notitie

Forum Standaardisatie
www.forumstandaardisatie.nl
info@forumstandaardisaties.nl
Bureau Forum Standaardisatie
gehuisvest bij Logius
Postadres
Postbus 96810
2509 JE Den Haag
Bezoekadres
Wilhelmina van Pruisenweg 52
2595 AN Den Haag
Bij bezoek aan Logius is legitimatie verplicht

FORUM STANDAARDISATIE 10 oktober 2018

Agendapunt 4. Open standaarden, adoptie
Stuknummer 4. Oplegnotitie adoptie

Van:	Stuurgroep open standaarden
Aan:	Forum Standaardisatie

Ter bespreking
U wordt gevraagd **te bespreken**:

A. Monitor openstandaarden-beleid [presentatie door Jaap Korpel - ICTU]
B. Laatste meting informatieveiligheidsstandaarden [bijlage B]
C. Forum-advies en reactie werkgroep Normatiek m.b.t. Baseline Informatiebeveiliging Overheid [bijlagen C1 en C2]
D. Overzicht verspreiden IV-meting en monitor onder achterban [bijlage D]
E. Sponsorschap leden Forum Standaardisatie [bijlage E]

Ter kennisname
U wordt gevraagd **kennis te nemen** van:

F. Wetsvoorstel Digitale Overheid [bijlagen F1, F2 en F3]
G. Formeel akkoord staatssecretaris van BZK op het voornemen HTTPS en HSTS te verplichten
H. BOMOS kennisbijeenkomst op 11 oktober
I. Voortgang onderzoek eDelivery (samenhang met dossier Digikoppeling)
J. Workshops toegankelijke documenten
K. Wettelijke verplichting toegankelijkheid
L. Overig nieuws

Ter bespreking

Ad A. Monitor openstandaarden-beleid [presentatie door Jaap Korpel - ICTU]

Jaap Korpel van ICTU geeft een presentatie over de concept-resultaten van de monitor openstandaarden-beleid 2018.

Ad B. Laatste meting informatieveiligheidsstandaarden [bijlage B]

Bijgevoegd vindt u de resultaten uit de meting informatieveiligheidsstandaarden van september 2018 (hierna: IV-meting). Aan het Forum wordt gevraagd om kennis te nemen van de resultaten uit de IV-meting en de resultaten in de achterban onder de aandacht brengen, met name bij de achterblijvers.

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). De meting omvat de afgeronde streefbeeldafspraak (eind 2017) om te zien welke progressie de groep achterblijvers maakt, en daarnaast de twee lopende streefbeeldafspraken (eind 2018 en eind 2019). Aangezien de meting is uitgebreid is ook de lijst met de te toetsen domeinnamen ten opzichte van de vorige meting geactualiseerd.

Voor de standaarden uit de eerdere metingen (DNSSEC, TLS, TLS cf NCSC, DMARC, DKIM en SPF) zien we dat de groei nog steeds doorzet met DNSSEC als uitschieter met 10 procentpunten naar 90%, maar ook de mailstandaarden zijn hard gestegen. Desondanks blijft DMARC, ondanks een stijging van 8 procentpunten, nog wel achter met 73%. Wel valt op dat de adoptie van TLS niet tot nauwelijks meer stijgt. Om 100% te bereiken zou een meer ‘één op één’ benadering nodig zijn. Van de standaarden met als streefdatum uiterlijk 2018 zien we dat HTTPS (89%) en TLS cf NCSC (87%) al een hoge adoptiegraad hebben terwijl HSTS nog wat achterblijft met 79%.

Als we kijken naar de nieuwe streefbeeldafspraak (implementatie uiterlijk 2019) dan verloopt de adoptie van de standaarden SPF Policy (85%) en STARTTLS (94%) erg goed. Voor deze standaarden kan worden verwacht dat ze eind 2019 zo goed als volledig zijn geadopteerd, wel heeft de correcte implementatie van STARTTLS cf NCSC (55%) nog extra aandacht nodig. Tot slot blijft de adoptie van DMARC Policy (28%) en DANE (22%) erg achter, al verschilt dit wel sterk per overheidslaag. Met name bij het Rijk en de Uitvoeringsorganisaties gaat het voor deze standaarden iets beter. Voor DANE is een stijging redelijk makkelijk te realiseren omdat DNSSEC MX op de 69% zit. Ook voor DMARC moet het mogelijk zijn omdat veel organisaties al wel DMARC beschikbaar hebben. Verder zien we, in lijn met de eerdere metingen, dat de aandacht voor de Web-standaarden significant groter is dan de aandacht voor de Mail-standaarden.

Een uitsplitsing van de resultaten naar overheidslaag laat eveneens zien dat er in iedere overheidslaag nog steeds sprake is van groei. Met name de waterschappen zijn sterk gegroeid met een gemiddelde van 12 procentpunten berekend over de standaarden DNSSEC, TLS conform NCSC, SPF, DKIM en DMARC, maar ook de provincies doen het goed met een stijging van 10 procentpunten. De waterschappen weten zelfs een 100% score te behalen voor de standaard TLS. Als we de nieuwe streefbeeldafspraken meenemen dan zien we dat voor de Web-standaard de gemeenten het beste scoren met een gemiddelde adoptie van 92%. Voor de mailstandaarden scoort het rijk het hoogst met een gemiddelde adoptie van 74%.

Ad C. Forum-advies en reactie werkgroep Normatiek m.b.t. Baseline Informatiebeveiliging Overheid [bijlage C1 en C2]

Het Forum Standaardisatie heeft op verzoek van Henk Wesseling, voorzitter van de interbestuurlijke Werkgroep Normatiek, een advies uitgebracht over het eindconcept van de BIO. Het definitieve advies is opgesteld na een schriftelijk ronde langs de Forum-leden. Het advies van het Forum is positief met een aantal kanttekeningen.

Met name de overheidsbrede samenwerking die leidt tot mee uniformering is een zeer positieve ontwikkeling. Ook is het goed dat wordt aangesloten bij NEN/ISO 27001/2:2013 die op de 'pas toe of leg uit'-lijst staan. Bovendien is het Forum positief over het feit dat de relevante open standaarden van de 'pas toe of leg uit'-lijst expliciet terugkomen in de BIO. Zoals bevestigd door Henk Wesseling, is voor deze open standaarden reeds centraal een risico-afweging gemaakt (door College/Nationaal beraad/OBDO) en moeten overheden deze toepassen.

Tegelijkertijd heeft het Forum gewezen op een aantal belangrijke aandachtspunten met betrekking tot governance, wettelijke verankering en verdieping. De werkgroep Normatiek heeft in reactie aan het Forum Standaardisatie laten weten hoe men deze aandachtpunten wil oppakken en meenemen, ook in het traject van verdere besluitvorming door OBDO.

Ad D. Overzicht verspreiden IV-meting en monitor onder achterban [bijlage D]

Forum Standaardisatie heeft afgesproken dat ieder Forum-lid de IV-meting en monitor verspreidt onder zijn/haar eigen achterban. Bijgaand een overzicht van de huidige stand van zaken voor zover bekend. U wordt gevraagd updates te melden.

Ad E. Sponsorschap leden Forum Standaardisatie [bijlage E]

Verschillende Forum-leden vervullen sponsor-functies voor bepaalde dossiers. In de bijlage het huidige overzicht. U wordt gevraagd uw interesse als sponsor te melden.

Ter kennisname

Ad F. Wetsvoorstel Digitale Overheid [bijlagen F1, F2, F3]

Het wetsvoorstel Digitale overheid is in juni op voorstel van staatssecretaris Knops van BZK aan de Tweede Kamer aangeboden. Als Forumbijlagen zijn toegevoegd het voorstel van Wet, de Memorie van Toelichting en het advies van de Raad van State. In de bijlagen zijn de onderdelen over standaarden/Forum-werk gearceerd.

In de wet betreft het met name artikel 3 (pagina 3) waarin een grondslag is opgenomen om een (open) standaard per AMvB te kunnen verplichten. Daarnaast heeft ook artikel 6 (pagina 5 en pagina 8) een link met het Forum werk aan de handreiking betrouwbaarheidsniveaus. Daarnaast zegt artikel 17 iets over het Toezicht op naleving van (o.a.) artikel 3.

In de Memorie van Toelichting wordt op pagina 2, en pagina 4 t/m 10 uitgebreid aandacht besteed aan het Forum Standaardisatie, de pas-toe-of-leg-uit lijst, en de achterliggende gedachte van de grondslag in de Wet.

Voorafgaand heeft de Raad van State in haar advies het belang van standaardisatie zeer flink benadrukt. Dat heeft geleid tot aanpassingen in het oorspronkelijke wetsvoorstel (in het bijgaande wetsvoorstel zijn ze deels verwerkt).

Voorbeeld: "Standaardisatie in de generieke digitale infrastructuur die overheidsorganisaties gebruiken [is] een noodzakelijke voorwaarde. Om deze voorwaarde te realiseren moet één verantwoordelijk bewindspersoon deze technische standaarden vaststellen en aan overheidsorganen (centraal en decentraal) dwingend kunnen voorschrijven, met bevoegdheden van toezicht en ingrijpen. Het wetsvoorstel regelt zulks op zijn best halfslachtig. Dat is onwerkbaar en gegeven het cruciale belang van standaardisatie niet verantwoord."

- Voorstel van Wet, voor de gearceerde versie zie Forum bijlage (link naar Kamerstuk: https://zoek.officielebekendmakingen.nl/kst-34972-2.html)
- Memorie van Toelichting, voor de gearceerde versie zie Forum bijlage (link naar Kamerstuk: https://zoek.officielebekendmakingen.nl/kst-34972-3.html)
- Advies van de Raad van State, met nota van wetgever hoe daarmee omgegaan is. Voor de gearceerde versie zie Forum bijlage (link naar Kamerstuk https://zoek.officielebekendmakingen.nl/kst-34972-4.html)

Wet Digitale Overheid en pas-toe-of-leg-uit, hoe zat het ook alweer ?

1. Wat is het verschil tussen de AMvB verplichting en pas-toe-of-leg-uit?

De pas-toe-of-leg-uit-verplichting geldt vanaf het moment dat overheidsorganisaties investeren in een systeem of dienst waarbij de pas-toe-of-leg-uit-standaarden een rol hebben. (bijvoorbeeld: investeert je in de website van de organisatie dan dien je op dat moment de ptolu-webstandaarden toe te passen en formeel gezien niet eerder). De kracht hiervan is dat organisteis zelf het optimale moment kiezen en zo eventuele desinvesteringen voorkomen. Bovendien is er altijd nog ruimte voor een geldige en onderbouwde reden om niet te voldoen (leg uit).

In sommige gevallen is pas-toe-of-leg-uit te weinig urgent of te vrijblijvend. Daarom geeft artikel 3 van de wetDO de minister van Binnenlandse Zaken de mogelijkheid om standaarden aan te wijzen die verplicht worden via een AMvB. Bij een dergelijke verplichting is er wel sprake van een harde deadline voor de implementatie van de standaarden en is geen ruimte meer om niet te voldoen.

2. Kan een standaard bij AMvB verplicht zijn en op de pas-toe-of-leg-uit-lijst staan?

Dit kan alleen als het toepassingsgebied van de AMvB verplichting anders is dan het toepassingsgebied van de pas-toe-of-leg-uit verplichting. Bij eenzelfde toepassingsgebied gaat een AMvB verplichting boven pas-toe-of-leg-uit en wordt de standaard van de lijst verwijderd.

3. Wat is de rol van het Forum bij de AMvB?

Welke standaard in aanmerking komt voor een AMvB is aan min. BZK. In het proces om te komen tot een AMvB heeft het Forum twee taken:

a) Mits de standaard al op de ptolu-lijst staat: Aanleveren aandachtspunten m.b.t. de standaard die uit de pas-toe-of-leg-uit toetsing naar voren kwamen. Dit kan gaan om eventuele beheerissues of adoptie issues die kunnen knellen bij een AMvB.
b) Aanleveren namen van stakeholders die tenminste in het AMvB traject betrokken moeten worden om eventuele issues weg te nemen of het draagvlak te vergroten.

Daarnaast geldt dat de Monitor van het Forum door min. BZK gebruikt kan worden om te bepalen hoe het met de adoptie van standaarden gesteld is en of een harde verplichting opportuun is. In ondergenoemde voorbeeld (ad E) van de voorgenomen https verplichting is de halfjaarlijkse IV-meting van het Forum van invloed geweest op het besluit om een AMvB traject in te zetten.

4. Hoe is toezicht op de AMvB verplichting geregeld?

Er is in de wet niet voorzien in één specifieke toezichtstructuur op alle AMvB's. Het reguliere bestuurlijke toezicht wordt gevolgd. De wetDO geeft daarnaast per AMvB de ruimte verschillende instrumenten in te zetten. Zo kan er gekozen worden om audits in te zetten of periodiek het gebruik te meten (bij de standaarden waar dit kan). Tot slot is in de wet opgenomen dat mens en bedrijf rechten mogen ontlenen aan de wetDO. (concreet: bij eventuele schade bij mens en bedrijf voortkomend uit het niet toepassen van de verplichte standaarden door overheden, kunnen zij verhalen op de overheid).

Ad G. Formeel akkoord staatssecretaris van BZK op het voornemen HTTPS en HSTS te verplichten

De staatssecretaris van Binnenlandse zaken heeft in augustus ingestemd met de startnotitie waarin de voorgenomen verplichting van de webstandaarden HTTPS en HSTS beschreven wordt. De afgelopen maanden is min. BZK begonnen met de beleidsvoorbereiding voor deze verplichting. Nu het akkoord van de staatssecretaris er ligt, begint in oktober het daadwerkelijke AMvB traject. Bij een soepel & spoedig verloop is de AMvB van kracht op 1 juli 2019.

Achtergrond
De wet Digitale Overheid (naar verwachting vanaf 2019 van kracht) geeft de Minister van BZK de mogelijkheid om open standaarden aan te wijzen voor een wettelijke verplichting door een AMvB. Begin 2017 heeft de minister de kamer toegezegd deze mogelijkheid te zullen gebruiken voor de https standaard.

HTTPS en HSTS staan op de pas-toe-of-leg-uit-lijst van Forum Standaardisatie en het

OBDO heeft het streefbeeld uitgesproken dat iedere overheidspartij deze standaarden, voor het einde van 2018, toepast. De verplichting via een AMvB in 2019 kan worden gezien als het sluitstuk op dit eerdere beleid en uitgesproeken streefbeeld. In de loop van 2019 bekijkt min. BZK welke andere standaarden eventueel in aanmerking komen voor een verplichting via een AMvB.

Rol van het Forum
Forum Standaardisatie voorziet min. BZK van de relevante informatie over deze standaarden en eventuele aandachtspunten vanuit het toetsingsproces voor de pas-toe-of-leg-uit-lijst. Daarnaast geeft FS aan welke belanghebbende partijen rond deze standaarden betrokken dienen te worden tijdens de procedure voor een breed gedragen besluitvorming.

Ad H. BOMOS kennisbijeenkomst op 11 oktober

Samen met Logius Centrum voor Standaarden en Geonovum, organiseert het Forum Standaardisatie op 11 oktober 2018 een bijeenkomst over het Beheer en OntwikkelModel voor Open Standaarden (BOMOS). Deze bijeenkomst heeft als doel om partijen die de BOMOS methodiek (willen) gebruiken voor het beheer en doorontwikkelen van standaarden, ervaringen uit te laten wisselen en van elkaar te leren.

Wat is BOMOS?
Het Beheer en OntwikkelModel voor Open Standaarden (BOMOS) is, zoals de naam zegt, een methode voor de (door)ontwikkeling en het beheer van standaarden. De methode is op basis van best practices ontwikkeld en hanteert openheid en transparantie als uitgangspunten bij het beheer van de standaard.

Forumleden hebben reeds per mail een uitnodiging ontvangen. Meer informatie over de bijeenkomst vindt u op onze website:
https://www.forumstandaardisatie.nl/nieuws/doe-mee-met-de-bomos-kennisbijeenkomst

Ad I. Voortgang onderzoek eDelivery (samenhang met dossier Digikoppeling)

VKA heeft in opdracht van Forum Standaardisatie een onderzoek gedaan naar het huidige en toekomstige gebruikerspotentieel van eDelivery in Nederland. Eind mei zijn de voorlopige resultaten van het onderzoek met de werkgroep eDelivery gedeeld en is besproken welke adviezen de werkgroep zal meegeven aan de stuurgroep.

De onderzoeksrapportage wordt momenteel definitief gemaakt en zal in december aan het Forum gepresenteerd worden.

Wat is eDelivery?
eDelivery is een EU-bouwblok bedoeld om veilige, grensoverschrijdende digitale dienstverlening tussen EU-lidstaten mogelijk te maken. Zonder dat een burger of bedrijf daarvoor fysiek informatie moet ophalen of brengen. Het koppelvlak is enigszins vergelijkbaar met de functie die Digikoppeling binnen Nederland heeft voor sectoroverstijgende informatie-uitwisseling en informatie-uitwisseling met de basisregistraties. Ze zijn echter niet direct compatible.

Waar gaat het onderzoek over?
Vanuit verschillende Nederlandse sectororen dient men aan de sluiten op eDelivery, maar deze sectoren gebruiken veelal al eigen sectorale standaarden, die niet zonder meer compatible zijn. Bovendien wordt met behulp van die sectorale standaarden vaak al internationaal informatie uitgewisseld. VKA onderzoekt de kansen van eDelivey voor deze rapportage hoe hier het best mee kan worden omgegaan.

Ad J. Workshops toegankelijke documenten

- BFS organiseert een sessie over 'Accessible government documents: the PDF challenge' op het Logius International Symposium dat op 4 oktober 2018 wordt gehouden in het Vredespaleis, en gericht is op deelnemers van publieke ICT service providers uit de EU Lidstaten. BFS heeft hiervoor sprekers aangetrokken uit Duitsland (Bundesministeriums für Umwelt, Naturschutz und nukleare Sicherheit), het Verenigd Koninkrijk (gov.uk) en Nederland (Ministerie van Algemene Zaken).

- Op 22 november organiseert BFS in samenwerking met digitoegankelijk.nl (Logius) een workshop over PDF en Toegankelijkheid in de Jaarbeurs in Utrecht. Vorig jaar trok dit evenement 90 deelnemers uit alle lagen van de Nederlandse overheid. Dit jaar verwachten we ook rond de honderd deelnemers.

Ad K. Wettelijke verplichting toegankelijkheid

Op 1 juli 2018 werd het Tijdelijk besluit toegankelijkheid digitale overheid van kracht (zie: https://zoek.officielebekendmakingen.nl/stb-2018-141.html). Dit besluit raakt ook de website van het Forum Standaardisatie. Op 23 september 2019 moet de website van het Forum voldoen aan de EN 301 549 toegankelijkheidseisen. Dit geldt ook voor de documenten op de website waaronder Forumstukken, handreikingen, publicaties en procedurele documenten voor het onderhoud van de lijsten open standaarden.

Afgezien van de wettelijke verplichting is het belangrijk dat het Forum Standaardisatie een voorbeeldfunctie vervult ten aanzien van digitale toegankelijkheid. BFS streeft ernaar dat alle documenten die na 23 september 2018 gepubliceerd worden, voldoen aan de wettelijke toegankelijkheidsverplichting. Het kan zijn dat de indeling en opmaak van sommige Forumstukken enigszins worden aangepast om aan de toegankelijkheidseisen te kunnen voldoen. Daarnaast onderzoekt BFS welke voor 23 september 2018 op de website gepubliceerde documenten zullen moeten worden omgezet naar een toegankelijke indeling.

Ad L. Overig nieuws

- DICTU/EZK heeft voor haar mailservers TLSA-records ingesteld. Daardoor zijn 103 door DICTU beheerde domeinen bereikbaar via een met DANE beveiligde mailverbinding. Voorbeelden van domeinnamen zijn minezk.nl, minez.nl en dictu.nl.
- "Achterblijven implementatie IPv6 schaadt Nederlands innovatieklimaat", https://www.sidn.nl/a/over-sidn/achterblijven-implementatie-ipv6-schaadt-nederlands-innovatieklimaat
- Voortgang IPv6 bij gemeenten: https://www.waarstaatjegemeente.nl/dashboard/IPv6--cgdgggcicyhgjiv
- "Update Aquo-standaard naar 2018-06", https://www.forumstandaardisatie.nl/nieuws/update-aquo-standaard-naar-2018-06
- "SIKB0101 bijgewerkt naar versie 13.5", https://www.forumstandaardisatie.nl/nieuws/sikb0101-bijgewerkt-naar-versie-135
- "OGC test standaarden in de praktijk", https://www.geonovum.nl/over-geonovum/actueel/ogc-test-standaarden-in-praktijk
- "E-mailtest op Internet.nl uitgebreid", https://internet.nl/article/email-test-on-internetnl-extended/
- Sessie over DANE voor beveiliging mailverbindingen tijdens One Conference op 2

oktober: https://internet.nl/article/email-test-on-internetnl-extended/

- "Oorkonde voor DMARC", https://www.forumstandaardisatie.nl/nieuws/oorkonde-voor-dmarc
- Artikel met Steven Luitjens en Michiel Steltman in Publiek Denken, "Een betrouwbare overheid kan niet zonder moderne veiligheidstandaarden": http://specials.publiekdenken.nl/special-isamenleving#!/perspectief-forum-standaardisatie