



notitie

FORUM STANDAARDISATIE 16 december 2014 Agendapunt 6. Open standaarden, adoptie Stuk 6. Oplegnotitie

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

Vooraf: Filmpje beveiligingsstandaarden

*U wordt gevraagd **in te stemmen** met:*

1. Rol Forum m.b.t. informatiebeveiliging

*U wordt gevraagd **te discussiëren** over:*

2. Voorlopige resultaten onderzoek eFactuur-standaarden (presentatie)
3. Adoptiestrategie; kansen&bottlenecks, mede op basis van uitkomst monitor (ingeleid door presentatie)

*U wordt gevraagd **kennis te nemen** van:*

4. ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) van NCSC
5. Bijeenkomsten

Ter besluitvorming:

Ad 1. Rol Forum m.b.t. informatiebeveiliging

Datum
16 december 2014

Het Forum Standaardisatie wordt gevraagd om in te stemmen met:

1. De uitvoering van een 'samenhang-onderzoek' binnen het domein Informatiebeveiliging;
2. De oprichting van een stuurgroep die dit onderzoek begeleidt en die de agenda rondom Informatiebeveiliging nader bepaalt;
3. De versterking van het Forum met een nieuw lid dat ruime bestuurlijke en inhoudelijke praktijkervaring heeft met Informatiebeveiliging.

Toelichting

Huidige rol en ambitie

- Forum Standaardisatie houdt zich al bezig met informatiebeveiliging. Zo staan verschillende informatiebeveiligingstandaarden op de 'pas toe of leg uit'-lijst. Het gaat om DNSSEC (veilige domeinnamen), DKIM (anti-phishing), TLS (beveiligde verbindingen), SAML (inloggen), Digikoppeling (betrouwbare gegevensuitwisseling), en NEN-ISO27001/27002 (organisatie van informatiebeveiliging). Het Forum heeft ook een review uitgevoerd op de nieuwe concept-versie van de 'ICT-beveiligingsrichtlijnen voor webapplicaties' van NCSC (waarvan een deel wordt gebruikt voor DigiD-audits). Daarnaast is het Forum betrokken bij de oprichting van het Platform Internetstandaarden dat ook veel aandacht besteedt aan informatiebeveiliging;
- Het Forum heeft de ambitie om vanaf 2015 een actievere rol rondom informatiebeveiliging te spelen, omdat rondom harmonisatie/standaardisatie (en bijgevolg verlichting auditdruk) en stimulering van de adoptie nog veel winst is te behalen. Het Forum heeft daarbij vanuit standaardisatie-perspectief een adviserende 'aanjaag'-functie. Andere partijen (NCSC, baselinebeheerders etc.) gaan over de inhoud en stellen standaarden of richtlijnen op.

Oprichting stuurgroep en nieuw Forum-lid

- Het voorstel is om een stuurgroep "standaarden en informatiebeveiliging" met 3 à 4 Forum-leden op te richten.
- De leden voor deze stuurgroep worden geselecteerd uit de Forum-leden die afgelopen Forum-vergadering hun interesse kenbaar maakten (Guus Bronkhorst, Erwin Bleumink, Cor Franke, Nico Romijn, Arianne de Man en Bert Uffen).
- Het Forum wordt uitgebreid met een nieuw lid. Van het nieuwe Forum-lid wordt verwacht dat hij ruime (bestuurlijke en inhoudelijke) praktijkervaring heeft met informatiebeveiliging en eveneens zal plaatsnemen in de genoemde stuurgroep. Ideeën voor andere kandidaten zijn welkom (ook uit de hoek van gemeenten).
- Bart Knubben van Bureau Forum Standaardisatie heeft al de nodige expertise rondom informatiebeveiliging en zal zich op dat vlak blijven ontwikkelen. Ook in het functieprofiel voor een nieuwe medewerker van BFS zal informatiebeveiliging als gevraagde expertise worden opgenomen.

Uitvoerig 'samenhangonderzoek' en bepalen agenda

- Als het nieuwe Forum-lid is aangesteld zal BFS begin 2015 een eerste bijeenkomst van de stuurgroep 'standaarden en informatiebeveiliging' organiseren. Het doel van deze eerste bijeenkomst is om de visie en agenda rondom het onderwerp nader te bepalen. Het resultaat zal vervolgens in het Forum aan de orde komen.

- Onderdeel van deze agenda is, zoals eerder door het Forum besloten, in ieder geval de uitvoering van een 'samenhang-onderzoek' waarin aandacht is voor:
 1. Blinde vlekken: Ontbreken er IB-standaarden op de PToLU-lijst en lijst met gangbare standaarden?
 2. Samenhang: Hoe verhouden de IB-standaarden zich tot elkaar?
 3. Nieuwe ontwikkeling/doorontwikkeling: Welke nieuwe IB-standaarden zouden ontwikkeld moeten worden en wie zou dat kunnen doen? Hoe zou je bestaande standaarden kunnen harmoniseren en de auditdruk kunnen verlichten?

Datum
16 december 2014

Ter discussie:

Ad 2. Voorlopige resultaten onderzoek eFactuur-standaarden (presentatie)

Aanleiding

Elektronisch factureren is vanwege de enorme potentie en het belang voor overheid en bedrijfsleven een belangrijke pijler van de Nederlandse elektronische overheid. College Standaardisatie heeft in het verleden over het gebruik van drie e-factuur standaarden geadviseerd: UBL (2007), SETU (2009) en het Semantisch factuurmodel (2013).

In 2010 heeft Forum Standaardisatie een onderzoek laten uitvoeren naar de voortgang en ontwikkelingen op het gebied van e-factureren en besloten het eerdere uitgangspunt te bekrachtigen. D.w.z. dat overheden worden geadviseerd om UBL toe te passen, of een in een specifiek domein, dominante standaard (zoals SETU), in afwachting van één Europese standaard voor e-factureren. Aanvullend werd geadviseerd om te komen tot een nationaal semantisch factuurmodel. Dit Semantische factuurmodel is door Logius ontwikkeld en in 2013 opgenomen op de lijst met 'pas toe of leg uit' -standaarden.

Inmiddels zijn verschillende nationale en internationale ontwikkelingen in het e-factuur domein een aanleiding om opnieuw te onderzoeken op welke e-factuurstandaarden de Nederlandse overheid het best kan inzetten en hoe men dat het best kan doen.

Vraagstelling

Specifiek heeft het Forum Standaardisatie gevraagd om:

1. Het huidige speelveld van standaarden voor e-factureren in kaart te brengen, en daarbij ook te kijken naar de huidige adoptie van deze standaarden, de onderlinge samenhang en relevante ontwikkelingen op dit gebied.
2. Te adviseren of het bestaande College-advies over standaarden voor elektronisch factureren, in het licht van dit actuele overzicht, nog passend is en of/hoe het aangescherpt/aangepast moet worden.
3. Adoptiedrempels rondom de geadviseerde standaarden UBL, SETU en Semantisch factuurmodel (SMef) te inventariseren en te adviseren over maatregelen die genomen kunnen worden om de adoptie van deze standaarden verder te bevorderen.

Presentatie

TNO zal tijdens het Forumoverleg de belangrijkste bevindingen en voorlopige aanbevelingen presenteren. Na bespreking in het Forum zal de rapportage definitief gemaakt worden en worden verspreid onder de Forumleden.

Ad 3. Adoptiestrategie; kansen&bottlenecks, mede op basis van uitkomst monitor (ingeleid door presentatie)

Datum
16 december 2014

Wat is het beeld? (monitor)

Het Forum heeft in de vorige vergadering de monitor besproken en goedgekeurd. De definitieve versie is te vinden via: <https://www.forumstandaardisatie.nl/open-standaarden/beleid-en-monitoring/>

1. *Zelfrapportage*: Een meerderheid van de overheidsorganisaties (58%) zegt het 'pas toe of leg uit'-principe te hebben ingevoerd. Aanvullend zegt 11% met een invoeringsbesluit bezig te zijn. Met name kleine gemeenten zijn nog niet bezig met het 'pas toe of leg uit'-principe.
2. *Generieke voorzieningen (incl. NUP-bouwstenen)*: Deze maken, evenals vorig jaar, redelijk goed gebruik van open standaarden. Het positieve effect hiervan is groot omdat deze voorzieningen vaak door meerdere partijen worden gebruikt. Met name Rijksoverheid.nl, DigiD en DWR hebben afgelopen jaar stappen gemaakt. Toch blijft er ook bij voorzieningen ruimte voor verbetering.
3. *Aanbestedingen*: De meting had betrekking op aanbestedingen van 2013. Het beeld is vergelijkbaar met het beeld van de monitor over 2012. In de meerderheid van de aanbestedingen (gelijk aan vorig jaar) wordt niet gevraagd om de relevante open standaarden en daarover ook geen uitleg gegeven in het jaarverslag. Het aantal gevallen waarin om alle relevante standaarden is gevraagd is voorzichtig gegroeid (met 5 procentpunt, van 9% naar 14%).
4. *Gebruiksgegevens*: Er zijn maar beperkte gegevens beschikbaar. Bij de wel bekende gegevens wisselt het beeld per standaard. StUF, Digikoppeling en Semantisch Model e-Factureren, worden op redelijk grote schaal door overheden gebruikt. Maar voor veel andere standaarden lijkt het daadwerkelijk gebruik aan de lage kant. Daarnaast vallen vier standaarden op doordat het gebruik duidelijk is gegroeid: Digikoppeling, DNSSEC, DKIM en SAML.

Wat doen we al? (huidige aanpak)

- Stimulering bij aanvang van investeringstrajecten o.a. door advisering (pro-actief of desgevraagd, het bureau werkt daarom aan laagdrempelige bereikbaarheid d.w.z. vraagbaak-functie);
- Adoptie-aanpak per standaard of cluster van samenhangende standaarden;
- Samenwerking met de regieraad Interconnectiviteit en het bureau van de Digicommissaris (Nationaal Commissaris Digitale Overheid): zij kunnen o.a. de adoptie van standaarden plannen en aanjagen.
- Samenwerking met stakeholders (o.a. KING, IPO, UvW, Manifestgroep, ICCIO, BRG, NORA, leveranciers);
- Stimulering via generieke voorzieningen;
- Gericht op feitelijk gebruik in de praktijk, naast stimulering via aanbestedingen. Onder andere via implementatieafspraken en introductie van 'accountmanager-schap' en streefcijfers bij het bureau.

Wat kunnen we nog meer doen? (stellingen)

1. *'Leveranciers zijn de sleutel': Het Forum moet zich meer richten op leveranciers met bijvoorbeeld een overheidsbrede softwarecatalogus of een nieuw Leveranciers Manifest Open Standaarden.'*
2. *'PToLU is te soft. Tijd voor comply or die?': Voor belangrijke standaarden moet er een mogelijkheid komen om die wettelijk te verplichten. Dit past ook bij de overheidsambitie van 'alles digitaal' per 2017.*
3. *'Practice what you preach': Ieder Forum-lid moet de voor zijn relevante standaarden ook toepassen binnen de eigen organisatie.*
4. *'Digicommissaris is het adoptie-kanon': Het Forum moet intensief optrekken met de Digicommissaris, het Nationaal beraad en de bijbehorende regieraden om de adoptie van standaarden verder te stimuleren.*
5. *'Visie, lef en lange adem houden': Voor de brede adoptie van standaarden gelden tijdslijnen van 5 tot 10 jaar.*
6. *'Verplichte standaarden-check': Overheden zijn verplicht om het PvE van ICT-investeringen van boven de EUR 100.000 te laten checken door Forum Standaardisatie.*
7. *'Transparantie via Rijks ICT-dashboard': Het Rijk moet ook via het Rijks ICT-dashboard transparant maken wat de toepassing van open standaarden is in grote ICT-projecten.*
8. *'Architecten doen het!': Het Forum moet meer optrekken met NORA en ervoor zorgen dat standaarden uitgebreid terugkomen in architecturen, zodat architecten niet om de standaarden heen kunnen;*
9. *... (uw stelling!)*

Datum
16 december 2014

Ter informatie:

Ad 4. ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) van NCSC

NCSC heeft "ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)" gepubliceerd. Met deze richtlijnen geeft het NCSC invulling aan één van de adviezen die het Forum Standaardisatie gaf bij de opname van TLS op de 'pas toe of leg uit'-lijst. Bureau Forum Standaardisatie heeft aan NCSC inbreng geleverd voor het opstellen van de richtlijnen.

TLS is een standaard voor het opzetten en gebruiken van een cryptografisch beveiligde verbinding tussen twee computersystemen. TLS is ook bekend onder de oude naam, Secure Sockets Layer (SSL). TLS wordt gebruikt in een breed scala van toepassingen. Bekende voorbeelden zijn webverkeer (HTTPS), e-mailverkeer (IMAP en SMTP over STARTTLS) en bepaalde typen virtual private network (VPN).

De richtlijnen helpen een organisatie te kiezen tussen alle mogelijke instellingen van TLS, om zo te komen tot een veilige configuratie. Voor webverkeer heeft NCSC aanvullend de factsheet 'HTTPS kan een stuk veiliger' gepubliceerd.

Zie:

- <https://www.ncsc.nl/dienstverlening/expertise-advies/kennisdeling/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html>
- <https://www.ncsc.nl/dienstverlening/expertise-advies/factsheets/factsheet-https-kan-een-stuk-veiliger.html>

Datum
16 december 2014

Ad 5. Bijeenkomsten

- Netwerk Kwaliteit Rijkswebsites (13 nov) : presentatie Bart Knubben (BFS) over internet- & en webstandaarden
- Leergang ICT & Inkopen (20 nov): sessie Ludwig Oberendorff (BFS) over inkoop en open standaarden
- ECP-congres (20 nov): sessie Platform Internetstandaarden olv kwartiermaker Gerben Klein Baltink
- LAC (26 nov): sessie Bart Knubben (BFS) en Jaap van der Veen (MinFin) over Security, standaarden en architectuur
- ODF Plugfest (8&9 dec): sessie Marijke Salters (BFS) en Jos van den Oever (KOOP) over standaarden en de document lifecycle
- Min VWS en SIKB: presentaties Lancelot Schellevis
- Bouw Informatie Raad: presentatie Marijke Salters over beheer van standaarden
- VIAG: presentatie ism KING over betrouwbaarheidsniveaus door Maarten van der Veen en René van den Assem