



notitie

FORUM STANDAARDISATIE 28 oktober 2014 Agendapunt 05. Open standaarden, adoptie Stuk 05. Oplegnotitie

Bijlagen:	A) Monitor OS B) TLS stavaza
Aan:	Forum Standaardisatie
Van:	Stuurgroep open standaarden

*U wordt gevraagd **in de stemmen** met de volgende adviezen:*

1. Resultaten van de Monitor openstandaarden-beleid 2013

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

2. Test veilige toepassing TLS (beveiligde verbindingen)

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

3. Terugblik seminar Nieuwe Internetstandaarden
4. Voortgang samenwerking ICCIO en College/Forum Standaardisatie

Ter besluitvorming:

Ad 1. Resultaten van de Monitor openstandaarden-beleid 2013

[Bijlage A]

Datum
16 oktober 2014

Het Forum Standaardisatie wordt gevraagd om in te stemmen met:

1. het doorgeleiden van de resultaten van het rapport naar de volgende vergadering van het Nationaal Beraad Digitale Overheid inclusief een oplegnotitie waarin aanvullende maatregelen ter aanscherping van de adoptie-aanpak terugkomen;
2. voortzetting van de begin 2013 ingezette koers voor adoptie en verdere aanscherping daarvan de komende periode in samenwerking met stakeholders.

Toelichting

Forum Standaardisatie monitort jaarlijks de effecten van het openstandaarden-beleid van de Nederlandse overheid. Het onderzoek is evenals vorig jaar uitgevoerd door ICTU.

Het rapport bevat vier onderzoeksonderdelen. Hieronder volgt per onderdeel kort het beeld dat naar voren komt.

1. Zelfrapportage: Een meerderheid van de overheidsorganisaties (58%) heeft het 'pas toe of leg uit'-principe ingevoerd. Aanvullend zegt 11% met een invoeringsbesluit bezig te zijn. Net als voorgaande jaren is ongeveer een kwart van de overheden (27%) helemaal nog niet bezig met het 'pas toe of leg uit'-principe. Dit geldt met name voor kleinere gemeenten. Het voorgaande beeld is vergelijkbaar met dat vorig jaar. Beide achterliggende doelen van het openstandaarden-beleid (interoperabiliteit en leveranciersonafhankelijkheid) worden, in het perspectief van Digitaal 2017, door het overgrote deel van de respondenten (97% resp. 81%) onderschreven.
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 41% (gelijk aan vorig jaar) van de onderzochte gevallen is om een deel of om alle relevante standaarden gevraagd. Het aantal gevallen waarin om alle relevante standaarden is gevraagd is voorzichtig gegroeid (met 5 procentpunt, van 9% naar 14%). 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. Aanbestedingen van met name de Belastingdienst, Dienst Publiek en Communicatie, Gemeente Stede Broec en Gemeente Dronten onderscheidden zich in positieve zin. Overigens loopt de adoptie van bepaalde standaarden niet alleen via aanbestedingen; bepaalde standaarden worden niet goed uitgevraagd, maar laten in het

onderzoeksonderdeel “gebruiksgegevens” wel een duidelijke gebruikstoename zien.

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.

Datum
16 oktober 2014

Transparantie

- Bij het onderzoek naar generieke voorzieningen bleek dat het niet altijd eenvoudig is om de gevraagde informatie boven tafel te krijgen. Positieve uitzondering daarop is Logius dat jaarlijks een helder overzicht publiceert. Hier ligt een rol voor de beheerders van de voorzieningen.
- Niet voor iedere standaard zijn kwantitatieve gebruiksgegevens beschikbaar. Hier ligt in veel gevallen een rol voor de desbetreffende standaardisatie-organisatie.

Adoptie-aanpak

De monitor vormt aanleiding om de begin 2013 ingezette koers aangescherpt voort te zetten. Deze koers komt terug in het werkplan 2015. Hoofdpunten voor deze koers zijn:

- Stimulering bij aanvang van investeringstrajecten o.a. door advisering (pro-actief of desgevraagd, het bureau werkt daarom aan laagdrempelige bereikbaarheid);
- 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’ bij het bureau.

Bureau Forum Standaardisatie zal de komende periode met stakeholders de koers verder aanscherpen en invulling geven voor 2015. De maatregelen zullen in de volgende Forum-vergadering op de agenda staan en daarna richting Nationaal Beraad Digitale Overheid in een oplegger bij de monitor worden gevoegd.

Ter discussie:

Ad 2. Test veilige toepassing TLS (*beveiligde verbindingen*) [Bijlage B]

Het Forum Standaardisatie wordt gevraagd om op basis van de testresultaten te discussiëren aan de hand de volgende vragen:

1. Hoe kunt u in uw eigen organisatie of bij uw eigen achterban de veilige toepassing van TLS bevorderen?
2. Welke mogelijkheden ziet u voor de verspreiding en het gebruik van de aanstaande NCSC-handreiking?

Toelichting

Uit de test blijkt dat er bij verschillende overheidswebsites verbeteringen mogelijk zijn voor de veilige toepassing van TLS. Op advies van het Forum/College stelt het NCSC momenteel een handreiking op hoe met het gebruik en de configuratie van TLS om te gaan. Deze handreiking zal actief moet worden verspreid en gebruikt.

Datum
16 oktober 2014

TLS staat sinds kort op de 'pas toe of leg uit'-lijst. TLS is de standaard die zorgt voor het opzetten van een met certificaten beveiligde verbinding (bijv. <https://...>). Bij de opname van TLS is bepaald dat voor een goede beveiliging het van belang is om TLS 1.2 (de nieuwste versie) te ondersteunen en daarnaast te zorgen voor veilige TLS-instellingen.

Zeer recent is er overigens een kwetsbaarheid bekend geworden in SSL versie 3, dat de voorganger is van TLS. Het NCSC adviseert om SSL versie 3 op servers en clients uit te schakelen waar mogelijk.¹

Ter kennisname:**Ad 3. Voortgang samenwerking ICCIO en College/Forum Standaardisatie**

In juli 2013 deed het College Standaardisatie een oproep aan het ICCIO om te komen tot een intensivering van de samenwerking tussen beide partijen². BZK/DGOBR heeft in onderstaande tekst kort de voortgang geschetst van een aantal van de samenwerkingsactiviteiten en bereikte resultaten van het afgelopen jaar. Deze tekst is in september ook met het College Standaardisatie gedeeld.

1. Sturen 'aan voorkant' op adoptie open standaarden

- a. Om generieke hergebruik van diensten en voorzieningen te bevorderen is de *enterprise architectuur rijksdienst (EAR)* in juni 2014 opgeleverd en vastgesteld in de ICBR.

In de EAR zijn de rijksregisters I-standaarden en generieke I-diensten (met de 'pas toe of leg uit'-standaarden van College Standaardisatie) opgenomen en geordend naar de verschillende informatiseringdomeinen. Hiermee wordt inzicht en ondersteuning geboden bij het gebruiken van standaarden en generieke I-diensten voor ICT-projecten en inkoopprocedures.

- b. *Kennisdeling, uitwisselen best practices, toegankelijke publicatie van lijsten en handreikingen voor de verschillende doelgroepen.*

Bureau Forum Standaardisatie enerzijds en het ICCIO anderzijds zijn structureel aangehaakt en stemmen af bij elkaars activiteiten.

Een aantal voorbeelden:

- De toetsing van 'pas toe of leg uit'- en Rijksstandaarden.
- De toetsing van "overweegvoorzieningen" en generieke i-diensten en voorzieningen.
- De ontwikkeling van de handreiking betrouwbaarheidsniveaus,
- De ontwikkeling van de generieke bestekteksten voor open standaarden
- Advisering over open standaarden bij aanbesteding (ON2013)
- Training ('Aanbesteden met ICT' bij Rafeb).

¹ Zie: <https://www.ncsc.nl/dienstverlening/response-op-dreigingen-en-incidenten/beveiligingsadviezen/NCSC-2014-0641+1.00+Kwetsbaarheid+in+SSL+3.0+ontdekt.html>

² Zie: <https://www.forumstandaardisatie.nl/sites/default/files/FS/2014/1028/Brief-College-Standaardisatie-aan-ICCIO-intensivering-samenwerking.pdf>

- c. *Rijksbrede ondersteuning bij adoptie per standaard(cluster) in rijksorganisaties.* Het gaat bijvoorbeeld om
- Programma Rijksoverheid 2.0
 - Overheidsbreed IP-nummerplan Minbzk (internet adressering met IPv6)
 - Taskforce BIR (baseline informatiebeveiliging rijksdienst): implementatie Informatiebeveiligingsstandaarden NEN/ISO 27001/27002.
 - Coördinatie invoering SEPA door Minfin (elektronisch betalingsverkeer)
 - Platform Rijksoverheid Online door Minaz (Webrichtlijnen).

Datum
16 oktober 2014

2. *Via generieke voorzieningen en shared services sturen op adoptie open standaarden*

- a. *De jaarlijkse monitor Open Standaarden Beleid is uitgebreid met generieke I-diensten en actualisatie van overheidsbrede (NUP-voorzieningen).* Door naast aanbestedingen waarin open standaarden terug (moeten) komen, het gebruik van open standaarden in deze diensten en voorzieningen te monitoren, ontstaat een beter inzicht in het gebruik van open standaarden bij de Nederlandse overheid.
- b. Verder stroomlijnen van shared services ICT en Inkoop. Voorbeelden: Aanbodstructurering generieke ICT is verder uitgewerkt, bijv. consolidatie datacenters, instelling Supplyboard (2013), instelling CTO-raad (2014). Van 350 inkooppunten naar 20 inkoopuitvoeringscentra (IUC's).
- c. Categoriemanagement Inkoop (9 ICT categorieën) en Strategisch Leveranciersmanagement (3 ICT leveranciers). Deze rijksbrede clustering maakt het mogelijk om de standaardisatie van ICT (open standaarden en generieke ICT) in het inkoopproces meer gericht te coördineren en professionaliseren.

Ad 4. Terugblik seminar Nieuwe Internetstandaarden

Op 9 oktober vond het seminar Nieuwe Internetstandaarden plaats. Meer dan 120 bezoekers (helpt bedrijfsleven, helpt overheid) waren aanwezig. Tijdens het seminar stond de nieuwe generatie internetstandaarden, die het internet veiliger en betrouwbaarder maakt, centraal. Specifiek gaat het daarbij om IPv6 (grote internetnummerreeks), DNSSEC (domeinnaambeveiliging), DKIM (phishingpreventie) en TLS (versleutelde verbindingen).

Het seminar startte met een videoboodschap van Vint Cerf (grondlegger internet, Google) en een keynote door Olaf Kolkman (chief Internet Technology Officer, Internet Society). Ook was er een interview met Gerben Klein Baltink die door EZ is aangesteld als kwartiermaker van het Platform Internetstandaarden. Vervolgens waren er twee tracks met bijdragen van o.a. de gemeente Heerlen, NCSC, Dienst Publiek en Communicatie, SURFnet, TNO, de Duitse overheid en het ministerie van Binnenlandse Zaken. Aan het afsluitende panel namen o.a. KNP Lokale Overheid en Ziggo deel.

Het seminar werd door het Forum Standaardisatie georganiseerd in samenwerking met ECP en Taskforce IPv6 en met support van SIDN, ISOC.nl en het Ministerie van Economische Zaken.