FS-20161214.01B

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@logius.nl
+ 31 (0) 6 5284 5592

VERSLAG FORUM STANDAARDISATIE 19 oktober 2016

Vergaderdatum en -tijd	woensdag 19 oktober 2016 9:30 tot 12:30 uur
Vergaderplaats	New Babylon (zaal 3.4) Anna van Buerenplein 29 2595 DA DEN HAAG

Aanwezig

Forum Standaardisatie

Nico Westpalm van Hoorn (voorzitter), Bob Papenhuijzen (secretaris, Logius), Erwin Bleumink (Surfnet), Cor Franke (Franke Interim Management), Gerard Hartsink (financiële sector), Gé Linssen (Ministerie van Economische Zaken), Joop van Lunteren (PBLQ HEC), Steven Luitjens (directeur Informatiesamenleving en Overheid, Ministerie van Binnenlandse Zaken), Wim van Nunspeet (CBS), Marcel Reuvers (Geonovum), Piet Ribbers (Universiteit van Tilburg), Nico Romijn (KING), Michiel Steltman (DINL), Bert Uffen, Harry Wever (als vervanger van Hans Wanders, Ministerie van Binnenlandse Zaken), Rob Verweij (Rinis)

Gasten

- Henk Wesseling (Berenschot)
- Paul Dam (VKA), agendapunt 5 Samenhang informatieveiligheidsstandaarden
- Jaap Korpel, agendapunt 7 Monitor 2016

Afwezig

Bruun Feijen (Ministerie van Financiën), David de Nood (VNO-NCW MKB-Nederland), Simon Spoormaker (Portbase, Cargonaut en COPAS), Anneke Spijker (IPO), Hans Wanders (CIO Rijk)

Bureau Forum Standaardisatie

Ludwig Oberendorff (hoofd), Marijke Abrahamse (adviseur), Désirée Castillo Gosker (adviseur), Han Zuidweg (adviseur) en Joram Verspaget (secretaris)

Nr. 1	**Opening, agenda, verslag**	Nico Westpalm van Hoorn	
bijlagen	• FS-20161019.01A Agenda • FS-20161019.01B Concept verslag Forum 8 juni 2016 • FS-20161019.01C Concept agenda Forum 14 december 2016		
Ter besluitvorming			

De voorzitter opent de vergadering en heet de aanwezigen welkom. Met name heet hij nieuw Forum-lid Rob Verweij welkom. Rob is directeur van het Routerings Instituut (inter)Nationale InformatieStromen (Rinis). Hij is door de Manifestgroep voorgedragen als opvolger van Bert Uffen.

Ter vergadering is een aangenomen motie van Oosenbrug (TK 2016-2017 32 802, nr. 31) uitgereikt. Hierin verzoekt de Kamer de regering onder andere om het gebruik van open standaarden te verplichten bij wet.

1A. Agenda

Geen opmerkingen.

1B. Concept verslag Forum 8 juni 2016

Geen opmerkingen. Vastgesteld.

1C Concept agenda Forum 14 december 2016

De volgende Forum-vergadering staat in het teken van de studiereis naar Rotterdam. Naast de reguliere agenda wordt vooral vooruitgekeken op de nieuwe kabinetsperiode en de nieuwe mandaatperiode van het Forum.

Cor Franke wijst in het kader van de nieuwe kabinetsperiode op de notitie 'Een ICT-paragraaf voor het komende regeerakkoord' van PBLQ. Deze wordt nagezonden aan het Forum [actiepunt BFS].

Finland, Italië en Estland worden genoemd als landen die vooruitlopen als het gaat om een ICT-paragraaf in een regeerakkoord.

Mogelijk bespreekpunt in december is het WRR-rapport 'publieke kern internet', waarin de WRR de protocollen en standaarden die tezamen de basisinfrastructuur van het internet vormen als mondiaal publiek goed beschouwt. Als het Forum dit rapport oppakt, adviseert Gerard Hartsink om Arnold van Rhijn (EZ) uit te nodigen en hierbij te betrekken.

Michiel Steltman ziet graag de uitgedeelde motie betrokken bij het onderdeel nieuwe mandaatperiode.

Nr. 2	**Werkplan Forum 2016/2017**	
bijlagen	• FS-20161019.02 Oplegnotitie • FS-20161019.02A Bijgewerkt werkplan voor 2017	
Ter bespreking		

2A. Bijgewerkt werkplan voor 2017

Ludwig Oberendorff geeft een korte toelichting op het werkplan. Om de Goals beter te kunnen realiseren is een aantal actiepunten toegevoegd en gewijzigd. Ook is een Strategie toegevoegd om taken en verantwoordelijkheden te borgen met het oog op een nieuwe mandaatperiode. Ook de verkennende onderzoeken hebben een structurele plaats in het werkplan (dashboard onder c, actieplan onder 3). Het Forum stemt in met het werkplan.

Nr. 3	**Open standaarden, lijsten**	Wim van Nunspeet
bijlagen	• FS-20161019.03 Oplegnotitie • FS-20161019.03A AdES Baseline Profiles • FS-20161019.03B Nieuwe versie SMeF • FS-20161019.03C Aanpassen Webrichtlijnen • FS-20161019.03D Update lijst met aanbevolen standaarden	
Ter besluitvorming en kennisname		

Wim van Nunspeet licht namens de Stuurgroep Open standaarden de voorgelegde punten toe.

3A. AdES Baseline Profiles

Naar aanleiding van de expertbijeenkomst en openbare consultatie staan er naar inzien van de stuurgroep Open Standaarden nog te veel vragen open om al te kunnen besluiten over opname van de AdES Baseline Profiles-standaard op de pas toe of leg uit-lijst. Het Forum wordt daarom geadviseerd om samen met de indiener van de standaard deze vragen nader uit te zoeken voordat wordt ingestemd met een eventuele opname.

Rob Verweij meldt namens Bruun Feijen dat de Belastingdienst akkoord is met een nader onderzoek en graag mee wil helpen.

Harry Wever meldt namens Hans Wanders het eens te zijn met de inhoud. Wel dient gecommuniceerd te worden dat een elektronische handtekening niet altijd noodzakelijk is. Ook moet goed naar het toepassingsgebied gekeken worden. Ten aanzien van het punt dat de elektronische handtekening niet altijd noodzakelijk is, geeft Cor Franke aan dat de vernieuwde handreiking betrouwbaarheidsniveaus ook andere opties noemt.

Het Forum stemt in met het voorstel tot nader onderzoek.

3B. Nieuwe versie SMeF

Akkoord.

3C. Aanpassen Webrichtlijnen

Meegenomen in het additioneel advies wordt dat het College voor de Rechten van de Mens niet de partij is voor het monitoren en evalueren van de voortgang. Het primaat van het meten dient bij Logius te liggen, afhankelijkheid van een derde partij is niet wenselijk. Een beheerder van de 'Principe Universeel'-standaard is er niet. Desondanks wordt deze standaard meegenomen op de lijst aanbevolen, omdat deze te goed wordt bevonden om helemaal van de lijsten te halen.

3D. Update lijst met aanbevolen standaarden

Het Forum stemt in met de update.

Aandacht wordt gevraagd voor de ontwikkelingen rond WSRM dat nu onderdeel is van Digikoppeling 3.0. Nu de behoefte aan WSRM als standaard op de ptolu lijst (als onderdeel van Digikoppeling 3.0) lijkt te zijn verdwenen, is de vraag aan de aanmelder/beheerder van Digikoppeling 3.0 (BZK-DIO/Logius) wat dat betekent voor de aanmelding van Digikoppeling 3.0 inclusief WSRM. Wordt WSRM uit Digikoppeling 3.0 verwijderd?

Wat daarbij aanvullend speelt is dat EbMS door het European Multistakeholders Platform is 'geïdentificeerd' (goedgekeurd voor implementatie door de lidstaten, d.w.z. te vragen bij aanbestedingen) en geen onderdeel van Digikoppeling 3.0. Het gaat daarbij om versie 3.0 van EbMS. Deze is aangedragen door het eSense-project en door het MSP als standaard voor asynchrone communicatie goedgekeurd. Versie 3.0 is niet backward compatible met versie 2.0.

Het Bureau legt contact met de aanmelders/beheerders van Digikoppeling 3.0 [actiepunt BFS].

Nr. 4	**Open standaarden, adoptie**	Wim van Nunspeet
bijlagen	• FS-20161019.04 Oplegnotitie • FS-20161019.04A Onderzoek Samenhang IV-standaarden • FS-20161019.04B Meting IV-standaarden • FS-20161019.04B1 Gebruiksgegevens domeinen Nationaal Beraad • FS-20161019.04B2 Gemeentescores per domein • FS-20161019.04C PvA adoptieondersteuning documentstandaarden • FS-20161019.04D Handreiking Open Standaarden bij inkopen	
Ter besluitvorming en kennisname		

Wim van Nunspeet licht namens de Stuurgroep Open standaarden de voorgelegde punten toe.

4A. Onderzoek Samenhang IV-standaarden
4B. Meting IV-standaarden

Aan de hand van een aantal infographics licht Ludwig Oberendorff de meting iv-standaarden van augustus toe. Voor het eerst worden ook gemeentelijke domeinnamen meegemeten. De oproep aan gemeenten is om eventuele ontbrekende (transactie)domeinen aan te melden (de IBD zet die vraag ook uit).

De toepassing van de veiligheidsstandaarden op het gebied van internet en email in de publieke sector is verder gestegen. Desalniettemin is de groei nog steeds dusdanig dat bij gelijke groei de standaarden eind 2017 nog niet overal – waar relevant – zijn

toegepast. Dit ondanks het streefbeeld en de adoptieimpuls die in februari in het Nationaal Beraad is afgesproken.
De vraag aan het Forum is hoe deze meting in het Nationaal Beraad te agenderen en wat het Forum kan doen om de adoptie verder op gang te brengen.

In de bespreking komen de volgende punten naar voren:

- Over de kwaliteit en wenselijkheid van de toepassing van deze standaarden is geen discussie. Die is respectievelijk eerder uitgebreid getoetst in de aanmeldprocedure (en op de lijst gezet door het College en daarna Nationaal Beraad), én er is een adoptieimpuls met streefbeeld afgesproken in het Nationaal Beraad.
- De kwaliteit van de standaarden wordt door de industrie krachtig onderschreven met de term 'basis-hygiëne'. Aanbieders van internetfaciliteiten, i.e. hosters, registrars, service en telecom providers die de standaarden niet ondersteunen zijn in de sector ongewenste uitzonderingen.
- Het is dus een kwestie van discipline om de adoptie ervan nu ook door te zetten, juist nu die achterblijft. Daar is een strak signaal voor nodig.
- Het Forum agendeert de meting daarom bij het Nationaal Beraad met een *call-for-action*. Het zijn immers de overheidsorganen (die nog niet voldoen) zélf die daar iets aan kunnen veranderen.
- De cijfers van de meting kunnen daarvoor goed worden ingezet, zo geeft Gé Linssen aan, die met de meting als signaalfunctie met DICTU een adoptieplan heeft afgesproken.
- Het Nationaal Beraad zou bijvoorbeeld rechtstreeks bij de CIO's en in het CIO-beraad dit geluid kunnen laten horen.
- Rob Verweij biedt aan het signaal te agenderen/presenteren in de Manifestgroep.
- Daarop aanvullend wordt aangegeven dat het signaal op individuele organisatie basis gebruikt kan worden om het gesprek aan te gaan.
- Daarnaast kan het Forum en het bureau nog meer inzetten op communicatie van de voordelen van het toepassen van iv-standaarden: het nut. Geredeneerd vanuit de business en eindgebruiker en niet vanuit de standaard. Daarnaast is meer duidelijkheid over de toepassingsgebieden gewenst (zie agendapunt 5).

4C. PvA adoptieondersteuning documentstandaarden

Het Forum ziet graag dat de nadruk wordt gelegd op publiceren en bewaren en niet op bewerken.

Het Forum stemt daarom in met de notitie.

4D. Handreiking Open Standaarden bij inkopen

Het Forum is akkoord met de handreiking en dankt de CBA voor het goede werk. Over de bestekteksten worden workshops en in house-cursussen georganiseerd. Een uitnodiging hiervoor volgt [actiepunt BFS].

Nr. 5	**Samenhang informatieveiligheids-standaarden**	Paul Dam (VKA)
Presentatie + standpuntneming		

Paul Dam (VKA) licht de bevindingen in het rapport 'Samenhang in ICT-beveiligingsstandaarden' van VKA toe.

Het Forum had gevraagd om inzicht te geven in de samenhang tussen de beveiligingsstandaarden en het identificeren van witte vlekken hierbij. VKA adviseert in dit kader om de BIO met prioriteit te ontwikkelen en te verwijzen naar richtlijnen per taakgebied, dit met een overheidsbrede governance. In deze governance moeten de acties, de inhoudelijke aansluiting en de consistentie bewaakt worden. Witte vlekken waar actie op nodig is zijn eID en vertrouwensdiensten, nieuwe kanalen elektronische dienstverlening, veilige applicatie-ontwikkeling, veilig profiel voor email, privacy-by-design, Internet of Things, Cloud en cyberthreats.

In de daaropvolgende bespreking in het Forum komt een aantal punten naar voren:

- Het piramideplaatje geeft overzichtelijk weer wat de verhouding is tussen de operationele informatieveiligheidsstandaarden op de ptolu-lijst en hogere kaders, zoals wetgeving, de informatieveiligheid standaard ISO27001/2 en BIO/BIR/BIG/BIWA.
- Daardoor wordt ook duidelijk dat die operationele informatieveiligheid standaarden (zoals TLS, DNSSEC, DKIM, SPF etc.) de operationele invulling zijn om te kunnen voldoen aan die hogere – abstracter geformuleerde – kaders. Tegelijkertijd maakt het plaatje duidelijk dat informatieveiligheid veel breder is dan de standaarden op de ptolu-lijst.
- Een van de voorstellen van de onderzoekers is om de samenhang tussen de verschillende lagen structureel te waarborgen door het inrichten van een governance-structuur. Het is echter evident dat het verantwoordelijk maken van één partij als centrale actor voor die governance niet gaat werken. Dat brengen zowel Henk Wesseling (voorzitter van de informele interbestuurlijke werkgroep normatiek, voortgekomen uit de taskforce Bestuur en Informatieveiligheid Dienstverlening (BID) als Steven Luitjens naar voren.
- Steven Luitjens licht verder toe dat de huidige stand van zaken is dat informatiebeveiliging terugkomt in de tweede tranche (in plaats van de eerste tranche) van de wet GDI. Hij geeft verder aan dat het van belang is om dit in kleine stappen op te pakken en niet in één keer. Tegelijkertijd is het niet verstandig om stappen te nemen zonder eindplaatje te willen oppakken. Het streven is naar een BIO en als tussenstap kan BIR 2.0 worden opgepakt. Qua governance moeten stappen moeten worden gemaakt naar een 'leidende coalitie' in plaats van één partij (zoals BZK/DIO) bovenin de piramide als systeemverantwoordelijke.
- De focus zou moeten liggen op dingen die voor burgers en bedrijven belangrijk zijn. Als daarover afspraken gemaakt zijn, zou men elkaar moeten houden aan gemeenschappelijke afspraken (inderdaad niet één partij).
- Samenhang is zeer belangrijk. Vanuit de hosting-industrie ziet men een megaprobleem opdoemen. Regie is van belang, want alleen bij convergerende eisen is compliance nog haalbaar. Auditresultaten zouden bijvoorbeeld herbruikbaar moeten zijn, anders hebben hostingpartijen alleen al een dagtaak aan het faciliteren van telkens – inhoudelijk dezelfde - audits.
- De conclusies uit het rapport zullen positief door de financiële sector worden ontvangen. In het kader van SWIFT is een nader gesprek met DNB wel gewenst.
- Dilemma's zijn:
  a) of het onderwerp, dat op zichzelf al groot genoeg is, wel kan worden opgevangen met een totaaloplossing, terwijl ophakken in kleinere delen het risico met zich meebrengt van eilandoplossingen zonder direct einddoel voor ogen.
  b) of met het oog op doorzetten één regisserende partij met eindverantwoordelijkheid gewenst is of dat de oplossing gevonden moet worden in regie door (polder)overleg. Daarnaast komt de vraag naar voren of een regiegedachte niet sowieso botst met de realiteit van de zich snel ontwikkelende en daarmee moeilijk te regisseren IT-sector.
- Andere kwesties die spelen zijn ketendenken versus interne systemen, (vertrouwen op) procedures versus (vertrouwen op) professionals en business cases met risicoanalyse (met een duidelijke waarom-vraag) versus normalisatie (via het NEN en daarmee zonder waarom). Dat laatste is overigens standaardafhankelijk (voor

sommige basishygiëne standaarden is de risicoanalyse al gemaakt, zie agendapunt 4).

- Ook is het gebruik van bestaand instrumentarium gewenst. Gevraagd wordt te kijken naar COBIT- en SABSA-methodestandaarden voor het inregelen van (standaarden voor) informatieveiligheid binnen een IT-beheeromgeving. Organisaties worden daarbij geholpen met handreikingen (best practices) over informatieveiligheid voor de opbouw van de architectuur.

De geschetste problematiek zal worden geagendeerd voor het Nationaal Beraad [actiepunt BFS]. Ook moeten deze kwesties worden meegenomen in de processen bij totstandkoming van de volgende BIR en/of BIO. In ieder geval moeten naast overheidspartijen ook partijen buiten de overheid betrokken zijn, zoals het bedrijfsleven, het bankwezen en maatschappelijke organisaties.

Geconcludeerd wordt dat informatieveiligheid veel breder is dan alleen toepassing van de iv-standaarden. Het gesprek erover mag daarom niet verengd worden tot deze standaarden, ook al spelen die standaarden een duidelijke rol. De rol van het Forum is dus eerder signalerend en agenderend dan dat het Forum zélf de partij is om deze problematiek verder te brengen. Gezocht gaat worden naar op welke wijze en door welke partij(en) dit verder gebracht kan worden, bijvoorbeeld naar het Nationaal Beraad.

Voor de studiereis van december zal het bureau zorgen voor een nadere aanpassing van het rapport en op zoek gaan naar een kansrijke manier om dit verder te brengen. Het onderwerp komt daar opnieuw aan de orde bij o.a. het vooruit kijken naar een nieuwe kabinets- en mandaatperiode [actiepunt BFS].

Nr. 6	**Handreiking betrouwbaarheidsniveaus**	Cor Franke
Presentatie		

Cor Franke geeft een toelichting op de handreiking betrouwbaarheidsniveaus. De handreiking heeft als doel overheidsorganisaties te helpen die e-diensten leveren aan burgers en bedrijven een goed onderbouwde afweging te maken ten aanzien van de benodigde betrouwbaarheidsniveaus voor die diensten.

De handreiking wordt door Cor gepresenteerd op het ECP-jaarcongres. Verkend wordt of er met eID een combinatie kan worden gemaakt op het ECP-congres [actiepunt BFS]. Ook zal de handreiking worden vertaald in het Engels [actiepunt BFS].

Nr. 7	**Monitor 2016**	Jaap Korpel (ICTU)
Toelichting		

Jaap Korpel (ICTU) licht de eerste resultaten van de Monitor toe.

Een van de bevindingen tot dusver is dat een deel van de beheerorganisaties van de open standaarden op de lijst het niet relevant lijkt te vinden in hoeverre hun standaarden worden gebruikt. Ten aanzien van de aanbestedingen blijkt dat de verbetering van vorig jaar is vastgehouden en licht verbeterd, maar dat het percentage waarin alle of alle cruciale standaarden is gevraagd is afgenomen. Ten aanzien van de

adoptie van standaarden in voorzieningen zijn er meer standaarden ter implementatie ingepland. De daadwerkelijke adoptie is procentueel gelijk gebleven.

De duiding en maatregelen die het Forum voorstelt wordt besproken tijdens de studiereis van het Forum in december. Dan zal de Monitor opnieuw geagendeerd worden aan de hand van het concept rapport [actiepunt BFS].

Nr. 8	**Aard verplichting pas-toe-of-leg-uit-lijst**	
bijlagen	• FS-20161019.08 Notitie aard verplichting ptolu-lijst	
Ter kennisname		

Het voorstel is om een analyse te maken van de functionele toepassingsgebieden op de ptolu-lijst, een prioritering te maken van waar het functioneel toepassingsgebied duidelijker kan en voor die geprioriteerde standaarden aan het Forum een voorstel te doen van wat de omschrijving zou moeten zijn. Daarbij komt ook de samenhang met andere normenkaders aan de orde en wordt een overzicht geboden van de verschillende soorten lijsten.

Hierbij moet consequent worden benadrukt dat de pas-toe-of-leg-uit-lijst een gezamenlijke afspraak betreft van in het Nationaal Beraad op hoogambtelijk niveau, overheidsbreed en van beleid en uitvoering. Dit is relevant voor de beeldvorming. Het is immers niet het Forum dat besluit.

Mede gelet op de discussie bij agendapunt 4, waarin een aantal 'basishygiëne' informatieveiligheidsstandaarden met kracht moet worden verder gebracht, stemt het Forum in met de aanpak in de notitie.

Nr. 9	**Informele analyse Qiy en Trusttester**	
bijlage	• FS-20161019.09 Oplegnotitie	
Ter kennisname		

Geen opmerkingen.

Nr. 10	**Voortgang**	
bijlagen	• FS-20161019.10 Voortgangsnotitie	
Ter kennisname		

Geen opmerkingen.

Nr. 11	Rondvraag	
Mondeling		

Geen opmerkingen.

Nr. 12	Sluiting		

Bert Uffen en Harry Wever nemen afscheid van het Forum. Harry begint binnen de Rijksoverheid bij het Ministerie van Infrastructuur en Milieu aan een andere uitdaging. Bert blijft aan het werk in de SUWI-keten en laat zich – op voordracht van de Manifestgroep - opvolgen door Rob Verweij.

De voorzitter dankt beiden voor hun tomeloze inzet voor het Forum en hun pleidooi voor het gebruik van open standaarden. Hij overhandigt – onder applaus van de overige Forumleden - aan ieder een presentje als aandenken en teken van dank.

Actiepunten:
- Nasturen aan Forum van PBLQ-notitie 'Een ICT-paragraaf voor het komende regeerakkoord'.
- Nasturen aan Forum van uitnodiging ECP-jaarcongres.
- Oppakken Digikoppeling 3.0 in overleg met de beheerder.
- Verzenden uitnodigingen voor workshops en in house-cursussen over bestekteksten.
- Agenderen problematiek rond internetveiligheidsstandaarden in NB.
- Aangepast rapport Samenhang interveiligheidsstandaarden voor studiereis Forum december.
- Verkennen combinatie eID met Handreiking Betrouwbaarheidsniveaus op ECP-jaarcongres.
- Monitor 2016 agenderen voor Forum december, inclusief de duiding en maatregelen die het Forum hierbij heeft voorgesteld.