2021, naast IPv4, volledig bereikbaar zijn via IPv6. Dat heeft het [Overheidsbreed Beleidsoverleg Digitale Overheid \(OBDO\) op 8 april 2020 besloten](#) op advies van het Forum Standaardisatie. Het besluit sluit aan op de intentieverklaring voor IPv6 die eind 2019 geïnitieerd werd door VNG en Logius. De door OBDO gemaakte afspraak werd overigens onlangs ook al aangekondigd door de [Staatssecretaris van EZK in antwoord op Kamervragen](#).
- Forum Standaardisatie was aanwezig met een stand op de CIO dag op 5 maart 2020: "Misbruik van de Internetdomeinen van jouw overheidsorganisatie voorkomen? E-mailphishing bestrijden en vertrouwelijkheid van web- en mailverkeer borgen? Wil je weten hoe jouw organisatie meer grip op Internetdomeinen kan krijgen? Kom vanmiddag langs bij de stand van Forum Standaardisatie op de #CIOdag2020." De CIO dag is er speciaal voor de CIO's, CTO's, CISO's of (beleids)adviseurs binnen het I-domein van het Rijk en de zbo's.

Ad H. Standaarden voor e-facturatie en administratie

- NLCIUS: Beheer en bevordering van het gebruik van NLCIUS is belegd bij het Standaardisatie-platform voor e-facturatie (STPE) waarin drie partijen samenwerken: NEN, TNO en Simplerinvoicing. Laatste is tevens PEPPOL-autoriteit van Nederland. Het initiatief wordt ondersteund door het Ministerie van Economische Zaken en Klimaat vanwege het maatschappelijke belang. Naast de beheerder STPE is het werkprogramma Nationaal Multi-Belanghebbenden Forum e-Factureren (NMBF) opgericht. Het STPE verzorgt de Nederlandse inbreng in de ontwikkeling van de Europese norm voor e-facturatie, ontwikkelt waar nodig nationale documenten gebaseerd op deze norm (inclusief coördinatie van sectorextenties) en bevordert de implementatie van de norm en aanpalende documenten in Nederland. Het NMBF, een adviserend orgaan, wordt gebruikt om de Nederlandse inbreng van alle mogelijke Nederlandse belanghebbenden te verzamelen en daarna te delen met de Europese Commissie in Brussel in het European Multi-Stakeholder Forum on Electronic Invoicing. Belangrijke toegevoegde waarde hierbij is dat het NMBF haar adviezen kan geven op basis van een breed draagvlak, zowel publiek als privaat. De schakel tussen beide ligt bij de Secretaris van het STPE die tevens lid is van het NMBF en vice versa. Deze ontwikkeling kan adoptie van de standaard bevorderen.

Zo heeft NMNF [animaties over e-factureren](#) helpen ontsluiten. En staat het verlagen van drempels voor grootschalige adoptie van e-facturatie in Nederland hoog op de agenda. Daarnaast heeft de beheerder STPE een nieuwe versie van het [specificatiedocument voor de NLCIUS](#) gepubliceerd. Dit is versie 1.0.3 en hierin zijn enkele kleine fouten hersteld en verduidelijkingen aangebracht.

- SETU: De [SETU-standaarden](#) worden gebruikt voor het elektronisch berichtenverkeer in de branche voor flexibele arbeid. SETU regelt het uitwisselen van berichten tussen aanbieders en afnemers (inleners) van tijdelijk personeel. De SETU-standaarden worden ontwikkeld en beheerd door de stichting SETU, waarin alle grote uitzendorganisaties in Nederland betrokken zijn. De stichting bestaat inmiddels meer dan 10 jaar. SETU beschikt, in lijn met voorgaande jaren, niet over kwantitatieve gegevens over het feitelijke gebruik van de standaarden. De gebruiksgegevens zijn lastig te bepalen, aangezien het berichtenverkeer niet via een centraal platform geregeld wordt en er recent ook geen metingen of enquêtes zijn uitgevoerd. TNO onderzocht in 2014 de adoptie van SETU en ontwikkelt de standaard in opdracht van de beheerder. Zij meldden dat alle grote spelers in de markt voor flexibele arbeid zijn aangesloten bij SETU en de SETU-standaarden gebruiken voor hun berichtuitwisseling. Deze spelers vertegenwoordigen 85% van de markt. Uit informele uitvraag bij werkgroepen blijkt dat deze spelers gestaag nieuwe koppelingen ontwikkelen met behulp van de SETU-standaarden. Voor de kleinere spelers in deze markt geldt dat zij afhankelijk zijn van hun softwareleveranciers. De standaard is nog niet 100% geadopteerd en op termijn gaat deze over in een andere vorm. Het adoptieplafond komt in zicht voor de grote partijen. Echter de kleine partijen lopen wel achter in de adoptie. Omdat de omvangrijke XML standaard (met wel 200 elementen) een te zwaar middel is voor deze kleine organisaties, is er een start gemaakt met nieuwe standaarden die flexibeler zijn. Sinds 2019 werkt men aan een 'proof of concept' en dit jaar staat in het teken van de ontwikkeling van ontologie en 'tooling'. Daarnaast denkt men na over de complexe beheersbaarheid van koppelvlakken. Dit initiatief van doorontwikkeling is los getrokken van het reguliere beheer van de SETU-standaard. Zo is afgelopen jaar SETU 'compliant' gemaakt aan [NLCIUS](#) (2.x versie gebaseerd op UBL). Doordat het aantal softwarepartijen hun lidmaatschap van de stichting heeft opgezegd, vindt er nu een peiling onder leden en niet-leden plaats. Naast het uitvragen naar reden van lidmaatschap, achterhaalt SETU de volumes waarin SETU-standaarden worden uitgevraagd al dan niet t.o.v. andere stromen. De verwachting is deze resultaten te delen met Forum Standaardisatie rond juni 2020. Op basis van deze informatie kan een betere inschatting gemaakt worden of de standaard als "gangbaar" kan worden gewalificeerd en eventueel kan worden verhuisd naar de zogenaamde lijst met [lijst met aanbevolen standaarden](#).

Ad I. Overig

- Consultatie Geonovum: nieuwe versies Nederlandse metadataprofielen, <https://www.forumstandaardisatie.nl/nieuws/consultatie-geonovum-nieuwe-versies-nederlandse-metadataprofielen>