



notitie

FORUM STANDAARDISATIE 13 maart 2019
Agendapunt 6 Open standaarden, adoptie

Aan: Forum Standaardisatie
Van: Stuurgroep Open Standaarden
Datum: 21-02-2019
Versie: 1.0
Bijlagen: FS-190313.6A Opzet Monitor 2019
FS-190313.6B Onderzoeksrapport Herkenbaarheid en betrouwbaarheid van websites en e-mails (**ONDER EMBARGO**)
FS-190313.6C1 Brief CCvDD aan Forum Standaardisatie inzake reikwijdte ptolu-lijst
FS-190313.6C2 Concept-reactie Forum op brief CCvDD
FS-190313.G Overzicht uitzetten Monitor 2018 en IV-meting medio-2018 in-achterban

Samenvatting

Ter bespreking

- A. Opzet monitor open standaarden 2019
- B. Onderzoek 'Herkenbaarheid van en vertrouwen in websites en e-mails van de overheid'
- C. Reactie van Forum Standaardisatie op brief Centraal College van Deskundigen-Datastandaarden (CCvDD)

Ter kennisname

- D. Ontwikkelingen documentstandaarden
- E. Ontwikkelingen API's
- F. Ontwikkelingen moderne internetbeveiligingsstandaarden
- G. Overzicht uitzetten Monitor 2018 en IV-meting medio-2018 in-achterban
- H. Overig

Ter bespreking

Ad A. Opzet monitor open standaarden 2019

[Bijlage A]

Het Forum Standaardisatie wordt gevraagd om in te stemmen met:

Opzet monitor open standaarden 2019

In bijlage A vindt u de aanpak van de Monitor Open Standaarden 2019 het onderzoek naar het gebruik van de standaarden op de 'pas toe of leg uit'-lijst.

De aanpak bevat als vanouds drie onderdelen:

1. Aanbestedingen: vragen inkopers/ opdrachtgevers de relevante standaarden uit?
2. Voorzieningen: passen beheerders van de voorzieningen de relevante standaarden toe?
3. Overig gebruik: wat kan nog meer gezegd worden over het gebruik van de standaarden op de pas toe of leg uit lijst?

Ad 1. Aanbestedingen

In de Monitor open standaarden 2019 zullen voor de tweede keer alle onderzochte aanbestedingen genoemd worden. In 2018 is dit voor het eerst gedaan. *Nieuw in 2019 is dat is het de bedoeling is om gedurende het onderzoek driemaal contact op te nemen met de aanbestedende organisatie. De eerste keer als de aanbesteding in beeld is op de groslijst. De tweede keer als de aanbesteding ook daadwerkelijk onderzocht wordt en de laatste keer om de onderzochte partijen te informeren over de uitkomst van het onderzoek.*

Het idee hierachter is om een adoptiewerking uit te laten gaan van het doen van het onderzoek zelf door op deze manier meer en eerder bij inkopers in beeld te komen. Het komt nog te veel voor dat inkopers de verplichting niet kennen om naar de relevante open standaarden te vragen en ook nog nooit gehoord hebben van de Monitor open standaarden. Op deze manier komt daar hopelijk verandering in.

Ad 2. Voorzieningen

Dit onderdeel blijft ongewijzigd ten opzichte van vorige jaren. De adoptie van open standaarden in centrale overheidsvoorzieningen verloopt over het algemeen goed en vermoedelijk houdt het jaarlijks contact dat de onderzoekers onderhouden met de beheerders van de voorzieningen verband hiermee.

Ad 3. Overig gebruik

In 2019 zal het Bureau Forum Standaardisatie - net als voor het eerst in 2018- ingezet worden om te achterhalen wat nog meer gezegd kan worden over het gebruik van de standaarden op de 'pas toe of leg uit'-lijst. De accountmanagers onderhouden hiertoe het contact met de beheerders van de open standaarden of hebben andere bronnen om verder nog een beeld te kunnen schetsen over het gebruik.

Ad B. Onderzoek 'Herkenbaarheid van en vertrouwen in websites en e-mails van de overheid'

[Bijlage B / Presentatie]

Het Forum Standaardisatie wordt gevraagd om:

In het kader van hun signalerende taak het Kantar rapport te bespreken en de mogelijkheden dat succesvol verder te brengen.

Omdat het voor eindgebruikers steeds moeilijker wordt om te zien van wie een website of e-mail is*, en om én phishing blijft aanhouden, heeft BZK/DIO een onderzoek laten uitvoeren naar de herkenbaarheid van overheidssites en e-mail.

Daaruit blijkt dat een zeer grote groep niet in staat is om te herkennen of een site of e-mail van de overheid is, of van een private partij. Daarnaast is een zeer grote groep niet goed in staat om een bonafide mail of site van een malafide mail of site te onderscheiden. Het onderzoek concludeert onder andere dat een standaard overheids subdomein, zoals *.overheid.nl of *.gov.nl, daarbij zou helpen. Als voorbeeld: de huidige logius.nl site, zou dan logius.overheid.nl gaan heten. In de UK (*.gov.uk), Duitsland (*.bund.de), Frankrijk (*.gouv.fr) en de EU bestaan die al.

In de vergadering wordt het publieksonderzoek van Kantar gepresenteerd, in- en uitgeleid door BFS.

De voorgenomen vervolgstap is dat vervolgens de impact van een dergelijke beleidslijn (incl. geleidelijke transitie) uitgebreid wordt onderzocht. De intentie is daarbij aan Rijkszijde op te trekken met AZ/DPC (Dienst PublieksCommunicatie) en CIO-Rijk.

Het bureau Forum Standaardisatie is (op de achtergrond) betrokken bij de opzet van het onderzoek.

Aanvullend

1. De huidige wilgroei aan domeinnamen, ook bij de overheid, lijkt een voorbeeld van wat de Raad van State in haar ongevraagd advies noemt: "de overheid de ambitie een iOverheid te worden [...] niet op een gecoördineerde wijze [nastreeft]. Het gemak van het functioneren van de overheid staat voorop. Bij de implicaties daarvan voor de verhouding tussen overheid en burger wordt onvoldoende stilgestaan. [...] Gevreesd moet daarom worden dat vooral de burger dreigt te worden opgezadeld met de risico's, het ongemak en de nadelen van het gebruik van deze technieken door de overheid.[§ 1]". Beter herkenbare overheidsdomeinnamen passen bij het beleidsvoornemen om de Burger Centraal te stellen.
2. Een dergelijk overheids domeinnaam beleid kan ook helpen bij de problemen die naar voren komen in het onderzoeksrapport "De schade van e-mail" van Cyberonderzoeksraad (Brenno de Winter c.s.): <https://dewinter.com/2019/02/15/cyberonderzoeksraad-rapport-de-schade-van-e-mail/>
Zij schrijven daar over op hun website: "De Cyberonderzoeksraad heeft een groot onderzoek uitgevoerd naar de gevoeligheid van e-mail. Meer dan 70 domeinnamen die op andere domeinen lijken, werden geregistreerd. Vervolgens werd gewacht op binnenkomende berichten. Er bleken ruim 15.000 e-mails binnen te komen. Na het filteren van spam en virussen bleven er zo'n 3.100 relevante berichten over. Tussen deze berichten zaten gevoelige zaken als processen-verbaal, aangiftes, medische dossiers, rekeningen, kopieën van bankafschriften, kopieën van identiteitspapieren, bestellingen (zelfs voor spionageapparatuur), vorderingen, departementaal vertrouwelijke stukken en meer."
3. Ook in het communicatie vakblad adformatie van november wordt gepleit voor "Herkenbaarheid. De Rijksoverheid is altijd, ongeacht het kanaal of het medium, herkenbaar als afzender" (2^e uitgangspunt voor overheidscommunicatie).

Ad C. Reactie van Forum Standaardisatie op brief CCvDD
[Bijlagen C1 en C2]

Het Forum Standaardisatie wordt gevraagd om:

De concept-brief van het Forum aan het CCvDD te bespreken en te accorderen voor verzending.

Het Centraal College voor Deskundigen-Datastandaarden (CCvDD) schreef eind oktober het Forum aan om twee knelpunten onder de aandacht te brengen. Het CCvDD ziet graag beter geborgd dat bestaande 'pas toe of leg uit'-standaarden expliciet uitgangspunt zijn bij de uitvoering en implementatie van wets- en beleidsontwikkelingen op rijksniveau. Ook geeft het College aan te signaleren dat de mate waarin de 'pas toe of leg uit'-lijst daadwerkelijk wordt gevolgd beperkt is en constateert dat de bekendheid van de lijst bij de decentrale overheden gering is.

In voorliggende concept-brief geeft het Forum aan beide punten te herkennen en de behoefte deze te verbeteren te onderschrijven. Wat voor het onderdeel wetsontwikkeling helpt, is dat sinds kort dit uitgangspunt ook is geborgd in de Aanwijzingen voor de regelgeving. Wat betreft de bekendheid van de lijst bij de (decentrale) overheden wordt in de brief aangegeven dat het Forum dit en komende jaren extra gaat inzetten op het kenbaar maken bij decentrale overheden van de lijst.

Ter kennisname

Ad D. Ontwikkelingen documentstandaarden

- Het aantal leden van de community site <https://opendocumentstandaarden.pleio.nl/> is sinds december 2018 meer dan verdubbeld. BFS beheert deze community site voor organisaties die ervaringen en kennis willen uitwisselen over toegankelijkheid en documenten. Omdat de community behoefte heeft aan een beter overzicht van het marktaanbod is er op de community site ruimte gemaakt voor leveranciers van toegankelijkheidsproducten en -diensten.
- Op 23 september 2019 moeten alle nieuwe overheidswebsites voldoen aan de toegankelijkheidswetgeving, dus ook onze community site op Pleio voor open documentstandaarden. Wij hebben geconstateerd dat het Pleio platform nog niet voldoet aan de toegankelijkheidswetgeving. Hierover zijn wij in gesprek met de stichting Pleio. Pleio doet op dit moment een nulmeting om de mate van toegankelijkheid van het platform te toetsen. In april zal Pleio doorontwikkeld worden om aan de toegankelijkheidswetgeving te voldoen. Bureau Forum Standaardisatie heeft Pleio hierbij aangeboden als dit nodig mocht zijn.
- Alle documenten gepubliceerd vanaf 23 september 2018 op de website van het Forum Standaardisatie moeten voldoen aan de toegankelijkheidswetgeving. Dit geldt ook voor oudere documenten die nog betrokken zijn bij actieve processen, bijvoorbeeld de beschrijving van de criteria en procedure voor de pas-toe-of-leg-uit lijst. Een aantal leden van Bureau Forum Standaardisatie heeft daarom samen met de leden van digitoegankelijk.nl een training 'Toegankelijke PDFs maken' gevolgd, met het doel om de eigen publicaties toegankelijk te publiceren. In maart zal de rest van Bureau Forum Standaardisatie de cursus volgen samen met een aantal deelnemers van Logius. Vanaf nu worden alle Forumstukken voor verzending en publicatie gecontroleerd op toegankelijkheid. Ook gaan wij werken aan het toegankelijk maken van bestaande documenten die nog betrokken zijn bij actieve processen.

Ad E. Ontwikkelingen API's

- Woensdag 13 februari 2019 presenteerde het Kennisplatform APIs het concept voor een API strategie voor de overheid (<https://docs.geostandaarden.nl/api/API-Strategie/>). Het Kennisplatform APIs werkt aan deze API strategie met als doel om overheden hun RESTful APIs op een uniforme gebruikersvriendelijke manier te laten aanbieden. Het Kennisplatform APIs kondigde op hetzelfde evenement de openbare consultatie aan van deze API strategie.
- Tegelijkertijd ligt er een overheidsprofiel voor OAuth ter consultatie (<https://docs.geostandaarden.nl/api/oauth/>). OAuth wordt met dit profiel gebruikt in applicaties waarbij gebruikers toestemming geven aan een dienst van een derde om namens deze dienst toegang te krijgen tot specifieke gegevens via een RESTful API. OAuth is in 2016 getoetst voor opname op de pas-toe-of-leg-uit lijst. In de vergadering van 19 april 2017 besloot het Forum Standaardisatie om OAuth pas op de pas-toe-of-leg-uit lijst te plaatsen na de ontwikkeling van een overheidsprofiel (<https://www.forumstandaardisatie.nl/sites/default/files/FS/2017/0419/FS-20170419.02B-Forumadvies-OAuth-2.0.pdf>). Wanneer dit overheidsprofiel is vastgesteld, zal het OBDO worden geadviseerd om OAuth op te nemen op de pas-toe-of-leg-uit lijst.
- Bij het evenement op 13 februari waarbij de openbare consultaties van de API strategie en OAuth zijn aangekondigd, werd ook de prijs voor de beste (overheids) API uitgereikt. Van de 10 inzendingen werden de API van Luchtmeetnet, de API van de Kamer van Koophandel en de BAG API van Kadaster genomineerd. De BAG API werd door de onafhankelijke jury (Jascha van Hoorn, Joeri Bekker, Brenno de Winter) gekozen als winnaar van de 'Gouden API' award.

Ad F. Ontwikkelingen moderne internetbeveiligingsstandaarden

- Platform Internetstandaarden, waarin Forum Standaardisatie participeert, heeft op 21 februari een nieuwe versie van Internet.nl gelanceerd. De nieuwe versie test ook op applicatie-beveiligingsoptie oftewel security headers. De resultaten van deze nieuwe testen tellen nog niet mee in de eindscore. Ook is de softwarecode als open source gepubliceerd. Voor meer informatie: <https://internet.nl/article/open-source-release/>
- NCSC en Forum Standaardisatie organiseerden in samenwerking met de Duitse BSI de 2de internationale workshop 'Modern E-Mail Security Standards for EU Governments' op 14 december in Den Haag. Verschillende deelnemers (o.a. Estland en Noorwegen) gaven presentaties over hun ervaringen en plannen. De Britten boden aan een volgende bijeenkomst in het voorjaar 2019 te willen organiseren. Ondertussen is er een mailinglist en online platform waarop deelnemers tussen de workshops kennis en ervaringen kunnen uitwisselen.
- Op 14 februari heeft Forum Standaardisatie het 19^{de} Overleg Betrouwbare OverheidsMail georganiseerd. Dit keer waren er inhoudelijke bijdragen van SSC-ICT, Politie, leverancier Infoblox, Platform Internetstandaarden (over DANE-configuratie) en de Belastingdienst (over Typosquatting/'look-alike' domeinnamen).
- Op 17 januari vond een bijeenkomst van Platform Internetstandaarden plaats, die Forum Standaardisatie i.s.m. ECP had voorbereid. Dit keer was het centrale thema internet routing security en in het bijzonder de RPKI-standaard. Er stonden bijdragen van Internet Society, RIPE NCC, BIT en NLnet Labs op de agenda.
- Overig:
 - Politie.nl scoort sinds kort 100% in zowel de website- als mailtest op Internet.nl
 - Voor DANE is door OBDO een overheidsbrede implementatieafspraken gemaakt die overheden verplicht om de standaard voor eind 2019 te implementeren. Uit medio 2018 uitgevoerde metingen van Forum Standaardisatie bleek dat meer dan 20% van de overheden DANE-records (voor veilige mailserver-verbindingen) publiceren. De groei zit er ondertussen behoorlijk in. SSC-ICT ondersteunt nu bijvoorbeeld ook DNSSEC en DANE op haar mailserver die door veel Rijksoverheden (zoals BZK en SZW) wordt gebruikt.
 - Gemeente Den Bosch ondersteunt als waarschijnlijk eerste gemeente DANE-verificatie (voor veilige mailserver-verbindingen).

Ad G. Overzicht uitzetten Monitor 2018 en IV-meting medio-2018 in-achterban

[bijlage G]

De leden van het Forum Standaardisatie hebben afgesproken dat ieder Forum-lid de IV-meting en de Monitor Open standaarden 2018 verspreidt onder en onder de aandacht brengt bij zijn/haar eigen achterban. Tevens hebben de leden van het Overheidsbrede Beleidoverleg Digitale Overheid (OBDO) op 12 februari ingestemd om de Monitor en de IV-meting te agenderen in hun organisatie en hun achterban. Daarnaast stemden zij in met het aansturen op het opnemen van eventuele 'let uit' in het jaarverslag van hun organisatie dan wel de jaarverslagen van hun achterban. Zie ook agendapunt 02C. van deze vergadering voor meer achtergrondinformatie over hetgeen het OBDO hierover besproken heeft.

In het voorliggende overzicht vindt u een overzicht van de huidige stand van zaken voor zover bekend en de gremia waarin de Monitor en IV-meting (kunnen) worden besproken, mede na instemming van het OBDO. U wordt gevraagd updates te melden

Ad H. Overig

- Magazine 'RO Standaarden. Van toen tot nu: 10 jaar beheer',
<https://www.geonovum.nl/over-geonovum/actueel/tien-jaar-beheer-ro-standaarden>
- Actualisatie overzicht leveranciers marktscan Digikoppeling gepubliceerd,
<https://www.vngrealisatie.nl/nieuws/actualisatie-overzicht-leveranciers-marktscan-digikoppeling-gepubliceerd>
- Gemeenten en VNG Realisatie ontwikkelen nieuwe standaard met 'agile' werkwijze,
<https://www.vngrealisatie.nl/nieuws/gemeenten-en-vng-realisatie-ontwikkelen-nieuwe-standaard-met-agile-werkwijze>
- E-facturatie in Europees formaat verplicht vanaf 18 april, <https://logius.nl/actueel/e-facturatie-europees-formaat-verplicht-vanaf-18-april>
- Toegankelijke overheid, <https://logius.nl/actueel/toegankelijke-overheid>