notitie

Forum Standaardisatie
www.forumstandaardisatie.nl
forumstandaardisatie@logius.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 19 oktober 2016

Agendapunt 8. Aard verplichting ptolu-lijst
Stuknummer 8. Notitie aard verplichting ptolu-lijst

Van:	Bureau Forum Standaardisatie
Aan:	Forum Standaardisatie
Bijlagen:	geen

Ter besluitvorming

Het Forum wordt gevraagd te bespreken/in te stemmen met de voorstellen:

1. een analyse te maken van de functionele toepassingsgebieden op de ptolu-lijst, een prioritering te maken van waar het functioneel toepassingsgebied duidelijker kan en voor die geprioriteerde standaarden aan het Forum een voorstel te doen van wat de omschrijving zou moeten zijn.

2. voortaan consequent in communicatie te benadrukken dat de pas-toe-of-leg-uit-lijst een gezamenlijke afspraak betreft van in het Nationaal Beraad, op hoogambtelijk niveau, overheidsbreed en van beleid en uitvoering.

Ter bespreking/instemming

1. Inleiding

In het Forum van 15 maart 2016, kwam de omschrijving van de functionele toepassingsgebieden op de pas-toe-of-leg-uit-lijst ter sprake, met name de behoefte aan meer duidelijkheid daarover.
In deze notitie wordt de instructie toegelicht (paragraaf 2). Daarna wordt een voorstel gedaan om meer helderheid te krijgen over hetgeen de geadresseerden van de verplichting moeten doen (paragraaf 3). En wordt in paragraaf 4 een ander - gerelateerd - probleem rondom de beeldvorming van de pas-toe-of-leg-uit-lijst geadresseerd, namelijk het onterechte beeld dat het Forum standaarden op de lijst zet in plaats van organisaties zelf.

2. Toelichting Rijks instructie

2a. Het pas-toe-deel

Rijksinstructie[1] Artikel 3 lid 1." Bij de aanschaf van een ICT-dienst of ICT-product voor een toepassingsgebied dat voorkomt op de lijst die op de website www.forumstandaardisatie.nl is gepubliceerd, wordt gekozen voor een ICT-dienst of een ICT-product dat gebruikt maakt van een bij het desbetreffende toepassingsgebied vermelde open standaard."

De onderbouwing van de instructie is dat overheidsorganisaties zoveel mogelijk dezelfde (open) standaarden gebruiken, zodat ze interoperabel zijn en eilandautomatisering wordt voorkomen: "het gebruik van open standaarden door overheidsorganisaties is niet meer vrijblijvend"[2].

Daarmee doorbreekt de instructie de louter eigen afweging van een overheidsorganisatie behoudens de mogelijkheid van 'leg-uit' (zie hieronder).

Doordat de instructie verwijst naar het desbetreffende toepassingsgebied van de ICT-dienst of het ICT-product wordt de inhoud van de verplichting mede bepaald door de omschrijving van het functionele toepassingsgebied.

2b. Het leg-uit-deel

Rijksinstructie Artikel 3 lid 2. "Van het eerste lid kan worden afgeweken indien een dergelijke dienst of product naar verwachting in onvoldoende mate wordt aangeboden, onvoldoende veilig of zeker functioneert, of om andere redenen van bijzonder gewicht."

Dit onderdeel van de Rijksinstructie voorkomt onzinnige toepassing van de standaarden (om te voorkomen dat het een 'wet van Meden en Perzen' wordt). Afwijkingen moeten overigens wel worden opgenomen in het jaarverslag van een organisatie (artikel 4).

2c. Voor wie is de instructie verplicht?
- Voor de Rijksdienst en de onder hen ressorterende diensten.[3]
- Voor de overige overheidsorganisaties die zijn vertegenwoordigd in het Nationaal Beraad[4].

[1] Rijksinstructie inzake aanschaf van ict-diensten en ict-producten. Staatscourant, 8 november 2008, nr. WJZ/8157380 https://zoek.officielebekendmakingen.nl/stcrt-2008-837.html
[2] Zie toelichting op Rijksinstructie.
[3] Het gaat daarbij ook om uitvoeringsorganisaties, zoals UWV en SVB (https://www.rijksoverheid.nl/ministeries/ministerie-van-sociale-zaken-en-werkgelegenheid/inhoud/diensten-en-instellingen-szw)
[4] Besluit van het Nationaal Beraad van mei 2015, tot verlening van de afspraak tot overheidsbrede werking van de instructie, zoals die eerder was overeengekomen in de bestuursakkoorden.

3. Meer duidelijkheid over inhoud verplichting rijksinstructie

Zoals gezegd wordt inhoud van de verplichting mede bepaald door de omschrijving van het functionele toepassingsgebied.

Voor een aantal standaarden is dat functionele toepassingsgebied momenteel helder omschreven:

> Bijvoorbeeld het Semantisch Model E-Factureren (SMEF): "De verzending van elektronische facturen door organisaties die deelnemen aan het economisch verkeer in Nederland (waaronder overheden) en de ontvangst hiervan door overheden."
> Daaruit volgt dat overheidsorganisaties wanneer ze elektronische facturen gebruiken ze deze in SMEF moeten kunnen ontvangen.
>
> Bijvoorbeeld SETU: "De elektronische berichtenuitwisseling rondom de bemiddeling/inhuur van flexibele arbeidskrachten."
> Daaruit volgt dat bij een investering in een ICT-dienst of –product dat elektronisch berichten uitwisselt over bemiddeling/inhuur van flexibele arbeidskrachten gekozen moet worden voor een product dat de SETU standaard gebruikt.[5]

Voor een aantal standaarden kan dat helderder:

> Zo staat er bij TLS "Het met behulp van certificaten beveiligen van de verbinding (op de transportlaag) tussen client- en serversystemen of tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internettechnologie."
>
> Wannéér de toepassing van certificaten moet plaatsvinden staat *niet* in de omschrijving van het functionele toepassingsgebied. Dat maakt minder helder wanneer TLS moet worden toegepast: wannéér je moet beveiligen.
>
> Een omschrijving van het functioneel toepassingsgebied zoals "e-overheidsdienstverlening - zoals websites en apps - die gevoelige gegevens uitwisselen zoals persoonsgegevens en financiële gegevens" is duidelijker.

Een dergelijke omschrijving sluit aan bij de invulling van bestaande verplichtingen zoals artikel 13 Wet Bescherming Persoonsgegevens (WBP[6]), de adviezen van het NCSC [link], de ISO27001-2/BIR/BIG/BIWA en de inhoud van de DigiD-assessments.

Door de omschrijving op de ptolu-lijst telkens meer te gieten in de vorm "als [overheidswebsite met financiele of persoonsgegevens]… dan …[TLS]," wordt voorkomen dat het een zoekplaatje wordt. Het probleem is immers niet alleen dat overheidsorganisaties verkeerde beveiligingsstandaarden voeren, maar ook dat ze soms helemaal geen beveiligingsstandaarden gebruiken.

Tegelijkertijd wordt door verwijzing naar voornoemde normenkaders duidelijk dat de standaarden een middel zijn om aan (een deel) van die verplichtingen te voldoen, én wordt de samenhang duidelijk: het betreft dus géén extra verplichting en het betekent ook dat je er – met alleen de implementatie van de beveiligingsstandaarden – nog niet bent (ze zijn een schakel in het geheel).

---

[5] De omschrijvingen verplichten niet elke overheidsorganisatie om de SMEF of SETU te gebruiken. Alleen wanneer je elektronische facturen gebruikt, of elektronische informatie over flexibele arbeidskrachten uitwisselt.

[6] Verder uitgewerkt in "CBP richtsnoer: beveiliging van persoonsgegevens" (http://wetten.overheid.nl/BWBR0033572/2013-03-01)

Verder wordt door een helderder functioneel toepassingsgebied voorkomen dat elke overheidsorganisatie een louter eigen afweging maakt voor de toepassing van de standaard, en daarmee de adoptie van de standaard achterblijft, waardoor het nut van de standaard (bijvoorbeeld dat een burger/bedrijf een overheidswebsite altijd op dezelfde wijze kan herkennen) onvoldoende is[7]. Het komt ook tegemoet aan de wens van De Kamer die consequent aandringt aan op betere adoptie en handhaving[8].

Voorstel is een analyse te maken van de functionele toepassingsgebieden op de ptolu-lijst, een prioritering te maken van waar het functioneel toepassingsgebied duidelijker kan en voor die geprioriteerde standaarden aan het FS een voorstel te doen van wat de omschrijving zou moeten zijn. Daarbij komt ook de samenhang met andere normenkaders aan de orde.

4. Framing van de inhoud van de pas-toe-of-leg-uit lijst

In de zoektocht naar *bottlenecks* bij de adoptie van standaarden is onder andere naar voren gekomen dat soms het beeld bestaat dat:

- Het Forum c.q. de procedure bestaat uit technische experts die een louter technische standaard-inhoudelijke afweging maken.
- Dat er wordt besloten over overheidsorganisaties zónder die overheidsorganisaties.

Die indruk is onterecht. Om dit beeld weg te nemen wordt – naast voortzetting van de inhoudelijke betrokkenheid van alle stakeholders – ingezet op het benadrukken van het feit dat het afspraken betreft in het overheidsbrede hoogambtelijk Nationaal Beraad, waarin beleid én uitvoering zijn vertegenwoordigd. In iedere communicatieuiting zal consequent worden benadrukt dat het overheidsbrede Nationaal Beraad tot de toepassing van een bepaalde standaard heeft besloten. Verder zal worden bekeken of het 'stempel' dat in het verleden werd gebruikt 'goedgekeurd door het College Standaardisatie' nieuw leven kan worden ingeblazen.

De benadrukking van de gezamenlijke afspraak beoogt ook de mogelijke reactie 'dat bepaal ik als organisatie zelf wel' weg te nemen. De invulling van de pas-toe-of-leg-uit-lijst, betreft namelijk *hun eigen* afspraak.

Voorstel: voortaan consequent te benadrukken dat de pas-toe-of-leg-uit-lijst een gezamenlijke afspraak betreft van in het Nationaal Beraad, op hoogambtelijk niveau, overheidsbreed en van beleid en uitvoering (bijvoorbeeld dmv. een stempel 'goedgekeurd door het Nationaal Beraad').

---

[7] Het nut van standaarden stijgt exponentieel bij de toepassing ervan. Dat betekent helaas ook dat het totale nut akelig snel afneemt wanneer partijen de standaard niet gebruiken (ter illustratie: het nut van de standaard 'rechts rijden op de snelweg' neemt zienderogen af wanneer een enkeling besluit links te rijden).

[8] Eindrapport commissie 'Elias' Tweede Kamer, vergaderjaar 2014-2015, 33 326, nr. 5, p. 21
Motie Oosenbrug/Gesthuizen, Tweede Kamer, vergaderjaar 2014-2015, 33 326, nr. 21
Motie Oosenbrug/Veldman, Tweede Kamer, vergaderjaar 2015-2016, 34 300 VII, nr. 36