Rapport

Monitor Open standaarden 2021

Onderzoek naar het gebruik van open standaarden van de ‘pas toe of leg uit’-lijst van het Forum Standaardisatie: bij aanbestedingen, in voorzieningen en per standaard

Van Jaap Korpel

Versie Versie 1.1

Datum 15-11-2021

Inhoudsopgave

Managementsamenvatting Monitor Open standaarden 2021

Iedere overheidsorganisatie is er zelf verantwoordelijk voor, dat haar ICT gebruik maakt van de open standaarden van de 'pas toe of leg uit'-lijst van het Forum Standaardisatie – overal waar deze van toepassing zijn.

ICTU rapporteert jaarlijks in hoeverre deze standaarden worden toegepast door ministeries, uitvoeringsorganisaties en ZBO's, gemeenten, provincies en waterschappen. De Monitor Open standaarden, in opdracht van het Forum Standaardisatie, wordt gebaseerd op drie deelonderzoeken:

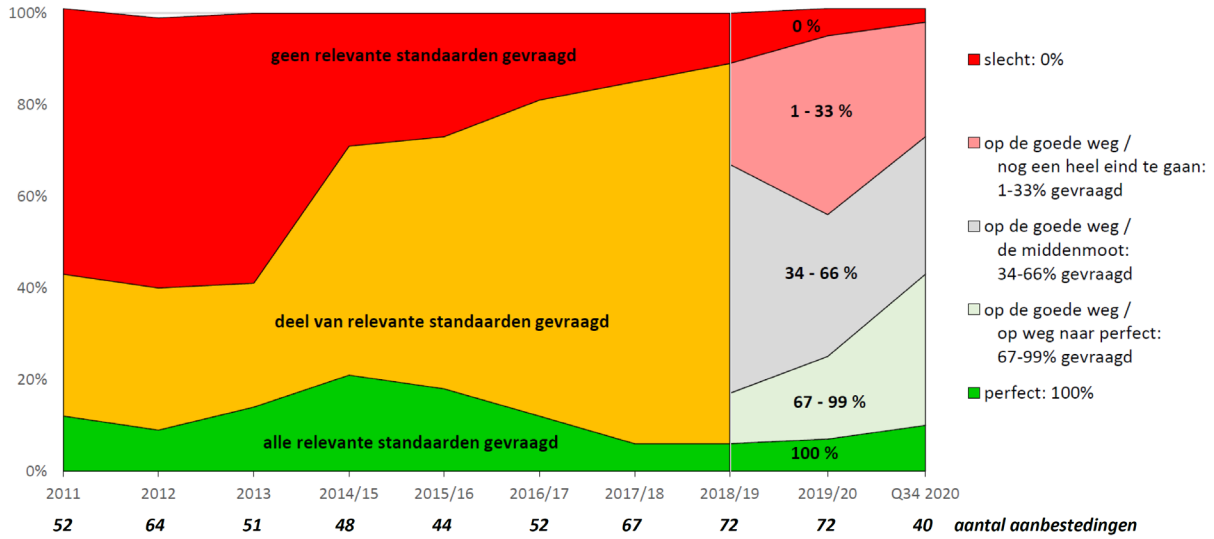
- onderzoek van aanbestedingen (in juli t/m december 2020): is daarbij om de relevante open standaarden gevraagd, en indien niet: is dat in het jaarverslag correct uitgelegd?; het glas is halfvol: om 54% van de relevante standaarden is gevraagd; dat percentage neemt langzaam toe en het is de helft van een steeds groeiend aantal (zie hoofdstuk 3);
- onderzoek van de toepassing van open standaarden bij voorzieningen (zomer van 2021); die is inmiddels op een heel redelijk niveau: aan 84% van de standaarden wordt voldaan, of deels voldaan, of daar wordt binnenkort aan voldaan (zie hoofdstuk 4);
- onderzoek naar gebruiksgegevens van een aantal open standaarden (zomer 2021); voor veel standaarden zijn geen harde gegevens beschikbaar, de meeste standaarden waarover wèl cijfers bekend zijn worden door veel overheden gebruikt (zie hoofdstuk 5).

Open standaarden zijn al 12 jaar de norm: voor de (semi-)publieke sector geldt sinds 2009 een 'pas toe of leg uit'-regime. Het open standaardenbeleid vergroot de interoperabiliteit en de leveranciersonafhankelijkheid van de publieke organisaties. Het maakt een kwalitatief hoogwaardige, kostenefficiënte en veilige informatie-uitwisseling mogelijk.

Aanbestedingen

Vanaf de volgende monitor zullen steeds aanbestedingen per kalenderjaar onderzocht worden (tot nu toe: van juli t/m juni). Daarom zijn dit jaar eenmalig alleen aanbestedingen uit tweede helft van 2020 onderzocht (de eerste helft is al voor de vorige monitor beoordeeld). Dat waren er dit keer 40 in totaal, waarvan 20 Rijksoverheid en 20 van mede-overheden.

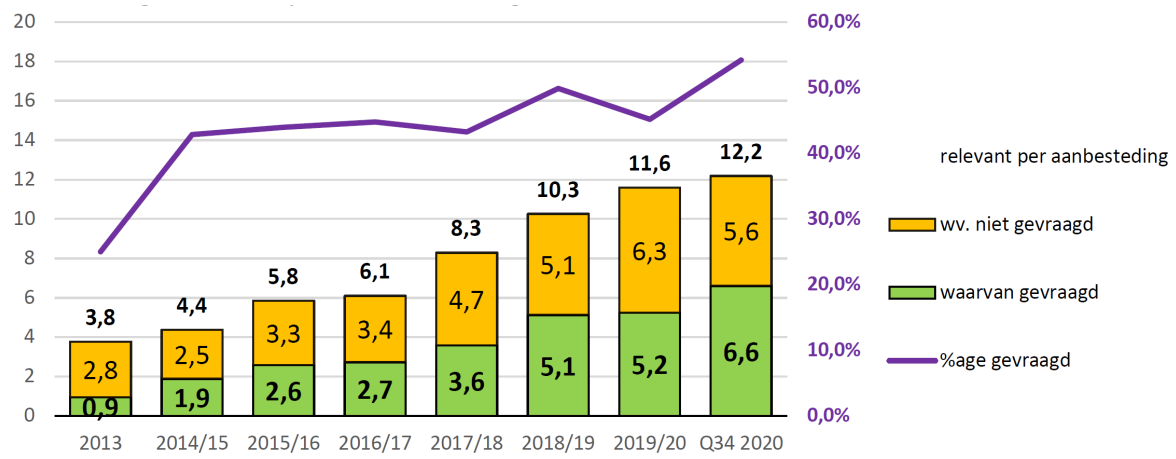
'Pas toe' bij aanbestedingen, 2011 – 2e helft 2020



Bij deze 40 aanbestedingen was 487 keer een standaard relevant, en 264 keer is daar ook om gevraagd: dat is 54 % (was vorig jaar 45 %). Goed nieuws is ook: vergeleken met vorig jaar zijn er nòg iets minder slechte en iets meer goede aanbestedingen. Bovendien waren er in de grote middencategorie – waar slechts om een deel van de standaarden is gevraagd – meer aanbestedingen 'op weg naar perfect' (lichtgroen, >66% van de standaarden gevraagd) en minder 'nog een lange weg te gaan' (lichtrood, <34%).

Daar komt nog bij, dat het gemiddelde aantal relevante standaarden per aanbesteding opnieuw verder is gegroeid: inmiddels 12,2 per aanbesteding (ruim 3 keer zoveel als in 2013). Dit jaar werd zoals gezegd om 54% daarvan gevraagd, dat percentage fluctueert maar neemt geleidelijk toe. Het is bovendien een stijgend percentage van een toenemend aantal.

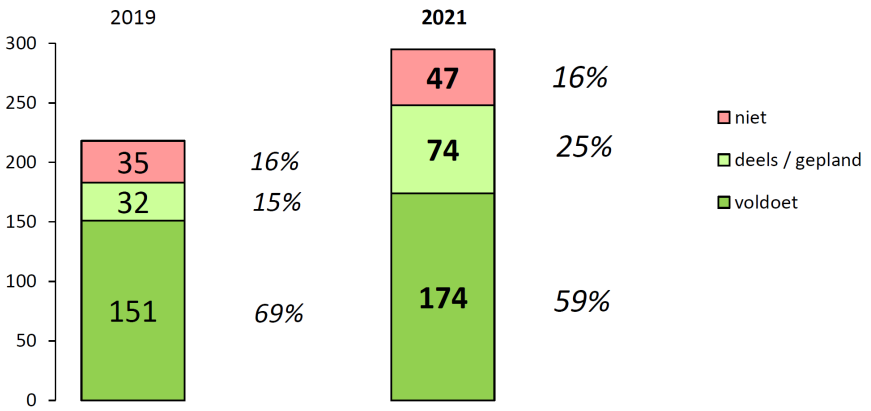
Aantal relevant standaarden, gemiddeld per aanbesteding



Voorzieningen

Sinds de vorige monitor (van 2020) onderzoeken wij jaarlijks om en om twee verschillende groepen voorzieningen. Vorig jaar: gegevensuitwisseling en communicatie met burgers en bedrijven (17 voorzieningen). Dit jaar: voorzieningen relevant voor de gegevensuitwisseling tussen overheden en de onderliggende infrastructuur (19 voorzieningen).

Dit jaar onderzocht: 19 voorzieningen
Relevant voor gegevensuitwisseling tussen overheden en onderliggende infrastructuur



Dit jaar bleek in totaal 295 keer een standaard relevant voor een voorziening (gemiddeld 15,5 keer per voorziening, vorig jaar 12,3). Dat aantal nam onder meer toe, doordat er enkele nieuwe standaarden op de lijst staan, en doordat dit jaar wèl op Digitoegankelijk getoetst is. De dit jaar onderzochte 19 voorzieningen blijken voor een groot deel te voldoen aan de voor hen relevante open standaarden. In 59% van de gevallen voldoet de voorziening daaraan, en 25% voldoet de voorziening er deels aan of heeft concrete plannen daarvoor. In 16 % van de gevallen voldoet een voorziening niet aan een relevante standaard (47 gevallen).

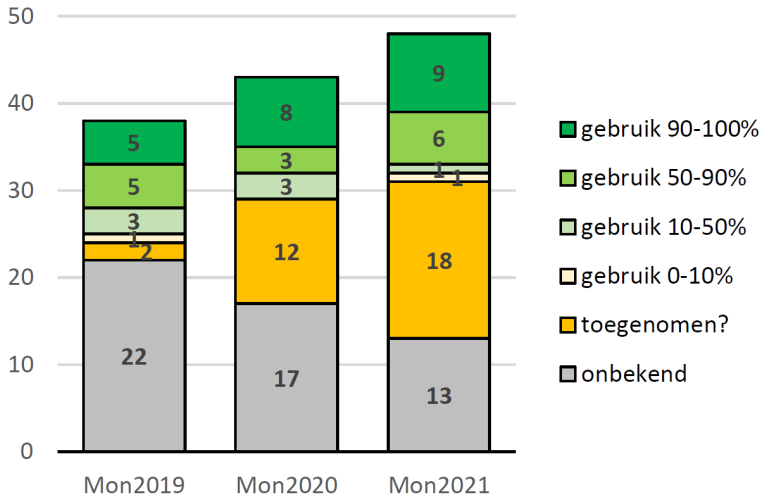
Vooral de vijftien standaarden uit het domein Internet & beveiliging waren vaak relevant voor een voorziening (samen goed voor 64 %), gevolgd door de zes standaarden uit het domein Document & (web)content (16 %) en de drie Stelselstandaarden (10 %).

Gebruiksgegevens

Gebruiksgegevens geven inzicht in het daadwerkelijke, overheidsbrede gebruik van de open standaarden. Dergelijke gegevens zijn echter niet in alle gevallen eenvoudig te verzamelen. Over meer dan de helft van de open standaarden zijn geen gebruiksgegevens beschikbaar.

Over de meeste standaarden uit het domein Internet & beveiliging en over enkele andere standaarden zijn wèl cijfers beschikbaar. Veel van deze standaarden worden door veel overheden gebruikt: voor 9 standaarden is het gebruik meer dan 90% en voor 6 standaarden is het 50 tot 90%. Daarnaast is voor meer standaarden waarover geen harde gegevens beschikbaar zijn, wel de indruk dat het gebruik toeneemt (in 2019 nog 2, inmiddels 18).

Gebruiksgegevens over open standaarden (aantallen)



1. Bevindingen van de Monitor Open standaarden 2021 – in het kort

Het open standaardenbeleid is gericht op het vergroten van de interoperabiliteit en van de leveranciers-onafhankelijkheid voor de publieke sector. Daardoor wordt een kwalitatief hoogwaardige, kostenefficiënte en veilige informatie-uitwisseling mogelijk gemaakt.

Al ruim tien jaar zijn open standaarden de norm: voor de gehele (semi-)publieke sector geldt sinds 2009 een 'pas toe of leg uit'-regime. Overheden moeten gebruik maken van de open standaarden van de 'pas toe of leg uit'-lijst van het Forum Standaardisatie – indien deze van toepassing zijn. Dat wordt onder meer voorgeschreven in de *Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten* (rijksoverheid en uitvoeringsorganisaties) en de verplichting geldt ook voor mede-overheden (gemeenten, provincies en waterschappen).

1.1. Waarom open standaarden – beleidsachtergrond en juridisch kader (zie H2)

Open standaarden voor 'pas toe of leg uit'

Er zijn veel open standaarden en een groot deel daarvan wordt ook in de publieke sector breed toegepast. Naast de 'pas toe of leg uit'-lijst beheert het Forum Standaardisatie ook een lijst met aanbevolen open standaarden. Op deze lijst staan standaarden die gangbaar zijn of die pril zijn en veelbelovend. Dit onderzoek beperkt zich tot de 'pas toe of leg uit'-lijst.

Voor een aantal open standaarden is een extra stimulans wenselijk, maar is een wettelijke verplichting nog een brug te ver. Het gaat daarbij om open standaarden die sterk bijdragen aan de interoperabiliteit en de leveranciers-onafhankelijkheid voor de publieke sector en waarvoor breed draagvlak bestaat, maar die op dit moment nog niet breed geadopteerd zijn. Deze worden, na een zorgvuldige en open toetsingsprocedure, door het Forum Standaardisatie op de lijst voor 'pas toe of leg uit' geplaatst. Op deze open standaarden (medio 2021 waren dit er 44) is het 'pas toe of leg uit'-regime van toepassing. Meer informatie over de beleidscontext en het juridisch kader staat in hoofdstuk 2.

1.2. Over de Monitor Open standaarden 2021 (zie H2)

ICTU verzorgt in opdracht van het Forum Standaardisatie jaarlijks een rapportage die inzicht geeft in het gebruik van de open standaarden op de lijst voor 'pas toe of leg uit': in hoeverre worden deze standaarden toegepast? Door ministeries, uitvoeringsorganisaties, gemeenten, provincies en waterschappen en daarbuiten?

In deze rapportage worden gegevens gepresenteerd afkomstig uit een drietal bronnen:

- onderzoek van aanbestedingen in de periode juli t/m december 2020,
- onderzoek van de toepassing van open standaarden bij overheidsbrede voorzieningen (situatie in de zomer van 2021),
- onderzoek naar gebruiksgegevens van een aantal open standaarden (zomer 2021).

In het navolgende worden de voornaamste bevindingen per deelonderzoek samengevat. De positieve bevindingen hebben een groen blokje ('goed nieuws'), de minder positieve een oranje ('minder goed').

1.3. Open standaarden bij aanbestedingen (zie H3)

Overheden moeten bij de aanschaf van ICT voor € 50.000 of meer kiezen voor een dienst of product dat voldoet aan alle relevante open standaarden van de lijst ('pas toe'). Doen zij dat niet dan moeten zij daarover verantwoording afleggen in hun jaarverslag ('leg uit'). Doen zij dat ook in de praktijk?

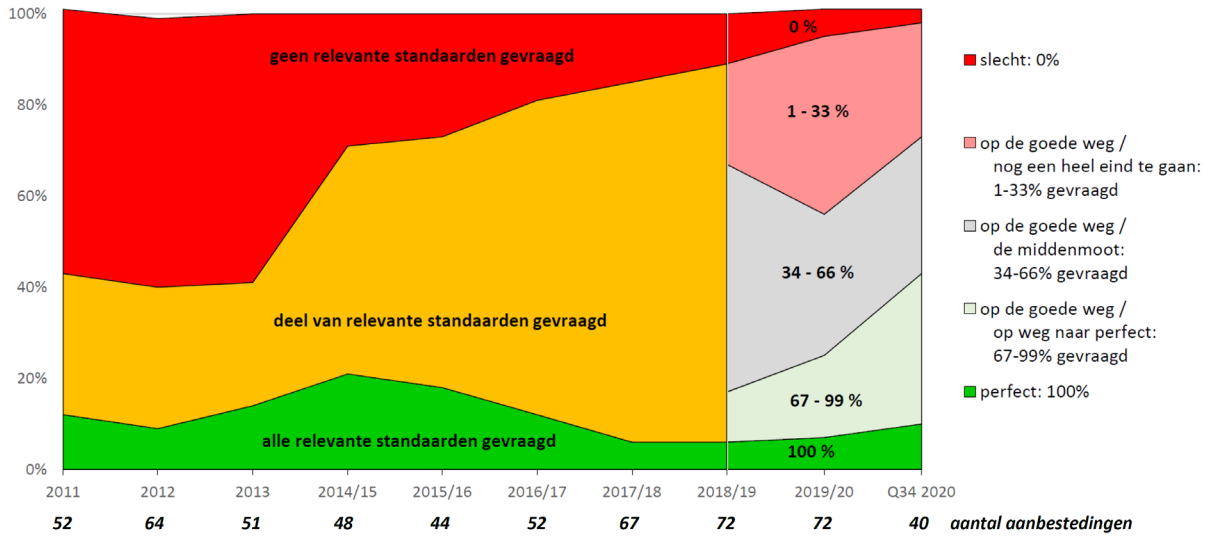
'Pas toe' bij aanbestedingen

We gaan er van uit, dat expliciet vragen om een standaard een voorwaarde is om te kunnen kiezen voor een dienst of product dat aan die standaard voldoet. Voor de monitor wordt daarom jaarlijks een groot aantal aanbestedingen hierop onderzocht. Dit keer zijn 20 aanbestedingen van de rijksoverheid en uitvoeringsorganisaties en 20 aanbestedingen van mede-overheden onderzocht, in totaal 40 aanbestedingen. Met ingang van de volgende monitor zullen telkens de aanbestedingen van een volledig kalenderjaar worden onderzocht (en niet meer voor een periode van juli tot en met juni), daarom onderzochten wij dit jaar voor één keer alleen aanbestedingen uit de periode juli tot en met december 2020. De resultaten worden beschreven in hoofdstuk 3.

Bij 10% van de 40 onderzochte aanbestedingen is gevraagd om alle relevante open standaarden (vorig jaar 7%). Het percentage aanbestedingen waarbij om een deel van de open standaarden is gevraagd – de grote middencategorie – is gelijk aan vorig jaar: 88%. Het percentage aanbestedingen waarbij niet om een open standaard is gevraagd, is verder teruggelopen van 6% naar 3%. En daar zijn net als vorig jaar geen aanbestedingen bij die strijdig zijn met het standaardenbeleid.

Deden de mede-overheden het vorig jaar beter dan de Rijksoverheid, dit jaar is het beeld omgekeerd: bij 50% van de aanbestedingen vroeg de Rijksoverheid om alle relevante standaarden of om tenminste tweederde daarvan (mede-overheden: 40%). De mede-overheden vroegen bij 65% van de aanbestedingen om geen enkele of om minder dan een derde van de relevante standaarden (Rijksoverheid: 20%).

'Pas toe' bij aanbestedingen, 2011 – 2e helft 2020



Het overall beeld voor aanbestedingen is positief, maar we zijn pas halverwege: veruit de meeste aanbestedingen (88%) vallen in de middengroep (niet heel goed, niet slecht). En van alle keren dat een open standaard voor een aanbesteding relevant was, werd daar in 54% van de gevallen om gevraagd.

De belangrijkste bevindingen uit het aanbestedingen-onderzoek (zie hoofdstuk 3) zijn:

goed nieuws	Bij 4 aanbestedingen (10%, vorig jaar 7%) is om alle relevante standaarden gevraagd. Het gaat om aanbestedingen van de Ministeries van BZK, Defensie en Financiën (Belastingdienst), en gemeenschappelijk gemeentelijk inkoopbureau Bizob (namens de Veiligheidsregio Brabant -Zuidoost).
goed nieuws	Daarnaast werd bij 35 aanbestedingen (88%) om een deel van de relevante open standaarden gevraagd. Dat is evenveel als vorig jaar (toen ook: 88%).
goed nieuws	Bij 1 van de 40 aanbestedingen (dat is 3%, vorig jaar was het 6%) is om geen enkele relevante standaard gevraagd.
goed nieuws	Dit jaar waren er geen aanbestedingen strijdig met het open standaardenbeleid.
goed nieuws	Van de 487 keer dat een open standaard voor een aanbesteding relevant was werd daar in 54 % van de gevallen door de aanbesteder om gevraagd. Vorig jaar lag dit percentage nog op 45%, en er tekent zich een heel geleidelijk stijgende trend af.
goed nieuws	Het gemiddeld aantal relevante standaarden per aanbesteding steeg van 4,4 (2015) tot 12,2 in 2021. Er wordt dus elk jaar gevraagd om een iets groter percentage van een gestaag groeiend aantal relevante standaarden.
goed nieuws	Sommige standaarden (vooral NEN-ISO/IEC 27001 en 27002, HTTPS & HSTS en TLS) zijn veel vaker (88% tot 98%) relevant bij een aanbesteding dan andere. Deze zelfde vier standaarden worden bovendien – àls zij relevant zijn – het vaakst ook daadwerkelijk gevraagd (variërend van 71% tot 89%). Nog 6 andere IV-standaarden waren ook vaak relevant (75% tot 83%), maar deze werden minder vaak gevraagd.
goed nieuws	Dit jaar werden ook enkele andere standaarden, àls ze relevant waren, redelijk vaak gevraagd: PDF (86%), StUF (85%) en NLCIUS (100%, maar van 4x relevant).
minder goed	IPv4 & IPv6 was voor 83% van de aanbestedingen relevant, maar er werd er slechts in 18% van die gevallen om de standaard gevraagd. Terwijl in het OBDO (onder andere) voor IPv4 & IPv6 'streefbeeldafspraken' zijn gemaakt (zie par. 5.2).

Een aantal aanbestedingen onderscheidde zich in positieve zin (zie ook paragraaf 3.2.2):

- Ministerie van BZK (vervangen Rijksportaal): voldoet aan alle 15 relevante open standaarden, en ruime aandacht voor open standaardenbeleid.
- Ministerie van Financiën (website voor de Rijksacademie): voldoet aan 7 van de 11 relevante open standaarden, en duidelijke aandacht voor open standaardenbeleid.
- Gemeente Apeldoorn (Integratievoorziening en implementatie van koppelingen): voldoet aan 13 van de 15 relevante open standaarden.
- Gemeente Purmerend (eHRM-systeem als SAAS-oplossing): voldoet aan 14 van de 18 relevante open standaarden.
- Regio Rivierenland (datadistributie-applicatie): voldoet aan 10 van de 13 relevante open standaarden.
- Gemeente Waddinxveen (burgerzaken-applicatie): voldoet aan 12 van de 16 relevante open standaarden.
- Daarnaast werd bij 3 andere aanbestedingen om alle relevante standaarden gevraagd, maar daarbij waren alleen de beide ISO-standaarden relevant: Ministerie van Defensie, Belastingdienst en Bizob / Veiligheidsregio Brabant Zuidoost.

‘Leg uit’ in jaarverslagen

Een organisatie die bij een aanbesteding niet vraagt om een open standaard die wel relevant is, moet daar een legitieme (zwaarwegende) reden voor hebben en daarvan verantwoording afleggen in het jaarverslag. Dit kan inzichten opleveren waarom het gebruik van sommige standaarden achterwege blijft. ‘Leg uit’ is dus verplicht, maar elk jaar opnieuw blijkt dat geen enkele overheidsorganisatie dat doet. Wel leggen sommige organisaties algemene verklaringen af over het gebruik van open standaarden. Maar dit is niet wat oorspronkelijk met ‘pas toe of leg uit’ werd bedoeld.

Voor de onderzochte aanbestedingen uit het 3e en 4e kwartaal van 2020 is nagegaan of er sprake is geweest van een geldige ‘Leg uit’. Voor 36 van de 40 aanbestedingen was 'Leg uit' vereist, omdat hierbij om één of meer relevante open standaarden niet gevraagd werd.

minder goed	Van expliciete 'Leg uit' voor met name genoemde aanbestedingen was in de jaarverslagen van de betreffende overheidsorganisaties (waaronder 7 ministeries) geen sprake: nergens wordt een concrete afwijking van de 'pas toe of leg uit'-lijst genoemd, laat staan verantwoord.
minder goed	Bij 36 aanbestedingen was ‘Leg uit’ noodzakelijk. Bij 19% hiervan (vorig jaar: 18%) was sprake van een beperkte verantwoording: 7 van de 12 ministeries hebben een algemene alinea over 'pas toe of leg uit' opgenomen in het jaarverslag. Bij de overige 81% was geen sprake van enige vorm van ’Leg uit’ (vorig jaar 82%).

Sinds enkele jaren informeren wij aanbesteders over de beoordeling van hun aanbesteding en interviewen wij bovendien enkele van hen. Dat leidt soms nog tot een (beperkte) aanpassing van de beoordeling. En, hoewel dit geen alternatief is voor ‘Leg Uit’, blijkt het wel in een behoefte te voorzien en bovendien interessante inzichten op te leveren.

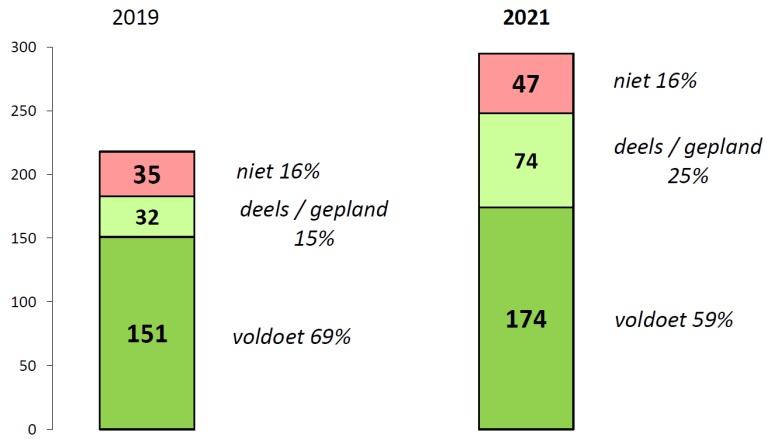
1.4. Toepassing van open standaarden via voorzieningen (zie H4)

Voor onderdelen van hun informatiesystemen maken overheden gebruik van verschillende overheidsbrede voorzieningen, bijvoorbeeld van de Basisinfrastructuur (voorheen GDI). Hoe meer daarin de relevante open standaarden worden toegepast, hoe meer dat leidt tot een breed gebruik van die open standaarden elders in de informatiesystemen. Passen de ontwikkelaars en beheerders van deze voorzieningen alle relevante open standaarden toe?

Met ingang van 2020 onderzoeken we het ene jaar 17 voorzieningen die direct raken aan de communicatie en gegevensuitwisseling met burgers en bedrijven. Het andere jaar (dit jaar) onderzoeken we de 19 voorzieningen die relevant zijn voor de gegevensuitwisseling en communicatie tussen overheden en/of voor de onderliggende infrastructuur, voorzieningen dus waarbij interoperabiliteit cruciaal is.

De dit jaar onderzochte voorzieningen blijken voor een groot deel te voldoen aan de relevante open standaarden. Er waren in totaal 295 gevallen waarbij een open standaard voor een voorziening relevant was. Het percentage ‘voldoet’ is afgenomen van 69% tot 59%. Het aantal gevallen waarin de voorziening deels aan de standaard voldoet of daarvoor concrete plannen heeft is juist gestegen van 15% vorig jaar naar 25% dit jaar. Samen met ‘voldoet’ is dat dit jaar dus net als vorig jaar 84%.

Dit jaar onderzocht: 19 voorzieningen
Relevant voor gegevensuitwisseling tussen overheden en onderliggende infrastructuur



De belangrijkste bevindingen uit het voorzieningen-onderzoek (zie hoofdstuk 4) zijn:

goed nieuws	Voor veel voorzieningen is een flink aantal open standaarden relevant: voor de dit jaar onderzochte voorzieningen gemiddeld 15,5 standaarden per voorziening. Van de 44 standaarden op de lijst voor 'pas toe of leg uit' zijn er 30 relevant voor één of meer van de dit jaar onderzochte voorzieningen.
goed nieuws	Voor 12 van deze 30 standaarden geldt dat minstens 80% van de onderzochte voorzieningen aan die standaard – indien relevant – voldoet. Van deze standaarden vallen er 6 in het domein 'Internet & beveiliging'. De andere 6 zijn verdeeld over vijf van de negen andere domeinen: Document & (web)content, REST API's, E-facturatie & administratie, Stelselstandaarden en Water & Bodem.
minder goed	Vijf standaarden scoren relatief laag: van de voorzieningen waarvoor deze relevant zijn voldoet er geen enkele (volledig) aan Digitoegankelijk en aan NLCIUS en de nieuwe standaard NL GOV. Daarnaast voldoet slechts 18% van de voorzieningen aan REST-API Design Rules, 22% aan SKOS en 28% aan OWMS.
goed nieuws	De voorzieningen voldoen aan redelijk veel standaarden: de 19 onderzochte voorzieningen voldoen aan 59% van de voor hen relevante standaarden.
minder goed	Vergeleken met twee jaar geleden is het percentage 'voldoet' afgenomen van 69% tot 59%. Het aantal gevallen waarin de voorziening deels aan de standaard voldoet of daarvoor concrete plannen heeft is wel gestegen van 15% vorig jaar naar 25% dit jaar. Samen met 'voldoet' is dat dit jaar dus net als vorig jaar 84%.
goed nieuws	Twee voorzieningen voldoen geheel of gedeeltelijk aan alle relevante open standaarden en/of hebben concrete plannen om daaraan op korte termijn te voldoen: Stelselcatalogus en Diginetwerk.

Opvallend is, dat vooral standaarden uit het domein Internet & Beveiliging vaak relevant zijn (64% van alle gevallen). De domeinen Document & Webcontent (16%) en Stelselstandaarden (10%) volgen op grote afstand. De 20 standaarden uit de zes andere domeinen zijn zelden relevant (samen slechts 10%).

Verschillende voorzieningen onderscheiden zich dit jaar in positieve zin:

- Zowel Stelselcatalogus (10 relevante standaarden) als Diginetwerk (4 standaarden relevant) voldoen dit jaar geheel of gedeeltelijk aan alle relevante open standaarden en/of hebben concrete plannen om daaraan op korte termijn te voldoen.

- Verschillende voorzieningen voldoen 'bijna' aan alle standaarden, doordat zij aan een groot deel voldoen en aan de meeste andere deels voldoen, of dat gepland hebben. Bijvoorbeeld de BRO (Basisregistratie Ondergrond) en de Digitale Werkomgeving Rijk.

1.5. Gebruiksgegevens van een aantal open standaarden (zie H5)

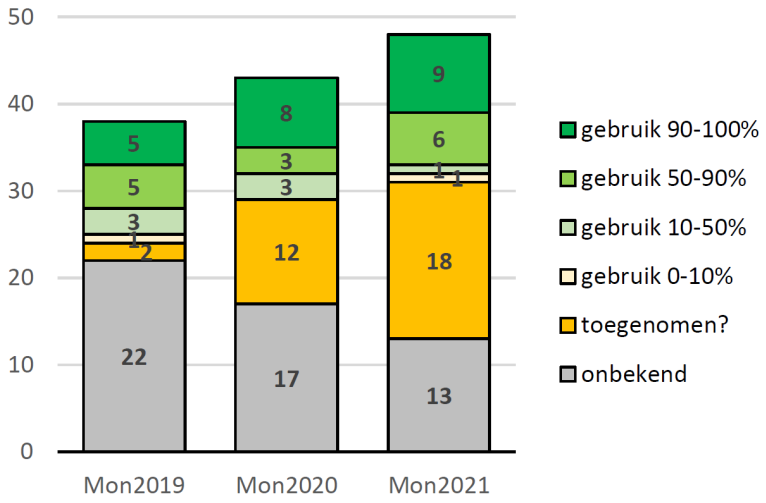
Het uiteindelijk doel van het open standaardenbeleid is een brede adoptie van de open standaarden van de lijst voor 'pas toe of leg uit' - daar waar deze van toepassing zijn - door alle overheden en andere organisaties in de publieke sector. Het is daarom interessant om te weten in welke mate deze open standaarden daadwerkelijk worden gebruikt.

Dergelijke gebruiksgegevens zijn niet in alle gevallen eenvoudig te verzamelen. Dat is door de accountmanagers van het Bureau Forum Standaardisatie gedaan, in de zomer van 2021, met de volgende uitkomsten:

minder goed	Over meer dan de helft van de open standaarden zijn geen gebruiksgegevens beschikbaar. Dat is in sommige gevallen begrijpelijk, maar in de andere gevallen lijken beheerorganisaties en/of initiatiefnemers daarin niet echt geïnteresseerd.
goed nieuws	Over de meeste standaarden uit het domein Internet & beveiliging zijn cijfers beschikbaar. Veel van deze standaarden worden door veel overheden gebruikt.
minder goed	Voor IPv4&IPv6 is nog een lange weg te gaan, terwijl het OBDO-streefbeeld is dat 100% adoptie eind 2021 bereikt moet zijn. Voor overheidswebsites steeg de toepassing van 64% in maart 2020 naar 79% in maart 2021, en voor overheidsemail van 17% in maart 2020 naar 40% in maart 2021.
goed nieuws	Voor verschillende standaarden uit het domein Document & (web)content is dit jaar een begin gemaakt met een nulmeting van gebruiksgegevens.

Veel van de standaarden waarover wèl gegevens beschikbaar zijn, worden door veel overheden gebruikt: voor 9 standaarden is het gebruik meer dan 90% en voor 6 standaarden is het 50 tot 90%. Daarnaast is voor meer standaarden waarover geen harde gegevens beschikbaar zijn, wel de indruk dat het gebruik toeneemt (in 2019 nog 2, inmiddels 18).

Gebruiksgegevens over open standaarden (aantallen)



Halfjaarlijkse meting Internetveiligheidsstandaarden (zie ook Bijlage B6)

Uit de *'Meting Informatieveiligheidstandaarden overheid - maart 2021'* blijkt dat het streefbeeld voor eind 2019 op het moment van de meting – ruim een jaar later – nog niet volledig was gerealiseerd. Wel is de toepassing van een aantal standaarden gegroeid.

goed nieuws	Van de webstandaarden wordt TLS het meest toegepast (100%), gevolgd door HTTPS (redirect) en DNSSEC (98%) en HSTS (92%). HSTS en TLS conform NCSC scoren lager (beide 83%).
goed nieuws	Van de mailstandaarden voor anti-phishing wordt SPF (99%) het meest toegepast, gevolgd door DKIM (96%), DMARC (95%) en SPF Policy (94%). En STARTTLS wordt van de mailstandaarden voor vertrouwelijkheid het meest toegepast (100%).
minder goed	De andere mailstandaarden worden minder vaak gebruikt: DMARC Policy (74%) voor anti-phishing, en STARTTLS cf. NCSC (69%), DNSSEC MX (64%) en DANE (55%) voor vertrouwelijkheid. Ook voor deze standaarden is de deadline voor het OBDO-streefbeeld reeds verstreken.
goed nieuws	De bereikbaarheid via IPv6 is voor overheidswebsites gegroeid van 64% in maart 2020 naar 79% in maart 2021. Voor overheidsemail is die wel gegroeid (van 17% in maart 2020 naar 40% in maart 2021), maar nog op een laag niveau.
minder goed	Het door het OBDO vastgestelde streefbeeld (100% van alle overheidswebsites en -email bereikbaar, uiterlijk eind 2021) is nog niet in zicht.

1.6. De drie deel-onderzoeken naast elkaar

Elk van de drie deel-onderzoeken kijkt vanuit een andere invalshoek naar de adoptie van open standaarden: 'pas toe' bij aanbestedingen, de compliance van voorzieningen en gebruiksgegevens van standaarden. Dergelijke gegevens kunnen niet zomaar naast elkaar gelegd worden. Tegelijkertijd komen in alle drie de deel-onderzoeken dezelfde open standaarden van de lijst voor 'pas toe of leg uit' voor. Wat levert het gecombineerde beeld uit deze drie bronnen op?

In de onderstaande tabel is dat in beeld gebracht. De cijfers in de kolom 'Aanbestedingen' zijn afkomstig uit Tabel 6 (hoofdstuk 3) en geven weer hoe vaak om standaard X is gevraagd, in procent van het aantal keer dat deze standaard relevant was bij een aanbesteding.

Voor de kolom 'Voorzieningen' zijn de scores van de 19 voorzieningen die dit jaar onderzocht zijn gecombineerd met de scores van de andere 17 voorzieningen (vorig jaar onderzocht). Berekend is voor hoeveel voorzieningen standaard X relevant was en hoeveel procent van die voorzieningen aan de standaard voldoet, of deels voldoet of binnenkort zal voldoen.

In de kolom 'Gebruiksgegevens' tenslotte is aangegeven hoeveel procent van bijvoorbeeld alle overheidsorganisaties of van de relevante web- of email-domeinnamen voldoet aan standaard X. Soms moest worden volstaan met een kwalitatieve inschatting van het gebruik.

De cijfers in deze eerste drie kolommen zijn met een kleur geaccentueerd: groen als de score 75% of hoger is, lichtgroen voor scores van 25% tot 75% en lichtoranje voor scores onder 25%. Als het absolute aantal erg klein is (1, 2 of 3), dan staat het percentage tussen haakjes.

In de rechterkolom ('Overall beeld') zijn deze drie cijfers per standaard zo goed als mogelijk samengevat tot één kwalificatie: positief, redelijk, wisselend, of matig. Een vraagteken betekent dat er onvoldoende informatie over de standaard beschikbaar is.

Het 'overall beeld' uit de drie deel-onderzoeken

Voor 11 van de 19 standaarden (incl. varianten) uit het domein *Internet & beveiliging* is het overall beeld positief, voor 3 standaarden is het redelijk en voor 3 standaarden is het beeld wisselend. Voor NL GOV Assurance zijn geen gegevens beschikbaar.

Ook in het domein *Stelselstandaarden* gaat het goed: voor alle drie de standaarden (Digikoppeling, Geo-standaarden en StUF) is het overall beeld positief.

In het domein *Document & (web)content* scoren twee van de 6 standaarden positief (Digitoegankelijk en PDF), twee scoren redelijk (Ades Baseline Profiles en OWMS) en twee scoren wisselend (ODF en SKOS).

De twee standaarden in het domein *REST API's* scoren allebei redelijk.

Van de vier standaarden in het domein *E-facturatie & administratie* is het overall beeld voor SETU en XBRL positief, en voor NLCIUS is het wisselend. Voor WDO Datamodel is onvoldoende informatie beschikbaar.

In het domein *Water & Bodem* is alleen over de Aquo standaard voldoende informatie beschikbaar: het overall beeld is wisselend.

Het overall beeld voor twee van de drie standaarden in het domein *Juridische verwijzingen* is wisselend. Voor de derde (JCDR) is onvoldoende informatie beschikbaar.

Over de standaarden in de domeinen *Bouw* en *Onderwijs & loopbaan* is onvoldoende informatie beschikbaar. Dat geldt ook voor de enige 'overige' standaard: EML_NL.

indicator:	**Aanbestedingen** # aanbestedingen waarbij OS is gevraagd in % van # waarbij OS relevant is	**Voorzieningen** # voorzieningen dat voldoet +deels +gepland in % van relevant	**Gebruiksgegevens** # overheden dat de standaard gebruikt in % van alle overheidsorganisaties	**Overall beeld**
Internet & beveiliging:				
DKIM	40%	96%	96 %	positief
DMARC	40%	90%	van 92% naar 95%	positief
en DMARC policy			van 66% naar 74%	redelijk
DNSSEC	30%	97%	van 94% naar 98%	positief
HTTPS	71%	91%	98 %	positief
en HSTS			van 92% naar 83%	positief
IPv6 en IPv4	18%	74%	van 69% naar 79%	wisselend
NEN-ISO\IEC 27001	98%	100%	[?]	positief
NEN-ISO\IEC 27002	98%	100%	[?]	positief
NL GOV Assurance	0%	0%	[?]	[?]
RPKI		78%	[licht toegenomen]	wisselend
SAML	55%	100%	[toegenomen]	positief
SPF	40%	96%	van 97% naar 99%	positief
en SPF policy			van 91% naar 94%	positief
STARTTLS	30%	68%	cf: van 42% naar 69%	redelijk
en DANE			van 53% naar 55%	redelijk
STIX & TAXII	0%	100%	[toegenomen]	wisselend
TLS	71%	91%	cf: van 78% naar 85%	positief
WPA2 Enterprise			[licht toegenomen]	[?]
Document & (web)content:				
Ades Baseline Profiles	50%	75%	[?]	redelijk
Digitoegankelijk	65%	100%	[?]	positief
ODF	0%	75%	3 %	wisselend
OWMS	50%	54%	van 28% naar 27%	redelijk
PDF	86%	96%	94 %	positief
SKOS		92%	[licht toegenomen]	wisselend
REST API's:				
OpenAPI Specification	30%	93%	[?]	redelijk
REST_API Design Rules	0%	73%	[?]	redelijk
E-facturatie & administratie:				
NLCIUS	100%	11%	[toegenomen]	wisselend
SETU	60%	100%	[stabiel]	positief
WDO Datamodel			[toegenomen]	[?]
XBRL	33%	100%	[stabiel]	positief
Stelselstandaarden:				
Digikoppeling	67%	95%	91 %	positief
Geo-standaarden	57%	100%	[toegenomen]	positief
StUF	85%	83%	[toegenomen]	positief
Water & Bodem:				
Aquo Standaard		100%	[stabiel]	wisselend
GWSW			[toegenomen]	[?]
SIKB 0101	0%		[toegenomen]	[?]
SIKB 0102			[toegenomen]	[?]
Bouw:				
COINS			[licht toegenomen]	[?]
IFC	0%		[gebruik beperkt]	[?]
NLCS			[licht toegenomen]	[?]
Visi			[licht toegenomen]	[?]
Juridische verwijzingen:				
BWB		100%	[toegenomen]	wisselend
ECLI			[toegenomen]	[?]
JCDR		100%	[toegenomen]	wisselend
Onderwijs & loopbaan:				
E–portfolio	0%		[?]	[?]
NL LOM			[?]	[?]
Overig:				
EML_NL			[overal toegepast]	[?]

2. Inleiding: het open standaardenbeleid en de opzet van dit onderzoek

2.1. Waarom open standaarden?

Voor een goede publieke dienstverlening is goed functionerende ICT nodig en voor goede ICT is het gebruik van open standaarden nodig.

Sinds 2008 voert het kabinet hiertoe het open standaardenbeleid uit, dat gericht is op het stimuleren van het gebruik van een aantal belangrijke open standaarden in de publieke sector. Het Forum Standaardisatie beheert hiervoor de 'pas toe of leg uit'-lijst, die inmiddels ruim 40 open standaarden omvat.

Het gebruik van deze standaarden is essentieel:

- om het digitale verkeer binnen en tussen overheden en tussen overheden en burgers en bedrijven soepel te laten doorstromen (interoperabiliteit),
- om grip te krijgen op de kosten voor ICT en keuzevrijheid bij de aanschaf te waarborgen (door leveranciersafhankelijkheid te beperken)
- en om te zorgen voor veiligheid en betrouwbaarheid in het digitale verkeer (bijvoorbeeld door cybercriminaliteit tegen te gaan en persoonsgegevens te beschermen) en om de toegankelijkheid van de digitale overheid voor al haar burgers en bedrijven te realiseren.

Voor de rijksoverheid is het gebruik van deze open standaarden geregeld in de Instructie Rijksdienst bij aanschaf ICT -diensten of ICT-producten (zie Bijlage B1). Gemeenten, provincies en waterschappen zijn hierop aangesloten via diverse bestuursakkoorden, die door het besluit van het Overheidsbreed Beleidsoverleg Digitale Overheid in 2018 voor het laatst zijn bekrachtigd. Dit betekent dat ook mede-overheden en uitvoeringsorganisaties bij de aanschaf van ICT moeten kiezen voor de relevante open standaarden van de 'pas toe of leg uit'-lijst. Hierover meer in paragraaf 2.2, over het juridisch kader.

Onder 'pas toe of leg uit' verstaan we het volgende:

Pas toe:
Overheden moeten bij de aanschaf van ICT voor € 50.000 of meer kiezen voor een dienst of product dat voldoet aan alle relevante open standaarden van de lijst ('pas toe'). Dat geldt voor een dienst, een product, een aanbesteding of inbesteding, en verbouw of nieuwbouw. Een standaard is relevant als de ICT valt onder het toepassingsgebied zoals beschreven op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie.

Leg uit:
Overheden mogen hiervan alleen afwijken als dit met een geldige reden gemotiveerd wordt uitgelegd in het jaarverslag. Het moet dan gaan om een geval waarin "… een dienst of product naar verwachting in onvoldoende mate wordt aangeboden, onvoldoende veilig of zeker functioneert, of om andere redenen van bijzonder gewicht."

Voor andere organisaties in de publieke sector is het toepassen of uitleggen van de open standaarden van de lijst geen verplichting, maar om dezelfde redenen als hierboven vermeld is ook voor hen het gebruiken van deze standaarden wel aanbevelenswaardig.

2.2. Juridisch kader van het 'pas toe of leg uit'-beleid

2.2.1. Ministeries en uitvoeringsorganisaties: Rijksinstructie en Rijksbegrotingsvoorschriften

Voor de rijksoverheid (zowel ministeries als uitvoeringsorganisaties) geldt sinds 2008 de Instructie Rijksdienst bij aanschaf ICT -diensten of ICT-producten (BWBR0024717):

> 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. (Art. 3, lid 1)

Deze verplichting geldt voor de aanbesteding, inkoop of ontwikkeling van ICT-producten en -diensten ter waarde van € 50.000 en meer. Niet alleen voor nieuwe producten of diensten, maar ook als het gaat om aanpassing van bestaande producten of diensten.

Een open standaard van de lijst is relevant als het betreffende ICT-product of -dienst valt binnen het functionele toepassingsgebied van die open standaard. Dit functionele toepassingsgebied is voor elke standaard omschreven in de lijst voor 'pas toe of leg uit'.

Wanneer besloten wordt om niet te vragen om één of meer standaarden die wèl van toepassing zijn, dan moet dit worden vastgelegd in de administratie en hierover moet verantwoording afgelegd worden in het jaarverslag. Afwijkingen zijn alleen mogelijk bij redenen van bijzonder gewicht (zie daarover ook de toelichting van de Instructie rijksdienst).

Daarnaast is sinds vele jaren in de RijksBegrotingsVoorschriften een bepaling opgenomen m.b.t. de paragraaf 'Rijksbrede bedrijfsvoeringsonderwerpen':

> Open standaarden en open source software: Dit onderwerp wordt in deze paragraaf alleen vermeld indien is afgeweken (het 'comply of explain'-beginsel) van artikel 3, eerste lid van de bijlage Instructie rijksdienst inzake aanschaf van ICT-diensten en ICT-producten. De Tweede Kamer wil dat de overheid meer gebruik maakt van open standaarden en open source software wanneer sprake is van de aankoop, inhuur en ontwikkeling van ICT-diensten of producten van € 50.000 of meer. De Instructie rijksdienst schrijft voor dat in beginsel gebruik wordt gemaakt van open standaarden van de lijst van het Forum Standaardisatie (www.forumstandaardisatie.nl). Valide afwijkingsgronden zijn opgenomen in de Instructie rijksdienst. Als er sprake is van afwijking van de Instructie rijksdienst dan wordt dit gemotiveerd aangegeven.

2.2.2. Mede-overheden: besluit OBDO en Richtlijnen commissie BBV

In de iNUP-bestuursakkoorden (met gemeenten, provincies en waterschappen) was als Resultaatafspraak 20 opgenomen, voor zover het open standaarden betreft:

> Gemeenten maken gebruik van de open standaarden zoals vastgesteld door het College standaardisatie en werken hierbij volgens het principe "pas toe of leg uit".

Op 18 april 2018 heeft het OBDO besloten dat ook mede-overheden bij aanschaf van ICT moeten kiezen voor de relevante open standaarden van de pas-toe-of-leg-uit-lijst.

Daarnaast is - voor gemeenten en provincies - in de Richtlijnen van de commissie BBV (Besluit begroting en verantwoording provincies en gemeenten) de aanbeveling opgenomen:

> 5a. De commissie BBV doet de aanbeveling om in de paragraaf bedrijfsvoering verantwoording af te leggen over het gebruik van open standaarden.

2.3. Over de Monitor Open standaarden 2021

ICTU verzorgt in opdracht van het Forum Standaardisatie jaarlijks een rapportage die inzicht geeft in het gebruik van de open standaarden op de lijst voor 'pas toe of leg uit': in hoeverre worden deze standaarden toegepast? Hierbij wordt vooral gekeken naar het gebruik door ministeries, uitvoeringsorganisaties, gemeenten, provincies en waterschappen, en soms ook door een andere publieke organisatie.

In deze rapportage worden gegevens gepresenteerd afkomstig uit een drietal bronnen:

- onderzoek van aanbestedingen in de tweede helft van 2020,
- onderzoek van de toepassing van open standaarden bij overheidsbrede voorzieningen,
- onderzoek naar overige gebruiksgegevens van een aantal open standaarden.

Het eindrapport zelf is overigens extern getoetst, het voldoet bijna volledig aan de eisen van de (voor overheden verplichte) open standaard DigiToegankelijk, zie voor de details daarvan de Toegankelijkheidsverklaring.

Onderzoek van aanbestedingen in tweede helft 2020

Dit jaar zijn aanbestedingen onderzocht van de rijksoverheid (en uitvoeringsorganisaties) en van mede-overheden, voor één keer alleen uit de periode juli tot en met december 2020.

Met ingang van de volgende monitor zullen namelijk telkens de aanbestedingen van het betreffende *kalenderjaar* worden onderzocht (tot nu toe onderzochten wij aanbestedingen van juli voorgaande jaar tot en met juni lopende jaar). De aanbestedingen van de eerste helft van 2020 zijn voor de vorige monitor reeds onderzocht.

Per aanbesteding is vastgesteld welke open standaarden van de lijst daarop van toepassing waren en in hoeverre daar daadwerkelijk om werd gevraagd ('pas toe'). Vervolgens is nagegaan in hoeverre overheden in hun jaarverslag ook verantwoording hebben afgelegd, wanneer bij aanbestedingen van de lijst werd afgeweken ('leg uit').

Onderzoek open standaarden bij overheidsbrede voorzieningen en shared services

Dit jaar onderzoeken wij 19 voorzieningen die relevant zijn voor de gegevensuitwisseling en communicatie tussen overheden en voor de onderliggende infrastructuur. Voor deze voorzieningen is onderzocht in hoeverre zij voldoen aan de open standaarden die daarvoor relevant zijn, hiervoor zijn de betreffende beheerorganisaties benaderd.

(Volgend jaar onderzoeken we – net als in de Monitor 2020 – opnieuw de voorzieningen de 17 voorzieningen, die vooral gericht zijn op de gegevensuitwisseling en communicatie met burgers en bedrijven.)

Onderzoek overige gebruiksgegevens van een aantal open standaarden

Om na te gaan in welke mate open standaarden daadwerkelijk worden toegepast zijn overige gebruiksgegevens verzameld voor een aantal open standaarden. Ook dit jaar zijn deze gebruiksgegevens verzameld in samenwerking met de accountmanagers van het Bureau Forum Standaardisatie.

3. Open standaarden bij aanbestedingen ('pas toe' en 'leg uit')

Het centrale beleidsinstrument van het open standaardenbeleid is het 'pas toe of leg uit'-principe. Dat houdt in: bij de aanschaf van ICT de relevante open standaarden van de lijst met verplichte standaarden toepassen, en verantwoording afleggen in het jaarverslag wanneer deze standaarden (ondanks dat zij relevant zijn) niet worden toegepast.

In het kader van de Monitor Open standaarden 2021 is voor inmiddels het tiende jaar onderzoek gedaan naar de toepassing van open standaarden bij aanbestedingen door overheden. Per aanbesteding is vastgesteld welke open standaarden van de lijst daarop van toepassing waren en in hoeverre daar daadwerkelijk om is gevraagd ('pas toe'). Vervolgens is nagegaan in hoeverre overheden in hun jaarverslag verantwoording hebben afgelegd, wanneer bij aanbestedingen van de lijst werd afgeweken ('leg uit').

Op het moment van rapporteren (zomer 2021) omvatte de 'pas toe of leg uit'-lijst 44 open standaarden. Voor dit onderzoek zijn alle 44 standaarden relevant. Daarbij is voor de praktijk van de beoordeling het volgende criterium aangehouden: de datum van de opname van de standaard op de 'pas toe of leg uit'-lijst moet eerder zijn dan de publicatie van de aanbesteding. Dat betekent dat twee standaarden (NL GOV Assurance profile for OAuth 2.0 en REST API Design Rules) buiten de beoordeling zijn gelaten van een enkele aanbesteding uit juli 2020.

De opzet van dit hoofdstuk is gelijk aan die van monitor-rapportages uit de afgelopen jaren. De aanpak van dit deelonderzoek wordt beschreven in paragraaf 3.1. De resultaten komen aan bod in paragrafen 3.2 ('pas toe' bij aanbestedingen), 3.3 (mate van 'pas toe' per open standaard), 3.4 (mate waarin open standaarden relevant waren bij de onderzochte aanbestedingen) en 3.5 ('leg uit' in jaarverslagen).

3.1. Onderzoek van aanbestedingen

Met ingang van deze monitor zullen telkens aanbestedingen van één volledig kalenderjaar worden onderzocht. Het onderzoek naar de aanbestedingen wijkt daarom dit jaar eenmalig af van de opzet van de afgelopen jaren. Voorheen werden namelijk de aanbestedingen van Q3+Q4 van het voorgaande jaar en Q1+Q2 van het lopende jaar onderzocht. Over de aanbestedingen in de eerste helft van 2020 is dus al gerapporteerd in de vorige monitor. Voor deze Monitor 2021 worden daarom eenmalig alleen de aanbestedingen in Q3 en Q4 van 2020 door het Rijk (met inbegrip van onder andere uitvoeringsorganisaties, agentschappen en ZBO's) en door de decentrale overheden onderzocht.

De resultaten van Q3 en Q4 van 2020 worden in dit hoofdstuk gepresenteerd. Dat zijn immers de nieuw onderzochte aanbestedingen. De resultaten worden vergeleken met de opbrengst uit de vorige monitor. Het aantal aanbestedingen is dit jaar uiteraard lager, maar het biedt voldoende basis om deze eenmalig afwijkende vergelijking verantwoord te kunnen maken.

Daarnaast worden de cijfers van de aanbestedingen uit Q1 en Q2 2020 (die voor de vorige monitor zijn onderzocht) toegevoegd aan de resultaten voor Q3 en Q4 (van deze monitor), zodat er ook resultaten voor het volledige kalenderjaar 2020 berekend kunnen worden. Dit samengevoegde overzicht over het hele kalenderjaar 2020 wordt in deze monitor verder niet

geanalyseerd maar dient als vergelijkingsbasis voor eventuele volgende monitors. Het overzicht over het kalenderjaar 2020 (Q1 tot en met Q4), in de vorm van een aantal tabellen zonder verdere beschouwing, is terug te vinden in bijlage B3.

Dit jaar was de rolverdeling tussen de experts vrijwel hetzelfde als vorig jaar. De beoordeling van aanbestedingen is uitgevoerd door Wouter van den Berg en Robin de Veer (TNO) en Arend-Jan Wiersma en Iris de Groot (ICT Recht) hebben de second opinion op de Rijks-aanbestedingen geleverd. De rapportage (dit hoofdstuk) is geschreven door Joost Vreuls.

Onderzocht zijn vooral aanbestedingen die op tenderned.nl zijn gepubliceerd. Het betreft daardoor veelal Europese aanbestedingen. Drempelwaarden daarvoor zijn voor de rijksoverheid > € 139.000 en voor decentrale overheden > € 214.000. Deze waarden worden telkens voor twee jaar door de Europese Commissie vastgesteld. Per 1 januari 2020 zijn deze drempelwaarden voor het laatst vastgesteld.

Aanbestedingen onder deze grenzen (maar groter dan € 50.000) worden weinig op tenderned.nl gepubliceerd en vallen om die reden grotendeels buiten het onderzoek. Verder zijn detacheringen (waaronder maatwerk-opdrachten) in principe niet onderzocht, omdat 'pas toe of leg uit' daarbij hoogstens op bijzondere wijze kan plaatsvinden (bijvoorbeeld door bepaalde competenties te eisen). Daarnaast is moeilijk te beoordelen of daarbij ICT-producten/-diensten gerealiseerd worden waarop open standaarden van toepassing zijn en in hoeverre die daarbij geëist worden. Een kanttekening hierbij: in de onderzoekspraktijk blijkt dat deze grens niet altijd even duidelijk is te trekken. Voor een goede beoordeling moeten alle relevante en beschikbare aanbestedingsdocumenten bestudeerd kunnen worden.

In principe worden elk jaar veel van de in de voorafgaande periode verzamelde relevante aanbestedingen van Rijksoverheid en uitvoeringsorganisaties beoordeeld; de speelruimte om een steekproef te trekken is beperkt. Dit jaar vielen ongeveer 10 aanbestedingen door de Rijksoverheid buiten de steekproef. Het aantal beoordeelde aanbestedingen van de Rijksoverheid (20) ligt dit jaar min of meer op het gebruikelijke niveau voor een halfjaarlijkse periode. Ook dit jaar is een beperkt aantal (4) aanvankelijk geselecteerde aanbestedingen van Rijksoverheid en uitvoeringsorganisaties bij nader inzien door de experts gekwalificeerd als 'niet beoordeelbaar'. Om toch tot het streef-aantal van 20 beoordeelde aanbestedingen te komen was de steekproef ruimer genomen. Bij de niet beoordeelbare aanbestedingen gaat het om de volgende casuïstiek:

- er is in drie gevallen bij nader inzien sprake van een raamovereenkomst zonder zicht op de inhoud van onderliggende nadere overeenkomsten en daarmee buiten scope;
- het op te leveren product is (niet meer dan) een Excel-bestand (plus een rapport); er vindt met het product geen verdere digitale communicatie of uitwisseling plaats.

Voor de medeoverheden wordt elk jaar een steekproef getrokken uit de (vele) gevonden aanbestedingen. Dit jaar zijn eveneens 20 aanbestedingen van medeoverheden beoordeeld over een halfjaarlijkse periode (vorig jaar 37 over 4 kwartalen). Ter herinnering: met ingang van de monitor 2018 is gekozen voor een verdubbeling van het aantal te onderzoeken aanbestedingen door medeoverheden om daar beter zicht op te krijgen.

In totaal zijn 40 aanbestedingen beoordeeld: 20 van het Rijk (departementen, uitvoerings-organisaties, agentschappen, ZBO's) en een steekproef van 20 aanbestedingen van

medeoverheden. De 40 beoordeelde aanbestedingen vormen een goede afspiegeling van de overheids-ICT-aanbestedingen, voor zover die binnen de beschreven zoek-kaders vallen.

Voor een goed begrip van het cijfermateriaal nog enkele opmerkingen over de praktijk van ICT-aanbestedingen door overheden:

- veel overheidsorganisaties werken met (ICT-)mantelovereenkomsten, die voor een langere periode van kracht zijn en/of met enkele jaren verlengd worden; aanbestedingen binnen de mantelovereenkomst worden direct bij de mantelpartijen uitgezet en zijn dus niet via tenderned.nl te achterhalen;
- de vervangingscyclus van veel bedrijfs-software is 5 tot 8 jaar, wat betekent dat dergelijke applicaties maar eens in de zoveel jaar (opnieuw) worden aanbesteed. Met name bij kleinere overheidsorganisaties kan dit betekenen dat men slechts zeer incidenteel van doen heeft met het beleid rond open standaarden;
- de huidige lijst voor 'pas toe of leg uit' bevat onder andere diverse semantische open standaarden, waaronder een aantal met een zeer specifiek toepassingsgebied. Dergelijke standaarden blijken in de praktijk vaker relevant voor maatwerk-oplossingen dan voor standaardsoftware-pakketten. Zoals gezegd valt juist een deel van de maatwerk-opdrachten buiten het onderzoek (detacheringen, mantelovereenkomsten).

Uit de praktijk van de beoordeling door de experts van de aanbestedingen blijkt dat een aantal standaarden uitsluitend in combinatie al dan niet relevant worden geacht, ook al staan deze standaarden los op de lijst. Voorbeelden van dergelijke combinaties zijn DKIM met DMARC en SPF (emailstandaarden), HTTPS&HSTS met TLS en ISO-27001 met ISO-27002.

De variatie in de aard van de ICT-producten en -diensten die werden aanbesteed is net als in de voorgaande jaren groot. Zie ook het overzicht van alle beoordeelde aanbestedingen in Bijlage B2. Bij wijze van bloemlezing enkele kleurrijke voorbeelden van aanbestedingen:

- Een aanbesteding voor websiteontwikkeling, het beheren en hosten van een state of the art website voor de Rijksacademie. Onderdeel is een vlekkeloos werkende koppeling met het opleidingsadministratiesysteem. Ook moet de website gebruikersvriendelijk zijn voor deelnemers en functioneel beheerders. De website moet inzicht bieden in de verschillende opleidingsactiviteiten, nieuwsberichten en ondersteunt deelnemers in het vinden van en inschrijven bij een opleiding.
- De opdrachtgever wil een model laten bouwen dat kan worden gebruikt om de economische haalbaarheid in te schatten van replicatie van telecommunicatie-netwerken in Nederland. Wanneer een verzoek binnen komt voor toegang op een bestaand netwerk heeft de opdrachtgever het model nodig om te kunnen beoordelen tot welk punt in het netwerk de toegangszoeker zijn eigen glasvezelnetwerk (op de meest efficiënte manier) kan uitrollen. Deze inschatting is nodig om toegangsregulering uit te voeren op een manier die in lijn is met de gewijzigde telecommunicatiewet.
- De opdrachtgever zoekt een partner die ruime ervaring heeft met het leveren, implementeren, beheren en onderhouden van audio- en videoapparatuur die bedoeld is voor opname van verhoren en het terugkijken en –luisteren daarvan, inclusief software.
- Door middel van deze aanbesteding wil een gemeente een oplossing geleverd krijgen waarmee:
    - omgevingswetbesluiten vastgesteld kunnen worden conform de Omgevingswet;
    - omgevingswetbesluiten onderhouden kunnen worden conform de toepassingsprofielen: omgevingsdocumenten, omgevingsplan en omgevingsvisie;

    - omgevingswetbesluiten gepubliceerd kunnen worden naar de Landelijke Voorziening Bekendmaken en Beschikbaarstellen (LVBB) via de standaard officiële overheidspublicaties;
    - de gemeente ondersteund wordt bij de doelstellingen binnen de projectstartarchitectuur.
- De gemeente wil één overeenkomst afsluiten voor de implementatie, hosting, doorontwikkeling en onderhoud van een zwembadapplicatie voor de plaatselijke zwembaden. Deze dienstverlening bestaat uit het leveren van een entree-kassasysteem, reserveringssysteem, horeca-kassa en een leerlingvolgsysteem. Eventueel wil de gemeente in de toekomst de toegang vergemakkelijken door het afnemen van tourniquets.

Toetsingskader

Het onderzoek is gebaseerd op de gepubliceerde, openbare informatie over de aanbestedingen. Dat is immers de informatie waarop de aanbieders zich hebben moeten baseren. Dat impliceert dat niet alleen informatie uit de eerste publicatie maar ook openbare informatie die in een later stadium vrij komt (bijvoorbeeld een Nota van Inlichtingen) ook mee mag wegen bij het opmaken van de beoordeling.

Het onderzoek toetst op basis van de openbare documenten in hoeverre de aanbesteding voldoet aan het 'pas toe of leg uit'-beginsel, zoals dat (voor de Rijksoverheid) is vastgelegd in de Instructie Rijksdienst.

Er is voor een aanbesteding sprake van een 'relevante open standaard', als het betreffende ICT-product of -dienst valt binnen het functionele toepassingsgebied van die standaard. Voor één aanbesteding kunnen uiteraard meerdere open standaarden relevant zijn.

Uitgangspunt daarbij is, dat bij de aanbesteding expliciet gevraagd moet worden om de standaard(en). Soms wordt alleen in algemene zin verwezen naar de ‘pas toe of leg uit’-lijst. De aanbieder krijgt daarmee de verantwoordelijkheid voor het correct toepassen ervan. In de praktijk levert dat niet het beoogde (beleids)effect op. De aanbiedingen zijn immers alleen te beoordelen op het correct toepassen van de lijst als de aanbesteder (a) zelf weet welke open standaarden van toepassing zijn, en (b) hierom ook expliciet gevraagd heeft.

Naderhand worden de aanbesteders geïnformeerd over de beoordeling. Dat geeft hen (onder andere) de gelegenheid om daarop te reageren. Soms leidt een dergelijke reactie tot een bijstelling van het oorspronkelijke oordeel. Jaarlijks voeren wij bovendien met zes aanbesteders een gesprek over het open standaardenbeleid en hun aanbesteding(en).

Daarnaast is onderzocht op welke wijze de verantwoording ('leg uit') over 2020 heeft plaatsgevonden (zie paragraaf 3.5). Wanneer de aanbestedende organisatie besluit om niet te vragen om één of meer open standaarden die wèl van toepassing zijn, dan moet dit worden vastgelegd in de departementale administratie en hierover moet verantwoording afgelegd worden in het jaarverslag. Afwijkingen zijn overigens alleen mogelijk bij redenen van bijzonder gewicht.

3.2. 'Pas toe' bij aanbestedingen in 2e helft 2020

In de 40 aanbestedingen uit Q3 en Q4 2020 die voor deze monitor zijn beoordeeld had in totaal om 487 open standaarden gevraagd moeten worden, feitelijk is er echter 264 keer om een open standaard gevraagd. Dat is 54% daarvan (zie de groene rijen in het gestippelde kader midden in Tabel 1), en dat is relatief hoog in vergelijking met de recent achter ons liggende jaren (vorig jaar 45%, het jaar daarvoor 50%). Het percentage van 54% is hoger dan de uitvraag-percentages van alle monitor-rapportages tot nu toe.

Deze toename van 45% naar 54% is in zijn geheel toe te schrijven aan een fors hoger uitvraag-percentage bij de Rijks-aanbestedingen: van 39% naar 59% (het percentage voor de medeoverheden is met 50% gelijk aan vorig jaar). Daarmee is de afname van het uitvraag-percentage bij Rijks-aanbestedingen van vorig jaar ten opzichte van het jaar daarvoor meer dan goed gemaakt.

3.2.1. 'Pas toe' per aanbesteding

Bij 4 van de 40 aanbestedingen (10%, zie de grijze kolommen in Tabel 1; vorig jaar 7%) werd **om alle relevante open standaarden gevraagd ('perfect')**, dat is 'pas toe' in strikte zin. Dit waren 3 aanbestedingen door ministeries (daarbij inbegrepen de Belastingdienst) en 1 door een gemeentelijk (gemeenschappelijk) inkoopbureau, in dit geval ten behoeve van een Veiligheidsregio.

Daarnaast werd bij 35 aanbestedingen (88%; vorig jaar eveneens 88%) gevraagd om een deel van de voor die aanbesteding relevante standaarden ('op de goede weg'). Bij de resterende aanbesteding (3%; vorig jaar 6%) waren vier standaarden relevant, maar werd om geen enkele gevraagd en was in de aanbestedingsdocumenten in het geheel geen aandacht voor open standaardenbeleid terug te vinden ('slecht').

De **categorie 'op de goede weg'** is – net als vorig jaar – erg groot en daardoor blijven de verschillen binnen die grote groep aanbestedingen onderbelicht. Er zijn aanbestedingen die op een enkele misser in de uitvraag na de score 'perfect' zouden hebben gehad, maar ook aanbestedingen die wel het predicaat 'op de goede weg' krijgen omdat er om één standaard van de relevante standaarden gevraagd is, maar waarbij de aandacht voor open standaarden verder heel marginaal is geweest.

Om die reden is binnen de categorie 'op de goede weg' net als vorig jaar een nadere nuancering aangebracht:

- 'op weg naar perfect' (aanbestedingen waarbij om 67% tot 99% van de relevante standaarden gevraagd is; zie de percentages in de rechter kolom van Bijlage B2);
- 'de middenmoot' (met uitvraag-scores van 34% - 66%);
- 'nog een heel eind te gaan' (met uitvraag-scores van 1% - 33%).

Deze nuancering leidt tot het volgende beeld:

- 33% van alle aanbestedingen is 'op weg naar perfect', 30% behoort tot de middenmoot en voor 25% geldt dat er nog een heel eind te gaan is;
- de rijksoverheid laat een gunstiger beeld zien dan de medeoverheden: het aandeel 'op weg naar perfect' is voor de rijksoverheid relatief groot, het aandeel 'nog een heel eind

te gaan' juist beduidend kleiner. Vorig jaar was het beeld net andersom: toen was sprake van een betere score voor medeoverheden in vergelijking met de rijksoverheid;
- in vergelijking met de vorige monitor is het beeld duidelijk verbeterd. Zo is het aandeel achterblijvers ("nog een heel eind te gaan") flink afgenomen (van 39% naar 25%) en is het aandeel 'op weg naar perfect' behoorlijk toegenomen (van 18% naar 33%). De omvang van de middenmoot is vrijwel gelijk gebleven.

Tabel 1: 'Pas toe' en 'leg uit' bij aanbestedingen tweede helft 2020
(Bron: onderzoek aanbestedingen juli t/m december 2020, uitgevoerd zomer 2021)

	Rijksoverheid		Mede-overheden		**Totaal 2e helft 2020**		Totaal 2019/2020	
	#	%	#	%	#	%	#	%
totaal aantal beoordeelde aanbestedingen waarbij OSn relevant waren	20	100%	20	100%	**40**	**100%**	72	100%
* **perfect**: alle relevante OSn gevraagd	3	15%	1	5%	**4**	**10%**	5	7%
* **op de goede weg**: deel van relevante OSn gevraagd	16	80%	19	95%	**35**	**88%**	63	88%
- op weg naar perfect (67-99%)	7	35%	6	30%	**13**	**33%**	13	18%
- de middenmoot (34-66%)	6	30%	6	30%	**12**	**30%**	22	31%
- nog een heel eind te gaan (1-33%)	3	15%	7	35%	**10**	**25%**	28	39%
geen relevante OSn gevraagd, waarvan	1	5%	0	0%	**1**	**3%**	4	6%
* **matig**: er is wel algemene aandacht voor architectuur-kaders en/of OSn-beleid	0	0%	0	0%	**0**	**0%**	0	0%
* **slecht**: geen aandacht voor OSn-beleid	1	5%	0	0%	**1**	**3%**	4	6%
* **heel slecht**: strijdig met OSn-beleid	0	0%	0	0%	**0**	**0%**	0	0%
In aantallen standaarden:								
totaal aantal relevante OSn	*216*	*100%*	*271*	*100%*	***487***	***100%***	*834*	*100%*
totaal aantal gevraagde relevante OSn	*128*	*59%*	*136*	*50%*	***264***	***54%***	*377*	*45%*
niet alle OSn gevraagd => Leg Uit vereist (voor toelichting: zie paragraaf 3.5)	17	100%	19	100%	**36**	**100%**	33	100%
- concrete verantwoording in jaarverslag	0	0%	0	0%	**0**	**0%**	0	0%
- beperkte verantwoording in jaarverslag	4	24%	0	0%	**4**	**12%**	1	3%
- geen Leg Uit in jaarverslag	13	76%	19	100%	**32**	**88%**	32	97%

In de categorie **'geen relevante open standaarden gevraagd'** viel maar één aanbesteding:
- matig: er is algemene aandacht voor architectuur-kaders en/of open standaardenbeleid (0%, vorig jaar eveneens 0%),
- slecht: er is geen aandacht voor open standaardenbeleid (1 aanbesteding = 3%, vorig jaar nog 6%);
- heel slecht: strijdig met het open standaardenbeleid: (dit jaar geen enkele aanbesteding, vorig jaar evenmin).

Alles bij elkaar genomen is deze verzamelcategorie 'geen relevante open standaarden gevraagd' dus nog iets kleiner geworden, na ook al een daling vorig jaar.

Uit het groen gemarkeerde gestippelde kader midden in de tabel valt op dat het **aantal standaarden** dat per aanbesteding relevant wordt geacht dit jaar wederom hoger ligt dan

vorig jaar (gemiddeld iets boven de 12 standaarden per aanbesteding, vergeleken met gemiddeld ongeveer 11,5 vorig jaar). We zien nu al enkele jaren achter elkaar een stijging van het aantal relevante standaarden per aanbesteding. De stijging manifesteert zich dit jaar alleen maar bij aanbestedingen rijksoverheid. Bij de medeoverheden ligt het gemiddelde aantal relevante standaarden per aanbesteding op een vergelijkbaar niveau als vorig jaar. Dit gemiddelde is overigens nog steeds beduidend hoger dan bij de rijksoverheid (een verschil van bijna 3 relevante standaarden per aanbesteding).

Tot slot is opvallend aan Tabel 1 dat het aandeel gevraagde standaarden voor Rijk en voor medeoverheden behoorlijk verschilt, dit keer in het voordeel van het Rijk: 59% versus 50%. De score bij het Rijk is fors toegenomen (van 39% naar 59%) terwijl de mede-overheden net als vorig jaar 50% scoren. Hierbij moet worden opgemerkt dat deze variabele door de jaren heen behoorlijk fluctueert zonder dat sprake is van een eenduidige ontwikkeling. Een rode draad is wel dat het Rijk – ook dit jaar weer – meestal een duidelijk hogere score laat zien dan de medeoverheden. De uitkomst van vorig jaar, toen medeoverheden beter scoorden dan het Rijk, lijkt met de kennis van nu eenmalig te zijn geweest.

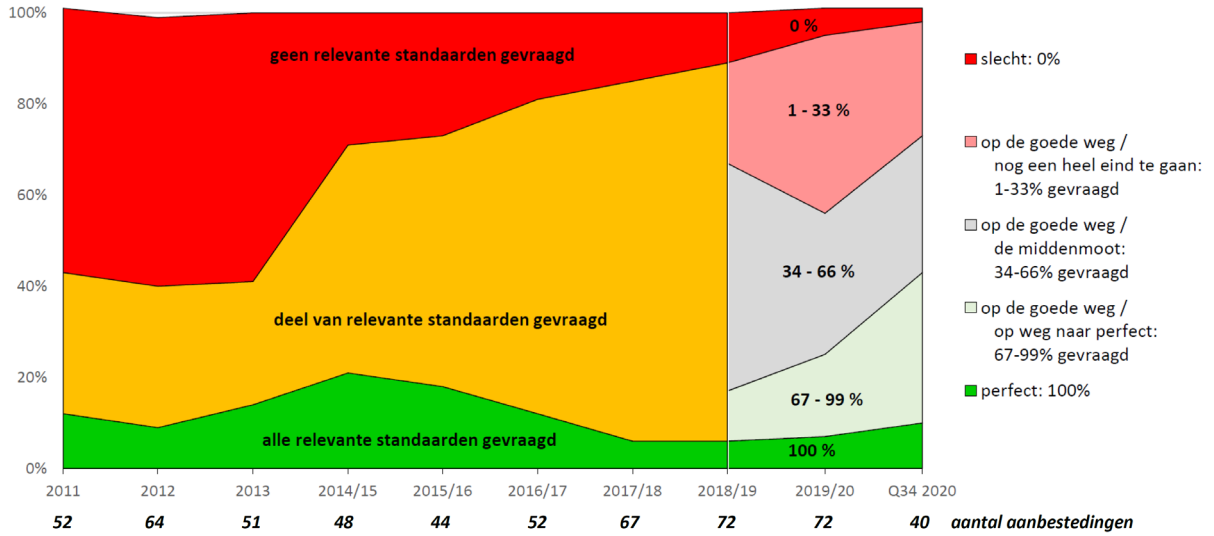
Op basis van Tabel 1 en de cijfers van voorgaande jaren is de ontwikkeling als volgt:

- Het aantal aanbestedingen waarbij om alle relevante standaarden is gevraagd ligt procentueel wat hoger dan vorig jaar; nu 10% tegen 7% vorig jaar. Voor een breder perspectief in de tijd: de drie jaren daarvoor lag de score steeds op 6% en in de jaren daarvoor was drie jaren op rij sprake van een afname (zeven jaar geleden lag dit percentage nog op 21%). De score bij de Rijksoverheid is - overigens net als vorig jaar - hoger dan bij de medeoverheden (15% tegen 5% bij medeoverheden).
- De midden-categorie - gekwalificeerd als 'op de goede weg' - is ook bij deze monitor weer op afstand de grootste met 88% (vorig jaar eveneens 88%). Binnen deze midden-categorie is het aantal aanbestedingen met de kwalificatie 'op weg naar perfect' toegenomen, voornamelijk dankzij een duidelijke verbetering bij de aanbestedingen Rijk. De kwalificatie 'nog een heel eind te gaan' is dit jaar beduidend minder vaak aan de orde in vergelijking met vorig jaar.
- Het aantal aanbestedingen waarbij om geen enkele standaard is gevraagd (met oordelen 'matig' dan wel 'slecht') is iets teruggelopen, van 6 % vorig jaar naar 3 % dit jaar.
- Net als vorig jaar is er dit jaar bij geen enkele aanbesteding sprake van strijdigheid met het open standaardenbeleid.

In Figuur 2 is de ontwikkeling in een breder tijdsperspectief geplaatst, vanaf het jaar 2011.

De middengroep ‘op de goede weg’, bestaande uit aanbestedingen waarbij wel om één of meer van de relevante standaarden gevraagd werd maar niet om alle, is in de loop der jaren flink gegroeid, inmiddels tot 88% van alle aanbestedingen (zie Figuur 2). Binnen die middengroep maken we nog een nadere onderverdeling tussen aanbestedingen waarbij maar om een klein deel van de relevante standaarden werd gevraagd (1-33%; ‘nog een heel eind te gaan’), een middensegment (34-66%; de middenmoot) en de groep die om een groter deel van de relevante standaarden heeft gevraagd (‘op weg naar perfect’). Zowel in Figuur 2 als in Figuur 3 is te zien, dat het segment van de middengroep met de hoogste scores (kwalificatie ‘op weg naar perfect’) voor het eerst het grootst is, op de voet gevolgd door de wat we hier ‘de middenmoot’ noemen. Waar het segment met de kwalificatie ‘nog een heel eind te gaan’ vorig jaar het grootst was, is dit segment dit jaar het kleinst.

Figuur 2: 'Pas toe' bij aanbestedingen, 2011 – 2e helft 2020



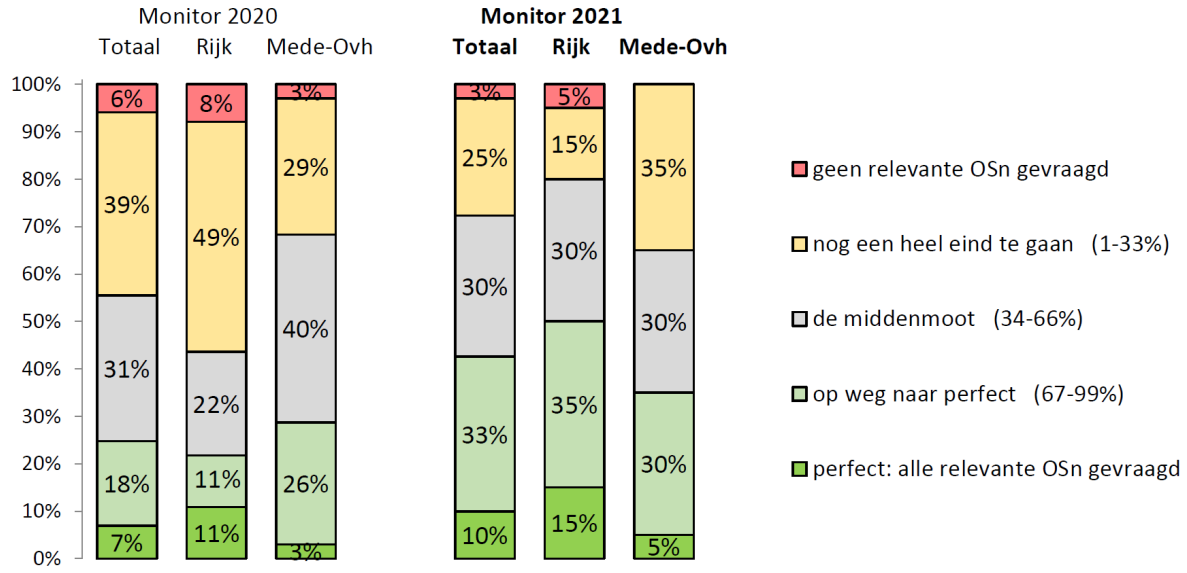
Het Rijk en uitvoeringsorganisaties deden het dit jaar, in tegenstelling tot vorig jaar, beter dan de mede-overheden: bij de helft van de aanbestedingen (50%) vroegen Rijk en uitvoeringsorganisaties om alle relevante standaarden ('perfect') of om tenminste tweederde daarvan ('op weg naar perfect'), voor de mede-overheden was dat 35%. De vergelijkbare scores van zowel Rijk als mede-overheden liggen overigens duidelijk hoger dan de vergelijkbare scores van vorig jaar (toen 22% respectievelijk 29%). Aan de andere kant van het spectrum: de Rijksoverheid vroeg bij slechts 20% van de aanbestedingen om geen enkele of om minder dan een derde van de relevante standaarden (medeoverheden: 35%). Met name de score bij Rijksoverheid is een forse verbetering ten opzichte van vorig jaar (toen maar liefst 57%).

In Figuur 3 zijn duidelijk de verschillen te zien tussen enerzijds Rijk en uitvoeringsorganisaties en anderzijds de medeoverheden, ook in vergelijking met vorig jaar:

- bij de Rijks-aanbestedingen is het aandeel 'perfect' iets toegenomen ten opzichte van vorig jaar (van 11% naar 15%) en het aandeel 'geen enkele standaard gevraagd' iets afgenomen (van 8% naar 5%), alles met kleine verschillen;
- ook bij de aanbestedingen van de medeoverheden is het aandeel 'perfect' iets toegenomen ten opzichte van vorig jaar (van 3% naar 5%), en ook hier is het aandeel 'geen enkele standaard gevraagd' iets afgenomen (van 3% naar 0%);
- de middencategorie 'op de goede weg' is bij de Rijks-aanbestedingen vrijwel even groot als vorig jaar; binnen die middencategorie is bij de Rijks-aanbestedingen echter sprake van een duidelijke verschuiving ten goede. Het aandeel 'op weg naar perfect' is flink gestegen (van 11% naar 35%) en het aandeel 'nog een heel eind te gaan' is juist flink kleiner geworden (van 49% naar 15%). Dit aandeel 'nog een heel eind te gaan' is dit jaar het kleinst bij de middencategorie Rijk terwijl dat aandeel vorig jaar nog het grootst was; het aandeel 'middenmoot' binnen de middencategorie van de Rijksaanbestedingen is gestegen van 22% naar 30%;
- ook bij de medeoverheden is de middencategorie 'op de goede weg' even groot als vorig jaar; bij de medeoverheden ontbreekt echter in de midden-categorie een verschuiving ten goede (zoals bij Rijks-aanbestedingen). Het aandeel 'op weg naar perfect' is weliswaar iets toegenomen (van 26% naar 30%) maar daar staat een stijging

tegenover bij de categorie ‘nog een heel eind te gaan’ (van 29% naar 35%); het aandeel ‘middenmoot’ bij de medeoverheden is gedaald van 40% naar 30%.

Figuur 3: 'Pas toe' bij aanbestedingen: uitsplitsing Rijk vs. Medeoverheden



Alle cijfers over ‘pas toe’ bij aanbestedingen overziend is het beeld behoorlijk positief.

- Zowel het aandeel aanbestedingen dat als ‘perfect’ of ‘op weg naar perfect’ werd beoordeeld is toegenomen (samen van 25% tot 43%). Deze beide stijgingen zien we terug bij zowel Rijk als medeoverheden, waarbij met name de score van Rijk sterk is verbeterd.
- En het aantal aanbestedingen waarbij geen enkele relevante standaard werd gevraagd nam verder af van 6% tot 3%. De afname zien we terug bij zowel Rijk als medeoverheden.
- Binnen de grote middengroep is sprake van een flinke verbetering: een duidelijke hogere score voor ‘op weg naar perfect’ (van 18% naar 33%) en een lagere score voor ‘nog een heel eind te gaan’ (van 39% naar 25%). Deze verbetering komt voor rekening van het Rijk.
- Van de in totaal 487 keer dat een open standaard voor een aanbesteding relevant was, werd daar in 54% van de gevallen om gevraagd (vorig jaar 45%), ook deze verbetering komt doordat het percentage ‘gevraagd’ bij Rijks-aanbestedingen steeg van 39% tot 59% (bij medeoverheden bleef het stabiel op 50%).

3.2.2. Enkele goede voorbeelden

Ook dit jaar brengen we weer enkele goede voorbeelden van aanbestedingen voor het voetlicht. Bij de keuze van de voorbeelden is het oordeel ‘perfect’ niet leidend geweest. Onder de vier aanbestedingen met dit oordeel ‘perfect’ zitten namelijk drie aanbestedingen met een zeer beperkt aantal relevant geachte standaarden waardoor een oordeel ‘perfect’ relatief makkelijk te bereiken is.

De enige aanbesteding met het oordeel ‘perfect’ met een complex beeld van relevant geachte aanbestedingen is van het Ministerie van BZK. Aanvullend hierop volgt hieronder nog een vijftal andere aanbestedingen waarbij weliswaar niet 100% werd uitgevraagd, maar die wel een expliciet positieve beoordeling kregen van de beoordelende experts: het

ministerie van Financiën, de gemeenten Waddinxveen, Apeldoorn en Purmerend en de Regio Rivierenland.

- **Ministerie van BZK**. Rijksportaal is het Rijksbrede intranet voor Rijksambtenaren bij alle ministeries. Het is dé digitale toegangspoort tot informatie, kennis en dienstverlening die Rijksmedewerkers ondersteunen in hun werkzaamheden. Men wil het huidige Rijksportaal vervangen.
  - Commentaar van de beoordelaars: "Een perfecte aanbesteding! Er is ruim aandacht voor open standaarden(beleid), de PTOLU-lijst en/of BFS. De open standaarden die relevant zijn worden verzameld weergegeven en toegelicht".
  - De volgende 15 standaarden zijn relevant en ook allemaal uitgevraagd: ISO 27001, ISO 27002, Digitoegankelijk, SAML, DNSSEC, HTTPS & HSTS, TLS, IPv4 & IPv6, SPF, DKIM, DMARC, STARTTLS & DANE, OpenAPI specification, OWMS en PDF.
- **Ministerie van Financiën**. Het betreft een aanbesteding voor websiteontwikkeling, beheren en hosten van een state of the art website voor de Rijksacademie. Onderdeel is een vlekkeloos werkende koppeling met het opleidingsadministratiesysteem. Ook moet de website gebruikersvriendelijk zijn voor deelnemers en functioneel beheerders. De website moet inzicht bieden in de verschillende opleidingsactiviteiten, nieuwsberichten en ondersteunt deelnemers in het vinden en inschrijven bij een opleiding.
  - Commentaar van de beoordelaars: "Het was een hele goede aanbesteding, alleen jammer dat de mailstandaarden niet zijn geëist en er twijfel is over de eis van DNSSEC (voordeel van de twijfel). Er wordt duidelijk aangegeven dat het ICT-product moet voldoen aan relevante open standaarden zoals gepubliceerd bij BFS. Er wordt ook veelvuldig verwezen naar specifieke open standaarden op de PTOLU-lijst.".
  - De volgende standaarden 11 zijn relevant geacht: ISO 27001, ISO 27002, HTTPS & HSTS, TLS, Digitoegankelijk, DNSSEC, IPv4 & IPv6 en de email-standaarden (SPF, DKIM, DMARC, STARTTLS & DANE); alleen deze laatste 4 zijn dus niet uitgevraagd.
- **Gemeente Waddinxveen**. De gemeente maakt al jaren gebruik van Cipers/iBurgerzaken van PinkRoccade als applicatie voor burgerzaken. Ook werkt Waddinxveen met de Makelaarsuite van PinkRoccade. De looptijd van deze overeenkomsten gaat eindigen en daarom voert Waddinxveen een aanbestedingsprocedure uit om de komende jaren invulling te geven aan de functionaliteit die deze applicaties momenteel bieden. De oplossing is een SaaS-oplossing dan wel een gehoste omgeving.
  - Commentaar van de beoordelaars: "Een goede aanbesteding! De oplossing dient te voldoen aan de verplichte open standaarden op de PTOLU-lijst van BFS. Veel standaarden zijn gevraagd, maar helaas zijn de belangrijke standaarden HTTPS/HSTS, TLS en IPv4/6 niet gevraagd.".
  - De volgende 16 standaarden zijn als relevant aangemerkt door de beoordelaars: DNSSEC, Digitoegankelijk, Digikoppeling, ISO 27001, ISO 27002, SAML, PDF, DKIM, DMARC, SPF, STARTTLS & DANE, StUF, ODF, HTTPS & HSTS, TLS en IPv4 & IPv6. (Naast de eerdergenoemde 3 niet gevraagde standaarden is ook ODF niet uitgevraagd).
- **Gemeente Apeldoorn**. De opdracht heeft betrekking op de levering, implementatie en migratie van een Integratievoorziening, bestaande uit een Enterprise Service Bus (ESB), een API Gateway en Digikoppeling, inclusief gerelateerde dienstverlening. Verder betreft het de (opnieuw) ontwikkeling en implementatie van tot en met eind 2020 reeds ontwikkelde koppelingen en de voor 2021 reeds geplande koppelingen.

    - De beoordelaars: “Een goede aanbesteding waarbij veel van de relevante standaarden zijn uitgevraagd. De oplossing dient te voldoen aan richtlijnen van NCSC, OWASP en relevante standaarden van het Forum Standaardisatie. Er moet worden voldaan aan de BIO en GIBIT”.
    - De volgende 15 standaarden zijn relevant: Digikoppeling, DNSSEC, HTTPS & HSTS, TLS, ISO 27001, ISO 27002, SAML, SPF, DKIM, DMARC, STARTTLS & DANE, PDF, StUF, ODF en Open API specification. Alleen de laatste twee zijn niet in de uitvraag meegenomen.
- **Gemeente Purmerend**. De gemeente wenst tot een overeenkomst te komen voor de dienstverlening eHRM. De gemeente is op zoek naar een “proven technology” oplossing. Het eHRM-systeem wordt geleverd op basis van een SAAS-oplossing.
    - Het commentaar van de beoordelaars is vergelijkbaar met dat bij de aanbesteding hierboven (gemeente Apeldoorn).
    - De volgende 18 standaarden zijn relevant: DNSSEC, Digikoppeling, HTTPS & HSTS, TLS, IPv4 & IPv6, ISO 27001, ISO 27002, StUF, PDF, SAML, SPF, DKIM, DMARC, STARTTLS & DANE, ODF, Open API specification, NL GOV Assurance profile en REST API Design Rules. De vier laatstgenoemde standaarden zijn niet uitgevraagd, met daarbij de kanttekening dat de laatste twee standaarden pas recent op de PToLU-lijst staan.
- **Regio Rivierenland**. Bedrijfsvoeringseenheid Bommelerwaard wil een partij contracteren voor het ontwikkelen, implementeren, beheren, onderhouden en doorontwikkelen van een datadistributiesysteem. De nieuwe datadistributie-applicatie gaat ingezet worden om de datadistributie en het beheer van gemeenten Zaltbommel en Maasdriel te faciliteren. De applicatie is de spin in het web van de gemeentelijke gegevensuitwisseling, maar is in gebruik en beheer niet complex. De oplossing wordt als SaaS opgeleverd.
    - Wederom het commentaar van de beoordelaars: “Een goede aanbesteding. Veel relevante standaarden zijn uitgevraagd. Er moet worden voldaan aan de open standaarden op de PToLU-lijst van BFS en de GIBIT”.
    - De 13 relevante standaarden: HTTPS & HSTS, TLS, ISO 27001, ISO 27002, IPv4 & IPv6, SPF, DKIM, DMARC, STARTTLS & DANE, StUF, ODF, DNSSEC en SAML. De drie laatste zijn niet uitgevraagd.

Voor de volgende drie aanbestedingen geldt: net als bij de eerste aanbesteding uit bovenstaande opsomming (Ministerie van BZK) ook 100% uitgevraagd, maar bij een veel kleiner aantal relevante standaarden (bij alle drie alleen de ISO-standaarden):

- **Ministerie van Defensie**. De aanbesteding betreft ICT-producten en vooral -diensten voor militair-operationeel gebruik. Het betreft enkel perceel 2 van een grotere aanbesteding. Perceel 2 gaat over 'engineering service', ook wel 'future ops' genoemd.
- **Belastingdienst**. Het betreft een overeenkomst om de continuïteit van de Installed Base Middleware, na afloop van de huidige raamovereenkomst, te kunnen waarborgen. Het betreft het leveren van Onderhoud en Support op de Installed Base van de Middleware infrastructuur (hierna Installed Base), het verlenen van Productspecifieke Diensten en het leveren van opleidingen voor producten uit de Installed Base.
- **Bizob**. De opdracht omvat beheer-, advies- en projectwerkzaamheden met betrekking tot de ICT-infrastructuur van Veiligheidsregio Brabant Zuidoost. Hierbij worden de volgende diensten onderscheiden:
    - Managed netwerkbeheer: het beheer van het lokale netwerk;

- adviserend beheer: periodiek advies over de status van toegepaste hardware en software van derden;
- ondersteunend beheer: derdelijns support om verstoringen te verhelpen;
- bemensing service desk: het plaatsen van beheerders op de service desk van VRBZO;
- projecten: de uitvoering van projectmatige werkzaamheden op basis van nader overeen te komen opdrachten.

3.3. 'Pas toe' per open standaard

Voor de mate waarin om een open standaard wordt gevraagd (wanneer die voor de aanbesteding relevant is) biedt Tabel 1 al een eerste indicatie. Bij 40 aanbestedingen was dit jaar in totaal 487 keer een open standaard relevant, en in 264 gevallen (54%) werd bij de aanbesteding daadwerkelijk om die standaard(en) gevraagd. Om deze cijfers in het juiste perspectief te plaatsen het volgende:

- het aantal relevant geachte standaarden per aanbesteding is gemiddeld (wederom) hoger dan vorig jaar (12,2 dit jaar tegen 11,6 standaarden per aanbesteding vorig jaar, nadat de drie jaren daarvoor ook al sprake was van een flinke stijging); terwijl het aantal standaarden op de lijst min of meer vergelijkbaar is met vorig jaar;
- het percentage daarvan dat is uitgevraagd is 54%, dat is hoger dan vorig jaar (toen 45%);
- de combinatie van bovenstaande twee constateringen betekent dat er dit jaar per aanbesteding gemiddeld meer standaarden zijn uitgevraagd dan vorig jaar (6,6 dit jaar, versus 5,2 vorig jaar);
- en het betekent dat er dit jaar minder relevant geachte standaarden NIET uitgevraagd zijn: het gemiddelde aantal niet-gevraagde standaarden per aanbesteding is dit jaar 5,6 (vorig jaar: 6,4). Dit is een duidelijke verbetering.

Dit is ook terug te zien in de scores voor 'Pas toe' per afzonderlijke standaard (zie Tabel 4). Het aantal standaarden dat beter is uitgevraagd dan vorig jaar is duidelijk hoger dan het aantal standaarden dat juist minder goed uitgevraagd is.

Andere zaken die opvallen bij nadere beschouwing van Tabel 4:

- Twaalf standaarden zijn vaker gevraagd dan gemiddeld (dus meer dan 54%): HTTPS & HSTS, ISO 27001/02, SAML, TLS, Digitoegankelijk, PDF, NLCIUS, SETU, Digikoppeling, Geo-stadaarden en StUF. In vergelijking met vorig jaar zijn WPA2Enterprise, Open API Specification, XBRL, COINS en ECLI uit dit rijtje verdwenen (CMIS ook maar die standaard staat dit jaar niet meer op de PToLU-lijst). Deze vijf standaarden waren vorig jaar alle nog nieuwkomers in dit rijtje. Nieuwkomers in dit jaar zijn NLCIUS, SETU, Digikoppeling en de Geo-standaarden.
- Deze nieuwkomers komen we meer dan incidenteel tegen bij aanbestedingen, variërend van 4 tot 12 keer op een totaal van dit jaar 40 onderzochte aanbestedingen.

Tabel 4: 'Pas toe' bij aanbestedingen in 2e helft 2020, per standaard

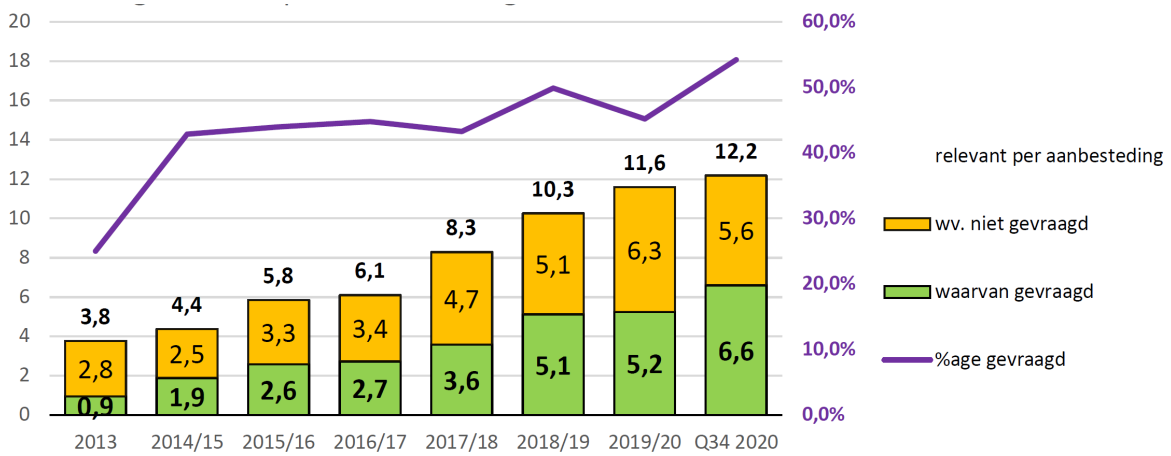
	Rijksoverheid		Mede-overheden		**Totaal 2e helft 2020**		2019/2020
	relevant	gevraagd in % relevant	relevant	gevraagd in % relevant	relevant	gevraagd in % relevant	gevraagd in % relevant
aantal aanbestedingen:	*20*		*20*		***40***		*72*
Internet & beveiliging:							
DKIM	11	45%	19	37%	**30**	**40%**	24%
DMARC	11	45%	19	37%	**30**	**40%**	24%
DNSSEC	14	36%	19	26%	**33**	**30%**	27%
HTTPS en HSTS	16	81%	19	63%	**35**	**71%**	58%
IPv6 en IPv4	16	25%	17	12%	**33**	**18%**	7%
NEN-ISO\IEC 27001:2005nl	19	100%	20	95%	**39**	**98%**	83%
NEN-ISO\IEC 27002:2007nl	19	100%	20	95%	**39**	**98%**	83%
NL GOV Assurance	1	0%	2	0%	**3**	**0%**	
RPKI	0		0		**0**		
SAML	8	63%	14	50%	**22**	**55%**	59%
SPF	11	45%	19	37%	**30**	**40%**	24%
STARTTLS en DANE	11	36%	19	26%	**30**	**30%**	16%
STIX en TAXII	1	0%	0		**1**	**0%**	
TLS	16	81%	19	63%	**35**	**71%**	58%
WPA2 Enterprise	0		0		**0**		100%
Document & (web)content:							
Ades Baseline Profiles	2	50%	0		**2**	**50%**	25%
Digitoegankelijk *)	10	80%	7	43%	**17**	**65%**	60%
ODF	7	0%	14	0%	**21**	**0%**	10%
OWMS	2	50%	0		**2**	**50%**	
PDF	12	75%	9	100%	**21**	**86%**	59%
SKOS	0		0		**0**		
REST API's:							
OpenAPI Specification	7	43%	3	0%	**10**	**30%**	60%
REST_API Design Rules	4	0%	2	0%	**6**	**0%**	
E-facturatie & administratie:							
NLCIUS	3	100%	1	100%	**4**	**100%**	25%
SETU	4	50%	1	100%	**5**	**60%**	0%
WDO Datamodel	0		0		**0**		
XBRL	1	100%	2	0%	**3**	**33%**	100%
Stelselstandaarden:							
Digikoppeling	3	33%	9	78%	**12**	**67%**	33%
Geo−standaarden	3	67%	4	50%	**7**	**57%**	33%
StUF	0		13	85%	**13**	**85%**	100%
Water & Bodem:							
Aquo Standaard	0		0		**0**		
GWSW	0		0		**0**		
SIKB 0101	1	0%	0		**1**	**0%**	
SIKB 0102	0		0		**0**		
Bouw:							
COINS	0		0		**0**		50%
IFC	1	0%	0		**1**	**0%**	33%
NLCS	0		0		**0**		0%
Visi	0		0		**0**		
Juridische verwijzingen:							
BWB	0		0		**0**		0%
ECLI	0		0		**0**		50%
JCDR	0		0		**0**		0%
Onderwijs & loopbaan:							
E−portfolio	2	0%	0		**2**	**0%**	0%
NL LOM	0		0		**0**		0%
Overig:							
EML_NL	0		0		**0**		0%
Totaal	216	59%	271	50%	**487**	**54%**	45%

- Vorig jaar was bij drie van de standaarden die behoorlijk vaak relevant waren (> 10 keer) het percentage gevraagd flink gestegen (meer dan 10%). Als we die criteria ook nu zouden toepassen, komen we uit op 11 standaarden. Vanwege de hogere uitvraag dit jaar ligt de lat nu bij een stijging van meer dan 15%. Een vijftal standaarden voldoet dit jaar aan het aangescherpte criterium: DKIM, DMARC, SPF, PDF en Digikoppeling.
- Bij de andere standaarden die vaak relevant waren (> 10 keer), vinden we vier dalers terug: SAML, ODF, Open API Specification en StUF. Bij StUF past in die zin een kanttekening dat die standaard vorig jaar een maximale uitvraag scoorde van 100%.
- Een opvallende uitschieter in negatieve zin in dit rijtje is de ODF-standaard. Deze is maar liefst 21 (van de 40) keer relevant geacht maar werd in geen enkel geval uitgevraagd.
- Eerder is al opgemerkt dat met name bij het Rijk het overall uitvraag-percentage flink is gestegen, van 39 % naar 59 %. Deze toename wordt grotendeels verklaard door het veel hogere uitvraag-percentage van DKIM, DMARC, SPF, STARTTLS & DANE en PDF.

Als we iets verder terugkijken in de tijd, dan blijkt het aantal standaarden dat (gemiddeld) per aanbesteding relevant is elk jaar gestaag te groeien: van 4,4 in 2015 tot 12,2 in de 2e helft van 2020 (zie Figuur 5).

Het percentage dat daarvan gevraagd werd ligt sinds 2015 ruwweg rond de 45% (zie de paarse lijn en de bijbehorende percentage-schaal). Gemiddeld wordt dus om iets minder dan de helft van de relevante standaarden gevraagd, maar er zijn wel ieder jaar meer standaarden relevant. De score van deze monitor (54%) steekt hier dus boven uit.

Figuur 5: Aantal relevante standaarden bij aanbestedingen, 2013-2020



De gestage groei van het aantal relevante standaarden per aanbesteding is slechts voor een klein deel te verklaren doordat er meer standaarden op de lijst komen te staan: in 2013 stonden er 34 standaarden op de lijst en ten behoeve van deze monitor 2e helft 2020 waren het er 44. De lijst groeide dus per saldo met 29 %. Dat is slechts een fractie van de toename van het aantal relevante standaarden (voor de 2e helft 2020 ruim 3 keer zoveel als in 2013). Een beperkt deel van de verklaring is, dat er enkele standaarden van de lijst afgevoerd zijn waarvan de meeste niet erg vaak relevant waren en tegelijkertijd er nieuwe standaarden op de lijst zijn gezet die vaak relevant zijn (uit het domein Internet & beveiliging). Overigens zijn er ook nieuwe standaarden op de lijst gekomen die niet bovengemiddeld vaak relevant zijn.

De voornaamste verklaring lijkt te zijn, dat een aantal standaarden de afgelopen jaren geleidelijk vaker relevant is geworden, en dat geldt het sterkste voor de standaarden uit het domein Internet & beveiliging. De 15 standaarden uit dit domein (eenderde van de lijst) zijn goed voor een belangrijk deel van het aantal keer relevant: in totaal was 487 keer een standaard relevant en daarvan betrof het 360 keer (74 %, vrijwel gelijk aan vorig jaar) een standaard uit het domein Internet & beveiliging.

Daarnaast (en mogelijk daarmee samenhangend): de toename van het aantal relevante standaarden per aanbesteding kan heel goed te maken hebben met veranderingen in de ICT, zoals bijvoorbeeld een toename van het aantal SAAS-applicaties.

3.4. Welke open standaarden waren relevant bij aanbestedingen

In het onderzoek is van elke aanbesteding vastgesteld welke standaarden van de 'pas-toe-of-leg-uit'-lijst daarvoor relevant waren. Dat levert ook interessante informatie op vanuit het perspectief van de adoptie van standaarden. In Tabel 6 is weergegeven hoe vaak elk van de standaarden van de lijst relevant is gebleken bij een aanbesteding.

Van de 44 standaarden op de lijst voor 'pas toe of leg uit' zijn er 29 (dus tweederde van de lijst) minimaal bij één aanbesteding relevant (vorig jaar waren dat er beduidend meer: toen 33 van de 41 = 80%). De andere 15 standaarden op de lijst waren dus dit jaar voor geen van de 40 onderzochte aanbestedingen relevant. Daarvan waren er vijf ook vorig jaar voor geen enkele onderzochte aanbesteding relevant: SKOS, WDO Datamodel, Aquo, SIKB 0102 en Visi. Acht standaarden (WPA2 Enterprise, COINS, NLCS, BWB, ECLI, JCDR, NL LOM en EMN_NL) waren bij de vorige monitor wel relevant, zij het heel marginaal. De resterende twee standaarden (GWSW en RPKI) zijn vorig jaar nog niet in de beoordeling van aanbestedingen meegenomen vanwege hun (indertijd) recente plaatsing op de PTOLU-lijst.

Een viertal standaarden steekt er met kop en schouders bovenuit als het gaat om de mate waarin zij relevant worden geacht: ISO 27001en ISO 27002 zijn bijna altijd relevant (98%) en ook TLS en HTTPS & HSTS (beide 88%). Deze standaarden vormden ook vorig jaar de kopgroep. Als we als criterium aanhouden ‘bij meer dan 50% van de 40 aanbestedingen relevant’, dan kunnen aan dit rijtje nog negen standaarden worden toegevoegd: DNSSEC (83%), IPv4 & IPv6 (83%), DKIM, DMARC, SPF en STARTTLS & DANE (alle 75%), SAML (55%), PDF (53%) en ODF (ook 53%). Alleen ODF is nieuw in dit rijtje.

Daarna volgt een groep van vier standaarden die bij 25 tot 50% van de aanbestedingen relevant was: Digitoegankelijk (43%), StUF (33%), Digikoppeling (30%) en Open API Specification (25%). Het geheel overziend is sprake van een behoorlijk constante groep standaarden die relatief vaak relevant zijn. Echte uitschieters zitten er niet tussen. Als we als criterium aanhouden een verschil van 10% zien we dit alleen terug bij ODF (+ 13%) en Open API Specification (+ 11%).

Tabel 6: Open standaarden relevant / gevraagd bij aanbestedingen in 2e helft 2020

(Bron: onderzoek aanbestedingen juli t/m december 2020, uitgevoerd zomer 2021)

	Rijksoverheid relevant in % aanbest.n	gevraagd in % aanbest.n	Mede-overheden relevant in % aanbest.n	gevraagd in % aanbest.n	**Totaal 2e helft 2020** relevant in % aanbest.n	gevraagd in % aanbest.n
aantal aanbestedingen:	*20*		*20*		***40***	
Internet & beveiliging:						
DKIM	55%	25%	95%	35%	**75%**	**30%**
DMARC	55%	25%	95%	35%	**75%**	**30%**
DNSSEC	70%	25%	95%	25%	**83%**	**25%**
HTTPS en HSTS	80%	65%	95%	60%	**88%**	**63%**
IPv6 en IPv4	80%	20%	85%	10%	**83%**	**15%**
NEN-ISO\IEC 27001:2005nl	95%	95%	100%	95%	**98%**	**95%**
NEN-ISO\IEC 27002:2007nl	95%	95%	100%	95%	**98%**	**95%**
NL GOV Assurance	5%	0%	10%	0%	**8%**	**0%**
RPKI	0%		0%		**0%**	
SAML	40%	25%	70%	35%	**55%**	**30%**
SPF	55%	25%	95%	35%	**75%**	**30%**
STARTTLS en DANE	55%	20%	95%	25%	**75%**	**23%**
STIX en TAXII	5%	0%	0%		**3%**	**0%**
TLS	80%	65%	95%	60%	**88%**	**63%**
WPA2 Enterprise	0%		0%		**0%**	
Document & (web)content:						
Ades Baseline Profiles	10%	5%	0%		**5%**	**3%**
Digitoegankelijk *)	50%	40%	35%	15%	**43%**	**28%**
ODF	35%	0%	70%	0%	**53%**	**0%**
OWMS	10%	5%	0%		**5%**	**3%**
PDF	60%	45%	45%	45%	**53%**	**45%**
SKOS	0%		0%		**0%**	
REST-API's:						
OpenAPI Specification	35%	15%	15%	0%	**25%**	**8%**
REST-API Design Rules	20%	0%	10%	0%	**15%**	**0%**
E-facturatie & administratie:						
NLCIUS	15%	15%	5%	5%	**10%**	**10%**
SETU	20%	10%	5%	5%	**13%**	**8%**
WDO Datamodel	0%		0%		**0%**	
XBRL	5%	5%	10%	0%	**8%**	**3%**
Stelselstandaarden:						
Digikoppeling	15%	5%	45%	35%	**30%**	**20%**
Geo−standaarden	15%	10%	20%	10%	**18%**	**10%**
StUF	0%		65%	55%	**33%**	**28%**
Water & Bodem:						
Aquo Standaard	0%		0%		**0%**	
GWSW	0%		0%		**0%**	
SIKB 0101	5%	0%	0%		**3%**	**0%**
SIKB 0102	0%		0%		**0%**	
Bouw:						
COINS	0%		0%		**0%**	
IFC	5%	0%	0%		**3%**	**0%**
NLCS	0%		0%		**0%**	
Visi	0%		0%		**0%**	
Juridische verwijzingen:						
BWB	0%		0%		**0%**	
ECLI	0%		0%		**0%**	
JCDR	0%		0%		**0%**	
Onderwijs & loopbaan:						
E−portfolio	10%	0%	0%		**5%**	**0%**
NL LOM	0%		0%		**0%**	
Overig:						
EML_NL	0%		0%		**0%**	

Aan de andere kant: van de 29 standaarden die bij de beoordeelde aanbestedingen relevant werden geacht, zijn er dit jaar 6 slechts incidenteel (1 of 2 keer) als relevant aangemerkt (vorig jaar waren dat er 7): Ades Baseline Profiles, OWMS en E Portfolio elk twee keer relevant en STIX & TAXII, SIKB0101en IFC elk één keer. In vergelijking met vorig jaar is bij dit rijtje geen sprake van enige overlap.

Eerder in dit hoofdstuk is al opgemerkt dat het aantal relevant geachte standaarden per aanbesteding hoger ligt dan vorig jaar. Dit valt ook terug te lezen in Tabel 6: de meeste standaarden scoren een hoger percentage 'relevant' dan vorig jaar. Er zijn niet echt uitschieters, of het moeten de eerder gememoreerde standaarden ODF en Open API specification zijn (zie vlak boven tabel 6). Bij veel standaarden is een stijging waar te nemen maar onder de 10%. Uitschieters de andere kant op – veel minder vaak 'relevant' dan vorig jaar – zijn er niet.

In vergelijking met de vorige monitor zijn er zoals eerder al opgemerkt acht standaarden deze keer bij geen enkele aanbesteding relevant gebleken en vorig jaar wel: WPA2 Enterprise, COINS, NLCS, BWB, ECLI, JCDR, NL LOM en EMN_NL. Daarbij moet wel worden aangetekend dat de relevantie van deze standaard vorig jaar ook al niet groot was. Andersom zijn er drie standaarden dit jaar wel relevant en vorig jaar niet (afgezien van de standaarden die vorig jaar vanwege recente plaatsing op de lijst niet waren meegenomen). Hierbij gaat het om STIX & TAXII, OWMS en SIKB0101.

Voor de feitelijke adoptie is uiteraard niet alleen van belang hoe vaak de standaard relevant bleek te zijn, maar vooral hoe vaak er daadwerkelijk om is gevraagd. Zoals al bleek in paragraaf 3.2 is er dit jaar bij aanbestedingen vaker dan vorig jaar om de relevante standaarden gevraagd: 54% dit jaar tegen 45% vorig jaar. In Tabel 6 is voor de afzonderlijke standaarden berekend hoe vaak daarom is gevraagd in % van het aantal aanbestedingen. De hoogste scores zijn in de betreffende kolom terug te vinden bij: NEN-ISO\IEC 27001/27002 (95% voor beide), HTTPS & HSTS (63%) TLS (63%) en PDF (45%). De afgelopen drie jaren stonden dezelfde vijf standaarden op dit punt bovenaan.

Na dit rijtje koplopers volgt nog een tiental standaarden met een score boven de 10%: DKIM, DMARC, SPF en ook SAML (30%), Digitoegankelijk en StUF (28%), DNSSEC (25%), STARTTLS & DANE (23%), Digikoppeling (20%) en IPv4 & IPv6 (15%). Digikoppeling en IPv4 en IPv6 zijn nieuw in dit rijtje, CMIS is verdwenen (van de Ptolu-lijst af). IPv4 & IPv6 behoorde vorig jaar nog tot de afvallers in deze opsomming.

Om de andere standaarden is slechts bij enkele aanbestedingen gevraagd of zelfs in het geheel niet. Dit laatste is het geval bij NL GOV Assurance, STIX & TAXII, ODF, REST-API Design Rules, SIKB010, IFC en E portfolio. Deze 0%-scores doen zich dit jaar ook voor bij enkele standaarden die meer dan twee keer als relevant zijn aangemerkt. Dit betreft NL GOV Assurance, ODF en REST-API Design Rules.

3.5. 'Leg uit' bij aanbestedingen

Voor twee sets van beoordeelde aanbestedingen is nagegaan in hoeverre inmiddels 'leg uit' plaatsgevonden heeft in jaarverslagen over 2020: de aanbestedingen uit Q3 en Q4 2020 die

in deze Monitor 2021 zijn beoordeeld èn voor de set aanbestedingen uit Q1 en Q2 2020 die vorig jaar zijn beoordeeld (in het kader van de Monitor 2020).

3.5.1. 'Leg uit' voor aanbestedingen uit Q3+Q4 2020 (dit jaar beoordeeld)

Bij vier aanbestedingen die in het kader van deze monitor 2021 zijn beoordeeld, is om alle relevante standaarden gevraagd. Bij de andere 36 aanbestedingen moet dus in het jaarverslag verantwoording afgelegd worden ('Leg uit') voor het niet toepassen van de relevante standaard(en). Voor deze 36 aanbestedingen (door 31 verschillende overheidsorganisaties: 13 vallend onder Rijk, waarvan dit jaar 7 ministeries, en 18 Medeoverheden) is in het Jaarverslag 2020 nagegaan of 'leg-uit' is toegepast. Van 'Leg uit' was in de jaarverslagen van deze 31 overheidsorganisaties echter geen sprake, in die zin dat in geen van de jaarverslagen een concrete aanbesteding wordt genoemd uit het voorliggende onderzoek waarbij van de lijst voor 'pas toe of leg uit' werd afgeweken.

Bij de decentrale overheden waarvan aanbestedingen zijn onderzocht is in de jaarverslagen c.q. jaarstukken (voor zover beschikbaar) vrijwel geen enkele verwijzing naar het open standaardenbeleid teruggevonden. Bij één gemeente wordt expliciet melding gemaakt van het bestaan van de Generieke Digitale Infrastructuur, overigens alleen in algemene termen. Van vier (van de 18) aanbestedende partijen is op de website geen jaarverslag 2020 (of een variant daarop) aangetroffen.

Bij de departementen ligt dat genuanceerder. Er is naar de jaarverslagen van alle 12 ministeries gekeken, hoewel strikt genomen alleen de volgende zeven departementen onderwerp van onderzoek zijn: Binnenlandse Zaken en Koninkrijksrelaties, Buitenlandse Zaken, Financiën (met inbegrip van de Belastingdienst), Defensie, Economische Zaken en Klimaat (lees: RVO), Onderwijs, Cultuur en Welzijn (lees: DUO) en Infrastructuur en Waterstaat (lees: RWS). Van deze zeven departementen zijn namelijk aanbestedingen beoordeeld uit Q3+Q4 2020, met een beoordeling die noodzaakt tot 'leg uit'.

Het overall-beeld voor 'Leg uit' door de 12 departementen is als volgt:

- Zeven ministeries (vorig jaar zes) hebben een vorm van verantwoording opgenomen in het jaarverslag 2020. Er is daarbij sprake van één nieuwkomer (het ministerie van Sociale Zaken en Werkgelegenheid). Voor het overige is het beeld op hoofdlijnen hetzelfde.
- Een viertal ministeries gaat relatief uitgebreid in op het beleid rond open standaarden, overigens zonder op concrete aanbestedingen in te gaan. Dit zijn de ministeries van Binnenlandse Zaken en Koninkrijksrelaties, Infrastructuur en Waterstaat, Onderwijs, Cultuur en Welzijn en Volksgezondheid, Welzijn en Sport. De drie eerstgenoemde ministeries geven daarbij expliciet aan dat niet is afgeweken van de afspraken rond het gebruik van open standaarden.
- De ministeries van Algemene Zaken, Defensie en Sociale Zaken en Werkgelegenheid zijn heel summier, zij melden alleen dat geen sprake is geweest van afwijkingen van de voorschriften.
- Een vijftal ministeries dat dit jaar niets meldt over het gebruik van open standaarden deed dat vorig jaar ook niet. Uit het overzicht hieronder valt af te leiden dat het gaat om de ministeries van Economische Zaken en Klimaat, Financiën, Buitenlandse Zaken, Justitie en Veiligheid en Landbouw, Natuur en Visserij.

In een enkel geval is dus sprake van een verklaring, dat niet was afgeweken van de Instructie Rijksdienst, en blijft daartoe ook beperkt. Enkele ministeries gaan verder en zijn in algemene bewoordingen ingegaan op het open standaardenbeleid en de wijze waarop zij daar invulling aan geven. In onderstaand overzicht zijn de bevindingen samengebracht.

[A] 'Leg uit' is voor één of meer aanbestedingen noodzakelijk

Ministerie	Uitvoering 'leg uit'
BZK	Open standaarden en open source software Ook het Ministerie van BZK heeft in 2020 gehandeld conform artikel 3, eerste lid van de «Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten». Er zijn in de regel geen nieuwe ICT-diensten of -producten aangeschaft waarbij is afgeweken van de open standaarden op de «pas toe of leg uit»- lijst van het Forum Standaardisatie. BZK stimuleert rijksbreed het gebruik van open source software. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf, onder paragraaf 2)*
BUZA	[Geen]
DEF	Gebruik open standaarden en open source software Er is in 2020 niet afgeweken van het voorschrift. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf, onder paragraaf 2)*
EZK	[Geen]
FIN	[Geen]
I&W	Gebruik open standaarden en open source software In 2020 is er niet afgeweken van het gebruik van de door het Forum Standaardisatie voorgeschreven open standaarden bij het verwerven of (door)ontwikkelen van de informatievoorziening van IenW. Net als in voorgaande jaren stuurt IenW op de toepassing daarvan bij het Werken onder Architectuur: de van toepassing zijnde open standaarden worden Tweede Kamer, vergaderjaar 2020–2021, 35 830 XII, nr. 1 179 opgenomen in de architectuurdocumenten van het betreffende project en worden vertaald naar eisen in de documenten t.b.v. inkoop of aanbesteding. Om de toepassing van open standaarden ten aanzien de Digitale Toegankelijkheid kracht bij te zetten, is binnen IenW een Handreiking en een Praktische Toepassing Verplichte Eisen aan Digitale Voorzieningen opgesteld. Hierin worden richtlijnen vertaald naar toepasbare, concrete eisen voor aanbestedings- en ontwerpdocumenten . IenW hanteert een in 2011 vastgestelde Open Source strategie die aangeeft dat - in geval van gelijke geschiktheid - bij verwerving of (door)ontwikkeling van de informatievoorziening, de voorkeur uitgaat naar de toepassing van Open Source Software. Ook hier is in 2020 niet van afgeweken. *(Bron: 6. Bedrijfsvoeringsparagraaf, onder paragraaf 2)*
OCW	Gebruik open standaarden en open source software De Instructie Rijksdienst schrijft voor dat bij de aanschaf en ontwikkeling van ICT-diensten of ICT-producten in beginsel gebruik moet worden gemaakt van open standaarden van de lijst van het Forum Standaardisatie (www.forumstandaardisatie.nl). Valide afwijkingsgronden zijn opgenomen in de Instructie Rijksdienst. Als er sprake is van afwijking van de Instructie Rijksdienst dan wordt dit gemotiveerd aangegeven. Bij het Ministerie van OCW is bij meting eind 2020 geen sprake geweest van afwijking van de Instructie Rijksdienst *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf onder 2)*

[B] Geen aanbestedingen beoordeeld waarvoor 'Leg uit' noodzakelijk is

Ministerie	Uitvoering 'leg uit'
AZ	Gebruik open standaarden en open source software Er zijn geen bijzonderheden te melden. *(Bron: B Beleidsverslag onder 5: bedrijfsvoeringsparagraaf, meerdere plaatsen.)*
J&V	[Geen]
LNV	[Geen]
SZW	Open standaarden en open source software Geen bijzonderheden te melden. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf, onder paragraaf 2)*
VWS	Gebruik open standaarden en open source software Binnen het concern VWS wordt gestreefd naar het gebruik van open standaarden. In een aantal gevallen, bijvoorbeeld precaire bedrijfsvoering met gevoelige informatie, is het gestandaardiseerd uitwisselen van gegevens niet altijd mogelijk en/of verantwoord. Ditzelfde principe geldt voor functionele inkoop van software binnen VWS. Indien het proces kan voldoen aan alle denkbare wensen en eisen van de gebruikers aan het informatiesysteem, hebben open source-oplossingen de voorkeur en worden als wens in het programma van eisen opgenomen. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf onder 2)*

3.5.2. 'Leg uit' voor aanbestedingen uit Q1+Q2 2020 (vorig jaar beoordeeld)

In de vorig jaar verschenen Monitor 2020 zijn onder andere aanbestedingen beoordeeld uit Q1+Q2 2020. Voor 35 van deze aanbestedingen was 'leg uit' aan de orde maar dat kon op dat moment nog niet onderzocht worden. Dat onderzoek heeft nu plaatsgevonden, omdat de Jaarverslagen 2020 nu wèl beschikbaar zijn.

Deze 35 aanbestedingen (door 28 overheidsorganisaties, waarvan 6 ministeries) zijn als volgt verdeeld: 16 aanbestedingen 'Rijk' en 19 aanbestedingen 'medeoverheden'. Van 'Leg uit' in strikte zin was in de jaarverslagen van deze 35 overheidsorganisaties evenmin sprake. In geen van de jaarverslagen wordt een concrete aanbesteding genoemd waarbij volgens het onderzoek van vorig jaar van de lijst voor 'pas toe of leg uit' werd afgeweken.

Evenals in voorgaande jaren kan worden vastgesteld dat de regels met betrekking tot 'leg uit' er nog niet toe hebben geleid, dat overheden zich in jaarverslagen over specifieke aanbestedingen (en daarvoor relevante open standaarden) verantwoorden voor het niet toepassen van relevante open standaarden. In vergelijking met de verslaglegging over 2019 in de Monitor 2020 valt (wederom) op dat dit jaar slechts bij één departement meer dan een verwijzing naar het beleid rond de toepassing van open standaarden is verschenen.

Sinds enkele jaren informeren wij aanbesteders over de beoordeling van hun aanbesteding en in het verlengde daarvan interviewen wij bovendien enkele van hen. Met sommige van de aanbesteders bespreken wij de beoordeling uitgebreider, en dat leidt soms nog tot een (beperkte) aanpassing van de beoordeling. Hoewel dit geen alternatief is voor 'Leg Uit', blijkt het wel in een behoefte te voorzien en bovendien interessante inzichten op te leveren.

4. Toepassing van open standaarden via voorzieningen

4.1. Over dit deelonderzoek

4.1.1. Waarom overheidsbrede voorzieningen relevant zijn

Elke afzonderlijke overheidsorganisatie is primair zelf verantwoordelijk voor het toepassen van open standaarden. Voor een deel van hun informatiesystemen maken overheden echter gebruik van overheidsbrede voorzieningen, zoals de voorzieningen van de basisinfrastructuur (vroeger: GDI), shared services et cetera, die door verschillende lagen van de overheid en daarbuiten ingezet kunnen worden. Zie EAR Online voor een overzicht geordend naar informatiseringsdomeinen. Deze voorzieningen kunnen door alle lagen van de overheid en daarbuiten ingezet worden. Sommige worden door allerlei publieke organisaties toegepast, andere vooral door de Rijksoverheid of vooral door mede-overheden. Als in voorzieningen de relevante open standaarden zijn toegepast, dan leidt dat ook elders tot een breder gebruik van die open standaarden. Daarom is dit jaar opnieuw onderzocht in hoeverre belangrijke overheidsbrede voorzieningen voldoen aan de relevante open standaarden.

Tot vorig jaar onderzochten wij een grote en gevarieerde verzameling van 35 voorzieningen elk jaar opnieuw. Inmiddels voldoen veel voorzieningen aan een redelijk groot deel van alle voor hen relevante voorzieningen. Het blijft belangrijk om de toepassing van open standaarden bij deze voorzieningen te blijven volgen, maar dat hoeft niet meer per sé jaarlijks. Een lagere frequentie biedt ook meer ruimte voor de implementatie van de standaarden, inclusief nieuwe standaarden op de lijst. En het beperkt de administratieve lasten voor de voorziening-beheerders.

Met ingang van 2020 onderzoeken we daarom het ene jaar een deel van de voorzieningen en het andere jaar de andere voorzieningen. Dat bood de gelegenheid om een logische tweedeling aan te brengen: tussen voorzieningen die direct raken aan de communicatie en gegevensuitwisseling met burgers en bedrijven en voorzieningen die vooral gericht zijn op de communicatie en gegevensuitwisseling tussen overheden onderling dan wel op de onderliggende infrastructuur.

Daarnaast voerden wij de afgelopen drie jaar telkens met zes beheerders van voorzieningen verdiepende gesprekken over de praktijk van adoptie van de relevante open standaarden, om de knelpunten en/of succesfactoren te achterhalen.

Dit deelonderzoek is uitgevoerd door Piet Hein Minnecré, Anne Graas en Jinne Samsom (PBLQ). In Bijlage B4 is de rapportage opgenomen met alle gedetailleerde informatie per onderzochte voorziening.

4.1.2. Welke voorzieningen zijn onderzocht?

Dit jaar zijn de 19 voorzieningen onderzocht die relevant zijn voor de gegevensuitwisseling en communicatie tussen overheden en/of voor de onderliggende infrastructuur, voorzieningen dus waarbij interoperabiliteit cruciaal is. Ten opzichte van het vorige onderzoek van deze voorzieningen (zie de Monitor Open standaarden 2019) zullen twee voorzieningen niet meer onderzocht worden: Rijkspas en P-Direct.

Het gaat om de volgende voorzieningen (linker kolom):

Dit jaar onderzocht: **Gegevensuitwisseling tussen overheden en onderliggende infrastructuur (19)**	*Vorig jaar onderzocht:* Gegevensuitwisseling en communicatie met burgers en bedrijven (17)
Identificeren en authenticeren	*Identificeren en authenticeren*
• BSN Beheervoorziening + GBA-V	• DigiD • DigiD Machtigen • Afsprakenstelsel ETD • PKI Overheid
Dienstverlening en informatieverstrekken	*Dienstverlening en informatieverstrekken*
• Doc-Direct • Rijksportaal	• MijnOverheid • Berichtenbox bedrijven • Overheid.nl • Ondernemersplein • Samenwerkende Catalogi • Rijksoverheid.nl / web-domein • Rijksoverheid.nl / email-domein • website RDW.nl (voertuigen) • website WOZ-waardeloket.nl
Gegevens en registreren	*Gegevens en registreren*
• BAG, BRK, BGT, WOZ en BRT • BRI (inkomen) • BRO (ondergrond) • BRV (voertuigen) • NHR (Nieuw HandelsRegister) • Digilevering • Digimelding • Stelselcatalogus	• website Handelsregister KvK (NHR) • website PDOK (open geo-data)
Dienstverlening en verbinden	*Dienstverlening en verbinden*
• DigiPoort • Diginetwerk • Digitale Werkomgeving Rijk	• TenderNed • Digi-Inkoop

4.1.3. Werkwijze

Voor dit onderzoek is gebruik gemaakt van de 'pas toe of leg uit'-lijst van 1 april 2021. Voor elke voorziening is (samen met de beheerder) gekeken of de standaarden op deze lijst relevant zijn. Daarbij is telkens uitgegaan van de eindgebruiker. Dat is degene die in de keten baat zou moeten hebben bij het gebruik van open standaarden. Dit is expliciet zo gekozen, omdat het beleid ten aanzien van standaardisatie vooral gericht is op het stimuleren van interoperabiliteit. In eerdere onderzoeken is gebleken dat beheerders van voorzieningen soms terminologie gebruiken zoals 'voorbereid' zijn op een standaard, het 'deels geïmplementeerd' hebben of 'standaard xyz-ready zijn'. Hiermee bedoelen zij dat ze zelf voldoen aan de standaard of bezig zijn de standaard te implementeren, maar dat de andere partijen in hun keten nog geen gebruik kunnen maken van de standaard. Er is bijgevolg dan ook geen sprake van interoperabiliteit op basis van gebruik van de standaard. Wanneer er geen sprake is van interoperabiliteit hebben we dat in deze rapportage aangegeven.

In dit onderzoek wordt per voorziening een overzicht opgesteld van relevante standaarden en de mate waarin daarvan gebruik wordt gemaakt. Het vertrekpunt daarbij is telkens het overzicht van het vorige meetmoment, in dit geval dus 2019. Waar mogelijk zijn de

standaarden opnieuw getoetst. Daarbij maken we onder meer gebruik van de testen die beschikbaar zijn via internet.nl en RIPEstat. Hiermee kan voor een groot deel van de standaarden getoetst worden of eraan voldaan wordt. Daarnaast kijken we – voor zover mogelijk – of de geplande activiteiten inmiddels uitgevoerd zijn. Voor nieuwe standaarden op de lijst maken we in samenspraak met de beheerders een inschatting of ze relevant zijn voor de voorzieningen.

Op basis van bovenstaande inschattingen en toetsen maken we een eerste overzicht per voorziening. Dat overzicht wordt met een aantal expliciete vragen toegestuurd aan de beheerders van de voorzieningen. Op basis van hun reactie wordt de verzamelde informatie aangescherpt. Het resultaat daarvan wordt voorgelegd aan de opdrachtgever, vervolgens in een definitieve versie toegestuurd aan de beheerders van de voorzieningen en na akkoord opgenomen in de rapportage. Meestal heeft dit proces meerdere iteraties nodig. Daar waar verschillen van mening zijn over het al dan niet voldoen aan de standaarden zijn deze verschillen nader met elkaar besproken. In de gevallen waar de verschillen ook na de gesprekken bleven bestaan, is dit duidelijk opgenomen in de rapportage.

4.1.4. Aandachtspunten voor de lezer

Voorzieningen en standaarden geordend op basis van functionaliteit

De voorzieningen in deze monitor zijn op basis van functionaliteit gegroepeerd. De volgende functionele groepen worden in deze monitor onderscheiden:

- Identificeren en authenticeren
- Dienstverlening en informatieverstrekken
- Gegevens en registreren
- Dienstverlening en verbinden

Status

In de rapportage is per voorziening een tabel opgenomen. Daarin staan de standaarden genoemd die relevant zijn voor de voorzieningen en de status van de standaard zoals toegekend door de onderzoekers. De status kan de volgende waarden hebben:

- Ja: De voorziening is conform de standaard,
- Nee: De voorziening is niet conform de standaard,
- Deels: Onderdelen van de voorziening zijn conform aan de standaard, maar niet alle onderdelen,
- Gepland: Er zijn concrete plannen (gekoppeld aan een datum) om de voorziening op korte termijn conform te maken aan de standaard.

Relevantie van de standaard

Voor de relevantiebepalingen zijn per standaard de beschrijvingen van het functioneel en organisatorisch toepassingsgebied zoals vermeld op de pas toe of leg uit-lijst van het Forum Standaardisatie gehanteerd. Standaarden die niet relevant zijn voor een voorziening zijn niet in de tabel opgenomen. In een beperkt aantal gevallen is onder de tabel nog een toevoeging opgenomen over standaarden die in de eerste inschatting wel relevant leken, maar dat bij nadere inspectie (nog) niet zijn. Ook in gevallen waar verwarring zou kunnen ontstaan over de relevantie is een nadere toelichting onder de tabel opgenomen. Daarnaast is voor de standaarden die dit jaar nieuw zijn op de lijst opgenomen of ze relevant zijn. Deze inschatting is samen met de beheerders van de voorzieningen gemaakt.

4.1.5. Wijze van toetsen standaard

Toetsen en het bevragen van beheerders

Het toetsen wanneer een voorziening aan een standaard voldoet is lastig. Het vereist een heldere afbakening van de voorziening en heldere voorwaarden wanneer voldaan wordt aan een standaard. Daarnaast zou het toetsten van compliancy in sommige gevallen buitengewoon veel tijd, maar ook toegang tot documenten en systemen vergen die de scope van dit onderzoek te buiten gaan. Deels hanteren we de reeds voor sommige standaarden beschikbare toetsen. Hieronder beschrijven we deze in meer detail.

Daarnaast bevragen we de beheerder van de voorziening, en vergelijken we die antwoorden met de resultaten van de toetsen, eerdere antwoorden, en met de antwoorden van andere gerelateerde voorzieningen (bijvoorbeeld indien gebruik gemaakt wordt van hetzelfde platform). Op die manier ontstaat een beeld van de mate waarin de voorziening voldoet aan de standaarden. Waar de antwoorden van de beheerder en PBLQ van elkaar afwijken, geven we dit helder aan in de rapportage. Per voorziening wordt het relevante onderdeel van de rapportage nog ter instemming voorgelegd aan de beheerder.

Bovenstaande werkwijze maakt het mogelijk om ondanks de uitdagingen bij het toetsen van standaarden toch tot een volledig en accuraat beeld te komen.

Gebruik van internet.nl

Voor een groot aantal standaarden hebben we gebruik gemaakt van de website internet.nl. De website is een initiatief van het Platform Internetstandaarden en maakt het mogelijk om het gebruik van standaarden te toetsen op basis van een specifiek domein. Het betreft de volgende standaarden:

- IPv4 en IPv6
- HTTPS/HSTS
- DMARC
- DKIM
- SPF
- STARTTLS en DANE
- TLS

In het onderzoek is de uitslag van deze toetsen vergeleken met de antwoorden van de beheerders van de voorzieningen. In geval van afwijkingen is samen met de beheerder gekeken waar dit aan kan liggen.

Gebruik van RIPEstat

De standaard RPKI wordt getoetst met RIPEstat. Aan de hand van een IP-adres kan worden nagegaan in hoeverre de RPKI-standaard is toegepast.

Webrichtlijnen en Digitoegankelijk

Op 24 mei 2018 is het Tijdelijk besluit digitale toegankelijkheid overheid gepubliceerd in het Staatsblad. Het besluit, dat de Europese toegankelijkheidsrichtlijn (2016/2102) omzet in bindende nationale regelgeving, is per 1 juli 2018 in werking getreden. Het doel is om de toegankelijkheid van websites en mobiele applicaties (apps) van overheidsinstanties te waarborgen.

Het besluit maakt deel uit van een breder pakket aan maatregelen met als doel een inclusieve benadering van digitale overheidsdienstverlening. Uitgangspunt daarbij is dat mensen met en zonder beperking op gelijke basis moeten kunnen deelnemen aan de maatschappij. Als websites goed in elkaar zitten kunnen ze door iedereen worden gebruikt, ook door bezoekers met een beperking.

Concreet moeten overheden vanaf 23 september 2020 voldoen aan het besluit. Vanaf deze datum moeten overheidsinstanties de toegankelijkheidsnorm toepassen op al hun websites. Als een website nog niet volledig toegankelijk is, dan moet de organisatie op basis van een gestructureerde aanpak binnen een redelijk haalbare termijn toewerken om volledig te voldoen aan alle toegankelijkheidseisen. In een toegankelijkheidsverklaring, die is ondertekend door een bestuurder of een verantwoordelijk functionaris, wordt verklaard hoever de overheidsinstantie is gevorderd met de toegankelijkheid van de website.

Dit jaar is gekeken naar de aanwezigheid van een toegankelijkheidsverklaring. Alle verklaringen worden gepubliceerd in het register van toegankelijkheidsverklaringen en kennen een nalevingsstatus. Deze geven aan hoever een overheidsinstantie is gevorderd met het toegankelijk maken van een website en kennen de volgende scores:

A. Voldoet volledig
B. Voldoet gedeeltelijk
C. Eerste maatregelen genomen
D. Voldoet niet
E. Geen toegankelijkheidsverklaring gepubliceerd

In de tabel is per voorziening aangegeven welke score de toegankelijkheidsverklaring heeft, indien deze is opgenomen in het register. In Tabel 8 is die score, voor de vergelijkbaarheid met andere standaarden, alsvolgt vertaald: A = Voldoet, B = Deels, C = Gepland, rest = Niet.

ISO 27001/2, en de BIO

Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines informatieveiligheid voor Gemeenten, Rijk, Waterschappen en Provincies. Binnen de Rijksoverheid dient elke organisatie een eigen implementatie van de BIO te hebben. De BIO is gestructureerd op de ISO 27001 en ISO 27002 standaard. Indien een organisatie voldoet aan de BIO, dan voldoen zij binnen de context van dit rapport ook aan de verplichting om de ISO 27002 standaard te gebruiken. Waar er een aparte certificering op het gebied van ISO 27001 is toegekend, geven wij dit apart aan.

RPKI

De standaard RPKI staat sinds eind november 2019 op de pas toe of leg uit-lijst van het Forum Standaardisatie. De standaard moet voorkomen dat internetverkeer wordt omgeleid naar systemen van niet-geautoriseerde netwerken en is instrumenteel in het voorkomen van een ‘hijack’ van het verkeer. De standaard draagt daarmee bij aan het voorkomen van het afhandig maken van gegevens van gebruikers en/of het (on)bewust bereikbaar maken van bepaalde websites.

RPKI is een standaard die sterk ‘onder de motorkap’ zit, en daarmee ver afstaat van het werk van de gemiddelde beheerder van een voorziening. In veel gevallen wordt ervan uitgegaan dat de netwerkleverancier dit regelt, maar de beheerder is nog steeds verantwoordelijk.

Daarnaast wekt het functioneel toepassingsgebied in de lijst met standaarden verwarring. In schijnbare tegenstelling tot de tekst bij het organisatorisch functioneringsgebied ("van toepassing op overheden en instellingen uit de publieke sector") geeft het functioneel toepassingsgebied aan dat RPKI moet worden toegepast door netwerkaanbieders en houders van blokken IP-adressen bij het aanbieden van netwerkconnectiviteit.

4.2. Overzicht: open standaarden in overheidsbrede voorzieningen

In Tabel 8a en 8b zijn de bevindingen over de overheidsbrede voorzieningen in één overzicht samengebracht. In de rapportage van PBLQ, opgenomen in Bijlage B4, wordt de mate waarin elke voorziening aan de relevante standaarden voldoet gedetailleerd besproken.

4.2.1. Per voorziening beschouwd

Zoals gezegd in paragraaf 4.1.2 onderzoeken wij dit jaar 19 voorzieningen die relevant zijn voor de gegevensuitwisseling en communicatie tussen overheden en de onderliggende infrastructuur, zoals de basisregistraties, Diginetwerk en de Stelselcatalogus. Wij richten ons in deze paragraaf vooral op die 19 voorzieningen.

Volgend jaar onderzoeken we opnieuw de 17 voorzieningen, die vooral gericht zijn op de gegevensuitwisseling en communicatie met burgers en bedrijven. De cijfers (van vorig jaar) over deze 17 voorzieningen zijn – voor een completer beeld – wèl opgenomen in Tabel 8b verderop.

Voor een deel van de dit jaar onderzochte voorzieningen zijn relatief veel open standaarden relevant. Bijvoorbeeld voor:

- de basisregistraties BAG, BRK, BGT, WOZ en BRT (elk 23 standaarden),
- NHR (Nieuw Handelsregister, 22 standaarden),
- de BSN Beheervoorziening en de GBA-V, en ook de BRV (20 standaarden),
- en Doc-Direct en de BRO (19 standaarden).

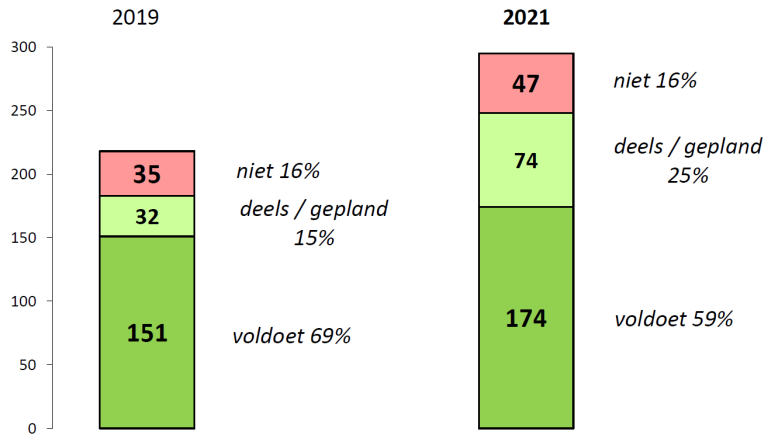
Voor andere voorzieningen zijn minder standaarden relevant: Diginetwerk (4 standaarden) en de BRI (BasisRegistratie Inkomen, 5 standaarden). Voor de 19 dit jaar onderzochte voorzieningen samen was in totaal 295 keer een open standaard relevant, dat is gemiddeld per voorziening 15,5 open standaarden.

In de meeste gevallen voldoen deze voorzieningen aan de relevante open standaarden. Maar vergeleken met twee jaar geleden is het percentage 'voldoet' is gedaald van 69% tot 59%. Het aantal gevallen waarin de voorziening deels aan de standaard voldoet of daarvoor concrete plannen heeft is juist gestegen van 15% vorig jaar naar 25% dit jaar. Samen met het percentage dat 'voldoet' is dat voor dit jaar dus net als twee jaar geleden 84%.

Op het eerste gezicht lijkt het alsof de onderzochte voorzieningen 'achteruit' gegaan zijn. Dat geldt echter alleen voor de percentages. Kijken we naar de absolute aantallen, dan is het beeld anders. Om te beginnen zijn er dit jaar veel meer gevallen waarin een standaard voor een voorziening relevant is: in 2019 ging het om 218 gevallen, dit jaar om 295 gevallen.

Figuur 7: Dit jaar onderzocht: 19 voorzieningen

Relevant voor gegevensuitwisseling tussen overheden en onderliggende infrastructuur



Het aantal keer 'voldoet' is gestegen van 151 naar 174 keer. Maar omdat het totale aantal veel sterker gestegen is, valt het percentage 'voldoet' dit jaar lager uit. Het aantal keer 'voldoet niet' is iets sterker toegenomen van 35 tot 47. Het is in dezelfde mate toegenomen als het totale aantal – waardoor dat percentage gelijk is gebleven. En het aantal keer 'deels/gepland' nam het meest toe: van 32 tot 74 keer. Dat is een sterkere stijging dan het totale aantal, waardoor het percentage 'deels/gepland' is gestegen.

Een nadere analyse van de veranderingen in de scores van de afzonderlijke voorzieningen geeft meer inzicht:

- In 2019 is DigiToegankelijk niet onderzocht, en dit jaar wel. Dat leidt tot 13 extra scores, waarvan 5 keer 'deels' en 8 keer 'gepland'.
- Drie van de vier standaarden die sinds 2019 nieuw op de lijst kwamen hebben ook extra scores opgeleverd. Voor NL_GOV alle 10 keer 'voldoet niet'. Voor RPKI en REST-API Design Rules samen zijn het 29 scores waarvan nog relatief weinig 'voldoet'(ongeveer de helft) en ongeveer een kwart 'voldoet niet'.
- Voor vijf basisregistraties (BAG, BRK, BGT, WOZ en BRT) gingen de scores voor TLS, PDF en SKOS van 'voldoet' naar 'deels'. In dit geval was er dus inderdaad sprake van achteruit gaan, zij het beperkt.

Nadere analyse wijst verder uit, dat twee voorzieningen hun plannen al jaren doorschuiven. Diginetwerk en Digitale Werkomgeving Rijk gaven in 2018 aan dat zij concrete plannen hadden om op korte termijn aan IPv4 & IPv6 te voldoen. Maar in 2019 was dat nog steeds 'gepland' en ook dit jaar is de status daarvan nog 'gepland'.

Verschillende voorzieningen onderscheiden zich dit jaar in positieve zin:

- Zowel Stelselcatalogus (10 relevante standaarden) als Diginetwerk (4 standaarden relevant) voldoen dit jaar geheel of gedeeltelijk aan alle relevante open standaarden en/of hebben concrete plannen om daaraan op korte termijn te voldoen.
- Verschillende voorzieningen voldoen 'bijna' aan alle standaarden, doordat zij aan een groot deel voldoen en aan de meeste andere deels voldoen, of dat gepland hebben. Bijvoorbeeld de BRO (Basisregistratie Ondergrond) en de Digitale Werkomgeving Rijk.

In Tabel 8a (hierna) is een gedetailleerd overzicht opgenomen van de 19 voorzieningen die vooral gericht zijn op de communicatie en de gegevensuitwisseling tussen overheden onderling of de onderliggende infrastructuur, de daarvoor relevante open standaarden en de mate waarin de voorziening daaraan voldoet. Naar verwachting zullen deze voorzieningen in 2023 opnieuw worden onderzocht.

Ter aanvulling zijn daarna in Tabel 8b de 'oude' gegevens (uit het onderzoek van vorig jaar) opgenomen voor de 17 voorzieningen, die van belang zijn voor communicatie en gegevensuitwisseling met burgers en bedrijven. In 2022 zullen deze voorzieningen naar verwachting weer worden onderzocht.

De mate waarin de voorziening aan een relevante standaard voldoet is, behalve met een kleurcode, ook met een letter aangegeven: V = voldoet, D = voldoet deels, G = gepland en N = voldoet niet. Als de cel leeg is, dan is de standaard niet relevant voor die voorziening.

De voorzieningen zijn onderverdeeld in vier groepen (conform de GDI):

- I&A = Identificeren & authenticeren
- D&I = Dienstverlening & informatieverstrekken
- G&R = Gegevens & registreren
- D&V = Dienstverlening & verbinden

Tabel 8a: Toepassing open standaarden in 19 voorzieningen die dit jaar onderzocht zijn

		I&A	D&I		G&R								D&V			
	V = voldoet *D = voldoet deels* *G = gepland* *N = voldoet niet* *(leeg = n.v.t.)*	BSN Beheervz + GBA-V (x2)	Rijksportaal	Doc-Direct	NHR (Nieuw HandelsReg.)	BAG, BRK, BGT, WOZ, BRT (x5)	BRO (ondergrond)	BRV (voertuigen)	BRI (inkomen)	Digilevering	Digimelding	Stelselcatalogus	DigiPoort	Diginetwerk	Dig. Werkomgeving Rijk	*aantal keer relevant Tabel A*
	aantal relevante Osn	*20*	*12*	*19*	*22*	*115*	*19*	*20*	*5*	*10*	*10*	*10*	*12*	*4*	*17*	*295*
	DKIM		N	V	V	V	V	V		V	V				V	*13*
	DMARC		N	V	V	V	V	V		V	V	V	V		D	*15*
	DNSSEC		N	V	G	V	D	G		V	V	V	V	V	D	*16*
	HTTPS & HSTS	V	N	D	V	D	D	D		V	V	V	V		D	*17*
	IPv4 & IPv6	V	N	V	D	V	D	D		N	N	G	N	G	G	*18*
	NEN-ISO\IEC 27001	V		V	V	V	V	V	V				V	V	V	*15*
	NEN-ISO\IEC 27002	V		V	V	V	V	V	V				V	V	V	*15*
	NL GOV	N			N	N		N							N	*10*
	RPKI	N	N	V	V	V	N	V	V	V	V	V	V		G	*18*
	SAML		V	V	V	D	V	V							V	*11*
	SPF		N	V	V	V	V	V		V	V		V		V	*14*
	STARTTLS & DANE			V	G	N		G		V	V				V	*11*
	STIX en TAXII														V	*1*
	TLS	V	V	V	V	D	V	V	V				V		V	*15*
	WPA2 Enterprise															*0*
	AdES Baseline Prof.			V	V											*2*
	Digitoegankelijk		G	D	G	G	D	D		D	D	G				*13*
	ODF 1.2		V	N											V	*3*
	OWMS			V		N		V								*7*
	PDF (NEN)		V	V	V	D	V	V				V			V	*12*
	SKOS			N	G	D		V				V				*9*
	OpenAPI Specific.				G	V	V	V								*8*
	REST-API Design R.	N			G	D	V	N				V				*11*
	NLCIUS				N	N										*6*
	SETU												V			*1*
	WDO Datamodel															*0*
	XBRL												V			*1*
	Digikoppeling	D		G	V	D	V	D	N	V	V		V		V	*16*
	Geo-standaarden					V	V									*6*
	StUF	N			V	V										*8*
	Aquo-standaarden						V									*1*
	GWSW															*0*
	SIKB 0101															*0*
	SIKB 0102															*0*
	COINS															*0*
	IFC															*0*
	NLCS															*0*
	VISI															*0*
	BWB						D					V				*2*
	ECLI															*0*
	JCDR															*0*
	e-Portfolio															*0*
	NL_LOM															*0*
	EML_NL															*0*

Tabel 8b: Toepassing open standaarden in 17 andere voorzieningen (onderzocht in 2020)

(Deze standaarden worden in 2022 weer onderzocht.)

		I&A				D&I									G&R		D&V		
	V = voldoet *D = voldoet deels* *G = gepland* *N = voldoet niet* *(leeg = n.v.t.)*	DigiD	DigiD Machtigen	PKI Overheid	Stelsel ETD	MijnOverheid	Berichtenbox bedrijven	Overheid.nl	Ondernemersplein	Samenwerkende Catalogi	Rijksoverheid.nl - web	Rijksoverheid.nl – email	*website* RDW.nl	*website* WOZ Waardeloket	*website* Handelsregister	*website* PDOK (geodata)	TenderNed	Digi-Inkoop	*aantal keer relevant Tabel B*
	aantal relevante Osn	*11*	*11*	*9*	*12*	*15*	*11*	*14*	*12*	*7*	*10*	*9*	*16*	*11*	*18*	*14*	*13*	*12*	*205*
	DKIM	V			V	V	V	V	D			V	V	V	V	V	V	V	*13*
	DMARC	V	V	V	G	V	V	V	V	V		V	G	N	V	V	V	N	*16*
	DNSSEC	V	V	V	V	V	V	V	V		V	V	D	V	G	V	V	V	*16*
	HTTPS & HSTS	V	V	D	V	V	G	V	V	N	V		G	V	V	G	N	V	*16*
	IPv4 & IPv6	V	V	N	D	V	G	V	N	V	V	G	N	V	N	V	N	G	*17*
	NEN-ISO\IEC 27001	V	V	V	V	V		V	V		V	V	V	V	V	V	V	V	*15*
	NEN-ISO\IEC 27002	V	V	V	V	V		V	V		V	V	V	V	V	V	V	V	*15*
	NL GOV																		*0*
	RPKI																		*0*
	SAML	V	V		V	V	V						V		V		V		*8*
	SPF	V	V		V	V	V		V	V		V	V	V	V	V	V	V	*14*
	STARTTLS & DANE	V			V	V		V	N			V	G	N	G	V	V		*11*
	STIX en TAXII																		*0*
	TLS	V	G	V	D	V	N	G	V	N	V	V	N	V	V	V	V	V	*17*
	WPA2 Enterprise																		*0*
	AdES Baseline Prof.												N		V				*2*
	Digitoegankelijk																		*0*
	ODF 1.2										V								*1*
	OWMS			V				V	N	V	V					V			*6*
	PDF (NEN)		V	V	V	V	V	V			D		V	N	V		V	V	*12*
	SKOS							V					V		G				*3*
	OpenAPI Specific.					V				V			V		D	V	N		*6*
	REST-API Design R.																		*0*
	NLCIUS												N		N			V	*3*
	SETU																	V	*1*
	WDO Datamodel																		*0*
	XBRL																		*0*
	Digikoppeling		D			V	V								V				*4*
	Geo-standaarden															V			*1*
	StUF					V	V								V	V			*4*
	Aquo-standaarden																		*0*
	GWSW																		*0*
	SIKB 0101																		*0*
	SIKB 0102																		*0*
	COINS																		*0*
	IFC																		*0*
	NLCS																		*0*
	VISI																		*0*
	BWB							V	V		V								*3*
	ECLI																		*0*
	JCDR							V											*1*
	e-Portfolio																		*0*
	NL_LOM																		*0*
	EML_NL																		*0*

4.2.2. *Per standaard beschouwd*

Van alle 44 open standaarden op de 'pas toe of leg uit'-lijst zijn er 30 relevant voor één of meer van de dit jaar onderzochte voorzieningen. Er zijn 16 open standaarden die voor meer dan 10 van de 19 voorzieningen relevant zijn:

- IPv6+IPv4 en RPKI (beide relevant voor 18 van de 19 dit jaar onderzochte voorzieningen),
- HTTPS & HSTS (relevant voor 17 voorzieningen), en DNSSEC en Digikoppeling (16),
- DMARC, NEN-ISO\IEC 27001, NEN-ISO\IEC 27002, TLS (15), SPF (14), DKIM, Digitoegankelijk (13), PDF (12) en SAML, STARTTLS & DANE en REST-API Design Rules (11).

De mate waarin voorzieningen aan de standaard (als die relevant is) voldoen is hoog: voor 12 van de 30 standaarden die relevant zijn geldt dat tenminste 80% van de voorzieningen aan die standaard voldoet. Het gaat om de volgende 12 open standaarden:

- voor 8 van deze 12 standaarden geldt dat alle voorzieningen waarvoor deze standaard relevant is er aan voldoen; 2 van die standaarden zijn voor veel voorzieningen relevant: NEN-ISO\IEC 27001 en NEN-ISO\IEC 27002; de andere standaarden zijn voor een beperkter aantal voorzieningen relevant, maar die voldoen wel allemaal aan die standaard: STIX & TAXII, AdES Baseline Profiles, SETU, XBRL, Geo-standaarden en de Aquo-standaard;
- de vier open standaarden waaraan tussen 80% en 99% van de voorzieningen voldoet zijn: SPF (93%), DKIM (92%), OpenAPI Specification (88%) en DMARC (87%).

Van deze 12 standaarden vallen er 6 in het domein ‘Internet & beveiliging’, en de andere helft is verspreid over het domein ‘Document & (web)content’ (1), het domein ‘REST API's’ (1), in ‘E-facturatie & administratie’ (2), onder de ‘Stelselstandaarden’ (1) en in het domein ‘Water & Bodem’ (1).

Vijf standaarden scoren juist relatief laag: van de voorzieningen waarvoor deze relevant zijn voldoet er geen enkele (volledig) aan Digitoegankelijk en ook geen enkele aan NLCIUS en aan de nieuwe standaard NL GOV. Daarnaast voldoet slechts 18% van de voorzieningen aan REST-API Design Rules, 22% aan SKOS en 28% aan OWMS.

De verschillen tussen de domeinen zijn groot. Vooral standaarden uit het domein ‘Internet & Beveiliging’ zijn bijvoorbeeld erg vaak relevant (64% van alle gevallen). De domeinen ‘Document & Webcontent’ (16%) en ‘Stelselstandaarden’ (10%) volgen op grote afstand. De 20 standaarden uit de zes andere domeinen samen zijn zelden relevant (samen slechts 10%).

Tabel 9: Open standaarden relevant / voldoet, twee sets voorzieningen

	onderzocht in 2021: **19 voorzieningen: gegevensuitwisseling overheden en infrastructuur eronder**			*vorig jaar onderzocht:* *17 voorzieningen: gegevensuitwisseling en communicatie burgers/bedrijven*		
	Relevant in % van 19	**Voldoet** in % relevant	**V + D + G** in % relevant	Relevant in % van 17	Voldoet in % relevant	V + D + G in % relevant
Internet & beveiliging:						
DKIM	**68%**	**92%**	**92%**	76%	92%	100%
DMARC	**79%**	**87%**	**93%**	94%	75%	88%
DNSSEC	**84%**	**69%**	**94%**	94%	88%	100%
HTTPS & HSTS	**89%**	**41%**	**94%**	94%	63%	88%
IPv4 & IPv6	**95%**	**44%**	**78%**	100%	47%	71%
NEN-ISO\IEC 27001	**79%**	**100%**	**100%**	88%	100%	100%
NEN-ISO\IEC 27002	**79%**	**100%**	**100%**	88%	100%	100%
NL GOV	**53%**	**0%**	**0%**			
RPKI	**95%**	**72%**	**78%**			
SAML	**58%**	**55%**	**100%**	47%	100%	100%
SPF	**74%**	**93%**	**93%**	82%	100%	100%
STARTTLS & DANE	**58%**	**36%**	**55%**	65%	64%	82%
STIX en TAXII	**5%**	**100%**	**100%**	0%		
TLS	**79%**	**67%**	**100%**	100%	65%	82%
WPA2 Enterprise	**0%**			0%		
Document & (web)content:						
AdES Baseline Profiles	**11%**	**100%**	**100%**	12%	50%	50%
Digitoegankelijk	**68%**	**0%**	**100%**	0%		
ODF 1.2	**16%**	**67%**	**67%**	6%	100%	100%
OWMS	**37%**	**29%**	**29%**	35%	83%	83%
PDF (NEN)	**63%**	**58%**	**100%**	71%	83%	92%
SKOS	**47%**	**22%**	**89%**	18%	67%	100%
REST API's:						
OpenAPI Specification	**42%**	**88%**	**100%**	35%	67%	83%
REST-API Design Rules	**58%**	**18%**	**73%**	0%		
E-facturatie & administratie:						
NLCIUS	**32%**	**0%**	**0%**	18%	33%	33%
SETU	**5%**	**100%**	**100%**	6%	100%	100%
WDO Datamodel	**0%**			0%		
XBRL	**5%**	**100%**	**100%**	0%		
Stelselstandaarden:						
Digikoppeling	**84%**	**38%**	**94%**	24%	75%	100%
Geo-standaarden	**32%**	**100%**	**100%**	6%	100%	100%
StUF	**42%**	**75%**	**75%**	24%	100%	100%
Water & Bodem:						
Aquo-standaarden	**5%**	**100%**	**100%**	0%		
GWSW	**0%**			0%		
SIKB 0101	**0%**			0%		
SIKB 0102	**0%**			0%		
Bouw:						
COINS	**0%**			0%		
IFC	**0%**			0%		
NLCS	**0%**			0%		
VISI	**0%**			0%		
Juridische verwijzingen:						
BWB	**11%**	**50%**	**100%**	18%	100%	100%
ECLI	**0%**			0%		
JCDR	**0%**			6%	100%	100%
Onderwijs & loopbaan:						
e-Portfolio	**0%**			0%		
NL_LOM	**0%**			0%		
Overig:						
EML_NL	**0%**			0%		

5. Gegevens over het gebruik van open standaarden

Het uiteindelijke doel van het open standaardenbeleid is een brede adoptie van de open standaarden van de lijst voor 'pas toe of leg uit' – daar waar deze van toepassing zijn – door alle overheden en andere organisaties in de publieke sector.

Het 'pas toe of leg uit'-regime is gericht op de aanschaf van ICT, en dus op het toepassen van open standaarden bij toevoegingen aan en bij vernieuwingen van het ICT-systeem. Gegevens over het feitelijk gebruik geven een beeld voor het gehele ICT-systeem. Bovendien gaat het bij het 'pas toe of leg uit'-regime om het vragen om open standaarden, en wordt niet gemeten in hoeverre het gevraagde ook (volledig) is geleverd. Tenslotte kunnen overheden open standaarden ook toepassen, mogelijk zelfs zonder zich daarvan bewust te zijn, doordat zij voorzieningen of producten gebruiken waarin deze open standaarden toegepast zijn.

Voor een completer beeld is het feitelijk gebruik dus een interessante indicator. Helaas is het lang niet altijd even eenvoudig gebleken om (voor alle open standaarden) vast te stellen in welke mate die feitelijk gebruikt worden. Dat is bij eerdere versies van de monitor overigens niet anders geweest.

Het opvragen van gegevens bij de verschillende beheerorganisaties is dit jaar wederom uitgevoerd door de accountmanagers van BFS. Vervolgens zijn de bevindingen vastgelegd in een kort verslag voor elk van de standaarden. Bundeling hiervan heeft geleid tot de notitie ‘Inventarisatie gebruiksgegevens 2021’ (zie Bijlage B5).

Daarnaast doet BFS elk halfjaar onderzoek naar internet-veiligheids-standaarden, een deel van de gebruiksgegevens is afkomstig uit de ‘Meting Informatieveiligheidstandaarden overheid - maart 2021’ (zie Bijlage B6).

5.1. Gebruiksgegevens 2021: inventarisatie door accountmanagers BFS

In de notitie ‘Inventarisatie gebruiksgegevens 2021’ (zie Bijlage B5) is beschreven welke gegevens de accountmanagers over het gebruik van de standaard hebben kunnen vinden en of daaruit een toename van het gebruik blijkt. In Tabel 10 zijn de uitkomsten van deze inventarisatie samengevat.

Over een aantal standaarden zijn geen gebruiksgegevens beschikbaar. Voor een (beperkt) aantal standaarden is dat gezien de aard van de standaard begrijpelijk. Maar ook waar dergelijke gegevens wèl zouden kunnen bestaan blijken beheerorganisaties daarin onvoldoende geïnteresseerd. Dat is vreemd, want de open standaarden zijn ooit op de lijst opgenomen omdat een impuls voor het gebruik door overheden van belang werd geacht.

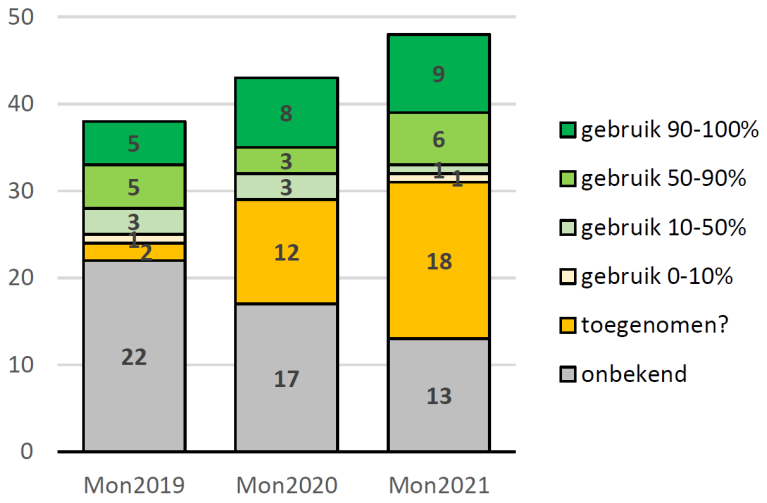
Tabel 10: Gebruiksgegevens 2021, per standaard

	Beeld BFS		**Resultaten IV-meting**
	ontwikkeling t.o.v. 2020	*gebruiksgegevens*	
Internet & beveiliging:			
DKIM	stabiel	96 %	96 %
DMARC	licht toegenomen	van 92% naar 95%	DMARC 95 %
en DMARC policy	toegenomen	van 66% naar 74%	DMARC policy 74 %
DNSSEC	toegenomen	van 94% naar 98%	98 %
HTTPS	stabiel	98 %	HTTPS 98 %
en HSTS	afgenomen	van 92% naar 83%	HSTS 83 %
IPv6 en IPv4	toegenomen	van 69% naar 79%	79 %
NEN-ISO\IEC 27001:2005nl	niet duidelijk	[geen cijfers]	
NEN-ISO\IEC 27002:2007nl	niet duidelijk	[geen cijfers]	
NL GOV Assurance	niet duidelijk	[geen cijfers]	
RPKI	licht toegenomen	beperkte cijfers	
SAML	toegenomen	beperkte cijfers	
SPF	licht toegenomen	van 97% naar 99%	SPF 99 %
en SPF policy	licht toegenomen	van 91% naar 94%	SPF policy 94 %
STARTTLS	toegenomen	cf: van 42% naar 69%	STARTTLS cf 69 %
en DANE	licht toegenomen	van 53% naar 55%	55 %
STIX & TAXII	toegenomen	beperkte cijfers	
TLS	toegenomen	cf: van 78% naar 85%	TLS cf 83 %
WPA2 Enterprise	licht toegenomen	van 563 naar 587	
Document & (web)content:			
Ades Baseline Profiles	onduidelijk	[geen cijfers]	
Digitoegankelijk	onduidelijk	[geen cijfers]	
ODF	beperkt gebruik	3 %	
OWMS	stagneert	van 28% naar 27%	
PDF	toegenomen	94 %	
SKOS	licht toegenomen	globale cijfers	
REST API's:			
OpenAPI Specification	onduidelijk	[geen cijfers]	
REST_API Design Rules	onduidelijk	[geen cijfers]	
E-facturatie & administratie:			
NLCIUS	toegenomen	globale cijfers	
SETU	stabiel	[geen cijfers]	
WDO Datamodel	toegenomen	[geen cijfers]	
XBRL	stabiel	diverse indicatoren	
Stelselstandaarden:			
Digikoppeling	stabiel	91 %	
Geo−standaarden	toegenomen	diverse indicatoren	
StUF	toegenomen	diverse indicatoren	
Water & Bodem:			
Aquo Standaard	stabiel	diverse indicatoren	
GWSW	toegenomen	diverse indicatoren	
SIKB 0101	toegenomen	[geen cijfers]	
SIKB 0102	toegenomen	[geen cijfers]	
Bouw:			
COINS	licht toegenomen	[geen cijfers]	
IFC	beperkt gebruik	6% (nulmeting)	
NLCS	licht toegenomen	[cijfers nog onduidelijk]	
Visi	licht toegenomen	diverse indicatoren	
Juridische verwijzingen:			
BWB	toegenomen	[nauwelijks cijfers]	
ECLI	toegenomen	[nauwelijks cijfers]	
JCDR	toegenomen	[nauwelijks cijfers]	
Onderwijs & loopbaan:			
E−portfolio	onduidelijk	[nauwelijks cijfers]	
NL LOM	onduidelijk	[geen cijfers]	
Overig:			
EML_NL	stabiel	[overal toegepast]	

Over de meeste standaarden uit het domein Internet & beveiliging zijn cijfers beschikbaar (dankzij de IV-meting). Veel van deze standaarden worden inmiddels door veel overheden gebruikt (zij het vaak nog niet voor de door het OBDO nagestreefde 100%). Uitzonderingen zijn IPv4&IPv6 (79%, stijgend), DANE (55%, licht toegenomen), STARTTLS (69%, stijgend) en TLS (83%, licht toegenomen).

Veel van de standaarden waarover wèl gegevens beschikbaar zijn worden ook door veel overheden gebruikt: voor 9 standaarden is het gebruik meer dan 90% en voor 6 standaarden is het 50 tot 90%. Daarnaast is inmiddels voor meer standaarden waarover geen harde gegevens beschikbaar zijn, wel de indruk dat het gebruik toeneemt (in 2019 gold dat nog voor slechts 2 standaarden, inmiddels voor 18 standaarden).

Figuur 11: Gebruiksgegevens over open standaarden (aantallen)



Voor verschillende standaarden uit het domein Document & (web)content is recent (deels dit jaar, deels vorig jaar) een begin gemaakt met een nulmeting van gebruiksgegevens. Voor de meeste andere domeinen en standaarden zijn nauwelijks bruikbare cijfers beschikbaar, enkele positieve uitzonderingen daar gelaten.

5.2. Gebruiksgegevens 2021: resultaten IV-meting

In het OBDO hebben de verschillende overheden afgesproken dat volledige adoptie (100%) voor de volgende standaarden stapsgewijs gerealiseerd moet worden:

- uiterlijk eind 2017: DNSSEC, HTTPS, TLS (web) en DKIM, DMARC, SPF (mail);
- uiterlijk eind 2018: HSTS, HTTPS, TLS: veilige configuratie conform NCSC (web);
- uiterlijk eind 2019: voor DMARC, SPF instellen van strikte policies, STARTTLS&DANE (mail);
- uiterlijk eind 2021: websites en e-maildomeinen van de overheid behalve via IPv4 ook volledig bereikbaar via IPv6.

Uit de 'Meting Informatieveiligheidstandaarden overheid - maart 2021' (zie Bijlage B6, de uitkomsten zijn opgenomen in de rechterkolom van Tabel 10) blijkt dat het streefbeeld voor eind 2019 op het moment van de meting – ruim een jaar na de laatste deadline – nog niet volledig was gerealiseerd. Wel is de toepassing van een aantal standaarden gegroeid.

Van de webstandaarden wordt alleen TLS inmiddels volledig toegepast (100%), gevolgd door HTTPS (redirect) en DNSSEC (beide 98%). Voor deze standaarden was de deadline voor 100% adoptie: eind 2017. Ook HSTS wordt veel toegepast (92%, deadline voor 100% was eind 2018). HSTS en TLS conform NCSC scoren lager (beide 83%).

Van de mailstandaarden voor anti-phishing wordt SPF (99%) het meest toegepast, gevolgd door DKIM (96%), DMARC (95%). Voor deze standaarden was de deadline voor 100% adoptie: eind 2017. Ook SPF Policy wordt veel toegepast (94%, deadline voor 100% was eind 2018). Van de mailstandaarden voor vertrouwelijkheid wordt STARTTLS volledig toegepast (100%).

De andere mailstandaarden worden in 2021 minder vaak toegepast: DMARC Policy (74%) voor anti-phishing, en STARTTLS cf. NCSC (69%), DNSSEC MX (64%) en DANE (55%) voor vertrouwelijkheid. Ook voor deze standaarden is de deadline voor het OBDO-streefbeeld reeds verstreken.

Het streefbeeld voor IPv6, eind 2021 alle websites en e-maildomeinen van de overheid behalve via IPv4 ook volledig bereikbaar via IPv6, is nog niet in zicht. Maar de toepassing van IPv6 is wel gegroeid: voor overheidswebsites van 64% in maart 2020 naar 79% in maart 2021, en voor overheidsemail van 17% in maart 2020 naar 40% in maart 2021.

BIJLAGEN

B1. Instructie Rijksdienst (inclusief toelichting)

B2. Overzicht van de beoordeelde aanbestedingen Q3+Q4 2020

B3. Tabellen voor het volledige kalenderjaar 2020 (Q1 tot en met Q4)

B4. Rapportage Open standaarden en voorzieningen (PBLQ)

B5. Inventarisatie gebruiksgegevens 2021 door BFS

B6. Rapportage IV-meting maart 2021 (BFS)

B1. Instructie Rijksdienst (inclusief toelichting)

STAATSCOURANT
Officiële uitgave van het Koninkrijk der Nederlanden sinds 1814.
Nr. 227
21 november
2008

Besluit van de Staatssecretaris van Economische Zaken van 8 november 2008, nr. WJZ/8157380, tot vaststelling Instructie rijksdienst inzake aanschaf ICT-diensten en ICT-producten

De Staatssecretaris van Economische Zaken,

Handelende mede namens de Staatssecretaris van Binnenlandse Zaken en Koninkrijksrelaties en in overeenstemming met het gevoelen van de ministerraad;

Besluit:

Artikel 1

Vastgesteld wordt de als bijlage bij dit besluit gevoegde instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten.

Artikel 2

Dit besluit treedt in werking met ingang van de tweede dag na de dagtekening van de Staatscourant waarin het wordt geplaatst.

Artikel 3

Dit besluit wordt aangehaald als 'Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten'.

Dit besluit zal met de bijlage en de daarbij behorende toelichting in de Staatscourant worden geplaatst.

Den Haag, 8 november 2008

De Staatssecretaris van Economische Zaken,
F. Heemskerk.

BIJLAGE INSTRUCTIE RIJKSDIENST INZAKE AANSCHAF VAN ICT-DIENSTEN EN ICT-PRODUCTEN

Artikel 1 (definities)

In deze instructie wordt verstaan onder:
a. *ICT-dienst of ICT-product:* een dienst of product ingericht om de uitwisseling van gegevens of archivering digitaal te doen verlopen, en welke bij aanschaf een waarde vertegenwoordigt van ten minste € 50.000,–;
b. *de aanschaf:* een complex van handelingen dat leidt tot het rechtmatig gebruik van een ICT-dienst of een ICT-product en dat resulteert in een overeenkomst met een derde, of dat leidt tot de ontwikkeling van die dienst of dat product door de Staat der Nederlanden.

Artikel 2 (adressaten)

Deze instructie wordt in acht genomen door de ministers en staatssecretarissen en de onder hen ressorterende dienstonderdelen.

Artikel 3 (pas toe of leg uit)

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.

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.

3. Afwijkingen van het eerste lid worden gemotiveerd vastgelegd in de departementale administratie, behalve wanneer ICT-diensten of ICT-producten voor militairoperationeel gebruik worden aangeschaft.

Artikel 4 (naleving)

Over de mate van naleving van artikel 3 wordt in de toelichting bij het departementaal jaarverslag bij de informatie over de bedrijfsvoering verantwoording afgelegd.

Artikel 5 (inwerkingtreding wijzigingen lijst)

Wijzigingen van de op de website www.forumstandaardisatie.nl gepubliceerde lijst met toepassingsgebieden met daarbij vermelde open standaarden zijn niet van toepassing bij de aanschaf van ICT-diensten of ICT-producten waarvan de aanschaf ten tijde van de inwerkingtreding van de lijst zodanig is gevorderd dat toepassing de continuïteit en betrouwbaarheid van de elektronische dienstverlening voor burgers en bedrijven in gevaar kan brengen.

TOELICHTING

Algemeen

Het kabinet streeft met ICT onder andere naar goede participatie van burgers, het verminderen van administratieve lasten en maatschappelijke problemen, duurzaamheid van gegevensopslag en innovatie. Het kabinet heeft aangegeven dat het gebruik van open standaarden en open source software belangrijke sleutels zijn voor innovatief en toekomstbestendig ICT-gebruik in (semi-) publieke sectoren. Hoe het gebruik van deze sleutels bevorderd wordt staat centraal in het actieplan Nederland Open in Verbinding dat bij brief van 17 september 2007 (Kamerstukken II 2006/07, 26 643, nr. 98), op 17 september 2007 namens het kabinet aan de Tweede Kamer is aangeboden door de Staatssecretaris van het ministerie van Economische Zaken en de Staatssecretaris van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties.

Door als overheid gebruik te maken van open standaarden in ICT-producten en ICT-diensten wordt gegevensuitwisseling tussen informatiesystemen van overheden met burgers en overheden met overheden eenvoudiger (interoperabiliteit), wordt gegevensopslag meer duurzaam en wordt de afhankelijkheid van ICT leveranciers verminderd. Op termijn zal dit leiden tot hogere kwaliteit van overheidsdienstverlening, efficiënter beheer van ICT-systemen en daardoor besparing van kosten.

Het kabinet heeft in het actieplan Nederland Open in Verbinding aangegeven dat het gebruik van open standaarden door overheidsorganisaties niet meer vrijblijvend is. In het actieplan is daartoe onder meer actielijn 2 aangekondigd. Deze instructie geeft invulling aan de bedoelde actielijn.

Deze instructie geeft rijksbreed aan hoe bij de aanschaf van ICT-diensten of ICT-producten te werk moet worden gegaan. Als regel dient er in het besluitvormingsproces dat aan de aanschaf vooraf gaat te worden gekozen voor een ICT-dienst of -product dat gebruik maakt van open standaarden. Als er goede gronden zijn om dat toch niet te doen, dient te worden vastgelegd welke die goede gronden zijn. Deze instructie laat dus de mogelijkheid open om na een gedegen afwegingsproces te komen tot de aanschaf van niet op open standaarden gebaseerde ICT-diensten of ICT-producten. Redenen om van de hoofdregel af te wijken zijn onder meer dat voor bepaalde toepassingen (nog) geen open standaarden beschikbaar zijn of de wel beschikbare open standaarden niet of onvoldoende worden ondersteund door ICT-aanbieders.

Deze instructie fungeert vervolgens ook als voorbeeld voor andere overheden en (semi-) publieke instellingen en hun uitvoeringsorganisaties voor de wijze waarop zij het gebruik van open standaarden kunnen bevorderen binnen hun eigen organisaties.

Deze instructie treedt formeel in werking op de tweede dag na de dagtekening van de Staatscourant waarin het besluit waarbij deze instructie wordt vastgesteld, wordt geplaatst. Er is niet voorzien in een overgangsbepaling bij de inwerkingtreding. In voorkomende gevallen zal een keuze voor een niet-open standaard moeten worden gemotiveerd. Dat in een voorkomend geval ook door aan te geven dat het eisen van een open standaard in het concrete geval de continuïteit en betrouwbaarheid van de elektronische dienstverlening voor burgers en bedrijven in gevaar kan brengen.

Artikelsgewijs

Artikel 1

Blijkens de definitie van ICT-dienst of -product geldt de instructie niet voor de aanschaf van dergelijke diensten of producten die naar verwachting minder zullen kosten dan € 50.000 euro (exclusief BTW). De keuze voor dit bedrag is zoals iedere keuze voor een bedrag in zekere mate arbitrair maar in de meeste gevallen zal het bij investeringen onder dit bedrag gaan om aanpassing van bestaande ICT-systemen. Het kiezen voor een andere standaard zal dan dikwijls leiden tot disproportioneel hoge kosten.
De definitie van het begrip 'aanschaf' maakt duidelijk dat de instructie niet alleen geldt bij de aankoop of de inhuur van ICT-producten en -diensten maar ook bij ontwikkeling daarvan door de Staat der Nederlanden. Ook maakt het voor de werking van de instructie niet uit of er sprake is van nieuwe diensten of producten, dan wel voorzetting van ook al eerder verleende diensten of de aanvulling op of wijziging van bestaande diensten of producten.

Artikel 3

Het eerste lid van artikel 3 laat zien dat de procedure alleen gevolgd moet worden als er ICT-diensten of ICT-producten worden aangeschaft voor een toepassinggebied waarvoor er een of meer open

standaarden zijn die voldoende gangbaar zijn. De lijst met toepassingsgebieden en open standaarden laat de geleidelijke verbreding van de reikwijdte van instructie toe. De lijst met toepassingsgebieden en de daarvoor bruikbare open standaarden is te raadplegen door middel van de website www.forum-standaardisatie.nl. De eerste versie van deze lijst met een toelichting is vanaf 1 maart 2008 in te zien. De desbetreffende lijst op de genoemde website is dynamisch en zal niet vaker dan twee keer per jaar worden bijgewerkt. Bij het opnemen van standaarden in de lijst wordt gekeken naar de waarde voor de uitvoering van publieke taken, de mate van openheid van een standaard en de mate van ondersteuning van een standaard door de markt. Het ligt in de bedoeling over wijzigingen en aanvullingen in de lijst vooraf te overleggen met deskundigen bij het Forum Standaardisatie. De website van het Forum Standaardisatie laat zien langs welke weg het Forum komt tot de deskundige inbreng in het proces van het samenstellen van de lijst en hoe derden daarbij inbreng kunnen hebben.

Het tweede lid laat zien dat de instructie zelf geen technische specificaties voorschrijft. Zoals ook hiervoor al aangegeven verplicht de instructie tot een bepaalde werkwijze. Indien de keuze voor een open standaard als technische specificatie niet gewenst is bij de voorgenomen aanschaf, kan, mits gemotiveerd, gekozen worden voor een andere standaard.
Van de redenen die er kunnen zijn om toch te kiezen voor een ICT-dienst die of ICT-product dat niet is gebaseerd op een open standaard worden in artikel 3 genoemd onvoldoende aanbod, onvoldoende veiligheid, onvoldoende zekerheid bij het functioneren, of andere redenen van bijzonder gewicht. Bij de laatste categorie zal het praktisch gezien gaan om aspecten van geld, tijd of capaciteit. Van onvoldoende aanbod zal bijvoorbeeld sprake zijn indien tevoren is te verwachten dat een product of dienst gebaseerd op een standaard uit de lijst naar verwachting niet of door een zeer gering aantal aanbieders wordt aangeboden.
De reden om niet te kiezen voor een open standaard zal wel enige substantie moeten hebben. Het is niet de bedoeling dat voor gesloten standaarden gekozen wordt enkel en alleen omdat het tijdsbeslag dan wat korter is of de kosten wat lager zijn. Het niet zelf beschikken over capaciteit is geen goede reden als die capaciteit eenvoudig valt in te huren of als er in de eigen organisatie nooit aandacht besteed wordt aan het op peil brengen van bestaande tekorten in de eigen capaciteit.

Om de belemmeringen die er in de praktijk blijken te bestaan bij de besluitvorming omtrent een open standaard in concrete situaties op te lossen kunnen betrokkenen het programmabureau 'Nederland Open in Verbinding' om informatie en ondersteuning vragen.

Bij het aanschaffen van ICT-diensten of ICT-producten zal er in veel gevallen sprake zijn van een aanbesteding. Het spreekt voor zich dat in een dergelijk geval de aanbestedingsrechtelijke regels gevolgd moeten worden. De onderhavige instructie betreft uitsluitend het interne besluitvormingsproces en raakt in geen enkel opzicht de verplichtingen die gevolgd moeten worden bij de verdere werkelijke aanschaf van een ICT-dienst of ICT-product.

Omdat bij de aanschaf van ICT-diensten en ICT-producten voor militairoperationeel gebruik veelal geen keus bestaat vanwege de noodzakelijke interoperabiliteit met onder andere NATO partners, wordt hiervoor een uitzondering gemaakt op de administratieplicht. Dit is geregeld in het derde lid.

Artikel 4 maakt duidelijk dat de diverse onderdelen van de rijksdienst de toepassing van de instructie zullen moeten administreren en verantwoorden in het onderdeel van het jaarverslag dat handelt over de bedrijfsvoering. Dit artikel brengt mee dat er binnen de rijksdienst zal worden toegezien op de naleving.

Artikel 5 maakt duidelijk dat wijzigingen van de lijst met toepassingsgebieden en open standaarden niet toepasselijk zijn bij een aanschaf die al zo ver is gevorderd dat deze niet zonder de continuïteit en betrouwbaarheid van de elektronische dienstverlening voor burgers en bedrijven in gevaar te brengen kan worden onderbroken of aangepast.

De Staatssecretaris van Economische Zaken,
F. Heemskerk.

B2. Overzicht van de beoordeelde aanbestedingen Q3+Q4 2020

De 20 aanbestedingen van Rijk en uitvoeringsorganisaties en de 20 van mede-overheden die dit jaar zijn beoordeeld zijn in respectievelijk Tabel B2.1 en Tabel B2.2 opgesomd, met een korte omschrijving van het onderwerp van de aanbesteding, de open standaarden die de beoordelaars relevant achten, om welke daarvan in de aanbesteding gevraagd is en de uiteindelijke beoordeling. Hiervoor is de volgende indeling gehanteerd (zie Hoofdstuk 3):

- er is om alle relevante open standaarden gevraagd > perfect
- er is om een deel van de open standaarden gevraagd > op de goede weg
- er is om geen enkele open standaard gevraagd:
    - alleen algemene aandacht voor architectuur-kaders en/of open standaardenbeleid > matig
    - er is geen aandacht voor open standaardenbeleid > slecht
- strijdig met het open standaardenbeleid > heel slecht

De midden-categorie 'op de goede weg' is nog onderverdeeld naar het aantal gevraagde standaarden in procenten van de relevante standaarden gevraagd is: 1-33% (nog een heel eind te gaan), 34-66% (de middenmoot) of 67-99% (op weg naar perfect).

Relevante standaarden waar in de aanbesteding om is gevraagd staan in de groene kolom, relevante standaarden waarom niet is gevraagd in de rode kolom daarnaast.

Tabel B2.1 Overzicht van beoordeelde aanbestedingen Rijk en uitvoeringsorganisaties

Aanbesteder	Onderwerp van aanbesteding	Relevante standaarden: gevraagd	Relevante standaarden: NIET gevraagd	Oordeel	
Ministerie van BZK	Het gaat om het vernieuwen van het Rijksportaal, het Rijksbrede intranet voor Rijksambtenaren bij alle ministeries.	ISO 27001 ISO 27002 Digitoegankelijk SAML DNSSEC HTTPS & HSTS TLS IPv4 & IPv6 SPF DKIM DMARC STARTTLS & DANE OpenAPI spec. OWMS PDF		perfect	100%
Ministerie van Defensie	Het leveren van technische diensten; engineering support van de communicatie en informatiesystemen (CIS Architectuur).	ISO 27001 ISO 27002		perfect	100%

Aanbesteder	Onderwerp van aanbesteding	Relevante standaarden: gevraagd	Relevante standaarden: NIET gevraagd	Oordeel	
Belasting-dienst	Waarborgen van de continuiteit van de Installed Base Middleware, na afloop van de huidige raamovereenkomst. Gevraagd wordt om het leveren van onderhoud en support, het verlenen van productspecifieke diensten en het leveren van opleidingen voor producten uit de Installed Base.	ISO 27001 ISO 27002		perfect	100%
Ministerie van Buitenlandse Zaken	Een IT-systeem dat het opdrachtgeven tot en uitvoeren van betalingen automatiseert Het betreft een SaaS oplossing.	ISO 27001 ISO 27002 SAML HTTPS & HSTS TLS DNSSEC	IPv4 & IPv6	op de goede weg: op weg naar perfect	86%
Ministerie van BZK	Het realiseren van gemeenschappelijke e-procurementvoorzieningen die minimaal noodzakelijk zijn om als 1 Rijksdienst naar buiten op te kunnen treden en het structureel beleggen van het beheer van deze voorzieningen.	ISO 27001 ISO 27002 HTTPS & HSTS TLS IPv4 & IPv6 DNSSEC SAML PDF Digikoppeling NLCIUS SETU Digitoegankelijk SPF DKIM DMARC STARTTLS & DANE	ODF OpenAPI spec. REST-API DR	op de goede weg: op weg naar perfect	84%

Ministerie van Defensie	Men zoekt een partner die ruime ervaring heeft met het leveren, implementeren, beheren en onderhouden van audio en video-apparatur bedoeld voor opname en terugkijken en –luisteren, inclusief software.	ISO 27001 ISO 27002 HTTPS & HSTS TLS PDF SAML IPv4 & IPv6 Digitoegankelijk	ODF DNSSEC	op de goede weg: op weg naar perfect	80%
UWV	De aanbestedende dienst wil alle facturen elektronisch ontvangen en verwerken van de opleidingsinstituten met behulp van een STAP-broker als tussenliggende dienstverlener (STAP staat voorstimulering van de arbeidsmarkt positie).	ISO 27001 ISO 27002 HTTPS & HSTS TLS NLCIUS PDF SETU SPF DKIM DMARC	DNSSEC IPv4 & IPv6 STARTTLS & DANE SAML	op de goede weg: op weg naar perfect	71%
Kamer van Koop-handel	Een ondertekendienst voor het door (laten) voeren van gegevenswijzigingen door externe gebruikers. Het gaat om een SaaS oplossing.	ISO 27001 ISO 27002 HTTPS & HSTS TLS Digitoegankelijk DNSSEC PDF SPF DKIM DMARC STARTTLS & DANE	Ades Baseline pr. OpenAPI spec. REST-API DR NL GOV Ass. IPv4 & IPv6	op de goede weg: op weg naar perfect	69%

Kamer van Koophandel	Levering, implementatie en onderhoud van een HRM systeem op basis van SaaS. Men streeft naar een eenvoudiger IT landschap met een grotere integratie en samenhang van HRM functionaliteiten.	ISO 27001 ISO 27002 HTTPS & HSTS TLS SPF DKIM DMARC STARTTLS & DANE PDF Digitoegankelijk Ades Baseline pr. OpenAPI spec.	IPv4 & IPv6 SETU E-portfolio SAML DNSSEC ODF	op de goede weg: op weg naar perfect	67%
Belasting-dienst	Er wordt gezocht naar een gebruiksvriendelijke, robuuste en toekomst-vaste loonberekening controle oplossing. Die oplossing moet het uitvoeren van adequaat toezicht op de loonheffing te ondersteunen. Daarvoor is een software-applicatie nodig, inclusief bijbehorende dienstverlening.	ISO 27001 ISO 27002	PDF	op de goede weg: op weg naar perfect	67%
Ministerie van Financien	Websiteontwikkeling, beheren en hosten van een state of the art website voor de Rijksacademie, met daarbij een vlekkeloos werkende koppeling met het opleidingsadministratiesysteem.	ISO 27001 ISO 27002 HTTPS & HSTS TLS Digitoegankelijk DNSSEC IPv4 & IPv6	SPF DKIM DMARC STARTTLS & DANE	op de goede weg: middenmoot	64%
CBR	Aanbesteding van een online-platform (SaaS) waarop het CBR enerzijds en zorgverleners anderzijds met elkaar relevante medische informatie zoals vragenlijsten en keuringsrapporten kunnen uitwisselen.	ISO 27001 ISO 27002 HTTPS & HSTS TLS PDF	IPv4 & IPv6 DNSSEC Digikoppeling	op de goede weg: middenmoot	63%

Kadaster	Ten behoeve van het beheer van het Nationaal Geo Register is dienstverlening nodig die voorziet in het leveren van een stabiele en beheerde versie van het GeoNetwork Opensource Coreproduct. Het gaat om beheer, onderhoud en hosting.	ISO 27001 ISO 27002 HTTPS & HSTS TLS OpenAPI spec. Geo-standaarden	IPv4 & IPv6 PDF Digitoegankelijk OWMS SPF DKIM DMARC STARTTLS & DANE	op de goede weg: middenmoot	43%
Ministerie van Financien	Het leveren van een HR SaaS oplossing in combinatie met personeels- en salarisadministratie voor Invest International, een bedrijf met een 100% staatsdeelneming (ministerie BZK).	ISO 27001 ISO 27002 HTTPS & HSTS TLS PDF SAML	IPv4 & IPv6 SPF DKIM DMARC STARTTLS & DANE DNSSEC ODF SETU	op de goede weg: middenmoot	43%
Ministerie van EZK, RVO	De scope is gericht op de Veilingdienst, de Ontwikkeldiensten en de Adviesdiensten om diverse frequentieveilingen mogelijk te maken(in opdracht van Agentschap Telecom).	ISO 27001 ISO 27002 HTTPS & HSTS TLS	IPv4 & IPv6 SPF DKIM DMARC STARTTLS & DANE DNSSEC	op de goede weg: middenmoot	40%
Ministerie EZK / RVO	Het beschikbaar stellen van satellietdata via een viewer met download-functie, Restful-API, API via OGC-standaarden en via een FTP-toegang tot de fileserver.	ISO 27001 ISO 27002 Geo-standaarden Digitoegankelijk	HTTPS & HSTS TLS DNSSEC OpenAPI spec. REST-API DR IPv4 & IPv6	op de goede weg: middenmoot	40%

Centrum Indicatie-stelling Zorg	Op zoek naar een geintegreerd SAAS ERP-systeemdat de HRM-processen, de financiele processen en de inkoopprocessen zoveel mogelijk digitaal en geautomatiseerd ondersteunt.	ISO 27001 ISO 27002 Digitoegankelijk NLCIUS PDF XBRL	DNSSEC HTTPS & HSTS TLS IPv4 & IPv6 SPF DKIM DMARC STARTTLS & DANE Digikoppeling E-portfolio ODF SAML	op de goede weg: nog een heel eind te gaan	33%
Nederlandse Zorgautoriteit	Vraag naar Managed Intrusion Detection dienstverlening voor monitoring van de huidige NZa infrastructuur.	ISO 27001 ISO 27002	HTTPS & HSTS TLS IPv4 & IPv6 STIX & TAXII	op de goede weg: nog een heel eind te gaan	33%
Dienst Uitvoering Onderwijs	Examensoftware ten behoeve van de afname van online examens die deel uitmaken van het vakbekwaamheidsstelsel Wet financieel toezicht. De software zal gebruikt worden voor het inschrijven van kandidaten, het beheer van de examenbank, het toezicht op de exameninstituten en de door hen gebruikte examenlocaties, het afnemen en de inzage van examens.	ISO 27001 ISO 27002 HTTPS & HSTS TLS	IPv4 & IPv6 DNSSEC PDF ODF SPF DKIM DMARC STARTTLS & DANE Digitoegankelijk OpenAPI spec. REST-API DR	op de goede weg: nog een heel eind te gaan	27%
RWS	Voor de rijkswegen in Nederland moeten de monitoringdata voor geluid, luchtkwaliteit en stikstofdepositie worden geactualiseerd en verwerkt.		Geo-standaarden IFC ODF SIKB0101	slecht	n.v.t.

Tabel B2.2 Overzicht van beoordeelde aanbestedingen Mede-overheden

Aanbesteder	Onderwerp van aanbesteding	Relevante standaarden: gevraagd	Relevante standaarden: NIET gevraagd	Oordeel	
Bizob	Beheer-, advies- en projectwerkzaamheden met betrekking tot de ICT-infrastructuur van de Veiligheidsregio Brabant - Zuidoost.	ISO 27001 ISO 27002		perfect	100%
Gemeente Apeldoorn	De levering, implementatie en migratie van een Integratievoorziening, bestaande uit een Enterprise Service Bus (ESB), een API Gateway en Digikoppeling, inclusief gerelateerde dienstverlening.	Digikoppeling DNSSEC HTTPS & HSTS TLS ISO 27001 ISO 27002 SAML SPF DKIM DMARC STARTTLS & DANE PDF StUF	OpenAPI spec. ODF	op de goede weg: op weg naar perfect	87%
Gemeente Purmerend	Op zoek naar dienstverlening eHRM. De gemeente is op zoek naar een “proven technology” oplossing. Het eHRM-systeem wordt geleverd op basis van een SAAS-oplossing.	DNSSEC Digikoppeling HTTPS & HSTS TLS IPv4 & IPv6 ISO 27001 ISO 27002 StUF PDF SAML SPF DKIM DMARC STARTTLS & DANE	ODF OpenAPI spec. REST-API DR NL GOV Ass.	op de goede weg: op weg naar perfect	78%

Aanbesteder	Onderwerp van aanbesteding	Relevante standaarden: gevraagd	Relevante standaarden: NIET gevraagd	Oordeel	
Regio Rivierenland	Het ontwikkelen, implementeren, beheren, onderhouden en doorontwikkelen van een datadistributiesysteem. De nieuwe datadistributie-applicatie gaat ingezet worden om de datadistributie en het beheer van gemeenten Zaltbommel en Maasdriel te faciliteren.	HTTPS & HSTS TLS ISO 27001 ISO 27002 IPv4 & IPv6 SPF DKIM DMARC STARTTLS & DANE StUF	ODF DNSSEC SAML	op de goede weg: op weg naar perfect	77%
Gemeente Waddinxveen	De gemeente Waddinxveen maakt al jaren gebruik van Cipers/iBurgerzaken van PinkRoccade als applicatie voor burgerzaken. Ook werkt Waddinxveen met de Makelaarsuite van PinkRoccade. De looptijd van deze overeenkomsten gaat eindigen en daarom voert Waddinxveen een aanbestedingsprocedure uit om de komende jaren invulling te geven aan de functionaliteit die deze applicaties momenteel bieden.	DNSSEC Digitoegankelijk Digikoppeling ISO 27001 ISO 27002 SAML PDF DKIM DMARC SPF STARTTLS & DANE StUF	ODF IPv4 & IPv6 HTTPS & HSTS TLS	op de goede weg: op weg naar perfect	75%

Aanbesteder	Onderwerp van aanbesteding	Relevante standaarden: gevraagd	Relevante standaarden: NIET gevraagd	Oordeel	
Stichting Waternet	Een planning&control systeem voor het digitaliseren van de P&C-producten/processen. Binnen deze P&C-tool werken zowel medewerkers van Waternet als bestuurders van AGV en de gemeente Amsterdam samen aan de realisatie van de P&C-producten.	DNSSEC HTTPS & HSTS TLS ISO 27001 ISO 27002 SPF DKIM DMARC STARTTLS & DANE PDF	Digitoegankelijk ODF IPv4 & IPv6 XBRL	op de goede weg: op weg naar perfect	71%
Gemeente Lelystad	Men wil de huidige belastingapplicatie vervangen voor een nieuwe applicatie (SaaS oplossing).	Digitoegankelijk Digikoppeling HTTPS & HSTS TLS ISO 27001 ISO 27002 StUF SPF DKIM DMARC PDF	DNSSEC ODF IPv4 & IPv6 SAML STARTTLS & DANE	op de goede weg: op weg naar perfect	69%
Gemeente Nunspeet	De aanbesteding betreft het leveren van een financieel systeem voor de gemeente Elburg en de gemeente Nunspeet. Naar alle waarschijnlijkheid middels een SaaS-oplossing.	DNSSEC ISO 27001 ISO 27002 HTTPS & HSTS TLS PDF NLCIUS StUF SPF DKIM DMARC	IPv4 & IPv6 Digikoppeling ODF SAML XBRL STARTTLS & DANE	op de goede weg: middenmoot	65%

Aanbesteder	Onderwerp van aanbesteding	Relevante standaarden: gevraagd	Relevante standaarden: NIET gevraagd	Oordeel	
Gemeente Vijfheerenlanden	Een oplossing ter ondersteuning van het documentmanagement (DMS) volgens de Archiefwet en van de werkprocessen.	Digikoppeling HTTPS & HSTS TLS ISO 27001 ISO 27002 SAML StUF Geo-standaarden	IPv4 & IPv6 DNSSEC ODF SPF DKIM DMARC STARTTLS & DANE	op de goede weg: middenmoot	53%
Stichting Waternet	De huur van Multifunctionele printers (MFP's), software en levering van supplies. De dienstverlening betreft de installatie van 38 MFP's (combinatie van kleurenapparatuur en zwart wit) inclusief configuratie en beheer. De aangeboden MFP's dienen op afstand middels een SaaS-oplossing en web interface geconfigureerd kunnen worden.	HTTPS & HSTS TLS ISO 27001 ISO 27002 PDF	IPv4 & IPv6 DNSSEC SPF DKIM DMARC STARTTLS & DANE	op de goede weg: middenmoot	45%
Veiligheidsregio IJsselland	Het leveren en onderhouden o.b.v. lease van multifunctionals aan de Veiligheidsregio IJsselland en de GGD IJsselland.	ISO 27001 ISO 27002 PDF HTTPS & HSTS TLS	DNSSEC ODF SAML SPF DKIM DMARC STARTTLS & DANE	op de goede weg: middenmoot	42%

Gemeente Deventer	Het leveren van een oplossing voor de uitvoeringsondersteuning van de processen in het sociaal domein voor de gemeenten Deventer, Olst-Wijhe en Raalte betrokken bij het DOWR samenwerkingsverband. De opdracht is om de applicaties in scope te (her)contracteren (incl. realisatie van technische en functionele implementatie, training en nazorg). De aanbesteder is op zoek naar een gedeeltelijk nieuwe informatiehuishouding in het sociale domein dat wendbaarder is en beter op elkaar aansluit/gekoppeld is.	HTTPS & HSTS TLS ISO 27001 ISO 27002 StUF SAML	IPv4 & IPv6 SPF DKIM DMARC STARTTLS & DANE ODF DNSSEC Digitoegankelijk Digikoppeling	op de goede weg: middenmoot	40%
Gemeente Noordenveld	ICT oplossing ter ondersteuning van de processen voor het heffen, invorderen, waarderen, bezwaar & beroep en E-loket van de gemeentelijke belastingen.	ISO 27001 ISO 27002 SAML StUF Digikoppeling Digitoegankelijk	HTTPS & HSTS TLS IPv4 & IPv6 SPF DKIM DMARC STARTTLS & DANE ODF DNSSEC	op de goede weg: middenmoot	40%

Inkoop Midden Groningen	Een oplossing waarmee: omgevingswetbesluiten vastgesteld kunnen worden conform de Omgevingswet; omgevingswetbesluiten onderhouden kunnen worden conform de toepassingsprofielen: omgevingsdocumenten (TPOD)1, omgevingsplan en omgevingsvisie; omgevingswetbesluiten gepubliceerd kunnen worden naar de LVBB via de standaard officiële overheidspublicaties (STOP); de gemeente ondersteund wordt bij de doelstellingen binnen de projectstartarchitectuur.	ISO 27001 ISO 27002 StUF Geo-standaarden	DNSSEC SPF DKIM DMARC STARTTLS & DANE IPv4 & IPv6 HTTPS & HSTS TLS	op de goede weg: nog een heel eind te gaan	33%
Gemeente Utrecht	De implementatie, hosting, doorontwikkeling en onderhoud van een zwembadapplicatie voor de Utrechtse zwembaden. Deze dienstverlening bestaat uit het leveren van een entreekassasysteem, reserveringssysteem, horeca-kassa en een leerlingvolgsysteem.	ISO 27001 ISO 27002 HTTPS & HSTS TLS	IPv4 & IPv6 SPF DKIM DMARC STARTTLS & DANE ODF DNSSEC Digitoegankelijk	op de goede weg: nog een heel eind te gaan	33%

Samenwerking Vastgoedinformatie Heffing en Waardebepaling	De verwerving van een applicatie voor het (BAG-)objectenbeheer voor de uitvoering van de WOZ- en BAG-werkzaamheden.	ISO 27001 ISO 27002 PDF StUF	HTTPS & HSTS TLS IPv4 & IPv6 ODF SPF DKIM DMARC STARTTLS & DANE DNSSEC SAML Geo-standaarden	op de goede weg: nog een heel eind te gaan	27%
Stichting Inkoopbureau Midden Nederland	Voor het Reinigingsbedrijf Midden Nederland wordt gezocht naar een partij die goed werkende bedrijfssoftware ter ondersteuning van primaire bedrijfsprocessen kan leveren.	ISO 27001 ISO 27002 SETU	HTTPS & HSTS TLS IPv4 & IPv6 SPF DKIM DMARC STARTTLS & DANE DNSSEC SAML StUF	op de goede weg: nog een heel eind te gaan	23%
Gemeente Bergen	Een softwareapplicatie voor de omgevingswet, gericht op de regelbeheer en omgevingsplan.	HTTPS & HSTS TLS Digikoppeling	DNSSEC SPF DKIM DMARC STARTTLS & DANE IPv4 & IPv6 Geo-standaarden SAMl StUF ISO 27001 ISO 27002	op de goede weg: nog een heel eind te gaan	21%

Gemeente Den Haag	Een IVR-SaaS oplossing voor het aan- en afmelden van kentekens van bezoekers door houders van een bezoekersvergunning als dienst (SaaS) inclusief toegang, beheer, onderhoud, functioneel beheer, verstoringsmanagement en hosting van het SaaS oplossing. Het leveren van maatwerk programmatuur in de vorm van een koppeling tussen het IVR-SaaS oplossing en de systemen van de gemeente. .	ISO 27001 ISO 27002	DNSSEC HTTPS & HSTS TLS SPF DKIM DMARC STARTTLS & DANE IPv4 & IPv6	op de goede weg: nog een heel eind te gaan	20%
Gemeente Hollands Kroon	Applicatie/ informatie systeem voor het Sociaal Domein. De huidige applicaties zijn geschikt voor het doel waar deze ooit voor zijn aangeschaft maar sluiten onvoldoende aan de huidige wensen, zoals bijvoorbeeld documenten opslaan in SharePoint en het onttrekken van data uit basisregistraties.	ISO 27001 ISO 27002 SAML	HTTPS & HSTS TLS SPF DKIM DMARC Digitoegankelijk DNSSEC IPv4 & IPv6 STARTTLS & DANE ODF OpenAPI spec. REST-API DR NL GOV Ass.	op de goede weg: nog een heel eind te gaan	19%

B3. Tabellen voor het volledige kalenderjaar 2020 (Q1 tot en met Q4)

Zoals toegelicht in paragraaf 3.1 zullen vanaf nu telkens aanbestedingen van één volledig kalenderjaar worden onderzocht. Voorheen werden de aanbestedingen van Q3+Q4 van het voorgaande jaar en Q1+Q2 van het lopende jaar onderzocht. Over de aanbestedingen in de eerste helft van 2020 is dus al gerapporteerd in de vorige monitor. Voor deze Monitor 2021 zijn eenmalig alleen de aanbestedingen in Q3 en Q4 van 2020 onderzocht.

In deze bijlage worden de cijfers van de aanbestedingen uit Q1 en Q2 2020 (die voor de vorige monitor zijn onderzocht) toegevoegd aan de resultaten voor Q3 en Q4 (van deze monitor), zodat de resultaten voor het volledige kalenderjaar 2020 berekend kunnen worden. Dit samengevoegde overzicht over het hele kalenderjaar 2020 wordt in deze monitor verder niet geanalyseerd, maar het dient als vergelijkingsbasis voor eventuele volgende monitors. Daarom worden de cijfers in deze bijlage zonder verdere toelichting gepresenteerd.

Tabel B3.A: 'Pas toe' en 'leg uit' bij aanbestedingen heel 2020

(Bron: monitor 2020 voor januari t/m juni 2020 en onderzoek aanbestedingen juli t/m december 2020, uitgevoerd zomer 2021 [grijze kolom]).

	Rijksoverheid 1e helft 2020		Mede-Overheden 1e helft 2020		**Totaal 2e helft 2020**		**Totaal 2020**	
	#	%	#	%	#	%	**#**	**%**
totaal aantal beoordeelde aanbestedingen waarbij OSn relevant waren	18	100%	18	100%	40	100%	**76**	**100%**
* **perfect**: alle relevante OSn gevraagd	2	11%	0		4	10%	**6**	**8%**
* **op de goede weg**: deel van relevante OSn gevraagd	14	78%	17	94%	35	88%	**66**	**87%**
- op weg naar perfect (67-99%)	3	17%	3	17%	13	33%	**19**	**25%**
- de middenmoot (34-66%)	4	22%	7	39%	12	30%	**23**	**30%**
- nog een heel eind te gaan (1-33%)	7	39%	7	39%	10	25%	**24**	**32%**
geen relevante OSn gevraagd, waarvan	2	11%	1	6%	1	3%	**4**	**5%**
* **matig**: er is wel algemene aandacht voor architectuur-kaders en/of OSn-beleid	0	0%	0	0%	0	0%	**0**	**0%**
* **slecht**: geen aandacht voor OSn-beleid	2	11%	1	6%	1	3%	**4**	**5%**
* **heel slecht**: strijdig met OSn-beleid	0	0%	0	0%	0	0%	**0**	**0%**
In aantallen standaarden:								
totaal aantal relevante OSn	177	100%	224	100%	487	100%	**888**	**100%**
totaal aantal gevraagde relevante OSn	73	41%	88	39%	264	54%	**425**	**48%**
niet alle OSn gevraagd => Leg Uit vereist (voor toelichting: zie paragraaf 3.5)	16	100%	18	100%	36	100%	**70**	**100%**
alle afkomstig uit 2020	16	100%	18	100%	36	100%	**70**	**100%**
- concrete verantwoording in jaarverslag	0	0%	0	0%	0	0%	**0**	**0%**
- beperkte verantwoording in jaarverslag	5	31%	0	0%	4	12%	**9**	**13%**
- geen Leg Uit in jaarverslag	11	69%	18	100%	32	88%	**61**	**87%**

Tabel B3.B: 'Pas toe' bij aanbestedingen in heel 2020, per standaard

	Rijksoverheid Q1+2 2020		Mede-overheden Q1+2 2020		Rijk + Mede-overheden Q3+4 2020		**Totaal heel 2020**
	relevant	gevraagd in % relevant	relevant	gevraagd in % relevant	relevant	gevraagd in % relevant	**gevraagd in % relevant**
aantal aanbestedingen:	*18*		*18*		*40*		**76**
Internet & beveiliging:							
DKIM	10	10%	13	15%	30	40%	**28%**
DMARC	10	10%	13	15%	30	40%	**28%**
DNSSEC	12	17%	14	29%	33	30%	**27%**
HTTPS en HSTS	15	47%	17	47%	35	71%	**60%**
IPv6 en IPv4	13	8%	16	0%	33	18%	**11%**
NEN-ISO\IEC 27001:2005nl	18	78%	18	89%	39	98%	**91%**
NEN-ISO\IEC 27002:2007nl	18	78%	18	89%	39	98%	**91%**
NL GOV Assurance	nvt		nvt		3	0%	**0%**
SAML	9	56%	9	56%	22	55%	**55%**
SPF	10	10%	13	15%	30	40%	**28%**
STARTTLS en DANE	10	10%	13	15%	30	30%	**23%**
STIX en TAXII	0		0		1	0%	**0%**
TLS	15	47%	17	47%	35	71%	**60%**
WPA2 Enterprise	0		1	100%	0		**100%**
Document &							
Ades Baseline Profiles	1	100%	0	0	2	50%	**67%**
CMIS	1	100%	5	40%	nvt		**50%**
Digitoegankelijk	5	80%	5	60%	17	65%	**67%**
ODF	7	29%	7	0%	21	0%	**6%**
OWMS	0		0		2	50%	**50%**
PDF	9	56%	12	50%	21	86%	**69%**
SKOS	0		0		0		
REST API's:							
OpenAPI Specification	4	75%	0	0%	10	30%	**43%**
REST_API Design Rules	0		0	0%	6	0%	**0%**
E-facturatie &							
NLCIUS	1	0%	2	50%	4	100%	**71%**
SETU	0		3	0%	5	60%	**38%**
WDO Datamodel	0		0		0		
XBRL	1	100%	1	100%	3	33%	**60%**
Stelselstandaarden:							
Digikoppeling	1	100%	8	25%	12	67%	**52%**
Geo−standaarden	3	0%	2	50%	7	57%	**42%**
StUF	0		6	100%	13	85%	**89%**
Water & Bodem:							
Aquo Standaard	0		0		0		
SIKB 0101	1	0%	0		1	0%	**0%**
SIKB 0102	0		0		0		
Bouw:							
COINS	0		1	0%	0		**0%**
IFC	1	100%	2	0%	1	0%	**25%**
NLCS	0		1	0%	0		**0%**
Visi	0		0		0		
Juridische verwijzingen:							
BWB	1	0%	1	0%	0		**0%**
ECLI	1	0%	0		0		**0%**
JCDR	1	0%	1	0%	0		**0%**
Onderwijs & loopbaan:							
E−portfolio	0		4	0%	2	0%	**0%**
NL LOM	0		1	0%	0		**0%**
Overig:							
EML_NL	0		0		0		
Totaal	177	41%	224	39%	487	54%	**48%**

Tabel B3.C: Open standaarden relevant / gevraagd bij aanbestedingen in heel 2020

(Bron: Monitor 2020 voor januari t/m juni 2020 en Monitor 2021voor juli t/m december 2020.)
Cijfers 2e helft 2020: zie Tabel 6 in hoofdstuk 3 (niet overgenomen in onderstaand overzicht).

	Rijksoverheid Q1+2 2020		Mede-overh. Q1+2 2020		**Totaal heel 2020**	
	relevant in % aanbest.n	gevraagd in % aanbest.n	relevant in % aanbest.n	gevraagd in % aanbest.n	relevant in % aanbest.n	gevraagd in % aanbest.n
aantal aanbestedingen:	*18*		*18*		**76**	
Internet & beveiliging:						
DKIM	56%	6%	72%	11%	**70%**	**20%**
DMARC	56%	6%	72%	11%	**70%**	**20%**
DNSSEC	67%	11%	78%	22%	**78%**	**21%**
HTTPS en HSTS	83%	39%	95%	60%	**88%**	**51%**
IPv6 en IPv4	72%	6%	94%	44%	**82%**	**9%**
NEN-ISO\IEC 27001:2005nl	100%	78%	100%	89%	**99%**	**89%**
NEN-ISO\IEC 27002:2007nl	100%	78%	100%	89%	**99%**	**89%**
NL GOV Assurance	nvt		nvt		**4%**	**0%**
SAML	50%	28%	50%	28%	**53%**	**29%**
SPF	56%	6%	72%	11%	**70%**	**20%**
STARTTLS en DANE	56%	6%	72%	11%	**70%**	**20%**
STIX en TAXII	0%		0%		**1%**	**0%**
TLS	83%	39%	95%	44%	**88%**	**51%**
WPA2 Enterprise	0%		6%	6%	**1%**	**0%**
Document & (web)content:						
Ades Baseline Profiles	6%	6%	0%		**4%**	**3%**
CMIS	6%	6%	28%	11%	**8%**	**4%**
Digitoegankelijk *)	28%	22%	28%	17%	**36%**	**24%**
ODF	39%	11%	39%	0%	**46%**	**3%**
OWMS	0%		0%		**3%**	**1%**
PDF	50%	28%	67%	33%	**55%**	**38%**
SKOS	0%		0%		**0%**	
REST-API's:						
OpenAPI Specification	22%	17%	0%		**18%**	**8%**
REST-API Design Rules	0%		0%		**8%**	**0%**
E-facturatie & administratie:						
NLCIUS	6%	0%	11%	6%	**9%**	**7%**
SETU	0%		17%	0%	**11%**	**4%**
WDO Datamodel	0%		0%		**0%**	
XBRL	6%	6%	6%	6%	**7%**	**4%**
Stelselstandaarden:						
Digikoppeling	6%	6%	44%	11%	**28%**	**14%**
Geo−standaarden	17%	0%	11%	6%	**16%**	**7%**
StUF	0%		33%	33%	**25%**	**22%**
Water & Bodem:						
Aquo Standaard	0%		0%		**0%**	
SIKB 0101	6%	0%	0%		**3%**	**0%**
SIKB 0102	0%		0%		**0%**	
Bouw:						
COINS	0%		6%	0%	**1%**	**0%**
IFC	6%	6%	11%	0%	**5%**	**1%**
NLCS	0%		6%	0%	**1%**	**0%**
Visi	0%		0%		**0%**	
Juridische verwijzingen:						
BWB	6%	0%	6%	0%	**5%**	**0%**
ECLI	6%	0%	0%		**1%**	**0%**
JCDR	6%	0%	6%	0%	**3%**	**0%**
Onderwijs & loopbaan:						
E−portfolio	11%	0%	0%		**5%**	**0%**
NL LOM	0%		6%	0%	**1%**	**0%**
Overig:						
EML_NL	0%		0%		**0%**	

B4. Rapportage Open standaarden en voorzieningen (PBLQ)

Auteurs: Anne Graas, Jinne Samsom, Piet Hein Minnecré, PBLQ, 13-8-2021

1. Inleiding

1.1. Aanleiding

De Monitor Open Standaardenbeleid brengt jaarlijks in kaart of het 'pas toe of leg uit'-principe door overheidsorganisaties is ingevoerd en wordt nageleefd. ICTU voert hiertoe jaarlijks een onderzoek uit in opdracht van Bureau Forum Standaardisatie en heeft PBLQ gevraagd een scan te maken van een aantal overheidsvoorzieningen.

1.2. Opdrachtformulering

Doel van deze opdracht is het creëren van een beeld van de toepassing van open standaarden bij de verschillende voorzieningen van de overheid. Oorspronkelijk bestond de te onderzoeken lijst uit voorzieningen in de Gemeenschappelijke Digitale Infrastructuur (GDI), maar op verzoek van het ministerie van BZK zijn daar andere voorzieningen aan toegevoegd. Dit maakt dat de voorzieningen die de laatste jaren zijn onderzocht een divers karakter hebben. In overleg met het Forum Standaardisatie wordt dit jaar een aangepaste lijst van voorzieningen onderzocht.

De oorspronkelijke lijst is opgedeeld in een set voorzieningen die direct raakt aan de communicatie en gegevensuitwisseling met burgers en bedrijven en een set voorzieningen die vooral gericht is op de communicatie en gegevensuitwisseling tussen overheden dan wel op de onderliggende infrastructuur.

Door een beperkte set van voorzieningen te onderzoeken:
- Reduceren we de administratieve lasten voor de beheerders van voorzieningen;
- Vergroten we de tijd tussen de onderzoeken zodat meer ruimte ontstaat voor de implementatie van de standaarden;
- Vergroten we de leesbaarheid van de rapportage. Door de logische tweedeling is het rapport minder lijvig.

Dit jaar zijn de voorzieningen onderzocht die vooral gericht zijn op de communicatie en gegevensuitwisseling tussen overheden dan wel op de onderliggende infrastructuur. Dit betekent dat in de regel een vergelijking is gemaakt met de bevindingen van de monitor uit 2019.

1.3. Werkwijze

Voor dit onderzoek is gebruik gemaakt van de 'pas toe of leg uit'-lijst van 1 april 2021. Voor elke voorziening is (samen met de beheerder) gekeken of de standaarden op deze lijst relevant zijn. Daarbij is telkens uitgegaan van de eindgebruiker. Dat is degene die in de keten baat zou moeten hebben bij het gebruik van open standaarden. Dit is expliciet zo gekozen, omdat het beleid ten aanzien van standaardisatie vooral gericht is op het stimuleren van interoperabiliteit. In eerdere onderzoeken is gebleken dat beheerders van voorzieningen soms terminologie gebruiken zoals 'voorbereid' zijn op een standaard, het ‘deels

geïmplementeerd' hebben of 'standaard xyz-ready zijn'. Hiermee bedoelen zij dat ze zelf voldoen aan de standaard of bezig zijn de standaard te implementeren, maar dat andere partijen in hun keten nog geen gebruik kunnen maken van de standaard. Er is bijgevolg dan ook geen sprake van interoperabiliteit op basis van gebruik van de standaard. Wanneer er geen sprake is van interoperabiliteit hebben we dat in deze rapportage aangegeven.

In dit onderzoek wordt per voorziening een overzicht opgesteld van relevante standaarden en de mate waarin daarvan gebruik wordt gemaakt. Het vertrekpunt daarbij is telkens het overzicht van het vorige meetmoment, in dit geval dus 2019. Waar mogelijk zijn de standaarden opnieuw getoetst. Daarbij maken we onder meer gebruik van de testen die beschikbaar zijn via internet.nl en RIPEstat. Hiermee kan voor een groot deel van de standaarden getoetst worden of eraan voldaan wordt. Daarnaast kijken we – voor zover mogelijk – of de geplande activiteiten inmiddels uitgevoerd zijn. Voor nieuwe standaarden op de lijst maken we in samenspraak met de beheerders een inschatting of ze relevant zijn voor de voorzieningen.

Op basis van bovenstaande inschattingen en toetsen maken we een eerste overzicht per voorziening. Dat overzicht wordt met een aantal expliciete vragen toegestuurd aan de beheerders van de voorzieningen. Op basis van hun reactie wordt de verzamelde informatie aangescherpt. Het resultaat daarvan wordt voorgelegd aan de opdrachtgever, vervolgens in een definitieve versie toegestuurd aan de beheerders van de voorzieningen en na akkoord opgenomen in de rapportage. Meestal heeft dit proces meerdere iteraties nodig. Daar waar verschillen van mening zijn over het al dan niet voldoen aan de standaarden zijn deze verschillen nader met elkaar besproken. In de gevallen waar de verschillen ook na de gesprekken bleven bestaan, is dit duidelijk opgenomen in de rapportage.

1.4. Aandachtspunten voor de lezer

1.4.1. Voorzieningen en standaarden geordend op basis van functionaliteit

De voorzieningen in deze monitor zijn op verzoek van de opdrachtgever op basis van functionaliteit gegroepeerd. De volgende functionele groepen worden in deze monitor onderscheiden:

- Identificeren en authenticeren
- Dienstverlening en informatieverstrekken
- Gegevens en registreren
- Dienstverlening en verbinden

1.4.2. Status

In de rapportage is per voorziening een tabel opgenomen. Daarin staan de standaarden genoemd die relevant zijn voor de voorzieningen en de status van de standaard zoals toegekend door de onderzoekers. De status kan de volgende waarden hebben:

- Ja: De voorziening is conform de standaard,
- Nee: De voorziening is niet conform de standaard,
- Deels: Onderdelen van de voorziening zijn conform aan de standaard, maar niet alle onderdelen,
- Gepland: Er zijn concrete plannen (gekoppeld aan een datum) om de voorziening op korte termijn conform te maken aan de standaard.

1.4.3. Relevantie standaard

Voor de relevantiebepalingen zijn per standaard de beschrijvingen van het functioneel en organisatorisch toepassingsgebied zoals vermeld op de pas toe of leg uit-lijst van het Forum Standaardisatie gehanteerd. Standaarden die niet relevant zijn voor een voorziening zijn niet in de tabel opgenomen. In een beperkt aantal gevallen is onder de tabel nog een toevoeging opgenomen over standaarden die in de eerste inschatting wel relevant leken, maar dat bij nadere inspectie (nog) niet zijn. Ook in gevallen waar verwarring zou kunnen ontstaan over de relevantie is een nadere toelichting onder de tabel opgenomen. Daarnaast is voor de standaarden die dit jaar nieuw zijn op de lijst opgenomen of ze relevant zijn. Deze inschatting is samen met de beheerders van de voorzieningen gemaakt.

1.4.4. Wijze van toetsen standaard

Toetsen en het bevragen van beheerders

Het toetsen wanneer een voorziening aan een standaard voldoet is lastig. Het vereist een heldere afbakening van de voorziening en heldere voorwaarden wanneer voldaan wordt aan een standaard. Daarnaast zou het toetsten van compliancy in sommige gevallen buitengewoon veel tijd, maar ook toegang tot documenten en systemen vergen die de scope van dit onderzoek te buiten gaan. Deels hanteren we de reeds voor sommige standaarden beschikbare toetsen. Hieronder beschrijven we deze in meer detail.

Daarnaast bevragen we de beheerder van de voorziening, en vergelijken we die antwoorden met de resultaten van de toetsen, eerdere antwoorden, en met de antwoorden van andere gerelateerde voorzieningen (bijvoorbeeld indien gebruik gemaakt wordt van hetzelfde platform). Op die manier ontstaat een beeld van de mate waarin de voorziening voldoet aan de standaarden. Waar de antwoorden van de beheerder en PBLQ van elkaar afwijken, geven we dit helder aan in de rapportage. Per voorziening wordt het relevante onderdeel van de rapportage nog ter instemming voorgelegd aan de beheerder.

Bovenstaande werkwijze maakt het mogelijk om ondanks de uitdagingen bij het toetsen van standaarden toch tot een volledig en accuraat beeld te komen.

Gebruik van internet.nl

Voor een groot aantal standaarden hebben we gebruik gemaakt van de website internet.nl. De website is een initiatief van het Platform Internetstandaarden en maakt het mogelijk om het gebruik van standaarden te toetsen op basis van een specifiek domein. Het betreft de volgende standaarden:

- IPv4 en IPv6
- HTTPS/HSTS
- DMARC
- DKIM
- SPF
- STARTTLS en DANE
- TLS

In het onderzoek is de uitslag van deze toetsen vergeleken met de antwoorden van de beheerders van de voorzieningen. In geval van afwijkingen is samen met de beheerder gekeken waar dit aan kan liggen.

Gebruik van RIPEstat

De standaard RPKI wordt getoetst met RIPEstat. Aan de hand van een IP-adres kan worden nagegaan in hoeverre de RPKI-standaard is toegepast.

Webrichtlijnen en Digitoegankelijk

Op 24 mei 2018 is het Tijdelijk besluit digitale toegankelijkheid overheid gepubliceerd in het Staatsblad. Het besluit, dat de Europese toegankelijkheidsrichtlijn (2016/2102) omzet in bindende nationale regelgeving, is per 1 juli 2018 in werking getreden. Het doel is om de toegankelijkheid van websites en mobiele applicaties (apps) van overheidsinstanties te waarborgen.

Het besluit maakt deel uit van een breder pakket aan maatregelen met als doel een inclusieve benadering van digitale overheidsdienstverlening. Uitgangspunt daarbij is dat mensen met en zonder beperking op gelijke basis moeten kunnen deelnemen aan de maatschappij. Als websites goed in elkaar zitten kunnen ze door iedereen worden gebruikt, ook door bezoekers met een beperking.

Concreet moeten overheden vanaf 23 september 2020 voldoen aan het besluit. Vanaf deze datum moeten overheidsinstanties de toegankelijkheidsnorm toepassen op al hun websites. Als een website nog niet volledig toegankelijk is, dan moet de organisatie op basis van een gestructureerde aanpak binnen een redelijk haalbare termijn toewerken om volledig te voldoen aan alle toegankelijkheidseisen. In een toegankelijkheidsverklaring, die is ondertekend door een bestuurder of een verantwoordelijk functionaris, wordt verklaard hoever de overheidsinstantie is gevorderd met de toegankelijkheid van de website.

Dit jaar is gekeken naar de aanwezigheid van een toegankelijkheidsverklaring. Alle verklaringen worden gepubliceerd in het register van toegankelijkheidsverklaringen en kennen een nalevingsstatus. Deze geven aan hoever een overheidsinstantie is gevorderd met het toegankelijk maken van een website en lopen uiteen van de score ‘A’ (Voldoet volledig), ‘B’ (Voldoet gedeeltelijk), ‘C’ (Eerste maatregelen genomen), ‘D’ (Voldoet niet) tot en met ‘E’ (Geen toegankelijkheidsverklaring gepubliceerd). In de tabel is per voorziening aangegeven welke score de toegankelijkheidsverklaring heeft, indien deze is opgenomen in het register.

ISO 27001/2 en de BIO

Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines informatieveiligheid voor Gemeenten, Rijk, Waterschappen en Provincies. Binnen de Rijksoverheid dient elke organisatie een eigen implementatie van de BIO te hebben. De BIO is gestructureerd op de ISO 27001 en ISO 27002 standaard. Indien een organisatie voldoet aan de BIO, dan voldoen zij binnen de context van dit rapport ook aan de verplichting om de ISO 27002 standaard te gebruiken. Waar er een aparte certificering op het gebied van ISO 27001 is toegekend, geven wij dit apart aan.

RPKI

De standaard RPKI staat sinds eind november 2019 op de pas toe of leg uit-lijst van het Forum Standaardisatie. De standaard moet voorkomen dat internetverkeer wordt omgeleid naar systemen van niet-geautoriseerde netwerken en is instrumenteel in het voorkomen van een ‘hijack’ van het verkeer. De standaard draagt daarmee bij aan het voorkomen van het

afhandig maken van gegevens van gebruikers en/of het (on)bewust bereikbaar maken van bepaalde websites.

RPKI is een standaard die sterk 'onder de motorkap' zit, en daarmee ver afstaat van het werk van de gemiddelde beheerder van een voorziening. In veel gevallen wordt ervan uitgegaan dat de netwerkleverancier dit regelt, maar de beheerder is nog steeds verantwoordelijk.

Daarnaast wekt het functioneel toepassingsgebied in de lijst met standaarden verwarring. In schijnbare tegenstelling tot de tekst bij het organisatorisch functioneringsgebied ("van toepassing op overheden en instellingen uit de publieke sector") geeft het functioneel toepassingsgebied aan dat RPKI moet worden toegepast door netwerkaanbieders en houders van blokken IP-adressen bij het aanbieden van netwerkconnectiviteit.

2. Identificeren en authentiseren

2.1. Beheervoorziening BSN en GBA-V

Beheerorganisatie: Rijksdienst voor Identiteitsgegevens (RvIG), Ministerie BZK

Werking en inhoud van BSN Beheervoorziening en GBA-V

De Beheervoorziening BSN (BV-BSN) is het geheel van voorzieningen dat zorgt voor het genereren, distribueren, beheren en raadplegen van het BSN. De GBA Verstrekkingsvoorziening (GBA-V) is de centrale component in het BRP-stelstel. Alle gegevens uit de gemeentelijke basisregistraties zijn ondergebracht in één centrale landelijke database: GBA-V. Beide worden beheerd door de RvIG en maken grotendeels gebruik van dezelfde standaarden. Om die reden worden ze hieronder gezamenlijk behandeld.

Standaard	Status	Toelichting beheerder 2021
Internet en beveiliging		
HTTPS/HSTS (Beveiligd, Versleuteld Webverkeer)	Ja	Op alle aangeboden webservices draaien HTTPS en HSTS.
IPv4 en IPv6 (Internetnummers)	Ja	De diensten GBA-V en BV-BSN zijn middels IPv6 ontsloten.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De Rijksdienst voor Identiteitsgegevens heeft een beveiligingsplan op basis van de BIO. Hier worden externe audits op gedaan. Er is een In Control Verklaring (ICV) aanwezig.
NL GOV Assurance profile for OAuth 2.0 (Beveiligingstandaard voor het autoriseren van toegang tot REST API's)	Nee	Er wordt een pilot in het kader van 'Haal Centraal' bij RvIG voorzien, die begin 2022 wordt gestart. Daarin zijn de uitgangspunten, zoveel mogelijk gebruik maken van het gedachtegoed van Common Ground, bijv. halen bij de bron. Ook wordt middels de NL API strategie en werkgroeplid 'beveiliging' van deze strategie vol ingezet op het oAUTH 2.0 profiel, de design rules en zeer waarschijnlijk ook het OIDC profiel.

REST-API Design Rules (Verzameling regels voor het structureren en documenteren van REST API's)	Nee	Er wordt een pilot in het kader van 'Haal Centraal' bij RvIG voorzien die begin 2022 wordt gestart. Daarin zijn de uitgangspunten, zoveel mogelijk gebruik maken van het gedachtegoed van Common Ground, bijv. halen bij de bron. Ook wordt middels de NL API strategie en werkgroeplid 'beveiliging' van deze strategie vol ingezet op het oAUTH 2.0 profiel, de design rules en zeer waarschijnlijk ook het OIDC profiel.
RPKI (Beveiligen van de routing infrastructuur)	Onbekend	De beheerder heeft geen status kunnen afgeven voor deze standaard.
TLS (Beveiligd Versleuteld emailverkeer)	Ja	De voorziening gebruikt standaard versie 1.2.
Document en (web/app)content		
Digikoppeling 2.0 (Veilige berichtuitwisseling)	Deels	Bij de ontsluiting van de webservices BRP wordt Digikoppeling gehanteerd. Ontsluiting van BV-BSN middels Digikoppeling zal niet plaatsvinden.
StUF (Uitwisseling administratieve overheidsgegevens)	Nee	Er worden stappen gezet richting de ontsluiting middels API's in het programma 'Haal Centraal'. Daarmee wordt niet meer ingezet op StUF.

Ten opzichte van 2019 voldoet de voorziening aan IPv4 en IPv6. De status was nee en is nu ja. De voorziening voldoet deels aan Digikoppeling 2.0. De status gaat van nee naar deels. Nieuw op de lijst staan profile for OAuth 2.0, REST-API Design Rules en RPKI. De voorziening voldoet niet aan NL GOV Assurance profile for OAuth 2.0 en REST-API Design Rules. Of de voorziening voldoet aan RPKI is onbekend.

Concluderend moeten voor de beheervoorziening BSN en GBA-V nog de volgende standaarden (volledig) worden geïmplementeerd: NL GOV Assurance profile for OAuth 2.0, REST-API Design Rules, RPKI en StUF.

3. Dienstverlening en informatieverstrekken

3.1. Rijksportaal

Beheer organisatie: SSC-ICT

Werking en inhoud van Rijksportaal

Rijksportaal is het (Rijksbrede) raamwerk voor intranettoepassing voor alle (kern)departementen en verschillende uitvoeringsinstanties. Hiermee is het merendeel van de oorspronkelijke intranetten van de(kern)departementen vervangen. Rijksportaal geeft de rijksambtenaar toegang tot Rijksbrede en departementspecifieke informatie, bronnen en toepassingen. Ook is het vanuit het Rijksportaal mogelijk om nieuws van andere

departementen te volgen en personeels- en facilitaire zaken te regelen. SSC-ICT voert het technisch beheer en (technisch) applicatiebeheer over het Rijksportaal uit in opdracht van de Dienst Publiek en Communicatie (DPC) van het Ministerie van Algemene Zaken en van CIO Rijk.

Voor Rijksportaal is door Algemene Zaken een aantal domeinnamen geregistreerd, om te voorkomen dat deze door anderen worden geclaimd. Het gaat om:

- rijksportaal.nl, deze verwijst door naar portal.rijksweb.nl
- portal.rp.rijksweb.nl

De eerste twee domeinnamen worden niet gebruikt. Er wordt ook geen e-mail gestuurd vanaf deze domeinen. De enige domeinnaam die gebruikt wordt is dus portal.rp.rijksweb.nl en die is alleen op het interne netwerk bereikbaar (op het internet krijg de gebruiker een melding dat deze niet in de DNS te vinden is). Vanaf dit domein wordt ook e-mail verstuurd.

Update 2021

De beheerder geeft aan dat het huidige Rijksportaal end-of-life is en dat aanpassingen daardoor vaak niet mogelijk zijn. Dit zou economisch gezien niet gewenst zijn aangezien het de bedoeling is dat het huidige Rijksportaal dit jaar nog wordt uitgefaseerd. De huidige planning voor livegang is 6 december 2021. De IV standaarden zijn uiteraard voor zover van toepassing opgenomen in het programma van eisen voor het vernieuwde Rijksportaal. Er zal ook getoetst worden op de toepassing hiervan.

Standaard	Status	Toelichting beheerder 2021
Internet en beveiliging		
DKIM (Preventie van mailspoofing/ phishing)	Nee	Binnen het besloten netwerk van de overheid wordt de mail niet voorzien van de volgende echtheidskenmerken SPF, DKIM en DMARC. Dit is conform beleid, omdat het alleen binnen het besloten netwerk van de overheid blijft.
DMARC (Anti-phishing)	Nee	Binnen het besloten netwerk van de overheid wordt de mail niet voorzien van de volgende echtheidskenmerken SPF, DKIM en DMARC. Dit is conform beleid, omdat het alleen binnen het besloten netwerk van de overheid blijft.
DNSSEC (Beveiligde domeinnamen)	Nee	DNSSEC wordt op het besloten netwerk van de overheid nog niet toegepast. Bij transitie Rijksportaal wordt deze bouwsteen opnieuw ingebracht.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Nee	HTTPS wordt toegepast. HSTS wordt niet ondersteund.
IPv4 en IPv6 (Internetnummers)	Nee	Op het besloten netwerk van de overheid wordt standaard IPv4 gebruikt. Voor IPv6 op het besloten netwerk is nog geen planning afgegeven (keten met Logius en Defensie).
RPKI (Beveiligen van de routing infrastructuur)	Nee	Voor het intranet is RPKI niet ingericht.

SAML (Inloggegevens)	Ja	Er is een project voor vernieuwing SSO Rijk waarin de aansluiting van alle departementen op SAML is gerealiseerd. Er zijn dus geen uitzonderingen meer in departementen in het gebruik van SAML.
SPF (Preventie van mailspoofing/phishing)	Nee	Binnen het besloten netwerk van de overheid wordt de mail niet voorzien van de volgende echtheidskenmerken SPF, DKIM en DMARC. Dit is conform beleid, omdat het alleen binnen het besloten netwerk van de overheid blijft.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Ja, Rijksportaal ondersteunt TLS 1.2, maar de voorziening ondersteunt ook TLS 1.0 en 1.1.
Document en (web/app)content		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	C - eerste - maatregelen genomen	Zelfverklaring aanwezig, zie https://www.toegankelijkheidsverklaring.nl/register/1414
ODF (Document-bewerkingen)	Ja	ODF wordt ondersteund: ODF-bestanden kunnen geüpload en gedownload worden en de inhoud van ODF-bestanden kan door de zoekmachine worden geïndexeerd. Naast ODF worden op het Rijksportaal ook andere documentformaten gebruikt; het gebruik van ODF wordt niet afgedwongen.
PDF 1.7 PDF/A-1, PDF/A-2 (Documentpublicatie/ archivering)	Ja	PDF wordt ondersteund: PDF-bestanden kunnen geüpload en gedownload worden en de inhoud van PDF-bestanden kan door de zoekmachine worden geïndexeerd. Naast PDF 1.7, PDF/A-1 en PDF/A-2 worden op het Rijksportaal ook andere PDF-versies gebruikt; het gebruik van PDF 1.7, PDF/A-1 en PDF/A-2 wordt niet afgedwongen.

Ten opzichte van 2019 voldoet Rijksportaal niet meer aan de standaard DMARC. Ten opzichte van 2019 zijn dit jaar de standaarden HTTPS/HSTS en TLS toegevoegd. De voorziening voldoet niet aan HTTPS/HSTS, maar wel aan TLS. Nieuw op de lijst is RPKI, de voorziening voldoet niet aan de standaard. Dit jaar is Digitoegankelijk getoetst, voor de voorziening zijn de eerste maatregelen genomen en is de score C.

Concluderend moeten voor Rijksportaal nog de volgende standaarden (volledig) geïmplementeerd worden: DNSSEC, HTTPS/HSTS, IPv4 en IPv6, RPKI, Digitoegankelijk, DKIM, DMARC en SPF. De beheerder heeft aangegeven de laatste drie standaarden niet te gaan toepassen. Bureau Forum Standaardisatie zou hierover met de beheerder in gesprek kunnen gaan. Voor de adoptie van overige standaarden heeft de beheerder te kennen gegeven dat hier bij de lancering van het nieuwe Rijksportaal aandacht voor is.

3.2. Doc-Direkt

Beheerorganisatie: Doc-Direkt

Werking en inhoud van Doc-Direkt

Doc-Direkt levert diensten aan een groot aantal onderdelen van de Rijksoverheid en notarissen. Ze wil ministeries en rijksdiensten van dienst zijn bij het organiseren en uitvoeren van informatiebeheer. En als dienstverlener informatievoorziening op de kaart zetten, verbeteren en doorontwikkelen naar hedendaagse en toekomstige eisen. De dienstverlening strekt zich derhalve uit van fysieke archiefbewerking, -beheer en -opslag tot aan het leveren van moderne digitale middelen om fysieke documentstromen (deels) te vervangen. In de nabije toekomst zal Doc-Direkt meer digitaal georiënteerde oplossingen gaan aanbieden om informatie te creëren, beheren, bewerken, delen en archiveren.

Daarnaast beheert Doc-Direkt voor drie ministeries het Document Management Systeem (DMS), een enterprise search oplossing en biedt daarnaast scan- en adviesdiensten op afroep om van ongestructureerde data(-opslag) een doorzoekbaar geheel te maken.

Standaard	Status	Toelichting beheerder 2021
Internet en beveiliging		
DKIM (Preventie van mailspoofing/phishing)	Ja	Doc-Direkt heeft geen eigen maildomeinen in gebruik. Voor het verzenden van mail maakt Doc-Direkt gebruik van de mailservers van SSC-ICT. De mailadressen van de medewerkers behoren tot het standaard maildomein van BZK, waarvoor DKIM actief is.
DMARC (Anti-phishing)	Ja	De mailadressen van de medewerkers behoren tot het standaard maildomein van BZK, waarvoor DMARC actief is.
DNSSEC (Beveiligde domeinnamen)	Ja	De mailadressen van de medewerkers behoren tot het standaard maildomein van BZK, waarvoor DNSSEC actief is.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels/ Gepland	Voor de website doc-direkt.nl wordt de standaard HTTPS/HSTS volledig toegepast. Voor het domein Handelingenbank.info biedt de webserver geen HSTS-policy aan, maar Doc-Direkt heeft een leverancier ingehuurd om dit uit te voeren.
IPv4 en IPv6 (Internetnummers)	Ja	Voor de website doc-direkt.nl en handelingenbank.info wordt de standaard volledig toegepast.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Doc-Direkt bouwt mee aan één CIO-stelsel voor BZK. Informatiebeveiliging en Privacy is een deelstelsel hierin. Via het CIO-stelsel werken we aan een Single Information Single Audit (SISA) methode om aan opdrachtgevers/verantwoorde-lijken te rapporteren over de vorderingen op het gebied van Informatiebeveiliging & Privacy. Doc-Direct bereidt de eerste van deze viermaandsrapportage momenteel voor.

RPKI (Beveiligen van de routing infrastructuur)	Ja	De standaard wordt toegepast.
SAML (Inloggegevens)	Ja	Via de werkplek DWR kunnen medewerkers via SSO inloggen op de door Doc-Direkt beheerde DMS applicatie. Voor aansluiting op de tekenomgeving wordt ook SAML toegepast door SSC-ICT.
SPF (Preventie van mailspoofing/phishing)	Ja	Het domein waar medewerkers van Doc-Direkt hun mailadressen aan ontlenen wordt volgens deze standaard beschermd.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	Het domein waar medewerkers van Doc-Direkt hun mailadressen aan ontlenen wordt volgens deze standaard beschermd.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De standaard wordt gebruikt voor netwerkverbindingen. SSC-ICT levert de werkplek DWR Next, welke geschikt is om TLS 1.2 en 1.3 standaard te verwerken.
Document en (web/app)content		
Ades Baseline Profiles (Digitaal ondertekenen van documenten)	Ja	Doc-Direkt biedt aan afnemers een tekenomgeving, waarin een certificaathouder documenten van een digitale handtekening kan voorzien. Het betreft persoonsgebonden certificaten, conform de standaard.
Digitoegankelijk (EN 301 549 met WCAG 2.1)	1x B en 2x C	Voor drie domeinen zelfverklaring aanwezig, zie: - website Doc-Direct (C) - Handelingenbank.info (C) - Applicatie DigiDoc (B)
ODF (Documentbewerkingen)	Nee	Voor bewerkbare documenten wordt alleen .doc-formaat gebruikt. Er zijn geen plannen ODF te gebruiken.
OWMS (Metadata overheidsinformatie)	Ja	Bij het aanbieden wordt volgens voorschrift metadata toegevoegd.
PDF 1.7 – PDF A/1 of PDF A/2 (Documentpublicatie/ archivering)	Ja	Doc-Direkt ondersteunt in haar archieven vooral PDF/A. Alles wat gescand wordt gaat naar PDF/A. Daarnaast wordt ook 1.7 veel gebruikt.
SKOS (Thesauri en begrippen-woordenboeken)	Nee	De standaard wordt nog niet toegepast. De beheerder gaat later dit jaar navraag doen bij de producteigenaren.
Stelselstandaarden		
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Gepland	Op basis van digikoppeling kan informatie worden uitgewisseld met Nationaal Archief in een acceptatieomgeving. Er wordt gewerkt aan de productieversie van een koppeling met het NA.

Ten opzichte van 2019 voldoet Doc-Direkt nu aan de standaarden TLS en Ades Baseline Profiles. De status is van nee naar ja gegaan. Daarnaast is er een planning afgegeven voor de standaarden Digikoppeling 2.0 (eerder nee) en HTTPS HSTS (eerder deels). Dit jaar zijn getoetst: DNSSEC, STARTTLS en DANE en OWMS. De voorziening voldoet aan deze

standaarden. Dit jaar is Digitoegankelijk getoetst voor meerdere domeinen. Voor één domein voldoet de voorziening gedeeltelijk en heeft een score B, voor de andere twee domeinen zijn nu de eerste maatregelen genomen en is de score C. Nieuw op de lijst staat RPKI, waaraan wordt voldaan.

Concluderend moeten voor Doc-Direkt nog de volgende standaarden (volledig) geïmplementeerd worden: HTTPS/HSTS, Digitoegankelijk, ODF, SKOS, Digikoppeling 2.0.

4. Gegevens en registreren

4.1. Basisregistraties

4.1.1. NHR (Handelsregister)

Beheerorganisatie: Kamer van Koophandel

Werking en inhoud NHR

Het Handelsregister is de basisregistratie waarin alle rechtspersonen en ondernemingen in Nederland zijn opgenomen. Aansluiten op de Basisregistratie Handelsregister gaat om het tot stand brengen van een elektronische verbinding tussen het Handelsregister en de afnemer. Actuele gegevens uit het Handelsregister kunnen worden overgebracht via de informatieproducten van het Handelsregister.

Deze voorziening is ook in 2020 getest en de resultaten zullen daarom ten opzichte van dat basisjaar worden vergeleken.

Standaard	Status	Toelichting beheerder 2021
Internet en beveiliging		
DKIM (Preventie van mailspoofing/phishing)	Ja	Het domein kvk.nl voldoet aan DKIM (zie: https://internet.nl/mail/kvk.nl/).
DMARC (Anti-phishing)	Ja	NHR voldoet op mailservers aan DMARC (zie: https://internet.nl/mail/kvk.nl/).
DNSSEC (Beveiligde domeinnamen)	Gepland	Er is nu outbound DNSSEC ondersteuning voor Exchange Online. Inbound ondersteuning voor het einde van 2021. Dit wel enkel voor Exchange Online diensten. Er is geen concrete planning voor de overige Microsoft 365 clouddiensten en wanneer deze DNSSEC gaan ondersteunen.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening gebruikt zowel HTTPS als HSTS.
IPv4 en IPv6 (Internetnummers)	Deels	Voor wat betreft de website kvk.nl is KVK compliant en wordt zowel IPv6 en IPv4 ondersteund. Enige uitzondering zijn nog de emailservers van de website, zie: kvk-nl.mail.protection.outlook.com.

NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De KvK is sinds 2016 ISO 27001 gecertificeerd en hanteert ISO27002.
NL GOV Assurance profile for OAuth 2.0 (Beveiligingstandaard voor het autoriseren van toegang tot REST API's)	Nee	Met het voldoen aan deze standaard is KVK bezig, maar is nog niet afgerond. Een zekere planning is niet af te geven vanwege interne prioriteitstellingen en andere wettelijke compliancy activiteiten. Of dit nog in 2021 af te ronden is, kunnen we niet met zekerheid zeggen.
Open API Specification (Beschrijven van REST-API's)	Gepland	KVK gebruikt de specificatie actief, de laatste operationele API die op de specificatie nog moet worden aangepast betreft de API Zoeken en Profile, dit wordt in 2021 afgerond.
REST-API Design Rules (Verzameling regels voor het structureren en documenteren van REST API's)	Gepland	De REST-API Design Rules worden toegepast door KVK bij het aanbieden van REST-API's. Er is nog 1 al langer bestaande API die hierop moet worden aangepast, dat is conform planning dit jaar afgerond.
RPKI (Beveiligen van de routing infrastructuur)	Ja	Dit is bij KVK ingeregeld voor zowel IPv4 als IPv6, zie: https://stat.ripe.net/widget/prefix-overview#w.resource=176.117.57.0/24 en https://stat.ripe.net/widget/prefix-overview#w.resource=2001:67c:17ec::/48.
SAML (Inloggegevens)	Ja	eHerkenning is SAML-based en wordt toegepast voor het aanleveren van jaarrekeningen en informatieverstrekking. In de notarisapplicatie kan de notaris van achter zijn computer rechtstreeks opgave doen. Ook hier wordt gebruik gemaakt van SAML als authenticatieprocedure. Omdat gebruik wordt gemaakt van een generiek identificatie- en authenticatiesysteem voor alle diensten van KvK kan SAML voor elke dienst ingezet worden voor authenticatie.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd voor NHR.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Gepland	De voorziening past STARTTLS toe, DANE nog niet (zie: https://internet.nl/mail/kvk.nl/). Volgens planning van Microsoft wordt STARTTLS en DANE eind 2021 ondersteund.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De KvK gebruikt TLS op de verbindingen waar voorheen SSL werd gebruikt. De KvK gebruikt versie TLS 1.2 (zie: https://internet.nl/site/www.kvk.nl/). KVK is actief bezig om alle TLS implementaties op versie 1.3 te krijgen, daarbij is ook de Wet Digitale Overheid een belangrijke aanleiding. Dat verloopt voorspoedig. Een uitzondering geldt voor een stuk

		legacy-programmatuur (AS/400 software) waar TLS 1.0 nog wordt gebruikt. Hiervoor zal een exceptie met risicoanalyse worden opgesteld ter nadere bespreking. In afwachting van de uitfasering van deze legacy willen wij zo min mogelijk aanpassingen daarin doen. Het uitfaseren van deze legacy heeft nogal wat vertraging bij ons opgelopen en zal naar verwachting pas in 2022 worden afgerond.
Document en (web/app)content		
Ades Baseline Profiles (Digitaal ondertekenen van documenten)	Ja	De NHR voldoet aan de Ades Baseline Profiles standaard.
Digitoegankelijk (EN 301 549 met WCAG 2.1)	C - Eerste maat-regelen genomen	Op https://www.kvk.nl/toegankelijkheid/ is de huidige status vermeld, inclusief de toegankelijkheidsverklaring en bevindingen uit het onderzoek van 2020. In juli 2021 wordt opnieuw een onderzoek ingesteld en worden resultaten gepubliceerd. In 2021 wordt ook de HR-app aangepast op toegankelijkheid.
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/ archivering)	Ja	Alle uittreksels en informatie uit het NHR wordt in PDF/A-vorm verstrekt. Het betreft al grotendeels PDF A/2. Er zijn nog documenten in PDF A/1 die moeten worden omgezet. Dit staat gepland om te doen in 2021.
SKOS (Thesauri en begrippen-woordenboeken)	Gepland	SKOS is nog niet geïmplementeerd in Gegevenscatalogus NHR. De standaard wordt wel voorzien door diverse ondersteunende software pakketten in gebruik bij de KVK rondom het NHR. Door herprioritering heeft de implementatie van SKOS in Gegevens-catalogus nog niet plaatsgevonden. Verwachting is nu eind 2021 maar waarschijnlijker 2022.
Stelselstandaarden		
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Ongeveer 10% van het verkeer van het NHR gaat naar medeoverheden. Die uitwisselingen vinden allemaal plaats via Digikoppeling en StUF.
STuF (Uitwisseling administratieve overheidsgegevens)	Ja	Ongeveer 10% van het verkeer van het NHR gaat naar medeoverheden. Die uitwisselingen vinden allemaal plaats via Digikoppeling en StuF.
NLCIUS (Elektronisch factureren)	Nee	Financieel systeem is compliant aan de standaard voor e-facturatie. De modelfactuur dient bij KVK in het Output Management systeem te worden geïmplementeerd. Controle op compliancy aan de modelfactuur moet nog plaatsvinden, inclusief eventuele corrigerende maatregelen.

Ten opzichte van 2020 is de status van de DNSSEC van gepland naar deels gegaan en van IPv4 en IPv6 van nee naar deels gegaan. Daarnaast is er een concrete planning om volledig

te voldoen aan de Open API Specification standaard. Nieuw op de lijst staan NL GOV Assurance profile for OAuth 2.0, REST-API Design Rules en RPKI. De voorziening voldoet aan RPKI en voldoet niet aan NL GOV Assurance profile for OAuth 2.0. Voor REST-API Design Rules is een planning afgegeven. Dit jaar is Digitoegankelijk getoetst, voor de voorziening zijn de eerste maatregelen genomen en is de score C.

Concluderend moeten voor NHR nog de volgende standaarden (volledig) worden geïmplementeerd: DNSSEC, IPv4 en IPv6, STARTTLS en DANE, NL GOV Assurance profile for OAuth 2.0, Open API Specification, REST-API Design Rules, Digitoegankelijk, SKOS en NLCIUS.

4.1.2. BAG, BRK, BGT, WOZ en BRT

Beheerorganisatie: Kadaster

Het Kadaster is de beherende partij voor deze vijf basisregistraties. Het gaat om de volgende basisregistraties:

- BAG: Basisregistratie Adressen en Gebouwen;
- BRK: Basisregistratie Kadaster;
- WOZ: Basisregistratie Waardering Onroerende Zaken (WOZ);
- BGT: Basisregistratie Grootschalige Topografie;
- BRT: Basisregistratie Topografie

Werking en inhoud BAG

De Basisregistraties Adressen en Gebouwen (BAG) zijn de registraties waarin gemeentelijke basisgegevens over alle gebouwen en adressen in Nederland zijn vastgelegd.

Werking en inhoud BRK

De Basisregistratie Kadaster (BRK) bevat informatie over percelen, eigendom, hypotheken, beperkte rechten (zoals recht van erfpacht, opstal en vruchtgebruik) en leidingnetwerken. In de Basisregistratie Kadaster staan kadastrale kaarten met perceel, perceelnummer, oppervlakte, kadastrale grens en de grenzen van het Rijk, de provincies en de gemeenten.

Werking en inhoud WOZ

De Basisregistratie Waarde Onroerende Zaken (WOZ) maakt het mogelijk dat de in de WOZ-beschikking vastgestelde WOZ-waarde door alle overheidsorganisaties, die daarvoor een wettelijke taak hebben, gebruikt kan worden. De Landelijke Voorziening WOZ (LV WOZ) maakt het mogelijk dat afnemers (mits daartoe geautoriseerd) via een centraal loket alle WOZ-gegevens kunnen krijgen.

Werking en inhoud BGT

De Basisregistratie Grootschalige Topografie (BGT) is de gedetailleerde grootschalige digitale kaart van heel Nederland. Alle fysieke objecten zoals gebouwen, wegen, water en natuur worden hierin vastgelegd. De opbouw van de BGT is sinds 10 oktober 2017 gereed. Voor overheden en andere wettelijke gebruikers is het gebruik van de BGT vanaf 1 juli 2017 verplicht.

Werking en inhoud BRT

De Basisregistratie Topografie (BRT) bestaat uit digitale topografische bestanden, veelal kaarten, op verschillende schaal niveaus.

Toelichting 2021:

In 2021 is in samenspraak met de beheerder gekeken naar een betere afbakening voor het onderzoeken van de basisregistraties beheerd door het Kadaster. Ten opzichte van voorgaande jaren zijn hieruit de volgende wijzigingen gekomen:

- Het onderzoeksgebied van webdomeinen is verbreed, naast kadaster.nl, met bag.basisregistraties.overheid.nl, brk.basisregistraties.overheid.nl, brt.basisregistraties.overheid.nl en mijn.kadaster.nl.
- We kijken niet naar pdok.nl (als end-point voor de BGT) en wozwaardeloket.nl (als end-point voor de WOZ). Deze webdomeinen zijn in 2020 onderzocht.
- In tegenstelling tot voorgaande jaren worden alle basisregistraties beheerd door het Kadaster in één paragraaf ondergebracht en in samenhang onderzocht.

Standaard	Status	Toelichting beheerder 2021
Internet en Beveiliging		
DKIM (Preventie van mailspoofing/ phishing)	Ja	Het Kadaster voldoet aan DKIM.
DMARC (Anti-phishing)	Ja	Deze standaard is geïmplementeerd.
DNSSEC (Beveiligde domeinnamen)	Ja	De website www.kadaster.nl ondersteunt DNSSEC (zie: https://internet.nl/domain/www.kadaster.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels	HTTPS en HSTS zijn deels geïmplementeerd (zie: https://internet.nl/domain/www.kadaster.nl/). Eerdere planningen voor volledige implementatie in Q1 en Q4 2018 zijn niet gehaald. HSTS is inmiddels op de meeste Kadaster endpoints geïmplementeerd. Er is een beperkte set aan Digikoppeling gerelateerde content (schema's) die nog niet over kunnen naar HTTPS en HSTS. Er is nog geen duidelijke planning voor.
IPv4 en IPv6 (Internetnummers)	Ja	Zowel IPv4 als IPv6 worden ondersteund door het Kadaster (zie: https://internet.nl/domain/www.kadaster.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Het Kadaster is gecertificeerd voor NEN-ISO/IEC 27001 en hanteert 27002. Het Handboek Beveiliging Kadaster is volledig op de BIO gebaseerd. In het jaarverslag is een in control statement opgenomen.
NL GOV Assurance profile for OAuth 2.0 (Beveiligingstandaard voor het autoriseren van toegang tot REST API's)	Nee	Kadaster gebruikt OAuth 2.0 maar nog niet conform het profiel. Dit heeft impact voor onze klanten. Die moeten hun clients aanpassen omdat het NL-profiel een andere client-authenticatie methode vereist.
Open API Specification (Beschrijven van REST-API's)	Ja	Voor de voorziening is de 3.0.x versie van de standaard geïmplementeerd.

REST-API Design Rules (Verzameling regels voor het structureren en documenteren van REST API's)	Deels	Daar waar API's worden toegevoegd / groot onderhoud plaatsvindt, wordt deze standaard toegepast.
RPKI (Beveiligen van de routing infrastructuur)	Ja	De voorziening voldoet aan RPKI.
SAML (inloggegevens)	Deels	Deels en vanuit het aansluiten op de WDO. We maken steeds meer gebruik van OAuth 2.0 en OpenID Connect.
SPF (Preventie van mailspoofing/ phishing)	Ja	SPF is geïmplementeerd (zie: https://internet.nl/mail/kadaster.nl/).
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Nee	Providers en Google en Microsoft hebben aangegeven deze standaard niet te willen volgen en achter MTA-STS (RFC 8461) en TLS Reporting (RFC 8460) te staan. Inmiddels heeft Microsoft toch aangegeven STARTTLS en DANE te willen ondersteunen. Daar wachten wij nu op.
TLS (Beveiligde, versleutelde verbindingen)	Deels	Deze standaard wordt door het Kadaster ondersteund. Rond 1 van de mailservers wordt hier nog aan gewerkt.
Document en (web/app)content		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	C - Voldoet gedeeltelijk	Er is een zelfverklaring aanwezig voor het webdomein kadaster.nl. Voor het domein basisregistraties.overheid.nl is geen zelfverklaring aangetroffen.
PDF 1.7, PDF/A-1 en PDF/A-2 (Documentpublicatie/ archivering)	Deels	Uittreksels worden verstrekt in PDF 1.4-formaat. Databestanden worden vooral in GML uitgewisseld. GML is een standaard XML-formaat voor Geo-data, gebaseerd op de Geo-standaarden. Afnemers melden geen problemen met het huidige PDF formaat. Daarom geeft het Kadaster geen prioriteit aan het vervangen van PDF 1.4. Voor het archiveren van kennisgevingen wordt gebruik gemaakt van PDF/A-1.
OWMS (Metadata overheidsinformatie)	Nee	OWMS is wel van toepassing, maar PDOK hanteert via het Nationaal GEO Register de wettelijk vastgelegde standaarden, gebaseerd op Inspire en ISO volgens het zogenaamde NL profiel. Data.overheid.nl harvest het NGR met behulp van de CSW standaard (Catalogue Services for the Web' een OGC-Geostandaard (Open Geospatial Consortium), ook onderdeel van INSPIRE). De BRT voldoet dus niet aan de standaard maar voldoet wel aan alternatieve internationale standaarden. Er zijn geen interoperabiliteitsproblemen hierdoor.

SKOS (Thesauri en begrippen-woordenboeken)	Deels	Het Kadaster hanteert SKOS voor de beschikbaarstelling van begrippenkaders van basisregistraties. De begrippenkaders voor de BRK zoals gepubliceerd op brk.basisregistraties.nl, de BAG zoals gepubliceerd op bag.basisregistraties.nl en de BGT (IMgeo) en BRT op definities.geostandaarden.nl zijn allemaal conform SKOS. Voor de WOZ moet deze slag nog worden gemaakt. (4 van de 5 BR's). Hiervoor is nog geen planning. Het Kadaster is alleen verantwoordelijk voor de hosting en het technisch beheer van de LV-WOZ de verantwoordelijkheid voor de implementatie van SKOS ligt bij de Waarderingskamer. Voor zover bij het Kadaster bekend is er geen planning voor de implementatie van SKOS voor de LV-WOZ.
E-facturatie en administratie		
NLCIUS (Elektronisch factureren)	Nee	Invoering van elektronisch factureren is sinds 2018 onderhanden. Blocking issue is daarbij de opzet van onze klanten administratie.
Stelselstandaarden		
Digikoppeling 2.0 (Veilige berichten-uitwisselingen)	Deels	Vrijwel alle koppelingen met afnemers, andere basisregistraties en evt. front-office systemen worden gelegd op basis van Digikoppeling: - de koppelingen voor het aanleveren van gegevens aan LV-BAG, LV-WOZ en LV-BGT zijn gebaseerd op Digikoppeling standaarden; - het aanleveren door bronhouders (o.a. notariaat) van gegevens aan de BRK is niet gebaseerd op Digikoppeling; - de koppelingen voor het verkrijgen van informatie van gegevens uit LV BAG en LV WOZ en BRK zijn gebaseerd op Digikoppeling. Daarnaast kan informatie uit LV's worden verkregen via PDOK (Publieke Dienstverlening op de Kaart) die gebruik maakt van de Open GEO-standaarden. Ook de informatie uit de BRT wordt op deze wijze geleverd. Gegevens uit de BGT zijn beschikbaar via PDOK. Verder wordt de slag gemaakt naar OpenAPI/REST.
Geo-Standaarden (Geografische informatie)	Ja	Naast de INSPIRE richtlijnen, maakt het Kadaster gebruik van NEN3610 en de meest gangbare Geo-standaarden voor de betreffende basisregistraties.
StUF (Uitwisseling administratieve overheidsgegevens)	Ja	Het Kadaster maakt deels gebruik van StUF en is deels volgens de Geo-standaarden (GML) opgemaakt. StUF wordt gebruikt voor aanlevering van bronhouder naar LV-BAG, LV-WOZ en LV-BGT. WOZ en BGT worden ook geleverd in StUF.

Ten opzichte van 2019 is de status van PDF, TLS en SKOS van 'ja' naar 'deels' gegaan. Nieuw op de lijst zijn de standaarden NL GOV Assurance profile for OAuth 2.0, REST-API Design Rules,

RPKI. Dit jaar is SAML getoetst. De voorziening voldoet volledig aan RPKI en SAML en gedeeltelijk aan REST-API. De voorziening voldoet niet aan NL GOV Assurance profile for OAuth 2.0. De Dit jaar is Digitoegankelijk getoetst, voor de voorziening zijn de eerste maatregelen genomen en is de score C.

Concluderend moeten voor de BAG, BRK, BGT, WOZ en BRT nog de volgende standaarden (volledig) worden geïmplementeerd: HTTPS HSTS, SAML, STARTTLS en DANE, TLS, PDF, NL GOV Assurance profile for OAuth 2.0, REST-API Design Rules, Digitoegankelijk, SKOS, NLCIUS en Digikoppeling 2.0.

4.1.3. BRO (Basisregistratie Ondergrond)

Beheer organisatie: Programmabureau BRO van het Ministerie BZK (afdeling DG Bestuur, Ruimte en Wonen– RO)

Werking en inhoud BRO

De Basisregistratie Ondergrond (BRO) brengt alle informatie over de Nederlandse ondergrond op één plek bij elkaar en stelt deze via één loket digitaal beschikbaar. Per 1 januari 2018 is de wet BRO in werking getreden voor de eerste tranche van registratieobjecten (Geotechnisch sondeeronderzoek, Booronderzoek, Grondwatermonitoringput). De ketenprocessen van de BRO zijn ingericht en de bronhouders zijn in staat om aan te (laten) leveren via het Bronhouderportaal aan de Landelijke Voorziening (LV). Er is een gebruiksplicht inwerking getreden voor overheidsorganisaties en iedereen die in opdracht van hen werkzaamheden verricht. Voor meer informatie over de BRO kunt u terecht op de webpagina https://basisregistratieondergrond.nl.

Vanuit de BRO onderzoeken we de volgende webdomeinen: bronhouderportaal-bro.nl, basisregistratieondergrond.nl, pdok.nl, dinoloket.nl, broloket.nl, bro-productomgeving.nl en bromonitor.nl.

Standaard	Status	Toelichting beheerder
Internet en beveiliging		
DKIM (Preventie van mailspoofing/ phishing)	Ja	De DKIM standaard is geïmplementeerd en actief voor bronhouderportaal-bro.nl en broservices.nl.
DMARC (Anti-phishing)	Ja	DMARC voldoen we aan, aangezien dat is ingeregeld door het Standaard Platform.
DNSSEC (Beveiligde domeinnamen)	Deels	Al onze domeinen zijn voorzien van DNSSEC beveiliging. Uitzondering is het mail spamfilter dat wij als cloud dienst afnemen. Voor dit filter is (nog) geen DNSSEC ingericht.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels	BRO website (https://www.basisregistratieondergrond.nl), BRO Bronhouderportaal (https://www.bronhouderportaal-bro.nl), BRO web applicaties (https://www.dinoloket.nl en https://www.broloket.nl), ICTU BRO Monitor (https://www.bromonitor.nl), BRO productomgeving (https://bro-productomgeving.nl), PDOK portaal (https://www.pdok.nl) en API's ondersteunen HTTPS. BRO Bronhouderportaal en ICTU BRO Monitor ondersteunen nog geen HTTPS doorverwijzing (HSTS). Dit is inmiddels wel op

		de backlog opgenomen van het BRO LV developers team. De planning voor implementatie is nog niet bekend. Alle huidige door TNO t.b.v. BRO beheerde websites en webservices zijn dus beveiligd met HTTPS. BRO website (https://www.basisregistratieondergrond.nl), BRO web applicaties (https://www.dinoloket.nl en https://www.broloket.nl), PDOK portaal (https://www.pdok.nl) en API's ondersteunen HSTS.
IPv4 en IPv6 (Internetnummers)	Deels	Alle door TNO t.b.v. BRO beheerde websites en webservices zijn zowel via IPv4 als IPv6 ontsloten. Voor bronhouderportaal-bro.nl en bromonitor.nl geldt dat het domein nog alleen via IPv4 bereikbaar is (webserver).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	TNO (en hosting partij Solvinity) zijn ISO 27001/27002 compliant. ICTU (en hosting partij SP | ODC-Noord) zijn ISO 27001/27002 compliant. PDOK (en hosting partij CapGemini) zijn ISO 27001/27002 compliant.
REST-API Design Rules (Verzameling regels voor het structureren en documenteren van REST API's)	Ja	We hebben ons aangemeld voor controle op de Standaard REST-API Design Rules. Het is nu wachten totdat we getest en goed bevonden worden, we staan hiervoor in de wachtrij.
RPKI (Beveiligen van de routing infrastructuur)	Nee	RPKI is bedoeld om spoofing van prefixen tegen te gaan en is 2 ledig inkomend en uitgaand. Inkomende prefixen (dus: routes die wij binnenkrijgen): wij maken geen gebruik van de full routing table maar van een default route. hierop valt niet te filteren. Onze primaire upstream provider die een default route naar ons adverteert is bezig RPKI uit te rollen. en daarmee liften wij mee op de RPKI bescherming voor inkomende prefixen. Uitgaande prefixen (dus: routes die wij adverteren) : Aangezien wij gebruik maken van een 3e partij voor anti-ddos diensten die daarvoor in ddos situaties more specific routes adverteert kunnen we geen minimal ROA toepassen zoals geadviseerd.
SAML (Inloggegevens)	Ja	Het Bronhouderportaal BRO maakt gebruik van eHerkenning voor authenticatie van gebruikers. eHerkenning ondersteunt SAML. Zie ook evaluatierapport SAML 2.0 Forum Standaardisatie https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS%20180314.3C%20Evaluatie%20SAML%202.0.pdf
SPF (Bescherming tegen e-mailphishing)	Ja	Het SPF record is correct toegevoegd op alle domeinen.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De BRO gebruikt SSL (TLS) certificaten voor inname en uitgifte APIs en voor beveiligde gegevensuitwisseling met PDOK.

Document en (web/app)content		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	B, C en D en deels niet beoordeeld	Enkele van de webdomeinen hebben een zelfverklaring met verschillende statussen (B, C of D). Zie hieronder de specificaties. **Website BRO:** Status B voor het domein https://basisregistratieondergrond.nl (TNO) De toegankelijkheid is getest door een onafhankelijk onderzoeksbureau. Is nu op weg naar Status A. (zie: https://www.toegankelijkheidsverklaring.nl/register/4038). **Overige domeinen:** - Status D voor het domein https://broloket.nl (TNO) Het programmabureau BRO bij BZK is opdracht aan het geven voor een Toegankelijkheidsonderzoek. (zie: https://www.toegankelijkheidsverklaring.nl/register/3565). - Status C voor het domein https://bromonitor.nl (ICTU) (zie: https://www.toegankelijkheidsverklaring.nl/register/4744). - Status C voor het domein https://pdok.nl (Kadaster) (zie: https://www.toegankelijkheidsverklaring.nl/register/1967).
Open API Specification (Beschrijven van REST-API's)	Ja	Het Bronhouderportaal BRO (voorportaal voor validatie van BRO gegevens voordat deze worden door geleverd naar de Landelijke Voorziening BRO) en de REST-API's van de LV-BRO voldoen aan de open API specificatie https://www.bronhouderportaal-bro.nl/bpbro-frontend/documentation/api.html. De Landelijke Voorziening BRO voldoet aan de PTOLU Digikoppeling standaard (SOAP-XML).
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie /archivering)	Ja	Dit is de standaard voor opslag documenten in PDF formaat in BRO DMS. Uiteraard ook voor documentatie die op de website wordt ontsloten.
Stelselstandaarden		
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Landelijke Voorziening BRO inname en uitgifte API's zijn gebaseerd op Digikoppeling 2.0.
Geo-standaarden (Geografische informatie)	Ja	BRO is een geo-basisregistratie. Geografische BRO gegevens worden o.a. beschikbaar gesteld via het GDI geo-knooppunt PDOK (www.pdok.nl). De PDOK APIs zijn gebaseerd op Open Geospatial Consortium standaarden (www.opengeospatial.org), waaronder OGC:WMS, OGC:WMTS, OGC:WFS, OGC:WCS. Geografische gegevens worden uitgeleverd in open bestandsformaten (OGC:GML, OGC:Geopackage, OGC:GeoTIFF). BRO metadata wordt via het Nationaal Georegister (NGR) (www.nationaalgeoregister.nl) ontsloten. Het NGR is gekoppeld met (=wordt geharvest door) data.overheid.nl.

		Het NGR is gebaseerd op de geo-standaarden CSW (Catalog Services fort he Web), ISO 19115 NL profiel (metadata voor geografische datasets), en ISO 19119 NL profiel (metadata voor geografische web services)
Water en bodem		
Aquo-standaard (Watermanagement informatie)	Ja	Relevante onderdelen worden meegenomen in de BRO standaardisatie van het grondwaterdomein (de aquo standaard omvat ook oppervlaktewater hetgeen buiten scope is voor de BRO).
Juridische verwijzingen		
BWB (Identificatie van en verwijzing naar wet- en regelgeving)	Deels	Nieuwe versies van GAS (globale architectuur schets) en PSA (project start architectuur) en aanvullende architectuurdocumenten zullen evenals relevante onderdelen van website en documentatie gebruik maken van deze standaard voor verwijzingen naar wet- en regelgeving. (zie voorbeeld https://www.overheid.nl/help/wet-en-regelgeving/verwijzen-naar-wet-en-regelgeving).

Ten opzichte van 2019 zijn nieuw opgenomen in de tabel DKIM, DMARC, REST-API Design Rules standaard, PDF 1.7, PDF A/1, PDF A/2 en RPKI. Al deze standaarden voldoen en hebben de status ja behalve RPKI, die standaard heeft de status nee. DNSSEC en HTTPS/HSTS zijn van ja naar deels gegaan. Digitoegankelijk is dit jaar getoetst voor verschillende domeinen en daarvan varieert de status. BWB is van gepland naar deels gegaan.

Voor SKOS, SIKB0101, SIKB0102, GWSW geldt dat deze standaarden (mogelijk) in de toekomst relevant zijn. I.v.m. SKOS: De BRO begrippen (o.a. registratieobjecten) worden binnenkort opgenomen in de Stelselcatalogus (gebaseerd op SKOS, zie https://www.noraonline.nl/wiki/Stelselcatalogus ondersteunde standaarden Stelselcatalogus). Het BRO standaardisatieteam o.l.v. Geonovum heeft hierover reeds contact met Logius. I.v.m. SIKB0101: Mogelijk op termijn van belang voor BRO (opname van onderzoeksgegevens over de milieu-hygiënische kwaliteit van de bodem in de BRO wordt op dit moment onderzocht). I.v.m. SIKB0102: Archeologische informatie is geen onderdeel van de BRO > In een mogelijk vervolgprogramma "BRO II" zullen archeologische gegevens mogelijk onderdeel gaan uitmaken van de BRO.

Concluderend moeten voor de BRO nog de volgende standaarden (volledig) worden geïmplementeerd: DNSSEC, HTTPS/HSTS, IPv4 en IPv6, RPKI, Digitoegankelijk en BWB.

4.1.4. BRV (Basisregistratie Voertuigen)

Beheerorganisatie: RDW (Dienst Wegverkeer)

Werking en inhoud van BRV

In de Basisregistratie Voertuigen (BRV) staan gegevens van voertuigen, kentekenbewijzen en personen aan wie het kentekenbewijs is afgegeven. Een organisatie is aangesloten op de Basisregistratie Voertuigen wanneer op een gestructureerde wijze (niet incidenteel) informatie wordt afgenomen uit het Kentekenregister. Alle gemeenten, provincies, waterschappen,

(relevante) departementen, manifestpartijen en andere overheidsorganisaties in en buiten de voertuigenketen zijn aan gesloten op de BRV.

Standaard	Status	Toelichting 2021
Internet en beveiliging		
DKIM (Preventie van mailspoofing/phishing)	Ja	De BRV (basisregistratie voertuigen) voldoet aan DKIM.
DMARC (Anti-phishing)	Ja	De BRV (basisregistratie voertuigen) voldoet aan DMARC.
DNSSEC (Beveiligde domeinnamen)	Gepland	De niet-gevoelige (technische) gegevens uit de BRV zijn te bevragen via www.rdw.nl. Alle .nl rdw domeinen zijn gesigned met DNSSEC. De diensten op (voertuig)gegevens draaien als microservices in de Azure cloud en het is bekend dat hierop geen DNSSEC en daarmee ook DANE mogelijk is. RDW en andere overheidspartijen hebben bij Microsoft gevraagd om dit op te lossen. Microsoft voert Q1-2022 wijzigingen door in de cloud, waardoor DNSSEC en DANE ook daar mogelijk zijn.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Deels	De informatiesite www.RDW.nl voldoet aan HSTS. Voor de domeinen http://rdw.nl en https://rdw.nl kent de HSTS-policy een te korte geldigheidsduur voor caching. Deze max-age wordt aangepast zodat de voorziening helemaal voldoet. De muterende diensten op (voertuig)gegevens, die als microservices in de Azure cloud draaien, voldoen aan HTTPS/HSTS.
IPv4 en IPv6 (Internetnummers)	Deels	Het websitedomein voldoet aan IPv4 en IPv6, maar het maildomein nog niet. IPv4 wordt ondersteund, IPv6 wordt nog niet ingezet. De BRV is te bevragen via www.rdw.nl. Op dit moment ziet de RDW voor de BRV nog geen noodzaak om op IPv6 over te gaan.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De BRV voldoet aan deze standaard, Zie website rdw.nl onder kopje onderzoeken en certificaten: https://www.rdw.nl/over-rdw/kwaliteits--en-servicenormen/onderzoeken
NL GOV Assurance profile for OAuth 2.0 (Beveiligingstandaard voor het autoriseren van toegang tot REST API's)	Nee	Vanuit security wordt aan een patroon voor oauth gewerkt waarin dit profiel voor het betreffende gebruik is gestandaardiseerd.

Open API Specification (Beschrijven van REST-API's)	Ja	De BRV voldoet aan Open API Specification.
REST-API Design Rules (Verzameling regels voor het structureren en documenteren van REST API's)	Nee	Deze standaard is dermate nieuw dat we hier nog niet op hebben kunnen inspelen.
RPKI (Beveiligen van de routing infrastructuur)	Ja	De BRV (basisregistratie voertuigen) voldoet aan RPKI.
SAML (Inloggegevens)	Ja	De BRV voldoet aan SAML.
SPF (Preventie van mailspoofing/phishing)	Ja	RDW ondersteunt en gebruikt de SPF standaard voor email verkeer.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Gepland	Huidige oplossing van Symantec Mail Gateway ondersteunt deze standaard niet en dat is op dit moment niet op te lossen. Daarom richten we ons niet op vervanging van de huidige oplossing, maar op de migratie van mailflow naar Exchange Online in Q1-2022 volgens de vastgestelde roadmap. Dan is het wel ondersteund.
TLS (Beveiligde, versleutelde verbindingen)	Ja	RDW ondersteunt en gebruikt de TLS protocollen op de e-mail servers en Digikoppeling. Er wordt nog gekeken naar verbetering van instellingen, zodat TLS voldoende veilig wordt geïmplementeerd (zie: https://internet.nl/mail/rdw.nl/).
Document en (web/app)content		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	B - voldoet gedeeltelijk	Er is een zelfverklaring aanwezig, zie https://www.toegankelijkheidsverklaring.nl/register/1979 In juli 2021 wordt een nulmeting uitgevoerd, gevolgd door een volledige toegankelijkheidstest op rdw.nl begin 2022. Oplossingen voor de mogelijk gemelde issues (op gebied van ontwerp, bouw en content) worden z.s.m. daarna doorgevoerd, waarbij in het 3e kwartaal 2022 een hertest toegankelijkheid wordt uitgevoerd op rdw.nl. De testen worden door een onafhankelijke partij uitgevoerd. Dit heeft tot doel om via deze aanpak niveau A te bereiken.
OWMS (Metadata overheidsinformatie)	Ja	De toegang tot BRV-data is op data.overheid.nl in overeenstemming met OWMS gemetadateerd beschikbaar.

PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie /archivering)	Ja	Bij digitale dienstverlening worden uittreksels en informatie uit de BRV in PDF/A vorm verstrekt.
SKOS (Thesauri en begrippen-woordenboeken)	Ja	De BRV voldoet aan SKOS.
Stelselstandaarden		
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Deels	RDW maakt voor alle nieuwe uitwisselingen gebruik van Digikoppeling. Dat is onder meer het geval in de uitwisseling met MijnOverheid (Berichtenbox), CJIB, Politie, ILT, CBR, de Belastingdienst, etc. De intentie is uitgesproken om ook bestaande koppelingen pro-actief te migreren om de voordelen van het diginetwerk te benutten. Een planning hiervoor is nog niet vastgesteld.

Ten opzichte van 2019 is de standaard DMARC helemaal doorgevoerd. Verder is er een concrete planning voor de standaarden DNSSEC en STARTTLS en DANE. Van 'nee' naar 'deels' is de standaard IPv4 en IPv6 gegaan. Nieuw op de lijst zijn staan NL GOV Assurance profile for OAuth 2.0 en REST-API Design Rules en RPKI. De voorziening voldoet aan RPKI en niet aan NL GOV Assurance profile for OAuth 2.0 en REST-API Design Rules. Dit jaar is Digitoegankelijk getoetst, de voorziening voldoet gedeeltelijk en heeft de score B.

Concluderend moeten voor de BRV de volgende standaarden nog (volledig) worden doorgevoerd: DNSSEC, HTTPS en HSTS, IPv4 en IPv6, STARTTLS en DANE, NL GOV Assurance profile for OAuth 2.0, REST-API Design Rules, Digitoegankelijk en Digikoppeling 2.0.

4.1.5. BRI (Basisregistratie Inkomen)

Beheerorganisatie: Belastingdienst

Werking en inhoud BRI

In de Basisregistratie Inkomen staat van ongeveer 13 miljoen burgers per jaar het authentiek inkomen gegeven dat gebaseerd is op het verzamelinkomen of het belastbaar jaarloon. Overheidsorganisaties gebruiken de BRI om toeslagen, subsidies of uitkeringen te bepalen.

Standaard	Status	Toelichting beheerder
Internet en beveiliging		
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De BRI voldoet aan de standaard beveiligingseisen van de Belastingdienst. Deze eisen zijn conform het VIR (Voorschrift Informatiebeveiliging Rijksdienst) met classificatie departementaal vertrouwelijk. Voor opsporingsgegevens (FIOD) geldt een strakker regime. Aangezien het beveiligingskader voor de gehele Belastingdienst geldt, is er geen apart in control statement voor de BRI.
RPKI (Beveiligen van de routing infrastructuur)	Ja	Eigen IP-adressen zijn ondertekend met RPKI. De BD valideert niet zelf RPKI ondertekende adressen, dat doet onze internetprovider.

TLS (Beveiligde, versleutelde verbindingen)	Ja	Versie 1.2 van TLS maakt deel uit van de standaard beveiligingsrichtlijnen van de Belastingdienst.
Stelselstandaarden		
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Nee	Digikoppeling wordt toegepast in de rol van afnemer van berichten van basisregistraties(HR). De ebMS-koppeling met Digilevering is operationeel in de productie-omgeving. De aansluiting op Digilevering wordt nu alleen gebruikt in de rol van afnemer van het stelsel van basisregistraties. Het aansluiten van de BRI als Basisregistratie/leverancier op Digilevering is niet gepland.

Ten opzichte van 2019 is er wel een reactie gekomen van de beheerder van de BRI. Anders dan in 2018 werd verwacht, voldoet de BRI nog niet aan de Digikoppeling 2.0. Nieuw op de lijst staat RPKI. De BRI voldoet aan deze standaard.

Samenvattend moeten voor de BRI nog de volgende standaarden (volledig) worden geïmplementeerd: Digikoppeling 2.0.

4.2. Digilevering

Beheerorganisatie: Logius

Inhoud en werking van Digilevering

Digilevering is een abonnementenvoorziening voor het automatisch verstrekken van gebeurtenisberichten vanuit een basisregistratie. Een gebeurtenisbericht is bijvoorbeeld het starten van een bedrijf of een verandering in iemands inkomen. Afnemers van basisregistraties ontvangen via Digilevering wijzigingen in de vorm van automatisch gegenereerde berichten waarop zij geabonneerd zijn.

(Opmerking m.b.t. DKIM, DNSSEC, HTTPS/HSTS, SPF en STARTTLS & DANE: Digimelding en Digilevering zijn op het Equinix-platform geïmplementeerd, de applicaties kunnen alleen via de mail-relay server van het platform e-mail versturen. Deze mail-relay server is niet van buitenaf benaderbaar, daarom kan dit met internet.nl niet getoetst worden.)

Standaard	Status	Toelichting beheerder
Internet en beveiliging		
DKIM (Preventie van mailspoofing/phishing)	Ja	Digilevering draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. DKIM is geïmplementeerd op de centrale voorziening mail relay.
DMARC (Anti-phishing)	Ja	DMARC is inmiddels geïmplementeerd en doorgevoerd in de DNS instellingen.

DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC is geïmplementeerd op de centrale voorziening DNS (portaal.digilevering.nl).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	Digilevering voldoet aan de HTTPS standaard. Voor Digilevering is een PKIO certificaat verplicht om te kunnen aanloggen op de applicatie. Zonder dit certificaat kan de https doorverwijzing niet slagen en biedt www.internet.nl geen toetsing. HSTS wordt aangeboden.
IPv4 en IPv6 (Internetnummers)	Nee	IPv6 kan niet worden aangeboden, omdat de infrastructuur van Logius dit nog niet voldoende ondersteunt. Dit is een Logius breed vraagstuk. De vraag hoe IPv6 geïmplementeerd dient te worden is wederom bij onze architecten ingediend. IPv6 wordt bij de overgang naar het Logius Standaard Platform ingericht.
RPKI (Beveiligen van de routing infrastructuur)	Ja	Digilevering gebruikt het Logius infrastructuur platform.
SPF (Preventie van mailspoofing/phishing)	Ja	Digilevering draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. SPF is geïmplementeerd op de centrale voorziening mail relay.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	Digilevering draait op het Logius Managed Services platform. Vanuit de clouddienst is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. DANE is in de DNS file opgenomen.
Document en (web/app)content		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	B - Voldoet gedeeltelijk	Eerste wijzingen vanuit het Digitoegankelijkheids onderzoek zijn doorgevoerd.
Stelselstandaarden		
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Digilevering maakt gebruik van Digikoppeling.

Ten opzichte van 2019 staat RPKI nieuw op de lijst. Digilevering lijkt bij toetsing te voldoen aan deze standaard. De beheerder kan dit echter niet bevestigen en geeft aan dat dit bij Equinix ligt. Dit jaar is Digitoegankelijk getoetst, de voorziening voldoet gedeeltelijk en heeft status B.

Samenvattend, moeten voor Digilevering de volgende standaarden nog (volledig) worden geïmplementeerd: IPv4 en IPv6 en Digitoegankelijk.

4.3. Digimelding

Beheerorganisatie: Logius

Inhoud en werking van Digimelding

Met Digimelding kunnen overheden bij gerede twijfel (vermeende) onjuistheden in de gegevens van Basisregistraties uniform en efficiënt terugmelden aan de bronhouders van die Basisregistraties. Bronhouders onderzoeken vervolgens de fout en verbeteren deze zo nodig in de basisregistratie. Digimelding is daarmee een onderdeel van een aantal middelen om de kwaliteit van het stelsel van Basisregistraties te borgen.

Standaard	Status	Toelichting beheerder
Internet en beveiliging		
DKIM (Preventie van mailspoofing/phishing)	Ja	DKIM is geïmplementeerd.
DMARC (Anti-phishing)	Ja	DMARC is geïmplementeerd.
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC is geïmplementeerd.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De url portaal.digimelding.nl voldoet aan HTTPS en HSTS.
IPv4 en IPv6 (Internetnummers)	Nee	Digimelding gebruikt het Logius infrastructuur-platform. IPv6 kan niet worden aangeboden, omdat de infrastructuur van Logius dit nog niet voldoende ondersteunt. Dit is een Logius breed vraagstuk. De vraag hoe IPv6 geïmplementeerd dient te worden is wederom bij onze architecten ingediend. Digimelding ondersteunt op dit moment alleen IPv4.
RPKI (Beveiligen van de routing infrastructuur)	Ja	Digimelding gebruikt het Logius infrastructuurplatform.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	Digimelding draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. STARTTLS en DANE opgenomen in DNS file.

Document en (web/app)content		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	B - Voldoet gedeeltelijk	De eerste wijziging zijn doorgevoerd.
Stelselstandaarden		
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Digimelding maakt gebruik van Digikoppeling.

Ten opzichte van 2019 is de status van DKIM van gepland naar ja gegaan en ik de status van STARTTLS en DANE van nee naar ja gegaan. Ten opzichte van 2019 staat RPKI nieuw op de lijst. Digimelding voldoet aan deze standaard. Dit jaar is Digitoegankelijk getoetst, de voorziening voldoet gedeeltelijk en heeft een score B.

Samenvattend, moeten voor Digimelding de volgende standaarden nog (volledig) worden geïmplementeerd: IPv4 en IPv6 en Digitoegankelijk.

4.4. Stelselcatalogus

Beheerorganisatie: Logius

Inhoud en werking van stelselcatalogus

De Stelselcatalogus geeft inzicht in de begrippen en definities die worden gebruikt binnen het stelsel van Basisregistraties. De Stelselcatalogus geeft gebruikers, afnemers, leveranciers en anderen een zo volledig mogelijk beeld van de beschikbare gegevens, begrippen en hun betekenis binnen het Stelsel van Basisregistraties. De Stelselcatalogus helpt op die manier om de overheidsdoelstelling van 'eenmalige gegevensaanlevering en meervoudig gebruik' te realiseren.

Standaard	Status	Toelichting beheerder
Internet en beveiliging		
DMARC (Anti-phishing)	Ja	De Stelselcatalogus voldoet aan DMARC (zie: https://internet.nl/mail/stelselcatalogus.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC is geïmplementeerd op de centrale voorziening DNS (zie: https://internet.nl/site/www.stelselcatalogus.nl/).
HTTPS/ HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening voldoet aan aan HTTPS (zie: https://internet.nl/site/www.stelselcatalogus.nl/).
IPv4 en IPv6 (Internetnummers)	Gepland	De Stelselcatalogus gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt niet de open standaard IPv4 en IPv6 voor internet gebruik. Stelselcatalogus ondersteunt geen IPv6 (zie: https://internet.nl/site/www.stelselcatalogus.nl/). Omdat de Stelselcatalogus (e.a. Logius voorzieningen) gaan migreren naar een nieuw infrastructuurplatform is besloten om voor deze voorzieningen IPv6 te gaan implementeren na de inframigratie. Planning is dat dit medio 2022 gebeurt.

REST-API Design Rules (Verzameling regels voor het structureren en documenteren van REST API's)	Ja	De voorziening voldoet aan deze standaard.
RPKI (Beveiligen van de routing infrastructuur)	Ja	De voorziening voldoet aan RPKI (zie: RIPEstat: LaunchpadSearch/144.43.243.69)
Document en (web/app)content		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	C - Eerste maat-regelen genomen	Toegankelijkheidsinspectie is uitgevoerd in week 16 (april 2021). Er wordt reeds aan 36 van de 50 inspectiepunten voldaan. Overige 14 punten zijn reeds toegevoegd aan de back log om uitgevoerd te worden. Planning is dat dit in Q4 2021 zal worden geïmplementeerd.
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/ archivering)	Ja	Documenten worden als PDF-A/1 aangeboden via de website.
SKOS (Thesauri en begrippen-woordenboeken)	Ja	SKOS wordt toegepast door de voorziening.
Juridische identificatie en verwijzing		
BWB (Wet- en regelgeving)	Ja	De Stelselcatalogus gebruikt het Basis Wetten Bestand (BWB) via Juriconnect als open standaard voor de link naar de wetgeving als bron. De Juriconnect Id's worden gebruikt om per gegeven of begrip in de Stelselcatalogus de link te leggen naar de wet en het artikel in het Basis Wetten Bestand.

Ten opzichte van 2019 voldoet de voorziening Stelselcatalogus aan de standaarden HTTPS/HSTS, wat maakt dat de status van gepland naar ja gaat. De status van IPv4 en IPv6 gaat van nee naar gepland. Nieuw op de lijst zijn REST-API Design Rules en RPKI. De voorziening voldoet aan beide standaarden. Dit jaar is Digitoegankelijk getoetst, voor de voorziening zijn de eerste maatregelen genomen en is de score C.

Samengevat moeten voor de voorziening stelselcatalogus nog de volgende standaarden (volledig) worden geïmplementeerd: IPv4 en IP6 en Digitoegankelijk.

5. Dienstverlening en verbinden

5.1. Digipoort

Beheerorganisatie: Logius

Werking en inhoud van Digipoort

DigiPoort is een ICT-centrale waar berichtenverkeer voor de overheid afgehandeld wordt. Overheden kunnen DigiPoort inzetten om bedrijfs- en ketenprocessen te automatiseren.

Omdat Digipoort slechts machine-naar-machine koppelingen levert en niet toegankelijk is vanaf het openbare internet, is gekozen voor de website aansluiten.procesinfrastructuur.nl, wat de voornaamste publieke website is van Digipoort, voor onderstaande verantwoording.

Standaard	Status	Toelichting beheerder
Internet en beveiliging		
DMARC (Anti-phishing)	Ja	Digipoort is nu DMARC compliant.
DNSSEC (Beveiligde domeinnamen)	Ja	In 2020 in de DNS-registratie verhuisd naar MinAZ. Hierdoor is een aantal zaken als DNSSEC standaard ingeregeld. Net als DMARC en SPF.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening voldoet aan HTTPS. Formeel wordt niet aan HSTS voldaan, maar de standaard HTTP (poort 80) is bij de voorziening helemaal niet ontsloten, zodat feitelijk alleen via HTTPS een verbinding gemaakt kan worden. In de geest voldoet de voorziening dus impliciet wel aan HSTS.
IPv4 en IPV6 (Internetnummers)	Nee	Digipoort gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt de open standaard IPv4 maar IPv6 voor internet gebruik niet. IPv6 kan niet worden aangeboden, omdat de infrastructuur van Logius dit nog niet voldoende ondersteunt. Implementatie van IPv6 stond gepland voor Q1 2019. De planning voor aanpassing ligt bij Generieke Infra van Logius.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Digipoort voldoet aan de BIO. Leveranciers voldoen aan ISO 27001 of een vergelijkbare standaard.
RPKI (Beveiligen van de routing infrastructuur)	Ja	Dit is ingeregeld en compliant.
SPF (Preventie van mailspoofing/phishing)	Ja	Digipoort is nu SPF compliant.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Digipoort ondersteunt TLS v1.2, maar niet meer de verouderde versies.

Stelselstandaarden		
Digikoppeling (Veilige berichten-uitwisselingen)	Ja	Digipoort voldoet aan deze standaard. Zie de koppelvlakspecificaties op Koppelvlakken Digipoort | Logius.
E-facturatie en administratie		
SETU (Informatie flexibele arbeidskrachten)	Ja	DigiPoort ondersteunt de uitwisseling van SETU-hr-XML berichten.
XBRL en Dimensions (Bedrijfsrapportages)	Ja	De standaard wordt ondersteund door Digipoort.

Ten opzichte van 2019 zijn DMARC, DNSSEC en SPF van gepland naar ja gegaan. Nieuw op de lijst is de RPKI standaard, die voldoet. DKIM is niet meer relevant. De in 2019 geconfigureerde mailserver is standaard onderdeel van de oplevering van een omgeving. Inmiddels is het duidelijk dat de voorziening deze niet nodig heeft en daarom is deze functionaliteit compleet verwijderd uit de DNS.

Samenvattend moeten voor de voorziening Digipoort de volgende standaarden nog (volledig) worden geïmplementeerd: IPv4 en IPv6.

5.2. Diginetwerk

Beheerorganisatie: Logius

Werking en inhoud van Diginetwerk

Diginetwerk is een afsprakenstelsel en bestaat uit een beschreven samenwerking, normenkaders, handhavingsmechanismen, toetredingseisen en een set van standaarden. Diginetwerk is opgebouwd uit een aantal aan elkaar gekoppelde besloten overheidsnetwerken, waarover overheden gegevens

veiliger (vertrouwelijkheid en beschikbaarheid) met andere overheden kunnen uitwisselen dan via het internet. Een belangrijk onderdeel van Diginetwerk is de Koppelnet Publieke Sector (KPS) voorziening, welke de fysieke koppeling tussen de diverse deelnemers verzorgt.

De binnen Diginetwerk toegepaste set standaarden heeft betrekking op het transport van data (netwerk standaarden), standaarden op applicatie- of gegevensniveau maken geen onderdeel uit van het afsprakenstelsel. Logius is als regievoerder/beheerder van het afsprakenstelsel in gesprek met het Forum Standaardisatie en deelnemers om de relevante standaarden van de PTOLU-lijst binnen Diginetwerk toe te passen. Standaarden worden toegepast als die een toegevoegde waarde hebben binnen het besloten netwerkstelsel en door de deelnemers geïmplementeerd kunnen worden zonder afbreuk te doen aan het besloten karakter.

Bij deze toetsing is voorlopig niet gekeken naar de standaarden in de hoger gelegen lagen van het OSI-model.

Standaard	Status	Toelichting beheerder
Internet en beveiliging		
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC valt voor het besloten netwerk buiten het afsprakenstelsel. Een aantal deelnemers maakt echter gebruik van de diginetwerk domeinnamen om ook op het openbare internet hun dienst ter beschikking te stellen. Hiervoor is besloten wel gebruik te maken van DNSSEC. DNSSEC is op alle externe gemeenschappelijke domein namen toegepast. Interne besloten domeinen zijn uitgezonderd. Dit in lijn met het advies van DNS Expertgroep.
IPv4 en IPv6 (Internetnummers)	Gepland	IPv4 is geïmplementeerd door de deelnemers aan Diginetwerk. De implementatie van IPv6 stond gepland voor Q4 2018. Vanwege aanbesteding KPS (koppelpunt van Diginetwerk) was ondersteuning van IPv6 onderdeel van de migratie naar de nieuwe KPS leverancier. Implementatie IPv6 is gestart en loopt tot medio 2022. Inmiddels is IPv6 geïmplementeerd op het KPS en KPS diensten. Alle Koppelnetwerken die op KPS zijn aangesloten zijn IPv6 ondersteuning aan het voorbereiden.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Deze standaard is onderdeel van het algemene beveiligingsbeleid van Logius. Logius voldoet aan deze standaard en Diginetwerk is ook gebaseerd op deze standaard.

Ten opzichte van 2019 is DNSSEC geïmplementeerd, waarbij de status van gepland naar ja gaat. De implementatie van IPv6 loopt en blijft op gepland staan.

Samenvattend moeten voor de voorziening Diginetwerk de volgende standaarden nog (volledig) worden geïmplementeerd: IPv4 en IPv6.

5.3. DWR

Beheerorganisatie: Ministerie BZK/ Shared Service Center-ICT

Werking en inhoud van DWR

De Digitale Werkomgeving Rijksdienst (DWR) is de ICT-werkomgeving voor rijksambtenaren. Deze werkomgeving is een onderdeel van de dienstverlening van SSC-ICT. SSC-ICT ontwikkelt en beheert DWR voor een groot aantal ministeries. De digitale werkomgeving bestaat uit verschillende onderdelen voor infrastructuur en connectiviteit. De drie belangrijkste zijn de uniforme digitale werkomgeving voor ambtenaren (DWR Next client), één website voor overheidsinformatie en diensten (rijksoverheid.nl), en gebruik van web 2.0 toepassingen om beter en sneller samen te werken. Komende jaren wordt de technologie verder geïntegreerd en zullen in afstemming met de afnemers van de dienstverlening de standaarden verder worden ingevuld; tussen 2019 – 2021 zijn onder meer de afnemers uit het domein van het Ministerie van Justitie en Veiligheid voorzien van de DWR Next Client.

Standaard	Status	Toelichting 2021
Internet en beveiliging		
DKIM (Preventie van mailspoofing/phishing)	Ja	De implementatie van DKIM is voor SSC-ICT zelf geheel afgerond.
DMARC (Anti-phishing)	Deels/Gepland	De technische implementatie van DMARC is afgerond. Het doorvoeren van de DMARC *reject policy* moet voor 35 hoofd/sub-domeinen nog worden uitgevoerd, maar dit kan nog niet vanwege (een aantal) externe applicaties die mailen of klanten die gebruik maken van externe mailingdiensten. De inrichting van deze standaard is projectmatig opgepakt en thans in de afrondende fase. Verwachte afronding: eind 2021 - SSC-ICT is voor de realisatie van de dienst ook afhankelijk van de medewerking van de betreffende klanten.
DNSSEC (Beveiligde domeinnamen)	Deels/Gepland	41 domeinen hebben nog geen DNSSEC. Een gedeelte wordt gehost bij Microsoft (Azure) die nog geen DNSSEC heeft. Eind 2021 voldoen alle webdomeinen aan de standaard of wijken we gemotiveerd af.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels/Gepland	HTTPS wordt toegepast op 576 van de 580 webdomeinen. HSTS wordt toegepast op 451 van de 580 webdomeinen. Eind 2021 voldoen alle webdomeinen aan de standaard of wijken we gemotiveerd af. Eerder stond dit gepland voor eind 2019.
IPv4 en IPV6 (Internetnummers)	Gepland	IPv4 is in gebruik. De gebruikte technische componenten van DWR ondersteunen wel IPv6. IPv6 is een onderdeel van de infrastructuur en IPv6 reeksen worden uitgedeeld door Logius. Implementatie van IPv6 is voor eind 2021 gepland i.p.v. eind 2019 voor de internet facing web-name en mailservices conform Pas-toe-of-leg-uit
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	SSC-ICT werkt via deze standaard en onderdelen van de dienstverlening worden hier ook regelmatig op geaudit. Ook in 2021 hebben weer verschillende audits plaatsgevonden.
NL GOV Assurance profile for OAuth 2.0 (Beveiligingstandaard voor het autoriseren van toegang tot REST API's)	Nee	Deze standaard is relevant voor de DWR-voorziening. Mogelijkheden t.a.v. implementatie worden verkend. Er is nog geen datum voor de implementatie vastgelegd.

RPKI (Beveiligen van de routing infrastructuur)	Gepland	Implementatie is gestart. Verwachte afronding: eind 2021.
SAML (Inloggegevens)	Ja	Single Sign-on (SSO) op basis van SAML 2.0 wordt aangeboden als dienst in de Servicecatalogus van SSC-ICT. Het SSO-koppelvlak is een generieke dienst. Het project DOorontwikkeling Single Sign-On (DOrSSOn) voorziet internet facing aanvulling van de huidige oplossing met open source componenten gebaseerd op de standaarden SAML 2.0 en OAuth 2.0 in opdracht van CIO Rijk.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF wordt op alle domeinen toegepast.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	STARTTLS en DANE zijn geïmplementeerd.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De op de werkplek aangeboden browsers ondersteunen TLS. De mailvoorziening werkt met STARTTLS. De webservers van de klanten zijn geen onderdeel van DWR, maar klantspecifieke voorzieningen.
WPA2 Enterprise (Toegang tot een WiFi-netwerk met account)	Ja	Op de wifivoorziening wordt deze standaard toegepast. Wifi wordt door SSC-ICT als voorziening geleverd in de kantoorpanden waar SSC-ICT IT-dienstverlener voor het pand is (IDV-P). WPA2-Enterprise is in 2021 ook aangezet op de gastnetwerken.
Document en (web/app)content		
ODF 1.2 (Documentbewerking en)	Ja	De DWR Next client wordt geleverd met zowel Libreoffice als Office 2016. Beide softwaresuites ondersteunen het lezen en schrijven van ODF-bestanden.
PDF 1.7 / PDF A/1 en PDF A/2 (Documentpublicatie/ archivering)	Ja	De DWR Next client kan alle types PDF lezen. Schrijven van PDF kan op meerdere manieren. Alle types worden ondersteund, al is daarvoor soms wel het installeren van Adobe Acrobat Professional benodigd. PDF A/2 is mogelijk voor klanten die Adobe Acrobat Pro afnemen. De regulier verstrekte Adobe Acrobat Standard ondersteunt PDF A/2 niet, maar wel PDF 1.7 en PDF A/1. De scanfunctionaliteit in het reguliere multifunctional printplatform voor de werkomgeving ondersteunt PDF 1.7 en PDF A/1.
Stelselstandaarden		
Digikoppeling 2.0	Ja	Binnen JenV vindt elektronisch berichtenverkeer interdepartementaal plaats via de Justitie Berichten Service (JUBES). JUBES is vanuit JenV het

(Veilige berichtenuitwisselingen)	koppelvlak voor de Digikoppelingdienst van Logius. De open standaarden eBMS en WUS zijn de daarbij gebruikte protocollen om de berichten veilig te versturen. Binnen BZ wordt deze standaard gebruikt voor de Mule koppeling. Verder nemen alle departementen uit het verzorgingsgebied van SSC-ICT deel aan eFacturatie. Op deze standaard wordt waar van toepassing aangesloten bij nieuwe koppelingen.

Ten opzichte van 2019 gaat de status van DMARC van 'nee' naar 'deels/gepland'. De voorziening voldoet niet meer DNSSEC, de status gaat van ja naar 'deels/gepland'. De planning van implementatie van HTTPS/HSTS en IPv4 en IPv6 is niet gehaald. Nieuw op de lijst staan NL GOV Assurance profile for OAuth 2.0 en RPKI. De voorziening voldoet niet aan NL GOV Assurance profile for OAuth 2.0 en heeft implementatie van RPKI gepland.

Samenvattend dienen voor de voorziening DWR de volgende standaarden nog (volledig) te worden geïmplementeerd: DMARC, DNSSEC, HTTPS/HSTS, IPv4 en IPv6 , NL GOV Assurance profile for OAuth 2.0 en RPKI.

6. Bijlage A: Geïnterviewde personen

Naam voorziening	Contactpersoon
BRO	Marjan Bevelander
BAG	Koen Huisstede
WOZ	Koen Huisstede
BGT	Koen Huisstede
BRK	Koen Huisstede
BRT	Koen Huisstede
BRI	Doekele Haagsma
BRV	Gert Stel
BSN en GBA-V	Bob te Riele
Digilevering	Albert Kafsek
Digimelding	Ed van der Ark
Diginetwerk	Sharmie Mahabier
DigiPoort	Jeroen Lambregts
Doc-Direkt	Olaf Holtrop
DWR	Rein Hennen
NHR	Rob Spoelstra
Rijksportaal	Jos van der Heiden
Stelselcatalogus	Kees-Jan Westmaas

7. Bijlage B: Lijst onderzochte verplichte open standaarden

Standaard
Ades Baseline Profiles
Aquo-standaard
BWB
COINS
Digikoppeling
Digitoegankelijk (EN 301 549 met WCAG 2.1)
DKIM
DMARC
DNSSEC
E-Portfolio NL
ECLI
EML_NL
Geo-Standaarden
GWSW
HTTPS en HSTS
IFC
IPv6 en IPv4
JCDR
NEN-ISO/IEC 27001
NEN-ISO/IEC 27002
NL GOV Assurance profile for OAuth 2.0
NL LOM
NLCIUS
NLCS
ODF
OpenAPI Specification
OWMS
PDF (NEN-ISO)
REST-API Design Rules
RPKI
SAML
SETU
SIKB0101
SIKB0102
SKOS
SPF
STARTTLS en DANE
STIX en TAXII
StUF
TLS
VISI
WDO Datamodel
WPA2 Enterprise
XBRL

B5. Inventarisatie gebruiksgegevens 2021 door BFS

Het uiteindelijke doel van het open standaardenbeleid is een brede adoptie van de open standaarden van de lijst voor 'pas toe of leg uit' – daar waar deze van toepassing zijn. Het 'pas toe of leg uit'-regime is gericht op aanbestedingen, voor een completer beeld van de adoptie is het feitelijk gebruik dus interessant.

Net als vorig jaar is dit deelonderzoek dit jaar uitgevoerd door de accountmanagers van het Bureau Forum Standaardisatie (BFS). Helaas is het niet altijd even eenvoudig om (voor alle open standaarden) vast te stellen in welke mate die feitelijk door overheden gebruikt worden. De accountmanagers van BFS hebben hiervoor contact opgenomen met beheerders van standaarden en sommige specifiek voor de standaard relevante voorzieningen. Voor een aantal standaarden uit het domein Internet en beveiliging zijn de gebruiksgegevens afkomstig uit het halfjaarlijkse onderzoek naar internet-veiligheids-standaarden (zie *Meting informatieveiligheidstandaarden overheid, maart 2021,* opgenomen in Bijlage B6).

Over het gebruik van de volgende vijf standaarden is dit jaar geen (actuele) informatie beschikbaar: NL GOV, Ades Baseline Profiles, DigiToegankelijk, OpenAPI Specification en REST-API Design Rules. De volgende drie standaarden stonden vorig jaar pas recent op de 'pas toe of leg uit' lijst: GWSW, NL GOV en REST-API Design Rules. Deze standaarden worden dit jaar voor het eerst meegenomen in het onderdeel 'gebruiksgegevens'.

B5.1. Domein Internet en beveiliging

Voor een aantal standaarden binnen dit domein is zoals gezegd gebruik gemaakt van de opbrengst van de meting IV-standaarden door Forum Standaardisatie. Het betreft de volgende standaarden: DKIM, DMARC, SPF, DNSSEC, HTTPS & HSTS, TLS, IPv6 en IPv4 en STARTTLS & DANE. In de meest recente meting (maart 2021) zijn 558 domeinnamen getoetst die ook in eerdere metingen centraal stonden (vorige monitor: 548). In deze maart-meting is daarnaast wederom een vergelijking gemaakt met de meetresultaten van een bredere selectie van circa 2.200 overheidsdomeinnamen (vorige monitor: 1.800). Uit deze vergelijking blijkt –als algemeen beeld- dat de scores van de bredere meting lager zijn dan de scores op het gebruik van de standaarden bij de groep van 558 primaire (veelgebruikte) internetdomeinen waarop in de IV-meting de focus ligt. In die zin is er nog de nodige winst te boeken. In de monitor 2020 werd ten aanzien van dit punt een soortgelijke conclusie getrokken.

DKIM, DMARC en SPF

Waarom belangrijk ?

De hier genoemde drie standaarden voorkomen in onderlinge samenhang e-mailspoofing waardoor phishing uit naam van overheidsorganisaties wordt bemoeilijkt:

- *DKIM: dit* is een techniek waarmee e-mailberichten kunnen worden gewaarmerkt. Een domeinnaamhouder kan in het DNS-record van de domeinnaam aangeven met welke sleutel e-mail namens de betreffende domeinnaam ondertekend moet worden (op de

'pas toe of leg uit' lijst sinds juni 2012 - we vermelden telkens de oorspronkelijke plaatsing op de 'pas toe of leg uit'-lijst);

- *DMARC:* maakt het mogelijk om beleid in te stellen over de manier waarop een e-mailprovider om moet gaan met e-mail waarvan niet kan worden vastgesteld dat deze afkomstig is van het vermelde afzenderdomein. Hierdoor kunnen organisaties voorkomen dat anderen e-mails versturen namens het e-maildomein van de organisatie (op de 'pas toe of leg uit'-lijst sinds mei 2015);
- *SPF: dit* is een techniek waarmee een domeinhouder de IP-adressen van verzendende mailservers kan publiceren in de DNS. Een ontvangende mailserver kan deze IP-adressen gebruiken om te controleren of een e-mail daadwerkelijk afkomstig is van een verzendende mailserver van de betreffende domeinhouder (op de 'pas toe of leg uit'-lijst sinds mei 2015).

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaarden kijken we naar de ondersteuning van DMARC, DKIM en SPF op 558 domeinen van de overheid. Zie hiervoor de IV-meting van maart 2021 (Bijlage B6).

Voor DMARC en SPF is met ingang van medio 2018 ook gemeten of de ingestelde policy voldoende strikt is. Wat niet is gemeten is of deze echtheidswaarmerken ook daadwerkelijk worden gebruikt op alle uitgaande mailstromen. Wat eveneens niet is gemeten is of inkomende overheidsmailservers controleren op DMARC, DKIM en SPF.

	medio 2018 (september)	begin 2019 (maart)	medio 2019 (september)	begin 2020 (maart)	medio 2020 (september)	**begin 2021** (maart)
DMARC	73 %	82 %	87 %	88 %	92 %	95 %
DMARC policy	28 %	37 %	49 %	58 %	66 %	74 %
DKIM	84 %	89 %	90%	92 %	96%	96 %
SPF	93 %	95 %	96 %	96 %	97 %	99 %
SPF Policy	85 %	88 %	89 %	91 %	91 %	94 %

Vergeleken met de vorige monitor is vrijwel over de gehele breedte sprake van een **toename van het gebruik**. Enige uitzondering daarop is DKIM met een stabilisatie op 96%. Kanttekening bij dat laatste: hoge percentages voor wat betreft het gebruik bieden nog maar weinig ruimte voor verdere groei.

Let wel: in de monitor 2020 is voor de bijlage 'gebruiksgegevens' gebruik gemaakt van de IV-meting uit september 2020. Dat is voor de betreffende standaarden dus de vergelijkingsbasis, tenzij anders vermeld. Op DMARC-policy na liggen de percentages inmiddels boven de 90%. Ook al laat DMARC policy in de achterliggende periode de grootste procentuele stijging zien, toch biedt een score van 74% begin 2021 nog steeds het grootste groeipotentieel.

Uit de IV-meting blijkt tot slot dat bij elke overheidslaag sprake is van een stijging van de gemiddelde toepassingsgraad van de mailstandaarden.

Als kanttekening bij dit gunstige beeld moet worden opgemerkt dat een vergelijking met de bredere selectie van circa 2.200 domeinnamen uitwijst dat het gebruik van deze standaarden daar substantieel lager ligt (11 tot 24 procentpunten lager). Dat impliceert dat de focus op de (primaire groep van) 558 domeinen een wat vertekend beeld geeft.

DNSSEC

Waarom belangrijk ?

Een domeinnaamhouder kan met DNSSEC een digitale handtekening toevoegen aan DNS-informatie. Met DNSSEC kan de ontvanger vervolgens de echtheid van de domeinnaam-informatie (waaronder IP-adressen) controleren. Dit voorkomt bijvoorbeeld dat een aanvaller het IP-adres ongemerkt manipuleert (DNS-spoofing) en daarmee verstuurde e-mails omleidt naar een eigen mailserver of gebruikers misleidt naar een frauduleuze website (op de 'pas toe of leg uit'-lijst sinds juni 2012).

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaard kijken we wederom naar het gebruik van DNSSEC-handtekeningen op 558 kern-domeinen van de overheid. Zie hiervoor de IV-meting van maart 2021(Bijlage B6).

DNSSEC-validatie (controle op handtekeningen) wordt niet gemeten in de IV-meting.

DNSSEC	**medio 2018** (september)	**begin 2019** (maart)	**medio 2019** (september)	**begin 2020** (maart)	**medio 2020** (september)	**begin 2021** (maart)
op hoofd-domein	90 %	93 %	94 %	95 %	94 %	98 %
op mailserver-domein	69 %	71 %	67 %	67 %	66 %	64 %

Vergeleken met de meting september 2020 is het gebruik **min of meer stabiel**. Voor web is sprake van een marginale stijging (2%) en voor email-verkeer van een daling van 2%. Inzoomend op de verschillende overheidslagen komen een paar opmerkelijke verschillen aan het licht (vergeleken met de monitor van vorig jaar):

- de onderlinge verschillen bij web zijn klein, met scores van 93% tot 100% (bij gemeenten en waterschappen). Met name bij de waterschappen is in vergelijking met de vorige monitor sprake van een substantiële procentuele stijging;
- er is wel sprake van grote verschillen tussen de overheidslagen voor wat betreft het gebruik van DNSSEC bij e-mail. Zo scoort het Rijk daar 98% (stabiel hoog) en de uitvoeringsorganisaties 80% (een lichte stijging ten opzichte van de vorige monitor). De andere overheidslagen laten elk een daling zien ten opzichte van de september-meting 2020. Dit betreft met name provincies en waterschappen en daar komt bij dat de percentages daar vorig jaar al relatief laag waren. Bij de provincies is sprake van een terugloop van 44% naar 32%, bij de waterschappen van 48% naar 42%.

In de IV-monitor wordt naar aanleiding van het algemene beeld van een stabilisatie bij wijze van duiding opgemerkt dat het toepassen van de standaarden vraagt om extra aandacht.

Dit geldt temeer als de vergelijking wordt gemaakt met het gebruik van deze standaard onder de bredere groep van circa 2.200 domeinen van de overheid, met name voor wat betreft het web. Voor die grotere groep liggen de procentuele scores van het gebruik 13 procentpunten lager (85% in plaats van 98%). Opvallend ander beeld zien we bij het gebruik van DNSSEC bij e-mail. Daar scoort de bredere groep van 2.200 juist 5 procentpunten beter (69% in plaats van 64%). Dat neemt niet weg dat voor beide geldt dat er voldoende groeipotentie aanwezig is.

HTTPS & HSTS en TLS

Waarom belangrijk ?

HTTPS & HSTS en ook TLS zorgen samen voor beveiligde verbindingen met websites, met als doel de veilige uitwisseling van gegevens tussen een webserver en client (vaak een webbrowser). Dit maakt het voor cybercriminelen moeilijker om verkeer om te leiden naar valse websites en om de inhoud van webverkeer te onderscheppen.

HTTPS zorgt voor het gebruik van HTTP over een met TLS beveiligde verbinding. Dit betekent dat het webverkeer door middel een certificaat wordt versleuteld.

HSTS zorgt ervoor dat een webbrowser, na het eerste contact over HTTPS, bij vervolgbezoek de website altijd direct over HTTPS opvraagt.

Deze standaarden staan op de 'pas toe of leg uit'-lijst sinds mei 2017.

TLS zorgt door middel van de uitwisseling van certificaten voor de versleuteling van gegevens tijdens het transport tussen internetsystemen. TLS staat op de 'pas toe of leg uit'-lijst sinds september 2014.

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaarden kijken we naar het gebruik op 558 kern-domeinen van de overheid. Zie ook de IV-meting van maart 2021 (Bijlage B6).

Er wordt niet gekeken naar de support van HTTPS door browsers op overheidswerkplekken.

	medio 2018 (september)	**begin 2019** (maart)	**medio 2019** (september)	**begin 2020** (maart)	**medio 2020** (september)	**begin 2021** (maart)
HTTPS	89 %	90 %	94 %	95 %	98 %	98 %
HSTS	79 %	79 %	85 %	88 %	92 %	83 %
TLS	96 %	96 %	97 %	98 %	100 %	100 %
TLS cf. NCSC	87 %	89 %	92%	93 %	78 %	85 %

Vergeleken met de cijfers uit de monitor van 2020 is het gebruik van **HTTPS & HSTS** (voor het eerst sinds tijden) niet toegenomen en zien we bij HSTS zelfs een afname, van 92% naar 83%. Deze terugval van 9% in de adoptiegraad van HSTS (voor het afdwingen van een beveiligde websiteverbinding) komt door een aanpassing in de minimum vereiste cache-geldigheidsduur. Deze is in de Internet.nl test verhoogd van 6 maanden naar 1 jaar en daarmee is de lat hoger komen te liggen. Dit is in overeenstemming met de gangbare good

practices. Bij HTTPS zijn de grenzen van de groei in zicht. Dit laatste geldt nog meer voor TLS met nu net als in de vorige monitor een 100%-score.

Het gebruik van **TLS conform NCSC** liet in de vorige monitor een afwijkend beeld zien, met een terugval. Dit was het gevolg van het feit dat voor het eerst is getoetst conform de tweede versie van de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) uit april 2019. Daarmee is de lat toen hoger komen te liggen bij de toetsing met een lager percentage gebruik als resultaat. Tussen nu en de september-meting van vorig jaar is de stijgende lijn weer opgepakt.

Ook voor deze standaarden is weer een vergelijking gemaakt met de meting onder de breder samengestelde groep van circa 2.200 domeinnamen van de overheid. TLS scoort ook voor die bredere groep zeer hoog (99%). Ook het gebruik van HTTPS is hoog (90% tegen 98% voor de kerngroep van 558 domeinen). Voor HSTS is de score wel duidelijk lager: 63% gebruik bij de breed samengestelde groep, 83% voor de kerngroep. TLS conform NCSC laat voor de bredere groep ook een lagere score zien dan de score uit bovenstaande tabel met de gegevens voor de groep van 558 domeinen: 70% tegen 85%.

Het algemene beeld in deze paragraaf luidt: HTTPS en TLS stabiel hoog, HSTS omlaag en TLS cf. NSCS omhoog. Van de vijf overheidslagen laten er drie ook zo'n beeld zien: Rijk, gemeenten en waterschappen. De uitzonderingen op dit algemene beeld zijn terug te vinden bij uitvoeringsorganisaties en provincies:

- bij uitvoeringsorganisaties zien we een stijging bij HSTS;
- bij provincies ook en daar tevens een daling van de score op TLS cf. NCSC.

IPv6 & IPv4

Waarom belangrijk ?

De standaard bepaalt dat ieder ICT-systeem binnen het netwerk een uniek nummer (IP-adres) heeft. Hierdoor kunnen ICT-systemen elkaar herkennen en onderling data uitwisselen. IPv6 heeft een veel grotere hoeveelheid beschikbare IP-adressen ten opzichte van de voorganger IPv4. Dit maakt verdere groei en innovatie van het internet mogelijk. IPv6 is niet backwards compatible. Dit wil zeggen dat een IPv4-systeem niet een IPv6-systeem kan bereiken, of andersom. Om die reden moet een organisatie bij de aanschaf van een ICT-product/-dienst beide versies uitvragen.

De standaard staat op de 'pas toe of leg uit' lijst sinds november 2010.

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaarden kijken we in eerste instantie naar de bereikbaarheid van overheids-websites via de internetstandaard IPv6 voor 558 kern-domeinen van de overheid.

Vergeleken met de uitkomsten in de monitor 2020 is het gebruik **toegenomen**, van 69% naar 79%. Dat geldt overigens niet voor elk van de overheidslagen in dezelfde mate. Met name bij gemeenten zet de stijging flink door.

	medio 2018 (september)	begin 2019 (maart)	medio 2019 (september)	begin 2020 (maart)	medio 2020 (september)	begin 2021 (maart)
Rijk	45 % *	58 %	60 %	64 %	62 %	66 %
Uitvoeringsorg.	45 % *	45 %	46 %	53 %	52 %	60 %
Gemeenten	25 %	49 %	58 %	67 %	75 %	86 %
Provincies	17 %	33 %	56 %	61 %	67 %	68 %
Waterschappen	13 %	27 %	44 %	50 %	59 %	65 %
Totaal	29 %	48 %	56 %	64 %	69 %	79 %

** In de meting september 2018 waren de scores voor Rijk en uitvoeringsorganisaties niet uitgesplitst.*

Aanvullend op de bereikbaarheid van overheidswebsites is in de IV-meting ook gekeken naar de bereikbaarheid van overheidsmail. De gebruikscijfers daarvan liggen een stuk lager maar zijn recent wel flink gestegen. Na een stabilisatie van ruim een jaar op 17% lag de score in september vorig jaar op 20% en blijkt uit de meest recente meting (maart 2021) dat de bereikbaarheid van overheidsmail (algemeen) nu ligt op 40%. Ondanks achterblijvende percentages is dus wel degelijk sprake van een **flinke toename**.

Relevante ontwikkeling

Op 8 april 2020 is door het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) afgesproken dat alle overheidswebsites en e-maildomeinen van de overheid uiterlijk eind 2021 behalve via IPv4 ook volledig bereikbaar moeten zijn via IPv6. Anders loopt de overheid het gevaar dat haar websites en e-maildomeinen voor bepaalde (groeiende) groepen gebruikers (met devices met IPv6 only) onbereikbaar is.

Dit streven is nog steeds leidend. Tot eind 2021 is het IPv6 Team Overheid NL beschikbaar voor alle overheidsorganisaties die ondersteuning willen bij de overgang.

NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002

Waarom belangrijk ?

De NEN-ISO/IEC 27001-standaard bevat eisen waar het managementsysteem voor informatiebeveiliging aan dient te voldoen. De standaard werkt uniformerend ten aanzien van het informatiebeveiligingsbeleid. Deze standaard specificeert eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's van een organisatie.

De NEN-ISO/IEC 27002-standaard is een best practice van beveiligingsmaatregelen ('controls') om informatiebeveiligingsrisico's aan te pakken met betrekking tot vertrouwelijkheid, integriteit en beschikbaarheid van de informatievoorziening. De standaard kan gezien worden als een nadere specificatie van NEN-ISO/IEC 27001. ISO 27002 geeft richtlijnen en principes voor het initiëren, implementeren, onderhouden en verbeteren van informatiebeveiliging binnen een organisatie.

Beide standaarden staan op de 'pas toe of leg uit' lijst sinds 18 mei 2015.

De Nederlandse overheid heeft haar eigen kaders voor informatiebeveiliging die zijn afgeleid van de 27001- en 27002-normen. Tot 2019 hadden alle bestuurslagen een eigen baseline, de

BIR (Rijk), BIG (gemeenten), IBI (provincies) en BIWA (waterschappen). Deze baselines zijn (met uitzondering van de BIR2017) voor een groot deel nog gebaseerd op de ISO-normering uit 2005 en lopen achter op de actuele ISO-normen. De BIO is gebaseerd op de actuele, internationale standaard voor informatiebeveiliging (NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002) en heeft risicomanagement als uitgangspunt. Alle overheidslagen hebben zichzelf verplicht de BIO toe te passen. Forum Standaardisatie heeft medio 2018 reeds geadviseerd om actief op adoptie van de BIO in te zetten, en de voortgang te monitoren. In reactie daarop heeft de werkgroep BIO aangegeven dat iedere overheidslaag zelf zal monitoren wat de voortgang is van de implementatie van de BIO. Vanaf 1 januari 2019 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines voor Rijk, Gemeenten, Waterschappen en Provincies.

Feitelijk gebruik

Voor de Monitor 2021 zijn door de verschillende overheidslagen geen kwantitatieve gegevens over het gebruik van hun beveiligingsbaselines aangeleverd. Verantwoording over de beveiliging vindt in beginsel plaats aan de eigen controlerende organen.

Rijksoverheid

CIO Rijk meldt dat de opvolger van de BIR2017, de BIO 1.04, op 11-2-2020 is gepubliceerd in de staatcourant en geldt voor alle overheidslagen. In 2020 hebben de departementen in de jaarlijkse CISO-gesprekken gemeld dat BIO 1.04 is of wordt geïmplementeerd. Een aantal departementen heeft ervoor gekozen om de BIO 1.04 in eigen departement specifieke baselines op te nemen. De departementen die hebben aangegeven dat de BIO 1.04 nog wordt geïmplementeerd verwachten dat deze implementaties uiterlijk eind 2022 worden afgerond.

Provincies

Alle provincies zijn bezig met het implementeren van de BIO en doen dat in combinatie met de ambitie om binnenkort ISO 27001 certificeerbaar te zijn.

In 2020 was één provincie ISO 27001 en BIO gecertificeerd. Dit is gerealiseerd door de BIO als extra normenkader aan de 27001-certificering toe te voegen. Twee andere provincies waren in 2020 ook bezig met een ISO 27001-certificeertraject en nemen daar de BIO ook expliciet in mee.

De andere provincies waren bezig met trajecten om ISO 27001 certificeerbaar te zijn en nemen daar de BIO ook in mee. Daarnaast zullen alle provincies op basis van risicoanalyses het juiste BBN niveau bepalen en daar de juiste maatregelen voor implementeren.

Medio 2021 krijgen alle provincies een audit door dezelfde auditor. De resultaten verwachten de provincies eind 2021.

Waterschappen

In de monitor van 2019 is het volgende tijdpad geschetst: Uiterlijk 1 januari 2019 heeft het waterschap de Baseline Informatiebeveiliging Waterschappen (BIWA) of de opvolger hiervan geïmplementeerd en uiterlijk 1 januari 2020 worden aanvullende maatregelen getroffen op basis van risicoanalyses. De BIO is bestuurlijk vastgesteld in de Ledenvergadering van 12

oktober 2018 van de Unie van Waterschappen. Concreet hebben de waterschappen ingestemd met:

- het besluit dat per 1 januari 2019 de BIO het nieuwe normenkader is voor alle waterschappen en hun samenwerkingsverbanden;
- het besluit om 2019 als overgangsjaar te hanteren om over te stappen van de Baseline Informatiebeveiliging Waterschappen (BIWA) naar de BIO. De BIO is dan vanaf 1 januari 2020 van toepassing.

Over de voortgang van dit traject is dit jaar geen actuele informatie beschikbaar. Ieder waterschap implementeert de BIO zelfstandig en dat wordt niet centraal gemonitord.

Gemeenten

Alle gemeenten hanteren de BIO als normenkader voor informatiebeveiliging. Implementatie is een doorlopend proces van plannen, uitvoeren, controleren en bijstellen. Er is geen punt waarop "de BIO is geïmplementeerd". De VNG houdt geen implementatievoortgang bij, wel ondersteunt VNG bij de implementatie. De VNG hanteert een risicogestuurde aanpak in lijn met de Agenda Digitale Veiligheid van gemeenten.

Het geheel van overheidslagen overziend wordt de vraag in welke mate een en ander inmiddels conform BIO is ingericht **niet of nauwelijks beantwoord**. De passages die betrekking hebben op de verschillende overheidslagen beperken zich voornamelijk tot een procedurele insteek. De monitoring waarover eerder in deze passage is gesproken (zie in de passage onder 'algemeen') heeft niet het gewenste beschikbare inzicht geboden. Een vergelijking met de stand van zaken vorig jaar is dan ook niet te maken.

Relevante ontwikkeling

ISO 27002 krijgt eind 2021 een update. Het is de verwachting dat er bij deze herziening aanzienlijke wijzigingen doorgevoerd worden, zowel in de structuur van het document als in de inhoud van de security controls. De BIO is op ISO 27001 en ISO27002 gebaseerd. De werkgroep BIO laat een impact analyse plaatsvinden wat de wijzingen voor impact hebben op de BIO.

NL GOV Assurance

Over deze standaard is helaas geen informatie beschikbaar.

RPKI

Waarom belangrijk ?

Resource Public Key Infrastructure (RPKI) is een standaard met als doel om zogenaamde route hijacks te voorkomen. Bij een route hijack wordt internetverkeer omgeleid naar de systemen van een niet-geautoriseerd netwerk. Een hijack kan het gevolg zijn van een simpele typefout van een netwerkbeheerder die daarmee onbedoeld internetverkeer omleidt, of van een doelgerichte aanval op de infrastructuur van het internet om bijvoorbeeld websites onbereikbaar te maken of om gegevens van internetgebruikers afhandig te maken. Deze standaard staat op de 'pas toe of leg uit'-lijst, sinds november 2019.

Feitelijk gebruik

In de vorige monitor is aan zeven deelnemers aan verdiepingssessies overheidsnetwerken (namelijk SSC-ICT, VNG, Belastingdienst, Rijkswaterstaat, ministeries van Defensie en Justitie en Veiligheid en Logius) een tweetal vragen gesteld om een eerste globale indruk te krijgen van het gebruik van RPKI: of routes met RPKI worden ondertekend en of RPKI-ondertekende routes worden gevalideerd.

Dit jaar zijn vragen voorgelegd aan 14 deelnemers aan Overheidsbrede Verdiepingssessies Connectiviteit, georganiseerd door Logius. Elf organisaties hebben gereageerd op de vragen: dezelfde organisaties als uit de vorige meting, met daar nu ook DUO, de Politie, het Kadaster en BKWI bij. De vraagstelling is dit jaar net iets anders dan vorig jaar. De drie vragen luiden aldus:

- Zijn de IP-adressen die uw organisatie zelf beheert ondertekend met RPKI?
- Zijn de IP-adressen van uw leveranciers ondertekend met RPKI?
- Valideert uw organisatie RPKI-ondertekende IP-adressen?

De eerste vraag wordt door zeven van de elf respondenten bevestigend beantwoord.

De tweede vraag wordt vanuit twee organisaties met “ja” beantwoord, door één organisatie met deels. Let wel: deze vraag is voor 4 organisaties niet van toepassing omdat bij hen geen sprake is van IP-adressen van leveranciers.

Bij de laatste vraag reageren drie organisaties bevestigend.

Ook al gaat de vergelijking met de vorige meting zoals aangegeven niet helemaal op, toch lijkt sprake te zijn van **enige groei van het gebruik** van RPKI, zowel waar het de ondertekening betreft als de validering.

Vorig jaar was aanvullende informatie beschikbaar met betrekking tot het gebruik van RPKI bij voorzieningen (RPKI-ondertekening op zowel IPv4 als IPv6?). Dit jaar is die informatie niet beschikbaar.

Relevante ontwikkeling

Een belangrijke stap om een completer beeld te verkrijgen van het gebruik van RPKI kan zijn om deze standaard onder te brengen bij internet.nl en langs die weg het gebruik te meten binnen het kader van de IV-meting. Vooralsnog is echter geen streefbeeld geformuleerd aangaande het gebruik van RPKI. Dat is wel een voorwaarde bij opname in de IV-meting.

SAML

Waarom belangrijk ?

Security Assertion Markup Language (SAML) is een standaard voor het veilig uitwisselen van authenticatie- en autorisatiegegevens van gebruikers tussen verschillende organisaties. SAML maakt het mogelijk om op een veilige manier via het internet toegang te krijgen tot diensten van verschillende organisaties, zonder dat je per dienst eigen inloggegevens nodig hebt, of bij elke dienst apart moet inloggen. Bij SAML spelen drie partijen een rol: de ‘gebruiker’, de ‘Identity Provider (IdP)’ en de ‘Service Provider (SP)’. De IdP regelt het authenticatieproces van de gebruiker en kan na succesvolle authenticatie aan de SP-gegevens verstrekken over

de identiteit, attributen en rechten van een gebruiker. SAML wordt gebruik bij onder andere DigiD machtigen en eHerkenning. SAML is een internationale standaard die is ontwikkeld door de standaardenorganisatie OASIS, en in een veelheid aan toepassingen kan worden geïmplementeerd. Er is geen centraal overzicht van toepassingen die op SAML gebaseerd zouden moeten zijn. Het is ook niet doelmatig om een dergelijk overzicht te creëren en actueel te houden. De standaard staat op de 'pas toe of leg uit' lijs sinds mei 2009.

Feitelijk gebruik

SAML is de standaard geworden voor (nieuwe) aansluitingen waarbij burgers of bedrijven inloggen bij de overheid. Twee belangrijke toepassingen van SAML in Nederland zijn eHerkenning en DigiD, waarmee bedrijven respectievelijk burgers zich kunnen authentiseren en identificeren bij overheden. Het aantal aansluitingen op deze voorzieningen is dan ook net als in voorgaande jaren als indicator genomen om het gebruik van SAML te meten.

	2016	**2017**	**2018**	**2019**	**2020**	**2021**
eHerkenning: SAML	168	203	359	439	458	493
DigiD: SAML	128	290	398	429	558	onbekend
eHerkenning + DigiD	296	493	757	868	1.016	onbekend

Bron: navraag bij de beheerders van eHerkenning en DigiD bij Logius (peildatum 31-12-2020).

Uit bovenstaand overzicht kan worden opgemaakt dat voor het vijfde achtereenvolgende jaar sprake is van een toename van het aantal aansluitingen en daarmee een **toename van het gebruik** van SAML (+ 8%). Kanttekening hierbij is dat dit jaar alleen cijfers over eHerkenning beschikbaar zijn.

STARTTLS & DANE

Waarom belangrijk ?

STARTTLS maakt het mogelijk om SMTP-verkeer tussen mailservers over een met TLS versleutelde verbinding te laten lopen.

DANE, dat voortbouwt op DNSSEC, geeft zekerheid over de identiteit van de ontvangende mailserver. Dit voorkomt dat een aanvaller zich kan uitgeven als ontvangende-mailserver, waardoor hij het mailverkeer kan onderscheppen. Daarnaast dwingt DANE het gebruik van TLS af. Dit voorkomt dat een aanvaller de opzet van STARTTLS kan blokkeren, om zo toegang tot de onversleutelde berichten te krijgen.

STARTTLS & DANE staan op de 'pas toe of leg uit' lijst sinds september 2016.

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaarden kijken we naar de ondersteuning van STARTTLS en DANE voor inkomende e-mail op 558 domeinen van de overheid. Zie hiervoor de IV-meting van maart 2021 (Bijlage B6).

Wat niet is gemeten is of mailservers ook uitgaande STARTTLS en DANE ondersteunen.

	medio 2018 (september)	begin 2019 (maart)	medio 2019 (september)	begin 2020 (maart)	medio 2020 (september)	begin 2021 (maart)
STARTTLS	94 %	94 %	97 %	98 %	99 %	100%
STARTTLS cf. NCSC	55 %	67 %	76 %	87 %	42 %	69 %
DANE	25 %	41 %	45 %	50 %	53 %	55 %

Vergeleken met vorig jaar is het gebruik van **STARTTLS toegenomen**. Met een percentage van 100% is geen sprake meer van enige groeipotentie. Het beeld van dezelfde standaard maar dan conform de aanbevolen configuratie volgens het NCSC laat een ander beeld zien. Tot en met de meting van maart 2020 zien we een gestage groei, maar bij de meting september 2020 is sprake van een forse terugval, van 87% naar 42%. Dit heeft te maken met een aangepaste norm waardoor de lat hoger is komen te liggen. Inmiddels is de **weg omhoog** weer ingeslagen **bij STARTTLS cf. NCSC** met een stijging van 42% naar 69% .

Het gebruik van **DANE neemt gestaag toe**. Daar zit ook nog steeds verbeterpotentieel. DNSSEC MX toont het directe potentieel voor DANE. Het kunnen gebruiken van DANE is immers technisch afhankelijk van de implementatie van DNSSEC voor mailservers (MX).

Een vergelijking met de meting onder de breder samengestelde groep van circa 2.200 domeinnamen van de overheid wijst uit dat het gebruik van STARTTLS ook daar zeer hoog scoort, met 97%. Voor DANE geldt dat echter in mindere mate; de score valt voor die standaard met 39% lager uit dan voor de kerngroep van 558 domeinen (55%).

Kijkend naar de invalshoek van verschillen in het gebruik tussen de diverse overheidslagen vallen tot slot nog enkele zaken op:

- het gebruik van STARTTLS is bij elk van de onderscheiden overheidslagen heel hoog (met een laagste score van 97% voor waterschappen, bij de andere overheidslagen 100%);
- na een eerdere terugval van STARTTLS conform NCSC vorig jaar is vastgesteld dat met de meting van maart 2021 de weg omhoog weer is gevonden. Deze beweging vinden we terug bij elk van de overheidslagen. En als de overheidslagen onderling worden vergeleken zien we dat naarmate de terugval bij de vorige monitor groter was, de stijging nu ook groter is;
- het Rijk scoort op het gebruik van DANE beduidend beter (87%) dan de andere overheidslagen, met uitvoeringsorganisaties als goede tweede (71%). Met name provincies en waterschappen blijven achter met scores van respectievelijk 32% en 27%. De score voor gemeenten ligt op 52%.

STIX & TAXII

Waarom belangrijk ?

STIX en TAXII zijn standaarden voor partijen die samenwerken op het gebied van cybersecurity. Door standaarden te gebruiken wordt het mogelijk om sneller en gemakkelijker informatie te delen over dreigingen en kwetsbaarheden en om zodoende de juiste maatregelen te kunnen nemen om computersystemen te beschermen. Daarbij is STIX een gegevensopslagformaat dat gebruikt wordt in threat intelligence platformen voor cybersecurity-analyses en TAXII is een protocol voor de uitwisseling van deze gegevens. Het

gebruik van deze standaarden is een belangrijke stimulans voor de versterking van de weerbaarheid tegen cyberdreigingen. De standaarden STIX en TAXII staan op de 'pas toe of leg uit' lijst sinds november 2017.

Feitelijk gebruik

Er is geen objectieve meetmethode voorhanden om het gebruik van STIX en TAXII inzichtelijk te maken. Op de markt voor cybersecurity-software is wel een beweging zichtbaar dat nieuwe producten steeds meer bij deze standaarden aansluiten. Dat zijn met name uitwisselingsdiensten van cybersecurity-informatie en geïntegreerde "security orchestration, automation and response-platformen" (SOAR-tooling). Deze systemen gebruiken de standaarden steeds vaker als opslag- en uitwisselingsformaat en anders hebben ze tenminste connectoren die daarmee kunnen uitwisselen. Om zicht te geven op het feitelijke gebruik moeten we kijken naar de organisaties die cybersecurity-informatie verwerken met onderscheid tussen de coördinerende instanties en de daarbij aangesloten organisaties.

<u>Nationaal niveau</u>

De standaarden STIX en TAXII worden onder meer gebruikt door het Nationaal Cyber Security Centrum (NCSC). Het NCSC maakt hiervan gebruik in het Nationaal Detectie Netwerk (NDN), een netwerk dat zich richt op het onderling delen van dreigingsinformatie. Het NDN is toegankelijk voor Rijksoverheidsorganisaties, vitaal verklaarde private organisaties en organisaties die onderdeel zijn van het Landelijk Dekkend Stelsel (LDS) zoals verscheidene CERT's en OKTT's, de zogeheten organisaties die Objectief Kenbaar Tot Taak hebben andere organisaties te informeren over dreigingen.

Binnen de Rijksoverheid zijn 155 van de 190 organisaties aangesloten bij het NDN, wat een dekkingsgraad geeft van 82% (vorig jaar 72%). Bij een vergelijking met 2 jaar terug is sprake van een groei van bijna 55%. Van de vitale partijen is het merendeel aangesloten; exacte aantallen hiervan worden niet vrijgegeven. Wanneer een Rijksoverheidspartij aansluit bij het NDN kan er een sensor geplaatst worden in het netwerk van betreffende organisatie. Deze sensor scant het netwerk op malafide indicatoren die door het NCSC worden aangeleverd. De meldingen worden door de organisatie zelf, eventueel in samenwerking met het NCSC, opgevolgd. Vitale organisaties ontvangen geen sensor, zij kunnen toegang krijgen tot, en/of een koppeling maken met de NDN-feed met dreigingsinformatie. Op deze manier wordt zo veel mogelijk dreigingsinformatie met de doelgroep gedeeld en kunnen deelnemers maatregelen nemen om schade te voorkomen of te beperken. Tenslotte, een incident voor de één, is preventie voor de ander.

Van alle NDN-deelnemers maken de meesten voor hun gegevensuitwisseling met NDN ook gebruik van TAXII. De STIX-standaard heeft vanwege zijn inzetmogelijkheden een kleiner toepassingsbereik en wordt alleen gebruikt door de grotere NDN deelnemers die ook over een eigen threat intelligence platform beschikken.

Het NDN maakt gebruik van verschillende threat intelligence platformen (TIP's), afhankelijk van de doelgroepen waarmee wordt samengewerkt. Die zijn in open source varianten verkrijgbaar maar ook steeds meer als commerciële softwareproducten. In deze platformen is het mogelijk om verschillende vormen van informatie over cyberdreigingen en cyberaanvallen op te nemen waaronder STIX. TAXII dient als transportmiddel van STIX en beide standaarden worden over het algemeen in combinatie met elkaar gebruikt. In

commerciële TIP's wordt met name de STIX-standaard soms op een eigen specifieke manier ingevuld en aangevuld waardoor verschillende dialecten ontstaan. Bij de aanschaf van software moet je dus opletten dat de standaarden zodanig worden toegepast dat de gegevens zo veel mogelijk zonder verlies kunnen worden uitgewisseld met producten en diensten van andere leveranciers.

Gemeentelijk niveau
De Informatiebeveiligingsdienst (IBD) van VNG Realisatie regelt de threat intelligence voor verschillende gemeenten als onderdeel van GGI-Veilig. Het overgrote deel van de gemeenten heeft immers niet het 'volwassenheidsniveau' om zelf het proces van threat intelligence uit te voeren. Een van de onderdelen waar het om gaat is SIEM/SOC-dienstverlening die door KPN geleverd wordt.

In de aanbesteding van GGI-veilig zijn eisen aan de SIEM/SOC-dienst gesteld. Hierin staat onder andere dat de dreigingsinformatie bi-directioneel via een koppeling wordt gedeeld. Voor wat betreft het kunnen uitwisselen van dreigingsinformatie geldt dat dit dient te gebeuren middels open standaarden (STIX/TAXII). Een verdere eis in de aanbesteding was dat de Advanced Threat Protection-oplossing het TAXII-protocol ondersteunt voor geautomatiseerde uitwisseling van cyberdreigingsinformatie (IoC's) op basis van het STIX-formaat.

Het nieuwe Cyber Threath Intelligence platform (CTI platform) dat onderdeel is van de SIEM/SO-dienst van KPN is in het derde kwartaal van 2021 in gebruik genomen. Hierbij is ook de NDN-feed ten behoeve van gemeenten gekoppeld. Het tempo waarin gemeenten aansluiten op GGI-Veilig Monitoring & Response (M&R) is bepalend voor de adoptiegraad van STIX/TAXII. Zolang men nog niks met M&R doet en dus ook niet met het CTI platform komen deze standaarden niet in beeld. Voor gemeenten die aangesloten zijn op GGI Veilig zijn deze standaarden dus geborgd, maar het is vooralsnog eenrichtingverkeer. Van terug delen is nog geen sprake. Als we het hebben over feitelijk gebruik, dan gaat het om nu om 5 organisaties die samen 10-12 gemeenten vertegenwoordigen. Er lopen gesprekken met tientallen andere gemeenten om ook aan te sluiten.

Relevante ontwikkeling

Sinds de vorige rapportage zijn nieuwe versies van beide standaarden beschikbaar gekomen. Ten opzichte van de oude versie 1.2.1 is een meer uitgebreide versie 2.0 vastgesteld die in de praktijk echter lastig bruikbaar is gebleken. Inmiddels zijn de kinderziektes verholpen en is een nieuwe versie 2.1 vastgesteld, die volgens NCSC veel beter bruikbaar is. Dat impliceert dat moet worden bezien of deze versie 2.1 op de pas-toe-of-leg-uit lijst kan komen te staan.

WPA2 Enterprise

Waarom belangrijk ?

WPA2 Enterprise maakt het mogelijk dat gebruikers automatisch en veilig toegang krijgen tot aangesloten WiFi-netwerken. Ook als deze WiFi-netwerken zich buiten de eigen organisatie bevinden. De authenticatie vindt plaats op basis van bestaande identiteitsgegevens van de gebruiker, hierdoor hoeven gebruikers niet opnieuw in te loggen. Met het gebruik van WPA2 Enterprise is ook de integriteit van de netwerkverbinding geborgd. Bij WPA2 Enterprise spelen

drie partijen een rol: de 'gebruiker', de 'Identity Provider (IdP)' en de 'Service Provider (SP)'. Zodra een gebruiker contact maakt met het betreffende WiFi-punt toetst de SP (beheerder van het WiFi-punt) op basis van de inloggegevens bij de IdP (de thuisorganisatie van de gebruiker) de identiteit van de gebruiker. Na positieve verificatie van de identiteit van de gebruiker, wordt toegang verleend tot het WiFi-netwerk zonder dat aanvullende inlog noodzakelijk is. Diensten zoals Govroam, Rijk2Air en Eduroam maken gebruik van WPA2 Enterprise. De standaard staat op de 'pas toe of leg uit' lijst sinds 2 februari 2016.

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaard wordt sinds 2016 het aantal deelnemende organisaties (peildatum begin september) geteld van Govroam en Eduroam. (Bron: https://govroam.nl/over-govroam/deelnemende-organisaties resp. https://eduroam.nl/instellingen). Eduroam is er al sinds 2003 en Govroam is in 2013 gelanceerd.

	2016 (september)	**2017** (september)	**2018** (september)	**2019** (september)	**2020** (juni)	**2021 (aug/sept)**
Govroam	49	132	244	307	332	337
Eduroam	157 (mei)	199	215	222	231	250
samen	206	331	459	529	563	587

Uit bovenstaand overzicht blijkt dat het gebruik van WPA2 Enterprise vergeleken met vorig jaar is **toegenomen** met ruim 4%. Deze stijging vinden we terug bij beide bronnen: zowel bij Govroam als bij Eduroam.

Het aantal gekoppelde instellingen aan Eduroam is hoog en zit tegen het maximum aan; de groeipotentie voor de komende periode is daarmee beperkt geworden. Het aantal gekoppelde organisaties aan Govroam stijgt gestaag. Hier ligt ook nog voldoende potentie om het aantal deelnemers te laten stijgen.

Relevante ontwikkeling

Vanuit de stichting Govroam zijn twee ontwikkelingen gemeld. Inmiddels is govguest officieel gelanceerd. Tevens zijn pilots gestart met getgovroam en govvpn. Getgovroam maakt het eenvoudig om via een app een govroam-profiel te genereren op basis van EAP-TLS, na inlog via SAML met de credentials van de thuisorganisatie, en is gebaseerd op geteduroam. GovVPN is wat de naam zegt: een VPN-dienst waarmee govroamgebruikers veilige toegang tot internet kunnen verkrijgen zelfs als ze met onveilige wifi-netwerken verbonden zijn.

B5.2. Domein Document en (web/app)content

Ades Baseline Profiles

Over deze standaard is helaas geen informatie beschikbaar..

Digitoegankelijk

Over deze standaard is helaas geen informatie beschikbaar.

ODF en PDF

Waarom belangrijk ?

ODF is een applicatie- en leveranciers-onafhankelijke, duurzaam toegankelijke documentstandaard. Ook in de toekomst blijven ODF-bestanden toegankelijk, ongeacht de kantoorapplicaties die op dat moment al dan niet worden ondersteund. ODF-bestanden hebben een structuur waardoor ze gemakkelijk te exporteren zijn naar PDF-documenten die voldoen aan duurzaamheids- en toegankelijkheidsrichtlijnen. Dankzij deze structuur kunnen zoekmachines ODF-bestanden goed indexeren en vinden. Alle gangbare kantoorapplicaties kunnen ODF-bestanden lezen en schrijven. Het gebruik van het standaardformaat ODF staat los van het al dan niet gebruiken van vrije of open source kantoorapplicaties. ODF heeft de interessante eigenschap dat het andere bestandsformaten zoals PDF kan inkapselen. Zo is het mogelijk om een document in ODF met z'n PDF-representatie in hetzelfde ODF-bestand op te slaan. ODF staat op de 'pas toe of leg uit' lijst sinds 15 juni 2012.

PDF is een format voor de uitwisseling van documenten die bedoeld zijn om op te slaan of af te drukken, en waarvan de pagina opmaak vastligt. Het uitgangspunt van PDF is dat gebruikers documenten kunnen uitwisselen, opslaan en afdrukken, onafhankelijk van de omgeving waarin ze zijn aangemaakt. Een PDF-document ziet er op alle apparaten en in alle omgevingen hetzelfde uit. PDF is minder geschikt voor het publiceren van online informatie die veel op mobiele apparaten wordt bekeken. PDF staat op de 'pas toe of leg uit' lijst sinds 18 november 2009.

Feitelijk gebruik

De meting is gedaan op basis van een steekproef bij overheidsorganisaties die vallen binnen het organisatorisch werkingsgebied van de pas-toe-of-leg-uit lijst. De steekproef bestaat uit een totaal van 98 organisaties uit verschillende delen van de overheid:

- De 30 meest bezochte websites van de overheid (volgens Communicatie Rijk).
- De 30 grootste gemeenten plus VNG en VNG Realisatie.
- De 12 provincies plus IPO.
- De 21 waterschappen plus UVW en waterschappen.nl.

Voor deze meting zijn op elke onderzochte website de documenten gezocht en is bepaald van welk type de documenten zijn. Daarbij wordt onderscheiden tussen PDF, ODF en Microsoft Office (.docx, .xlsx, .pptx, .doc, .xls, .ppt) bestanden. Verder wordt op elke website één willekeurig PDF document van na 2018 gekozen en wordt vastgesteld of de PDF voldoet aan de standaarden (PDF/A, PDF 1.7) die op de pas-toe-of-leg-uit lijst staan. Ook wordt vastgesteld of het willekeurig gekozen bestand PDF bestand digitaal toegankelijk is.

Voor het zoeken van documenten op websites is gebruik gemaakt van Google search (https://www.google.com). Hoewel de steekproef en de methode hetzelfde was als in 2020 en 2019 is sprake van aanzienlijke verschillen in de resultaten, vooral in het aantal gevonden Microsoft Office documenten en in mindere mate ODF (zie de tweede en derde regel in de tabel). Dat komt waarschijnlijk omdat de telling dit jaar door een andere organisatie en op

een andere desktopomgeving uitgevoerd dan de twee voorgaande jaren. Google levert zoekresultaten op basis van het profiel van de vrager en andere contextuele informatie zoals de omgeving waarop de zoekopdracht wordt uitgevoerd. Twee dezelfde Google zoekopdrachten kunnen daarom verschillende resultaten opleveren, afhankelijk van wie de zoekopdracht op welk moment en vanaf welk apparaat doet. Google zoekopdrachten zijn daarom niet zonder meer reproduceerbaar, en we moeten dus rekening houden met een aanzienlijke 'meetfout'. Dit is een groot nadeel van de huidige meetmethode maar er is vooralsnog geen werkbaar alternatief voor.

De getoonde uitkomsten in onderstaande tabel geven dus niet meer dan een indicatie van trends op basis van een steekproef (tussen haakjes de gegevens uit 2019 en 2020).

	Top 30 overheid	**G30 gemeenten**	**Provincies**	**Water-schappen**
Aantal gevonden PDF	312.540 (325008, 381849)	183.370 (168005, 197482)	150.451 (116886, 173860)	19.711 (22951, 34268)
Aantal gevonden ODF	952 (17, 15)	15 (4, 2)	181 (8, 4)	3 (1, 2)
Aantal gevonden MS Office	14.523 (39, 123)	17.928 (30, 98)	10.886 (25, 51)	348 (6, 52)
Percentage PDF van alle gevonden documenten	95,28% (99,99%, 99,13%)	91,09 (99,98, 99,95%)	93,15% (99,97%, 99,87%)	98,25% (99,97, 99,72%)
Percentage ODF van de gevonden bewerkbare documenten	6% (30% ,11%)	<1% (12%, 2%)	2% (24%, 7%)	1% (14%, 4%)
Percentage ISO PDF	35% (47%, 36%)	45% (43%, 47%)	33% (33%, 57%)	67% (29%, 41%)
Percentage digitaal toegankelijke PDF	23% (23%)	7% (17%)	17% (25%)	0% (0%)

De belangrijkste observaties naar aanleiding van dit overzicht:

- 11% meer documenten dan in 2020 op websites van overheden, maar 11% minder dan in 2019. Als rekening wordt gehouden met de meetfout die samenhangt met de onbetrouwbaarheid van Google zoekopdrachten, is er geen duidelijke trend zichtbaar. Het globale aantal documenten op websites van de overheid lijkt in grote lijnen stabiel over de afgelopen twee jaar.
- PDF blijft veruit het meest gebruikte format voor de publicatie van documenten. Over alle gemeten websites heeft 94% van de documenten een PDF format. Dat lijkt minder dan de >99% in voorgaande jaren, maar het verschil kan te wijten zijn aan de meetfout die door Google zoekopdrachten wordt veroorzaakt. Ondanks deze meetfout blijft het evident dat PDF bestanden de grote overhand hebben op websites van de overheid.
- Op de 98 onderzochte websites zijn in totaal 666.072 PDF-bestanden gevonden. Dat is een gemiddelde van 6.797 PDF-bestanden per website. Dit gemiddelde is in lijn met de voorgaande jaren, zelfs als we rekening houden met de meetfout. Net als vorige jaren constateren we grote verschillen in aantallen PDF's tussen websites. Sommige websites hebben slechts enkele tientallen PDF-documenten, andere hebben er duizenden.
- Van de steekproef van 98 PDF-bestanden (1 per onderzochte organisatie) voldeed 46% aan de ISO standaard PDF 1.7 of PDF/A op de 'pas toe of leg uit'-lijst. Dat is iets meer dan de 40% die we in 2020 vaststelden. De groei aan ISO PDF documenten is vooral te zien bij de Waterschappen, terwijl de 30 grootste overheidswebsites juist iets terugvielen.

- Van de steekproef van 98 PDF-bestanden van na 2018 is slechts 12% digitaal toegankelijk (en voldoet dus aan de wettelijke verplichting). Dat is minder dan de 16% die we maten in 2020. Het verschil kan echter verklaard worden door het feit dat we dit jaar een verbeterde validatiemethode hanteren die minder 'valse positieven' doorlaat. We constateren namelijk wel dat er dit jaar meer websites zijn die geen PDF's van voor 2018 meer aanbieden. Zeven van de 30 grootste websites van de overheid (23%) hebben geen PDF's meer van voor 2018 en publiceren hun informatie dus in andere formats zoals HTML, die beter digitaal toegankelijk te maken zijn. Daaruit zouden we kunnen opmaken dat er bij de overheid wel degelijk een beweging op gang is om digitaal toegankelijker te publiceren. De Rijksoverheid lijkt hierin voor te lopen op de gemeenten, provincies en waterschappen.
- ODF vormt slechts 3,42% van de bewerkbare documenten op alle onderzochte websites. Dat is veel minder dan de gemeten 23% in 2020 en meer in lijn met de 6,7% in 2019. Het verschil is te verklaren doordat er dit jaar veel meer Microsoft Office documenten gevonden werden dan in 2020. Het aantal gevonden ODF documenten is niet minder geworden en zelfs gegroeid (vooral bij de Rijksoverheid en provincies).

In de monitor van vorig jaar werd opgemerkt dat sprake was van een sterke terugloop van Microsoft Office bestanden en een groei van het percentage ODF-bestanden. We concludeerden in 2020 dat overheden zich beter aan het 'pas toe of leg uit' beleid lijken te houden. De resultaten van dit jaar suggereren dat dit een vertekend beeld is geweest, veroorzaakt door de onbetrouwbaarheid van Google zoekopdrachten. Het beeld van 2021 komt beter overeen met het beeld van 2019, maar laat zelfs ten opzichte van dat jaar geen verbetering zien.

Zelfs met de kanttekening van onbetrouwbare Google-metingen kunnen we concluderen dat **ODF weinig wordt toegepast** waar dat verplicht is. Op basis van de meting van dit jaar ligt de conclusie voor de hand dat er **geen positieve trend** is, in tegenstelling tot wat wij vorig jaar dachten te zien. Anderzijds zien we dat overheden **meer PDF-bestanden publiceren die aan de ISO-normen voldoen** die op de 'pas toe of leg uit' lijst staan. Iets minder dan de helft van de 98 onderzochte documenten uit de steekproef voldoet aan de verplichte open PDF-standaarden, en dit aantal lijkt ieder jaar iets toe te nemen.

Relevante ontwikkeling

ODF wordt beheerd door OASIS. Deze internationale organisatie heeft geen specifieke ambities om het gebruik van ODF bij de Nederlandse overheid te stimuleren. In Nederland wordt het gebruik van ODF gestimuleerd door de OpenDoc Society en NLnet. De laatste drie jaar zijn deze organisaties echter niet actief geweest met het stimuleren van het ODF-gebruik.

PDF/A en PDF 1.7 worden beheerd door ISO. Deze internationale organisatie heeft evenmin specifieke ambities om het gebruik van PDF bij de Nederlandse overheid te stimuleren. Dit geldt ook voor de NEN die de ISO specificaties beschikbaar stelt. De PDF Association stimuleert het gebruik van PDF/A en PDF 1.7 en heeft een Benelux Chapter met een contact in Nederland. Deze PDF Association en in het bijzonder de Benelux Chapter worden gedragen door leveranciers van producten gerelateerd aan PDF. De stimulering en ondersteuning van PDF/A en PDF 1.7 vanuit de PDF Association is daarom nauw verweven met het commerciële aanbod.

OWMS

Waarom belangrijk ?

OWMS specificeert een verzameling meta-data, dat wil zeggen gegevens die gegevens beschrijven. Het doel van meta-data is de eigenschappen van ongestructureerde gegevens (bijvoorbeeld de inhoud van een website) te kenmerken zodat deze meer structuur krijgen. Hierdoor wordt de overheidsinformatie op het internet beter vindbaar en beter te interpreteren. Een organisatie gebruikt OWMS als de organisatie metadatering toepast en daarbij tenminste de in de OWMS standaard verplichte metadata elementen toepast. De OWMS-standaard staat op de 'pas toe of leg uit' lijst sinds 15 november 2011.

Feitelijk gebruik

Het feitelijk gebruik wordt gemeten op basis van een steekproef bij organisaties van de overheid die vallen binnen het organisatorisch werkingsgebied van de pas-toe-of-leg-uit lijst. De steekproef bestaat uit 98 organisaties van verschillende groepen overheden:

- De 30 meest bezochte websites van de overheid (volgens Communicatie Rijk).
- De 30 grootste gemeenten plus VNG en VNG Realisatie.
- De 12 provincies plus IPO.
- De 21 waterschappen plus UVW en waterschappen.nl.

Deze steekproef is gelijk aan de steekproef die in 2019 en 2020 gebruikt werd, waardoor de resultaten volledig te vergelijken zijn.

Bij elke website is gekeken of er metadatering plaatsvindt en of de volgens OWMS verplichte metadata aanwezig is. Conform het functioneel toepassingsgebied van OWMS worden alleen organisaties beoordeeld die metadatering toepassen op hun website. Een website voldoet alleen aan OWMS als alle volgens de standaard verplichte metadata aanwezig is. Sommige websites hebben enkele OWMS elementen maar missen één of meer elementen die verplicht zijn volgens de standaard. Deze gevallen worden apart vermeld in de onderstaande tabel met resultaten per overheidsgroep. De cursief gedrukte percentages op de tweede rij in elke cel betreft het resultaat van de meting van 2020.

	Top 30 overheid	**G30 gemeenten**	**Provincies**	**Water-schappen**	**Totaal**
Voldoet aan OWMS	11 (37%) *(43%)*	2 (6%) *(6%)*	5 (38%) *(38%)*	8 (35%) *(30%)*	26 (27%) *(28%)*
Voldoet helemaal niet: gebruikt andere metadata	14 (47%) *(47%)*	17 (53%) *(53%)*	2 (15%) *(15%)*	6 (26%) *(30%)*	39 (40%) *(42%)*
Voldoet niet, heeft wel enkele DC elementen	4 (13%) *(10%)*	7 (22%) *(22%)*	6 (46%) *(38%)*	9 (39%) *(35%)*	26 (27%) *(23%)*
Geen metadata	1 (3%) *(0%)*	6 (19%) *(19%)*	0 0% *(8%)*	0 (0%) *(4%)*	7 (7%) *(7%)*
TOTAAL	30 (100%)	32 (100%)	13 (100%)	23 (100%)	98 (100%)

Uit de tabel kan onder meer het volgende worden afgelezen:

- 91 van de 98 onderzochte organisaties (93%) publiceren metadata op hun website (vorig jaar eveneens 93%);

- in totaal voldoen 26 van deze 91 organisaties (27% van het totaal van 98) aan OWMS (vorig jaar 28%). Dit duidt op een **stagnatie**;
- bij de gemeenten wordt OWMS beduidend minder toegepast dan bij rijksoverheden, provincies en waterschappen;
- nog eens 26 van deze 91 organisaties (27% van 98) heeft een deel van de door OWMS verplichte metadata maar voldoet formeel niet aan de standaard. Een aantal organisaties past wel elementen van OWMS toe, maar doet dat onvolledig waardoor ze formeel niet aan de standaard voldoen. Deze tellen niet mee als organisaties die aan OWMS voldoen omdat OWMS een minimum aantal aanwezige elementen vereist;
- in zijn algemeenheid is er ten opzichte van de vorige meting sprake van minieme verschillen. In de kolom 'gemeenten' is het beeld zelfs identiek aan dat van vorig jaar;
- op vrijwel alle onderzochte websites is de metadata op alle pagina's hetzelfde, of alleen op de homepage aanwezig. Organisaties publiceren zelden specifieke metadata voor elke pagina op de website. Volgens de beheerder van OWMS heeft deze manier van metadatering maar beperkte waarde.

Als nadere duiding kan hier nog aan worden toegevoegd dat het gebruik van andere schema's voor metadatering zoals OpenGraph (Facebook) en Twitter toeneemt ten koste van het gebruik van OWMS.

Relevante ontwikkeling

OWMS moet gebruikt worden door alle overheidsorganisaties die metadatering toepassen op hun website. OWMS is een relatief gemakkelijk toe te passen standaard, zodat 100% gebruik ook echt haalbaar is daar waar de standaard verplicht is. Wel moet worden aangetekend dat het toepassen van de standaard weinig zegt over de kwaliteit van de metadata, die moeilijk objectief te bepalen is.

Er is sprake van de ontwikkeling van een nieuwe standaard voor metadatering die speciaal toegespitst is op het Platform Open Overheidsinformatie, PLOOI (https://www.open-overheid.nl/plooi/).). Deze nieuwe standaard voor metadatering zou in de plaats moeten komen van OWMS. Forum standaardisatie is hierover met de beheerorganisatie in gesprek.

SKOS

Waarom belangrijk ?

Het publiceren van gegevensbestanden in de vorm van begrippenlijsten, digitale woordenboeken en taxonomieën door overheidsorganisaties gebeurt vaak in de vorm van documenten die niet bruikbaar zijn voor computerprogramma's. SKOS zorgt ervoor dat deze kennisrepresentaties via het internet aan elkaar kunnen worden gekoppeld en maakt het mogelijk dat gegevensbestanden makkelijker als open data kunnen worden hergebruikt. Door het toepassen van de standaard worden de (familie)relaties tussen de verschillende definities van begrippen beter inzichtelijk en is data uit verschillende systemen beter te vergelijken en te interpreteren. De standaard staat op de 'pas toe of leg uit' lijst sinds 18 mei 2015.

Feitelijk gebruik

In principe kan het gebruik van SKOS vrijwel automatisch worden gemeten op de Linked Open Vocabularies (https://lov.linkeddata.es/dataset/lov/), maar daar lijkt vooralsnog alleen

de linked open data van het Kadaster te zijn aangemeld. De LOD Laundromat die vroeger toegang bood tot alle linked data wereldwijd, bestaat inmiddels niet meer. De makers van de LOD Laundromat hebben inmiddels een commerciële start-up TriplyDB opgericht, maar hier zijn nog geen datasets van de Nederlandse overheid te vinden.

Net als in voorgaande jaren lijkt een enquête de beste manier om iets van gebruiksgegevens van SKOS boven water te krijgen. De enquête is in juli 2021 uitgezet bij 64 overheden en semi-overheden. De steekproef van 2021 is vrijwel gelijk aan de steekproef gebruikt bij de meting van 2019 en 2020 en bestaat voornamelijk uit gebruikers van de LOD Nederland groep op LinkedIn. De inhoud van de enquête is dezelfde als vorig jaar, zodat de resultaten goed te vergelijken zijn. Ook dit jaar is gebruik gemaakt van EUSurvey, de open enquête applicatie van de Europese Commissie.

In totaal reageerden dit jaar 26 organisaties (41% van de ondervraagden). Dat is meer dan vorig jaar (26%), maar nog altijd aan de lage kant gezien het totaal aantal uitgezette enquêtes. Ter herinnering: twee jaar geleden lag de respons op 58%. Net als vorig jaar kan de aanhoudende COVID-19 pandemie en de zomerperiode iets te maken hebben met de relatief lage respons.

Van de 26 respondenten geeft 50% (13 organisaties) aan een begrippenlijst, woordenboek of taxonomie op het internet te publiceren. Vorig jaar lag het aandeel ook op 50%. Dit zijn in principe de organisaties die in aanmerking komen voor de verplichting van SKOS. Als wordt ingezoomd op deze 13 organisaties die kwalificeren voor een verplichting van SKOS dan zien we het volgende:

- 10 daarvan gebruiken SKOS (77% van 13). Dat is meer dan de 56% van vorig jaar, en meer in lijn met de 74% van 2019. Het lagere percentage van 2020 is dan ook waarschijnlijk te wijten aan de lage respons toen waardoor de steekproef dat jaar te weinig representatief was. Het percentage van 77% lijkt meer realistisch te zijn, en lijkt ook een licht stijgende lijn aan te geven.
- Over deze 10 gebruikers van SKOS nog het volgende:
  - 3 organisaties maken alleen gebruik van SKOS
  - 7 organisaties geven aan zowel SKOS als Web Ontolgy Language (OWL) te gebruiken. OWL is een andere open standaard met een soortgelijk functioneel toepassingsgebied als SKOS. SKOS en OWL zijn ook goed in combinatie te gebruiken zijn.
- 3 van de 13 organisaties gebruiken SKOS niet maar deze organisaties gebruiken wel OWL.
- 6 van de 13 organisaties (46%) gebruiken naast SKOS ook de open standaard SHACL. Dit is een aanbevelenswaardige combinatie omdat SHACL de kwaliteit van datasets borgt. SHACL staat (net als OWL) op de lijst aanbevolen standaarden van het Forum Standaardisatie.

De basis om een uitspraak te doen over de ontwikkeling van het gebruik van SKOS is smal. Met inachtneming van die constatering lijkt het erop dat sprake is van een **beperkte stijging** van het gebruik van SKOS. En een belangrijke bijbehorende conclusie is ook: daar waar deze open standaarden (SKOS maar als alternatief ook OWL) gebruikt *moeten* worden, gebeurt dat ook. De groeipotentie voor wat betreft het gebruik van SKOS zit hem er vooral in dat nog relatief weinig organisaties überhaupt linked data publiceren.

Enkele aanvullende observaties:

- Waar de overheid linked data toepast en publiceert, gebeurt dit vrijwel altijd met open standaarden.
- De resultaten bevestigen het beeld dat SKOS meestal gebruikt wordt waar het 'pas toe of leg uit' beleid dat verplicht. De resultaten zijn in lijn met de resultaten van eerdere jaren en laten een licht stijgende lijn zien.
- Ook het beeld uit 2019 en 2020 dat vooral uitvoeringsorganisaties SKOS en linked data toepassen, zien we dit jaar terug bij de respons. Wel was er iets meer respons vanuit provincies en waterschappen dan eerdere jaren.
- Het feit dat een organisatie SKOS gebruikt zegt niets over de kwaliteit van de datasets. De kwaliteit van de kennisrepresentatie met SKOS is minstens even belangrijk als de inzet van de standaard op zich, maar is veel moeilijker objectief te beoordelen zonder gedetailleerde kennis van het domein.
- Veel organisaties die SKOS gebruiken, gebruiken ook de OWL-standaard. De toepassingsgebieden van SKOS en OWL overlappen deels, waarbij OWL de 'zwaardere' standaard is die bij formelere kennissystemen wordt ingezet. Dit suggereert dat ook SKOS meestal wordt toegepast in grotere, serieuze linked data projecten. Vanwege de overlap zou het interessant zijn om te onderzoeken hoe deze organisaties SKOS en OWL combineren. De deze keer uitgezette enquête lijkt de 'alles of niets' trend van vorige jaren te bevestigen: óf een organisatie doet helemaal niet aan linked data, óf een organisatie pakt het meteen serieus aan.

Relevante ontwikkeling

SKOS wordt beheerd door W3C. Deze internationale organisatie heeft geen specifieke ambities om het gebruik van SKOS bij de Nederlandse overheid te stimuleren. In Nederland wordt het gebruik van linked data en SKOS ondersteund door het Platform Linked Data Nederland (PLDN).

Overheidsorganisaties kunnen bij het PLDN terecht voor informatie en hulp bij het toepassen van linked data en SKOS.

Het publiceren van linked data, en (SKOS) kennissystemen in het bijzonder, vereist veel specialistische kennis over semantiek en standaarden. Linked data komt langzaam maar zeker uit de experimentele hoek en het aantal linked data sets in productie neemt ieder jaar iets toe.

Op dit moment staan de linked data standaarden verspreid over de 'pas toe of leg uit' lijst en de lijst aanbevolen standaarden. SKOS staat op de 'pas toe of leg uit' lijst terwijl RDF, OWL en SHACL op de lijst aanbevolen standaarden staan. In de praktijk worden linked data standaarden vrijwel altijd in combinatie toegepast. Dit blijkt ook uit de enquête.

Forum Standaardisatie overlegt daarom momenteel met het Platform Linked Data Nederland over de mogelijke meerwaarde van het combineren van linked data standaarden in één groep op de lijst. Dit naar analogie van de stelselstandaarden Geo-standaarden, Digikoppeling en StUF die op de 'pas toe of leg uit' lijst staan en die ook uit verschillende deelstandaarden bestaan. Er is nog discussie over de vraag of de gecombineerde linked data standaarden dan als groep op de 'pas toe of leg uit' lijst of de lijst aanbevolen standaarden moet komen. Een vervolg hierop is komende herfst te verwachten.

B5.3. Domein REST API's

OpenAPI Specification

Over deze standaard is helaas geen informatie beschikbaar.

REST_API Design Rules

Over deze standaard is helaas geen informatie beschikbaar.

B5.4. Domein E-facturatie en administratie

NLCIUS

Waarom belangrijk ?

NLCIUS is een nieuwe versie van de oude standaard Semantisch Model e-Factureren (SMeF) en is een aanvullende specificatie op de Europese Norm EN16931 voor toepassing in Nederland. NLCIUS heeft net als de oude standaard tot doel om op semantisch niveau te komen tot één model voor elektronische facturen. In combinatie met de Europese Norm (EN)16931 beschrijft NLCIUS welke gegevenselementen er in een elektronische factuur opgenomen dienen en kunnen worden, wat de samenhang is tussen deze elementen en wat de betekenis is van deze elementen. Hierdoor wordt het eenvoudiger om meerdere standaarden te ondersteunen omdat een dergelijk model overheid en bedrijfsleven duidelijkheid biedt over welke elementen er op een elektronische factuur opgenomen dienen te worden ongeacht de onderliggende techniek van uitwisseling. De standaard staat op de 'pas toe of leg uit'- lijst sinds mei 2018.

Feitelijk gebruik

Beheer en bevordering van het gebruik van NLCIUS is belegd bij het Standaardisatieplatform e-factureren (STPE) waarin twee partijen samenwerken: NEN en TNO. Het initiatief wordt ondersteund door het Ministerie van Economische Zaken en Klimaat vanwege het maatschappelijke belang.

De belangrijkste gebruikers zijn aangesloten bij het Nationaal Multi-belanghebbenden Forum e_Procurement (NMBF): softwareleveranciers van financiële pakketten, leveranciers van telecommunicatie en IT en overheden (het Rijk, provincies en gemeenten).

Met betrekking tot (de ontwikkeling van) het gebruik van NLCIUS zijn de volgende globale indicaties beschikbaar, gebaseerd op een peilmoment mei 2021: (bron: Simplerinvoicing en NPa):

- het totaal aantal registraties op het Peppol-netwerk is ten opzichte van 2020 gestegen met 50%;
- het aantal serviceverzoeken (vragen) met betrekking tot NLCIUS is vergelijkbaar met de stroom aan vragen vorig jaar;

- het totale volume van verzonden en ontvangen e-facturen via Peppol is ten opzichte van vorig jaar gestegen met 25%.

Op basis van deze indicaties kan worden gesteld dat het **gebruik** van NCIUS **toeneemt**.

Relevante ontwikkeling

In de vorige monitor is melding gemaakt van het voornemen om in de komende periode (2021 – 2023) meer structureel het gebruik van de standaard te gaan monitoren. Dit voornemen is nog steeds actueel en is geformaliseerd in de vorm van een resultaatsverplichting in het werkplan van STPE: "inzicht krijgen in de adoptie van NLCIUS".

SETU

Waarom belangrijk ?

De SETU-standaarden worden gebruikt voor het elektronisch berichtenverkeer in de branche voor flexibele arbeid. SETU regelt het uitwisselen van berichten tussen aanbieders en afnemers (inleners) van tijdelijk personeel.

De SETU-standaarden zijn Nederlandse implementaties van internationaal geldende standaarden, namelijk HR-XML en voor de factuur ook UBL. Deze standaarden specificeren voor de Nederlandse uitzendbranche welke gegevenselementen verplicht en welke optioneel zijn bij de uitwisseling van informatie. Deze gegevenselementen worden vervolgens afgebeeld op de gegevens in de HR-XML standaarden waardoor er toepassingsprofielen ontstaan.

De SETU-standaarden worden ontwikkeld en beheerd door de Stichting SETU waarin alle grote uitzendorganisaties in Nederland betrokken zijn. Ook kleinere uitzendorganisaties en softwareleveranciers voor de branche voor flexibele arbeid kunnen actief participeren in de ontwikkeling.

De SETU-standaarden staan op de 'pas toe of leg uit' lijst sinds 20 mei 2009.

Feitelijk gebruik

Belangrijke gebruikers van de SETU-standaarden zijn de participanten en abonnees van SETU: daaronder naast uitzendorganisaties ook uitvoeringsorganisaties (Logius, UWV), softwareleveranciers en publiekrechtelijke organisaties als TNO.

In 2020 heeft de SETU een gebruikerspeiling uitgevoerd, waarin ook is nagegaan in welke volumes haar achterban berichtuitwisseling doet op basis van de SETU standaarden. Op jaarbasis komt dat per SETU bericht uit op het volgende:

SETU bericht	volumes op jaarbasis per organisatie
Invoice	range 20.000 – 2.500.000
Timecard	range 350.000- 2.500.000
Assignment	range 40.000 – 800.000
Human Resource	range 40.000 – 800.000
Staffing order	range 0 – 500.000

Hieruit blijkt dat er grote verschillen bestaan tussen de implementatie van de diverse berichten in de standaard. Zo worden de factuur (Invoice) en urenbrief (Timecard) op veel grotere schaal geadopteerd dan de overige berichten, die aan het begin van het proces toegepast dienen te worden.

Op de totale volumes heeft de SETU geen zicht, aangezien het berichtenverkeer niet via een centraal platform geregeld wordt.

Van de kant van de beheerorganisatie wordt de inschatting gemaakt dat het gebruik van de standaard **gelijk is gebleven**. Er hebben zich in de afgelopen periode geen ontwikkelingen voorgedaan die aanleiding hebben gegeven tot wijziging in het gebruik.

Uit dezelfde gebruikerspeiling heeft SETU de volgende conclusies getrokken:
- Toegevoegde waarde van de SETU-standaarden en -lidmaatschap is onvoldoende bekend in de branche. En helaas geldt hier 'onbekend maakt onbemind'.
- SETU-standaarden in gebruik laagdrempeliger maken. Hoe laagdrempeliger, hoe eenvoudiger de keuze voor adoptie. Specifiek voor het koppelen met MKB-partijen is integratie in bestaande softwarepakketten gewenst om adoptie van SETU te verbeteren.
- SETU-standaarden en -organisatie toekomstbestendiger maken.

Deze resultaten vormen een belangrijke bron voor het SETU-jaarplan 2021.

Relevante ontwikkeling

Dit jaar is de verwachting dat na een positieve consultatie onderstaande versies voor SETU-standaarden doorgevoerd worden:
- SETU Standard for Ordering and Selection v1.4
- SETU Standard for Assignment v1.4
- SETU Standard for Reporting Time and Expenses v1.4
- SETU Standard for Invoicing v2.2
- SETU Standard for Vacancies v1.1 (nieuw)

'Standard for Vacancies' betreft een nieuwe standaard in de set van SETU-standaarden, gericht op het uitwisselen van vacatures tussen uitzendbureaus, jobboards, het UWV Werkbedrijf en bedrijven en/of opdrachtgevers.

In 2021 start de SETU met een nieuwe werkgroep, die zich niet specifiek richt op de doorontwikkeling van SETU-standaarden, maar focust op relevante ontwikkelingen op het gebied van digitalisering en data-uitwisseling in de sector. Deze werkgroep richt zich op het voortijdig veranderingen in het uitzenddomein signaleren die impact hebben op de data-uitwisseling, afstemmen over en datadefinities uniformeren om zo te komen tot meer herbruikbare implementaties en identificeren van (nieuwe) behoeftes rondom data-uitwisseling waar de SETU gestandaardiseerde koppelvlakken voor kan opstellen. Daarnaast organiseert de SETU per 2021 webinars om alle geïnteresseerden op de hoogte brengen van relevante ontwikkelingen rondom de SETU, maar ook breder rondom digitalisering en data-uitwisseling.

De verwachting is dat deze initiatieven leiden tot toename van de bruikbaarheid en het gebruik van de standaarden.

WDO Datamodel

Waarom belangrijk ?

Het WDO Datamodel (WDO: Wereld Douane Organisatie) is een wereldwijde gegevensstandaard die als basis dient voor het elektronisch uitwisselen van gegevens en berichten wanneer goederen, personen en vervoermiddelen de grens over gaan. De gegevensstroom verloopt tussen bedrijven en overheden en tussen overheden onderling. Het WDO Datamodel voorziet erin om deze uitwisseling van gegevens te simplificeren en te harmoniseren.

Het WDO Datamodel is niet alleen van nut voor de Douane maar ook voor andere overheidsinstellingen die betrokken zijn bij grensoverschrijdend verkeer zoals Rijkswaterstaat, de Havenautoriteiten, de Koninklijke Marechaussee en de Nederlandse Voedsel en Warenautoriteit. Voor de Douane betreft het gebruik van de standaard de goederenstromen, maar daarnaast biedt het WDO Datamodel zoals gezegd ook informatie over personen (voor bijvoorbeeld de Marechaussee) en informatie over vervoermiddelen (voor bijvoorbeeld Rijkswaterstaat). De standaard staat op de 'pas toe of leg uit' lijst sinds 15 april 2014.

In veel landen wordt de douaneaangifte nog steeds (gedeeltelijk) op papier ingediend. Daarnaast moeten veel gerelateerde documenten, bijvoorbeeld certificaten van oorsprong of landbouwcertificaten, op papier bij andere overheidspartijen worden ingediend. In veel andere landen wordt al elektronisch gecommuniceerd, maar worden lokale standaarden gebruikt. Het betreft hier vaak nog verschillende standaarden omdat overheidsorganisaties vaak een eigen standaard voorschrijven, ook binnen de Europese Unie.

Door het gebruik van deze standaard kunnen de diverse overheidsorganisaties dezelfde taal spreken en eenvoudig informatie uitwisselen. Voor de administratie van import en export bevat het WDO Datamodel namelijk zogenaamde 'informatiepakketten' voor gegevensuitwisseling. Een informatiepakket beschrijft de semantiek van de uitgewisselde informatie: gegevens- en procesmodellen en hiervan afgeleide berichtspecificaties (Message Implementation Guidelines). Het doel van het gebruik van de standaard is een efficiënt verloop van de aankomst, het vertrek, de doorvoer en de vrijgave van goederen, vervoersmiddelen en personen in de internationale handel.

Feitelijk gebruik

De douane (beheerder van de standaard) meldt dat het WDO Datamodel momenteel gebruikt wordt voor de volgende bericht- en aangiftestromen:

- Single window: dit betreft 22 binnenkomende en 15 uitgaande berichttypes, alle gebaseerd op het WDO Datamodel. Gebruikers: Douane, Rijkswaterstaat en overige grensbewaking;
- Douane aangifte (DMS): dit betreft 2 binnenkomende en 1 uitgaand berichttypen, deels gebaseerd op EU CDM (en dus ook op WDO Datamodel omdat het een subset van het WDO Datamodel is), met de Douane als gebruiker;
- Douane eCommerce (DECO): dit betreft 2 binnenkomende en 1 uitgaand berichttypen, ook deels gebaseerd op EU CDM, met de Douane als gebruiker;

- Control bericht (gebruikt voor ontvangstbevestigingen en het melden van (syntax)fouten) en Meta Data (gebruikt als enveloppe voor alle aangiftestromen), beide gebaseerd op het WDO Datamodel.

Omdat in deze monitor, net als in de vorige monitor harde gegevens over het feitelijk gebruik ontbreken, is een goede vergelijking met het gebruik vorig jaar gebaseerd op cijfers niet te maken. Dat neemt niet weg dat de Douane melding maakt van **een toename van het gebruik**. Deze toename van het aantal op WDO Datamodel gebaseerde berichten zal zich vooral op de korte termijn verder gaan manifesteren nu eCommerce (DECO) daadwerkelijk in gebruik is genomen.

Relevante ontwikkeling

Aanvullend op de opsomming bij het overzicht van het feitelijk gebruik staan de volgende twee bericht- / aangiftestromen op de rol om in gebruik genomen te worden:

- Presentation Notification ICS2: dit betreft 1 binnenkomend en 1 uitgaand berichttype, gebaseerd op het WDO Datamodel;
- Douane Vervoersaangifte (DVA): dit betreft Transit en is momenteel nog in ontwikkeling. Het betreft 2 binnenkomende en 1 uitgaand berichttypen, ook deels gebaseerd op EU CDM.

Voor deze laatste onderdelen wordt de Douane als enige toekomstige gebruiker vermeld.

Op afzienbare termijn zal ook de Nederlandse Voedsel- en Waren Autoriteit tot de kring van gebruikers gaan behoren. Voor Landbouw zijn al stappen gezet om de fytosanitaire en veterinaire aangifte in WDO-formaat aan te kunnen leveren. Deze aangiften zijn echter vanwege andere prioriteiten (gebaseerd op EU-wetgeving) nog niet in productie genomen. Verdere uitbreiding naar andere gebruikers van het WDO Datamodel binnen de overheid die te maken hebben met binnen scope vallende processen is zeker een issue maar wordt in dit stadium niet als een echte prioriteit gezien.

XBRL

Waarom belangrijk ?

Organisaties wisselen bedrijfsinformatie uit op de meest uiteenlopende manieren (op papier of elektronisch, als Word-document, als Pdf, als spreadsheet, etc.). XBRL, eXtensible Business Reporting Language, is een internationale open standaard om deze bedrijfsrapportages met een financiële component op eenvoudige wijze te verzamelen, elektronisch uit te wisselen, te analyseren en zo nodig nader te bewerken. Deze XBRL-standaard staat op de pas-toe-of-leg-uit-lijst sinds 17 april 2010.

Feitelijk gebruik

Het gebruik van XBRL wordt al een aantal jaren in de Monitor Open Standaarden gemeten door te kijken naar het gebruik van de nationale standaard SBR (Standard Business Reporting) die gebruikt wordt in de voorziening Digipoort. In onderstaande tabel staat het aantal XBRL-berichten. Deze cijfers zijn in het kader van SBR gerapporteerd t.b.v. de monitor GDI. De cijfers van SBR zijn totalen inclusief machtigen en de cijfers zijn afgerond. Belangrijke voorstanders van deze XBRL-standaard binnen het publiek-private SBR-samenwerkingsverband zijn terug te vinden in de tabel: de Kamer van Koophandel, de Woningcorporatiesector, DUO en de Belastingdienst.

	Realisatie 2018	Realisatie 2019	Realisatie 2020	Realisatie 2021 t/m april
Belastingdienst				
Aangifte IB + VPB	17.167.811	16.558.025	15.568.706	6.660.188
Loonheffingen (incl. UZGB)	8.481.840	8.650.532	8.869.092	3.088.626
Erfbelasting + Schenkbelasting	231	4.073	16.115	12.040
Aangifte OB + Intercomm. prestaties	4.921.431	5.429.106	5.890.273	2.703.472
Toeslagen	1.242.836	1.325.719	1.279.414	523.013
KvK – Reporting Services (SBR)				
Jaarrekeningen	866.497	1.020.450	886.373	225.888
DUO – Reporting Services (SBR)				
Jaarrekeningen	1.838	1.953	1.942	120
SBR Wonen - Reporting Services (SBR)				
DPI (prognose informatie)	852	1.112	1.194	147
DVI (verantwoordingsinformatie)		1.363	1.370	5
SBR Wonen Jaarrekening		1.364	1.242	6

Een vergelijking van de cijfers over de (volledige) jaren 2018, 2019 en 2020 lijkt erop te duiden dat de adoptie van SBR en daarmee XBRL binnen Nederland per saldo even **stilstaat**.

Er is nog potentie voor verdere groei van het gebruik van XBRL binnen Nederland. Immers, indien er van uit wordt gegaan dat bij financiële verantwoordingsrapportages SBR gebruikt zou moeten worden dan impliceert dat dat dat alle ministeries, provincies, waterschappen, gemeenten, uitvoeringsinstanties en ZBO's gebruik zouden moeten maken van SBR. Dit is echter nog niet de praktijk.

Relevante ontwikkeling

In september 2020 is het Kenniscentrum XBRL opgericht. De eerder genoemde uitvragende partijen kunnen hier onder meer met hun vragen op het gebied van XBRL terecht. Hoofdtaak van dit Kenniscentrum is het ontwikkelen en beheren van taxonomieën voor deze publieke partijen. Zo helpt het Kenniscentrum mee met het opstellen van gegevensdefinities en worden afspraken beheerd die zijn vastgelegd in de Nederlandse Taxonomie Architectuur (NTA). Daarnaast levert het Kenniscentrum een bijdrage aan de internationale XBRL-standaard en zorgt ervoor dat mondiale ontwikkelingen ook worden opgenomen in de NTA.

Ook internationaal wordt de standaard breed gebruikt door financiële toezichthouders zoals de Europese Centrale Bank maar ook nationale partijen zoals de SEC (USA) en de ESMA (EU). Een recente trend is de toename van duurzaamheidsrapportages. Er wordt onderzoek gedaan naar mogelijkheden om deze duurzaamheidsrapportages ook in XBRL uit te vragen.

B5.5. Domein Stelselstandaarden

Digikoppeling

Waarom belangrijk ?

Digikoppeling bestaat uit een set standaarden voor elektronisch berichtenverkeer tussen systemen van overheidsorganisaties. Digikoppeling onderkent twee hoofdvormen van berichtenverkeer:

- Synchroon berichtenverkeer: een verzoek waarbij het vragende informatiesysteem wacht op een antwoord. Snelheid van afleveren is belangrijk. Als een antwoord uitblijft kan de vrager de vraag opnieuw stellen.
- Asynchroon berichtenverkeer: het meldende systeem stuurt een bericht en –eventueel- volgt op een later tijdstip een antwoord. Bij meldingen is de betrouwbare aflevering van het bericht essentieel. De melder moet zekerheid hebben dat zijn melding is ontvangen.

Digikoppeling staat op de 'pas toe of leg uit' lijst sinds 20 mei 2009.

Feitelijk gebruik

Logius (Stelselvoorzieningen) heeft op verschillende peilmomenten (maart 2013, augustus 2013, augustus 2014, augustus 2015, zomer 2016 tot en met 2021) lijsten aangeleverd waarop (onderdelen van) overheden en uitvoeringsorganisaties stonden die op Digikoppeling zeggen te zijn aangesloten. Daaruit is het onderstaande overzicht af te leiden.

Het overzicht wijst uit dat gedurende een reeks van jaren sprake is van een **gestage groei** van het gebruik van Digikoppeling, die over het afgelopen jaar lijkt te stagneren.

Dit is niet per definitie slecht nieuws. In de categorieën gemeenten, provincies en waterschappen is de dekking sinds 2019 volledig te noemen. Voor de categorie Rijk en uitvoeringsorganisaties geldt dat **het gebruik sinds de laatste meting wel degelijk is toegenomen**, maar omdat de groep zelf ook is gegroeid (er is met name een flinke toename in het aantal gemeenschappelijke regelingen) blijft het totaalpercentage sinds de laatste meting toch gelijk (65% in deze groep). In 2016 gebeurde hetzelfde, waardoor destijds het percentage zakte van 64% naar 40%.

Digikoppeling	Rijk + Uitvoerings-Organisaties/ ZBO's + OOV + eOverheid	Ministeries + BR's + GR's ZBO's + HCS + AC's + RO's	Gemeenten	Provincies	Waterschappen	**Totaal**
Voorjaar 2013	3 %		31 %	8 %	14 %	22 %
Zomer 2013	4 %		42 %	15 %	14 %	29 %
Zomer 2014	5 % [1]		57 %	23 %	14 %	40 %
Zomer 2015	64 %		63 %	42 %	24 %	58 %
Zomer 2016	40 %		75 %	67 %	46 %	64 %
Zomer 2017	67 %		92 %	67 %	50 %	76 %
Zomer 2018	X [2]		98 %	75 %	59 %	95 % [3]
Zomer 2019		60 %	100 %	100 %	100 %	90 % [2]
Zomer 2020		65 %	100 %	100 %	100 %	91%
Zomer 2021		65 % [4]	100 %	100 %	100 %	91%

Bron: opgave beheerorganisatie Logius

Over de verantwoording van bovenstaande cijfers nog het volgende. Het meten van de toepassing van de Digikoppeling standaard is lastig omdat het gebruik van dit transportprotocol buiten het zicht van de beheerder – Logius- omgaat. Digikoppeling kent geen centrale component waarlangs berichten worden gevoerd en inzicht in het gebruik kan dus niet op basis van kwantitatieve metingen worden gedaan. Verder zet de trend steeds meer door dat overheidsorganisaties gebruikmaken van Cloudoplossingen aangeboden door zowel publieke als private dienstverleners waardoor de vraag "*organisatie gebruikt Digikoppeling*" een complex antwoord kan hebben. Er bestaat echter een objectief meetinstrument om te bepalen of een organisatie Digikoppeling toepast in een van haar ketens van elektronische gegevensuitwisseling. Digikoppeling vereist namelijk een OIN – het Organisatie Identificatienummer. Het OIN-register is onderdeel van de Digikoppeling standaard en wordt beheerd door Logius. Dit register is voor dit peilmoment als primaire bron gebruikt om te bepalen of een organisatie gebruik maakt van Digikoppeling.

[1] In 2013 en 2014 is het aantal aansluitingen gedeeld op het aantal overheidsinstellingen. In 2015 en 2016 is aansluiting gezocht bij de rekenwijze van Logius waarbij alleen de overheidsorganisaties zijn betrokken waar uitwisseling via Digikoppeling aan de orde zou moeten zijn.

[2] In deze berekening in 2018 konden de overheidsorganisaties die zijn betrokken waar uitwisseling via Digikoppeling niet worden achterhaald. Als enkel naar de combinatie ZBO's, Uitvoeringsorganisaties en samenwerkingsverbanden wordt gekeken, dus zonder noodzakelijke betrekking op uitwisseling via Digikoppeling is dit percentage 36%

[3] Hierin zijn voor 2018 alleen de aantallen voor gemeenten, provincies en waterschappen opgenomen.

[4] Hoewel in 2021 het aantal OIN's is toegenomen in de groep Rijksoverheid + Uitvoeringsorganisaties, is de groep zelf ook gegroeid (met name de groep gemeenschappelijke regelingen) waardoor het percentage niet is veranderd.

Relevante ontwikkeling

De Digikoppeling standaard is een levende standaard en wordt continue doorontwikkeld Twee ontwikkelingen in het afgelopen jaar hebben een aanzienlijk impact op de standaard:

- Begin 2021 heeft het Technisch Overleg Digikoppeling een RESTful API-profiel aan Digikoppeling toegevoegd. Dankzij dit nieuwe profiel is het nu ook mogelijk om binnen het toepassingsgebied van Digikoppeling API's toe te passen conform de Restful API DesignRules (eveneens een 'pas toe of leg uit' -standaard).
- De Digikoppeling architectuur is aangepast. Enerzijds om het nieuwe RESTful API-profiel op te kunnen nemen in de Digikoppeling standaard. Anderzijds om de harde koppeling tussen het type bevraging en de specifieke Digikoppeling koppelvlakken los te laten. In de nieuwe architectuur worden verschillende transactiepatronen beschreven en wordt weergegeven hoe dit met de verschillende koppelvlakken kan worden ingevuld.

Zowel het RESTful API-profiel als de nieuwe architectuur liggen zomer 2021 ter toetsing bij Forum Standaardisatie en worden naar verwachting begin 2022 bestendigd door het OBDO.

Geo-Standaarden

Waarom belangrijk ?

Het geheel van Geo-standaarden is een van de drie stelselstandaarden op de pas-toe-of-leg-uit lijst. In Nederland zijn organisaties in verschillende domeinen betrokken bij het registreren en uitwisselen van informatie met een geografische component. Dat wil zeggen: informatie over objecten die gerelateerd zijn aan een locatie op het aardoppervlak. Voorbeelden hiervan zijn kadastrale informatie en informatie over waterhuishouding. Om ervoor te zorgen dat de geo-informatiehuishouding van deze domeinen op elkaar aansluit zodat informatie tussen domeinen uitgewisseld kan worden, zijn afspraken nodig over de te gebruiken standaarden. De Geo-standaarden voorzien hierin. Of, om met de woorden van de beheerorganisatie achter de Geo-standaarden (Geonovum) te spreken: de set Geo-standaarden maakt geo-informatie FAIR:

- Findable: Nederlandse metadataprofielen stellen gebruikers in staat om datasets en dataservices te vinden en vervolgens te beoordelen op geschiktheid voor gebruik (dankzij implementatie in het Nationaal Georegister);
- Accessible, dankzij de Nederlandse profielen op WMS en WFS;
- Interoperable, dankzij de semantische standaardisatie conform NEN3610;
- Re-usable doordat de belangrijkste basisgegevens in de geo-basisregistraties (BGT, BAG, BRT, BRO, BRK, WOZ) allemaal als open data beschikbaar gemaakt worden.

Als indicator voor het feitelijk gebruik van deze open standaarden kijken we in eerste instantie naar de gebruikscijfers van Publieke Dienstverlening Op de Kaart (PDOK), het platform voor het ontsluiten van geodatasets van Nederlandse overheden. Het beheer van PDOK is belegd bij het Kadaster. Dit zijn actuele en betrouwbare gegevens voor zowel de publieke als private sector. PDOK stelt digitale geo-informatie als dataservices en bestanden beschikbaar. De PDOK diensten zijn gebaseerd op open data en daarom voor iedereen vrij beschikbaar. De datasets zijn benaderbaar via geo-webservices, RESTful API's en beschikbaar als downloads en linked data. Deze voorziening vormt samen met de geobasisregistraties die via PDOK worden ontsloten, de kern van de Nederlandse geo-informatie infrastructuur. De set Geo-standaarden fungeert als ruggengraat van die infrastructuur.

Het aantal hits is de beste indicator van het gebruik van de standaarden aan de afnamekant, het aantal datasets (en daaraan gekoppeld het aantal services) dat ervoor kiest om ontsloten te worden via PDOK, als indicator voor het gebruik van de standaarden aan de aanbodzijde.

Feitelijk gebruik

In de laatste twee monitors stond al vermeld dat PDOK elk jaar aanzienlijke groeicijfers laat zien. De meest actuele beschikbare gegevens bevestigen dat beeld ook nu weer (bron: PDOK factsheet 2020). Voor verschillende variabelen ziet de ontwikkeling er als volgt uit:

- aan de afnamekant is er een groei van 14,4 miljard hits op PDOK over 2019 naar 30,9 miljard hits over 2020, een groei van 115%;
- aan de aanbodzijde is het aantal datasets gegroeid van 192 (2019) naar 218 in 2020, een groei van 14%;
- het aantal services is gestegen van 505 in 2019 naar 562 in 2020, ook een toename (+11%);
- het aantal hits op het Nationaal Georegister (NGR) kende daarentegen een afname: van 32,9 miljoen in 2019 naar 20,8 miljoen in 2020 (-37%);
- aantal instanties dat via PDOK geregistreerd staat als gebruiker: ruim 450 (gelijk aan 2019).

Het geheel overziend is wederom sprake van **substantiële groei van het gebruik;** de gebruikscijfers zijn ruimschoots verdubbeld in 2020. Mede door dit succes, maar ook door de verdere ontwikkeling van bijvoorbeeld de Basisregistratie Ondergrond, blijft er ook aan de aanbodzijde een duidelijke groei zichtbaar. Eigenlijk is alleen bij het gebruik van metadata een opvallende daling van het gebruik te zien. Voor deze daling van het gebruik van het NGR is niet met zekerheid een verklaring te geven. Zeker omdat het gebruik van data, die met het NGR gevonden zouden kunnen worden, enorm gestegen is, bestaat het vermoeden dat gebruikers data in toenemende mate vinden via zoekmachines waardoor het gebruik van metadatacatalogi terugloopt. Om op deze veranderende situatie in te spelen, wordt in de tweede helft van 2021 een onderzoek naar de toekomst van (geo) metadata uitgevoerd.

Het gaat eigenlijk op alle vlakken goed. Alleen op metadata-terrein valt op dat er nog partijen zijn (met name gemeenten) die al hun open data direct in data.overheid.nl registreren, terwijl zij de metadata van hun open geodata in het Nationaal Georegister zouden moeten registreren conform de Nederlandse metadataprofielen. Dit is deels het gevolg van een gebrek aan kennis bij gemeenten, maar deels ook van het optreden van enkele marktpartijen die ‘kant-en-klare’ open data portalen verkopen aan gemeenten en daarbij claimen dat die volledig voldoen aan de relevante standaarden. Aan de zijde van data.overheid.nl zouden de negatieve gevolgen voor gebruikers grotendeels ondervangen kunnen worden, wanneer er werk gemaakt gaat worden van een Nederlands profiel op DCAT 2.0.

Relevante ontwikkeling

Er wordt een verdere groei in het gebruik van de standaarden verwacht, omdat ruimtelijke data in steeds meer maatschappelijke opgaven een prominentere rol gaat spelen. Daarnaast zal op termijn de set Geostandaarden ook geactualiseerd worden, omdat er internationaal gewerkt wordt aan de op REST API’s gebaseerde opvolgers van o.a. WMS en WFS. Grote softwareleveranciers sorteren nu al voor op implementatie van die standaarden,

waarmee het in de toekomst nog eenvoudiger zal worden om de conform standaarden ontsloten data direct te gebruiken in werkprocessen.

StUF

Waarom belangrijk ?

De StUF-standaard is één van de drie stelselstandaarden van de 'pas toe of leg uit' lijst. Het betreft - een familie van samenhangende gegevens- en berichtenstandaarden, bedoeld voor de uitwisseling van administratieve overheidsgegevens. StUF richt zich op de standaardisatie van de inhoud van informatie, berichten en services. StUF is als open standaard vastgesteld voor uitwisseling van basisgegevens zoals Personen (GBA), Adressen (BRA), Gebouwen (BAG), Kadaster (BRK), Bedrijven (NHR) en Waarde Onroerende Zaken (WOZ), zaakgegevens van gemeenten en ketens waarin gemeenten participeren en waarvoor geen andere (inter)nationale (XML-gebaseerde) berichtenstandaard is vastgesteld. De standaard staat op de 'pas toe of leg uit' lijst sinds november 2008.

Het beheer van de StUF-standaard wordt uitgevoerd door meerdere overheidsorganisaties. VNG Realisatie beheert de overkoepelende delen van de familie. De StUF-standaarden worden breed ingezet en dat blijkt ook bij inzet in diverse ketens (GGK, Jeugdzorg, Omgevingswet, etc.). Juist in ketens waar gemeenten een rol spelen, zien we hergebruik van de uitgangspunten over de gegevensuitwisseling. Bij diverse ontwikkelingen in de digitale overheid zien we dit terug. Zo is ook het convenant samenwerking WOZ-ICT vanuit de waarderingskamer net vernieuwd.

Rondom deze familie van standaarden zijn de afgelopen jaren naast de doorontwikkeling van standaarden zelf veel uitbreidingen gerealiseerd in de processen, kaders en bijbehorende instrumenten, zoals:

- zwaardere inbedding van standaarden in architectuur en binnen grootschalige (landelijke) ontwikkelingen;
- leveranciersmanagement;
- instrumentarium voor preventief testen, model gedreven ontwikkeling;
- landelijke softwarecatalogus voor markttransparantie en applicatiemanagement;
- periodieke Monitoring over digitalisering en compliance van softwareproducten;
- uniforme inkoopvoorwaarden en contractgenerator;
- bestekteksten, opleidingen en communicatie, enz.

Feitelijk gebruik

Het gebruik van de StUF wordt voornamelijk uitgelezen via de applicaties. Dit is het aantal berichten dat heen en weer gaat tussen diverse systemen/applicaties. Het gaat daarbij om grote aantallen. Alleen al het GGK (Gemeentelijk Gegevens Knooppunt) verwerkt 10 miljoen berichten per jaar met een StUF envelop. Maar ook mutaties BAG, Kadaster, BRP en vele andere worden via StUF berichten uitgewisseld. Dit gaat dus over vele miljoenen berichten per jaar.

Uit de cijfers blijkt dat gemeenten, ketenpartners en hun leveranciers StUF breed gebruiken. Er is veel pakketsoftware op de markt of dit komt binnenkort op de markt. De adoptie neemt nog steeds toe. Onderstaande tabel geeft een beeld van de adoptie van twee StUF

onderdelen (StUF-BG en StUF-ZKN) door de ICT-markt. Op één uitzondering na is bij alle variabelen sprake van **een stijging ten opzichte van de meting van vorig jaar**.

	Totaal		StUF-BG		StUF-ZKN	
Aantal leveranciers	258	(231)	80	(74)	69	(62)
Aantal softwareproducten (incl. versies)	3413	(3229)	1291	(1211)	755	(713)
wv. beschikbaar/in gebruik	1551	(1530)	416	(402)	262	(241)
wv. gepland/in ontwikkeling	112	(122)	52	(47)	28	(25)

Peildatum juni 2021 (tussen haakjes de cijfers van de vorige monitor)
(bron VNG-Realisatie: www.softwarecatalogus.nl)

Uit het overzicht valt af te lezen dat het aantal leveranciers is gestegen (overall een stijging van 12%). Dit komt onder andere doordat het gebruik van de softwarecatalogus niet meer van een convenant afhankelijk is. Dit heeft voor een overall toename van pakketten gezorgd; het aantal softwarepakketten stijgt met 6%. Als aanvulling op de cijfers uit de tabel: het gebruik van de softwarecatalogus door gemeenten is gelijk aan het gebruik bij de vorige meting in 2020.

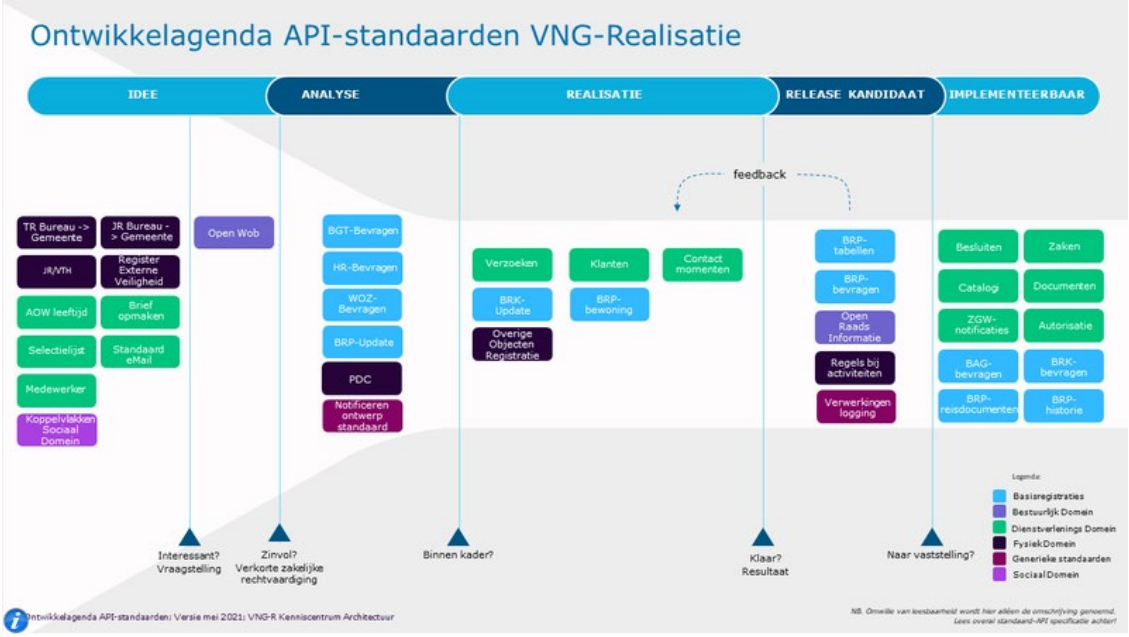
Er is sprake van enkele toetreders en er is ook sprake van een beweging van samenvoeging door samenwerking tussen partijen of overname van pakketten door een leveranciersgroep.

Er zijn geen grote wijzigingen doorgevoerd in STuF koppelvlakken. Trendmatig zien we deze periode een lichte vermindering van het aantal tests door leveranciers. Dit valt samen met de ontwikkeling richting het gebruik van API's voor het zaakgericht werken (zie hieronder bij relevante ontwikkeling).

Bij de beheerorganisatie zijn geen bijzonderheden bekend over specifieke organisaties die de standaarden wel zouden moeten gebruiken, maar deze niet gebruiken. Feitelijk gebruiken alle gemeenten StUF.

Relevante ontwikkeling

VNG Realisatie zet in het kader van Common Ground in op het gebruik van REST API standaarden. In verband daarmee worden er REST API standaarden ontwikkeld als alternatief voor de StUF standaarden. Ook wordt gestuurd op het vervangen van de StUF standaarden in het gemeentelijke IT landschap. Met name bij Zaakgericht Werken worden daar resultaten geboekt. Op de lange termijn zal dit in ieder geval leiden tot een afname van het gebruik van de StUF standaard en zo mogelijk zelf tot het verdwijnen van de StUF standaarden.



Bron: https://www.gemmaonline.nl/index.php/Ontwikkelagenda_API-standaarden

Deze transitie is een doorlopend proces en de verwachting is dat de StUF standaarden voorlopig nog wel in gebruik zullen blijven.

B5.6. Domein Water en bodem

Aquo-standaard

Waarom belangrijk ?

De Aquo-standaard is één van de drie stelselstandaarden op de 'pas toe of leg uit' lijst. De standaard maakt het mogelijk om op een uniforme manier gegevens uit te wisselen tussen partijen die betrokken zijn bij het waterbeheer. Daardoor draagt Aquo bij aan een kwaliteitsverbetering van het waterbeheer. Aquo is bedoeld voor iedereen die te maken heeft met het vastleggen en gebruiken van gegevens; zowel op zee als binnendijks, in beekdalen en polders, bij grond- en afvalwater, voor waterkwaliteit, -kwantiteit, -systeem en –veiligheid. De Aquo-standaard wordt beheerd door het Informatiehuis Water (IHW).

De standaard staat op de 'pas toe of leg uit' lijst sinds 17 mei 2016.

Feitelijk gebruik

Het gebruik van de Aquo-standaard binnen het waterbeheer is groot. Zo hebben de waterbeheerders (waterschappen, de provincies en Rijkswaterstaat) jaarlijks de verplichting om aan bij het ministerie van Infrastructuur & Waterstaat te rapporteren over de waterkwaliteit en waterveiligheid. Hiervoor zijn verschillende informatiestromen ingericht die het Informatiehuis Water (IHW) organiseert en faciliteert. Door daarbij gebruik te maken van de Aquo-standaard is sprake van uniforme en efficiënte gegevensuitwisseling. De volgende informatie over het gebruik van de Aquo standaard is afkomstig uit het jaarverslag 2020 van het IHW:

- Aquo-Domeintabellen Service (raadplegen): ca. 5.000.000 keer
- IM Metingen (uitwisselen): ca. 10.000.000 keer
- Aquo-kit webservice: meer dan 480.000 keer
- Binnen Z-info: ca. 1.000.000 keer
- In de Centrale Distributielaag van het Waterschapshuis ca. 40.000 keer

Voor de meeste onderdelen geldt dat het gebruik in 2020 **ongeveer hetzelfde** is als in 2019.

Gebruikers van de Aquo-standaard zijn ook middels het indienen van wijzigingsverzoeken en het melden van incidenten (gestelde vragen) betrokken bij de ontwikkeling van de standaard. Een deel van de door IHW verstrekte gegevens over het gebruik van de Aquo-standaard haakt hierop in:

- Instroom op de Aquo-standaard:
  - aantal ingediende wijzigingsvoorstellen: 132 (vorig jaar: 124)
  - gemelde incidenten: 117 (vorig jaar: 89). Deze stijging heeft te maken met de toegankelijkheid van Aquo-sharepoint 2020.
- aantal waterbeheerders dat een wijzigingsaanvraag indient / een incident meldt:
  - betrokken instanties bij wijzigingsaanvragen: 27 (vorig jaar: 31)
  - betrokken instanties bij melden incident: 44 (vorig jaar: 41)

GWSW

Waarom belangrijk ?

In het beheer van stedelijk water en riolering worden gegevens steeds belangrijker. Er zijn meerdere ketenpartners betrokken bij dit beheer: gemeenten, waterschappen en ingenieurs-bureaus. Het doelmatig managen van (afval)watersystemen vereist een gemeenschappelijke taal. Ook maatschappelijke opgaven zoals klimaatadaptatie, energietransitie en de bouwopgave vereisen een (digitale) integrale aanpak, waarbij gezamenlijke definities van gegevens een voorwaarde zijn. Het Gegevenswoordenboek Stedelijk Water (GWSW) voorziet hierin. Het is een ontologie, een speciale datastructuur die systemen en processen op het gebied van stedelijk waterbeheer beschrijft. De GWSW-ontologie draagt bij aan het uniform vastleggen, uitwisselen en hergebruiken van gegevens in het stedelijke waterbeheer.

De standaard staat op de ‘pas toe of leg uit’ lijst sinds 23 maart 2020.

Feitelijk gebruik

Eind 2020 hebben inmiddels 120 gemeenten rioleringsdatasets op het landelijke dataplatform met rioleringsdatasets geplaats. Een jaar daarvoor, eind 2019, waren dat nog 40 gemeenten. Deze groei is toe te schrijven aan het volgende:

- in 2020 zijn meer beheerapplicaties het GWSW gaan ondersteunen waardoor gemeenten in staat zijn het GWSW zelf toe te passen;
- andere (software-)toepassingen gaan GWSW-conforme rioleringsdata benutten waardoor gemeenten gemotiveerd raken het GWSW zelf ook te gaan toepassen;
- toenemende regionale samenwerking is voor gemeenten en waterschappen een prikkel om het GWSW te gebruiken als basis voor hun beheer en daarbij benodigde data(uitwisseling).

Verder mag in het kader van het realiseren van de randvoorwaarden voor het gebruik van GWSW het volgende niet onvermeld blijven:

- alle bestekken voor rioolreiniging en –inspectie schrijven het RibX uitwisselformaat voor;
- en voor wat betreft de applicatietoets: de helft van de rioleringsbeheerpakketten, alle inspectiesoftware en alle modelleringssoftware kunnen de voorgeschreven GWSW-formaten uitwisselen.

Relevante ontwikkeling

Het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) heeft op 12 mei 2021 op voorspraak van Forum Standaardisatie een aantal mutaties op de officiële lijsten met open standaarden bekrachtigd. GWSW versie 1.4 is daarmee op de 'Pas toe of leg uit'-lijst vervangen door versie 1.5.1. Overheden zijn verplicht bij alle relevante software-aanbestedingen de GWSW-standaard inclusief gespecificeerde uitwisselformaten OroX, HydX en RibX te eisen. Met deze wijziging is de standaard functioneel rijker geworden door de nieuwe toevoegingen. Met name de toevoeging van module GWSW-HYD ten behoeve van hydraulische modellering en de ontsluiting rioleringsdata naar Publieke Dienstverlening op Kaart (PDOK) leiden tot meer gebruiksmogelijkheden voor gemeenten, waterschappen en adviesbureaus.

Voor gemeenten is het nog niet vanzelfsprekend dat de vigerende GWSW-standaard en uitwisselformaten als eis gelden voor hun integraal softwarepakket voor beheer van (objecten in) de openbare ruimte. Hoewel het draagvlak bij functioneel beheerders afgelopen twee jaar wel sterk gegroeid is, is dat bij inkoopafdelingen, management en bestuur nog verre van vanzelfsprekend. Omdat implementatie van het GWSW op termijn wel zal leiden tot aanpassingen in werkprocessen, benodigde competenties en inrichting van ICT-systemen, is ook daar wel draagvlak nodig. De PTOLU-status zal daar naar verwachting aan bijdragen.

SIKB0101 en SIKB0102

Waarom belangrijk ?

SIKB0101 is een standaard voor de uitwisseling van bodemkwaliteitsgegevens, inclusief geografische en administratieve gegevens. Op basis daarvan kan worden vastgesteld of sprake is van schadelijke gevolgen voor de volksgezondheid en het milieu ten gevolge van bodemvervuiling. Deze inzichten dragen ook bij aan het voorkomen van dergelijke schadelijke effecten. Zo wordt een bijdrage geleverd aan de bescherming van de volksgezondheid en het milieu. Belangrijke gebruikers binnen de overheid zijn Rijkswaterstaat, omgevingsdiensten en gemeenten. SIKB 0101 staat op de 'pas toe of leg uit' lijst sinds juni 2012.

SIKB0102 voorziet in de optimalisering van de digitale uitwisseling van archeologische gegevens tussen opgravende instanties, vondstendepots en/of archeologische registers.

Een opgravende instantie, overheidsorganisatie of een bedrijf dat archeologisch onderzoek en/of vondsten doet heeft namelijk een wettelijke plicht om binnen twee jaar na afronding van de opgraving de verzamelde informatie beschikbaar te stellen aan daartoe ingestelde depots binnen de overheid (landelijk, provinciaal, en op gemeentelijk niveau). SIKB0102 staat op de 'pas toe of leg uit' lijst sinds februari 2016.

Feitelijk gebruik

SIKB0101 en SIKB0102 zijn breed geïmplementeerde standaarden binnen de domeinen Bodem en Archeologie. Jaarlijks worden miljoenen data uitgewisseld via SIKB0101 tussen applicaties die deze standaarden hebben geïmplementeerd. Via SIKB0102 is sprake van uitwisseling van duizenden data; dit betreft een veel kleinere markt dan die van SIKB0101.

Voor beide standaarden geldt dat het **gebruik is toegenomen**. Voor wat betreft SIKB0101 is dit vooral toe te schrijven aan een breder gebruik, bij SIKB0102 is vooral sprake van toename in de keten bij opgravende bedrijven. De beheerorganisatie achter de standaarden, SIKB, ziet dit aan de toename van het aantal softwareleveranciers en -ontwikkelaars die een deelnameovereenkomst hebben met SIKB voor het gebruik van SIKB0102 (en ondersteuning). Ook wordt een toenemend gebruik van de validatietool waargenomen. Dit geldt zowel voor marktpartijen (opgravende bedrijven) als depots.

Specifiek met betrekking tot *SIKB0101* is de praktijk dat alle gemeenten, omgevingsdiensten en provincies werken met software die gebruik maakt van de datastandaard SIKB0101. Dit blijkt uit de overeenkomsten die SIKB heeft met de leveranciers van software die SIKB0101 gebruiken. Deze leveranciers zijn lid van de Technische Werkgroep die de wijzigingsverzoeken behandelt voor SIKB0101. Softwareleveranciers als ook de eindgebruikers van data zijn in het Centraal College van Deskundigen (CCvD) Datastandaarden vertegenwoordigd, waar besluitvorming plaatsvindt over de doorontwikkeling van de standaard. Daarnaast zijn de koepelorganisaties van de gemeenten (VNG), de provincies (IPO) en de waterschappen (UvW) ondertekenaar van het Convenant bodem en ondergrond 2016-2020. Hierin wordt expliciet de standaard genoemd als uitwisselstandaard voor (digitale) bodeminformatie.

De volgende partijen gebruiken de datastandaard *SIKB0102* in hun software en stellen het gebruik ervan verplicht:

- landelijk registratiesysteem ARCHIS van de Rijksdienst voor het Culturele Erfgoed (RCE);
- Data Archiving and Networking Services (DANS). Het E-depot voor de duurzame opslag van digitale data;
- BIJ12, beheerder van het provinciaal depot beheer system (Archeodepot). Archeodepot wordt inmiddels door 11 van de 12 provincies gebruikt.

Relevante ontwikkeling

De drinkwatersector (publiek/privaat) is sinds 2019 gestart met de implementatie van SIKB0101. In nauw overleg met Geonovum worden gesprekken gevoerd over harmonisatie van de standaarden van de Basisregistratie Ondergrond (BRO) met SIKB0101. Bij de voorziene uitbreiding van de BRO met data over de milieuhygiënische kwaliteit van de bodem zal SIKB0101 als uitgangspunt dienen (voorzien vanaf 2022). De groeipotentie voor wat betreft het aantal gebruikers uit de overheidssector is overigens niet (meer) zo groot bij SIKB0101.

Voor de komende jaren zal Archeodepot ook open worden gesteld voor de ongeveer 40 gemeentelijke depots waarmee de standaard SIKB0102 ook binnen de gemeenten een steeds belangrijkere rol gaat spelen. Een aantal pilots bij vier gemeenten is voor 2021 in voorbereiding. Met name bij gemeenten valt dan ook nog winst te behalen voor wat betreft het gebruik, maar ook bij provincies die nu pas starten met digitale uitwisseling.

B5.7. Domein Bouw

COINS

Waarom belangrijk ?

In de ontwerp-, realisatie-, en onderhoudsfases van bouwprojecten wisselen opdrachtgevers en opdrachtnemers heel diverse informatie uit, die wel met elkaar verbonden is. De uitwisseling van deze informatie gaat vaak moeizaam omdat partijen verschillende software gebruiken waardoor de informatie niet uitwisselbaar of leesbaar is. COINS maakt het mogelijk om data over objecten, opgeslagen in verschillende digitale formaten die voldoen aan verschillende standaarden, in onderlinge samenhang en systeemonafhankelijk uit te wisselen. Dankzij COINS kunnen opdrachtgevers en opdrachtnemers die software van verschillende leveranciers gebruiken gemakkelijker samenwerken.

COINS 2.0 bestaat uit twee onderdelen:

- een 'container' waarin je bestanden of datasets aan elkaar linkt, zodat je de gegevens kan uitwisselen;
- een datamodel voor de gegevens in een dataset.

Inmiddels zijn de twee onderdelen van COINS 2.0 doorontwikkeld op internationaal niveau.

- *de 'container'*: ICDD, Information container for linked document delivery, is de internationale opvolger van de 'container'. In deze internationale variant kunnen ook standaarden, kennis en ervaringen van experts uit andere landen verwerkt worden;
- *het Datamodel*: het combineren van verschillende datamodellen, bijvoorbeeld COINS 2.0 met een eigen Objecttypebibliotheek, is lastig als die datamodellen gebaseerd zijn op andere uitgangspunten. Daarom hebben Nederlandse experts onder de vlag van NEN samengewerkt aan de NTA 8035. Dit is de opvolger van het datamodel.

Toch gebruiken sommige organisaties nog COINS 2.0. Dit is bijvoorbeeld het geval wanneer een organisatie software heeft ingericht en een Objecttypebibliotheek heeft gemodelleerd met COINS 2.0 als basis. COINS staat op de 'pas toe of leg uit' lijst sinds mei 2018.

Feitelijk gebruik

COINS 2.0 is in gebruik in lopende projecten van de provincie Gelderland. Het aantal lopende projecten is **iets groter** dan in 2020, omdat de provincie **BIM meer aan het uitrollen** is. Rijkswaterstaat gebruikt COINS nog voor een enkel project. Ten aanzien van het gedachtengoed zelf zijn er wel initiatieven/pilots om een opvolger te implementeren.

Relevante ontwikkeling

Momenteel wordt gewerkt aan implementatieondersteuning voor ICDD en NTA8035. De verwachting is dat dit zal leiden tot meer gebruik, omdat deze standaarden makkelijker te implementeren zijn dan COINS.

IFC

Waarom belangrijk ?

IFC is een standaard voor zowel semantische afspraken als voor dataformats en richt zich specifiek op BIM-informatie over bouwwerken. De standaard maakt het mogelijk om een driedimensionaal geometrisch model van een bouwwerk digitaal vast te leggen, inclusief de gegevens van de daarin ondergebrachte elementen en hun onderlinge relaties. Deze beschrijving kan vervolgens in IFC formaat uitgewisseld worden tussen partijen die betrokken zijn bij de ontwikkeling, vergunningverlening, beheer en onderhoud van een gebouw. Zo verloopt de informatie-uitwisseling tussen overheden onderling en tussen overheden en vergunning-aanvragers of bouwondernemers efficiënter. Dit is bijvoorbeeld nuttig bij het verlenen van bouwvergunningen en bij de ontwikkeling en het ontwerpen van gebouwen. De IFC-standaard staat op de 'pas-toe-of-leg-uit'-lijst sinds november 2011.

Feitelijk gebruik

Er zijn lang geen gegevens geweest over het feitelijk gebruik van de IFC-standaard bij overheden. Daarin is onlangs verandering gekomen met het verschijnen in juni dit jaar van een 1e Nationale BIM monitor. Deze rapportage kan als een 0-meting worden beschouwd. De BIM monitor is gebaseerd op een enquête onder de belangrijkste deelsectoren uit de Nederlandse bouwkolom, waaronder ook de opdrachtgevers. Onder de 577 respondenten bevinden zich 76 overheidsorganisaties, alle in de rol van opdrachtgever. Uit de monitor kunnen enkele uitspraken worden gedestilleerd over de categorie van 150 opdrachtgevers; over de subcategorie 'overheden' daarbinnen is niet afzonderlijk gerapporteerd.

Over de categorie opdrachtgevers kan in relatie tot IFC het volgende worden vastgesteld:

- bekendheid met IFC: 22 %
- gebruik van IFC: 6 %

Bij een volgende meting zal moeten blijken hoe een en ander zich ontwikkelt. Vooralsnog is sprake van lage scores op kennis en gebruik van deze standaard bij de genoemde deelsector. Dit beeld sluit aan bij de opbrengst van het in augustus jl. verschenen Evaluatierapport Bouwstandaarden, uitgevoerd in opdracht van Bureau Forum Standaardisatie. Enkele conclusies uit die evaluatie luiden als volgt:

- het aantal IFC-experts werkzaam bij de overheid is erg beperkt;
- experts geven unaniem aan dat IFC op de 'Pas toe of leg uit'-lijst hoort, ondanks de beperkte kennis en toepassing binnen overheidspartijen;
- de bekendheid van IFC binnen de overheid is nog beperkt; hier is nog veel werk te verzetten.

Relevante ontwikkeling

In de eerdergenoemde evaluatie van bouwstandaarden zijn de volgende twee relevante ontwikkelingen opgetekend:

- de verbreding van de standaard naar infra en spoor, in combinatie met de kracht van 3D, mede in lijn met de ontwikkelingen binnen de Omgevingswet, maakt het belang van een open standaard als IFC voor de overheid groot;
- de aan IFC gerelateerde 3D modellering biedt extra mogelijkheden in de vergunningverlening en handhaving hiervan. 2D is echter nog steeds het meest gebruikt binnen de overheid.

Beide ontwikkelingen onderstrepen het belang om de groeipotentie van het gebruik van deze standaard binnen de overheid te stimuleren.

NLCS

Waarom belangrijk ?

Organisaties hanteren vaak een eigen tekenstandaard voor digitale tekeningen. Hiermee geeft een organisatie een eigen signatuur af. Maar het belemmert ook de uitwisseling en het hergebruik van tekeningen waardoor tekeningen vaak opnieuw moeten worden getekend. NLCS zorgt voor meer eenheid in het tekenwerk. NLCS is een tekenstandaard voor het maken van 2D-ontwerptekening en gaat uit van objectgericht werken. Alle informatie in een tekening wordt gekoppeld aan objecten die in lagen worden geordend in een tekening. Gebruikers kunnen hiervoor een standaard objectenbibliotheek gebruiken die met NLCS wordt meegeleverd. NLCS staat op de 'pas toe of leg uit' lijst sinds mei 2018.

Feitelijk gebruik

Het feitelijk gebruik door overheidsorganisaties ziet er als volgt uit.

Type overheid	Aantal gebruikers CAD Software met NLCS in 2019	Aantal gebruikers CAD Software met NLCS in 2020
Gemeenten	140	138
Waterschappen	8	15
Provincies	12	10
Rijksoverheid	2	5
Netbeheerders	niet gemeten	5
Kennisinstellingen	niet gemeten	6
Totaal	162	179

Van de 179 gebruikers leveren er 55 ook een bijdrage aan de ontwikkeling van de standaard. Een vergelijking met de uitkomst van de vorige monitor (2020) is nog niet goed mogelijk. Een voorzichtige conclusie is dat per saldo sprake lijkt van een geringe toename van het gebruik.

Over de groeipotentie van het gebruik van NLCS het volgende. Zeker in de gemeentelijke markt beschikken niet alle organisaties over een civieltechnische afdeling en/of medewerkers met vakinhoudelijke kennis. Deze gemeenten laten zich voor de ontwerpwerkzaamheden conform NLCS volledig ontzorgen door marktpartijen (opdrachtnemers). Deze gemeenten voldoen dus indirect wel aan de 'pas toe of leg uit' norm, maar zullen niet beschikken over eigen software oplossingen. Verder is het gebruik van de standaard bij beheerders van ondergrondse infrastructuur nog een stuk lager dan zou kunnen. Diverse organisaties gebruiken nog eigen laagindelingen. Dat is wel aan het veranderen en zal nog een stuk sneller gaan wanneer NLCS geschikt wordt gemaakt voor deze sector.

Relevante ontwikkeling

Voor de toekomst wordt er gekeken naar aansluiting tussen de NLCS en informatiemodellen.

Op dit moment kent de NLCS een eigen decompositie en naamgeving van objecten, en hun kenmerken. De naamgeving, kenmerken en bijbehorende definities worden domein specifiek vastgelegd in informatiemodellen als o.a. IMBOR, IMKL en het GWSW. De huidige versie van de NLCS sluit hier nog niet 100 procent op aan. De eerste stap is om de NLCS objecten af te stemmen op de vigerende informatie standaarden. Onderzocht wordt de mogelijkheid om met de CAD-applicatie de objecten te definiëren vanuit het datamodel (OTL) inclusief de kenmerken (attributen) en deze vervolgens middels tooling als NLCS objecten te tekenen. Het doel is om aanvullende kenmerken als data aan de NLCS-objecten te koppelen, zodat hier vervolgens een dataset uit gegenereerd kan worden volgens o.a. de GWSW-methodiek.

Naast de koppeling met de verschillende informatiemodellen wordt een grote kans gezien voor een koppeling tussen NLCS en de RAW-systematiek. Al 15 jaar doet de markt pogingen om CAD- en RAW-programma's met elkaar te verbinden. Eerder bleek dit niet opportuun, onder andere door het ontbreken van een standaard voor CAD-tekeningen en een sterk verzuilde bedrijfscultuur. Inmiddels zijn de benodigde standaarden beschikbaar en groeit het besef dat je met digitalisering de werkzaamheden efficiënter uit kunt voeren. Zaak is de verzuiling in de branche te doorbreken, door standaarden in samenhang te zetten. Met als uiteindelijk doel integrale digitale samenwerking tussen tekenaars, bestekschrijvers, calculators en beheerders.

Dat er nog geen samenhangend geheel is, is een gemiste kans als je bedenkt dat circa 80 procent van de werkzaamheden in de buitenruimte tot stand komt op basis van NLCS-tekeningen en een RAW-contract. Met de huidige werkmethode is het doorvoeren van wijzigingen in het ontwerp een arbeidsintensieve, handmatige en foutgevoelige exercitie. En dat lijdt uiteindelijk weer tot discussies over meer- en minderwerk door tegenstrijdigheden tussen tekeningen en het contract.

VISI

Waarom belangrijk ?

VISI is een open standaard, die zich richt op digitale communicatie tussen partijen in een bouwproject. Met behulp van VISI wordt bepaald wanneer (proces), wie (rol), wat (informatie), aan wie (rol) aanlevert. Hierbij kan gedacht worden aan het geven van opdrachten, het aanleveren van tijdschema's, het opleveren van resultaten en het melden van afwijkingen. Het doel van VISI is om de transparantie en traceerbaarheid van het bouwproces te vergroten en hiermee de kwaliteit en efficiency te verhogen en de doorlooptijd te verkorten. Visi staat op de pas-toe-of-leg-uit-lijst sinds 9 december 2014.

Feitelijk gebruik

De standaard wordt toegepast door een drietal software-leveranciers. Met betrekking tot het gebruik vanuit de overheidshoek zijn de volgende gegevens aangeleverd vanuit de beheerorganisatie (BIM-loket):

- overheidsorganisaties: 129 (118)
- individuele gebruikers bij overheden 12.839 (11.480)
- overheidsprojecten 7.774 (5.747)

(Peildatum: zomer 2021. Tussen haakjes staan de gegevens uit de monitor van vorig jaar.)

De beheerorganisatie geeft aan dat sprake is van een **lichte toename van het gebruik**. Op elk van de drie variabelen in bovenstaand overzichtje is sprake van een stijging.

De impact van covid-19 is merkbaar op nieuwe initiatieven binnen overheden ten aanzien van het starten met de open standaard VISI. Het aantal overheidsorganisaties, dat het afgelopen jaar gestart is met VISI, is beperkt. Tweede trend is dat veel gebruikers van VISI het afgelopen jaar veel meer gebruikgemaakt hebben van VISI als digitaal projectcommunicatie platform. Als gevolg daarvan is het aantal organisaties uit de categorie aannemers en ingenieursbureaus - die gebruik gemaakt hebben van VISI - in het afgelopen jaar gestegen.

Relevante ontwikkeling

Er is nog veel potentie voor kleine en middelgrote gemeenten om VISI te gaan gebruiken. Veel gehoorde argumenten om niet het werkproces te digitaliseren zijn de grootte van de gemeente en de grootte van de projecten.

VISI is in 2020 geëvalueerd door het bureau forum standaardisatie. Komende tijd werkt de beheerorganisatie hard aan de verbeterpunten.

B5.8. Domein Juridische identificatie en verwijzing

BWB, ECLI en JCDR

Waarom belangrijk ?

BWB

BWB, de Juriconnect-standaard voor identificatie van en verwijzing naar wet- en regelgeving, staat op de 'pas toe of leg uit'-lijst sinds 2 februari 2016. Deze standaard wordt ook wel "logische links naar wetgeving" genoemd. De standaard is een URI, een Uniform Resource Identifier, een unieke computer-leesbare identificatiecode voor een ding, een stuk informatie of data. In dit geval dus voor wet- en regelgeving. De standaard BWB is vernoemd naar het Basiswettenbestand en wordt o.a. toegepast in de website wetten.overheid.nl. Conform de wettelijke opdracht bevat wetten.overheid.nl de geldende, geconsolideerde, regelgeving van de Nederlandse Rijksoverheid.

BWB en relevante ontwikkeling

De BWB standaard heeft tekortkomingen waarvoor mogelijke oplossingsrichtingen worden onderzocht. Daarbij wordt ook gekeken naar de STOP-standaard (Standaard Officiële Publicaties) die in het kader van het Digitaal Stelsel Omgevingswet is ontwikkeld. STOP is gebaseerd op de Akoma Ntoso-standaard van OASIS. Ook wordt gekeken naar mogelijke implementatie van de European Legislation Identifier (ELI). Op korte termijn wordt echter geen uitfasering verwacht van de BWB standaard. Hiervan werd ook al melding gemaakt in de Monitor Open Standaarden 2020.

JCDR

JCDR is de Juriconnect standaard voor identificatie van en verwijzing naar decentrale regelgeving en staat op de 'pas toe of leg uit'- lijst sinds 28 november 2013. De JCDR

standaard, eveneens een URI , werd aanvankelijk ontwikkeld binnen de Centrale Voorziening voor Decentrale Regelgeving (CVDR), in 2018 overgegaan in DROP, de voorziening voor Decentrale Regelgeving en Officiële Publicaties. In DROP kunnen decentrale overheidsorganisaties zorgen voor consolidatie en publicatie van hun regelgeving.

JCDR en relevante ontwikkeling

Waarschijnlijk zal een nieuwe, in het kader van BWB te ontwikkelen standaard ook toepasbaar zijn op identificatie van en verwijzing naar decentrale regelgeving.

ECLI

ECLI is de Europese standaard voor de identificatie van rechterlijke uitspraken en verwijzing daarnaar, op de 'pas toe of leg uit'- lijst sinds 28 november 2013. In Nederland wordt de ECLI toegepast in de publicatie van alle uitspraken van alle (tucht)rechterlijke instanties. Alle rechterlijke uitspraken zijn met ECLI te vinden op Rechtspraak.nl. De tuchtrechtelijke uitspraken staan op Tuchtrecht.nl. Ook uitspraken die door uitgevers of alleen rechtspraak-intern zijn gepubliceerd hebben een ECLI. Gebruikers van ECLI zijn rechters in vonnissen en arresten, rechtsgeleerden en ambtenaren, maar ook juridische studenten, journalisten en burgers. Ook in de rest van Europa is ECLI de leidende standaard voor het identificeren en citeren van rechterlijke uitspraken. In juli 2021 waren dat 18 EU lidstaten en drie Europese gerechten. Het gebruik van ECLI wordt voorgeschreven in de Aanwijzingen voor de regelgeving en de Leidraad voor juridische auteurs. Het is door brede dekking inmiddels de leidende standaard.

ECLI en relevante ontwikkeling

Een nieuwe versie van de standaard is in oktober 2019 gepubliceerd in het Publicatieblad van de Europese Unie. Deze nieuwe versie bevat vooral uitbreidingen; de functionaliteit van de oorspronkelijke standaard blijft ongewijzigd. De nieuwe versie wordt niet nog gebruikt; dit is mede afhankelijk van nog te maken implementatiekeuzes op Europees en nationaal niveau.

Feitelijk gebruik

In LiDO, linkeddata.overheid.nl komt de toepassing van alle drie de juridische standaarden samen. LiDO is een databank met miljoenen hyperlinks, waarmee iemand snel inzicht kan krijgen in de verbanden tussen nationale en Europese regelgeving, uitspraken van Nederlandse en Europese rechters, parlementaire documenten en officiële bekendmakingen. De bezoekers zijn (her)gebruikers van juridische overheidsdata. Hierbij gaat het om overheid (centraal en decentraal), uitgevers van juridische informatie, content integrators, uitvoeringsorganisaties, studenten en rechtswetenschappers van universiteiten en hogescholen.

Het gebruik van LiDO wordt sinds de Monitor Open standaarden 2018 aangemerkt als een graadmeter voor het gebruik van de standaarden BWB, JCDR en ECLI samen. Het gebruik ligt op ongeveer 540.000 bezoeken en 1.400.000 page-views per maand (peilmoment: 1 januari 2021). Deze cijfers liggen beduidend hoger dan de opgave tijdens de vorige monitor met toen als peildatum juni 2020.

Mede op grond van het toenemend gebruik van LiDO wordt vanuit de beheerorganisatie net als in 2020 de inschatting gemaakt dat het gebruik van de standaarden **geleidelijk**

toeneemt, zowel vanuit de publieke als vanuit de private sector. Zo maken veel juridische uitgevers en legal-tech-bedrijven (vaak start-ups) gebruik van deze standaarden. Als verklaring voor deze stijging wordt vanuit de beheerorganisatie aangegeven dat dat een gevolg is van een groeiend besef van de noodzaak tot het gebruik van de standaarden en van de voordelen ervan. Deze voordelen zitten onder meer in de mogelijkheden om informatie te koppelen met andere gegevensbronnen en om de eigen gegevensverzamelingen beter beheersbaar en doorzoekbaar te maken, zoals LiDO bijvoorbeeld ook laat zien.

Meer specifiek met betrekking de drie onderliggende standaarden kan tot slot het volgende worden opgemerkt:

- ECLI wordt zeer goed gebruikt. Dit is mede een gevolg van het feit dat deze standaard wordt gebruikt in de uitspraken-databank van de Rechtspraak en door het Hof van Justitie van de EU;
- gebruik van de beide andere standaarden -BWB en JCDR- is vaak onzichtbaar en daardoor moeilijk meer precies te duiden.

B5.9. Domein Onderwijs en loopbaan

E-Portfolio NL NEN 2035

Waarom belangrijk ?

Door de invoering van competentiegericht leren en toenemende interesse in het gebruik van e-portfolio's is het van belang een afspraak te hebben voor het uitwisselen van e-portfoliogegevens. Met E-portfolio NL kunnen de competenties van een individu worden bijgehouden. Het voordeel van deze standaard is dat de student/lerende medewerker zijn profiel mee kan nemen naar verschillende organisaties. E-portfolio NL (beheerorganisatie: NEN) is een toepassingsprofiel voor studenten en werknemers bij Nederlandse organisaties, van de internationale IMS ePortfolio specificatie. De standaard staat op de ‘pas toe of leg uit’ lijst sinds mei 2010.

Feitelijk gebruik

Volgens de gegevens van NEN is de standaard in 2020 4 keer aangeschaft en 12 keer ingezien via NEN Connect (het licentiesysteem van NEN). In hoeverre het hier om publieke organisaties gaat is niet bekend. Deze cijfers liggen lager dan vorig jaar. Deze cijfers zeggen echter nog niet alles over het daadwerkelijke gebruik.

Hoeveel organisaties de standaard daadwerkelijk gebruiken is moeilijk in te schatten. Met name bij het inzien via NEN Connect is namelijk niet na te gaan of dit alleen informatief is, of dat de standaard daadwerkelijk wordt gebruikt. Daarnaast geldt dat, als organisaties de standaard al in bezit hebben, niet inzichtelijk is of deze nogmaals is toegepast.

Het volgende biedt wel enig houvast. In 2020 zijn gesprekken gevoerd met 30 stakeholders die in eerdere jaren de norm hebben aangeschaft. De meerderheid van hen geeft aan de norm niet meer te gebruiken. Een beperkt aantal stakeholders (20%) geeft aan de norm nog

wel te gebruiken binnen de eigen organisatie. Geen van de stakeholders heeft aangegeven NEN 2035 te gebruiken in aanbestedingen of contracten.

Dergelijke gesprekken met stakeholders zijn gevoerd omdat NEN 2035 inmiddels 6 jaar bestaat, en NEN na 5 jaar gewoonlijk inventariseert of er behoefte is aan een herziening van de norm. De stakeholders gaven aan de norm ofwel niet meer te gebruiken (een meerderheid), ofwel te gebruiken in de huidige vorm en geen behoefte aan een herziening te hebben.

Relevante ontwikkeling

In 2020 is een herziene versie van de internationale norm ISO/IEC 20013 gepubliceerd. Deze norm heeft dezelfde scope als NEN 2035. Onderzocht is of ISO/IEC 20013 en NEN 2035 tegenstrijdigheden bevatten. Dat is niet het geval. Daar waar de normen overlappen (wat slechts in kleine delen het geval is), schrijven zij dezelfde werkwijze en toepassing voor. ISO/IEC 20013 is in 2020 in totaal 26 keer verkocht of geraadpleegd.

Stakeholders geven in de eerder gememoreerde inventarisatie-ronde aan dat, als er een internationale norm is die vergelijkbaar is met de nationale norm, het de voorkeur heeft de internationale norm te gebruiken. De uitkomst is in dit stadium nog ongewis.

NL LOM

Waarom belangrijk ?

Door het metadateren van onderwijsmateriaal is zowel het eigen materiaal als het materiaal van anderen (beter) terug te vinden en op verschillende plekken beschikbaar. Dit bevordert de herbruikbaarheid van onderwijsmateriaal. In NL LOM staat beschreven welke metadata toegekend moeten worden aan educatieve content om de vindbaarheid en vergelijkbaarheid van leermateriaal te vergroten. Metadata beschrijven in dit geval de kenmerken van leerobjecten. Te denken valt aan auteursgegevens, titel, uitgever, taal, en dergelijke. NL LOM is een Nederlands toepassingsprofiel van de internationale standaard IEEE-LOM. Deze standaard staat op de pas-toe-of-leg-uit-lijst sinds 29 mei 2011.

Feitelijk gebruik

NL-LOM wordt gebruikt door verschillende organisaties in de onderwijs- en publieke sector. Over de mate van het gebruik is voor deze monitor kwantitatieve noch kwalitatieve informatie aangeleverd. Uitspraken over een ontwikkeling van het gebruik zijn dan ook niet mogelijk.

Relevante ontwikkeling

Met Edusources kunnen docenten en studenten gemakkelijk digitale leermiddelen vinden en hergebruiken voor hun onderwijs of studie. Edusources breidt in de toekomst uit. Onderdeel daarvan is koppeling van opslagsystemen en ‘harvesting’ van metadata, idealiter gebruikmakend van NL-LOM standaard. Ook wordt samengewerkt Bureau Edustandaard aan de doorontwikkeling van de standaard, onder andere door de ontwikkeling van vak vocabulaires voor het hoger onderwijs.

Bureau Edustandaard geeft aan dat de standaard in het onderwijsveld goed geadopteerd is en dat daarmee het werkingsgebied is verzadigd. SURF, de ICT-coöperatie van onderwijs en

onderzoek, heeft de ambitie uitgesproken het werkingsgebied uit te willen breiden naar onder andere de culturele sector, bijvoorbeeld bij het Rijksmuseum. Daarnaast is de ambitie uitgesproken door SURF om overheidsbreed de adoptiegraad te verhogen. De komende tijd moet uitwijzen of deze ambities worden gerealiseerd.

B5.10. Domein Overig

EML_NL

Waarom belangrijk ?

EML_NL is het Nederlands toepassingsprofiel op de Election Markup Language standaard. De standaard definieert de gegevens en de uitwisseling van digitale gegevens bij verkiezingen (die vallen onder de Nederlandse Kieswet). Daarbij gaat het om de uitwisseling van gegevens over kandidaten en over uitslagen om zo de verkiezingsuitslag en zetelverdeling vast te kunnen stellen. EML_NL draagt ertoe bij dat het verkiezingsproces transparant plaatsvindt en met minder kans op overname- en optelfouten. De standaard staat op de 'pas toe of leg uit'-lijst sinds 28 november 2013.

Feitelijk gebruik

De EML_NL standaard is opgenomen in de Ondersteunende Software Verkiezingen OSV2020. Het gebruik van de OSV2020 is daarmee een indicator voor het gebruik van de EML_NL standaard. OSV2020 wordt beschikbaar gesteld bij verkiezingen die onder de Kieswet vallen.

Alle bij het verkiezingsproces betrokken overheden maken gebruik van OSV2020 programmatuur bij verkiezingen en passen zo de EML_NL toe. Zo is de OSV2020 en daarmee de EML_NL standaard toegepast bij de Tweede Kamerverkiezing van 17 maart 2021.

Relevante ontwikkeling

Het gegeven dat inmiddels alle overheden in geval van verkiezingen gebruik maken van de OSV2020 programmatuur maakt dat met deze standaard in de huidige vorm een 100% doelbereik wordt gerealiseerd. Het dossier ten aanzien van verkiezingsprogrammatuur is momenteel onderwerp van gesprek tussen de Kiesraad, het ministerie van BZK en de VNG. Afhankelijk van de uitkomst van dat overleg zou het kunnen zijn dat kaders en eisen ten aanzien de OSV2020 worden herzien met mogelijk ook gevolgen voor de manier waarop het gebruik van EML_NL wordt voorgeschreven. Tegen die achtergrond blijft de EML_NL standaard voorlopig nog op de PToLU-lijst staan.

Meting Informatieveiligheidstandaarden overheid maart 2021

Inclusief IPv6-meting overheid

Datum 11 juni 2021

Status Definitief t.b.v. OBDO

Forum Standaardisatie

Standaard Samenwerken

1. Inleiding

Burgers en ondernemers moeten erop kunnen vertrouwen dat gegevensuitwisseling met de overheid en tussen overheden veilig verloopt. Recente phishing-incidenten waarin e-mails en websites van de overheid werden nagemaakt onderstrepen het belang van overheidsbrede adoptie van informatieveiligheidstandaarden. Binnen de overheid zijn daarom implementatieafspraken gemaakt over standaarden voor het beveiligen van mail en websites. Deze overheidsbrede streefbeeldafspraken, met uiterlijke implementatiedata, zijn een aanvulling op het staande 'pas toe of leg uit'-beleid.

Om de voortgang van deze afspraken bij te houden voert het Forum Standaardisatie op verzoek van het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) twee keer per jaar deze Meting Informatieveiligheidstandaarden uit naar het gebruik van informatieveiligheidstandaarden door overheidsorganisaties. De meting laat zien of overheidsorganisaties voldoen aan de gemaakte afspraken en wat de voortgang is.

Door toepassing van de informatieveiligheidstandaarden wordt:

- de verbinding met overheidswebsites beter beveiligd, zodat criminelen niet zomaar uitgewisselde gegevens kunnen onderscheppen of manipuleren;
- e-mailverkeer met de overheid beter beveiligd, zodat criminelen niet zomaar
- e-mails kunnen onderscheppen of manipuleren;
- overheidsdomeinen kunnen misbruiken als afzenddomein voor bijvoorbeeld phishing-aanvallen.

Tevens is op 8 april 2020 door het OBDO afgesproken dat alle overheidswebsites en e-mail-domeinen van de overheid uiterlijk eind 2021, behalve via IPv4, ook volledig bereikbaar moeten zijn via IPv6. Forum Standaardisatie meet op verzoek van OBDO halfjaarlijks de implementatievoortgang van deze afspraak, en in dit document wordt voor het eerst over deze afspraak gerapporteerd.

Voorliggende meting dateert van eind maart 2021. In de meting zijn 558 domeinnamen die ook in eerdere metingen centraal stonden getoetst. Daarnaast is een vergelijking gemaakt met de meetresultaten van een bredere selectie van circa 2200 overheidsdomeinen. Uit deze meting blijkt dat het stijgende gebruik van de standaarden doorzet, maar dat aandacht nodig is voor een veilige configuratie van internetstandaarden, en dat overheden hun leverancier actief moeten (blijven) vragen om ondersteuning van verplichte standaarden.

2. Samenvatting

2.1. Hoofdzakelijke bevindingen

2.1.1. Groei gebruik informatieveiligheidstandaarden, twee uitzonderingen

Het gebruik van de meeste informatieveiligheidstandaarden is afgelopen halfjaar wederom gegroeid. De uitzonderingen hierop zijn HSTS (web) en DNSSEC MX (e-mail). De terugval van 9% in de adoptiegraad (83%) van HSTS (voor het afdwingen van een beveiligde websiteverbinding) komt door een aanpassing in de minimum vereiste cache-geldigheidsduur, deze is in de Internet.nl test verhoogd van 6 maanden naar 1 jaar. Dit is in overeenstemming met de gangbare good practices. De lichte terugval van 2% in de adoptiegraad (64%) van DNSSEC MX (domeinnaambeveiliging voor mailservers) komt door toenemend gebruik van clouddiensten van voornamelijk Amerikaanse (moeder)bedrijven, waar DNSSEC minder gemeengoed is dan in Nederland. Dit heeft een remmend effect op de adoptie van zowel DNSSEC MX als DANE (voor het afdwingen van een beveiligde e-mailverbinding), hoewel de DANE-adoptie nog wel gegroeid is van 53% naar 55%.

2.1.2. Toekomstvaste TLS-configuraties

In de voorgaande meting (september 2020) zagen we een forse daling in het gebruik van TLS conform de aanbevolen configuratie volgens het NCSC, bij zowel web als e-mail. Dit werd veroorzaakt door een strengere vereisten. Inmiddels zien we dat overheden hun TLS-configuraties verbeteren. STARTTLS (veilige e-mailverbindingen) conform de NCSC-aanbevelingen is gegroeid van 42% naar 69%. HTTPS (veilige websiteverbindingen) conform de NCSC-aanbevelingen is gegroeid van 78% naar 83%.

2.1.3. Voorkomen van e-mailvervalsing

Om phishingmails uit naam van overheidsorganisaties (inclusief bewindspersonen) te voorkomen, moet meer dan een kwart van de halfjaarlijks gemeten domeinen nog een strikt DMARC-beleid instellen. Het streefbeeld was om dit eind 2019 voor elkaar te hebben. Kijken we breder dan de halfjaarlijks gemeten set domeinen, dan blijkt dat meer dan één derde van de overheidsdomeinen nog niet voldoet.

2.1.4. IPv6

Tot slot zien we dat er meer aandacht nodig is voor IPv6. IPv6 adoptie voor websites beweegt langzaam de goede kant op (adoptiegraad van 78%), maar het groeitempo lijkt te kort te komen om het nieuwe streefbeeld, dat in april 2020 in het OBDO is afgesproken, te gaan halen. Het groeitempo van IPv6 voor e-maildomeinen is gestegen, we constateren een verdubbeling ten opzichte van een half jaar geleden, maar met de huidige adoptiegraad van 40% wordt de het doel van 100% eind dit jaar hoogstwaarschijnlijk niet gehaald.

2.2. Webstandaarden

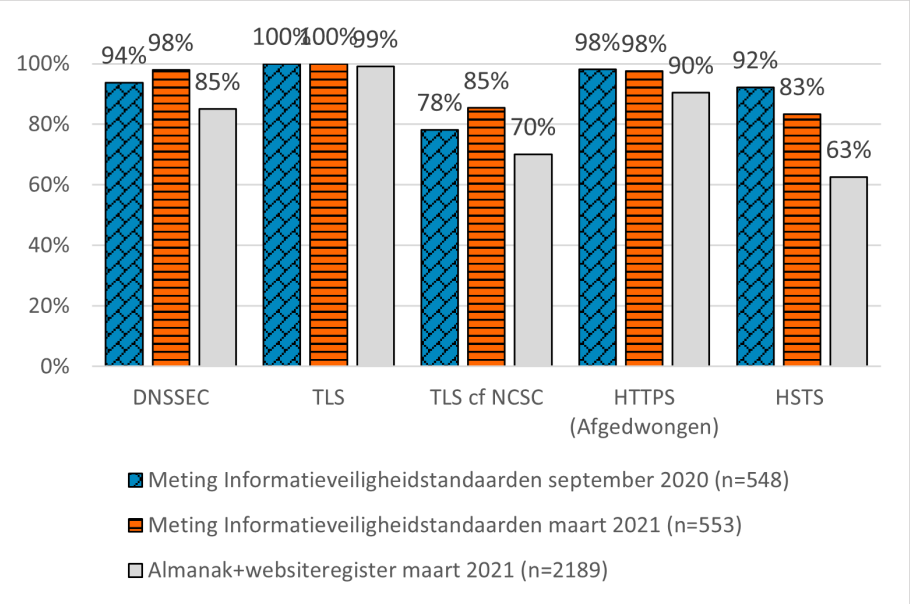
Positief is dat alle webdomeinen uit de originele meting HTTPS (TLS) gebruiken. Echter is de TLS-configuratie bij bijna één op de vijf overheden niet toekomstvast geconfigureerd. Overheden dienen hun TLS-verbindingen te configureren op basis van de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS).

Ook zien we dat het gebruik van HTTPS nog iets beter kan worden afgedwongen door gebruik te maken van veilige redirects en door HSTS (goed) toe te passen.

De terugval bij HSTS komt door strengere eisen aan de configuratie. HTTP Strict Transport Security (HSTS) dwingt een webbrowser om direct via HTTPS te verbinden bij het opnieuw bezoeken van een website. Dit helpt bij het voorkomen van man-in-the-middle aanvallen. De minimum HSTS cache geldigheidsduur is verlegnd van 6 maanden naar 1 jaar (max-age=31536000). Dit is in overeenstemming met de gangbare good practices.

De vergelijking met een bredere selectie van internetdomeinen van de overheid toont dat er buiten de belangrijkste internetdomeinen van de overheid extra aandacht nodig is voor de beveiliging van andere websites van de overheid.

Adoptie webbeveiligingsstandaarden: originele metingen t.o.v. bredere selectie



2.3. E-mailstandaarden voor bestrijding van phishing

Phishing is aan de orde van de dag. Ook phishing uit naam van de overheid, waarbij overheidsdomeinnamen worden misbruikt.

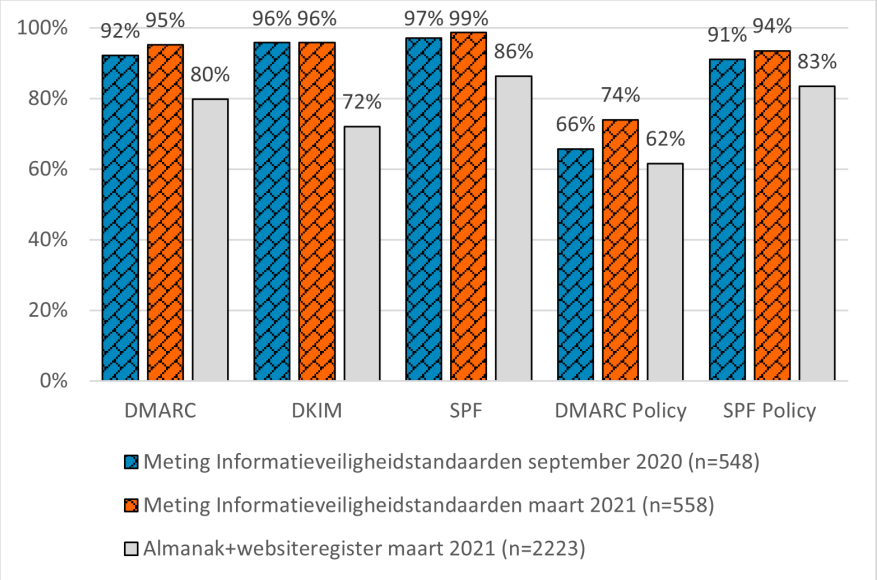
Met de implementatie en juiste strikte configuratie van anti-e-mailvervalsingstandaarden kan phishing worden bestreden.

De OBDO streefbeeldafspraak om dat eind 2019 bij 100% van de gemeten e-maildomeinen op orde te hebben is nog niet gehaald. Meer dan een kwart van de overheden voldoet nog niet. Phishingmails namens de achterblijvende organisaties (inclusief bewindspersonen) komen daardoor nog steeds bij burgers en bedrijven aan.

Bij de e-mailstandaarden die in samenhang e-mailspoofing voorkomen en daarmee phishing uit naam van overheidsorganisaties bemoeilijkt, zien we een groei in adoptiegraad ten opzichte van de vorige meting. Wel blijft aandacht nodig voor het toepassen van strikte DMARC policies om vervalste e-mails ook echt tegen te houden.

De vergelijking met de bredere selectie domeinen toont aan dat de focus op primaire domeinen leidt tot hogere adoptiecijfers, maar legt tevens bloot dat een groot deel van de online overheid nog werk aan de winkel heeft.

Adoptie e-mailstandaarden anti-phishing: originele metingen t.o.v. bredere selectie

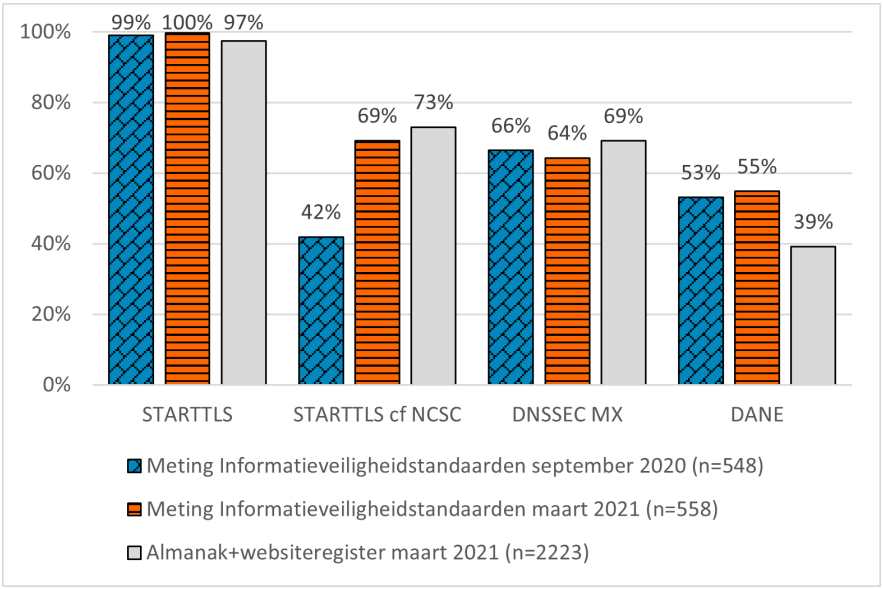


2.4. E-mailstandaarden voor vertrouwelijkheid e-mailverkeer

Positief is het beeld dat bijna alle mailservers STARTTLS gebruiken voor het versleutelen van het e-mailverkeer. Aandachtspunten blijven echter de veilige configuratie volgens de laatste beveiligingsrichtlijnen van het NCSC, en het afdwingen van de beveiligde verbinding middels DANE. DNSSEC voor mailservers is hiervoor een randvoorwaarde.

Het toenemend gebruik van clouddiensten van voornamelijk Amerikaanse (moeder)bedrijven, een land waar DNSSEC minder gemeengoed is dan in Nederland, heeft een remmend effect op DNSSEC en DANE adoptie.

Adoptie e-mailstandaarden vertrouwelijkheid: originele metingen t.o.v. bredere selectie

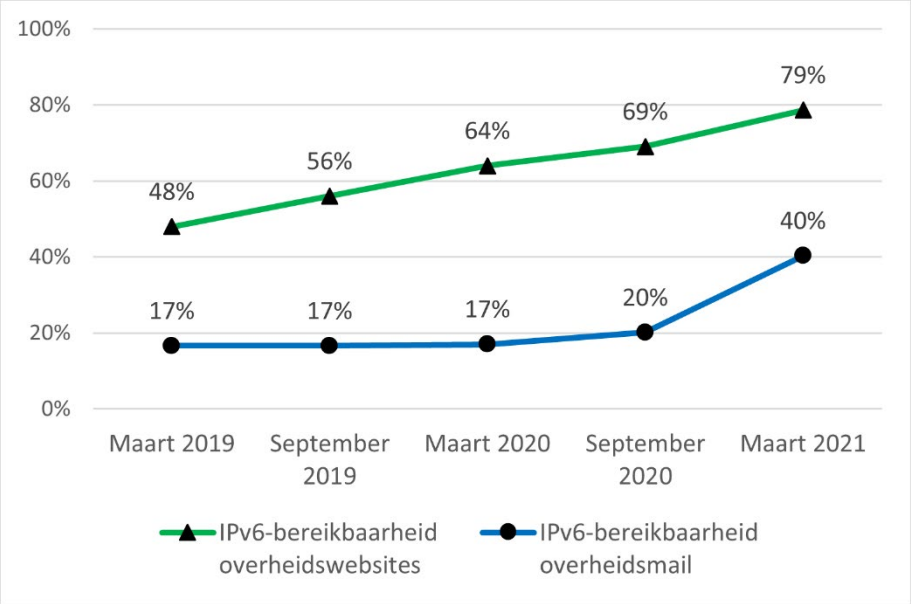


2.5. Bereikbaarheid via IPv6

Hoewel de adoptiegroei van IPv6 voor zowel websites als e-mail in deze meting een versnelling laat zien ten opzichte van de vorige meetpunten is er een flinke inhaalslag nodig om bij het streefbeeld van 100% adoptie voor het einde van dit jaar te komen. Met name de adoptiegroei van IPv6 voor e-mail ligt erg laag, en als dit niet heel snel omhoog gaat wordt het streefbeeld op dit aspect niet gehaald. Ook de adoptie van IPv6 voor websites vergt veel meer aandacht wil dit over heen half jaar in de buurt van de 100% komen.

De uitdaging ligt enerzijds bij gemeenschappelijke overheidsdienstverleners, om hun diensten 'by default' ook via IPv6 aan te bieden en de bestaande diensten actief via IPv6 bereikbaar te maken, zonder dat klanten hier zelf een wijzigingsverzoek voor hoeven in te dienen. Anderzijds is het aan overheidsorganisaties zaak om hun leveranciers actief te vragen om hun websites en e-mailvoorzieningen per IPv6 bereikbaar te maken.

Trend bereikbaarheid van websites en e-maildomeinen overheid via internetstandaard IPv6



2.6. Handelingsperspectief

Hoewel de gemiddelde adoptie van informatieveiligheidstandaarden in de afgelopen jaren sterk is gegroeid zijn we er nog niet. De volgende aanvullende inspanningen zijn noodzakelijk om verbeteringen te realiseren en daarmee Nederland digitaal weerbaarder te maken.

1. Overheden die nog niet voldoen aan de afgesproken standaarden dienen dringend (opnieuw) hun leverancier formeel te verzoeken om ondersteuning, en daarbij te wijzen op beschikbare how-to's en te vragen om een concrete planning.
2. Overheden wordt verzocht om de ontvangen leverancier splanningen ter informatie te delen met het Forum Standaardisatie. Forum Standaardisatie is bereid om desgewenst het gesprek aan te gaan met grotere overheidsleveranciers die nog niet te voldoen te coördineren.

3. Als de huidige leverancier te weinig medewerking verleent, dienen overheden te overwegen om over te stappen naar een leverancier die wel voldoet aan de afgesproken standaarden. Om geschikte leveranciers te vinden kan geleerd worden van collega-overheden die wel de afgesproken standaarden ondersteunen.

4. Forum Standaardisatie zal overheidsorganisaties, in samenwerking met koepelorganisaties, individueel aanspreken en helpen.

Meer specifiek met betrekking tot de mailstandaarden:

5. Het instellen van een voldoende strikte DMARC-policy is een kwestie van een goed, zorgvuldig configuratie-traject door de ICT-dienstverlener. SPF en DKIM zijn noodzakelijk randvoorwaarden voor DMARC-policy. De meting laat zien dat die standaarden al zeer veel worden toegepast (op tenminste 95% van de domeinen). Er ligt dus een duidelijk groeipotentieel voor DMARC-policy.

6. Het toepassen van DANE is een actie die ligt bij de beheerder van de mailserver. DNSSEC MX is een randvoorwaarde voor DANE en wordt al toegepast op 64% van de domeinnamen. Als een mailserver al DNSSEC doet, dan is het ondersteunen van DANE een relatief kleine stap ('laaghangend fruit'). Een aantal overheidsorganisaties maakt gebruik van cloud mailservers die nog geen DNSSEC MX en DANE ondersteunen. Het is van belang dat overheden ook bij deze leveranciers formele ondersteuningsverzoeken indienen.

7. Forum Standaardisatie heeft contact met veelvoorkomende mailproviders en mailsoftware-leveranciers die nog geen DNSSEC en DANE voor de mailservers ondersteunen, om de implementatieplannen te achterhalen en waar nodig te bespoedigen door de behoefte te articuleren. Dit gebeurt zoveel mogelijk in samenspraak met klanten en koepels. Het heeft er onder andere toe geleid dat Microsoft heeft aangekondigd om in 2021 DNSSEC en DANE te implementeren op Office 365 (Exchange Online). Mede langs deze weg is DANE-verificatie onlangs ook beschikbaar gekomen in Proofpoint EE (gedeeltelijke implementatie) en in Fortmail.

Meer specifiek met betrekking tot IPv6:

8. Adoptiegroei binnen de categorieën Rijk en uitvoering is met name te behalen als shared service providers, zoals SSC-ICT, ook stappen zetten om de servers via IPv6 bereikbaar te maken. Partijen als DPC en DICTU doen dit al. Met name SSC-ICT kan nog flinke stappen zetten, hun name-, web- en mailservers zijn bijvoorbeeld nog niet per IPv6 bereikbaar.

Bij gebruik van cloudmailoplossingen is het zaak aan overheidsorganisaties om hun leverancier te vragen om diensten ook via IPv6 bereikbaar te maken. Zo kunnen overheidsorganisaties die gebruik maken van Microsoft's Office 365 (Exchange Online) dit via de leverancier op verzoek laten activeren.

2.7. Regie op internetdomeinen

Tot slot blijkt uit een vergelijking tussen de hoofdresultaten van de meting met een bredere set overheidsdomeinen dat er nog een wereld te winnen valt. Focus op primaire (veelgebruikte) internetdomeinen is een logische eerste stap om belangrijke verbeteringen te realiseren. Maar sturing op het bredere domeinnaamportfolio is noodzakelijk om risico's voor zowel organisaties als burgers verdergaand te kunnen beheersen. Daarom roepen wij overheidsorganisaties op actief te werken aan het inrichten van regie op internetdomeinen. Als handreiking heeft Forum Standaardisatie vijf basisprincipes voor goed domeinnaam-beheer uiteengezet in de publicatie 'Regie op internetdomeinen: Lessen uit de praktijk'.

3. Achtergrond

Sinds 2015 biedt het Platform Internetstandaarden de mogelijkheid om via de website Internet.nl domeinen te toetsen op het gebruik van verschillende moderne internetstandaarden, waaronder een aantal informatieveiligheidstandaarden, die op de 'pas toe of leg uit'-lijst van Forum Standaardisatie staan. In datzelfde jaar is Forum Standaardisatie gestart om met behulp van Internet.nl een halfjaarlijkse meting van de adoptiegraad van informatieveiligheidsstandaarden voor overheidsdomeinen (web en e-mail) uit te voeren.

Die metingen hebben ertoe geleid dat het Nationaal Beraad in februari 2016 de ambitie uitsprak deze standaarden versneld te willen adopteren. Dit betekent concreet dat voor deze standaarden niet het tempo van 'pas toe of leg uit' wordt gevolgd (d.w.z. wachten op een volgend investeringsmoment en dan de standaarden implementeren), maar dat actief wordt ingezet op implementatie van de standaarden op de kortere termijn. Onderdeel van deze afspraak is dat Forum Standaardisatie de voortgang van de adoptie meet en inzichtelijk maakt. De halfjaarlijkse Meting Informatieveiligheidstandaarden is ook onderdeel van de jaarlijkse Monitor Open Standaarden.

Na de eerste interbestuurlijke afspraak zijn er door het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) drie aanvullende streefbeeldafspraken met verschillende uiterlijke implementatiedeadlines gemaakt. Onderdeel van de afspraken is ook de juiste configuratie van de standaarden. Van websites en e-mail van de overheid wordt vereist dat deze na het verlopen van de deadlines aan de standaarden en juiste configuratie voldoet.

3.1. Om welke standaarden gaat het

Het Nationaal Beraad en het OBDO hebben streefbeeldafspraken gemaakt met betrekking tot de volgende standaarden:

Implementatie-deadline	**Betreffende standaarden**
uiterlijk EIND 2017	TLS/HTTPS: beveiligde verbindingen van (transactie)websites DNSSEC: domeinnaambeveiliging SPF: anti-phishing van email DKIM: anti-phishing van email DMARC: anti-phishing van email
uiterlijk EIND 2018	HTTPS, HSTS en TLS conform de NCSC richtlijn (externe link): beveiligde verbindingen van alle websites
uiterlijk EIND 2019	STARTTLS en DANE: encryptie van mailverkeer SPF en DMARC: het instellen van strikte policies voor deze emailstandaarden
uiterlijk EIND 2021	IPv6 (naast IPv4): moderne internetadressering van overheidswebsites en e-maildomeinen van e overheid

3.2. Om welke domeinnamen gaat het

In totaal zijn in deze meting 558 domeinnamen van overheidsorganisaties getoetst, bestaande uit:

- Domeinen die horen bij de deelnemers van het OBDO;
- De domeinen die horen bij voorzieningen van de basisinfrastructuur (GDI);
- De 30 best bezochte domeinen van Rijksoverheden (en uitvoerders);
- De domeinen van de andere overheidsorganisaties die direct of indirect vertegenwoordigd zijn in het OBDO, zoals:
    - Uitvoerders (de Manifestpartijen);
    - Partijen die behorend tot Klein LEF;
    - Gemeenten;
    - Provincies;
    - Waterschappen.

Bij de selectie van de relevante domeinnamen is telkens gekozen voor het hoofddomein waarop de website van de overheidsorganisatie bereikbaar is. Daarnaast is gekozen voor het hoofddomein dat de desbetreffende overheidsorganisatie gebruikt voor e-mail (vaak dezelfde als voor web). Bij uitzondering zijn ook subdomeinen geselecteerd, bijvoorbeeld voor bekende inlogportalen of op verzoek van de beheerder.

De lijst betreft een selectie van alle overheidsdomeinnamen. De lijst is niet volledig en kan dat ook niet zijn omdat de overheid momenteel geen overzicht heeft over alle domeinnamen. De gemeten domeinen zijn bij lange na niet alle domeinen waar het OBDO direct en indirect voor verantwoordelijk is. Zo beheert het ministerie van AZ al meer dan 12.000 domeinnamen. Een 100%-score op de gemeten domeinen garandeert geenszins dat hiermee *alle* overheidsdomeinen beschermd zijn tegen bijvoorbeeld phishing. Indien uwer inziens een relevante domeinnaam ontbreekt, dan verzoeken we om deze aan ons door te geven.

Voor een betere waardering van de resultaten is in deze meting ook een vergelijking opgenomen met een meting van een bredere set aan overheidsdomeinen. Het gaat om bijna 2200 internetdomeinen die zijn ontleend aan het Register van Overheidsorganisaties en het Websiteregister Rijksoverheid. Omwille van de omvang zijn de detailresultaten van deze aanvullende meting niet opgenomen in de bijlagen.

3.3. Hoe wordt gemeten

De meting geeft de stand van zaken weer op de peildatum 31 maart 2020. De meting laat zien of op een domeinnaam de standaarden worden toegepast. De resultaten zijn voorgelegd aan een aantal koepelorganisaties en stakeholders en tot eind september geactualiseerd indien nodig.

De meting wordt uitgevoerd middels een bulktoets via de API van Internet.nl. Voor de web-standaarden wordt het hoofddomein getoetst met de toevoeging www. (dus: www.forumstandaardisatie.nl), omdat het gebruikelijk is dat de website daarop bereikbaar is. Voor de maildomeinen wordt getoetst zonder enig voorvoegsel omdat dat doorgaans gebruikt wordt als e-maildomein (dus @forumstandaardisatie.nl).

Op Internet.nl is eenvoudig te testen of een website of e-mail een aantal moderne internetstandaarden ondersteunen, ook de standaarden waarover streefbeeldafspraken zijn gemaakt zijn onderdeel van de test. De score die een domeinnaam op Internet.nl kan halen (namelijk max. 100%) heeft een directe relatie met het resultaat uit deze meting, aangezien deze meting alle standaarden bevat die de Internet.nl score kunnen beïnvloeden.

De website Internet.nl is een initiatief van het Platform Internetstandaarden. In het platform participeren verschillende partners uit de internetgemeenschap (zoals Internet Society, RIPE NCC, SIDN en SURFnet) en Nederlandse overheid (Forum Standaardisatie, het Ministerie van Economische Zaken en Klimaat, en NCSC). Het uitgangspunt is dat Internet.nl de adviezen van Forum Standaardisatie en NCSC met betrekking tot de Internetstandaarden volgt.

De meting geeft geen inzicht in het risiconiveau van een bepaald domein. Zo is het aannemelijk dat de aantrekkelijkheid van misbruik hoger is bij domeinen van grote uitvoerders (zoals *phishing* met aanmaningen) dan bij domeinen van kleine gemeenten.

3.4. Wat wordt niet gemeten

In de meting wordt alleen gekeken naar de toepassing van standaarden op domeinnamen. Er wordt in de meting (nog) niet gekeken naar de validatie op de standaarden. Dat betekent dat de volgende zaken niet worden gemeten:

1. validatie van DNSSEC door de DNS-resolver van een overheidsorganisatie;
2. validatie van de DMARC-, DKIM- en SPF-kenmerken door ontvangende mailservers van een overheidsorganisatie;
3. validatie van DANE-kenmerken door verzendende mailservers van een overheidsorganisatie.

In 2021/2022 zal naar verwachting de functionaliteit van Internet.nl worden aangepast zodat het mogelijk zal zijn om te controleren of DMARC-, DKIM-, SPF- en DANE-validatie wordt toegepast.

3.5. Over de standaarden

Er worden zowel web- als mailstandaarden gemeten. Hieronder per standaard een korte uitleg over wat deze doet. Overigens is meer (technische) informatie over wat er wordt getoetst te vinden op Internet.nl.

3.5.1. Webstandaarden

Wij meten het gebruik van de beveiligingsstandaarden voor het web ook op domeinen die alleen gebruikt worden voor mail omdat dit vaak wel domeinnamen zijn die re-directen naar het hoofddomein. Ook hiervoor moeten de standaarden juist worden toegepast en burgers weten vaak niet hoe deze domeinen worden gebruikt. Als redirects worden toepast dan moeten ook de doorverwijzende domeinen met HTTPS beveiligd zijn, anders is de beginschakel niet veilig en daarmee is ook de gehele keten onveilig. Dit geldt ook wanneer een zogenaamde ‘parking page’ wordt getoond. Alleen als een geregistreerd domein geen webpagina bevat dan is HTTPS niet nodig (en niet mogelijk).

DNSSEC	Domain Name System (DNS) is het registratiesysteem van namen en bijbehorende internetnummers en andere domeinnaaminformatie. Het is vergelijkbaar met een telefoonboek. Dit systeem kan worden bevraagd om namen naar nummers te vertalen en omgekeerd. Er is getest of de domeinnaam ondertekend is met DNSSEC, zodat de integriteit van de DNS-informatie is beschermd. De streefbeeldafspraak was om hier vóór 2018 aan te voldoen.
TLS	Als een bezoeker een onbeveiligde HTTP-verbinding heeft met een website, dan kan een kwaadwillende eenvoudig gegevens onderweg afluisteren of aanpassen, of zelfs het contact volledig overnemen. Getest wordt of TLS is toegevoegd aan HTTP om de verbinding te beveiligen. Op Internet.nl heet deze subtest 'HTTPS available'. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
TLS cf. NCSC	We maken een onderscheid tussen 'TLS' en 'TLS conform NCSC'. In het eerste geval wordt gebruik gemaakt van TLS en in het tweede geval is TLS bovendien zodanig geconfigureerd dat deze voldoet aan de aanbevelingen van het Nationaal Cyber Security Center (NCSC). Zodat de vertrouwelijkheid, de authenticiteit en integriteit van een bezoek aan een website is gegarandeerd. De streefbeeldafspraak was om hier voor 2019 aan te voldoen.
HTTPS redirect	Er wordt getest of een webserver bezoekers automatisch doorverwijst van HTTP naar HTTPS op dezelfde domeinnaam óf dat deze ondersteuning biedt voor alleen HTTPS en niet voor HTTP. Op Internet.nl heet deze subtest 'HTTPS Redirect'. De streefbeeldafspraak was om hier voor 2019 aan te voldoen.
HSTS	HSTS zorgt ervoor dat een browser eist dat een website altijd HTTPS blijft gebruiken na het eerste contact over HTTPS. Dit helpt voorkomen dat een derde -bijvoorbeeld een kwaadaardige WiFi hotspot- een browser kan omleiden naar een valse website. Door HTTPS samen met HSTS te gebruiken wordt het gebruik van beveiligde verbindingen zoveel mogelijk afgedwongen. De streefbeeldafspraak was om hier vóór 2019 aan te voldoen.

3.5.2. Mailstandaarden

Wij meten het gebruik van e-mailbeveiligingsstandaarden ook op domeinen waarvan een organisatie geen e-mail verstuurt. Dit is relevant omdat ook die domeinen worden misbruikt (burgers weten vaak niet dat deze domeinen niet door de organisatie worden gebruikt), en juist domeinen waarvandaan niet gemaild wordt, makkelijk kunnen worden geblokkeerd met behulp van SPF en DMARC (met de policies –all en p=reject).

DMARC	Met DMARC kan een e-mailprovider kenbaar maken hoe andere (ontvangende) mailservers om dienen te gaan met de resultaten van de SPF- en/of DKIM-controles van ontvangen e-mails. Dit gebeurt door het publiceren van een DMARC beleid in het DNS-record van een domein. In deze test wordt alleen gekeken of DMARC beschikbaar is, niet of er beleid is ingesteld. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
DMARC Policy	Zolang er geen beleid is ingesteld weet de ontvanger nog niet wat te doen met verdachte e-mail. De configuratie moet op orde zijn. (Opm: Actieve policies zijn ~all en –all voor SPF, en p=quarantine en p=reject voor DMARC) Er wordt gecontroleerd of de syntax van de DMARC-record correct is en of deze een voldoende strikte policy bevat. De streefbeeldafspraak was om hier voor 2020 aan te voldoen.
DKIM	Met DKIM kunnen e-mailberichten worden gewaarmerkt. De ontvanger van een e-mail kan op die manier controleren of een e-mailbericht écht van de afzender afkomstig is en of het bericht onderweg ongewijzigd is gebleven. Getest wordt of de domeinnaam DKIM ondersteunt. Voor non-mail domeinen waar dit goed is ingesteld heeft DKIM verder geen toegevoegde waarde. In de meting wordt dit weergegeven middels de score “NVT” (niet van toepassing) voor DKIM. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
SPF	SPF heeft als doel spam te verminderen. SPF controleert of een verzendende mailserver die e-mail namens een domein wil versturen, ook daadwerkelijk gerechtigd is om dit te mogen doen. Getest wordt of de domeinnaam een SPF-record heeft. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
SPF Policy	Aanvullend op bovenstaande test wordt gecontroleerd of de syntax van de SPF-record geldig is en of deze een voldoende strikte policy bevat om misbruik van het domein door phishers en spammers tegen te gaan. De streefbeeldafspraak was om hier voor 2020 aan te voldoen.
STARTTLS	STARTTLS in combinatie met DANE gaan het afluisteren of manipuleren van mailverkeer tegen. STARTTLS maakt het mogelijk om transportverbindingen tussen e-mailservers op basis van certificaten met TLS te beveiligen. Er wordt getest of de ontvangende mailservers (MX) ondersteuning bieden voor STARTTLS. De streefbeeldafspraak is om hier voor 2020 aan te voldoen. Als er geen mailservers aanwezig is voor het domein dan wordt dit weergeven met NVT. Dit geldt ook voor STARTTLS CF. NCSC, DANE en DNSSEC MX.

STARTTLS CF. NCSC	Net zoals bij HTTPS kan er bij STARTTLS gebruik worden gemaakt van verschillende versies van het TLS en verschillende versleutelingsstandaarden (ciphers). Aangezien niet alle versies en combinaties als voldoende veilig worden beschouwd, is het belangrijk om hierin de juiste keuze te maken en ook regelmatig te controleren of de gebruikte instellingen nog veilig zijn. Getest wordt of STARTTLS is geconfigureerd zoals door het NCSC is aanbevolen. De streefbeeldafspraak was om hier vóór 2020 aan te voldoen.
DANE	DANE, dat voortbouwt op DNSSEC, zorgt er in combinatie met STARTTLS voor dat een verzendende e-mailserver de authenticiteit van een ontvangende e-mailserver kan controleren en het kan het gebruik van TLS bovendien afdwingen. Getest wordt of de nameservers van de mailservers één of meer TLSA-records voor DANE bevatten. De streefbeeldafspraak was om hier voor 2020 aan te voldoen.
DNSSEC MX	DNSSEC is een randvoorwaarde voor het instellen van DANE. Daarom wordt getest of de domeinnamen van de mailservers (MX) ondertekend zijn met DNSSEC. Dit in het kader van de streefbeeldafspraak om voor 2020 STARTTLS en DANE te ondersteunen.

4. Resultaten meting maart 2021

In dit hoofdstuk staan de resultaten van de web- en e-mailbeveiligingsstandaarden die onderdeel uitmaken van de streefbeeldafspraken van het OBDO. De resultaten zijn geordend per standaard en per "overheidslaag".

4.1. Per standaard

De volgende drie diagrammen tonen de adoptiestatus van de individuele standaarden voor zowel de webstandaarden als de e-mailstandaarden (anti-phishing en vertrouwelijkheid van e-mail). Er is een vergelijking gemaakt met de voorgaande twee metingen.

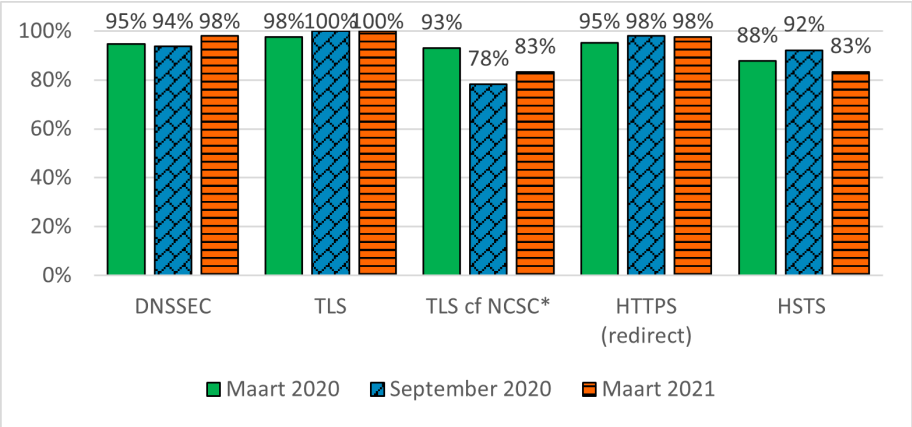
4.1.1. Webstandaarden

De toepassing van versleuteling van webverkeer – in de vorm van HTTPS op basis van TLS - is in de basis gemeengoed met 100% adoptiegraad. Echter is de TLS-configuratie bij bijna één op de vijf overheden niet toekomstvast geconfigureerd. Overheden dienen hun TLS-verbindingen te configureren op basis van de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS).

Ook zien we dat het gebruik van HTTPS nog iets beter kan worden afgedwongen. Twee procent van de overheden maakt nog gebruik van onveilige redirects, en bijna één op de vijf overheden past HSTS niet of niet strikt genoeg toe.

De terugval van 9% in de adoptiegraad (83%) van HSTS (voor het afdwingen van een beveiligde websiteverbinding) komt door een aanpassing in de minimum vereiste cache-geldigheidsduur, deze is in de Internet.nl test verhoogd van 6 maanden naar 1 jaar. Dit is in overeenstemming met de gangbare good practices.

Gemiddelde adoptie webstandaarden



Bij de vorige meting ontstond na een verscherping van de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) een terugval op 'TLS conform NCSC'. In deze meting zien we dat een deel van de overheden de TLS-configuratie hebben verbeterd. Ook bij DNSSEC zien we een vooruitgang van 4% na een lichte daling bij de vorige meting.

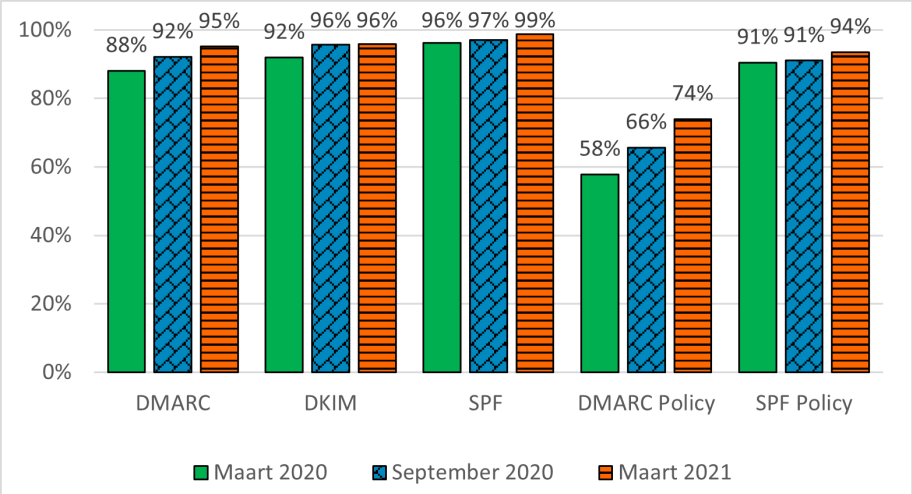
Voor overheden is het van belang om hun internetdomeinen periodiek te controleren met Internet.nl om vast te stellen of de configuraties nog voldoen aan de actuele vereisten.

4.1.2. E-mailstandaarden voor het bestrijden van e-mailvervalsing (anti-phishing)

Bij de e-mailstandaarden die in samenhang e-mailspoofing voorkomen en daarmee phishing uit naam van overheidsorganisaties bemoeilijkt, zien we bijna overal groei. Alleen het gebruik van DKIM is blijven steken op 96%.

De grootste stijging zien we bij de toepassing van een strikte DMARC policy waarmee het gebruik van DKIM en SPF beter wordt afgedwongen. Wel blijft aandacht nodig voor het toepassen van strikte DMARC policies om vervalste e-mails ook echt tegen te houden, meer dan een kwart van de overheden heeft nog geen voldoende strikt DMARC policy ingesteld. Hierdoor kunnen vervalste e-mails – bijvoorbeeld namens bewindspersonen of de financiële administratie – nog steeds bij burgers aankomen.

Gemiddelde adoptie mailstandaarden: voorkomen e-mailspoofing (anti-phishing)



Het Bureau Forum Standaardisatie spreekt reeds actief partijen aan op de noodzaak om actieve, strikte policies voor zowel DMARC en SPF in te stellen, en zal hier blijvend aandacht aan schenken.

4.1.3. E-mailstandaarden voor vertrouwelijkheid e-mailverkeer

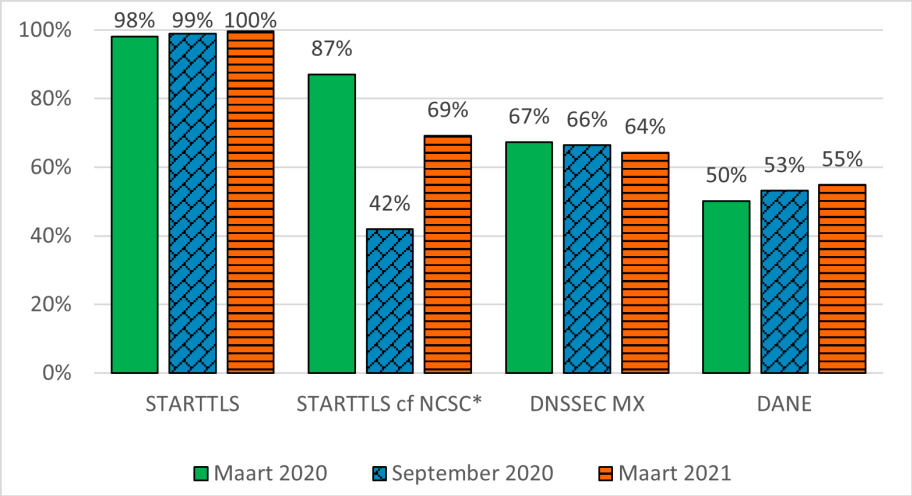
De toepassing van versleuteling van e-mailverkeer – in de vorm van STARTTLS op basis van TLS – is in de basis gemeengoed met 100% adoptiegraad. Echter is de TLS-configuratie bij bijna één op de drie overheden niet toekomstvast geconfigureerd. Overheden dienen hun TLS-verbindingen te configureren op basis van de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS).

Bij de vorige meting ontstond na een verscherping van de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) een terugval op 'STARTTLS conform NCSC'. In deze meting zien we dat een groot deel van de overheden de TLS-configuratie hebben verbeterd, wat zich uit in een stijging van 42% toekomstvaste configuraties naar 69% toekomstvaste configuraties.

Daarnaast valt de aanhoudende daling van DNSSEC voor mailservers (MX) op. Deze beweging wordt veroorzaakt door overheden die overstappen op cloudmailproducten die geen DNSSEC ondersteunen. We zien dat als gevolg hiervan het groeitempo van DANE blijft afzwakken. Het kunnen gebruiken van DANE is technisch afhankelijk van de implementatie

van DNSSEC voor mailservers (MX). Wel zien we aan de hand van het adoptiepercentage van DNSSEC voor mailservers nog een direct groeipotentieel van 9% voor DANE.

Gemiddelde adoptie e-mailstandaarden: beveiligde verbinding (vertrouwelijkheid)



Het achterblijven van DANE blijft zorgwekkend, omdat dit overheidsmail die niet voldoet onnodig kwetsbaar maakt voor afluisteren. De meest voorkomende mailprovider die nog geen DNSSEC en DANE ondersteund is Microsoft. Ook andere cloudproviders zoals Google, Proofpoint, Mimecast en Barracuda ondersteunen nog geen DNSSEC en DANE. De publieke planning van Microsoft is nog steeds om eind 2021 DANE support te kunnen bieden. Dit zal naar verwachting op termijn een aanzienlijk positief effect op de adoptiecijfers van DANE hebben, en daarmee op de veiligheid van overheidsmail.

Het Bureau Forum Standaardisatie blijft in contact met veelvoorkomende mailproviders die nog geen DNSSEC en DANE voor de mailservers ondersteunen, om de implementatieplannen te achterhalen en waar nodig te bespoedigen door de behoefte te articuleren. Dat laatste waar nodig in samenspraak met klanten en koepels.

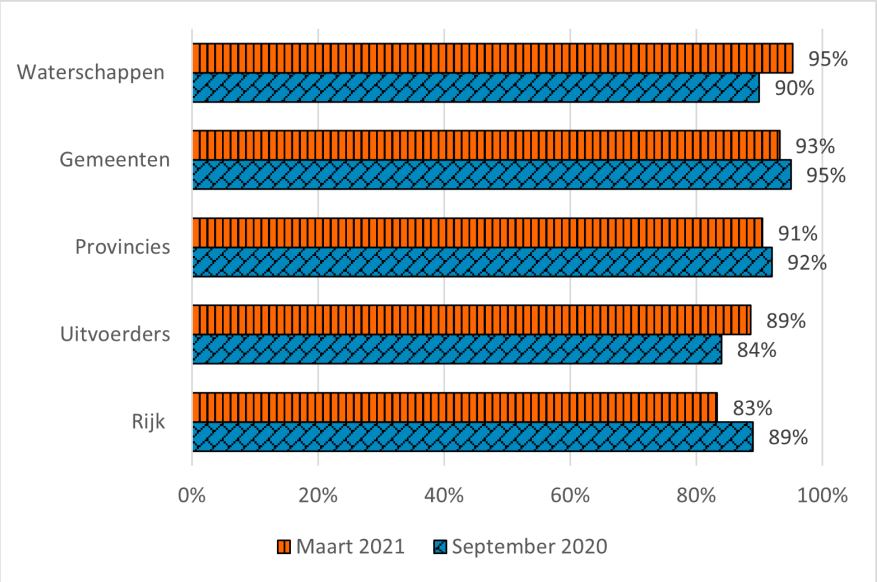
4.2. Per overheidslaag

Een uitsplitsing van de resultaten van de meting naar overheidslaag laten bij de meeste overheidslagen een daling zien ten opzichte van de voorgaande meting. De daling is veroorzaakt door de strengere norm voor TLS conform de beveiligingsrichtlijnen van het NCSC. De gemiddelden geven een vertekend beeld, alle andere adoptiepercentages – m.u.v. DNSSEC (MX) – zijn gestegen. Zonder de strengere norm voor TLS zouden we een gemiddelde groei zien. Wel geeft de meting een reëel beeld, waarbij beveiligingsnormen noodzakelijk zijn aangepast aan de veranderende werkelijkheid. De diagrammen maken zichtbaar hoe de overheidslagen gemiddeld gezien ten opzichte van elkaar scoren.

4.2.1. Webstandaarden

Alleen de waterschappen en uitvoerders hebben gemiddeld gezien een groei doorgemaakt. De waterschappen lopen nu voorop in de toepassing van webstandaarden met een gemiddelde toepassingsgraad van 95%. Het Rijk is als gevolg van verminderde toepassing van HSTS en veilige HTTPS-redirects de sterkste daler van 89% naar 83%.

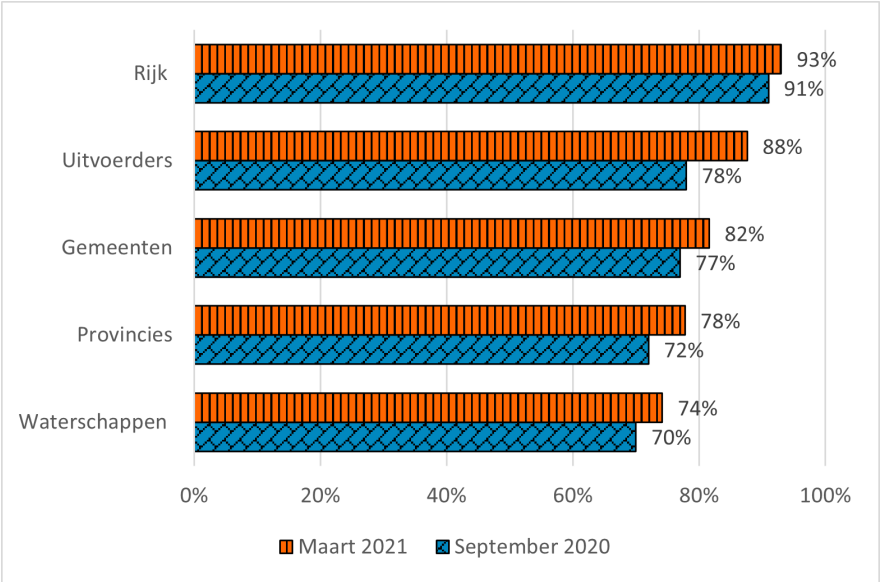
Gemiddelde adoptiegraad webstandaarden per overheidslaag (van hoog naar laag)



4.2.2. E-mailstandaarden

Bij de e-mailstandaarden zien we in de gemiddelde toepassingsgraad bij iedere overheidslaag groei. Het Rijk blijft koploper en de waterschappen blijven hekkensluiter. Bij de uitvoerders zien we de grootste stijging in de toepassing van e-mailstandaarden, tien procent.

Gemiddelde adoptiegraad e-mailstandaarden per overheidslaag (van hoog naar laag)

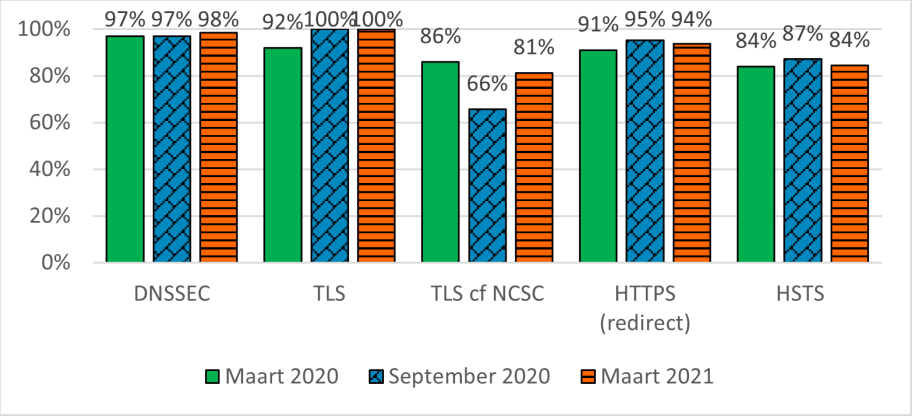


In het vervolg van de rapportage wordt per overheidslaag toegelicht welke standaarden gemiddeld veel worden toegepast en welke minder.

Het Rijk

Bij de webstandaarden zien we dat het Rijk nog werk aan de winkel heeft om voor alle websites een toekomstvaste TLS-configuratie te implementeren, en om de TLS-verbinding goed af te dwingen door doorverwijzingen (van bijvoorbeeld www.minvenj.nl naar www.rijksoverheid.nl) en standaard HSTS goed te configureren.

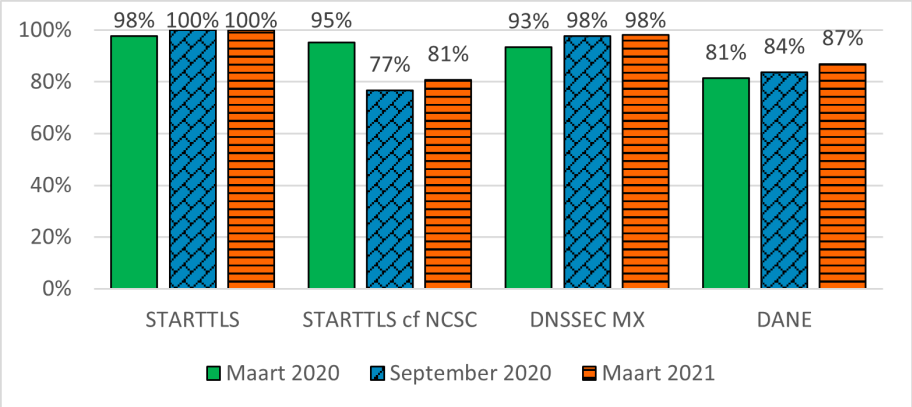
Gemiddelde adoptie Rijk: webstandaarden



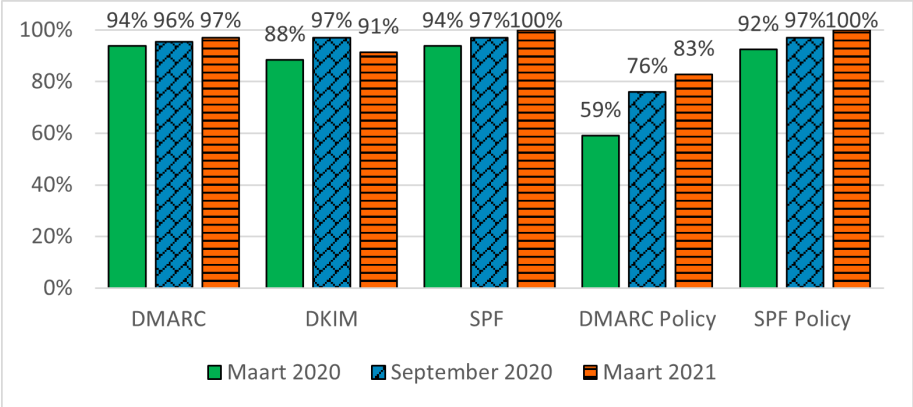
Hoewel het Rijk relatief beter scoort dan andere overheidslagen als het gaat om de mailstandaarden is het streefbeeld om 100% van de gemeten e-maildomeinen op orde te hebben nog niet gehaald. Met name bij STARTTLS conform de TLS-beveiligingsrichtlijnen van het NCSC, een strikt DMARC policy en DANE vragen aandacht. Hoewel het Rijk bepaalde schaalvoordelen heeft doordat het beheer van de mailservers bij een relatief klein aantal partijen belegd is, ligt er nog wel een opgave. Een voordeel is dat aanpassing bij die partijen een grote impact kan hebben op de gemiddelde score van het Rijk.

Verder valt de terugval in de toepassing van DKIM op. De toepassingsgraad is gedaald van 97% naar 91%.

Gemiddelde adoptie Rijk: mailstandaarden - beveiligde verbinding



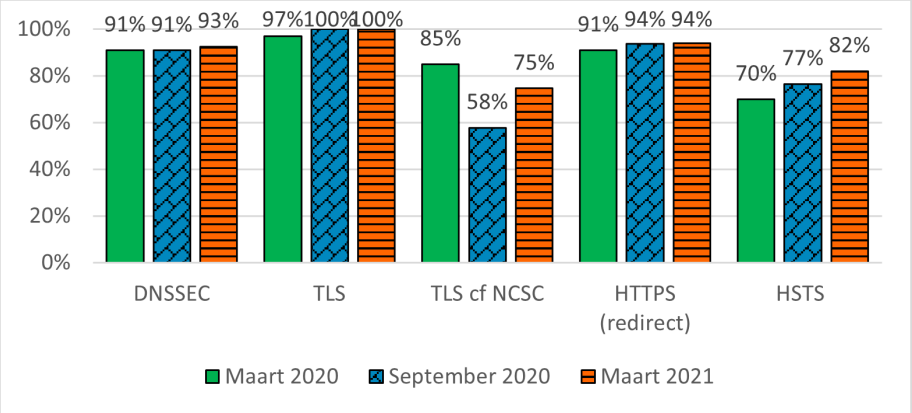
Gemiddelde adoptie Rijk: mailstandaarden - anti-phishing



4.2.3. Uitvoering

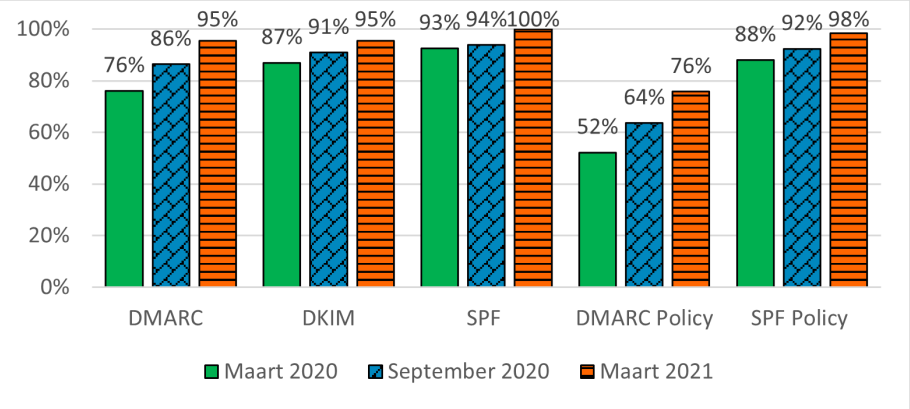
Bij de uitvoeringsorganisaties zien we dat er nog steeds onvoldoende aandacht is voor DNSSEC, deze staat op een adoptiegraad van 93% t.o.v. 98% overheidsbreed. Hoewel ook alle uitvoeringsorganisaties nu TLS toepassen, scoren zij met een adoptiegraad van 75% ondergemiddeld op TLS conform de TLS-beveiligingsrichtlijnen, dat is overheidsbreed 85%. Ondanks groei bij HSTS, wordt ook deze standaard gemiddeld gezien ondergemiddeld toegepast met een adoptiegraad van 82%.

Gemiddelde adoptie uitvoerders: webstandaarden

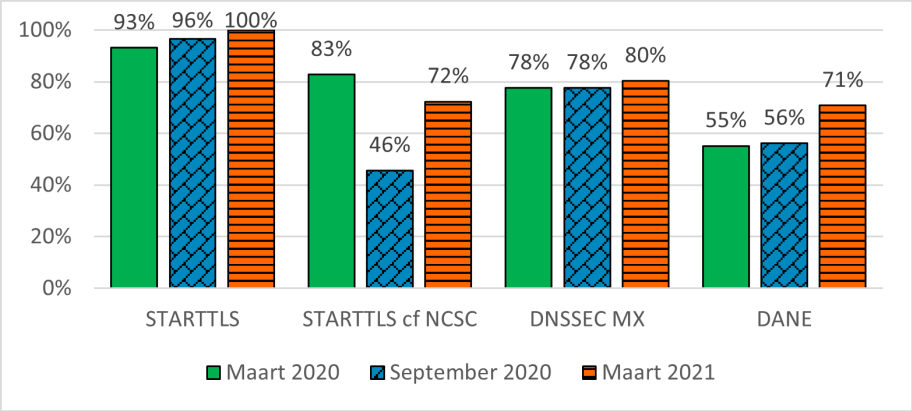


De groei bij e-mailstandaarden, die we bij de uitvoeringsorganisaties in de vorige meting constateerden, is doorgezet. Met name DMARC, mét en zonder strikte policy, wordt vaker toegepast, hoewel er nog meer ruimte is voor groei. Opvallend is de flinke groei van 15% in het gebruik van DANE voor het afdwingen van een versleutelde verbindinng. Afgeleid van het adoptiepercentage van DNSSEC MX, is er nog een groeipotentieel van 9% om DANE voor inkomend verkeer mogelijk te maken.

Gemiddelde adoptie uitvoerders: mailstandaarden - anti-phishing



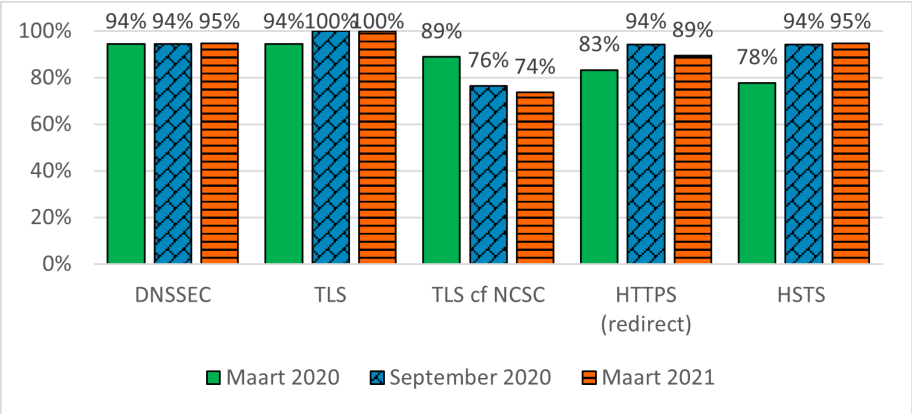
Gemiddelde adoptie uitvoerders: mailstandaarden - beveiligde verbinding



4.2.4. Provincies

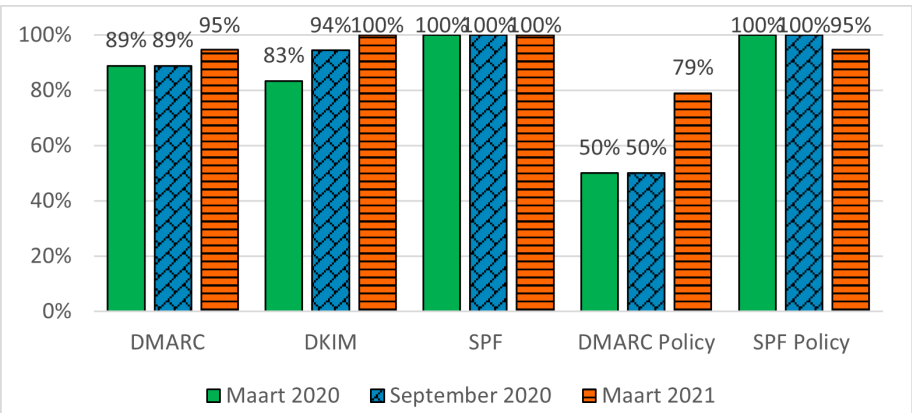
Bij de provincies zien we een stagnatie in de adoptie van veilige webstandaarden. Het gebruik van HSTS blijft met 95% bovengemiddeld. Het gebruik van een veilige TLS-configuratie ligt met 74% echter 11% onder het gemiddelde van 85%.

Gemiddelde adoptie provincies: webstandaarden



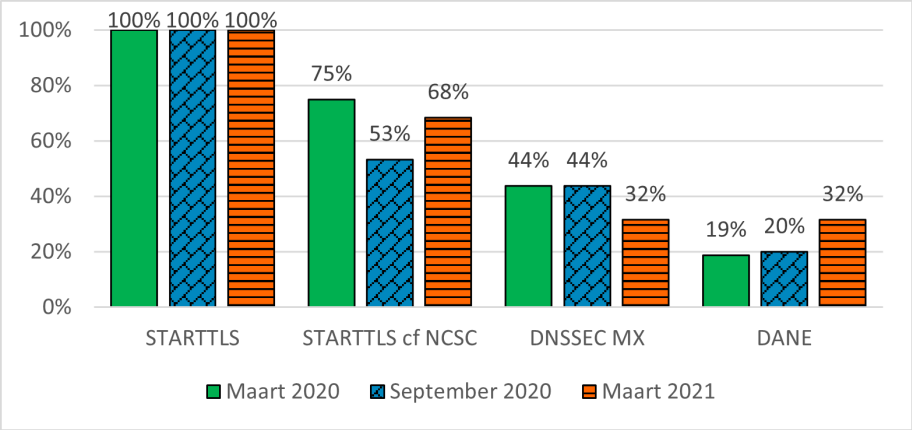
Bij de mailstandaarden valt de groei in de toepassing van een strikte DMARC policy op. Bij de vorige meting waren de provincies nog de meest 'spoofbare' overheidslaag, met de laagste adoptiegraad van een strikte DMARC policy (50%), maar nu scoren zij met 79% adoptiegraad bovengemiddeld, ten opzichte van een adoptiegraad van 74% overheidsbreed.

Gemiddelde adoptie provincies: mailstandaarden - anti-phishing



De adoptiegraad van DNSSEC en DANE zijn met 32% vrij laag, dit komt door relatief hoog gebruik van cloudmailproducten die deze standaarden nog niet ondersteunen.

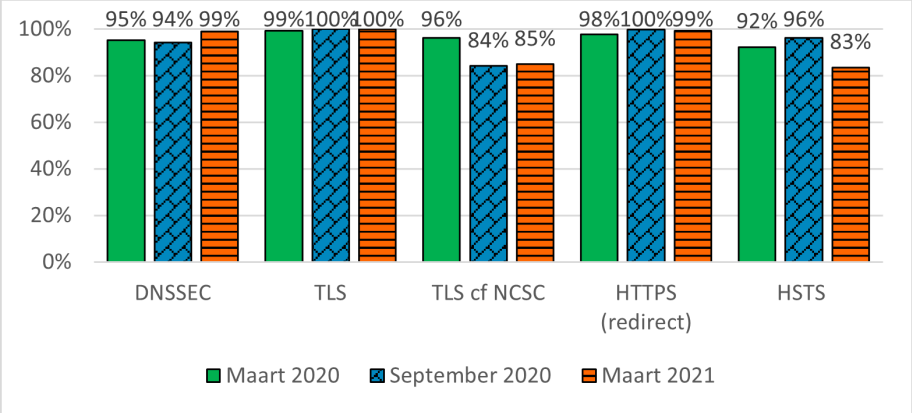
Gemiddelde adoptie provincies: mailstandaarden - beveiligde verbinding



4.2.5. Gemeenten

De voornaamste uitdaging voor gemeenten is om hun TLS en HSTS configuraties conform de actuele vereisten te houden. Het loont voor gemeenten om de beveiligingsrichtlijnen van het NCSC in de gaten te houden en hun internetdomeinen periodiek te controleren met Internet.nl. Gemiddeld gezien scoren de gemeenten echter bovengemiddeld hoog ten opzichte van de meeste overheidslagen, met uitzondering van de waterschappen.

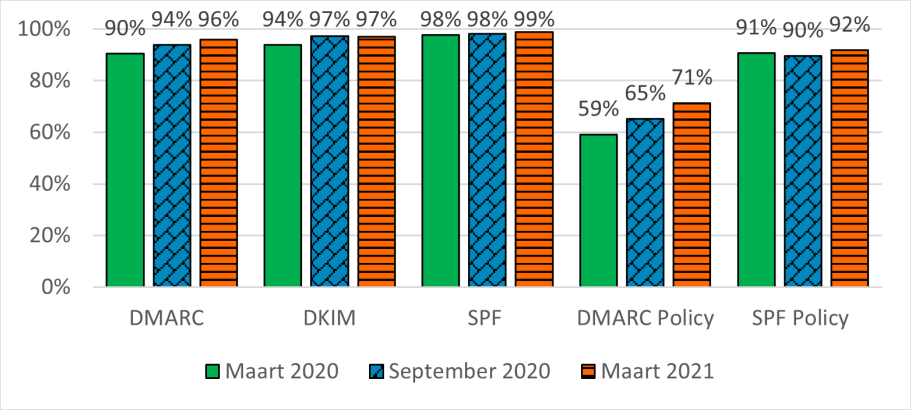
Gemiddelde adoptie gemeenten: webstandaarden



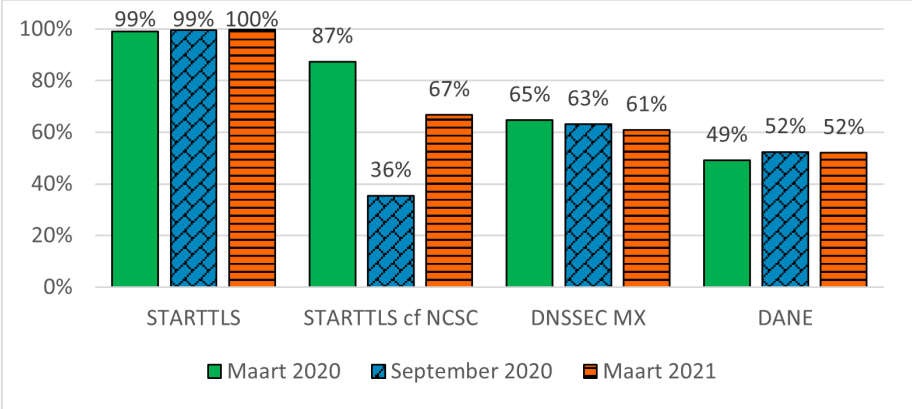
Bij de mailstandaarden zien we dat er nog aandacht nodig is voor het strikt afstellen van DMARC policy (71%) en SPF policy (92%).

De terugval bij STARTTLS conform de TLS-beveiligingsrichtlijnen uit de vorige meting is enigszins ingelopen. Toch moet één op de drie gemeenten STARTTLS nog toekomstvast configureren. Er blijft aandacht nodig voor de toepassing van DNSSEC voor mailservers en DANE, waarmee de beveiligde verbinding kan worden afgedwongen en zogenaamde 'downgrade attacks' kunnen worden voorkomen.

Gemiddelde adoptie gemeenten: mailstandaarden - anti-phishing



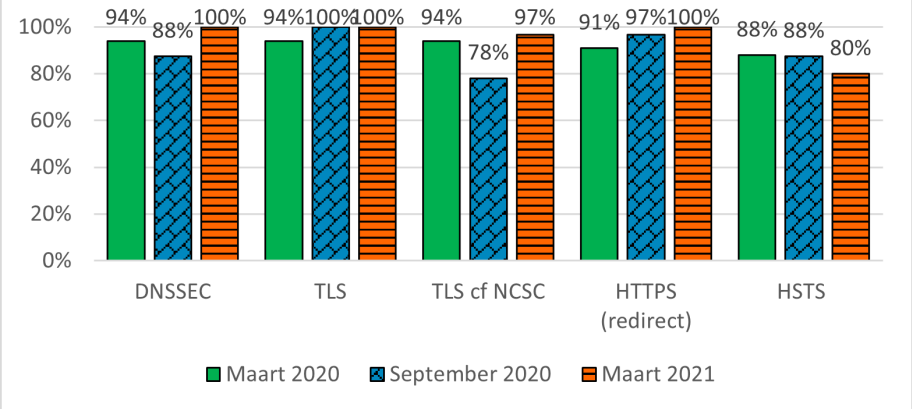
Gemiddelde adoptie gemeenten: mailstandaarden - beveiligde verbinding



4.2.6. Waterschappen

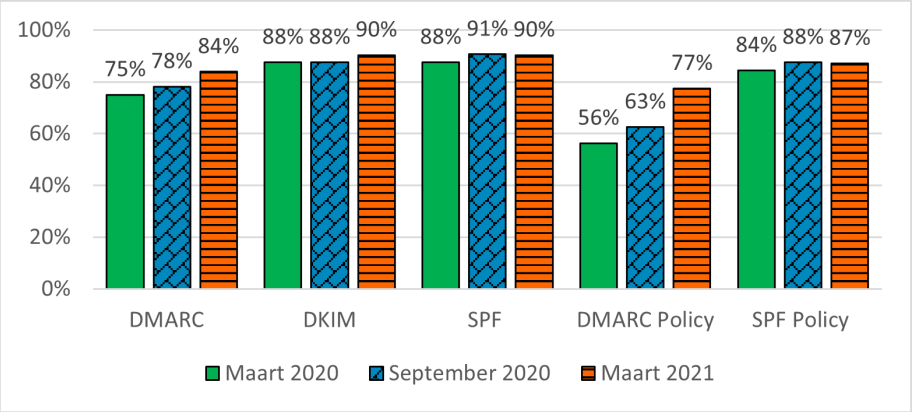
De waterschappen zijn sinds deze meting koploper in de toepassing van webstandaarden voor informatieveiligheid. Aandachter blijft nodig voor de correcte toepassing van HSTS.

Gemiddelde adoptie waterschappen: webstandaarden

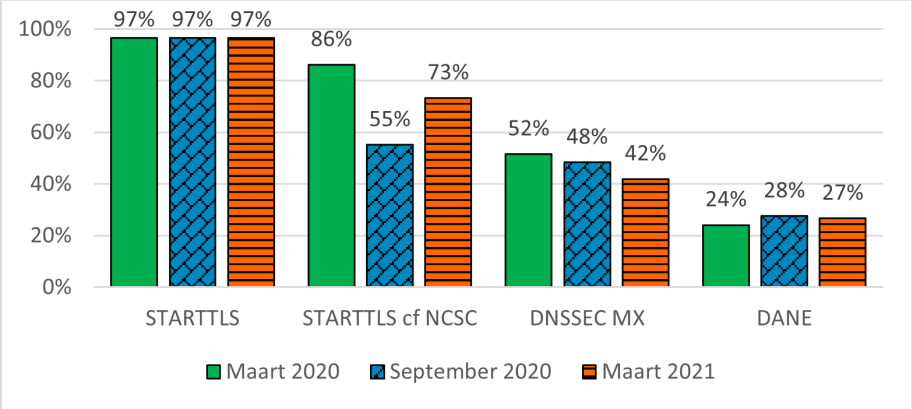


Op het vlak van e-mailbeveiligingsstandaarden lopen de waterschappen wat achter op de overige overheidslagen. Met name verbindingsbeveiliging vergt aandacht, maar ook de DMARC policies kunnen strikter worden ingesteld.

Gemiddelde adoptie waterschappen: mailstandaarden - anti-phishing



Gemiddelde adoptie waterschappen: mailstandaarden - beveiligde verbinding



5. IPv6-meting overheidswebsites en e-maildomeinen

Alle overheidswebsites en e-maildomeinen van de overheid moeten uiterlijk eind 2021, behalve via IPv4, ook volledig bereikbaar zijn via IPv6. Dat besloot het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) op 8 april 2020. Forum Standaardisatie meet halfjaarlijks de implementatievoortgang van IPv6.

5.1. Over IPv6

IPv6 is de open internetstandaard die iedere internetgebruiker nodig heeft om ook in de toekomst onbelemmerd gebruik te kunnen maken van internet. Er zijn verschillende goede redenen om voor IPv6 te kiezen, juist ook als overheid: groei en innovatie van internet, directere en snellere dienstverlening, en tegengaan van fraude.

Internet Protocol versie 6 (IPv6) maakt communicatie van data tussen ICT-systemen op het Internet mogelijk. De standaard bepaalt dat ieder ICT-systeem op het Internet een uniek nummer (IPv6-adres zoals 2a07:3506:4c:3207::1:0) heeft. Hierdoor kunnen ICT-systemen elkaar herkennen en onderling data uitwisselen. IPv6 heeft een veel grotere hoeveelheid beschikbare IP-adressen ten opzichte van de voorganger IPv4. Een computer met een IPv4-adres kan niet communiceren met een computer die alleen een IPv6-adres heeft. Wel kunnen versie 4 en versie 6 naast elkaar worden gebruikt, maar uiteindelijk zal IPv4 volledig worden vervangen door IPv6. In november 2019 zijn de laatst beschikbare IPv4-adressen voor Europa uitgegeven.

5.2. Over de IPv6-meting

De domeinen en meetwijze zijn in de basis gelijk aan de Meting Informatieveiligheidstandaarden. Voor meer informatie hierover kunt u terecht in hoofdstuk 3.

De volgende tabel geeft aan wat is getest.

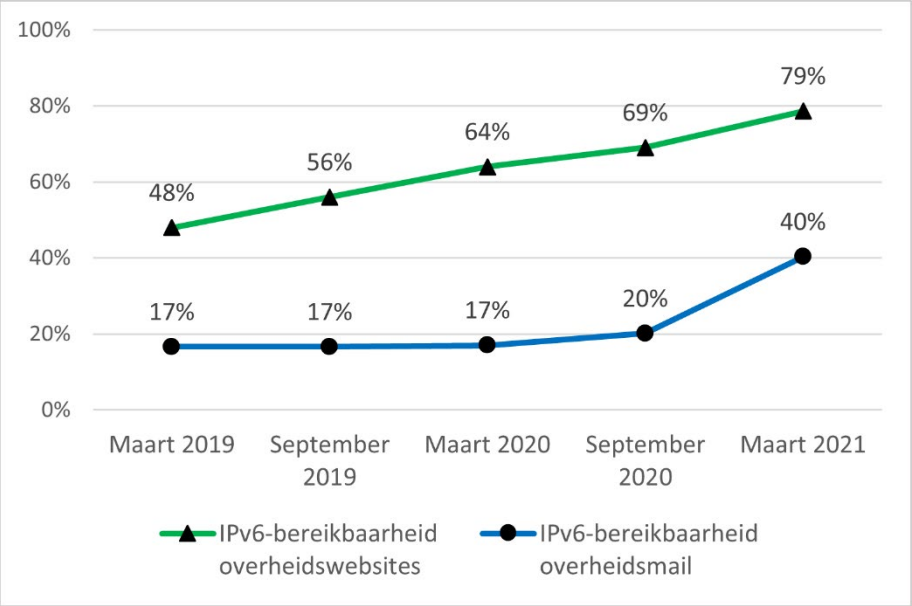
IPv6 web	Er wordt getest of alle nameservers (minimaal twee) en tenminste één webserver een IPv6-adres hebben en bereikbaar zijn. Er wordt ook getest of de IPv6 website gelijkt lijkt aan de IPv4 website. De streefbeeldafspraak is om hier vóór 2022 aan te voldoen.
IPv6 e-mail	Er wordt getest of alle nameservers (minimaal twee) van het e-maildomein en alle mailservers (MX) een IPv6-adres hebben en bereikbaar zijn. De streefbeeldafspraak is om hier vóór 2022 aan te voldoen.

5.3. Trend bereikbaarheid overheid via IPv6

Onderstaande grafiek toont de trend in het toepassen van IPv6 voor websites en e-mail van de overheid. Hoewel de adoptiegroei van IPv6 voor zowel websites als e-mail in deze meting

een versnelling laat zien ten opzichte van de vorige meetpunten is er een flinke inhaalslag nodig om bij het streefbeeld van 100% adoptie voor het einde van dit jaar te komen.

Trend bereikbaarheid van websites en e-maildomeinen overheid via internetstandaard IPv6



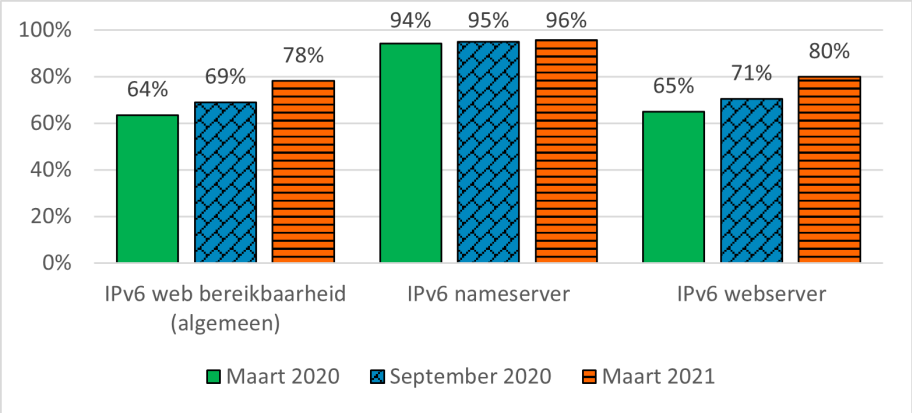
Tot eind 2021 is het IPv6 Team Overheid NL beschikbaar voor alle overheidsorganisaties die ondersteuning willen bij de overgang.

5.4. Bereikbaarheid overheidswebsites via IPv6

5.4.1. Gemiddelde bereikbaarheid

De gemiddelde bereikbaarheid van websites (78%) wordt met name geremd door de adoptie van IPv6 op webservers. De adoptiegraad is 80%. De adoptiegraad op nameservers is al relatief hoog, en dat illustreert dat het streefbeeld van 100% adoptie op dat aspect binnen bereik ligt.

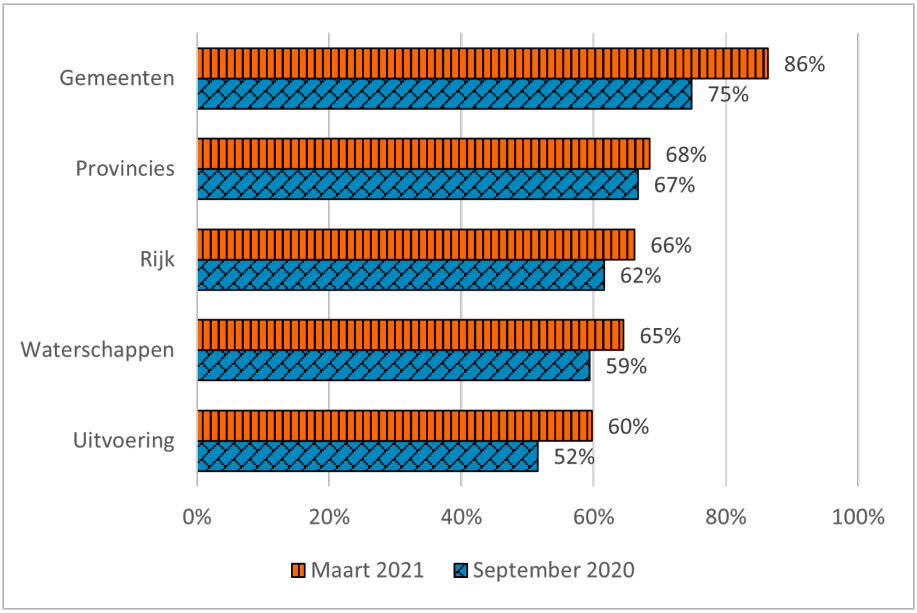
Bereikbaarheid overheidswebsites via IPv6



5.4.2. *Per overheidslaag*

De gemeenten scoren het beste op de bereikbaarheid van websites via IPv6 (86%). Dit komt met name door het ondersteuningsprogramma van VNG Realisatie waarmee gemeenten worden geholpen bij de implementatie van IPv6.

Bereikbaarheid websites via IPv6 per overheidslaag (van hoog naar laag)

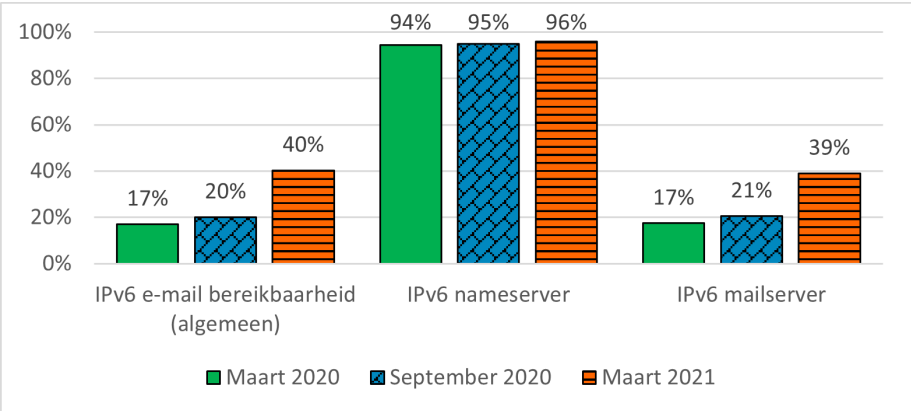


5.5. Bereikbaarheid e-maildomeinen via IPv6

5.5.1. *Gemiddelde bereikbaarheid*

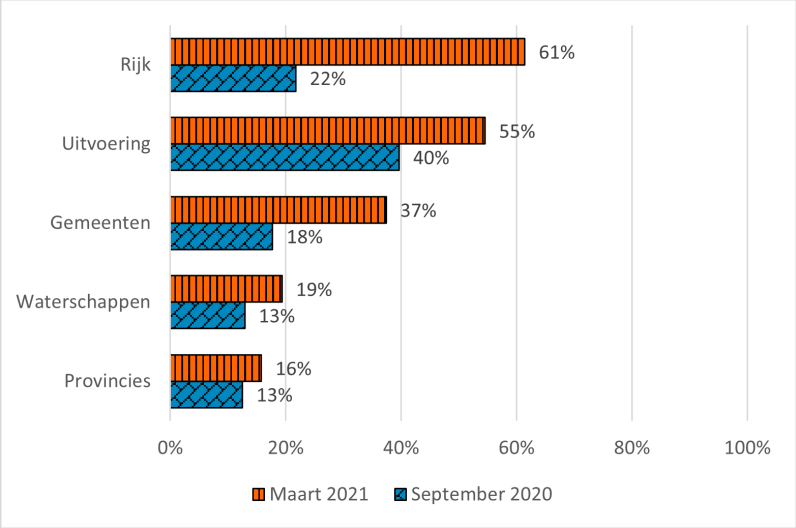
De gemiddelde bereikbaarheid van e-maildomeinen wordt met name geremd door de adoptie van IPv6 op mailservers. De adoptiegraad is na een sterke groei nu 39%. De adoptiegraad op nameservers is al relatief hoog, en dat illustreert dat het streefbeeld van 100% adoptie op dat aspect binnen bereik ligt.

Bereikbaarheid e-maildomeinen overheid via IPv6



5.5.2. *Per overheidslaag*

Bereikbaarheid e-maildomeinen via IPv6 per overheidslaag (van hoog naar laag)



Het Rijk en uitvoerders scoren gemiddeld het hoogst op IPv6. Dit komt onder meer doordat een aantal domeinen zijn aangesloten op de centrale mailvoorziening van Justitie en Veiligheid en DICTU die IPv6 ondersteunen.

Adoptiegroei binnen de categorieën Rijk en uitvoering is met name te behalen als shared service provider SSC-ICT ook stappen zet om de servers via IPv6 bereikbaar te maken.

Bij decentrale overheden zien we over het algemeen vaker gebruik van cloudmail-oplossingen. Hierbij is het zaak de leverancier actief te vragen om e-mail via IPv6 mogelijk te maken. Zo kunnen overheidsorganisaties die gebruik maken van Microsoft's Office 365 (Exchange Online) dit via de leverancier op verzoek laten activeren.

De originele publicatie van deze IV-meting (zie OBDO-210707-Agp-5a-Hamerstuk-Standaardisatie.pdf (forumstandaardisatie.nl)) bevat een uitgebreide bijlage (34 pagina's) met alle individuele resultaten per domeinnaam. Die is hier niet overgenomen.