FS-20191211.05A3

Notitie

Duiding en maatregelen Monitor Open standaarden 2019

FORUM STANDAARDISATIE woensdag 11 december 2019

Aan:	Forum Standaardisatie
Van:	Het Bureau Forum Standaardisatie
Betreft:	Besluitvorming duiding en vervolgacties Monitor Open Standaarden 2019
Datum:	3 december 2019
Versie:	Concept 0.5
Bijlage:	Monitor Open Standaarden 2019

Inleiding

Forum Standaardisatie beheert een lijst met open standaarden *voor de gehele publieke sector*. Op deze lijst staan aanbevolen standaarden en de 'pas toe of leg uit'- standaarden, die voor overheidsorganisaties verplicht zijn. Verplicht omdat meer en beter gebruik van deze standaarden hard nodig is om te komen tot goede, betrouwbare en begrijpelijke digitale dienstverlening.

In zijn brief aan de Tweede Kamer bij het rapport Inventarisatie standaardisatie, verwoordt Minister Knops het zo:

"Het gebruik van open standaarden is nodig om het veilig en betrouwbaar elektronisch uitwisselen van gegevens tussen ICT-systemen en met burgers en bedrijven mogelijk te maken. Een standaard is open, wanneer die vrij bruikbaar is en door iedere softwareleverancier kan worden ingebouwd in een ICT-systeem"

In 2019 heeft het Forum Standaardisatie voor de achtste keer opdracht gegeven om onderzoek te doen naar het gebruik van de standaarden op de 'pas toe of leg uit'-lijst. Voor de meeste overheidsorganisaties is dit gebruik verplicht. Het monitoronderzoek bestaat uit vier onderdelen:

1. Het gebruik in aanbestedingen: Vragen overheidsorganisaties om de relevante open standaarden in aanbestedingen?
2. Het naar 'leg uit': Leggen overheidsorganisaties afwijkingen correct uit in het jaarverslag?
3. Het gebruik in voorzieningen: Passen beheerorganisaties de relevante open standaarden toe in generieke overheidsvoorzieningen?
4. Overig gebruik: Wat is, bezien per standaard, verder nog bekend over het gebruik van de standaarden op de 'pas toe of leg uit'- lijst?

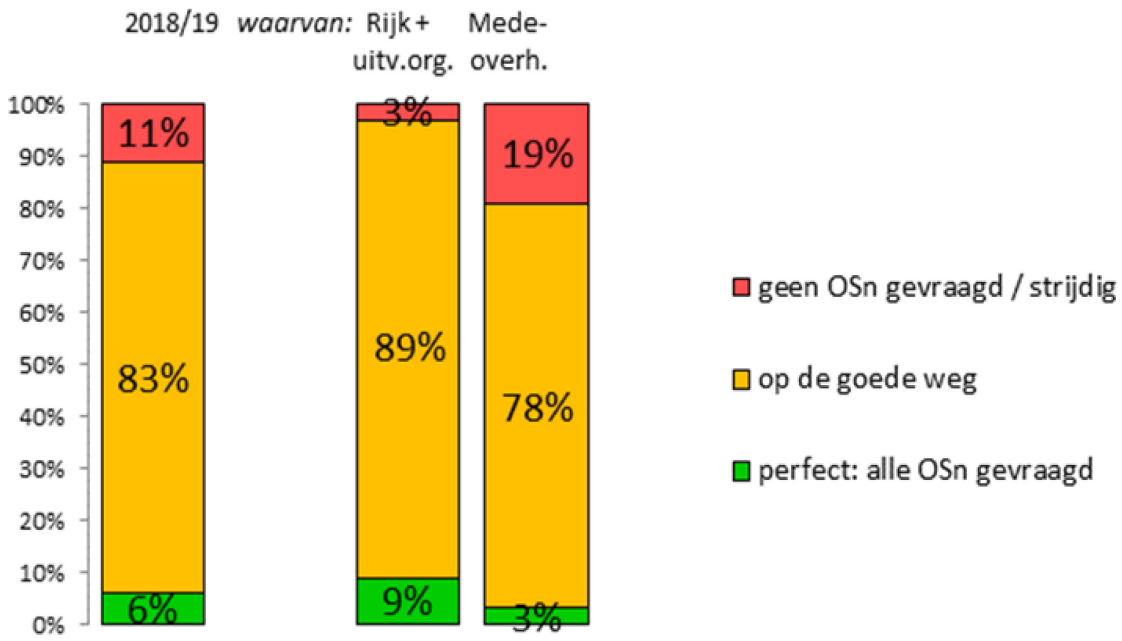
Het jaarlijkse monitoronderzoek is hét moment om terug te blikken (check/ duiding) en acties aan te scherpen (act/ acties) als het gaat om het gebruik van de 'pas toe of leg uit'- standaarden.

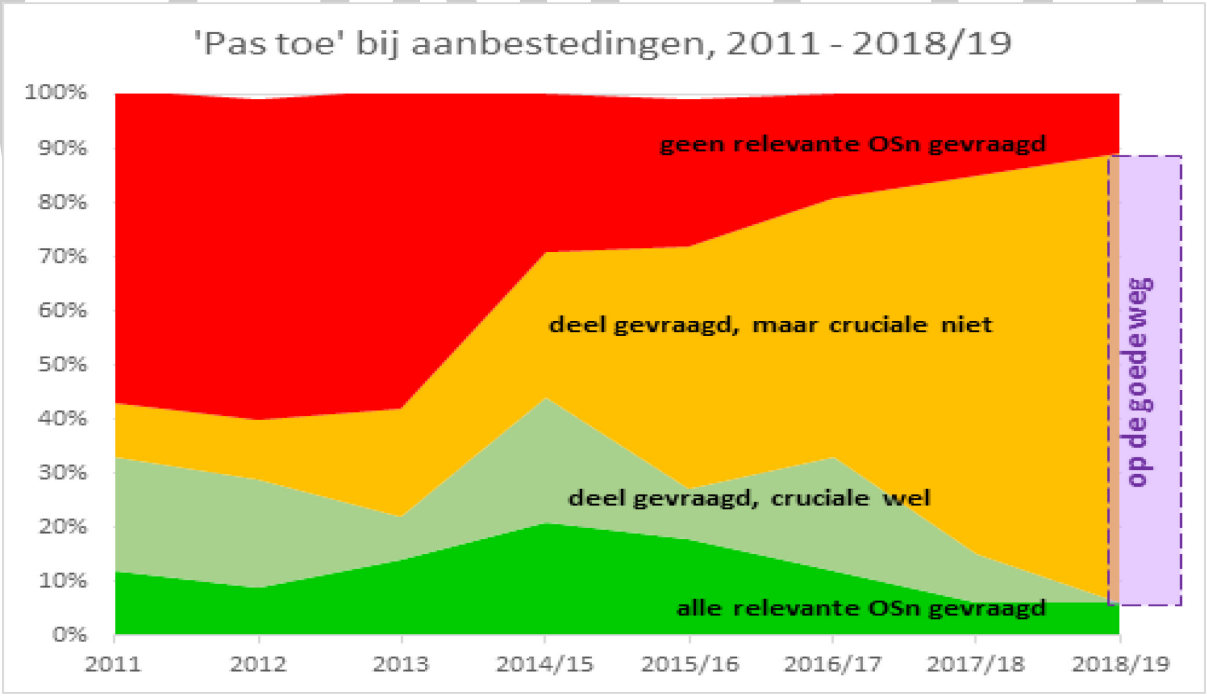
Dus nu de resultaten van de Monitor Open Standaarden 2019 bekend zijn, wat zijn de hoofdpunten uit het onderzoek volgens het Forum Standaardisatie?

Aanbestedingen en leg uit

De Monitor Open standaarden 2019 toont de volgende twee figuren, die gaan over de vraag naar de relevante open standaarden in aanbestedingen.

Een paar opmerkingen hierover:
- OSn= Open Standaarden
- In de tabel van Rijk en uitvoeringsorganisaties komt wegens afronding naar boven van de perfect scorende aanbestedingen (8,5%) en de aanbestedingen "op de goede weg " (88,5%) het totaal op 101%.
- De in 2019 ingevoerde term "op de goede weg" betekent dat één of meer open standaarden zijn uitgevraagd in een aanbesteding. Met andere woorden: een deel van alle de relevante standaarden.
- Het eerder gemaakte onderscheid "cruciaal en niet-cruciaal" komt vanaf 2019 niet meer voor in de weergave van de resultaten.


2018/19
waarvan: Rijk+ uitv.org.
Mede-overh.
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
11%
83%
6%
3%
89%
9%
19%
78%
3%
geen OSn gevraagd / strijdig
op de goede weg
perfect: alle OSn gevraagd


'Pas toe' bij aanbestedingen, 2011 - 2018/19
100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
2011
2012
2013
2014/15
2015/16
2016/17
2017/18
2018/19
geen relevante OSn gevraagd
deel gevraagd, maar cruciale niet
deel gevraagd, cruciale wel
alle relevante OSn gevraagd
op de goede weg

Deze twee grafieken en de conclusies van ICTU komen neer op een lichte stijging in de vraag naar open standaarden in aanbestedingen. Dat is ok. Als we kijken naar de eerste goal van het Forum Standaardisatie in het werkplan van 2019 dan staat daar:

De overheid is beter en veiliger verbonden doordat in minstens 90% van de aanbestedingen één of meer 'pas toe of leg uit'-standaarden wordt uitgevraagd.

Uit de Monitor blijkt dat in 6% van de aanbestedingen alle standaarden worden uitgevraagd en in 83% procent van de aanbestedingen ene deel van de relevante aanbestedingen. Dat maakt samen 89%. Dat betekent dat - op 1% na- het doel van 2019 is bereikt.

Aan de andere kant: de groep waar de relevante standaarden 'deels' zijn uitgevraagd is weliswaar "op de goede weg" maar nog steeds erg groot. Gemiddeld 83% van de aanbestedingen valt binnen deze categorie. Om hierin onderscheid te maken is per onderzochte aanbesteding een percentage gegeven van de mate waarin een aanbesteding 'op de goed weg is'. Hieruit blijkt is dat de meeste aanbestedingen in het midden van het midden zitten. Of met andere woorden: is een standaard relevant in een aanbesteding dan maakt deze circa 50% kans om in een aanbesteding ook daadwerkelijk uitgevraagd te worden. Met 50% kans is het net kop of munt. Wat geeft nu de doorslag?

Contact dat BFS had met inkopers – mede naar aanleiding van de Monitor Open standaarden- leert dat bekendheid met 'pas toe of leg uit' nog veel te wensen over laat. Vaak hebben inkopers nog nooit van de 'pas toe of leg uit'- lijst gehoord. Dit beeld wordt versterkt door klachten van leveranciers die de verplichte standaarden wél ondersteunen en zien dat opdrachten desondanks naar concurrenten gaan die dat niet doen. Zij zeggen: *"put your money where your mouth is"*.

Het Forum Standaardisatie vindt de grote groep aanbestedingen die "op de goede weg" zijn dus positief maar er is ook reden genoeg om vooral door te gaan op de reeds ingeslagen weg van (blijven zoeken naar) zo handig mogelijk communiceren over nut en noodzaak van open standaarden en stimuleren dat de aandacht voor de verplichting meer en beter in het inkoopproces vervlecht raakt.

Uit de staafgrafiek valt op dat rijksoverheidsorganisaties over het algemeen beter de verplichting naleven dan mede overheden. Dat is al jaren zo en wellicht ook niet zo verwonderlijk, gelet op het feit dat de instructie rijksdienst bij aanschaf van ICT-diensten en ICT- producten (integraal opgenomen als bijlage) klip en klaar ziet op de aanschaf van ICT bij het *rijk*. Dat mede overheidsorganisaties zoals gemeenten, provincies, uitvoeringsorganisaties en waterschappen *óók* verplicht zijn tot het gebruik van open standaarden, is minder duidelijk aangezien dat geen regelgeving betreft, maar een bestuurlijke afspraak in het OBDO (en voorheen Nationaal Beraad en College Standaardisatie).

Verder blijkt ook dit jaar weer dat in de jaarverslagen nergens correct wordt uitgelegd. En dat is erg.

Open standaarden toepassen in aanbestedingen en uitleggen in het jaarverslag

Het Forum Standaardisatie laat de volgende acties onder deze noemer vallen:

1. Het informeren van organisaties wanneer zij in beeld zijn voor het Monitoronderzoek. In het kader van het genereren van bekendheid van nut en noodzaak/ de verplichting worden door de onderzoekers van de Monitor Open Standaarden vanaf begin 2019 notificaties per e-mail verstuurd aan de contactpersonen bij een aanbesteding. Wanneer de aanbesteding op de groslijst staat voor nader onderzoek, wanneer de aanbesteding daadwerkelijk beoordeeld wordt en wat in dat geval de beoordeling is. In deze notificatie(s) wordt de contactpersoon/ de organisatie herinnerd aan de verplichting om open standaarden uit te vragen en worden tools aangereikt om aan de verplichting te kunnen voldoen. Zoals de *Beslisboom Open Standaarden* en *de handreiking vragen om open standaarden bij inkoop*.

2. De leden van het Forum Standaardisatie en het OBDO in stelling brengen om 'pas toe of leg uit' duidelijk te communiceren met de achterban, door de resultaten van de Monitor Open Standaarden en de IV metingen te agenderen in de gremia genoemd in onderstaande twee tabellen.

Gremium	**Groep**
CIO-raad	Rijk - ICT opdrachtgever
CTO-raad	Rijk - ICT opdrachtnemers
College van dienstverleningszaken	Gemeenten / VNG
CIO & CISO BZK	BZK
CIBO	Provincies
ICIA	Rijk - Inkoop
IMO	Rijk inkoop
Manifestgroep	Uitvoeringsorganisaties
o.a. CERT-WM	Waterschappen
PM	

3. Het Forum Standaardisatie vraagt aan het OBDO om opdracht te geven om open standaarden een structurele plaats te geven in de inkoop- en aanbestedingsprocessen van hun organisaties.

4. Het ministerie van BZK voert IN 2020 een verkenning uit naar aanleiding van het rapport Inventarisatie Standaardisatie om met inkopers en opdrachtgevers voor de organisaties vertegenwoordigd in het OBDO, na te gaan welke mogelijkheden er zijn binnen het bestaand instrumentarium om de toepassing van open standaarden te vergroten. Zie hiervoor de eerder genoemde brief aan de Tweede Kamer.
5. Het ministerie van BZK spreekt met de ADR spreken over het prioriteren van de handhaving van zowel 'pas toe' in aanbestedingen als 'leg uit'. Ook dit staat genoemd in voornoemde brief aan de Tweede Kamer. Want dat heeft momenteel geen prioriteit in de handhaving.

Voorzieningen

De tweede doelstelling in het werkplan van het Forum Standaardisatie luidt:

Overheid is beter en veiliger verbonden doordat in voorzieningen in minstens 80% van de gevallen voldaan wordt aan de relevante open standaarden.

Uit de Monitor Open Standaarden 2019 blijkt dat in 69% van de gevallen dat een standaard relevant is, voorzieningen voldoen aan de relevante open standaarden. In 15% van de gevallen staat de open standaard gepland en 16% van de gevallen voldoet een voorziening niet. Hoewel daarmee de doelstelling nog niet gehaald is kan wel gezegd worden dat het gebruik hier over het algemeen goed gaat. Toch wordt in sommige voorzieningen (al een aantal jaar) nog niet aan álle relevante standaarden voldaan.

Bij voorzieningen is vaak – in tegenstelling tot de aanbestedingen- niet de onbekendheid met open standaarden het probleem. Doordat de onderzoekers van de Monitor iedere jaar bij (meestal dezelfde) beheerders terugkomen, blijft de aandacht voor open standaarden aangewakkerd. Voor zover bekend gaat het bij voorzieningen vaker om vragen als "Wie moet wat nu precies gaan doen en wanneer?" en "is het niet toepassen van de standaard dan zo erg?".

Acties om bij voorzieningen de druk erop te houden zijn:

1. Beheerders van voorzieningen aanschrijven met de resultaten van de Monitor Open Standaarden en voor zover de voorziening (nog) niet voldoet, aandringen op het opnemen van open standaarden in de *release planningen* van die voorzieningen en in *the definition of done* bij organisaties met een Agile werkwijze.
2. Het ministerie van BZK zal vanaf begin 2020 verkennen hoe de toepassing van onder andere informatieveiligheid-standaarden van de pas-toe-of-leg-uit lijst in de reguliere informatieveiligheids-, bedrijfsvoerings- en controlprocessen kan worden versterkt
3. Nadrukkelijke agendering van de tabellen op pagina 40 en 41 in het OBDO met de mate waarin voorzieningen al dan niet aan de relevante open standaarden voldoen.

Overig gebruik per standaard

Het onderzoek naar wat per standaard verder nog bekend is over het gebruik, laat ook dit jaar een divers beeld zien. Zie de tabel op pagina 12 van de Monitor Open Standaarden 2019.

Van circa de helft van de standaarden op de 'pas toe of leg uit'- lijst is weinig tot niets bekend als het gaat om het gebruik. Dit werd ook al in 2018 geconstateerd. Hoe hiermee om te gaan is in 2019 nadrukkelijk ter sprake gebracht door de accountmanagers van het Forum Standaardisatie met de indieners en beheerders van de desbetreffende standaarden. In deze gesprekken zijn vragen gesteld als: kan de adoptie-ambitie explicieter en meetbaarder worden gemaakt, is de standaard inmiddels gangbaar of wat is nut en noodzaak van de 'pas toe of leg uit'-status voor deze standaard? In de loop van 2020 mag het Forum Standaardisatie een nader advies verwachten als het gaat om standaarden waarover weinig gebruiksgegevens bekend zijn. Het ligt voor de hand dat deze adviezen betrekking zullen hebben op de toepassing van de aanmeld- en (her)toetsingscriteria voor open standaarden op de 'pas toe of leg uit'-lijst.

Terug naar het laatste deel van het monitoronderzoek. Uit de tabel op pagina 12 blijkt ook dat er een andere groep standaarden is (grofweg de andere helft) waarvan het gebruik redelijk goed in beeld is. Dit geldt met name voor de internet- en beveiligingsstandaarden die gemeten kunnen worden via internet.nl. Uit de Monitor Open Standaarden blijkt dat het gebruik van deze standaarden nog steeds stijgt. Ook hier weer, dat is mooi maar het gaat soms niet hard genoeg.

Aan het einde van deze notitie maakt het Forum Standaardisatie daarom van de gelegenheid gebruik om een standaard uit te lichten en de volgende oproep te doen:

Geeft opdracht DMARC te implementeren

Zie opdrachtbeschrijving in de bijlage

Uit de laatste IV-meting, die als bijlage is gevoegd bij de Monitor Open Standaarden 2019, blijkt namelijk dat het streng afstellen van DMARC blijft steken waardoor criminelen zich nog steeds makkelijk als overheidsorganisatie kunnen voordoen. Het Forum Standaardisatie maakt zich hier bijzonder ongerust over en heeft daarom een concept opdrachtomschrijving 'traject strenger afstellen anti-phishing maatregelen (DMARC)' opgesteld om te gebruiken voor de lezer van deze notitie in de hoedanigheid als ICT opdrachtgever.

Deze opdrachtomschrijving gaat hierbij als bijlage met het dringende verzoek deze te gebruiken om DMARC te laten implementeren. Dit verzoek zal het Forum Standaardisatie ook aan het OBDO doen.