Notitie

FORUM STANDAARDISATIE 8 december 2021
Agendapunt 4 Open standaarden, adoptie

Nummer:	FS 20211208.4
Aan:	Forum Standaardisatie
Van:	Stuurgroep Open Standaarden
Datum:	25 november 2021
Versie:	1.0
Bijlagen:	FS-20211208.4A-Agendering-sponsorschap-en-aanwezigheid-Forum-leden FS-20211208.4B-Meting-informatieveiligheidsstandaarden-sept-2021 FS-20211208.4C1-Duiding-en-maatregelen-Monitor-Open-standaarden-2021 FS-20211208.4C2-Monitor-Open-standaarden-2021-v1.0 FS-20211208.4D-Opzet-Monitor-Open-standaarden-2022-dd-23-nov-2021-verkorte-versie

Samenvatting

Ter bespreking

A. Agendering IV-meting en Monitor, sponsorschap door Forumleden, en aanwezigheid
B. Meting informatieveiligheidsstandaarden september 2021
C. Monitor Open standaarden 2021: duiding en maatregelen
D. Monitor Open standaarden 2022: onderzoeksopzet

Ter kennisname

E. Streefbeeldafspraak IPv6 voor duurzame bereikbaarheid
F. Standaarden voor veiliger internet
G. Standaarden voor inclusie en digitale toegankelijkheid
H. API's voor betere, snellere gegevensuitwisseling en samenwerking
I. Herkenbare en veilige digitale overheid
J. Eenduidige dienstverlening

Ter bespreking

Ad A. Agendering IV-meting en Monitor, sponsorschap door Forumleden, en aanwezigheid

[bijlage FS-20211208.4A-Agendering-sponsorschap-en-aanwezigheid-Forum-leden]

Ieder Forumlid wordt gevraagd om:

1. een update te geven over het verspreiden en agenderen van de monitor Open Standaarden en IV-meting onder zijn/haar achterban;
2. een update te geven over hun sponsorschap;
3. kennis te nemen van het overzicht van de aanwezigheid.

Toelichting

1. In de bijlage treft u een overzicht aan van de huidige stand van zaken (voor zover bekend) met betrekking tot de verspreiding en agendering van de Monitor Open Standaarden en van de laatste meting informatieveiligheidsstandaarden (hierna: IV-meting).

   A. De leden van het Forum Standaardisatie hebben afgesproken dat ieder Forum-lid de Monitor Open Standaarden en IV-meting actief onder de aandacht brengt bij zijn/haar eigen achterban.

      1) Monitor 2021: voor verspreiding kunt u gebruikmaken van de laatste monitor en daarin opgenomen managementsamenvatting zoals binnenkort beschikbaar op de pagina over de Monitor Open Standaarden op de website van Forum Standaardisatie.

      2) IV-meting medio 2021: voor de verspreiding van de laatste meting van september 2021 kunt u gebruikmaken van het nieuwsbericht waarin ook wordt verwezen naar het achterliggende rapport.

   B. Daarnaast hebben de leden van het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) op 18 maart 2020 herbevestigd om de Monitor Open Standaarden en de IV-meting te agenderen in hun organisatie en hun achterban, inclusief verschillende gremia waar beleid wordt ontwikkeld met een sterke ICT-component. Tevens herbevestigden zij aan te sturen op het opnemen van eventuele 'leg uit' in het jaarverslag van hun organisatie dan wel de jaarverslagen van hun achterban.

2. De Forumleden zijn ook sponsor van een of meerdere Forum-onderwerpen. Dit is eveneens weergegeven in bijgaand overzicht.

3. Tevens wordt een overzicht gegeven van de aanwezigheid van de Forumleden sinds 13 juni 2018.

Ad B. Meting informatieveiligheidsstandaarden september 2021

[Bijlage: FS-20211208.4B-Meting-informatieveiligheidsstandaarden-sept-2021]

Het Forum Standaardisatie wordt gevraagd om:

1. De eigen organisatie en achterban aan te sporen om de verplichte moderne internetstandaarden te implementeren;
2. Aan te geven wat eventuele knelpunten zijn voor adoptie binnen de eigen organisatie en achterban.

Toelichting

Forum Standaardisatie onderzoekt ieder half jaar het gebruik van verplichte standaarden voor de beveiliging van websites en e-mail bij overheidsorganisaties, en bekijkt of deze website via IPv6 bereikbaar zijn. Bijgaand rapport toont de resultaten van de laatste meting, uitgevoerd in september 2021. Dit rapport is reeds binnen het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) verspreid. Hieronder treft u de voornaamste bevindingen:

Algemene bevindingen:

- Het gebruik van verplichte standaarden voor de beveiliging van overheidswebsites en overheidsmail toont in het afgelopen halfjaar een bescheiden groei van gemiddeld 2%.
- Ondanks gestage groei in de afgelopen jaren, zijn de streefbeeldafspraken uit 2017, 2018 en 2019 nog niet gehaald.
- Doordat afgesproken anti-phishing standaarden nog niet zijn geadopteerd, komt valse e-mail, verstuurd uit naam van (bijv. bestuurders van) overheidsorganisaties, nog steeds bij burgers, bedrijven en ambtenaren aan. Met alle risico's op ransomware, ceo-fraude, phishing en desinformatie van dien.
- In de uitzending van Zembla op 7 oktober over gebreken in de beveiliging van vitale infrastructuur, kwamen deze risico's ook naar voren. Een aantal publieke organisaties (veiligheidsregio's), en een groter percentage vitale private organisaties bleken deze beveiliging nog niet op orde te hebben: *"Een aanzienlijk deel van de vitale bedrijven en organisaties in Nederland, waaronder Veiligheidsregio's en de kerncentrale Borssele, beschermt zijn e-mail onvoldoende tegen cybercriminaliteit. Uit onderzoek van Zembla en de Internet Cleanup Foundation blijkt dat 43 van de 100 onderzochte bedrijven en organisaties de e-mailsystemen niet optimaal hebben beveiligd tegen phishing, spoofing en ransomware."*

Specifieke bevindingen:

- Om phishingmails uit naam van overheidsorganisaties (inclusief bewindspersonen) te voorkomen, moet bijna een kwart van de halfjaarlijks gemeten domeinen nog een strikt DMARC-beleid instellen.
- De e-mailvertrouwelijkheidstandaarden DNSSEC en DANE tonen een lichte terugval door toenemend gebruik van clouddiensten van voornamelijk Amerikaanse (moeder)bedrijven die deze standaarden nog niet ondersteunen. Het is cruciaal dat overheden die nog niet voldoen aan de verplichtingen, hun leverancier blijven vragen om ondersteuning van alle standaarden.
- De TLS-configuratie is bij een op de tien overheidswebsites, en bij bijna een kwart van de e-mailservers, niet toekomstvast geconfigureerd. Overheden dienen hun TLS-verbindingen te configureren op basis van de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) van het NCSC.
- De IPv6 adoptie voor websites en e-mailsystemen is het laatste halfjaar nagenoeg stilgevallen. Het groeitempo komt te kort om het streefbeeld van 100% adoptie, dat in april 2020 in het OBDO is afgesproken, te gaan halen. Mede met steun van IPO, VNG, CIO-Rijk en het Forum Standaardisatie, is het IPv6 Team Overheid NL beschikbaar voor alle overheidsorganisaties die ondersteuning willen bij de overgang.

Nadere informatie omtrent het handelingsperspectief om verdere adoptiegroei te bereiken staat op pagina's 8 en 9 van het rapport. Overheden kunnen contact opnemen met het Bureau Forum Standaardisatie voor hulp of advies bij de implementatie van de informatieveiligheidstandaarden.

Ad C. Monitor Open standaarden 2021: duiding en maatregelen

[bijlagen: FS-20211208.4C1-Duiding-en-maatregelen-Monitor-Open-standaarden-2021 en FS-20211208.4C2-Monitor-Open-standaarden-2021-v1.0]

Het Forum Standaardisatie wordt gevraagd om:

- In te stemmen met de duiding van de Monitor, inclusief het advies over de voorgestelde maatregelen, ter doorgeleiding aan het OBDO.

Toelichting

Het Forum Standaardisatie wordt met name gevraagd mee te denken, welke strategische beslissingen rond maatregelen aan het OBDO worden voorgelegd. Het gaat om maatregelen, die de adoptie bij achterblijvende overheidsorganisaties verbetert. Ook suggesties voor aanvullende maatregelen zijn welkom.

In de notitie worden de volgende 3 (concept) maatregelen genoemd.

1) Het is van belang de resultaten van de monitor open standaarden en de IV-meting in uw organisatie en achterban terug te leggen, met het oog op adoptie bij de achterblijvers[1].
   Er zijn goede ervaringen met het bespreken van de meerwaarde voor maatschappij en organisatie in departementale en koepelgremia. Het Forum Standaardisatie helpt graag bij een op maat gesneden bespreking, aan de hand van voor dat gremium relevante meetresultaten.
2) Het is daarbij goed om de verplichte open standaarden te verweven in bestaande kaders, zoals
   a. Kaders rond i-Control & ICT-kwaliteitsaspecten (CIO's)
   b. Informatiebeveiliging (BIO) en bedrijfsvoering (CISO's)
   c. Aanschaf en inkoop (gebruik de Beslisboom Open Standaarden)
   d. Architectuurkaders (zoals NORA, en Enterprise Architectuur Rijk).

   De ervaring leert dat met een dergelijke aanpak veel winst behaald kan worden. Zo heeft VWS een methode rond domeinnaamregie (op orde krijgen van web- en emaildomeinen) ontwikkeld, jaagt de Nationale Politie de adoptie van de iv-standaarden bij haar ketenpartners aan, en heeft CIO-BZK opdracht gegeven voor een BZK-breed project rond haar domeinnamen. Daarnaast heeft HIS het Forum Standaardisatie een aantal keer gevraagd om mee te denken over relevante standaarden in het Programma van Eisen bij grote verwervingen. Bij gemeenten zijn de standaarden meegenomen in de GIBIT & modelovereenkomsten. Verder leidt verweving in de BIO ertoe dat duidelijk is wat de standaarden aan informatieveiligheid bijdragen, en wordt 'stapeling van kaders' voorkomen. De toepassing van de standaarden draait dan mee in bestaande plan-&control-cyclus.

   Deze aanpak is echter nog niet overal doorgevoerd. Om die reden wordt voorgesteld de sturing op de toepassing van standaarden via CIO's en ICT-opdrachtgeverschap (de kaderstellende vraagkant) te versterken. Dat kan bijvoorbeeld door open standaarden op te nemen in toetskaders. Om dit te realiseren kan gebruik worden gemaakt en geleerd van bovengenoemde en andere bestaande goede ervaringen ('good practices').
3) Extra aandacht te genereren voor de achterblijvende adoptie van open standaarden, door een vraaggestuurd onderzoek op dat punt aan te vragen bij de Rekenkamer.

[1] Dat sluit aan bij de taak uit het instellingsbesluit OBDO art 4 lid 2.

Ad D. Monitor Open standaarden 2022: onderzoeksopzet

[bijlage: FS-20211208.4D-Opzet-Monitor-Open-standaarden-2022-dd-23-nov-2021-verkorte-versie]

Het Forum Standaardisatie wordt gevraagd om:

- In te stemmen met de aanpak en opzet van de Monitor Open standaarden 2022.

Toelichting

De Monitor Open standaarden 2022, inmiddels het 11e jaarlijkse onderzoek naar het gebruik van open standaarden van het Forum Standaardisatie, bestaat uit drie onderzoeken:
1) aanbestedingen, 2) voorzieningen, 3) gebruiksgegevens.

Hoofddoel is het meten van de mate waarin aan open standaarden wordt voldaan. Deze onderzoeken vormen op zichzelf bovendien een adoptie-bevorderende activiteit, mede omdat resultaten met verschillende betrokken organisaties besproken worden. In het verlengde daarvan omvat de opdracht nog verschillende andere activiteiten die bijdragen aan de adoptie en aan de werkzaamheden van het Forum Standaardisatie.

In de notitie staat wat de nieuwe elementen in de voorgestelde opzet zijn.

Ter kennisname

Ad E. Streefbeeldafspraak IPv6 voor duurzame bereikbaarheid

- Alle overheidswebsites en e-maildomeinen van de overheid moeten voor het einde van 2021, naast via IPv4, volledig bereikbaar zijn via de IPv6-standaard. Dat besloot het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) op 8 april 2020. Voor de laatste meetgegevens zie agendapunt "B. Meting informatieveiligheidsstandaarden september 2021".
- In samenwerking met Logius heeft BFS een nieuwsbericht over de aflopende streefbeeldafspraak voor IPv6 opgesteld en verspreid. Het nieuwsbericht werd overgenomen door onder andere Security.nl, AGconnect, Tweakers, en Executive People.
- SSC-ICT ondersteunt sinds begin november 2021 de standaard IPv6 op haar website- en e-maildiensten. Door deze mooie stap van SSC-ICT voldoen de domeinnamen van hun klanten (vooral rijksoverheden) nu aan de streefbeeldafspraak voor IPv6. Bovendien scoren deze domeinnamen nu 100% in zowel de websitetest als mailtest op Internet.nl. Het gaat om domeinnamen zoals bijvoorbeeld minszw.nl, minbzk.nl en logius.nl. De verbetering zal te zien zijn in de IV-meting die Bureau Forum Standaardisatie (BFS) begin 2022 zal uitvoeren.
- In samenwerking met IPv6 team NL Overheid heeft BFS ervoor gezorgd dat bijna 60 medewerkers van de Nederlandse overheid (o.a. van gemeente Apeldoorn, gemeente Rotterdam, VNG, DICTU, SSC-ICT en NCSC) op 11 november 2021 hebben meegedaan aan de cursus "IPv6 Fundamentals" die door RIPE NCC (uitgifte-instantie van IP-adressen in Europa en het Midden-Oosten en delen van centraal Azië) in het kader van een pilot kosteloos is aangeboden.
- Het IPv6 Team Overheid NL heeft onlangs verschillende nieuwe podcasts over IPv6 gepubliceerd (o.a. met SURF, SIDN, Bureau Forum Standaardisatie, KPN en Freedom Internet).

Ad F. Standaarden voor veiliger internet

- De Politie heeft eind oktober 2021 een brief naar gemeenten gestuurd waarin ze gemeenten dringend oproept om aan alle verplichte e-mailbeveiligingsstandaarden te voldoen. De inhoud van de brief sluit aan bij de overheidsbrede afspraken die door het OBDO op advies van het Forum Standaardisatie voor de in de brief genoemde e-mailbeveiligingsstandaarden zijn gemaakt. De uiterste implementatiedata voor deze afspraken zijn verlopen sinds eind 2019. De Politie zelf komt overigens positief terug in de IV-meting van het Forum Standaardisatie en ook in de meting van vitale organisaties die recentelijk door het tv-programma Zembla is uitgevoerd. Veiligheidsregio's komen ook terug in de Zembla-meting en scoorden voor een aanzienlijk deel "Onvoldoende". Gemeenten komen in deze meting niet terug.
- Op 23 september vond het derde overleg Betrouwbare OverheidsMail (BOM) van dit jaar plaats. Hierbij waren 29 personen aanwezig, waaronder drie gasten van ICT-dienstverlener Solvinity. ACM nam voor het eerst deel aan het overleg. Er was specifiek aandacht voor de adoptie van IPv6 en de eindsprint die nodig is om ervoor te zorgen dat alle overheidswebsites en e-maildomeinen van de overheid voor het einde van het jaar, naast IPv4, volledig bereikbaar zijn via IPv6. Verder deelden Rijkswaterstaat, SVB en Solvinity hun kennis van en ervaringen met de e-mailstandaarden. Het volgende overleg is gepland op 27 januari 2022.
- In samenwerking met Platform Internetstandaarden organiseerde BFS op 27 oktober tijdens het NCSC onderzoekssymposium "Let's do Cybersecurity Research Together" een paneldiscussie "The Power of Internet Standards" over commerciële en geopolitieke belangen in het internetstandaardisatieproces. Deelnemers waren Niels ten Oever (UvA), Marietje Schaake (Stanford Cyber Policy Center), Marco Hogewoning (RIPE NCC) en Olivier Bringer (Europese Commissie, DG CONNECT). Het gesprek werd gemodereerd door Gerben Klein Baltink (voorzitter Platform Internetstandaarden).
- Microsoft heeft BFS laten weten dat ze de DANE-standaard (t.b.v. versleuteling van e-mailtransport) ondertussen stapsgewijs voor uitgaande mail op Exchange Onine aan het activeren zijn. Eind volgend jaar staat ook DANE-ondersteuning voor inkomende mail gepland. Onlangs heeft Larissa Zegveld i.s.m. BFS een gesprek met Google Nederland gehad waarin ook de ondersteuning van DANE (opnieuw) onder de aandacht is gebracht. Dit gesprek krijgt een vervolg. In samenwerking met SIDN en Platform Internetstandaarden worden met

verschillende Nederlandse hosters gesprekken gevoerd om internet- en beveiligingsstandaarden beter te gaan ondersteunen.
- Samen met collega's van de Duitse overheid werkt BFS aan de organisatie van een volgende (virtuele) bijeenkomst van het internationale kennisnetwerk "Modern E-mail Security Standards for EU governments" (MESSEU) op 20 januari 2022.
- De Tsjechische overheid heeft onlangs e-mailbeveiligingsstandaarden, waaronder de standaarden DANE (voor versleuteld mailtransport) en DMARC (ter voorkoming van mailspoofing), verplicht gesteld voor de overheid en vitale organisaties.

Ad G. Standaarden voor inclusie en digitale toegankelijkheid

PDFs van de overheid digitaal toegankelijk online

De overheid zet veel informatie online in PDF. Deze documenten moeten sinds 2018 voldoen aan de wettelijke eisen van digitale toegankelijkheid. Het publiceren van digitaal toegankelijke PDF-bestanden blijkt een grote uitdaging. Overheidsorganisaties hebben veel behoefte aan hulpmiddelen om de digitale toegankelijkheid van PDF-bestanden te checken voordat ze online gezet worden. Daarom heeft BFS in samenwerking met Pleio een digitale toegankelijkheidschecker gebouwd voor PDF-bestanden. Met dit hulpmiddel willen wij bereiken dat een groter deel van de PDF-documenten die de overheid online zet, voldoen aan de eisen van digitale toegankelijkheid. Wij ondersteunen hiermee de initiatieven van digitoegankelijk.nl en het onderliggende beleid van minBZK.

Begin oktober ging pdfchecker.nl live. Dankzij pdfchecker.nl kan nu iedere auteur met een internetverbinding direct zelf checken hoe digitaal toegankelijk zijn of haar document is, en wat eraan verbeterd kan worden. Al in de eerste weken kwam er zowel vanuit de overheid als de private sector veel positieve feedback op dit online hulpmiddel. SIDN stelde financiering beschikbaar voor de doorontwikkeling van het tool. In het forum pdfchecker.nl is meer informatie te vinden over deze PDF checker.

Ondersteuning van standaarden voor inclusie door Microsoft

Het overgrote deel van de PDF-bestanden dat de overheid online publiceert, vindt zijn oorsprong in Microsoft Word documenten. Een goede ondersteuning van digitale toegankelijkheid bij de bron, dus bij de digitale werkplek van de ambtenaren, verhoogt de kans dat daar digitaal toegankelijke PDF-bestanden uit komen.

Via het Klantenberaad Microsoft van de overheid is BFS in gesprek met Microsoft over de ondersteuning van digitale toegankelijkheid in Officeproducten en op de digitale werkplekken van rijksambtenaren. BFS biedt Microsoft aan om kennis te delen en samen te werken in de verbetering van digitale toegankelijkheidschecks en de creatie van een PDF/UA-exportfunctie in onder andere Word. Begin 2022 moet dit tot concretere samenwerking gaan leiden.

Kennis op maat over digitale toegankelijkheid

BFS zet zich in om overheidsorganisaties gericht te helpen meer digitaal toegankelijk te publiceren. In het najaar organiseerde BFS weer een aantal webinars over digitaal toegankelijk publiceren in open documentformats. Deze webinars werden op maat verzorgd voor de organisaties aan wie ze gegeven werden. Op 28 september 2021 gaf Han Zuidweg van BFS een webinar voor de Werkgroep Digitale Toegankelijkheid van het IPO, en op 18 oktober 2021 een webinar over PDF en toegankelijkheid voor medewerkers van minIenW. Voor 2021 staat ook nog een webinar voor organisaties aangesloten op de MijnOverheid Berichtenbox gepland.

Enkele reacties op de webinar voor minIenW (uit de chatlog):

- *"Eye-opener; dwingt om eens hiermee aan de slag te gaan."*
- *"Zeer duidelijke presentatie. Strookt ook precies met hoe we het intern bij het PBL belegd hebben."*
- *"Informatief en helder, en spannend hoe wij een berg aan PDF's en Office documenten klaar gaan stomen voor het nieuwe Rijksportaal."*

Practice what you preach

Met '*practice what you preach*' wil BFS digitale toegankelijkheid en open documentstandaarden op een geloofwaardige manier stimuleren. De Accessibility Officer van BFS heeft daarom de toegankelijkheidsverklaringen van een aantal websites onder beheer van BFS geactualiseerd. Het gaat hierbij om de websites digitaaltoegankelijk.pleio.nl, bom.pleio.nl, data.forumstandaardisatie.nl, beslisboom.forumstandaardisatie.nl en magazine.forumstandaardisatie.nl. Hierbij baseerde hij zich op de toegankelijkheidsonderzoeken die in juli door Cardan Technobility werden uitgevoerd. Een aantal van deze websites heeft hierdoor een betere toegankelijkheidsscore gekregen, die in de komende maanden nog verder verbeterd zal worden.

Ad H. API's voor een betere, snellere gegevensuitwisseling en samenwerking

- Het kennisplatform API's heeft het vernieuwde hoofdstuk 'Strategie en Beleid' van 15 september tot en met 13 oktober in publieke consultatie gezet. Het hoofdstuk kent de onderdelen: visie (kern), intentieovereenkomst, praktijkvoorbeelden en een samenvatting. De KvK en de VNG hebben gereageerd op het vernieuwde hoofdstuk. KvK kwam met een aanvulling om meer een inhoudelijk koppeling te leggen met de EU-data strategie en cyber strategie. De VNG kwam met de opmerking de structuur van de strategie te verbeteren en ook goed aan te sluiten om bestaande beleidstukken rondom API's. De Werkgroep (API) Strategie en Beleid kwam bijeen op 28 oktober om deze binnengekomen reacties op de publieke consultatie te bespreken. De resultaten van de discussies uit de werkgroep zijn openbaar gedocumenteerd op Github. In de komende periode worden de reacties formeel verwerkt en besproken met de werkgroep eventueel wordt het vernieuwde hoofdstuk daarop aangepast. Na verwerking in het hoofdstuk 'Strategie en Beleid' is het streven dit te ondertekenen door partijen in de publieke sector met als doel de digitale diensten op een betere en eenvoudige wijze te laten samenwerken. Organisaties die veel ervaring hebben in het aanbieden van digitale diensten als SVB, RvIG, KvK, VNG hebben aangegeven open te staan voor een dergelijke ondertekening.

- Op 24 november organiseert het Kennisplatform API's met alle werkgroepen (API Keten Architectuur, API Design Rules, Beveiliging, Strategie en Beleid) een bijeenkomst. Op de agenda staan actualiteiten, terugkoppeling vanuit de werksessies en een paneldiscussie over de toekomst van API's. In het definitieve programma staat meer informatie.

- Het kennisplatform API's heeft op 30 september een masterclass API – De Blauwe Knop georganiseerd. De Blauwe Knop biedt mensen de mogelijkheid hun persoonlijke data te downloaden van overheidswebsites, waardoor ze meer inzicht krijgen in hun financiële situatie. Het correct en veilig omgaan met gegevens is hierbij essentieel.

- Op 2 november heeft het Ministerie van Infrastructuur en Waterstaat een masterclass API gehouden in de wereld van de TOMP API. Dit is een belangrijke API die kan bijdragen dat reizigers drempelloos kunnen reizen. Waarbij reizigers gebruikmaken van één app om al hun reizen te plannen, boeken en betalen. Deze API wordt in een internationaal werkgroep met publieke en private stakeholders ontwikkeld.

- In de Nederlandse API-strategie, is een extensie 'Geospatial' opgenomen over het uitwisselen van geo-informatie via APIs. Deze extensie is nog een concept. Om dit concept vast te stellen wil Geonovum deze extensie met experts uit het werkveld bespreken. Aanmelden voor deze subwerkgroep kan hier.

Ad I. Herkenbare en veilige digitale overheid

In de digitale communicatie tussen overheden, en burgers en ondernemers neemt het belang van informatieveiligheid toe. Moderne veiligheidsstandaarden in ICT gaan misbruik van afzenderschap tegen, zorgen voor veilige gegevensuitwisseling en zorgen ervoor dat de communicatie van overheden met burgers en ondernemers niet zomaar afgeluisterd of gemanipuleerd kan worden. Daarnaast moeten overheidswebsites en e-mails voor burgers en ondernemers duidelijk herkenbaar zijn. Uit onderzoek blijkt echter dat veel burgers moeite hebben om goed te herkennen of een website of e-mailbericht al dan niet van de overheid is. Fraudeurs maken hiervan misbruik. Bovendien ondermijnt de onduidelijkheid het vertrouwen van burgers in echte overheidswebsites/-mails.

Zodoende heeft directie Digitale Samenleving van het ministerie van BZK een aantal oplossingsrichtingen verkend om het probleem van de herkenbaarheid en veiligheid van de digitale overheid aan te pakken:

- Inrichten van een overheidsbreed internetdomein- en validatieregister. Een overheidsbreed register biedt de overheid inzicht in haar portfolio aan internetdomeinen, wat op dit moment ontbreekt, en maakt effectievere monitoring op de overheidsbrede naleving van informatieveiligheidsstandaarden mogelijk.
- Nader onderzoek naar de mogelijkheden voor invoering van een uniforme domeinnaamextensie zoals overheid.nl of gov.nl achter de bestaande domeinnaam, voor overheid.
- Uitwerking van een eenduidig domeinnaambeleid voor de gehele overheid, zodat overheidsbreed op eenduidige wijze regie kan worden gevoerd. Op dit moment wordt onderzoek gedaan door het Forum Standaardisatie over mogelijkheden om het domeinnaambeleid te actualiseren.

Register Internetdomeinen Overheid (RIO)

Naast meer inzicht in het portfolio aan internetdomeinen en de kansen die dat biedt voor kwaliteitsverbetering, biedt een overheidsbreed register van internetdomeinen burgers en ondernemers bovendien handelingsperspectief om de echtheid van overheidswebsites te controleren en kan het vertrouwen in de digitale overheid verhogen.

Dit najaar heeft directie Digitale Samenleving daarom opdracht gegeven aan UBR|KOOP, het Kennis- en Exploitatiecentrum voor Officiële Overheidspublicaties, om te starten met de ontwikkeling en bouw van een Register Internetdomeinen Overheid (RIO).

Het RIO wordt gerealiseerd in het bestaande Register van Overheidsorganisaties (ROO). Start van de bouw staat gepland voor januari 2022.

Technische impactanalyse Eenduidige Domeinnaam

Om overheidsdomeinnamen van websites herkenbaarder en veiliger te maken voor burgers en ondernemers kan een oplossing zijn het laatste deel van de domeinnaam hetzelfde te maken, bijvoorbeeld door *.overheid.nl of *.gov.nl (2nd level domein) in te voeren.

CIO Rijk heeft ICTU-opdracht gegeven een technische impactanalyse en kostenberekening uit te voeren naar een eenduidige domeinnaam. Met de impactanalyse wordt gekeken naar aspecten van security, kansen en risico's en beheerbaarheid, en de scenario's en oplossingen voor het doorvoeren van de wijzigingen. Voor de impactanalyse worden praktijkproeven uitgevoerd met websites van Forum Standaardisatie en de Rijksdienst voor Ondernemend Nederland (RVO). De resultaten van het onderzoek zullen een indicatie geven van de kosten en baten voor websites. Het rapport zal ook een beschrijving van de dienstverlening door een uitgiftepunt van domeinnamen bevatten, inclusief de relatie tot de beheerorganisatie van een website en de verdeling van verantwoordelijkheden.

De resultaten van de technische impactanalyse worden januari 2022 verwacht.

Onderzoek overheidsbreed domeinnaambeleid

De overheid worstelt al enige jaren met een wildgroei aan internetdomeinen, en huidige afspraken omtrent domeinnaambeleid lijken dit niet effectief genoeg tegen te gaan. Overheidsorganisaties hebben vaak geen overzicht van hun domeinnamen en hebben daardoor weinig grip op kwaliteitsaspecten (zoals veiligheid, herkenbaarheid, toegankelijkheid, rechtmatigheid en effectiviteit) van de domeinnamen, en de onlinemiddelen die daarachter zitten.

Beleidsmakers zijn zich er steeds meer van bewust dat onvoldoende beheersing van het domeinportfolio significante risico's met zich meebrengt. Om de risico's te beperken is het van belang dat de overheid meer regie voert op het gebruik van internetdomeinen. Staatssecretaris Knops schreef op 18 maart 2021 aan de Kamer: "Overheidsbreed wordt de komende jaren gewerkt aan verankering van afspraken op het gebied van domeinnaambeleid via bijvoorbeeld de BIO en het Forum Standaardisatie."

In voorbereiding op deze toezegging aan de Tweede Kamer voert Bureau Forum Standaardisatie in opdracht van directie Digitale Samenleving van het ministerie van BZK een onderzoek uit naar de regie op internetdomeinen binnen de overheid. Dit onderzoek richt zich op de vraag, 'Hoe zou toekomstig overheidsbreed domeinnaambeleid er idealiter uitzien?' en leidt tot een adviesrapport dat kan fungeren als basis voor overheidsbreed domeinnaambeleid. Met effectief beleid voor het gebruik van internetdomeinen kan de overheid beter sturen op de kwaliteit en het beheer van internetdomeinnamen en achterliggende onlinemiddelen.

Het onderzoek richt zich op:

1) Het inzichtelijk krijgen van de stand van zaken van domeinnaambeheer binnen de overheid, en de behoeften en belangen van overheden evalueren
2) Het evalueren hoe overheden beter aangestuurd kunnen worden om overzicht en inzicht te verkrijgen in hun domeinnamen en verantwoordelijkheid te nemen voorgoed domeinnaambeheer
3) Het adviseren over het opstellen van richtlijnen, randvoorwaarden en/of kaders voor toepassing van domeinnaambeleid in de praktijk
4) Analyseren hoe de adoptiegraad van de pas-toe-of-leg-uit-lijst van het Forum Standaardisatie en andere verplichte richtlijnen verhoogd kan worden
5) Het adviseren over opties en oplossingsrichtingen om wildgroei te beperken en kwaliteitsaspecten als veiligheid en herkenbaarheid te verbeteren

Het onderzoek is opgedeeld in twee consultatiefases met stakeholders en andere relevante betrokkenen. In de eerste fase wordt het huidige beleid geëvalueerd, waarbij knelpunten in de toepassing van dit beleid in de praktijk in kaart worden gebracht. In de tweede fase worden oplossingsrichtingen verkend. De analyse van de knelpunten en oplossingsrichtingen zal uitmonden in een beleidsadvies.

De eerste consultatiefase is begin november begonnen. De eerste interviews zijn gevoerd met deskundigen van onder meer BZK, het NCSC, het Waterschapshuis, en SIDN. Naar verwachting wordt het onderzoek eind februari afgerond en zal het adviesrapport worden aangeboden aan directie Digitale Samenleving.

Ad J. Eenduidige dienstverlening

MCU, spoor 1: 'toekomstbestendige dienstverlening'

Op 11 september 2020 is het rapport "Werk aan uitvoering fase II" naar de Tweede Kamer gestuurd. Dit rapport is opgesteld door ABDTOPConsult. In het rapport zijn voorstellen gedaan om de dienstverlening aan burgers, instellingen en bedrijven te versterken en de wendbaarheid, continuïteit en toekomstbestendigheid van de uitvoering te vergroten. De zes handelingsperspectieven uit "Werk aan uitvoering (WAU)" is uitgewerkt door bestuurlijke trekkers per thema.

Voor het handelingsperspectief 'toekomstbestendige dienstverlening' zijn dit de heren Sibma (SVB), Van Hout (gemeente Nijmegen), en Den Hollander (BZK). Deze bestuurlijke trekkers hebben de opdracht om het handelingsperspectief uit WAU de visie en de daarbij behorende oplossingstappen om te zetten in een werkagenda en plan van aanpak: wat heeft nu prioriteit, wat kan snel worden opgepakt, wat op langere termijn, hoe gaan we het uitvoeren en wat moet op de formatietafel landen? De parlementaire druk loopt op en om tijdverlies te voorkomen laat de inspiratiegroep (Ministeriele Commissie Uitvoering, MCU) de visie niet vaststellen maar als richtsnoer gebruiken.

Ook Forum Standaardisatie draagt met haar specifieke expertise bij aan maatwerk voor dienstverleningsprincipes (spoor 1: loketfunctie). Op de laatste bijeenkomst 13 oktober jl. sluit onze beoogde werkconferentie 'Een werkende uitkomst voor werklozen!' naadloos aan op de behoefte van MCU-praktijkvoorbeelden op te halen voor plan van aanpak. Alle deelnemers zijn dan ook van harte uitgenodigd.

Luister ook naar de podcast van Simon Sibma (SvB).

Werkconferentie: "Een werkende uitkomst voor werklozen!"

Met de Belastingdienst, de Nationale politie, het Kadaster, Divosa en het programma mens Centraal is de invulling bepaald van het programma van de werkconferentie "Een werkbare uitkomst voor werklozen". De conferentie is vanwege corona verplaatst naar dinsdag 5 april 2022.

Gesteld criterium is dat de bijeenkomst fysiek kan plaatsvinden met 60 personen. Dit om een echte dialoog te kunnen voeren over de kansen die de gepresenteerde praktijkcases bieden. Het betreft 3 cases waarin semantiek en standaardisatie centraal staat:

- Belastingdienst - Wetsanalyse voor wetsuitvoering met ICT (Mariëtte Lokin)
- Nationale Politie - Het hoe en waarom van semantiek in strijd tegen strafbare feiten (Tjeerd Schoemaker)
- Kadaster – Zorgeloos vastgoed; stressvrij kopen met 'slimme' contracten (Arjen Santema)

Voor deelname zijn gericht mensen aangeschreven op bestuurlijk en strategisch niveau bij o.a. VNG, Divosa, SZW, BZK, BD, UWV, DUO, SVB.