FS-20181212.01B

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.

Contactpersoon
Joram Verspaget
secretaris BFS
joram.verspaget@forumstandaardisatie.nl
+ 31 (0) 6 5284 5592

VERSLAG FORUM STANDAARDISATIE woensdag 10 oktober 2018

Vergaderdatum	woensdag 10 oktober 2018
Vergadertijd	09:30 tot 12:00 uur
Vergaderplaats	New Babylon, zaal 3.5 Anna van Buerenplein 29 2496 RZ Den Haag

---

Aanwezig

Forum Standaardisatie
Nico Westpalm van Hoorn (voorzitter), Yvonne van der Brugge (Logius, secretaris), Gijs Boudewijn (Betaalvereniging), Gerard Hartsink (financiële sector), Cor Franke (Franke Interim Management), Marc van Hilvoorde (namens CIO Rijk), Floor Jas (Surfnet), Joop van Lunteren (adviseur, PBLQ HEC), Geert Moelker (Ministerie van Economische Zaken en Klimaat), Wim van Nunspeet (CBS), Benno Overeinder (NLnet Labs), Friso Penninga (Geonovum), Theo Peters (VNG Realisatie), Katinka Petronia (namens Ministerie van Binnenlandse Zaken, DIO), Ad Reuijl (Manifestgroep/CIP), Harry Roumen (Ministerie van Financiën/DG Belastingdienst), Gerard Smits (Waterschapshuis),Anneke Spijker (Interprovinciaal Overleg), Rob Verweij (Rinis)

Afmeldingen:

Rudi Bekkers (Technische Universiteit Eindhoven), Gé Linssen (Ministerie van Binnenlandse Zaken, DI&O), Nico Romijn (VNG Realisatie), Michiel Steltman (DINL)

Aanwezig namens het bureau
Ludwig Oberendorff (hoofd), Désirée Castillo Gosker (adviseur), Lancelot Schellevis (adviseur), Maarten van der Veen (adviseur), Joram Verspaget (bureausecretaris, notulen), Han Zuidweg (adviseur).

Te gast
Petie Slangen en Paul Zeef voor agendapunt 2C Phishing Mijn Overheid [presentatie]

1 Opening, agenda, verslag

actie	Ter besluitvorming en ter kennisname
tijd	09:30-09:35 uur
	FS 181010.**1A** Agenda FS 181010.**1B** Verslag Forum Standaardisatie woensdag 13 juni 2018

1A Agenda

Agendapunt 05. Presentatie Mijn Overheid voor Ondernemers (MOvO) komt te vervallen (zie aldaar voor nadere toelichting).

1B Verslag Forum Standaardisatie woensdag 13 juni 2018

Akkoord, geen nadere opmerkingen.

2 OBDO en Forum Standaardisatie

actie	Ter besluitvorming en ter kennisname
tijd	09:35-10:05 uur
	FS 181010.**2** Oplegnotitie FS 181010.**2A** Werkplan Forum Standaardisatie 2019 FS 181010.**2B** Rapportage op werkplan 2018, periode mei tot en met augustus 2018 FS 181010.**2C** Phishing Mijn Overheid [presentatie] Ter kennisname / mondeling toegelicht: FS 181010.**2D** Beleidsagenda NL Digibeter [bijlage 1] [bijlage 2] FS 181010.**2E** Stand van zaken standaardisatie-agenda FS 181010.**2F** Stand van zaken nieuwe voorzitter FS 181010.**2G** Studiereis Forum Standaardisatie 12 december 2018

2A Werkplan Forum Standaardisatie 2019

Het Forum Standaardisatie wordt gevraagd om het voorgelegde concept-werkplan Forum Standaardisatie 2019 (concept) te bespreken en/of aan te vullen. Het werkplan bouwt voort op de discussie uit december 2017 over de prioritering van de dossiers, toen het onderwerp API's naar voren kwam als een aandachtspunt. Hoewel het hier het werkplan voor 2019 betreft, is het de insteek dat de onderdelen ervan worden doorvertaald naar de periode 2020-2022.

Het Forum ziet graag aandacht voor de volgende punten:

- De internationale dimensie, waaronder ontwikkelingen in Europa: gewerkt wordt aan een European Unique Identifier (EUID) voor alle bedrijven in de Europese Unie. Met de EUID kunnen bedrijven op Europees niveau worden geïdentificeerd. Verder is er de Single Digitale Gateway. En daarnaast is er de internationale dimensie van blockchain (dit onderwerp wordt geagendeerd voor een komende Forum-vergadering).
- Toevoegen aan het Objective: het vinden en toetsen van de juiste standaarden om pas-toe-of-leg-uit status aan te geven, ook in relatie tot internationale ontwikkelingen op standaardisatie.
- Een haakje voor het onderwerp Semantiek
-

Het bureau verwerkt de gemaakte opmerkingen voor de versie die 12 december aan het Forum wordt voorgelegd.

2B Rapportage op werkplan 2018, periode mei tot en met augustus 2018

Ter kennisname wordt de rapportage over de periode januari tot en met juni voor het werkplan 2018 aan het Forum voorgelegd.

Verzocht wordt om voortaan in de rapportage in het overzicht ook de knelpunten aan te geven, inclusief welke rol het Forum/Forumleden zouden kunnen spelen om die te verbeteren.

Het Forum heeft geen verdere opmerkingen.

2C Phishing Mijn Overheid [presentatie]

Afgelopen juni vond een phishing aanval plaats, waarbij (de namen van) DigiD en MijnOverheid en RDW zijn misbruikt om inloggegevens van gebruikers van deze diensten en instanties te ontfutselen. E-mails met een link naar een malafide website leken afkomstig te zijn van deze voorzieningen en instanties, omdat in het mailadres de domeinen overheid.nl en rdw.nl werden gebruikt. Dit misbruik kon ondermeer plaatsvinden omdat de mailservers van die adressen niet (afdoende) gebruik maakten van de anti-phishing standaard DMARC, die op de pas-toe-of-leg-uit-lijs staat (incl. de strenge configuratie van die standaard). Deze standaard maakt e-mailverkeer veiliger door misbruik van domeinnamen bij e-mail tegen te gaan.

Het incident onderstreept het belang van het juiste gebruik van informatieveiligheidsstandaarden (IV-standaarden) en het niet-gebruiken van hyperlinks in e-mailcommunicatie.

Naar aanleiding van de presentatie komt een aantal punten naar voren:

In het bedrijfsleven en bij de overheid (provincies) wordt hiervoor gebruik gemaakt van de inzet van 'ethical hackers'. Deze hackers breken in opdracht van de opdrachtgevers digitaal bij de opdrachtgevers in om zwakheden in de beveiliging zonder schade voor de opdrachtgever te achterhalen en te rapporteren. Dit helpt bestuur en management om gericht actie te kunnen ondernemen voor correct gebruik van IV-standaarden in eigen organisatie. Ook moeten burgers en consumenten zich bewust zijn van het gevaar van social engineering (menselijke misleiding). Het Ministerie van Binnenlandse Zaken en Koninkrijkrelaties heeft budget vrijgemaakt voor een communicatieprogramma hiervoor. De uitvoering hiervan gebeurt in samenhang met bestaande gelijksoortige programma's.

Wat verder kan bijdragen aan de beveiliging van e-mailverkeer is het laten certificeren van e-mailbeveiligingstandaarden middels de .X509-standaard. Dit zou in lijn zijn met het 'know your supplier'-principe van Consumer International, een organisatie die wereldwijd opkomt voor de belangen van consumenten. De standaard garandeert dat de afzender (de leverancier van de mail) ook daadwerkelijk de afzender is die de afzender zegt te zijn.

Het correcte gebruik van de juiste IV-standaarden is ook relevant met het oog op PSD2, de nieuwe Europese wet (richtlijn) voor het betalingsverkeer van consumenten en bedrijven. Consumenten kunnen sinds de inwerkingtreding van PSD2 aan een derde partij (bijvoorbeeld een andere financiële instelling) toegang geven tot hun betaalrekening bij hun bank om hen te kunnen adviseren over op maat gemaakte producten en diensten. Deze toegang voor derden kan druk zetten op de veiligheid van het proces en de inzet van authenticatiemiddelen.

Om de laatste ontwikkelingen rond informatieveiligheid te kunnen volgen is het raadzaam dat organisaties zich o.a. aansluiten bij browser communities.

Vanuit Provincies en Waterschappen wordt aangegeven dat de presentatie van Yvonne kan helpen om het onderwerp daar goed bij het management op de agenda te krijgen. Logius en het bureau Forum Standaardisatie ondersteunen graag hierbij. Daarnaast kan het voor deze partijen een optie zijn om aansluiting te zoeken bij de Veilige Email Coalitie. De deelnemers aan de coalitie pakken gezamenlijk misbruik zoals phishing en het afluisteren van e-mail aan met het invoeren van maatregelen voor het beveiligen van e-mailverkeer. Daarvoor wordt gebruik gemaakt van de informatieveiligheid standaarden van de pas-toe-of-leg-uit lijst, en wordt bijvoorbeeld gezamenlijk materiaal ontwikkeld, zoals communictiemateriaal.Gijs Boudewijn geeft aan dat er al goed Nederlandstalig materiaal ligt bij de Betaalvereniging dat kan worden (her)gebruikt.
Gerard Hartsink zal via het bureau de ICC Cybersecurity Guide for Business rondsturen. Indien beschikbaar volgt ook de Nederlandse vertaling.

Verder komt naar voren dat het ook van belang is dat er awareness bij burgers en bedrijven komt. Als die niet weten waar ze op moeten letten (bijv. afzenderadres of domeinnaam), dan helpen de standaarden ook niet goed.

Bekeken wordt of/hoe dit onderwerp aan de hand van dit voorbeeld ook in het OBDO behandeld kan worden.

2D Beleidsagenda NL Digibeter
2E Stand van zaken standaardisatie-agenda

Ter vergadering wordt een hard copy-versie van de Agenda NL Digibeter (een gezamenlijke agenda van alle overheden met belangrijke publieke en private partners) uitgedeeld. De agenda zet uiteen hoe het contact van de overheid met burgers en ondernemers slimmer, toegankelijker en persoonlijker kan. Hiermee wil het kabinet de kansen van digitalisering benutten en de regie van burgers en ondernemers versterken.

Standaardisatie vormt door de agenda heen een rode draad. De standaardisatieagenda zet hier verder op in, onder andere middels een extern onderzoek naar welke standaardisatiekansen er liggen. Onderdeel daarvan vormt welke standaarden mogelijk extra aandacht behoeven, bijvoorbeeld door plaatsing op de pas-toe-of-leg-uit-lijst. Maar het onderzoek kijkt breder en gaat nou juist ook op zoek naar standaardisatie kansen die niet in de huidige scope van het Forum zitten.

2F Stand van zaken nieuwe voorzitter

Het ministerie van Binnenlandse Zaken en Koninkrijksrelaties verkent momenteel de mogelijkheden voor de opvolging van de huidige voorzitter van het Forum Standaardisatie. Het streven is om vóór eind 2018 een gedegen opvolger te hebben gevonden.

2G Studiereis Forum Standaardisatie 12 december 2018

Het bureau werkt momenteel aan het programma voor de studiereis van het Forum, zoals dat traditioneel plaatsvindt in de maand december. Het programma duurt van 12:00 tot 22:00 uur. Nadere informatie over de locatie en verdere invulling van het programma ontvangen de leden van het Forum zodra bekend.

3 Open standaarden, lijsten

actie	Ter besluitvorming en ter kennisname
tijd	10:05-10:25 uur
voorzitter	Anneke Spijker namens de Stuurgroep open standaarden
	FS 181010.**3** Oplegnotitie Pas-toe-of-leg-uit-lijst: FS 181010.**3A** Plaatsing van TLS 1.3 *(nieuwe versie van standaard voor de beveiliging van Internetverbindingen)* naast TLS 1.2 en verwijdering van TLS 1.0 en TLS 1.1 FS 181010.**3B** Vervanging van versie 1.1.2 van EN 301 549 door versie 2.1.2 *(nieuwe versie Europese norm voor digitale toegankelijkheid)*; starten van een toetsingsprocedure ter verwijdering van EN 301 549 op 23 september 2019 [in oplegnotitie, geen bijlage] FS 181010.**3C** Uitbreiding van het functioneel toepassingsgebied van STARTTLS in combinatie met DANE *(e-mailveiligheidstandaarden tegen het afluisteren of manipuleren van mailverkeer)* FS 181010.**3D** Verwijdering van STOSAG 1.0 *(standaard voor informatie-uitwisseling in de afvalverwerking)*. FS 181010.**3E** Starten procedure ter inperking van het functioneel toepassingsgebied van COINS 2.0 *(opslag- en uitwisselingsstandaard voor de bouw)* [in oplegnotitie, geen bijlage] Lijst aanbevolen standaarden: FS 181010.**3F** Plaatsing van SHACL *(linked data standaard)* FS 181010.**3G** Plaatsing van S/MIME *(standaard voor aanvullende e-mail beveiliging)* voor uitsluitend digitale ondertekening, niet voor versleuteling van e-mail [in oplegnotitie, geen bijlage] In oplegnotitie, ter kennisname: FS 181010.**3H** Aanvullend onderzoek voor plaatsing PDF/UA *(documentstandaard die wettelijke toegankelijkheidseisen ondersteunt)* op de pas-toe-of-leg-uit-lijst

Floor Jas is lid geworden van de Stuurgroep.

Anneke Spijker licht namens de Stuurgroep open standaarden het agendapunt toe.

3A Plaatsing van TLS 1.3 (nieuwe versie van standaard voor de beveiliging van Internetverbindingen) naast TLS 1.2 en verwijdering van TLS 1.0 en TLS 1.1

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

Om TLS op oudere devices te kunnen blijven gebruiken werd in het proces gevraagd om te verkennen wat de mogelijkheden zijn om TLS 1.0 en 1.1 nog één jaar op de lijst te laten staan maar niet verplicht te stellen voor uitvraag bij aanbestedingen (daarvoor geldt TLS 1.3).

De mogelijkheid om TLS 1.0 en 1.1 op de lijst te laten staan om TLS ook op oudere devices te kunnen blijven gebruiken wordt niet opportuun geacht omdat het pas-toe-of-leg-uit-beleid gaat over het verplichte uitvragen bij aanbestedingen in plaats van het gebruik van de standaard(en) zelf (dat maakt verwijdering van de lijst niet onmogelijk).

Ondanks dat TLS 1.3 recent is gepubliceerd, kan het als een technisch stabiele en uitgekristalliseerde standaard worden beschouwd. TLS 1.3 is echter niet backward compatible en nog niet algemeen geadopteerd. Besloten wordt daarom om TLS 1.2 als terugval-versie op de lijst te laten staan naast TLS 1.3.

3B Vervanging van versie 1.1.2 van EN 301 549 door versie 2.1.2 (nieuwe versie Europese norm voor digi tale toegankelijkheid); starten van een toetsingsprocedure ter verwijdering van EN 301 549 op 23 sep tember 2019

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.

De internationale Web Content Accessibility Guidelines (WCAG) 2.0 zijn een integraal onderdeel van de standaard.

Het Forum stemt zonder verdere opmerkingen in met het voorgestelde advies.

3C Uitbreiding van het functioneel toepassingsgebied van STARTTLS in combinatie met DANE (e-mailvei ligheidstandaarden tegen het afluisteren of manipuleren van mailverkeer)

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."

Het Forum stemt hiermee in.

3D Verwijdering van STOSAG 1.0 (standaard voor informatie-uitwisseling in de afvalverwerking)

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.

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 Forum stemt in met verwijdering van STOSAG 1.0 van de pas-toe-of-leg-uit-lijst.

3E Starten procedure ter inperking van het functioneel toepassingsgebied van COINS 2.0 (opslag- en uitwisselingsstandaard voor de bouw)

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.

Binnen het Nationaal BIM Platform (BIM staat voor Bouwwerk Informatie Modellen) bestaat consensus over de voorgestelde aanpassing van het toepassingsgebied van COINS 2.0.

Het Forum stemt in met het voorstel.

3F Plaatsing van SHACL (linked data standaard)

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

Plaatsing van SHACL op de lijst aanbevolen standaarden.

Het Forum stemt in met het voorstel.

3G Plaatsing van S/MIME (standaard voor aanvullende e-mail beveiliging) voor uitsluitend digitale onderte kening, niet voor versleuteling van e-mail

In de vergadering van 25 april 2018 stemde het Forum Standaardisatie in met de plaatsing van S/MIME op de lijst aanbevolen standaarden, dit na een zorgvuldig doorlopen procedure. 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. Daarom was S/MIME nog niet voorgelegd aan het OBDO, en is aanvullend onderzoek gedaan naar de gepubliceerde kwetsbaarheid. In het aanvullend onderzoek is met name het NCSC geraadpleegd.

Het Forum Standaardisatie wordt nu 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.

Opgemerkt wordt dat een nadien geconstateerde kwetsbaarheid niet vanzelfsprekend een reden is om deze voor te dragen voor verwijdering van de pas-toe-of-leg-uit-lijst of de lijst aanbevolen standaarden.
Vaak is een kwetsbaarheid immers niet terug te voeren op de standaard zelf, maar op de softwarematige implementatie ervan.Gelet de ernst van het veiligheidsprobleem bij S/MIME was in dit geval wel te verantwoorden dat S/MIME niet onmiddellijk is voorgelegd aan het OBDO, en dat ervoor is gekozen om eerst een aanvullend onderzoek te doen en dit terug te leggen aan het Forum. Opgemerkt wordt dat het goed is om deze handelswijze (aanhouden tot nader onderzoek, wanneer na instemming door het Forum alsnog een kwetsbaarheid ontstaat) in het proces vast te leggen, met mandaat voor de voorzitter van het Forum in afstemming met BFS.

Inhoudelijk wordt na nader onderzoek besloten om het toepassingsgebied van de standaard op de aanbevolen lijst te beperken tot digitale ondertekening, en niet meer op versleuteling met het oog op het voorkomen van meelezen (daar heeft de kwetsbaarheid namelijk mee te maken).

Binnen de internetgemeenschap rond S/MIME wordt gezocht naar een oplossing voor het veiligheidsprobleem (bij het voorkomen van meelezen). Dit heeft ook de aandacht van de Veilige Email Coalitie (VEC).

De gemaakte opmerkingen meenemende stemt het Forum in met het voorstel.

3H Aanvullend onderzoek voor plaatsing PDF/UA (documentstandaard die wettelijke toegankelijkheidseisen ondersteunt) op de pas-toe-of-leg-uit-lijst

De resultaten van het onderzoek worden geagendeerd voor de Forum-vergadering van 12 december a.s.

Het Forum heeft verder geen opmerkingen.

4 Open standaarden, adoptie

actie	Ter besluitvorming en ter kennisname
Tijd	10:25-10:55 uur
voorzitter	Anneke Spijker namens de Stuurgroep open standaarden
	FS 181010.**4** Oplegnotitie Ter bespreking: FS 181010.**4A** Monitor open standaarden [presentatie] FS 181010.**4B** Laatste meting informatieveiligheidsstandaarden september 2018 FS 181010.**4C** Forum-reactie Op Baseline Informatiebeveiliging Overheid [bijlage 1] [bijlage 2] FS 181010.**4D** Overzicht verspreiden IV-meting en monitor in achterban FS 181010.**4E** Sponsorschap leden Forum Standaardisatie Ter kennisname: FS 181010.**4F** Wetsvoorstel Digitale Overheid [bijlage 1] [bijlage 2] [bijlage 3] In oplegnotitie, ter kennisname: FS 181010.**4G** Formeel akkoord staatssecretaris van BZK op het voornemen HTTPS en HSTS te verplichten FS 181010.**4H** BOMOS kennisbijeenkomst op 11 oktober FS 181010.**4I** Voortgang onderzoek eDelivery (samenhang met dossier Digikoppeling) FS 181010.**4J** Workshops toegankelijke documenten FS 181010.**4K** Wettelijke verplichting toegankelijkheid FS 181010.**4L** Overig nieuws

4A Monitor open standaarden [presentatie Jaap Korpel]

ICTU heeft in opdracht van het Forum Standaardisatie net als voorgaande jaren onderzoek gedaan naar het gebruik van open standaarden van de pas-toe-of-leg-uit-lijst door overheidsorganisaties bij aanbestedingen en in overheidsbrede voorzieningen. Voor de 35 onderzochte voorzieningen was in totaal 464 keer een open standaard relevant, de voorzieningen voldoen in 70% van deze 464 gevallen aan de relevante open standaard. Hieruit blijkt dat het aantal voorzieningen waarbij de juiste open standaarden worden gebruikt en daarmee voldoet aan het pas-toe-of-leg-uit-beleid is toegenomen. Lag dit in 2016 nog op 60% en in 2017 op 67%, in 2018 is dit percentage verder gestegen naar 70%.

Om de meting overheidsbreed meer representatief te maken zijn de Monitor 2018 extra aanbestedingen van de decentrale overheden (provincies, gemeenten en waterschappen) beoordeeld. Hiermee is het aandeel van de decentrale overheden in de meting toegenomen.

Het aantal aanbestedingen overheidsbreed waarin om open standaarden wordt gevraagd is weer verder gestegen: van 72% (2016) naar 81% (2017) tot 85% (2018). Echter het aantal aanbestedingen waarin alle relevante en/of in ieder geval cruciale open standaarden zijn uitgevraagd is gedaald van 33% in 2017 naar 15% in 2018. Als alleen naar het Rijk wordt gekeken is de daling minder groot: van 40% in 2017 naar 26% in 2018. Niet precies is te duiden waarom het Rijk een hogere score heeft dan de decentrale overheden. Het blijkt in de praktijk voor decentrale overheden ingewikkeld om te bepalen welke open standaarden relevant zijn.

Het gemiddelde aantal uitgevraagde relevante open standaarden per aanbesteding toegenomen van 5,8 in 2016 naar 6,1 in 2017 en 8,3 in 2018.

De definitieve Monitor 2018 wordt in december ter kennisname voorgelegd aan het Forum. Hierin wordt ook nader geduid waarom en welke standaarden als relevant worden geduid.

Het Forum zal zich ook buigen over welke acties het dient te ondernemen op basis van de gepresenteerde resultaten, onder ander richting betrokken juridische en inkoopafdelingen bij het aanbestedingsproces. Het informeren van de achterban door Forum en/of OBDO leden, over het de resultaten van de monitor en de IV-metingen is hierbij effectief. Daarmee zijn positieve ervaringen opgedaan bij o.a. het CIP met behulp van internet.nl met de oproep tot de implementatie van de informatieveiligheidsstandaarden. Aansluiting bij de Veilige Email Coalitie (VEC), het Platform internetstandaarden (PLIS) en Alert Online zijn ook aanvliegroutes die bijdragen aan een beter bewustzijn over het pas-toe-of-leg-uit-beleid bij aanbestedingen. In sommige gremia hebben de adviezen van het Nationaal Cyber Security Centrum (NCSC) en de score op Internet.nl meer impact dan de pas-toe-of-leg-uit-lijst van het Forum. Met het oog op effectiviteit zal er steeds voor worden gekozen om de aanvliegroute met de meeste impact te kiezen, het gaat uiteindelijk immers om het gebruik.

Komend jaar zal in de monitor speciaal aandacht worden besteed aan de groep standaarden die zelden relevant zijn en/of uitgevraagd worden.

4B Laatste meting informatieveiligheidsstandaarden september 2018

Lancelot Schellevis van het bureau Forum Standaardisatie licht de laatste meting adoptie informatieveiligheidsstandaarden (IV-meting) 2018 toe. 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 IV-standaarden 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.

Bij de gemiddelde adoptie van de webstandaarden is zichtbaar dat de groei van het gebruik zich de afgelopen maanden heeft doorgezet. Het streefbeeld van 100% wordt dit jaar echter niet meer gehaald. Aanbevolen wordt om de achterblijvers *een-op-een* te benaderen hierover. Het gebruik van de webstandaarden is hoger bij de decentrale overheden dan bij het Rijk. De gemeenten scoren het beste met een gemiddelde adoptie van 92% van de webstandaarden. Met name is een grote groei zichtbaar bij de waterschappen en provincies. De waterschappen scoren zelfs als eerste een 100%, namelijk voor TLS. Het Rijk blijft echter achter in adoptie. Dit komt onder andere door de domeinen die *redirecten* naar rijksoverheid.nl. Die domeinnamen zijn zelf nog te vaak niet beveiligd (waardoor ze misbruikt kunnen worden als springplank kunnen naar een malafide site).

Bij de gemiddelde adoptie van de mailstandaarden is te zien dat de groei in adoptie van DMARC[1], DKIM[2] en SPF[3] doorzet. Het streefmoment voor volledige adoptie van deze drie standaarden was uiterlijk eind 2017, wat ook dit jaar niet wordt gehaald. Het Rijk scoort het beste met een gemiddelde adoptie van 74%. De waterschappen hebben een grote sprong gemaakt met de adoptie van de webstandaarden, maar blijven achter bij hun adoptie van de mailstandaarden.

4C Forum-reactie Op Baseline Informatiebeveiliging Overheid

Het Forum heeft gereageerd op de Baseline Informatiebeveiliging Overheid (BIO).

Vanuit de BIO wordt teruggegeven dat zal worden verkend of o.a. de samenwerkingsinzichten uit het Beheer- en Ontwikkelmodel voor Open Standaarden (BOMOS) bij het beheer van de BIO kan worden gebruikt. Het Forum wordt hier later over geïnformeerd.

De BIO zal aan het OBDO worden voorgelegd. Aansluitend wordt de BIO voorgelegd aan de Ministerraad en mogelijk

[1] een standaard voor het veiliger maken van e-mail verkeer door het tegengaan van spam en phisingmail door misbruik van domeinnamen bij e-mail te voorkomen)

[2] een beveiligingsstandaard die een e-mailbericht aan een domeinnaam koppelt met behulp van een digitale handtekening. Het stelt de ontvanger in staat om te bepalen welke domeinnaam (en daarmee welke achterliggende organisatie) verantwoordelijk is voor het zenden van de e-mail.

[3] een standaard voor het veiliger maken van email verkeer door het tegengaan van spam en phisingmail door misbruik van domeinnamen bij e-mail te voorkomen.

opgenomen in een Algemene Maatregel van Bestuur.

Geen nadere opmerkingen.

4D Overzicht verspreiden IV-meting en monitor in achterban

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

Als voorbeeld wordt de benadering van de achterban van het CIP genoemd. Elk betrokken organisatie (in totaal 550) heeft een gepersonaliseerde mail ontvangen over zijn status (vastgesteld middels internet.nl) met betrekking tot het gebruik van de informatieveiligheidsstandaarden van de pas-toe-of-leg-uit-lijst. Het CIP biedt haar mailmerge scripts aan voor hergebruik door andere partijen (zoals koepels). Hiermee kunnen zij individuele partijen, geautomatiseerd een op hun score toegesneden mail sturen.

Bureau Forum Standaardisatie onderzoekt of een soortgelijke automatisering van een mailing kan worden geleverd voor alle leden van het Forum.

De resultaten van de IV-meting zullen worden voorgelegd aan het eerstvolgende Overheidsbrede Overleg Digitale Overheid (OBDO).

4E Sponsorschap leden Forum Standaardisatie
4F Wetsvoorstel Digitale Overheid
4G Formeel akkoord staatssecretaris van BZK op het voornemen HTTPS en HSTS te verplichten
4H BOMOS kennisbijeenkomst op 11 oktober
4I Voortgang onderzoek eDelivery (samenhang met dossier Digikoppeling)
4J Workshops toegankelijke documenten
4K Wettelijke verplichting toegankelijkheid
4L Overig nieuws

Geen nadere opmerkingen.

5 Presentatie Mijn Overheid voor Ondernemers (MOvO)

actie	Ter bespreking
tijd	11:15-11:50 uur

De geagendeerde presentatie over de digitale omgeving Mijn Overheid voor Ondernemers (MOvO) kan niet doorgaan en wordt geagendeerd voor een komende vergadering.

6 Voortgang

actie	Ter kennisname
tijd	11:50-11:55 uur
	FS 181010.**6** Voortgangsnotitie

Geen opmerkingen.

7 Rondvraag

actie	Mondeling
tijd	11:55-12:00 uur
	Geen

Verkend zal worden of het Standaardisatie Instituut voor de VerzekeringsIndustrie (SIVI), een partij die werkt aan standaardisatie in de verzekeringswereld, zich kan en/of wil aansluiten bij het Forum Standaardisatie. Hetzelfde geldt voor de Betaalvereniging bij de Veilige Email Coalitie.

8 Sluiting

actie	Mondeling
tijd	12:00 uur

De voorzitter sluit de vergadering om 12:00 uur.

Actiepunten

Monitor 2018:
- Nader onderzoeken waarom sommige standaarden minder gevraagd worden dan andere standaarden in aanbestedingen.
- Delen concept tabel voorzieningen uit monitor met Friso Penninga (Geonovum).

Overzicht verspreiden IV-meting en monitor in achterban:
- Bureau Forum Standaardisatie onderzoekt of een automatisering van een mailing gelijk aan die van CIP aan eigen achterban kan worden geleverd voor alle leden van het Forum.

- Verkend zal worden of:
    - het Standaardisatie Instituut voor de VerzekeringsIndustrie (SIVI), een partij die werkt aan standaardisatie in de verzekeringswereld, zich kan en/of wil aansluiten bij het Forum Standaardisatie.
    - de Betaalvereniging zich kan en/of wil aansluiten bij de Veilige Email Coalitie.