FS-20160315.06

notitie

FORUM STANDAARDISATIE 15 maart 2016
Agendapunt 6. Open standaarden, adoptie
Stuknummer 6. Oplegnotitie adoptie

Van:	Stuurgroep open standaarden
Aan:	Forum Standaardisatie
Bijlagen:	A: PvA Handreiking betrouwbaarheidsniveaus v4 B: Handreiking open standaarden bij ICT inkoop C: Impactanalyse DMARC+SPF+DKIM (KING/IBD) D: Factsheet TLS (KING/IBD) E: Factsheet DNSSEC (KING/IBD)

Ter Besluitvorming
U wordt gevraagd in te stemmen met:

1. Plan van Aanpak voor nieuwe versie van handreiking betrouwbaarheidsniveaus

Ter bespreking
U wordt gevraagd te discussiëren over:

2. Nieuwe handreiking Open Standaarden bij ICT-inkoop (Forumpresentatie door Wob Rombouts)

3. Impactanalyse en factsheets beveiligingsstandaarden KING/IBD (Forumpresentatie door Peter van Dijk)

Ter kennisname
U wordt gevraagd om kennis te nemen van:

4. Voortgang onderzoek beveiligingsstandaarden VKA

5. Workshop mailauthenticatiestandaarden

6. Voortgang Internet.nl

7. De factsheets TLS en DNSSEC

Ter Besluitvorming

Ad 1. Plan van Aanpak voor nieuwe versie van handreiking betrouwbaarheidsniveaus [Bijlage A]
(Toelichting door Cor Franke)

Gevraagd besluit

He Forum Standaardisatie wordt gevraagd in te stemmen met het bijgevoegde plan van aanpak om te komen tot een nieuwe versie van de handreiking betrouwbaarheidniveaus.

Achtergrond

Op 2 december jongstleden vond een bijeenkomst plaats van de Klankbordgroep voor de Handreiking Betrouwbaarheidsniveaus. Tijdens de goed bezochte bijeenkomst besprak de klankbordgroep de recente ontwikkelingen in het authenticatiedomein en de mogelijke impact van die ontwikkelingen op de handreiking betrouwbaarheidsniveaus. De conclusie van de klankbordgroep was dat een aantal recente aanpassingen in wet- en regelgeving een actualiseringslag van de handreiking noodzakelijk maakt. De constateringen en conclusie van de klankbordgroep zijn tijdens het forumoverleg van 16 december met u gedeeld.

Wat ligt voor

Op basis van de constateringen van de klankbordgroep en een aantal aanvullende gesprekken met experts is een plan van aanpak opgesteld om te komen tot een nieuwe versie van de handreiking.

Belangrijkste wijzigingen die een actualisatieslag noodzakelijk maken:

- De komst van de eIDAS-verordening en de bijbehorende methodiek voor bepalen betrouwbaarheidsniveaus;
- Veranderingen in de AWB / Wet Elektronisch Bestuurlijk Verkeer en de komst van de EU Privacy-verordening;
- Het verlaten van de CBP norm A&V 23 voor de beveiliging van persoonsgegevens ten faveure van een geheel procesgerichte, open norm “Richtsnoeren beveiliging persoonsgegevens”.

Er is onveranderd een grote behoefte aan een handreiking voor e-dienstverleners. Deze moet inzichtelijk maken wat er rond eID’s en vertrouwensdiensten op dienstverleners afkomt en welke keuzes daarin zijn te maken, juist in de huidige periode waarin er veel in wet- en regelgeving wijzigt.

Voorgestelde wijzigingen, door te voeren in de nieuwe versie van de handreiking:

1. De systematiek voor de definitie van betrouwbaarheidsniveaus gaat naar de eIDAS-indeling (inclusief transitietabel van STORK naar eIDAS).
2. De eisen met betrekking tot authenticatie, zoals die voor de Wet GDI in voorbereiding zijn, zullen een gepaste plaats krijgen in de handreiking.

3. Toevoeging van een indeling voor de privacygevoeligheid van een dienst in relatie tot het betrouwbaarheidsniveau van de authenticatie.

4. De juridische paragrafen zullen aan de huidige juridische situatie worden aangepast, c.q. aan de te verwachten juridische situatie per medio 2016.

5. Het hoofdstuk ondertekenen wordt aangepast aan de eIDAS-verordening.

6. Nieuwe eIDAS-vertrouwensdiensten worden middels korte teksten toegelicht. (Het betreft dan met name tijdstempels, elektronische zegels en elektronische bezorgdiensten).

Ter attentie:

- De nieuwe privacy-verordening die per 2018 ingaat wordt niet opgenomen in de nieuwe versie.

- De diepgang van de behandeling van vertrouwensdiensten zal in deze versie nog beperkt zijn.

- De nieuwe versie zal nog geen aandacht geven aan Bevoegdheden als uitbreiding op Machtigingen. Dit is een onderwerp voor toekomstige uitbreiding wanneer het gedachtegoed rond bevoegdheden in het eID-Stelsel / Stelsel Elektronische Toegangsdiensten is uitgekristalliseerd.

Planning en tijdslijn

De uitvoering start medio maart 2016 en het resultaat kan naar verwachting in **oktober 2016** aan het Forum worden voorgelegd.

Mensen die zich willen aanmelden voor de klankbordgroep kunnen dat doen bij Maarten van der Veen (Maarten.vander.veen@logius.nl)

Ter bespreking

Ad 2. Nieuwe handreiking Open Standaarden bij ICT-inkoop [Bijlage B]

Aanleiding

In 2013 heeft het Forum Standaardisatie het document "Generieke bestekteksten voor verplichte ICT-standaarden" gepubliceerd[1]. Aanbestedende diensten hebben de afgelopen jaren de wens geuit om meer specifiek per open standaard suggesties voor bestekteksten ter beschikking te hebben. Om die reden is mede op basis van de generieke teksten deze handreiking samengesteld. De handreiking bevat specifieke bestekteksten voor de verplichte standaarden uit de domeinen 'Internet en Beveiliging' en 'Document en (web)content'.

Doel en doelgroep

Het doel van het document is om inkooporganisaties van aanbestedende diensten te ondersteunen in het uitvragen van verplichte Open Standaarden en het 'pas toe of leg uit'-principe op een juiste wijze te hanteren.

De handreiking stelt de inkoper van ICT-systemen in staat om de verplichte open standaarden op een goede wijze op te nemen in aanbestedingsdocumenten en dit af te stemmen met andere betrokkenen zoals de opdrachtgever.

De doelgroep is daarmee in eerste instantie de inkoper bij een aanbestedende dienst die te maken heeft met een inkoopproject met ICT-aspecten. Daarnaast kunnen de aanwijzingen in dit document de ICT-materiedeskundige, de jurist en de opdrachtgever ondersteunen.

Afronding

Bijgevoegde versie is het laatste concept welke is voorgelegd aan onder andere de Interdepartementale Commissie Bedrijfsjuridisch Advies (CBA). Eventueel commentaar wordt samen met de opmerkingen van het Forum verwerkt in de definitieve versie. De definitieve versie wordt vervolgens gepubliceerd op onder andere de website van Pianoo (het expertisecentrum aanbesteden van de publieke sector) en de website van het Forum Standaardisatie. Daarnaast zal BFS in 2016 de nodige workshops en promotieactiviteiten inzetten om de handreiking onder de aandacht te brengen van inkopers en overige belangstellenden.

Ad 3. Impactanalyse en factsheets beveiligingsstandaarden KING/IBD [Bijlage C, D, E]

Achtergrond

Begin 2015 heeft Forum Standaardisatie een voorstel gedaan richting het Nationaal Beraad om voor een set van vijf informatiebeveiligingsstandaarden aanvullende adoptieafspraken te maken (DNSSEC, TLS, DMARC+DKIM+SPF)[2].

[1] Generieke bestekteksten voor verplichte ICT-standaarden, 26 maart 2013", https://www.forumstandaardisatie.nl/sites/default/files/FS/2013/1217/20130326-Generieke-bestekteksten-open-standaarden-v1.12.pdf

[2] *www.forumstandaardisatie.nl/ptolu*

Deze afspraken hielden in dat de partijen die vertegenwoordigd zijn in of via het Nationaal Beraad deze vijf standaarden versneld gaan toepassen.

In het Nationaal Beraad gaf de VNG aan dat zij niet zonder meer een toezegging konden doen met betrekking tot de versnelling van de adoptie van deze standaarden voor het gehele gemeentelijke domein. BFS heeft de Informatiebeveiligingsdienst van KING (IBD) daarop gevraagd een impactanalyse te doen naar de toepassing van deze standaarden in het gemeentelijke domein om zo inzichtelijk te krijgen of er sprake is van serieuze hindernissen en drempels.

Factsheets en impactanalyse

Voor de standaarden DNSSEC en TLS (HTTPS) werd snel duidelijk dat de impact in termen van benodigde tijd en kosten van implementatie zeer beperkt is. KING/IBD heeft voor deze standaarden factsheets [bijlagen D en E] ontwikkeld om de adoptie bij gemeenten actief te stimuleren.

Voor DMARC+DKIM+SPF was de impact minder duidelijk. Om die reden is met dertig gemeenten een praktijkcasus uitgevoerd. Bij deze gemeenten is DMARC geactiveerd en zodanig geconfigureerd dat de IBD de resultaten kon verzamelen en analyseren. De resultaten zijn vastgelegd in bijgevoegde rapportage van de impactanalyse [bijlage C][3]. Hieronder volgen de bevindingen en aanbevelingen.

Belangrijkste bevindingen (impactanalyse DMARC+DKIM+SPF)

- DMARC leeft nog niet echt bij de meeste gemeenten. Uitleg over nut en noodzaak en kennisoverdracht heeft dus tijd nodig.
- Bij veel gemeenten is enige terughoudendheid merkbaar bij het implementeren van een correct SPF-record. De angst is aanwezig dat er mailstromen zijn die hier hinder van kunnen ondervinden.
- Het toevoegen van een DMARC-record aan de DNS is op zich weinig werk met een korte doorlooptijd. Niet alle gemeenten beheren hun eigen DNS en moeten dan een ticket hiervoor aanmaken bij hun provider, die daar in een enkel geval een klein bedrag voor in rekening bracht.
- Voor het identificeren van de mailstromen vanuit de terugkoppelingen van de mailproviders is kennis en tooling nodig.
- Vaak gebruiken leveranciers van klantcontactcentra en afsprakensoftware een externe hostingpartij waardoor het uitzoeken of een mailstroom legitiem is veel tijd kost.
- Gemeenten maken veel gebruik van dezelfde leveranciers voor mail en hebben de kantoormail uitbesteed aan externe hostingpartijen.
- Per gemeente zijn gemiddeld vier à vijf verschillende mailstromen te onderscheiden.
- De belangrijkste mailstromen die we bij de praktijkcasus zijn tegengekomen zijn kantoormail, afsprakenmodules van klantcontactcentra en diverse nieuwsbrieven.
- Er zijn vrijwel geen mailstromen geconstateerd vanuit de grote gemeentelijke backoffice-applicaties.
- Er zijn diverse mailstromen geïdentificeerd die buiten de Europese Economische Ruimte worden gehost.
- Inhoudelijke terugkoppelingen vanuit mailproviders(zogenaamde forensics) zouden een privacyrisico kunnen opleveren.

[3] *De verzender geeft met DMARC aan dat de e-mails zijn beschermd door SPF en/of DKIM en vertelt de ontvanger wat deze moet doen als het niet door de SPF/DKIM-test komt. Deze policy wordt in het publieke DNS gepubliceerd en is voor iedereen beschikbaar.*

- Bij het analyseren van de gezamenlijke terugkoppelingen van alle domeinen is geconstateerd dat bij vrijwel alle onderzochte domeinen misbruik heeft plaatsgevonden. De domeinnamen werden gebruikt voor het versturen van spam. Onduidelijk is of de betreffende domeinnamen ook zichtbaar zijn voor ontvangers van de mail. Van het misbruik is melding gemaakt bij NCSC en politie.

Aanbevelingen van de IBD (impactanalyse DMARC+DKIM+SPF)

- Onderzoek de mogelijkheid om DMARC-terugkoppelingen van alle gemeenten of misschien wel alle overheidsorganisaties centraal te verzamelen naar aanleiding van de constatering van misbruik op grote schaal.
- Maak voor gemeenten de resultaten beschikbaar van door andere gemeenten al geïdentificeerde mailstromen, bijvoorbeeld met behulp van tooling.
- Formuleer een ondersteuningsaanpak vanuit de IBD voor gemeenten.
- Informeer de betrokken leveranciers van klantcontactcentra, hostingpartijen, providers en dergelijke over de nieuwe standaard zodat ze zich klaar kunnen maken voor vragen van gemeenten.
- Maak duidelijke factsheets gericht op gemeenten.
- Adviseer gemeenten over de ontwikkeling of aanschaf van tooling waarmee ze de terugkoppelingen van mailproviders gemakkelijk kunnen interpreteren.

Ter kennisname

Ad 4. Voortgang onderzoek beveiligingsstandaarden
BFS laat momenteel, conform eerder besluit van het Forum, een onderzoek uitvoeren naar de adoptie van en samenhang tussen de verschillende beveiligingsstandaarden. Het doel is om het domein van beveiligingsstandaarden nader in kaart te brengen en te komen tot een strategische agenda. Daarbij wordt tevens geïnventariseerd welke beveiligingsstandaarden nog niet op de lijst van het Forum staan, maar hier wel op zouden thuishoren. Dit omdat zij de werking van de reeds opgenomen standaarden aanvullen of versterken. Het onderzoek sluit ook aan bij de Nationale Cyber Security Strategie 2 van eind 2013, waarin het onderwerp standaarden een prominente plek heeft.

In december 2015 heeft een workshop met experts plaatsgevonden. De resultaten van dit onderzoek en eventuele kandidaatstandaarden worden naar verwachting in juni aan het Forum gepresenteerd.

Ad 5. Workshop mailauthenticatiestandaarden
In april organiseert het Bureau Forum Standaardisatie een workshop over open standaarden die e-mailfraude (DMARC+DKIM+SPF) helpen bestrijden. De workshop is gericht op ICT-beheerders, ICT-projectmanagers en beveiligingsadviseurs van de organisaties die betrokken zijn bij het Nationaal Beraad, de Regieraad Interconnectiviteit en de Manifestgroep. Het doel van de workshop is om ervaringen en best practices over het gebruik van e-mailbeveiligingsstandaarden uit te wisselen. Naast de presentaties zal er de gelegenheid zijn om te netwerken en contacten op te doen met collega’s die ervaring hebben met e-mailbeveiliging.

Willy Rovers (CIO Belastingdienst) zal de workshop voorzitten. We verwachten sprekers van de Belastingdienst, NCSC, UWV/CIP, IND, SSC-ICT en Logius. De workshop is gepland voor donderdag 14 april van 12.30 tot 16.00 uur (onder klein voorbehoud).

Aanmelden voor deze workshop kan via Bart Knubben (bart.knubben@logius.nl)

Ad 6. Voortgang Internet.nl

Op 5 februari vond opnieuw een bijeenkomst plaats van het Platform Internetstandaarden (met o.a. EZ, SIDN, RIPE NCC, NCSC, ECP en SURFnet). Tijdens deze bijeenkomst is onder andere gesproken over:

- doorontwikkeling van de testtool Internet.nl;
- hoe aandacht gevraagd kan worden voor de standaarden via 'bepalende partijen', zoals het CIO-platform;
- hoe in 2016 verschillende domeinen (overheid en niet-overheid) op een ludieke manier benaderd kunnen worden met hun scores op de internet.nl-test (onder andere de leveranciers van het Leveranciersmanifest open standaarden);
- het feit dat het platform ook internationaal bekend begint te raken. Zo is er een verzoek binnengekomen vanuit Polen om de website te vertalen.

Sinds april 2015 zijn er op Internet.nl meer dan 75.000 testen uitgevoerd.

Ad 7. De factsheets TLS en DNSSEC

De bijgevoegde factsheets richten zich op gemeenten ten behoeve van het veilig verbinden met gemeentelijke websites (TLS) en op gemeenten die het DNS-beheer hebben uitbesteed en gebruik willen maken van de beveiligingsstandaard DNSSEC.