FS-20170614.03

notitie

Forum Standaardisatie
www.forumstandaardisatie.nl
info@forumstandaardisatie.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 14 juni 2017

Agendapunt 3. Open standaarden, adoptie
Stuknummer 3. Oplegnotitie adoptie

Van:	Stuurgroep open standaarden
Aan:	Forum Standaardisatie
Bijlagen:	geen

Ter kennisname
U wordt gevraagd om kennis te nemen van:

1. Online tool Handreiking Betrouwbaarheidsniveaus voor Digitale dienstverlening
2. Voortgang Veilige E-mail Coalitie
3. Review Uniforme Set van Eisen - eID
4. Monitor open standaarden naar Tweede Kamer
5. Antwoord Kamervragen adoptie IV-standaarden
6. Overig (Geo-standaarden, Digikoppeling en KING)

Ter kennisname

Ad 1) Online tool Handreiking Betrouwbaarheidsniveaus voor Digitale dienstverlening

In november 2016 lanceerde Forum Standaardisatie de vierde editie van de handreiking 'Betrouwbaarheidsniveaus voor Digitale Dienstverlening'. Deze handreiking helpt overheidsorganisaties een inschatting te maken welk betrouwbaarheidsniveau past bij hun digitale diensten. Hiervoor bevat de handreiking een classificatiemodel dat in de nieuwe versie volledig is gebaseerd op de EIDAS-verordening[1].

Classificatiemodel als online tool
In samenwerking met de RVO heeft BFS het classificatiemodel uit de handreiking inmiddels verwekt in een online tool. Gebruikers van de tool kunnen aan de hand van een aantal vragen inschatten welk betrouwbaarheidsniveau voor hun dienst passend is. Na het doorlopen van de tool krijgen gebruikers het passende niveau op het scherm gepresenteerd en – indien gewenst- in een downloadbare rapportage.

De tool wordt naar verwachting medio juni gelanceerd. BFS zal hier – samen met de uitgave van de tweede druk van de handreiking - de nodige aandacht aan geven.

De tool is alvast te proberen op: https://regelhulptest.bridge-to-knowledge.nl/ez-test/fs.html?modelname=betrouwbaarheidsniveau_digitale_dienstverlening.

Ad 2) Voortgang Veilige E-mail Coalitie
Op 18 mei jl. heeft de tweede bijeenkomst van de Veilige E-mail Coalitie (VEC) plaatsgevonden bij het ministerie van EZ. Eerst werd met de kerngroep gesproken over de koers van de coalitie en de 0-meting onder de deelnemers die is uitgevoerd m.b.v. Internet.nl. Vervolgens sloten nieuwe deelnemers aan. XS4ALL gaf een presentatie over hun ervaringen en ambities met veilige e-mail. Vervolgens gaf NCSC een presentatie over hun recente facstsheet "Beveilig verbindingen van mailservers" (m.b.t. STARTTLS en DANE). Tot slot gaf BFS een presentatie over de resultaten van de meting Informatieveiligheidsstandaarden begin 2017. Bij de bijeenkomst waren meer dan dertig partijen aanwezig waaronder PostNL, KPN, Ziggo, Betaalvereniging Nederland, Thuiswinkel.org, VNO-NCW, MKB-Nederland, XS4ALL, Fraudehelpdesk, Schiphol en de Belastingdienst.

Top 16 mei tijdens de internationale OneConference in Den Haag verzorgden KPN en PostNL onder begeleiding van Gerben Klein Baltink (voorzitter Platform Internetstandaarden en VEC) een sessie over veilige e-mail (zie: https://www.ncsc.nl/english/conference/programme/day+1).

Over de Veilige E-mail Coalitie verschenen artikelen in Publiek Denken en in AG Connect: http://specials.publiekdenken.nl/special-i-samenleving#!/veilige-e-mail-coalitie en https://agconnect.nl/artikel/de-6-maatregelen-van-de-veilige-e-mail-coalitie.

[1] *https://www.forumstandaardisatie.nl/thema/handreiking-betrouwbaarheidsniveaus*

Ad 3) Review Uniforme Set van Eisen – eID
In het kader van de openbare consultatie van de Wet GDI (https://www.internetconsultatie.nl/wetgdi/) is door Bureau Forum Standaardisatie onderstaande reactie gestuurd m.b.t. de zogenaamde "Uniforme Set van Eisen" (USvE). De invalshoek van de reactie is (uiteraard) vooral vanuit open standaarden en interoperabiliteit. Vanuit het programma eID heeft BFS ondertussen vernomen dat men de komende periode aan de slag gaat met de verwerking van deze en andere ontvangen reacties om in de tweede helft van 2017 te komen tot een nieuwe versie van de Uniforme Set van Eisen.

I. Algemene opmerkingen

1. Document ziet er goed en doorwrocht uit en heeft een behoorlijk heldere opzet. Wellicht dat perspectief van eindgebruiker nog wat inzichtelijker kan ("wat betekent het voor eindgebruiker?").
2. In de titel duidelijk maken waarop de Uniforme Set van Eisen betrekking heeft. Bijv. eID?
3. Goed dat IETF RFC 2119 wordt gevolgd. Dit lijkt alleen niet overal consequent doorgevoerd. Zo wordt ook een aantal keer het begrip "RECOMMENDED" gehanteerd.
4. Lijkt logischer om (uiteindelijk) een volledig Nederlandse en een Engelse versie uit te brengen.
5. Het document zelf is nu PDF1.5. Beter is PDF/A. PDF/A is een van de standaarden die het Forum Standaardisatie voorschrijft en zorgt voor (duurzame) toegankelijkheid.
6. Op pagina 9 verwijst "Open standaarden" naar een externe wikipagina waar je moet inloggen. Wellicht is dat bij meer links het geval.
7. USvE lijkt niets te zeggen over de keuze van een betrouwbaarheidsniveau door een dienstverlener. Zie 'Handreiking betrouwbaarheidsniveaus' van Forum Standaardisatie (https://www.forumstandaardisatie.nl/thema/handreiking-betrouwbaarheidsniveaus).
8. Er loopt momenteel een consultatie OIN-beleid. Lijkt relevant voor eID. Zie: https://www.logius.nl/over-logius/actueel/item/titel/openbare-consultatie-voorwaarden-digikoppeling/

II. Open standaarden
Hieronder volgt een aantal opmerkingen m.b.t. open standaarden.

Algemeen:

9. Goed dat open standaarden als uitgangspunt worden gehanteerd.
10. Je zou bij iedere genoemde open standaard naar de (core) specificatie kunnen verwijzen (met een URL). Daarmee wordt ook direct duidelijk om welke versie het gaat.
11. In ieder geval de paragraaf "Technical security requirements" laten checken door NCSC, voor zover dat niet al gedaan is. We kennen de crypto-adviseur bij NCSC. Eventueel kunnen we jullie met hem in contact brengen.

DNSSEC:

12. Waarom is validatie 'should' en niet 'must' voor participants?
13. En waarom is publicatie en validatie niet op zijn minst 'should' voor service providers?

14. Je zou ook nog eisen kunnen stellen aan het ondertekeningsalgoritme (bijv. niet lager dan alo 8) en dat NSEC3 (en niet NSEC) wordt gebruikt om 'zone walking' te voorkomen.
15. Overigens in de ICT-beveiligingsrichtlijnen voor Webapplicaties van NCSC (Verdieping) wordt DNSSEC ook geadviseerd en dit is overgenomen in de vernieuwde DigiD-beveiligingsassessments.

TLS:

16. Hier nog wat strakker aansluiten bij ICT-beveiligingsrichtlijnen voor TLS en voor Webapplicaties van NCSC (Beveiligingsrichtlijn U/WA.05, Verdieping).
17. Bij verbinding met eindgebruiker is upgrade nodig van HTTP naar HTTPS. HSTS is hierbij van belang. Deze standaard ontbreekt nu in USvE. NCSC adviseert dit en dezestandaard wordt ook eerdaags opgenomen op PToLU-lijst.
18. Bij back channel-verbindingen moet er juist geen HTTP maar alleen HTTPS mogelijk zijn. Je zou dit als expliciete eis kunnen opnemen.
19. "the client-certificate(s) used MUST be listed in the metadata." – Welke metadata?

ISO27001/2:

20. Deze staan ook op de ptolu-lijst. Wellicht goed om te melden in USvE.
21. Relatie met Baselines IB overheid, zoals BIR en BIG, komt nauwelijks terug.
22. Verwachten jullie van participants dat ze zich tegen ISO27001 laten certificeren?

SAML:

23. In welke mate verschillen de gedefinieerde koppelvlakspecs van de huidige koppelvlakspecs van eHerkenning en van DigiD?
24. Wordt gebruik gemaakt van SAML-functionaliteit die beschikbaar is in standaard off-the-shelf" producten? En aansluit bij profielen van anderen (https://kantarainitiative.github.io/SAMLprofiles/ en https://lists.oasis-open.org/archives/security-services/201703/msg00000.html)? Lijkt me goed om keuzes voor te leggen aan OASIS Security Services (SAML) TC, zoals eerder ook al eens gebeurd is. Of is dat reeds gebeurd?
25. Komt er een testvoorziening waarmee conformiteit van implementaties getest kan worden?

Webservices/Digikoppeling:

26. "When web services are used within Uniforme Set van Eisen, the web service standards as defined in DigiKoppeling/Forum Standaardisatie "pas toe of leg uit" (comply or explain) are adhered to." --> De verhouding tussen deze paragraaf en de andere technische eisen is ons niet helemaal duidelijk. Er lijkt in het document niet/nauwelijks gerefereerd te worden aan Web services/Digikoppeling.
27. "the connection MUST be secured using (mutual authenticated) TLS, with the parameters as defined under Secure Uniforme Set van Eisen, versie 1.0 (15-12-2016) connection (TLS)." --> Let op: Digikoppeling stelt zelf ook eisen aan TLS. Zie: https://www.forumstandaardisatie.nl/sites/default/files/FS/2017/0614/Digikoppeling-Beveiligingsstandaarden-en-voorschriften-v1.2.pdf

Tot slot, voor de volledigheid volgen hieronder links naar de eerdere adviezen aan eID van Forum Standaardisatie:

- https://www.forumstandaardisatie.nl/sites/default/files/FS/2013/0416/FS-20130416.06D-Adviesrol-FS-eID-stelsel.pdf
- https://www.forumstandaardisatie.nl/sites/default/files/FS/2013/0903/FS-20130903.07C-20130822-Notitie-reactie-eID-v09.pdf

---

Ad 4) Monitor open standaarden naar Tweede Kamer
Minister Kamp van Economische Zaken heeft op 9 mei jl. met een brief de Monitor Open Standaarden Beleid 2016 aangeboden aan de Tweede Kamer [Kamerstuk 26643 nr. 462, https://zoek.officielebekendmakingen.nl/kst-26643-462.html]. Het monitor-rapport is als bijlage bijgevoegd bij de brief. Hieronder een tweetal citaten uit de brief:

- *"Doel van het openstandaardenbeleid is de brede adoptie van open standaarden door alle overheden voor moderne en veilige overheidsdienstverlening aan bedrijven en burgers. De afgelopen jaren zijn goede resultaten geboekt en het is zaak om deze verbetering vast te houden en door te zetten, om voor alle ICT-aanbestedingen aan de aangewezen open standaarden van de «pas toe of leg uit»-lijst te kunnen voldoen. De monitor laat onder meer zien dat in 2016 in 73% van de aanbestedingen is gevraagd om een of meer relevante standaarden van de verplichte lijst. Gelet op de motie van de leden Oosenbrug en Gesthuizen (Kamerstuk 33 326, nr. 21) is dit nog niet optimaal en moeten alle aanbestedingen van de overheid vanaf eind 2015 aan het «pas toe of leg uit»-beleid van het Forum Standaardisatie voldoen. Mijn collega voor Wonen en Rijksdienst heeft aangegeven welke acties daarvoor zijn ingezet (Kamerstukken 26 643 en 33 326, nr. 389). Daarnaast vormen open standaarden een belangrijk onderdeel van de wet Generieke Digitale Infrastructuur, die onlangs in consultatie is geweest."*
- *"Ik waardeer de inzet van het Forum Standaardisatie. Standaardisatie is een relevant onderdeel van de digitalisering en bovengenoemde initiatieven dragen bij aan een veilige, efficiënte en betrouwbare digitale infrastructuur. Burgers, bedrijven en overheden moeten daarop kunnen vertrouwen. Voor de verdere groei van de digitale economie is dit essentieel."*

Ad 5) Antwoord Kamervragen adoptie IV-standaarden
Minister Plasterk van Binnenlandse Zaken en Koninkrijksrelaties heeft vragen van het lid Gijs vanDijk (PvdA) beantwoord over het bericht dat er binnen de gehele overheid informatieveiligheid nodig is (ingezonden 11 april 2017) [Kamervragen (Aanhangsel) 2016-2017 nr. 1671, https://zoek.officielebekendmakingen.nl/ah-tk-20162017-1671.html]. Hieronder volgen de antwoorden op de twee vragen die betrekking hadden op informatieveiligheidstandaarden.

"

Vraag 3
Deelt u de mening van de Digicommissaris dat er een snellere implementatie van moderne internetstandaarden nodig is? Deelt u dan ook de mening van de Internet Society Nederland dat er een wettelijke verplichting om beveiligingsstandaarden te gebruiken moet komen? Zo ja, waarom en wat kunt u doen om dit te bewerkstelligen? Zo nee, waarom niet?

Antwoord 3
Er is inderdaad een snellere implementatie van moderne internetstandaarden nodig, met name op het gebied van beveiligingsstandaarden. Daarom worden diverse acties ondernomen. Zo is de rijksoverheid een van de initiatiefnemers van de «veilige e-mailcoalitie», waarin bedrijfsleven en overheid samenwerken om phishing terug te dringen. Daarnaast wordt er deelgenomen aan het Platform Internetstandaarden dat de implementatie van de beveiligingsstandaarden meetbaar maakt via internet.nl, en hebben de overheden in het Nationaal Beraad Digitale Overheid afgesproken om informatieveiligheidsstandaarden een impuls te geven. De standaarden zijn opgenomen in factsheets van het NCSC en de Informatiebeveiligingsdienst voor gemeenten van VNG/KING.

Het voorstel voor de wet Generieke Digitale Infrastructuur, dat onlangs in consultatie was, bevat een grondslag om bij algemene maatregel van bestuur open standaarden, waaronder beveiligingsstandaarden, aan te wijzen die overheden dienen te hanteren in het elektronisch verkeer met andere overheden, met burgers en met bedrijven. Deze aanwijzing zal plaatsvinden indien dit noodzakelijk en proportioneel is gelet op de goede werking, veiligheid, betrouwbaarheid of de doelmatigheid van het elektronisch verkeer, of indien dit voortvloeit uit verdragen of besluiten van volkenrechtelijke organisaties.

Vraag 4
Wat is de stand van zaken met betrekking tot de afspraak tussen de Digicommissaris en het Nationaal Beraad Digitale Overheid over de implementatie van moderne beveiligingstandaarden bij de e-mail van gemeenten per 2018?

Antwoord 4
De stand van zaken van de implementatie van een set informatieveiligheidsstandaarden wordt op verzoek van het Nationaal Beraad halfjaarlijks – via internet.nl – door het Forum Standaardisatie gemeten. De laatste meting treft u aan op de pagina: www.forumstandaardisatie.nl/thema/iv-meting. Uit de laatste meting van begin 2017 blijkt dat de implementatie gestaag groeit. Vooral gemeenten hebben het laatste half jaar een flinke inhaalslag gemaakt. De groei moet echter overheidsbreed verder worden doorgezet, zodat het streefbeeld kan worden gehaald om deze standaarden eind 2017 overal waar van toepassing, te hebben geïmplementeerd.
”

Ad 6) Overig (Geo-standaarden, Digikoppeling en KING)

- Update van de Nederlandse metadataprofielen Geo-standaarden, http://www.geonovum.nl/onderwerpen/metadata/nieuws/werk-mee-aan-de-update-van-de-nederlandse-metadataprofielen
- Logius en KING actualiseren marktscan Digikoppeling, https://www.logius.nl/over-logius/actueel/item/titel/logius-en-king-actualiseren-marktscan-digikoppeling/
- Openbare consultatie voorwaarden Digikoppeling (m.n. OIN-beleid), https://www.logius.nl/over-logius/actueel/item/titel/openbare-consultatie-voorwaarden-digikoppeling/
- Presentatie KING-congres i.s.m. IBD en gemeente Den Bosch over informatieveiligheidsstandaarden, https://www.da2020.nl/congres/programma/veilig-digitaal-verkeer