notitie

Forum Standaardisatie
www.forumstandaardisatie.nl
forumstandaardisatie@logius.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 19 oktober 2016
Agendapunt 4. Open standaarden, adoptie
Stuknummer 4. Oplegnotitie adoptie

Van:	Stuurgroep open standaarden
Aan:	Forum Standaardisatie
Bijlagen:	• FS-20161019.04A Onderzoek samenhang Informatiebeveiligingstandaarden • FS-20161019.04B Meting IV-standaarden (incl. 2 bijlagen) • FS-20161019.04C PvA adoptieondersteuning documentstandaarden • FS-20161019.04D Handreiking Open Standaarden bij inkopen (‘Bestekteksten’) • FS-20161019.04E Brief CBA

Ter bespreking
U wordt gevraagd het volgende punt te bespreken:

1. Onderzoek samenhang Informatiebeveiligingstandaarden [presentatie & bijllage]
2. Meting informatieveiligheidsstandaarden [bijlage]
3. Plan van aanpak adoptieondersteuning documentstandaarden [bijlage]

Ter kennisname
U wordt gevraagd om kennis te nemen van:

4. Concept Monitor 2016 [presentatie]
5. Definitieve Handreiking Open Standaarden bij inkopen (‘Bestekteksten’) [bijlagen]

Ter bespreking

Ad 1. Onderzoek Samenhang Informatiebeveiligingstandaarden [presentatie en bijlage]

Achtergrond
Bijgaand treft u het adviesrapport aan dat VKA heeft opgeleverd over samenhang in ICT-beveiligingsstandaarden voor de overheid. Door het Forum Standaardisatie is in de oplegnotitie "Adoptie open standaarden" van 10 juni 2015 de behoefte geuit om meer overzicht en samenhang te verkrijgen in huidige ICT-beveiligingsstandaarden op de diverse lijsten van het Forum én in mogelijke toekomstige uitbreidingen van de lijsten op dit gebied.

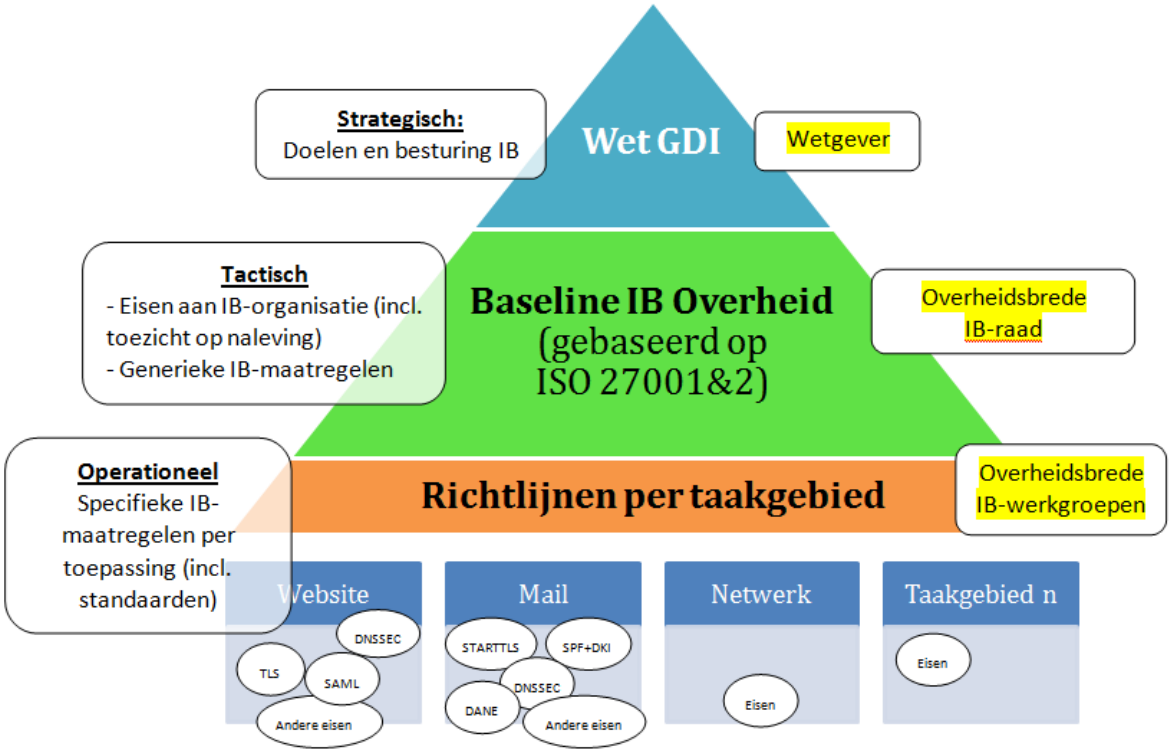
Inhoud
In het bijgaande adviesrapport komen 3 zaken aan de orde:

1. Ordening van bestaande ICT-beveiligingsstandaarden en aanpassingen van de lijst gangbare/aanbevolen standaarden. Hiervan is in bijlage A van het rapport een weergave te vinden. De resultaten van dit deel van het onderzoek zijn integraal meegenomen in het onderzoek "Aanvullende aanbevolen standaarden".
2. Een met stakeholders opgestelde lijst van aanbevolen acties omtrent ICT-beveiligingsstandaarden. Deze acties komen in hoofdstuk 5 van het rapport aan bod.
3. Naast de bovenstaande punten komt in de analyse en het advies van de onderzoekers nadrukkelijk ook de governance-problematiek aan bod, waar twee verschillende invalshoeken zijn belicht. Enerzijds is er overlap in de vele eisen die door verantwoordelijke organisaties worden gesteld en anderzijds is het voor uitvoerende organisaties een zoekplaatje om te bepalen welke ICT-beveiligingsstandaarden van toepassing zijn, wat hun onderlinge verhouding is en welke status deze hebben.

Advies
Op het laatste punt constateren de onderzoekers een behoefte aan coördinatie tussen de verschillende partijen binnen Nederland die normatieve documenten en richtlijnen opstellen, waarbij tevens een model wordt aangereikt om te komen tot het minder versplinterd aanbevelen van losse ICT-beveiligingsstandaarden.

Het advies is om met urgentie te werken aan een geharmoniseerd normenkader voor informatiebeveiliging dat overheidsbreed verplicht is en voldoende diepgang kent. Het uitgangspunt daarvoor is één overheidsbreed basisniveau voor informatiebeveiliging (op tactisch niveau) in de vorm van de **Baseline Informatiebeveiliging Overheid**. Deze BIO krijgt diepgang door (op uitvoerend niveau) **richtlijnen per inhoudelijke taakgebied** (bijv. voor website, e-mail, netwerken etc.) vast te stellen en daarin ook technische standaarden (zoals HTTPS en DNSSEC) te positioneren. De **status** van en de **governance** (zoals vaststellingsprocedure) voor een BIO inclusief de onderliggende operationele richtlijnen dienen (op strategisch niveau) **wettelijk verankerd** te zijn.

Een en ander zal leiden tot meer duidelijkheid en betere toepassing. Ook helpt het om verantwoordingen en audits eenvoudiger en beter te maken.



Dit is een aanbeveling die de rol van het Forum Standaardisatie overstijgt. Tegelijkertijd kan het Forum in samenwerking met andere partijen wel een stimulerende rol vervullen om deze transitie te realiseren.

In het Forum willen we het rapport, na een inleiding door een van de betrokken onderzoekers van VKA, behandelen aan de hand van de volgende vragen:

1) Herkent het Forum zich in de geschetste situatie op het gebied van governance?
2) Wil het Forum dit issue omtrent de governance (mede-)agenderen bij de Regieraad Interconnectiviteit en het Nationaal Beraad?
3) Welke rol wenst het Forum in het proces om tot verbetering van de governance te komen? Is het Forum bereid om (mede-) opdrachtgever te zijn voor een opdracht om draagvlak te verwerven om dit issue aan te pakken in samenwerking met alle stakeholders?
4) Heeft het Forum een beeld welke rol zij zelf zou willen vervullen in het uiteindelijk resulterende speelveld?

Indien de tijd het toelaat zouden we ook graag de discussie over de concrete standaardisatieacties (onderwerp 2 van het onderzoek) voeren.

Ad 2. Meting Informatieveiligheidsstandaarden [bijlage]

Achtergrond
Het Nationaal Beraad sprak eind 2015 de ambitie uit om de informatieveligheidsstandaarden (DNSSEC, TLS, DKIM, SPF en DMARC) versneld te adopteren en bovendien over de voortgang te rapporteren.
Voorliggende meting gaat daarom niet alleen naar het Nationaal Beraad, maar is ook onderdeel van de Monitor OSB 2016.

Resultaten
De meest recente meting bevat naast de eerder gemeten 152 (niet gemeentelijke) Nationaal Beraad domeinen, nu ook 398 gemeentelijke domeinen.

Uit de meest recente meting van augustus 2016, blijkt dat, bij beide sets met domeinen, het groeitempo van de adoptie nagenoeg gelijk is (ca. 14% per jaar).

Dit betekent dat de adoptie van de IV-standaarden niet is versneld. Met het huidige groeitempo is de gemiddelde adoptie van de genoemde standaarden eind 2017 ca. 70%

De bijgevoegde notie bevat daarom een oproep aan het Nationaal Beraad om aan de slag te gaan met deze standaarden. Uit de impactanalyse en verschillende factsheets die de IBD heeft laten opstellen voor deze standaarden[1] blijkt dat de kosten en inspanning om aan deze standaarden te voldoen geen belemmering vormen.

Bureau Forum Standaardisatie kan bovendien helpen bij vragen en onduidelijkheden.

Ad 3. Plan van aanpak adoptieondersteuning documentstandaarden [bijlage]

De documentstandaarden op de 'pas-toe-of-leg-uit' lijst vormen een heterogene groep standaarden met uiteenlopende toepassingsgebieden. De ondersteuning van de adoptie van deze standaarden is daardoor niet triviaal. Waar PDF/A bijvoorbeeld al veel wordt gebuikt bij de overheid, stuit ODF nog op actieve weerstand.

Het Bureau Forum Standaardisatie achtte het daarom relevant om een plan van aanpak te maken voor de adoptieondersteuning van documentstandaarden. Het plan heeft tot doel om documentstandaarden een adoptie impuls te geven, rekening houdend met de het actuele draagvlak van de diverse standaarden en de complexiteit van hun toepassingsgebied.

We vragen het Forum het plan van aanpak te bespreken en feedback te geven. We verwelkomen commentaar, suggesties en eventuele accentverschuivingen voor het plan van aanpak.

[1] *Zie https://www.ibdgemeenten.nl/ibd-publiceert-factsheets-e-mailauthenticatie/ & https://www.ibdgemeenten.nl/3619-2/*

Ter kennisname

Ad 4. Concept Monitor 2016 [presentatie]

In de Forumvergadering van juni stemde het Forum in met het definitieve plan van aanpak voor de Monitor open standaarden Beleid 2016. De eerste resultaten worden tijdens dit Forum overleg gepresenteerd **(Agendapunt 8)** . In de Forumvergadering van december zal de Monitorrapportage voorliggen ter besluitvorming.

In grote lijnen bestaat de Monitor uit drie hoofdonderdelen en één aanvullend onderdeel:

A. Gebruiksgegevens (feitelijke toepassing van open standaarden)
B. Voorzieningen (toepassing van relevante open standaarden)
C. Aanbestedingen 2e helft 2015 & 1e helft 2016 (compliance aan 'pas toe of leg uit')
D. *Aanvullend:* Leveranciers (ervaringen als input voor open standaardenbeleid)

[A] Gebruiksgegevens

Internet en beveiliging
De Monitor bevat een onderzoek naar het gebruik cq. het toepassen van **DKIM**, **DMARC**, **DNSSEC**, **TLS** en **SPF** en daarnaast van **IPv6** m.b.v. de webtool internet.nl Hiervoor wordt de BFS-set van domeinnamen gehanteerd, die bestaat uit ongeveer 150 unieke domeinen (Nationaal Beraad, GDI voorzieningen en deelnemende partijen)

Document en (web)content
Onderzoek naar het voldoen aan **Webrichtlijnen** voor de set domeinnamen van BFS (zie 1), o.b.v. gegevens van Waarmerk Drempelvrij.

Overige standaarden
Uitvraag van gegevens over het gebruik onder beheerorganisaties voor de overige standaarden van de lijst.

[B] Voorzieningen

ICTU heeft **37 generieke voorzieningen** onderzocht**:**
a. 29 van de voorzieningen die samen de GDI (Generieke Digitale Infrastructuur) vormen

b. en 8 overige generieke voorzieningen die vorige jaren zijn onderzocht.

Net als vorig jaar onderzocht ICTU welke open standaarden relevant zijn voor de voorziening, in hoeverre de voorziening daaraan op dit moment voldoet en indien niet of er expliciete plannen zijn om daaraan binnenkort te gaan voldoen.

[C] Aanbestedingen

Onderzoek van **aanbestedingen** op basis van openbare documenten **(pas toe)**
34 aanbestedingen Rijksoverheid + 16 van mede-overheden.

De aanbestedingen worden in twee rondes beoordeeld: eerst Q3+Q4 2015 en in de zomer Q1 2016 & Q2 2016.

De resultaten worden door BFS besproken met de aanbestedende partijen die daarom vragen en/of waar BFS zelf graag mee wil spreken (iig 10 partijen) .

Audit van jaarverslagen (leg uit): voor alle organisaties die bij één of meer aanbestedingen in 2015 (Q1+Q2 o.b.v. onderzoek vorig jaar, Q3+Q4 o.b.v. onderzoek dit jaar) niet om alle relevante standaarden hebben gevraagd wordt nagegaan in hoeverre zij in het jaarverslag over 2015 daarover expliciet verantwoording hebben afgelegd.

[D] Leveranciers *(resultaten worden gepresenteerd in december)*

Gesprekken met acht à tien leveranciers om enerzijds te achterhalen of en hoe zij in aanbestedingen van overheden de vraag om open standaarden terug zien komen en hoe zij daarmee omgaan. Anderzijds zijn leveranciers bevraagd naar welke relevante ontwikkelingen zij zien, waar het Forum actief op zou moeten aanhaken.

5. Definitieve Handreiking Open Standaarden bij inkopen (‘Bestekteksten’) [bijlagen]

De interdepartementale Commissie Bedrijfsjuridisch Advies (CBA) heeft op 18 augustus 2016 per brief een positief advies gegeven over de Handreiking Open Standaarden bij inkopen.

De enkele in het positieve CBA-advies genoemde verbeterpunten zijn inmiddels verwerkt in een definitieve versie van de handreiking. Deze zal gepubliceerd worden op de website van het Forum Standaardisatie. Daarnaast organiseert Bureau Forum Standaardisatie rondom de handreiking en de beslisboom workshops voor inkopers en juristen. De eerste vond plaats op 15 september.

Forum-leden wordt gevraagd om de handreiking actief door te geleiden naar inkopers en andere geïnteresseerden binnen de eigen organisatie en hen te attenderen op de workshops.