Rapport

Monitor Open standaarden 2020

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_DT

Datum 30-11-2021

Deze versie van het document is op een later moment (meer) Digitoegankelijk gemaakt. Inhoudelijk is er niets aan de tekst veranderd.

Inhoudsopgave

1. Managementsamenvatting

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).

De kernvraag van de Monitor Open standaarden is: worden de verplichte open standaarden daadwerkelijk toegepast, en zo ja in welke mate? In grote lijnen luidt het antwoord op die vraag dit jaar:

- Het gebruik van de verplichte open standaarden is een aantal jaren geleidelijk verder toegenomen. Maar het einddoel dat alle overheden de relevante open standaarden toepassen is ook in 2020 nog niet bereikt, en de ontwikkeling lijkt al enige tijd te stagneren.
- Bij 94% van de 72 dit jaar onderzochte aanbestedingen werd om één of meer van de relevante open standaarden gevraagd, maar vaak niet om alle relevante standaarden. Dit is een iets betere score dan vorig jaar (89%). Van de 834 keer dat een open standaard voor een aanbesteding relevant was, werd daar in 45 % van de gevallen om gevraagd. Dat is een iets lagere score dan vorig jaar (50%) en dit percentage stagneert al zes jaar.
- Bij de meeste aanbestedingen was 'Leg uit' verplicht, omdat niet gevraagd is om alle relevante standaarden. In geen enkel jaarverslag is een expliciete 'Leg uit' opgenomen voor met name genoemde aanbestedingen. Dat is overigens al ruim tien jaar zo.
- Voor de meeste van de voorzieningen die dit jaar zijn onderzocht is inmiddels een behoorlijk niveau van toepassing bereikt: de dit jaar onderzochte 17 voorzieningen blijken voor een groot deel te voldoen aan de voor hen relevante open standaarden. Er waren in totaal 209 gevallen waarbij een open standaard voor een voorziening relevant was. De 13 ook eerder al onderzochte voorzieningen voldoen aan 82% van de voor hen relevante standaarden. Van de vier nieuw toegevoegde websites voldoet 67% daaraan.
- Over meer dan de helft van de standaarden op de lijst zijn geen gebruiksgegevens beschikbaar. Voor de standaarden waarover wèl gebruiksgegevens zijn verzameld (waaronder veel Internetveiligheidstandaarden) is het beeld positief: het gebruik groeit richting 90% à 100%, zij het in een lager tempo dan in het OBDO afgesproken.

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

1.1.1. 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 (begin 2020 waren dit er 42) 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 2020 (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 toegepast? En daarbuiten?

In deze rapportage worden gegevens gepresenteerd afkomstig uit een drietal bronnen:
- onderzoek van aanbestedingen in de periode juli 2019 t/m juni 2020,
- onderzoek van de toepassing van open standaarden bij overheidsbrede voorzieningen (situatie in de zomer van 2020),
- onderzoek naar gebruiksgegevens van een aantal open standaarden (zomer 2020).

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’).

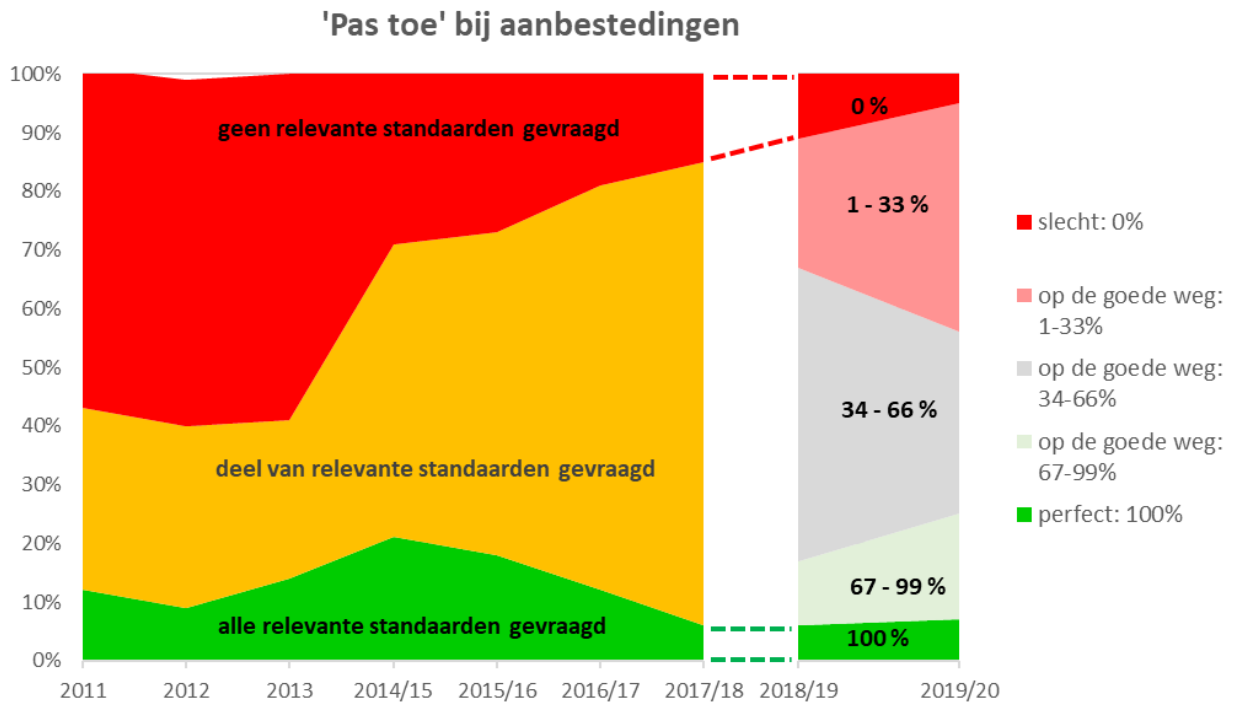
1.3. Open standaarden bij aanbestedingen (zie H3)

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 om vragen om een standaard nodig is om te kunnen kiezen voor een dienst of product dat aan die standaard voldoet. Voor de monitor is daarom, net als in de voorgaande jaren, een groot aantal aanbestedingen hierop onderzocht. Dit keer zijn 37 aanbestedingen van de rijksoverheid en uitvoeringsorganisaties en 35 aanbestedingen van mede-overheden onderzocht, in totaal 72 aanbestedingen (uit het 3e en 4e kwartaal van 2019 en 1e en 2e kwartaal van 2020). De resultaten worden beschreven in hoofdstuk 3.

Bij 7% van deze 72 aanbestedingen is gevraagd om alle relevante open standaarden (vorig jaar 6%). Het percentage aanbestedingen waarbij om een deel van de open standaarden is gevraagd – de grote middencategorie – is opnieuw iets toegenomen, van 83% vorig jaar naar 88% dit jaar. Het percentage aanbestedingen waarbij niet om een open standaard is gevraagd of waarbij sprake is van strijdigheid met het open standaardenbeleid, is in

vergelijking met de vorige meting verder teruggelopen van 11% naar 6%. En in tegenstelling tot vorig jaar zijn daar geen aanbestedingen bij die strijdig zijn met het standaardenbeleid. De mede-overheden deden het dit jaar, in tegenstelling tot vorig jaar, beter dan de Rijksoverheid: bij 29% van de aanbestedingen vroegen de mede-overheden om alle relevante standaarden of om tenminste tweederde daarvan (Rijk: 22%). De Rijksoverheid vroeg bij 57% van de aanbestedingen om geen enkele of om minder dan een derde van de relevante standaarden (mede-overheden: 32%).



Het overall beeld voor aanbestedingen is weliswaar redelijk positief, maar de ontwikkeling lijkt in twee opzichten in het midden te blijven steken. Ten eerste vallen veruit de meeste aanbestedingen (88%) in de middengroep (niet heel goed, niet slecht). Ten tweede werd van alle keren dat een open standaard voor een aanbesteding relevant was, daar in 45% van de gevallen om gevraagd.

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

goed nieuws	Bij 5 aanbestedingen (7%, vorig jaar 6%) is om alle relevante standaarden gevraagd. Het gaat om aanbestedingen van de Ministeries van BZK en Financiën, de Raad van State, de Rijksdienst voor Ondernemend Nederland en de Gemeente Gorinchem.
goed nieuws	Daarnaast werd bij 63 aanbestedingen (88%) om een deel van de relevante open standaarden gevraagd. Dat is iets hoger als vorig jaar (toen: 83%).
goed nieuws	Bij 4 aanbestedingen (dat is 6%, vorig jaar was het 11%) is om geen enkele relevante standaard gevraagd.
goed nieuws	Dit jaar waren er geen aanbestedingen strijdig met het open standaardenbeleid.
minder goed	Van de 834 keer dat een open standaard voor een aanbesteding relevant was werd daar in 45 % van de gevallen door de aanbesteder om gevraagd. Vorig jaar lag dit percentage nog op 50%, ook de jaren ervoor lag het rond de 45%.
goed nieuws	Het gemiddeld aantal relevante standaarden per aanbesteding steeg van 4,4 (2015) tot 11,6 in 2020. Er wordt dus elk jaar gevraagd om 45% van een groeiend aantal.

goed nieuws	Sommige standaarden (vooral NEN-ISO/IEC 27001 en 27002, HTTPS & HSTS en TLS) zijn veel vaker (90% tot 99%) relevant bij een aanbesteding dan andere. Deze zelfde vier standaarden worden bovendien – àls zij relevant zijn – het vaakst ook daadwerkelijk gevraagd (variërend van 53% tot 79%).
minder goed	Drie standaarden werden relatief weinig gevraagd: IPv4 & IPv6, STARTTLS & DANE en ODF werden vaak als relevant aangemerkt, maar er werd er slechts in respectievelijk 6%, 11% en 4% van die gevallen om de standaard gevraagd. Terwijl voor IPv4 & IPv6 en STARTTLS & DANE in het OBDO 'streefbeeldafspraken' zijn gemaakt (zie par. 5.2).

Een aantal aanbestedingen onderscheidde zich in positieve zin (zie ook paragraaf 3.2):

- Ministerie van BZK (facilitair managementinformatiesysteem): voldoet aan alle 15 relevante open standaarden.
- Raad van State (koppelfunctionaliteit, SaaS): alle 15 open standaarden gevraagd.
- Gemeente Gorinchem (applicatie vergunningverlening, toezicht en handhaving): voldoet aan alle 15 relevante open standaarden.
- RVO i.o.v. Netherlands Space Office (bewerken van satellietdata): alleen de Geo-standaarden relevant, en die zijn uitgevraagd.
- Belastingdienst (AIX-platform): alleen ISO 27001 en ISO 27002 relevant, en die zijn uitgevraagd.
- Bizob, gemeentelijk inkoopbureau (burgerzaken-applicatie, SaaS): bijna perfecte score, 15 van de 17 standaarden gevraagd (alleen IPv4/IPv6 en ODF niet), en aandacht voor open standaarden(beleid).
- Gemeente Purmerend (zaaksysteem): uitmuntende aanbesteding, 15 van de 17 standaarden gevraagd (ODF en Digikoppeling niet), en aandacht voor open standaarden(beleid).
- Veiligheidsregio Groningen (ondersteuning beheerprocessen, SaaS): 11 van de 13 relevante standaarden gevraagd (ODF en IPv4/IPv6 niet), en aandacht voor open standaarden(beleid).

'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. Voor zover bekend heeft nog geen enkele organisatie dit gedaan. Wel leggen sommige organisaties algemene verklaringen af over het gebruik van open standaarden. Maar dit is niet wat oorspronkelijk met het 'pas toe of leg uit' werd bedoeld.

Of er sprake is geweest van een geldige 'Leg uit' is op dit moment alleen na te gaan voor de onderzochte aanbestedingen uit het 3e en 4e kwartaal van 2019 (want over 2020 zal pas verantwoording afgelegd worden in het jaarverslag dat voorjaar 2021 verschijnt). Voor 33 van de aanbestedingen in het 3e en 4e kwartaal van 2019 was 'Leg uit' zonder twijfel 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 4 ministeries) geen sprake: nergens wordt een concrete afwijking van de 'pas toe of leg uit'-lijst genoemd, laat staan verantwoord.
minder goed	Bij 33 aanbestedingen was 'Leg uit' noodzakelijk. Bij 18% hiervan (vorig jaar: 15%) was sprake van een beperkte verantwoording: 6 van de 11 ministeries hebben een algemene alinea over 'pas toe of leg uit' opgenomen in het jaarverslag. Bij de overige 82% was geen sprake van enige vorm van 'Leg uit' (vorig jaar 85%).
goed nieuws	Het ministerie van BZK verwijst (net als vorig jaar) naar het jaarlijkse overzicht van Logius met de afwijkingen in haar ICT-producten en -diensten en bedrijfsvoering.

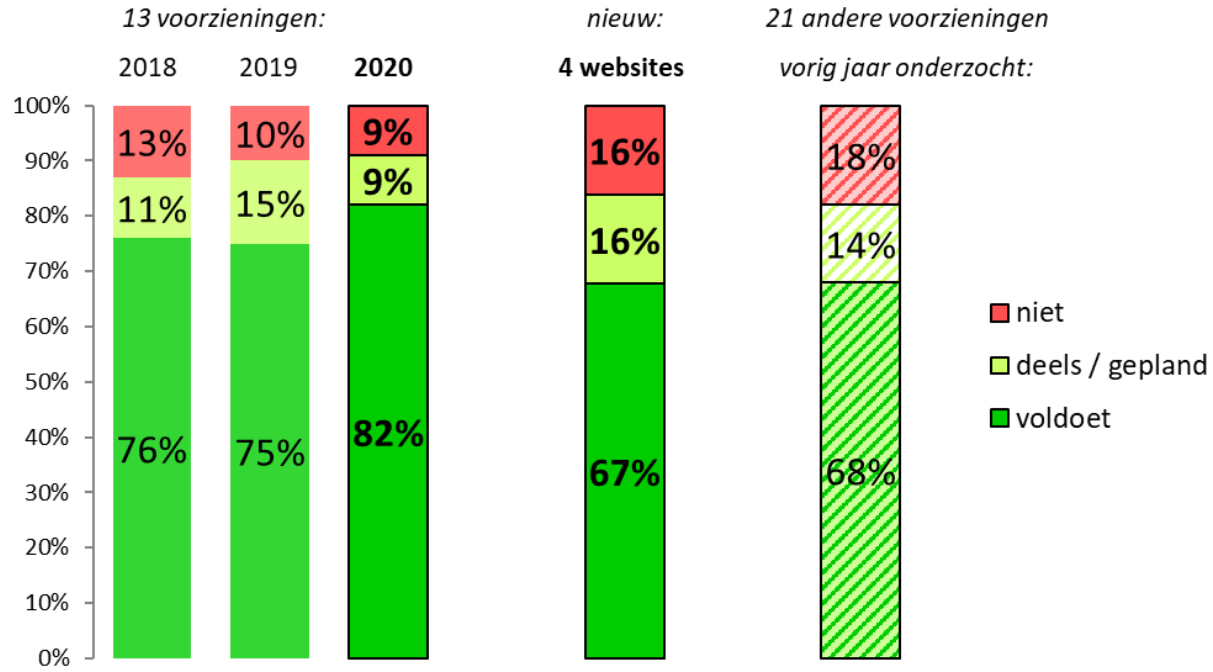
‘Leg uit’ is dus verplicht, maar elk jaar opnieuw blijkt dat geen enkele overheidsorganisatie zich daaraan houdt. Dat roept de vraag op, hoe dit beter in de praktijk gebracht kan worden en door wie.

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, zoals DigiD, MijnOverheid en Ondernemersplein. Daaronder ook vier websites van registraties (Handelsregister, PDOK, RDW en WOZ Waardeloket), die dit jaar nieuw toegevoegd zijn.

Het andere jaar (volgend jaar) onderzoeken we de 21 voorzieningen die vooral gericht zijn op de communicatie en gegevensuitwisseling tussen overheden onderling dan wel op de onderliggende infrastructuur.



De dit jaar onderzochte voorzieningen blijken voor een groot deel te voldoen aan de relevante open standaarden. Er waren in totaal 209 gevallen waarbij een open standaard voor een voorziening relevant was. Voor (alleen) de 13 ook eerder al onderzochte voorzieningen kan de ontwikkeling in de tijd worden gepresenteerd (de vier websites zijn voor het eerst onderzocht). De 13 voorzieningen doen het steeds beter: ‘voldoet’ is gestegen van 75% tot 82%. Het aantal gevallen waarin de voorziening deels aan de standaard voldoet of

daarvoor concrete plannen heeft is afgenomen van 15% vorig jaar naar 9% dit jaar. Samen met 'voldoet' is dat dit jaar dus 91%.

Van de vier nieuw toegevoegde websites voldoet 67% aan de relevante standaarden. Hier is dus nog veel ruimte voor verbetering. Dat geldt overigens ook voor de 21 voorzieningen die dit jaar *niet* zijn onderzocht (hun scores van vorig jaar zijn rechts in de figuur opgenomen).

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 12,3 standaarden per voorziening. Van de 43 standaarden op de lijst voor 'pas toe of leg uit' zijn er 26 relevant voor één of meer van de dit jaar onderzochte voorzieningen.
goed nieuws	Voor 14 van deze 26 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', 3 in het domein 'Document & (web)content', 2 onder de 'Stelselstandaarden', 2 in het domein 'Juridische verwijzingen' en de laatste in 'E-facturatie & administratie'.
minder goed	Vijf standaarden scoren relatief laag: van de voorzieningen waarvoor deze relevant zijn voldoet er geen enkele aan CMIS en aan de nieuwe standaard RPKI. Daarnaast voldoet slechts 33% aan NLCIUS en 47% aan IPv4 & IPv6.
goed nieuws	In de meeste gevallen voldoen de onderzochte voorzieningen aan de meeste ervoor relevante standaarden: de 13 ook eerder onderzochte voorzieningen voldoen aan 82% van de voor hen relevante standaarden. Van de vier nieuw toegevoegde websites voldoet 67% daaraan.
goed nieuws	Voor (alleen) de 13 ook eerder onderzochte voorzieningen kan de ontwikkeling in de tijd worden gepresenteerd. Deze 13 voorzieningen doen het steeds beter: 'voldoet' is gestegen van 75% tot 82%. Het aantal gevallen 'deels' of 'gepland' is afgenomen van 15% vorig jaar naar 9% dit jaar. Samen met 'voldoet' is dat voor de ook eerder onderzochte voorzieningen dit jaar dus 91%.
goed nieuws	Dit jaar voldoen 7 van de 17 voorzieningen geheel of gedeeltelijk aan alle relevante open standaarden en/of hebben concrete plannen om daaraan op korte termijn te voldoen. Eén daarvan is voor het eerst onderzocht: PDOK.nl.

Opvallend is, dat vooral standaarden uit het domein Internet & Beveiliging vaak relevant zijn (76% van alle gevallen). De domeinen Document & Webcontent (13%) en Stelselstandaarden (4%) volgen op grote afstand. De standaarden uit de zes andere domeinen zijn zelden relevant (samen slechts 7%). Wat betekent dat voor interoperabiliteit en voor leveranciers-onafhankelijkheid, de andere doelstellingen van het open standaardenbeleid?

Verschillende voorzieningen onderscheiden zich dit jaar in positieve zin:

- Zowel MijnOverheid (15 relevante standaarden) als DigiD (11 standaarden relevant) voldoen dit jaar aan alle relevante standaarden.
- 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 nieuw onderzochte website PDOK.nl (voor alle 14 relevante standaarden) en de website van het Handelsregister (voor 17 van de 19 relevante standaarden).

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 2020, 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 (69%, is wel stijgend), terwijl het OBDO-streefbeeld is dat 100% adoptie eind 2021 bereikt moet zijn.
goed nieuws	Voor verschillende standaarden uit het domein Document & (web)content is dit jaar een begin gemaakt met een nulmeting van gebruiksgegevens.

Halfjaarlijkse meting Internetveiligheidsstandaarden (zie ook Bijlage B4)
Uit de *'Meting Informatieveiligheidstandaarden overheid - september 2020'* blijkt dat het streefbeeld voor eind 2019 op het moment van de meting – september 2020 – nog niet volledig was gerealiseerd. Wel is de toepassing van een aantal standaarden gegroeid.

goed nieuws	Van de webstandaarden wordt HTTPS (redirect) het meest toegepast (98%), gevolgd door DNSSEC (94%) en HSTS (92%). TLS conform NCSC scoort lager (78%), en de deadline voor het OBDO-streefbeeld (eind 2018) is al lang gepasseerd.
goed nieuws	Van de mailstandaarden voor anti-phishing worden SPF (97%) en DKIM (96%) het meest toegepast, gevolgd door DMARC (92%) en SPF Policy (91%). En STARTTLS (99%) wordt van de mailstandaarden voor vertrouwelijkheid het meest toegepast.
minder goed	De andere mailstandaarden worden minder vaak gebruikt: DMARC Policy (66%) voor anti-phishing, en DNSSEC MX (66%), DANE (53%) en STARTTLS conform NCSC (42%) voor vertrouwelijkheid. Ook voor deze standaarden is de deadline voor het OBDO-streefbeeld reeds verstreken.

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 17 voorzieningen die dit jaar onderzocht zijn gecombineerd met de scores van de andere 21 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 acht van de vijftien standaarden uit het domein *Internet & beveiliging* is het overall beeld positief, en voor zes standaarden is het beeld wisselend. Voor STIX & TAXII 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* scoort één van de acht standaarden positief (PDF), twee scoren redelijk (CMIS en Open API Specification) en één scoort wisselend (SKOS). Drie standaarden scoren matig: Ades Baseline Profiles, ODF en OWMS. (Over Digitoegankelijk zijn dit jaar te weinig gegevens beschikbaar.)

Van de vier standaarden in het domein *E-facturatie & administratie* is het overall beeld voor XBRL positief, en voor NLCIUS is het matig. Voor de andere twee standaarden 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.

	Aanbestedingen	Voorzieningen	Gebruiksgegevens	Overall beeld
indicator:	*# aanbestedingen waarbij OS is gevraagd in % van # waarbij OS relevant is*	*# voorzieningen dat voldoet +deels +gepland in % van relevant*	*# overheden dat de standaard gebruikt in % van alle overheidsorganisaties*	
Internet & beveiliging:				
DKIM	24 %	96 %	van 89% naar 96%	**wisselend**
DMARC	24 %	88 %	van 82% naar 92%	**wisselend**
DNSSEC	27 %	91 %	van 93% naar 94%	**positief**
HTTPS	58 %	94 %	van 90% naar 98%	**positief**
en HSTS			van 79% naar 92%	**positief**
IPv6 en IPv4	7 %	58 %	van 48% naar 69%	**wisselend**
NEN-ISO\IEC 27001:2005nl	83 %	100 %	*[?]*	**positief**
NEN-ISO\IEC 27002:2007nl	83 %	100 %	*[?]*	**positief**
SAML	59 %	100 %	(van 868 naar 1016)	**positief**
SPF	24 %	96 %	van 95% naar 97%	**wisselend**
STARTTLS	16 %	57 %	cf: van 67% naar 42%	**wisselend**
en DANE			van 41% naar 53%	**wisselend**
STIX & TAXII			*[?]*	[?]
TLS	58 %	88 %	cf: van 89% naar 78%	**positief**
WPA2 Enterprise	(100 %)	(100 %)	(van 529 naar 563)	**positief**
Document & (web)content:				
Ades Baseline Profiles	25 %	40 %	*NIET ONDERZOCHT*	**matig**
CMIS	67 %	43 %	*NIET ONDERZOCHT*	**redelijk**
Digitoegankelijk *)	60 %	*NIET ONDERZOCHT*	*[?]*	[?]
ODF	10 %	60 %	van 8% naar 24%	**matig**
OpenAPI Specification	60 %	92 %	*[?]*	**redelijk**
OWMS		75 %	van 36% naar 28%	**matig**
PDF	59 %	96 %	bijna 100%	**positief**
SKOS		83 %	*[?]*	**wisselend**
E-facturatie & administratie:				
NLCIUS	25 %	13 %	(toegenomen)	**matig**
SETU	0 %	(100 %)	*[?]*	[?]
WDO Datamodel			*[?]*	[?]
XBRL	(100 %)	(100 %)	(toegenomen)	**positief**
Stelselstandaarden:				
Digikoppeling	33 %	86 %	van 90% naar 91%	**positief**
Geo−standaarden	33 %	100 %	(toegenomen)	**positief**
StUF	100 %	82 %	(licht toegenomen)	**positief**
Water & Bodem:				
Aquo Standaard		(100 %)	(stabiel)	**wisselend**
SIKB 0101			*[?]*	[?]
SIKB 0102			*[?]*	[?]
Bouw:				
COINS	(50 %)		*[?]*	[?]
IFC	(33 %)		*NIET ONDERZOCHT*	[?]
NLCS	(0 %)		(toegenomen)	[?]
Visi			(toegenomen)	[?]
Juridische verwijzingen:				
BWB	(0 %)	100 %	(toegenomen)	**wisselend**
ECLI	(50 %)		(toegenomen)	**wisselend**
JCDR	(0 %)	(100 %)	(toegenomen)	[?]
Onderwijs & loopbaan:				
E−portfolio	0 %		(stabiel)	[?]
NL LOM	(0 %)		(toegenomen)	[?]
Overig:				
EML_NL	(0 %)		(veel toegepast)	[?]

2. Inleiding: beleidscontext en onderzoeksopzet

2.1. Waarom open standaarden?

Voor 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.

Om deze redenen is voor overheden het gebruik van deze open standaarden verplicht, via het 'pas toe of leg uit'-beleid. Dat heeft onder meer vorm gekregen

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 moet hierover 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':

> *Gebruik 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 Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten). De Tweede Kamer wil dat de overheid meer gebruik maakt van 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 College Standaardisatie. 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 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".*

Deze resultaatafspraak was van toepassing op gemeenten, provincies en waterschappen.

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 2020

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 2019/2020,
- onderzoek van de toepassing van open standaarden bij overheidsbrede voorzieningen,
- onderzoek naar overige gebruiksgegevens van een aantal open standaarden.

Het eindrapport zelf voldoet overigens aan de eisen van DigiToegankelijk.

Onderzoek van aanbestedingen in 2019/2020
Dit jaar zijn aanbestedingen onderzocht van de rijksoverheid (en uitvoeringsorganisaties) en van mede-overheden uit de periode juli 2019 tot en met juni 2020. Er zit soms een organisatie bij die strikt genomen niet verplicht is om open standaarden van de lijst toe te passen, maar dit wel doet. Dit jaar bijvoorbeeld de Raad van State, een hoog college van staat. Voor een breder beeld van het gebruik van open standaarden betrekken we deze aanbestedingen soms ook in het onderzoek.

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 zijn 17 voorzieningen onderzocht die belangrijk zijn voor de communicatie en gegevensuitwisseling met burgers en bedrijven, met daarbij voor het eerst ook vier websites van registraties (Handelsregister, PDOK, RDW en WOZ Waardeloket). 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 de voorzieningen die vooral gericht zijn op communicatie en gegevensuitwisseling tussen overheden onderling of op de onderliggende infrastructuur.)

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. Dit jaar is dat net als vorig jaar gedaan door 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: 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 2020 is voor inmiddels het negende 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 2020) omvatte de 'pas toe of leg uit'-lijst 45 open standaarden. Voor dit onderzoek zijn er 41 relevant. De overige vier staan namelijk pas recent op de lijst en daardoor was bij de voor deze monitor beoordeelde aanbestedingen uitvragen van deze standaarden nog niet aan de orde. Concreet gaat het om de volgende vier standaarden: GWSW, NL GOV Assurance profile for OAuth 2.0, REST API Design Rules en RPKI.

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 ('leg uit' in jaarverslagen) en 3.5 (mate waarin open standaarden relevant waren bij de onderzochte aanbestedingen).

3.1. Onderzoek van aanbestedingen

Dit jaar is, net als in de voorgaande jaren, onderzoek gedaan naar de aanbestedingen in de periode Q3 en Q4 2019 en Q1 en Q2 2020 door het Rijk (met inbegrip van onder andere uitvoeringsorganisaties, agentschappen en ZBO's) en door de decentrale overheden. 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 (ICT Recht) heeft de second opinion op de Rijks-aanbestedingen geleverd.

Onderzocht zijn vooral aanbestedingen die op tenderned.nl zijn gepubliceerd. Het betreft daardoor veelal Europese aanbestedingen, drempelwaarden daarvoor zijn voor de rijksoverheid > € 144.000 en voor decentrale overheden > € 221.000). Deze waarden worden telkens voor twee jaar door de Europese Commissie vastgesteld. Per 1 januari 2020 zijn de drempelwaarden voor de Europese Commissie verlaagd: voor de rijksoverheid > € 139.000 en voor decentrale overheden > € 214.000.

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 bijna alle gevonden relevante aanbestedingen van Rijksoverheid en uitvoeringsorganisaties beoordeeld. Dit jaar vielen ongeveer 15 aanbestedingen door de Rijksoverheid buiten de steekproef. Het aantal beoordeelde aanbestedingen van de Rijksoverheid (37) ligt dit jaar min of meer op het gebruikelijke niveau. Dat neemt niet weg dat ook dit jaar een beperkt aantal (5) aanvankelijk geselecteerde aanbestedingen bij nader inzien door de experts als 'niet beoordeelbaar' gekwalificeerd moest worden. Daarbij gaat het om de volgende casuïstiek:

- een aanbesteding lijkt niet over ICT te gaan maar over inhuur van personeel voor de eerstelijns diensten van het klantcontactcentrum;
- een andere aanbesteding betreft de aanschaf van ICT voor militair operationeel gebruik. In de Instructie Rijksdienst inzake aanschaf van ICT-diensten en ICT-producten (art. 3) staat dat voor dergelijke aanbestedingen geen verantwoording afgelegd hoeft te worden over het gebruik van open standaarden;
- een aanbesteding is voortijdig stopgezet omdat de opdracht niet werd gegund. Daarnaast lijkt het hier te gaan om de inhuur van personeel dat ondersteuning biedt op de werkvloer;
- vergelijkbaar met de vorige aanbesteding: ook hier is sprake van voortijdig stopzetten en daar komt bij dat in de aanbestedingsdocumenten niet is ingegaan op de ICT-producten die moeten worden onderhouden, dus kan geen inschatting gemaakt worden welke open standaarden hiervoor relevant zijn;
- het betreft de ontwikkeling van een model. Dit model kan niet worden gezien als een ICT-product of ICT-dienst en er zijn ook geen IT-componenten onderdeel van de aanbesteding.

Voor de mede-overheden wordt elk jaar een steekproef getrokken uit de (vele) gevonden aanbestedingen. Dit jaar zijn 35 aanbestedingen van mede-overheden beoordeeld (vorig jaar 37). Met ingang van de monitor 2018 is gekozen voor een verdubbeling van het aantal te onderzoeken aanbestedingen door mede-overheden om daar beter zicht op te krijgen.

In totaal zijn 72 aanbestedingen beoordeeld: 37 van het Rijk (departementen, uitvoerings-organisaties, agentschappen, ZBO's) en een steekproef van 35 aanbestedingen van mede-overheden. De 72 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 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, mantel-overeenkomsten);
- 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 in Bijlage B2. Bij wijze van bloemlezing enkele kleurrijke voorbeelden van aanbestedingen:

- Hielprik-opdrachten worden vanuit het Praeventis systeem van het RIVM digitaal aan de JGZ-organisaties verzonden. Maar de JGZ organisaties op hun beurt voeren nu nog handmatig gegevens weer terug in Praeventis via de post. Deze aanbesteding betreft een applicatie waarmee de screeners namens de JGZ gegevens digitaal aan het Praeventis systeem kunnen leveren. De opdrachtnemer wordt geacht de hosting van de applicatie te verzorgen (agentschap / Rijk);
- Het ten behoeve van het 24/7 BZ ContactCenter implementeren, leveren en beheren van een Cloud dienstverlening voor het ontsluiten en gebruiken van diverse functionaliteiten op het gebied van ContactCenter, Workforce Management (WFM), kennisbank en casemanagement. Een team staat de BZ-klant, 24 uur per dag zeven dagen per week te woord om al hun vragen te beantwoorden, telefonisch, via e-mail, social media en WhatsApp. Ook is het 24/7 BZ ContactCenter verantwoordelijk voor de content op de websites www.nederlandwereldwijd.nl en www.netherlandsandyou.nl, de primaire online kanalen voor klanten (ministerie / Rijk);
- Het betreft een aanbesteding voor de ontwikkeling van een Individual- or Agent-Based model (IBM /AMB) voor zeevogels die tegen windmolens botsen op de Noordzee. RWS wil zo accuraat mogelijk in kunnen schatten hoeveel vogelsterfte ontstaat door botsingen tegen windmolens. Het doel van de huidige opdracht is om een IBM / ABM-model voor de kleine mantelmeeuw te ontwikkelen en de internationale wenselijkheid en de haalbaarheid van een IBM / ABM voor drie aanvullende (prioriteits) zeevogelsoorten te bepalen (agentschap / Rijk);
- De opdracht betreft examenafnamesoftware (SAAS) ten behoeve van de afname van inburgeringsexamens en de Naturalisatietoets in Nederland en het buitenland. De logistiek en administratie van deze examens voert DUO uit met behulp van een informatiesysteem. In dit geval betreft dat een specifiek voor DUO ingerichte SAP-omgeving. Wijze van examineren is zowel online (inburgeringsexamens) als offline (basisexamen inburgering, Naturalisatietoets) (agentschap / Rijk);
- De gemeente is op zoek naar een handhaafsysteem om haar handhavingstaken zoveel als mogelijk digitaal en informatie gestuurd uit te voeren, te registreren en te ondersteunen. In ieder geval op een wijze die het mobiel digitaal handhaven mogelijk

maakt, zodanig dat handhavers op straat direct beschikking hebben over alle voor hun werk relevante informatie (input) en dat handhavers een zo groot mogelijk deel van de administratieve afhandeling en rapportages op straat kunnen uitvoeren (output) (gemeente).

Toetsingskader

Het onderzoek is gebaseerd op de gepubliceerde, openbare informatie over de aanbestedingen. Dat is immers de informatie waarop de aanbieders zich (in elk geval in eerste instantie) hebben moeten baseren. Dat impliceert dat informatie uit bijvoorbeeld een Nota van Inlichtingen ook niet mee mag wegen bij het opmaken van de beoordeling[1].

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 (a) de aanbesteder 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. 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 2019 heeft plaatsgevonden (zie paragraaf 3.4). 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 administratie en moet hierover verantwoording afgelegd worden in het jaarverslag. Afwijkingen zijn overigens alleen mogelijk bij redenen van bijzonder gewicht.

3.2. 'Pas toe' bij aanbestedingen in 2019/2020

In de 72 aanbestedingen die dit jaar zijn beoordeeld had in totaal om 834 open standaarden gevraagd moeten worden, feitelijk is er echter 377 keer om een open standaard gevraagd. Dat is dus 45% daarvan (zie de groene rijen midden in Tabel 1), dat is lager dan in 2019 (50%). Deze afname van 50% naar 45% wordt vrijwel geheel veroorzaakt door een afname van het uitvraag-percentage bij de Rijks-aanbestedingen: van 50% naar 39% (het percentage voor de mede-overheden is met 50% gelijk aan vorig jaar). Met het huidige percentage van 45% komen we weer op het niveau terecht van de percentages van de jaren 2014 tot en met 2018, fluctuerend tussen 43% en 45%. In de jaren daarvoor (2012 en 2013) lag dit percentage beduidend lager, op respectievelijk 30% en 25%.

[1] Voor de volgende monitor in 2021 zullen wij over dit uitgangspunt nog een nadere discussie hebben.

'Pas toe' per aanbesteding

Bij 5 van de 72 aanbestedingen (7%, zie de grijze kolommen in Tabel 1; vorig jaar 6%) werd om alle relevante open standaarden gevraagd ('perfect'), dat is 'pas toe' in strikte zin. Dit waren 2 aanbestedingen door een ministerie, 1 door een agentschap, 1 door een Hoog College van Staat en 1 door een gemeente. Daarnaast werd bij 63 aanbestedingen (88%; vorig jaar 83%) gevraagd om een deel van de voor die aanbesteding relevante standaarden ('op de goede weg'). Bij de resterende 4 aanbestedingen (6%; vorig jaar 11%) - waarbij één of meer open standaarden relevant waren - werd om geen enkele open standaard gevraagd en was in de aanbestedingsdocumenten in het geheel geen aandacht voor open standaarden-beleid terug te vinden ('slecht').

Tabel 1: 'Pas toe' en 'leg uit' bij aanbestedingen 2019/2020

(Bron: onderzoek aanbestedingen juli 2019 t/m juni 2020, uitgevoerd zomer 2020)

	Rijksoverheid		Mede-overheden		**Totaal 2019/2020**		Totaal 2018/2019	
	#	%	#	%	#	%	#	%
totaal aantal beoordeelde aanbestedingen waarbij OSn relevant waren	**37**	100%	**35**	100%	**72**	**100%**	72	100%
*** perfect**: alle relevante OSn gevraagd	4	11 %	1	3 %	**5**	**7 %**	4	6 %
*** op de goede weg**: deel van relevante OSn gevraagd	30	81 %	33	94 %	**63**	**88 %**	60	83 %
- op weg naar perfect (67-99%)	4	11 %	9	26 %	**13**	**18 %**	8	11 %
- de middenmoot (34-66%)	8	22 %	14	40 %	**22**	**31 %**	36	50 %
- nog een heel eind te gaan (1-33%)	18	49 %	10	29 %	**28**	**39 %**	16	22 %
geen relevante OSn gevraagd, waarvan	3	8 %	1	3 %	**4**	**6 %**	8	11 %
*** matig**: er is wel algemene aandacht voor architectuur-kaders en/of OSn-beleid	0	0 %	0	0 %	**0**	**0 %**	1	1 %
*** slecht**: geen aandacht voor OSn-beleid	3	8 %	1	3 %	**4**	**6 %**	2	3 %
*** heel slecht**: strijdig met OSn-beleid	0	0 %	0	0 %	**0**	**0 %**	5	7 %
totaal aantal relevante OSn	358	100%	476	100%	**834**	**100%**	738	100%
totaal aantal gevraagde relevante OSn	141	39 %	236	50 %	**377**	**45 %**	368	50 %
niet alle OSn gevraagd => Leg Uit vereist	33		34		**67**		68	
*idem, maar beperkt tot Q3+Q4 2019 *)*	*17*	*100%*	*16*	*100%*	***33***	***100%***	*33*	*100%*
- concrete verantwoording in jaarverslag	*0*	*0 %*	*0*	*0 %*	***0***	***0 %***	*0*	*0 %*
- beperkte verantwoording in jaarverslag	*1*	*6 %*	*0*	*0 %*	***1***	***3 %***	*5*	*15 %*
- geen Leg Uit in jaarverslag	*16*	*94 %*	*16*	*100%*	***32***	***97 %***	*28*	*85 %*

NB: groene gearceerde rijen betreft aantallen standaarden, rest van tabel aantallen aanbestedingen

**) Controle op de toepassing van 'leg uit' was uiteraard alleen mogelijk voor aanbestedingen uit 2019, waarover verantwoording had moeten worden afgelegd in het Jaarverslag 2019.*

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' een nadere nuancering aangebracht:

- 'op weg naar perfect' (aanbestedingen waarbij om 67% tot 99% van de relevante standaarden gevraagd is; zie de percentages in 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:

- 18% van alle aanbestedingen is op weg naar perfect, 31% behoort tot de 'echte' middenmoot en voor 39% geldt dat er nog een heel eind te gaan is;
- de mede-overheden laten een gunstiger beeld zien dan de rijksoverheid: het aandeel 'op weg naar perfect' is voor de mede-overheden relatief groter, het aandeel 'nog een heel eind te gaan' juist beduidend lager;
- in vergelijking met de vorige monitor is het aandeel achterblijvers ("nog een heel eind te gaan") flink toegenomen. Daar staat als pluspunt tegenover dat het aandeel 'op weg naar perfect' licht is toegenomen. De omvang van de middenmoot is behoorlijk teruggelopen.

De uit vorige monitors gangbare onderverdeling van de categorie 'geen relevante open standaarden gevraagd' is wel gehandhaafd, maar in een iets aangepaste vorm (die vorig jaar voor het eerst is gebruikt):

- matig: er is algemene aandacht voor architectuur-kaders en/of open standaardenbeleid (0%, vorig jaar 1%),
- slecht: er is geen aandacht voor open standaardenbeleid (6%, vorig jaar nog 3%);
- heel slecht: strijdig met het open standaardenbeleid: (dit jaar geen enkele aanbesteding, vorig jaar 7%).

Alles bij elkaar genomen is deze verzamelcategorie 'geen relevante open standaarden gevraagd' dus kleiner geworden.

Uit het horizontaal met groen gemarkeerde blok in de tabel valt op dat het aantal standaarden dat per aanbesteding relevant wordt geacht dit jaar wederom duidelijk hoger ligt dan vorig jaar (gemiddeld 11 à 12 standaarden per aanbesteding, vergeleken met ruim 10 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 ook bij het Rijk maar met name bij de mede-overheden.

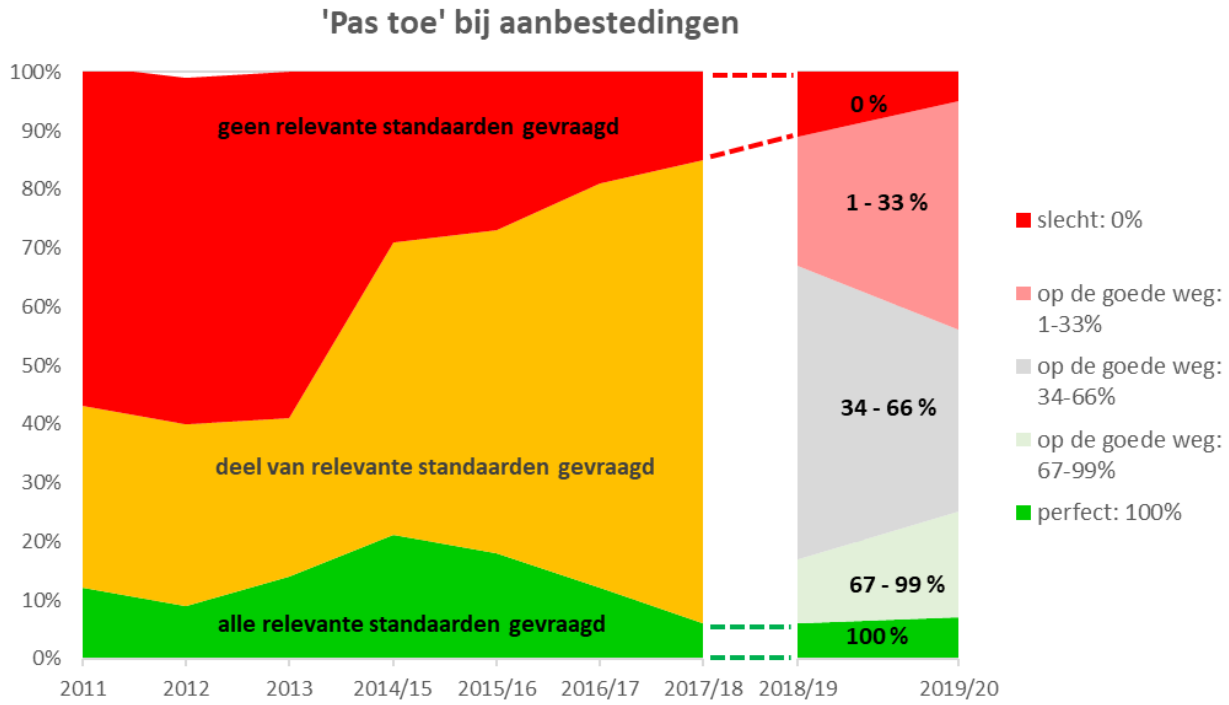
Tot slot is opvallend aan Tabel 1 dat het aandeel bevraagde standaarden voor het Rijk en mede-overheden weer uit elkaar is gegroeid (39% versus 50%) terwijl dat vorig jaar nog gelijk was (50% tegen 50%). In de vorige monitor is al opgemerkt dat deze variabele door de jaren heen behoorlijke fluctuaties laat zien zonder dat sprake is van een eenduidige ontwikkelingsrichting. Opvallend in deze jaargang van de monitor is wel dat het Rijk een duidelijk lagere score laat zien dan de mede-overheden. Daarvan was in de achterliggende jaren niet eerder sprake.

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

- Het aantal aanbestedingen waarbij om alle relevante standaarden is gevraagd is met 1 gestegen tot 5 (7%). Deze min of meer stabiele score in vergelijking met de afgelopen drie jaren (telkens 6%) volgt op een periode waarin drie jaren op rij sprake is van een afname (zes jaar geleden lag dit percentage nog op 21%). De stabilisatie doet zich zowel bij de Rijksoverheid als bij de mede-overheden voor.
- De midden-categorie - dit jaar wederom gekwalificeerd als 'op de goede weg' - is ook bij deze monitor weer de grootste met 88% (vorig jaar 83%). Binnen deze middencategorie is echter het aantal aanbestedingen die nog een heel eind te gaan hebben toegenomen, voornamelijk toe te schrijven aan de aanbestedingen Rijk.
- Het aantal aanbestedingen waarbij om geen enkele standaard is gevraagd (met oordelen 'matig' dan wel 'slecht') is iets opgelopen, van 4 % vorig jaar naar 6 % dit jaar.
- Deze ongunstige ontwikkeling wordt voor een belangrijk deel gecompenseerd door het feit dat dit jaar bij geen enkele aanbesteding sprake is van strijdigheid met het open standaardenbeleid. Vorig jaar waren dat er nog 5 (7 %).

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

Figuur 2: 'Pas toe' bij aanbestedingen, 2011 - 2019/20

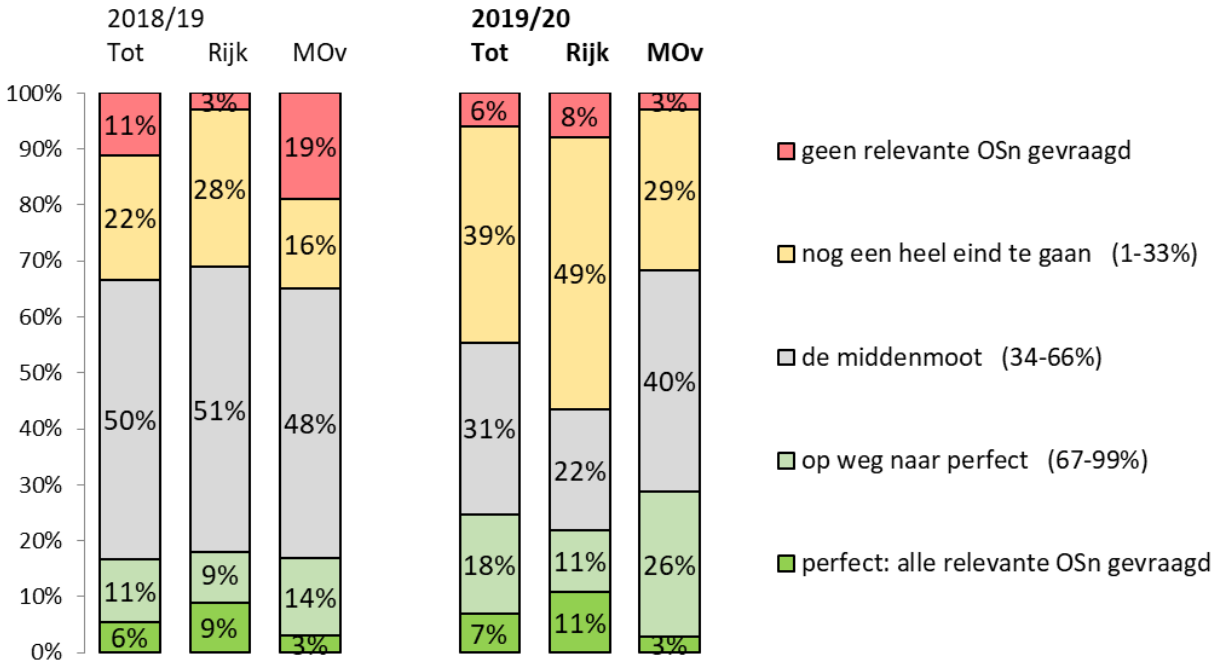


De middengroep 'op de goede weg', bestaande uit aanbestedingen waarbij wel om één of meer van de relevante standaarden gevraagd werd maar niet om alle, is inmiddels gegroeid tot 88% van alle aanbestedingen (zie Figuur 2). We hebben daarbinnen net als vorig jaar nog een nadere onderverdeling gemaakt tussen 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 middensegment van de middengroep niet langer het grootst is maar dat dat nu het segment met de kwalificatie 'nog een heel eind te gaan' is.

De mede-overheden deden het dit jaar, in tegenstelling tot vorig jaar, beter dan Rijk en uitvoeringsorganisaties: bij 29% van de aanbestedingen vroegen de mede-overheden om alle relevante standaarden of om tenminste tweederde daarvan (Rijk: 22%). De Rijksoverheid vroeg bij 57% van de aanbestedingen om geen enkele of om minder dan een derde van de relevante standaarden (mede-overheden: 32%).

In Figuur 3 zijn duidelijk de verschillen te zien tussen enerzijds Rijk en uitvoeringsorganisaties en anderzijds de mede-overheden:

- bij 49% van de Rijks-aanbestedingen werd slechts om een klein deel van de relevante standaarden gevraagd en bijna de helft van de Rijks-aanbestedingen heeft daarom 'nog een heel eind te gaan' (mede-overheden: 29%);
- van de aanbestedingen door mede-overheden daarentegen valt juist een groot deel (40%) in 'de middenmoot' (Rijk: 22%) en ook nog een flink deel (26%) in 'op weg naar perfect' (Rijk: 11%);
- bij 11% van de Rijks-aanbestedingen is om alle relevante standaarden gevraagd en deze vallen dus in de categorie 'perfect' (mede-overheden: 3%);
- vergeleken bij vorig jaar valt om te beginnen op, dat bij veel minder aanbestedingen van mede-overheden om geen enkele van de relevante standaarden is gevraagd (gedaald van 19% naar 3%);
- zowel bij het Rijk als bij mede-overheden nam de categorie 'nog een heel eind te gaan' sterk toe (respectievelijk van 28% naar 49% , en van 16% naar 29%);
- 'de middenmoot' is vooral bij het Rijk flink afgenomen (van 51% tot 22%);
- bij het Rijk zijn de categorieën 'op weg naar perfect' en 'perfect' licht gegroeid, bij de mede-overheden is 'op weg naar perfect' gegroeid van 14% tot 26%.



Alle cijfers over 'pas toe' bij aanbestedingen overziend is het beeld wisselend: er zijn positieve signalen maar daar staan ook enkele minder positieve signalen tegenover.

- Het aantal aanbestedingen dat als 'perfect' of 'op weg naar perfect' werd beoordeeld is toegenomen (van 17% tot 25%). Kanttekening daarbij: hierop werd enkele jaren terug hoger gescoord;
- En het aantal aanbestedingen waarbij geen enkele relevante standaard werd gevraagd nam verder af van 11% tot 6%;
- Binnen de grote middengroep is echter het aantal aanbestedingen waarbij slechts om een klein deel van de relevante standaarden werd gevraagd ('nog een heel eind te gaan') toegenomen van 22% tot 39%;
- Van de 834 keer dat een open standaard voor een aanbesteding relevant was werd daar in 45% van de gevallen om gevraagd (vorig jaar 50%), doordat het percentage 'gevraagd' bij Rijks-aanbestedingen daalde van 50% tot 39%.

Enkele goede voorbeelden

Ook dit jaar brengen we weer enkele goede voorbeelden van aanbestedingen voor het voetlicht. Drie aanbestedingen steken er dit keer met kop en schouders boven uit: een aanbesteding van het ministerie van BZK, één van de Raad van State en een aanbesteding van de gemeente Gorinchem. In elk van deze drie gevallen is sprake van een complex beeld van relevante standaarden, die ook alle zijn uitgevraagd. Ook de Rijksdienst voor Ondernemend Nederland (RVO), uitvoeringsorganisatie van het ministerie van EZ & Klimaat en de Belastingdienst zijn in die zin 'taart-kandidaat' dat ook zij een 100%-uitvraag laten zien bij een aanbesteding, ook al is het aantal relevant geachte standaarden bij die twee casus zeer klein. Aanvullend hierop volgt nog een drietal aanbestedingen waarbij weliswaar niet 100% werd uitgevraagd, maar die wel een zeer positieve beoordeling kregen van de beoordelende experts: Bizob, de gemeente Purmerend en de Veiligheidsregio Groningen.

Ministerie van BZK. Het betreft een aanbesteding voor de levering, implementatie (waaronder tenminste: ontsluiting, integratie, configuratie, migratie en conversie), beheer, onderhoud, door-ontwikkeling en hosting van een facilitair managementinformatiesysteem (FMIS). Daarbij inbegrepen een gebruiksvriendelijk gebruikersportaal en mobiele app's, geleverd op basis van SaaS dienstverlening. Dit alles ter ondersteuning van de facilitaire processen van FMHaaglanden.
De volgende standaarden zijn alle relevant en uitgevraagd: ISO 27001, ISO 27002, HTTPS en HSTS, TLS, Digitoegankelijk, DNSSEC, IPv4/IPv6, ODF, PDF, OpenAPI, DKIM, DMARC, SPF, STARTTLS & DANE en SAML.

Raad van State. De Raad wenst data-uitwisseling mogelijk te maken, via één koppeldienst, tussen hun SaaS- en "On Premise"-oplossingen. Om dergelijke data-uitwisseling mogelijk te maken is een koppelfunctionaliteit en/of een berichtenmakelaar nodig. Deze functionaliteit gaat afgenomen worden als één SaaS-oplossing bij de leverancier. De beoordelaars van de aanbestedingen hebben bij deze casus de volgende kanttekening gemaakt: "een zeer goede aanbesteding met duidelijke verwijzing naar de pas-toe-of-leg-uit lijst. Nog beter zou zijn als de tabel met open standaarden ook een toelichting per standaard zou bevatten op de reden van relevantie met deze aanbesteding. Nu bevat de tabel alleen generieke een beschrijving van de standaard zoals die ook op de website van Forum Standaardisatie is te vinden."
De volgende standaarden worden relevant geacht: ISO 27001, ISO 27002, HTTPS en HSTS, TLS, Digikoppeling, IPv4/IPv6, CMIS, DNSSEC, ECLI, Open API, SAML, COINS, Digitoegankelijk, PDF en StUF. Deze standaarden zijn alle uitgevraagd.

Gemeente Gorinchem. Dit betreft een aanbesteding voor het leveren, implementeren en onderhoud/ondersteuning van een standaard on-premise ICT-applicatie ten behoeve van de vergunningverlening, toezicht en handhaving (VTH). De ICT-applicatie moet aangesloten worden op het Digitaal Stelsel Omgevingswet (DSO). Door de beoordelaars wordt het volgende opgemerkt: "in bijlage (…) worden de standaarden beschreven die gelden voor het VTH-systeem. Wel staan er een aantal standaarden in de lijst die juist niet relevant zijn voor deze aanbesteding. Voor sommige standaarden wordt verwezen naar de PTOLU-lijst van het BFS."

De volgende standaarden zijn relevant en alle uitgevraagd: ISO 27001, ISO 27002, HTTPS en HSTS, TLS, DNSSEC, Digikoppeling, Geo, OpenAPI, DKIM, DMARC, SPF, STARTTLS & DANE, StUF en SAML.

Bizob (een van de eerste gemeentelijke inkoopbureaus van Nederland.). De overeenkomst bestaat uit het werkend opleveren en vervolgens het ter beschikking stellen van een burgerzaken-applicatie, inclusief onderhoud en ondersteuning. De burgerzaken-applicatie draait off-premise, waarbij de verantwoordelijkheid voor de hosting en onderhoud van de burgerzakenapplicatie bij de inschrijver ligt (SAAS). Voorbeelden van kerntaken die de applicatie ondersteunt zijn: persoonsinformatie/identiteits-management, document verstrekking en e-diensten via webformulieren.
Commentaar van de beoordelaars: "Zeer goede aanbesteding. Bijna perfecte score. Er wordt uitvoerig verwezen naar Forum Standaardisatie, open standaarden(beleid) en de pas-toe-of-leg-uit lijst."
De volgende relevante standaarden zijn uitgevraagd: Digitoegankelijk, Digikoppeling, DNSSEC, HTTPS en HSTS, TLS, ISO 27001, ISO 27002, SAML, SPF, DKIM, DMARC, STARTTLS & DANE, OpenAPI, PDF en StUF.
Twee standaarden zijn niet uitgevraagd: IPv4/IPv6 en ODF.

Gemeente Purmerend. De aanbesteding betreft een zaaksysteem (zaakgericht werken). De gemeente Purmerend zoekt een nieuw Zaaksysteem omdat het huidige systeem is verouderd en het contract met de leverancier afloopt. De gemeente spreekt nadrukkelijke de wens uit dat het zaaksysteem moet aansluiten met de ontwikkelingen rond Common Ground, zoals het onafhankelijk maken van gegevens van processen en koppelingen die worden gemaakt op basis van de API-technologieën.
Het commentaar van de beoordelaars luid als volgt: "Dit is een uitmuntende aanbesteding. Het niet vragen van Digikoppeling mag niet zwaar wegen, aangezien in eis (…) is te lezen dat de gemeente gebruik maakt van 2Secure van EnableU. Deze partij zorgt voor de Digikoppeling implementatie voor deze gemeente. In de aanbesteding wordt expliciet verwezen (als eis) naar de open standaarden van Forum Standaardisatie.
Van alle relevant geachte open standaarden (DNSSEC, Digitoegankelijk, HTTPS en HSTS, TLS, IPv4/IPv6, ISO 27001, ISO 27002, CMIS, StUF, PDF, SAML, SPF, DKIM, DMARC, STARTTLS & DANE, ODF en Digikoppeling) worden alleen de laatste twee niet uitgevraagd.

Veiligheidsregio Groningen. Veiligheidsregio Groningen (VRG) wil in 2020 een technisch platform voor de ondersteuning van de beheerprocessen van hun teams Techniek & Ondersteuning (T&O), Facilitaire Zaken (FZ) en Informatiemanagement (IM) realiseren. Door samenhang tussen de Materiele-, Logistieke-, Facilitaire- en IM(IT)- beheerprocessen te realiseren en afhandeling vanuit dezelfde applicatie te doen, moeten de teams efficiënter en uniformer kunnen werken. De oplossing moet als SaaS ingericht zijn.
De beoordelaars merken het volgende op: "De aanbesteding besteedt veel aandacht aan open standaarden en verwijst veelvuldig naar Forum Standaardisatie. In dat opzicht is dit een zeer goede aanbesteding. Het missen van ODF en IPv4 en IPv6 is interessant: een gesprek tussen BFS/ICTU en de aanbestedende dienst zou voor beide partijen leerzaam kunnen zijn."
DNSSEC, HTTPS en HSTS, TLS, ISO 27001, ISO 27002, PDF, SAML, SPF, DKIM, DMARC en STARTTLS & DANE worden alle uitgevraagd. ODF en IPv4/IPv6 zoals gezegd niet.

Ook 100% gevraagd, maar bij een veel kleiner aantal relevante standaarden, hebben:

RVO. Deze aanbesteding wordt uitgevoerd in opdracht van Netherlands Space Office. De werkzaamheden binnen deze opdracht omvatten het verwerken van onbewerkte satellietdata tot bruikbare producten, die via het Satellietdataportaal beschikbaar worden gesteld. Opdrachtnemer dient tijdens deze opdracht samen te werken met de beheerder van het Satellietdataportaal en met de leverancier van de onbewerkte data.
Alleen de Geo-standaarden worden relevant geacht. Deze zijn ook uitgevraagd.

Belastingdienst. Het betreft een aanbesteding voor het waarborgen van de continuïteit van het AIX-platform (AIX is een besturingssysteem van IBM gebaseerd op Unix), na afloop van de huidige raamovereenkomsten voor dit platform. Bestaat uit het leveren van onderhoud en support op de Installed Base van het AIX platform en/of additionele diensten. Het huidige platform met AIX Apparatuur bestaat uit 50 IBM Power Systems en 10 Hardware Management Consoles (HMC's). Op de 50 IBM Power Systems draaien ongeveer 1200 virtuele AIX partities. Commentaar van de beoordelaars: "Er wordt geen aandacht besteed aan open standaarden(beleid), de PTOLU-lijst en BFS. In die zin een makkelijk verdiende "Perfect-score".
Alleen de beide ISO's (ISO 27001 en ISO 27002) zijn relevant en worden ook uitgevraagd.

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 72 aanbestedingen was dit jaar in totaal 834 keer een open standaard relevant, en in 377 gevallen (45%) 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 (11,6 dit jaar tegen 10,3 standaarden per aanbesteding vorig jaar, nadat de twee 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 45%, dat is lager dan vorig jaar (toen 50%);
- de combinatie van bovenstaande twee punten betekent per saldo dat er dit jaar per aanbesteding vrijwel evenveel standaarden zijn uitgevraagd als vorig jaar (5,2 dit jaar, versus 5,1 vorig jaar);
- er zijn meer relevant geachte standaarden NIET uitgevraagd: het gemiddelde aantal niet-gevraagde standaarden per aanbesteding is dit jaar 6,4 (vorig jaar: 5,2). Dit moet worden beschouwd als een achteruitgang.

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 lager dan het aantal standaarden die juist minder goed uitgevraagd is.

Andere zaken die opvallen bij nadere beschouwing van Tabel 4:

- veertien standaarden zijn vaker gevraagd dan gemiddeld (dus meer dan 45%): HTTPS & HSTS, ISO 27001/02, SAML, TLS, WPA2 Enterprise, CMIS, Digitoegankelijk, OpenAPI specification, PDF, XBRL, StUF COINS en ECLI. In vergelijking met vorig jaar is STARTTLS en DANE uit dit rijtje verdwenen. Nieuwkomers zijn WPA2 Enterprise, Digitoegankelijk, OpenAPI specification, XBRL, COINS en ECLI.
- Kanttekening bij de genoemde nieuwkomers: in drie gevallen is sprake van kleine aantallen, namelijk voor WPA2 Enterprise, COINS en ECLI (alle 2 maal relevant).
- Voor drie van de standaarden die behoorlijk vaak relevant waren (> 10 keer) is het percentage gevraagd flink gestegen: Digitoegankelijk, OpenAPI specification en StUF.
- Bij de andere standaarden die vaak relevant waren, is STARTTLS en DANE de grootste daler, van 54% uitgevraagd vorig jaar naar 16% uitgevraagd dit jaar. Andere opmerkelijke dalers zijn DNSSEC en IPv4 en IPv6.
- Eerder is al opgemerkt dat met name bij het Rijk het overall uitvraag-percentage is afgenomen, van 50 % naar 39 %. Deze afname wordt grotendeels verklaard door het veel lagere uitvraag-percentage van DKIM, DMARC, DNSSEC, SAML, SPF en (met name) STARTTLS en DANE.

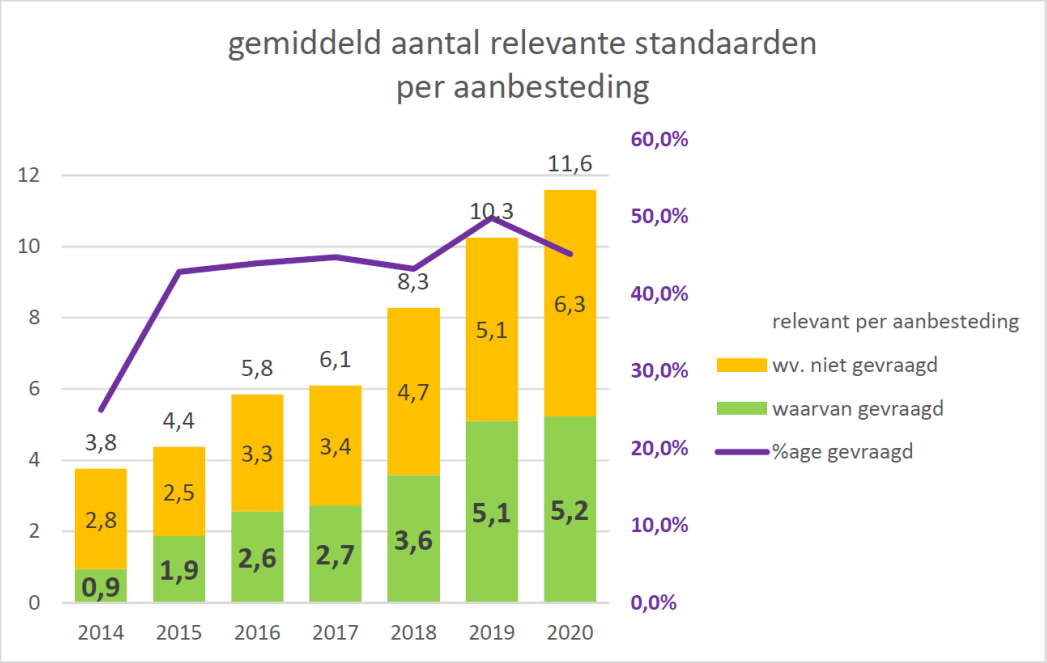
Tabel 4: 'Pas toe' bij aanbestedingen in 2019/2020, per standaard

	Rijksoverheid		Mede-overheden		**Totaal 2019/2020**		2018/2019
aantal aanbestedingen:	*37*		*35*		*72*		*72*
	relevant	gevraagd in % relevant	relevant	gevraagd in % relevant	Relevant	gevraagd in % relevant	gevraagd in % relevant
Internet & beveiliging:							
DKIM	21	5 %	29	38 %	50	24 %	31 %
DMARC	21	5 %	29	38 %	50	24 %	31 %
DNSSEC	26	12 %	30	40 %	56	27 %	40 %
HTTPS en HSTS	31	55 %	34	62 %	65	58 %	61 %
IPv6 en IPv4	25	8 %	32	6 %	57	7 %	23 %
NEN-ISO\IEC 27001:2005nl	36	81 %	35	86 %	71	83 %	83 %
NEN-ISO\IEC 27002:2007nl	36	81 %	35	86 %	71	83 %	83 %
SAML	16	44 %	23	70 %	39	59 %	58 %
SPF	21	5 %	29	38 %	50	24 %	31 %
STARTTLS en DANE	21	5 %	29	24 %	50	16 %	54 %
STIX en TAXII	0		0		0		
TLS	31	55 %	34	62 %	65	58 %	61 %
WPA2 Enterprise	0		2	100 %	2	100 %	20 %
Document & (web)content:							
Ades Baseline Profiles	1	100 %	3	0 %	4	25 %	0 %
CMIS	4	50 %	11	73 %	15	67 %	71 %
Digitoegankelijk *)	10	70 %	15	53 %	25	60 %	40 %
ODF	13	15 %	16	6 %	29	10 %	11 %
OpenAPI Specification	7	57 %	3	67 %	10	60 %	25 %
OWMS	0		0		0		50 %
PDF	20	45 %	24	71 %	44	59 %	60 %
SKOS	0		0		0		
E-facturatie & administratie:							
NLCIUS	1	0 %	3	33 %	4	25 %	36 %
SETU	0		5	0 %	5	0 %	33 %
WDO Datamodel	0		0		0		0 %
XBRL	1	100 %	1	100 %	2	100 %	33 %
Stelselstandaarden:							
Digikoppeling	3	67 %	18	28 %	21	33 %	26 %
Geo−standaarden	6	17 %	6	50 %	12	33 %	29 %
StUF	1	100 %	16	100 %	17	100 %	81 %
Water & Bodem:							
Aquo Standaard	0		0		0		
SIKB 0101	0		0		0		100 %
SIKB 0102	0		0		0		
Bouw:							
COINS	1	100 %	1	0 %	2	50 %	
IFC	1	100 %	2	0 %	3	33 %	
NLCS	0		1	0 %	1	0 %	
Visi	0		0		0		
Juridische verwijzingen:							
BWB	1	0 %	1	0 %	2	0 %	0 %
ECLI	2	50 %	0		2	50 %	0 %
JCDR	1	0 %	1	0 %	2	0 %	0 %
Onderwijs & loopbaan:							
E−portfolio	0	0 %	6	0 %	6	0 %	0 %
NL LOM	0	0 %	1	0 %	1	0 %	0 %
Overig:							
EML_NL	0		1	0 %	1	0 %	0 %
Totaal	**361**	**39 %**	**476**	**49 %**	**837**	**45 %**	**50 %**

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 11,6 in 2020.

Het percentage dat daarvan gevraagd werd ligt sinds 2015 ruwweg rond de 45% (zie de paarse lijn en de schaal rechts). Gemiddeld wordt dus om iets minder dan de helft van de relevante standaarden gevraagd, maar er zijn wel ieder jaar meer standaarden relevant.

Figuur 5: Aantal relevante standaarden bij aanbestedingen, 2014-2020



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 2014 stonden er 35 standaarden op de lijst en in 2020 waren het er 41. De lijst groeide dus per saldo met 14 %, dat is slechts een fractie van de toename van het aantal relevante standaarden (in 2020 ruim 2½ keer zoveel als in 2014). 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 13 standaarden uit dit domein (bijna eenderde van de lijst) zijn goed voor een belangrijk deel van het aantal keer relevant: in totaal was 834 keer een standaard relevant en daarvan betrof het 626 keer (75 %) 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 41 standaarden op de lijst voor 'pas toe of leg uit' waren 33 standaarden minimaal bij één aanbesteding relevant (vorig jaar exact dezelfde score), de andere 8 waren dus voor geen van de 72 onderzochte aanbestedingen relevant. Daarvan waren er vijf ook vorig jaar voor geen enkele onderzochte aanbesteding relevant: STIX en TAXII, SKOS, Aquo, SIKB 0102 en Visi. De overige drie standaarden (OWMS, WDO Datamodel en SIKB 0101) waren bij de vorige monitor wel relevant, zij het heel marginaal.

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 (99%) en ook TLS en HTTPS & HSTS (beide 90%). Deze standaarden behoorden ook vorig jaar tot de kopgroep. Als we als criterium aanhouden ‘bij meer dan 50% van de 72 aanbestedingen relevant’, dan kunnen aan dit rijtje nog acht standaarden worden toegevoegd: IPv4 & IPv6 (79%), DNSSEC (78%), DKIM, DMARC, SPF en STARTTLS en DANE (alle 67%), PDF (58%) en SAML (54%).

Daarna volgt een groep van drie standaarden die bij 25 tot 50% van de aanbestedingen relevant was: ODF (40%), Digitoegankelijk (35%) en Digikoppeling (29%). Het geheel overziend is sprake van een constante groep standaarden die relatief hoge percentages scoort, met dien verstande dat met name een aantal standaarden uit de categorie ‘internet en beveiliging’ zijn opgeschoven van de categorie ’25 tot 50%’ relevant naar ‘meer dan 50% relevant’.

Aan de andere kant: van de 33 standaarden die bij de beoordeelde aanbestedingen relevant werden geacht, zijn er dit jaar 7 slechts incidenteel (1 of 2 keer) als relevant aangemerkt (vorig jaar waren dat er 5): de drie juridische standaarden (BWB, ECLI en JCDR) elk twee keer evenals COINS, en EMN_NL, NL LOM en NLCS elk één keer. In vergelijking met vorig jaar beperkt de overlap zich tot EMN_NL en NL LOM die toen eveneens één keer relevant waren. Drie standaarden zijn uit deze opsomming verdwenen omdat ze dit jaar bij geen enkele aanbesteding relevant zijn (OWMS, SIKB 0101 en WDO Datamodel).

Tabel 6: Open standaarden relevant / gevraagd bij aanbestedingen in 2019/2020

(Bron: onderzoek aanbestedingen juli 2019 t/m juni 2020, uitgevoerd zomer 2020)

	Rijksoverheid		Mede-overheden		**Totaal 2019/2020**	
aantal aanbestedingen:	*37*		*35*		*72*	
	relevant in % van aanbest.n	gevraagd in % van aanbest.n	relevant in % van aanbest.n	gevraagd in % van aanbest.n	relevant in % van aanbest.n	gevraagd in % van aanbest.n
Internet & beveiliging:						
DKIM	57 %	3 %	83 %	31 %	**67 %**	**17 %**
DMARC	57 %	3 %	83 %	31 %	**67 %**	**17 %**
DNSSEC	70 %	8 %	86 %	34 %	**78 %**	**21 %**
HTTPS en HSTS	84 %	46 %	97 %	60 %	**90 %**	**53 %**
IPv6 en IPv4	68 %	5 %	91 %	6 %	**79 %**	**6 %**
NEN-ISO\IEC 27001:2005nl	97 %	78 %	100 %	86 %	**99 %**	**82 %**
NEN-ISO\IEC 27002:2007nl	97 %	78 %	100 %	86 %	**99 %**	**82 %**
SAML	43 %	19 %	66 %	46 %	**54 %**	**32 %**
SPF	57 %	3 %	83 %	31 %	**67 %**	**17 %**
STARTTLS en DANE	57 %	3 %	83 %	20 %	**67 %**	**11 %**
STIX en TAXII	0 %		0 %		**0 %**	
TLS	84 %	46 %	97 %	60 %	**90 %**	**53 %**
WPA2 Enterprise	0 %		6 %	6 %	**3 %**	**3 %**
Document & (web)content:						
Ades Baseline Profiles	3 %	3 %	9 %	0 %	**6 %**	**1 %**
CMIS	11 %	5 %	31%	23 %	**21 %**	**14 %**
Digitoegankelijk *)	27 %	19 %	43 %	23 %	**35 %**	**21 %**
ODF	35 %	5 %	46 %	3 %	**40 %**	**4 %**
OpenAPI Specification	19 %	11 %	9 %	6 %	**14 %**	**8 %**
OWMS	0 %		0 %		**0 %**	
PDF	54 %	24 %	69 %	49 %	**58 %**	**36 %**
SKOS	0 %		0 %		**0 %**	
E-facturatie & administratie:						
NLCIUS	3 %	0 %	9 %	3 %	**6 %**	**1 %**
SETU	0 %		14 %	0 %	**7 %**	**0 %**
WDO Datamodel	0 %		0 %		**0 %**	
XBRL	3 %	3 %	3 %	3 %	**3 %**	**3 %**
Stelselstandaarden:						
Digikoppeling	8 %	5 %	51 %	14 %	**29 %**	**10 %**
Geo−standaarden	16 %	3 %	17 %	9 %	**17 %**	**6 %**
StUF	3 %	3 %	46 %	46 %	**24 %**	**24 %**
Water & Bodem:						
Aquo Standaard	0 %		0 %		**0 %**	
SIKB 0101	0 %		0 %		**0 %**	
SIKB 0102	0 %		0 %		**0 %**	
Bouw:						
COINS	3 %	3 %	3 %	0 %	**3 %**	**1 %**
IFC	3 %	3 %	6 %	0 %	**4 %**	**1 %**
NLCS	0 %		3 %	0 %	**1 %**	**0 %**
Visi	0 %		0 %		**0 %**	
Juridische verwijzingen:						
BWB	3 %	0 %	3 %	0 %	**3 %**	**0 %**
ECLI	5 %	3 %	0 %		**3 %**	**1 %**
JCDR	3 %	0 %	3 %	0 %	**3 %**	**0 %**
Onderwijs & loopbaan:						
E−portfolio	0 %		17 %	0 %	**8 %**	**0 %**
NL LOM	0 %		3 %	0 %	**1 %**	**0 %**
Overig:						
EML_NL	0 %		3 %	0 %	**1 %**	**0 %**

Eerder in dit hoofdstuk is al opgemerkt dat het aantal relevant geachte standaarden per aanbesteding duidelijk 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. Uitschieters daarbij zijn DNSSEC, IPv4 & IPv6, SAML, de combinatie DKIM, DMARC en SPF en STARTTLS & DANE met percentages relevant die tussen de 15 en 20 procentpunten hoger liggen dan vorig jaar. Flinke uitschieters de andere kant op – veel minder vaak 'relevant' dan vorig jaar – zijn er niet, ook al lopen met name ODF en PDF wat terug (ongeveer 10 % lagere scores relevant dan vorig jaar).

In vergelijking met de vorige monitor zijn er drie standaarden deze keer bij geen enkele aanbesteding relevant gebleken en vorig jaar wel: OWMS, WDO Datamodel en SIKB 0101. Daarbij moet wel worden aangetekend dat de relevantie van deze standaard vorig jaar ook al niet groot was. Andersom is er slechts één standaard 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 IFC.

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 minder vaak dan vorig jaar om de relevante standaarden gevraagd: 45% dit jaar tegen 50% 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 (79% voor beide), HTTPS & HSTS (53%) TLS (53%) en PDF (36%). Vorig jaar (en overigens ook het jaar daarvoor) stonden dezelfde vijf standaarden op dit punt bovenaan.

Na dit rijtje koplopers volgt nog een negental standaarden met een score boven de 10%: SAML (32%), StUF (24%), DNSSEC (21%), Digitoegankelijk (voorheen: Webrichtlijnen) met 21%, de combinatie DKIM, DMARC en SPF (17%), CMIS (14%) en STARTTLS (11%). Vergeleken met vorig jaar is IPv4 en IPv6 weggevallen uit deze opsomming en zijn CMIS en STARTTLS toegevoegd.

Om de andere standaarden is slechts bij enkele aanbestedingen gevraagd of zelfs in het geheel niet. Dit laatste is het geval bij SETU, NLCS, BWB en JCDR, E-portfolio, NL LOM en EMN_NL. Deze 0%-scores doen zich dit jaar ook voor bij enkele standaarden die meer dan twee keer als relevant zijn aangemerkt. Dit betreft de SETU en E-portfolio.

3.5. 'Leg uit' bij aanbestedingen

Voor twee sets van beoordeelde aanbestedingen is nagegaan in hoeverre inmiddels 'leg uit' plaatsgevonden heeft in jaarverslagen over 2019: de aanbestedingen uit Q3 en Q4 2019 die in deze Monitor 2020 zijn beoordeeld èn de set aanbestedingen uit Q1 en Q2 2019 die vorig jaar zijn beoordeeld (in het kader van de Monitor 2019).

Bij vijf aanbestedingen die in het kader van deze monitor 2020 zijn beoordeeld, is om alle relevante standaarden gevraagd. Bij de andere 67 aanbestedingen moet dus in het jaarverslag verantwoording afgelegd worden ('Leg uit') voor het niet toepassen van de betreffende relevante standaard(en). Voor 33 van deze 67 aanbestedingen (door 29 overheidsorganisaties, waarvan dit jaar 4 ministeries) is het op dit moment mogelijk om in het Jaarverslag 2019 te controleren of 'leg-uit' is toegepast; deze 33 aanbestedingen dateren uit Q3 - Q4 2019. Voor de resterende 34 aanbestedingen kan dat pas na het verschijnen van de jaarverslagen over 2020. Van 'Leg uit' was in de jaarverslagen van deze 29 overheids-organisaties 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) geen enkele verwijzing naar het open standaardenbeleid teruggevonden. Van zeven aanbestedende partijen is op de website geen jaarverslag 2019 (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 vier departementen onderwerp van onderzoek zijn: Binnenlandse Zaken en Koninkrijksrelaties, Buitenlandse Zaken, Financiën (lees: Belastingdienst) en Infrastructuur en Waterstaat (lees: RWS). Van deze vier departementen zijn namelijk aanbestedingen beoordeeld uit Q3+Q4 2019, met een beoordeling die noodzaakt tot 'leg uit'.

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

- Zes ministeries (vorig jaar vijf) hebben een vorm van verantwoording opgenomen in het jaarverslag 2019. Er is sprake van twee nieuwkomers in dit rijtje (het ministerie van OCW en het ministerie van Defensie). Daar staat tegenover dat het ministerie van SZW dit jaar in tegenstelling tot vorig jaar niets in het jaarverslag heeft opgenomen dat in verband kan worden gebracht met het gebruik van open standaarden.
- Vrij uitgebreid (maar zonder op concrete aanbestedingen in te gaan) is het ministerie van BZK; niet alleen is in het jaarverslag een alinea over 'pas toe of leg uit' opgenomen, maar BZK meldt bovendien dat zij (conform de Instructie Rijksdienst) een lijst bijhoudt van afwijkingen van de lijst. Daarnaast verwijst BZK naar het overzicht dat Logius jaarlijks publiceert met afwijkingen van de lijst voor 'pas toe of leg uit'.
- De ministeries van I&W en VWS hebben de betreffende passages wat aangepast en uitgebreid.
- In het Jaarverslag 2019 van het ministerie van OCW staat een relatief uitgebreide passage, met daarbij de kanttekening dat geen duidelijke relatie wordt gelegd met het doen van ICT-aanbestedingen waarvoor regels zijn opgesteld betreffende het gebruik van open standaarden.
- De ministeries van AZ en Defensie zijn heel summier in hun melding dat geen sprake is geweest van afwijkingen van de voorschriften.
- De andere zes ministeries vermelden niets over open standaarden.

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.

Ministerie	Uitvoering 'leg uit'
'Leg uit' is voor één of meer aanbestedingen noodzakelijk	
AZ	<u>Gebruik open standaarden en open source software</u> Er zijn geen bijzonderheden te melden. *(Bron: B Beleidsverslag onder 5: bedrijfsvoeringsparagraaf, onder 2).* (Dezelfde teksten voor Kabinet van de Koning en de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten).
BZK	<u>Gebruik open standaarden en open source software</u> Het Ministerie van BZK heeft in 2019 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. Binnen BZK stuurt de CIO-BZK, in samenwerking met de partners uit het interne CIO-beraad, er zoveel mogelijk op aan dat er actief invulling wordt gegeven aan het gebruik van open standaarden en open source. Jaarlijks publiceert Logius in zijn online jaaroverzicht een overzicht van de toepassing van open standaarden binnen de Logius-producten met eventuele afwijkingen en toelichting. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf, onder paragraaf 2)*
DEF	*Gebruik open standaarden en open source software* Er is in 2019 niet afgeweken van het voorschrift. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf, onder paragraaf 2)*
EZK	[Geen]
FIN	[Geen]
I&W	<u>Gebruik open standaarden en open source software</u> In 2019 is er niet afgeweken van het gebruik van open standaarden of het gebruik van 'open source' bij het verwerven of ontwikkelen van informatievoorzieningen (IV). Net als vorig jaar stuurt IenW op de door het 'College Standaardisatie' vastgestelde open standaarden door toepassing daarvan in Project Start Architecturen (PSA). Verder zijn in 2019 ook voor Rijkswaterstaat (RWS) geen afwijkingen te melden ten aanzien van het gebruik van vastgestelde open standaarden. Door middel van het Forum Standaardisatie beoogt RWS op een transparante wijze de vastgestelde open standaarden daar waar mogelijk toe te passen bij het ontwikkelen van ICT diensten. *(Bron: 3. Beleidsverslag onder 3.4: Bedrijfsvoeringsparagraaf, onderdeel 2)*
VWS	<u>Gebruik open standaarden en open source software</u> Er zijn geen gevallen bekend binnen het concern VWS waarbij is afgeweken van het gebruik van open standaarden. Bij een functionele inkoop uitvraag van software binnen VWS hebben open source oplossingen de voorkeur en worden als wens in het programma van eisen opgenomen. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf onder 2)*
Geen aanbestedingen beoordeeld waarvoor 'Leg uit' noodzakelijk is	
BUZA	[Geen]
J&V	[Geen]
OCW	<u>Gebruik open standaarden en open source software</u> In het kader van veilig internet- en mailverkeer zijn er diverse 'open standaarden' van toepassing. Deze worden steeds strikter toegepast. De overheid heeft zich verplicht om per 1 januari 2020 deze standaarden geïmplementeerd te hebben, zodat een burger zekerheid heeft over het verkeer met het Ministerie van OCW en vice versa. Het Ministerie van OCW heeft deze datum niet volledig gehaald. Een deel van de webomgeving en een deel van de mailomgeving voldoet niet aan alle afgesproken open standaarden. De oorzaak hiervan ligt bij de inrichting van een nieuwe werkplek omgeving waarbij focus is gegeven aan een correcte migratie. De beschermende maatregelen uit de oude omgeving zijn meegenomen naar de huidige omgeving. Door

	inzet van de betreffende openstandaarden kan spam-mail met een hogere accuratesse worden herkend. Eind 2019 is de migratie van de werkplek afgerond. Nu volgt in een tweede stap de aanpassing van omgeving naar de open standaarden. De afronding van deze implementatie van open standaarden zal in de tweede helft van 2020 zijn voltooid. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf onder 2)*
SZW	[Geen]
LNV	[Geen]

'Leg uit' voor aanbestedingen uit Q1+Q2 2019 (vorig jaar beoordeeld)

In de vorig jaar verschenen Monitor 2019 zijn onder andere aanbestedingen beoordeeld uit Q1+Q2 2019. 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 2019 nu wèl beschikbaar zijn.

Deze 35 aanbestedingen (door 33 overheidsorganisaties, waarvan 5 ministeries[2]) zijn als volgt verdeeld: 16 aanbestedingen 'Rijk' en 19 aanbestedingen 'mede-overheden'. 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.

Dat een goede verantwoording best mogelijk is bewijst Logius: in het Jaarverslag 2019 is een uitgebreid overzicht opgenomen[3] met de relevante open standaarden van Logius-diensten en -voorzieningen en de mate waarin aan die standaarden is voldaan.

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 2018 in de Monitor 2019 valt op dat dit jaar per saldo bij één departement meer een verwijzing naar het beleid rond de toepassing van open standaarden is verschenen.

[2] Te weten de ministeries van BZK, SZW, VWS, Financiën (in dit geval niet alleen Belastingdienst) en AZ.
[3] Zie: https://magazines.logius.nl/logiusjaarverslag/2019/01/relevante-open-standaarden.

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.

De afgelopen acht jaren onderzochten wij een grote en gevarieerde verzameling van in totaal 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 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.

Met ingang van dit jaar worden vier websites van registraties toegevoegd (Handelsregister, PDOK, RDW en WOZ Waardeloket). Binnen Rijksoverheid.nl maken we nu onderscheid tussen het webdomein en het emaildomein. Niet meer onderzocht worden eFactureren en SBR (eerder standaarden dan voorzieningen) en ODC Noord (een datacentre waarbinnen voorzieningen geplaatst worden, maar is zelf geen voorziening).

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 B5 is de rapportage opgenomen met alle gedetailleerde informatie per onderzochte voorziening.

4.1.2. Welke voorzieningen zijn onderzocht?

Dit jaar zijn de 17 voorzieningen onderzocht die direct raken aan de communicatie en gegevensuitwisseling met burgers en bedrijven.

Het gaat om de volgende voorzieningen (links):

Dit jaar onderzocht: Gegevensuitwisseling en communicatie met burgers en bedrijven *(13 + 4)*	*Volgend jaar:* Gegevensuitwisseling tussen overheden en onderliggende infrastructuur *(21)*
Identificeren en authenticeren • DigiD • DigiD Machtigen • Afsprakenstelsel ETD • PKI Overheid	*Identificeren en authenticeren* • BSN Beheervoorziening + GBA-V • Rijkspas
Dienstverlening en informatieverstrekken • MijnOverheid • Berichtenbox bedrijven • Overheid.nl • Ondernemersplein • Samenwerkende Catalogi • Rijksoverheid.nl * web-domein * email-domein + website RDW.nl (voertuigen) + website WOZ-waardeloket.nl	*Dienstverlening en informatieverstrekken* • Doc-Direct • Rijksportaal
Gegevens en registreren + website Handelsregister KvK (NHR) + website PDOK (open geo-data)	*Gegevens en registreren* • BAG, BRK, WOZ en BGT • BRI (inkomen) • BRO (ondergrond) • BRT (topografie) • BRV (voertuigen) • NHR (Nieuw HandelsRegister) • Digilevering • Digimelding • Stelselcatalogus • P-Direct
Dienstverlening en verbinden • TenderNed • Digi-Inkoop	*Dienstverlening en verbinden* • DigiPoort • Diginetwerk • Digitale Werkomgeving Rijk

4.1.3. Werkwijze

Voor dit onderzoek is gebruik gemaakt van de 'pas toe of leg uit'-lijst van 1 april 2020. Voor elke voorziening is 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 vorig jaar. Waar mogelijk zijn de standaarden opnieuw getoetst. Daarbij maken we onder meer gebruik van de testen die beschikbaar zijn via https://internet.nl. Hiermee kan voor een groot deel van de standaarden getoetst worden of eraan voldaan wordt. Er zijn enkele uitzonderingen. Vaak betreft het 'besloten' voorzieningen die niet publiek via internet toegankelijk zijn. Daarnaast kijken we – voor zover mogelijk – of de geplande activiteiten inmiddels uitgevoerd zijn. Voor nieuwe voorzieningen maken we een inschatting welke standaarden relevant zijn. Voor nieuwe standaarden op de lijst maken we 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 vertegenwoordigers 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 c.q. vertegenwoordigers 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 verschillen ook na de gesprekken bleven bestaan is dit duidelijk vermeld 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 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

Voor de volgorde van het overzicht van standaarden is de volgorde van de flyer[4] met standaarden van het Forum Standaardisatie aangehouden.

Status
In de rapportage, opgenomen in Bijlage B5, is per voorziening een tabel opgenomen. Daarin staan de standaarden genoemd die relevant zijn voor de voorzieningen. Alsmede de status

[4] https://www.forumstandaardisatie.nl/sites/bfs/files/Lijst_verplichte_open_standaarden_sept-2018_0.pdf

van de standaard zoals toegekend door de onderzoekers. De status kan de volgende waarden hebben:

- Ja: De voorziening is conform de standaard,
  Met 'conform' wordt in dit onderzoek bedoeld dat de standaard door de eindgebruiker te gebruiken is.
- Nee: De voorziening is niet conform de standaard,
- Deels: Onderdelen van de voorziening zijn conform aan, maar niet alle onderdelen,
  Idealiter voldoen alle onderdelen van een voorziening aan de relevante standaarden. Dat is echter niet altijd het geval. Sommige onderdelen kunnen wel en andere niet voldoen. 'Deels voldoen' betekent dat een onderdeel van de voorziening helemaal aan de standaard voldoet maar één of meer andere onderdelen niet.
- 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 toepassingsgebied en van het organisatorisch toepassingsgebied, zoals vermeld op de pas-toe-of-leg-uit lijst van het Forum Standaardisatie gehanteerd.[5] 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 van wanneer een voorziening aan een standaard voldoet is lastig. Het vereist een heldere afbakening van de voorziening en heldere voorwaarden voor 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 de 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 afwijken van elkaar geven we dit helder aan in de rapportage. Per voorziening wordt het relevante onderdeel van de rapportage nog ter instemming voorgelegd aan de beheerder.

[5] Zie: https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht

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

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[6] 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 & 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.

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 dat een inclusieve benadering van digitale overheidsdienstverlening moet realiseren. 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 en binnen een redelijk haalbare termijn, toewerken naar volledig 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.

Momenteel is de wijze waarop overheden omspringen met de verplichting nog zeer divers. Gelet daarop en gelet op het feit dat 23 september 2020 bij de start van dit onderzoek nog een half jaar verder lag, is in overleg met de opdrachtgever besloten pas volgend jaar te toetsen op het al dan niet hebben van een toegankelijkheidsverklaring. We zullen dan ook (in overleg met de beheerder van de standaard) kijken of er een verdere objectivering van de beoordeling van het al dan niet voldoen aan de standaard mogelijk en wenselijk is.

[6] https://internet.nl/about/

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 27001/2 standaard. Indien een organisatie voldoet aan de BIO, dan voldoen zij binnen de context van dit rapport ook aan de verplichting om de ISO 27001/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.

In het onderzoek is gebleken dat er onduidelijkheid was bij een groot aantal beheerders van voorzieningen over de vraag of de standaard voor hen van toepassing is.

- 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 gaat men ervan uit dat de netwerkleverancier dit regelt.
- 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.

Vanwege de verwarring is in overleg met Bureau Forum Standaardisatie besloten de standaard dit jaar nog niet in de tabel op te nemen. We hebben in het kader van dit onderzoek wel getoetst[7] of de standaard wordt toegepast en naar aanleiding van het onderzoek hebben ook een aantal voorzieningen de standaard alsnog geadopteerd. Voorzieningen die niet voldoen hebben daarnaast een mail ontvangen met deze boodschap. In een volgende monitor wordt de standaard wel in de tabel opgenomen.

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 B5, wordt de mate waarin elke voorziening aan de relevante standaarden voldoet gedetailleerd besproken.

[7] De toetsing van RPKI is in samenwerking met het Bureau Forum Standaardisatie uitgevoerd. Voor de toetsing zijn de relevantie ip-adressen van de voorzieningen gecontroleerd via https://stat.ripe.net/46.22.185.32#tabId=routing

4.2.1. Per voorziening beschouwd

Zoals gezegd in paragraaf 4.1.2 onderzoeken wij dit jaar 17 voorzieningen die direct raken aan de communicatie en de gegevensuitwisseling met burgers en bedrijven, zoals DigiD, MijnOverheid en Ondernemersplein. Daaronder ook vier websites van registraties die dit jaar nieuw toegevoegd zijn (Handelsregister, PDOK, RDW.nl en WOZ Waardeloket). Wij richten ons in deze paragraaf vooral op die 17 voorzieningen.

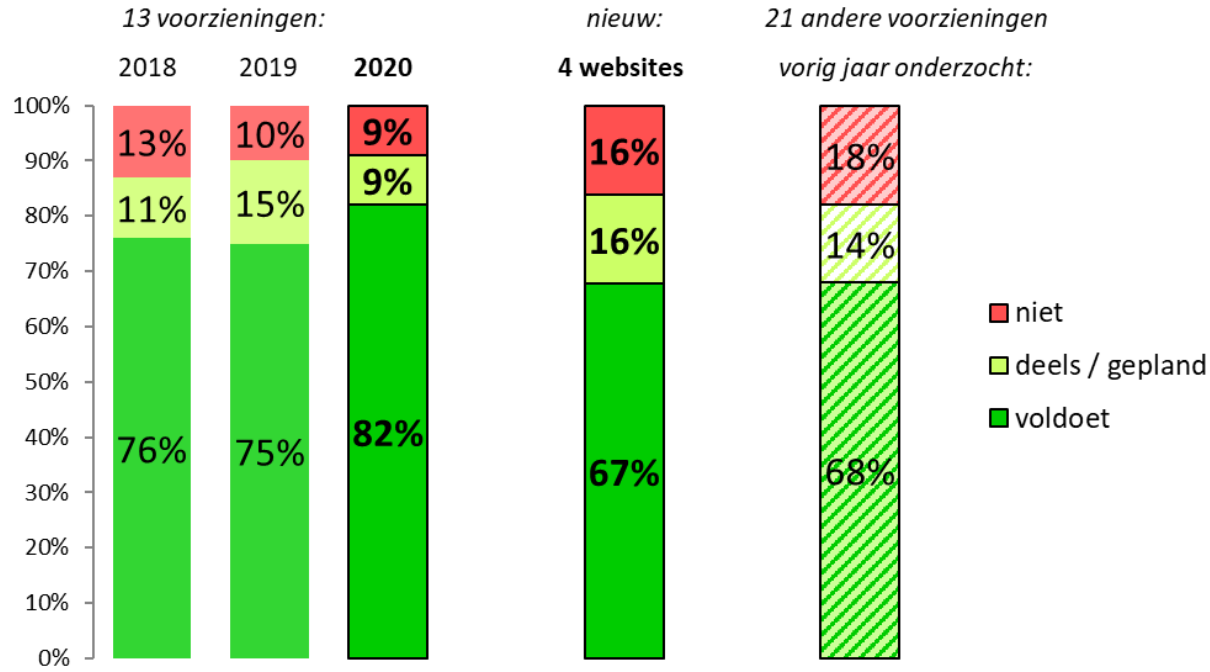
Volgend jaar onderzoeken we 21 voorzieningen, die vooral gericht op de communicatie en gegevensuitwisseling tussen overheden onderling of op de onderliggende infrastructuur. De gegevens (van vorig jaar) over deze 21 voorzieningen zijn – ter aanvulling van het beeld – wèl opgenomen in Tabel 8b verderop.

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

- de website van het Handelsregister (19 standaarden),
- de website RDW.nl (17 standaarden),
- en MijnOverheid (15 standaarden).

Voor andere voorzieningen zijn minder standaarden relevant, zoals voor PKI Overheid (9) en Samenwerkende Catalogi (7). Voor de dit jaar onderzochte 17 voorzieningen zijn gemiddeld per voorziening 12,3 open standaarden relevant.

Figuur 7: Toepassing open standaarden in 17 voorzieningen



In de meeste gevallen voldoen deze voorzieningen aan de relevante open standaarden. Voor (alleen) de 13 voorzieningen die ook in voorgaande jaren zijn onderzocht kan de ontwikkeling in de tijd worden gepresenteerd (zie het linker gedeelte van Figuur 7). Deze voorzieningen doen het steeds beter: het percentage 'voldoet' is gestegen van 75% tot 82%. Het aantal gevallen waarin de voorziening deels aan de standaard voldoet of daarvoor

concrete plannen heeft is afgenomen van 15% vorig jaar naar 9% dit jaar. Samen met het percentage dat 'voldoet' is dat voor dit jaar dus 91%.

Dit jaar voldoen zeven van de 17 voorzieningen geheel of gedeeltelijk aan alle relevante standaarden en/of zij hebben concrete plannen om daaraan op korte termijn te voldoen. Eén daarvan is voor het eerst onderzocht: PDOK.nl.

De vier nieuw toegevoegde websites (middenin Figuur 7) voldoen aan 67% van de relevante standaarden. In 16% van de gevallen voldoen zij deels aan de standaard of hebben zij daarvoor concrete plannen. Hier is dus nog veel ruimte voor verbetering.

Dat geldt overigens ook voor de 21 voorzieningen die dit jaar niet zijn onderzocht (hun scores van vorig jaar zijn rechts in de figuur opgenomen).

Verschillende voorzieningen onderscheiden zich dit jaar in positieve zin:

- Zowel MijnOverheid (15 relevante standaarden) als DigiD (11 standaarden relevant) voldoen dit jaar aan alle relevante standaarden.
- 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 nieuw onderzochte website PDOK.nl (voor alle 14 relevante standaarden) en de website van het Handelsregister (voor 17 van de 19 relevante standaarden).

In Tabel 8a (hierna) is een gedetailleerd overzicht opgenomen van de 17 voorzieningen die van belang zijn voor communicatie en gegevensuitwisseling met burgers en bedrijven, de daarvoor relevante open standaarden en de mate waarin de voorziening daaraan voldoet. Naar verwachting zullen deze voorzieningen in 2022 opnieuw worden onderzocht.

Ter aanvulling zijn daarna in Tabel 8b de 'oude' gegevens (uit het onderzoek van vorig jaar) opgenomen voor de 21 voorzieningen die vooral gericht zijn op de communicatie en de gegevensuitwisseling tussen overheden onderling of de onderliggende infrastructuur. In 2021 zullen deze voorzieningen naar verwachting weer worden onderzocht.

Tabel 8a: Toepassing open standaarden in 17 voorzieningen die dit jaar onderzocht zijn

	Onderzocht in 2020:	Identificeren & authenticeren				Dienstverlening & informatieverstrekken									Gegevens & registreren		Dienstverlening & verbinden		
	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 - webdomein	Rijksoverheid.nl - emaildomein	*website* RDW.nl	*website* WOZ Waardeloket	*website* Handelsregister KvK	*website* PDOK (geodata)	TenderNed	Digi-Inkoop	*aantal keer relevant*
	aantal relevante OSn:	*11*	*11*	*9*	*12*	*15*	*11*	*14*	*13*	*7*	*11*	*9*	*17*	*11*	*19*	*14*	*13*	*12*	*209*
Internet & beveiliging	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*
	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*
Document & (web)content	AdES Baseline Prof.												N		V				*2*
	CMIS								N				N		G				*3*
	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*
RES T	OpenAPI Specific.					V				V			V		D	V	N		*6*
E-facturatie & administratie	NLCIUS												N		N			V	*3*
	SETU																	V	*1*
	WDO Datamodel																		*0*
	XBRL																		*0*
Stelsel-standaarden	Digikoppeling		D			V	V								V				*4*
	Geo-standaarden															V			*1*
	StUF					V	V								V	V			*4*
Water & Bodem	Aquo-standaarden																		*0*
	SIKB 0101																		*0*
	SIKB 0102																		*0*
Bouw	COINS																		*0*
	IFC																		*0*
	NLCS																		*0*
	VISI																		*0*
Juridische verwijzingen	BWB							V	V		V								*3*
	ECLI																		*0*
	JCDR							V											*1*
Onderwijs	e-Portfolio																		*0*
	NL_LOM																		*0*
Overig	EML_NL																		*0*

Tabel 8b: Toepassing open standaarden in 21 andere voorzieningen (onderzocht in 2019)

(Deze standaarden worden in 2021 weer onderzocht.)

Vorig jaar onderzocht:		Identificeren & authent.		Dienstverl. & inform.vs.		Gegevens & registreren									Dienstverlening & verbinden			
	V = voldoet *D = voldoet deels* *G = gepland* *N = voldoet niet* *(leeg = n.v.t.)*	BSN Beheervz + GBA-V (x2)	Rijkspas	Rijksportaal	Doc-Direct	NHR (Nieuw HandelsReg.)	BAG, BRK, WOZ en BGT (x4)	BRO (ondergrond)	BRT (topografie)	BRV (voertuigen)	BRI (inkomen)	Digilevering	Digimelding	Stelselcatalogus	P-Direct	DigiPoort	Diginetwerk	Dig. Werkomgeving Rijk	*aantal keer relevant*
	aantal relevante OSn	*14*	*11*	*8*	*15*	*19*	*68*	*13*	*9*	*17*	*5*	*8*	*8*	*7*	*16*	*12*	*4*	*15*	*249*
Internet & beveiliging	DKIM		G	N	V	V	V			V		V	G		V	V		V	*14*
	DMARC		N	V	V	V	V		V	D	V	V	V	V	V	G		N	*17*
	DNSSEC		G	N		N	V	V		D		V	V	V	N	G	G	V	*16*
	HTTPS & HSTS	V			D	V	D	V	D	D		V	V	G	V	V		G	*17*
	IPv4 & IPv6	N	N	N	V	D	V	D		N		N	N	N	N	N	G	G	*19*
	NEN-ISO\IEC 27001	V	V		V	V	V	V	V	V	V				V	V	V	V	*17*
	NEN-ISO\IEC 27002	V	V		V	V	V	V	V	V	V				V	V	V	V	*17*
	SAML		V	V	V	V		V		V					V			V	*8*
	SPF		V	N	V	V	V			V		V	V		V	G		V	*14*
	STARTTLS & DANE		N			D	N		N	V		V	N		N			V	*12*
	STIX en TAXII																		*0*
	TLS	V	V		N	V	V	V	V	V	V				V	V		V	*16*
	WPA2 Enterprise																	V	*1*
Document & (web)content	AdES Baseline Prof.				N	V									N				*3*
	CMIS				N	D		V		N									*4*
	Digitoegankelijk																		*0*
	ODF 1.2			V	N										N			V	*4*
	OWMS								N	V									*2*
	PDF (NEN)			V	V	V	V			V				V	V			V	*11*
	SKOS				N	N	D		V	V				V					*9*
RES T	OpenAPI Specific.					D	V	V		V									*7*
E-facturatie & administratie	NLCIUS					N	N												*5*
	SETU															V			*1*
	WDO Datamodel																		*0*
	XBRL															V			*1*
Stelsel-standaarden	Digikoppeling	N	V		N	V	D	V		D	V	V	V		V	V		V	*17*
	Geo-standaarden						V	V	V										*6*
	StUF	N				V	V												*7*
Water & Bodem	Aquo-standaarden							V											*1*
	SIKB 0101																		*0*
	SIKB 0102																		*0*
Bouw	COINS																		*0*
	IFC																		*0*
	NLCS																		*0*
	VISI																		*0*
Juridische verwijzingen	BWB							G						V	V				*3*
	ECLI																		*0*
	JCDR																		*0*
Onderwijs	e-Portfolio																		*0*
	NL_LOM																		*0*
Overig	EML_NL																		*0*

4.2.2. Per standaard beschouwd

Van alle 43 open standaarden op de 'pas toe of leg uit'-lijst zijn er 26 relevant voor één of meer van de dit jaar onderzochte voorzieningen. Er zijn 11 open standaarden die voor meer dan 10 van de 17 voorzieningen relevant zijn:

- IPv6+IPv4 en TLS (beide relevant voor alle 17 dit jaar onderzochte voorzieningen),
- DMARC, DNSSEC en HTTPS+HSTS (relevant voor 16 van de 17 voorzieningen),
- NEN-ISO\IEC 27001 en NEN-ISO\IEC 27002 (15), SPF (14), DKIM (13) en PDF (12).

De mate waarin voorzieningen aan de standaard (als die relevant is) voldoen is hoog: voor 14 van de 26 standaarden die relevant zijn geldt dat tenminste 80% van de voorzieningen aan die standaard voldoet. Het gaat om de volgende 14 open standaarden:

- voor 10 standaarden geldt dat alle voorzieningen waarvoor deze standaard relevant is er aan voldoen; voor een deel zijn dat standaarden die voor veel voorzieningen relevant zijn, zoals : NEN-ISO\IEC 27001, NEN-ISO\IEC 27002, SAML en SPF; de andere standaarden zijn voor een beperkter aantal voorzieningen relevant, maar die voldoen wel allemaal aan die standaard: ODF, SETU, Geo-standaarden, StUF, BWB en JCDR;
- de vier standaarden waaraan tussen 80% en 99% van de voorzieningen voldoet zijn: DKIM (92%), DNSSEC (88%), OWMS en PDF (beide 83%).

Van deze standaarden vallen er 6 in het domein 'Internet & beveiliging', 3 in het domein 'Document & (web)content', 2 onder de 'Stelselstandaarden', 2 in het domein 'Juridische verwijzingen' en de laatste in 'E-facturatie & administratie'.

Vijf standaarden scoren juist relatief laag: van de voorzieningen waarvoor deze relevant zijn voldoet er geen enkele aan CMIS en aan de nieuwe standaard RPKI. Daarnaast voldoet slechts 33% van de voorzieningen aan NLCIUS en 47% aan IPv4 & IPv6.

De verschillen tussen de domeinen zijn groot. Vooral standaarden uit het domein 'Internet & Beveiliging' zijn bijvoorbeeld erg vaak relevant (76% van alle gevallen). De domeinen 'Document & Webcontent' (13%) en 'Stelselstandaarden' (4%) volgen op grote afstand. Standaarden uit de zes andere domeinen zijn zelden relevant (samen slechts 7%). Dat roept de vraag op hoe het zit met de doelstellingen van het open standaardenbeleid: met name interoperabiliteit en leveranciersonafhankelijkheid.

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

	onderzocht in 2020: **set van 17 voorzieningen voor gegevensuitwisseling / communicatie met burgers en bedrijven**			*vorig jaar onderzocht:* set van 21 voorzieningen voor gegevensuitwisseling overheden en onderliggende infrastructuur		
	relevant in % van 17	**voldoet in % relevant**	voldoet + deels/gepland in % relevant	relevant in % van 21	voldoet in % relevant	voldoet + deels/gepland in % relevant
Internet & beveiliging:						
DKIM	**76 %**	**92 %**	**100 %**	67 %	79 %	93 %
DMARC	**94 %**	**75 %**	**88 %**	81 %	76 %	88 %
DNSSEC	**94 %**	**88 %**	**100 %**	76 %	56 %	81 %
HTTPS en HSTS	**94 %**	**63 %**	**88 %**	81 %	47 %	100 %
IPv6 en IPv4	**100 %**	**47 %**	**71 %**	90 %	26 %	47 %
NEN-ISO\IEC 27001:2005nl	**88 %**	**100 %**	**100 %**	81 %	100 %	100 %
NEN-ISO\IEC 27002:2007nl	**88 %**	**100 %**	**100 %**	81 %	100 %	100 %
SAML	**47 %**	**100 %**	**100 %**	38 %	100 %	100 %
SPF	**82 %**	**100 %**	**100 %**	67 %	86 %	93 %
STARTTLS en DANE	**65 %**	**64 %**	**82 %**	57 %	25 %	33 %
STIX en TAXII	**0 %**			0 %		
TLS	**100 %**	**65 %**	**82 %**	76 %	94 %	94 %
WPA2 Enterprise	**0 %**			5 %	100 %	100 %
Document & (web)content:						
Ades Baseline Profiles	**12 %**	**50 %**	**50 %**	14 %	33 %	33 %
CMIS	**18 %**	**0 %**	**33 %**	19 %	25 %	50 %
Digitoegankelijk	**0 %**			0 %		
ODF	**6 %**	**100 %**	**100 %**	19 %	50 %	50 %
OpenAPI Specification	**35 %**	**67 %**	**83 %**	33 %	86 %	100 %
OWMS	**35 %**	**83 %**	**83 %**	10 %	50 %	50 %
PDF	**71 %**	**83 %**	**92 %**	52 %	100 %	100 %
SKOS	**18 %**	**67 %**	**100 %**	43 %	33 %	78 %
E-facturatie & administratie:						
NLCIUS	**18 %**	**33 %**	**33 %**	24 %	0 %	0 %
SETU	**6 %**	**100 %**	**100 %**	5 %	100 %	100 %
WDO Datamodel	**0 %**			0 %		
XBRL	**0 %**			5 %	100 %	100 %
Stelselstandaarden:						
Digikoppeling	**24 %**	**75 %**	**100 %**	81 %	53 %	82 %
Geo−standaarden	**6 %**	**100 %**	**100 %**	29 %	100 %	100 %
StUF	**24 %**	**100 %**	**100 %**	33 %	71 %	71 %
Water & Bodem:						
Aquo Standaard	**0 %**			5 %	100 %	100 %
SIKB 0101	**0 %**			0 %		
SIKB 0102	**0 %**			0 %		
Bouw:						
COINS	**0 %**			0 %		
IFC	**0 %**			0 %		
NLCS	**0 %**			0 %		
Visi	**0 %**			0 %		
Juridische verwijzingen:						
BWB	**18 %**	**100 %**	**100 %**	14 %	67 %	100 %
ECLI	**0 %**			0 %		
JCDR	**6 %**	**100 %**	**100 %**	0 %		
Onderwijs & loopbaan:						
E−portfolio	**0 %**			0 %		
NL LOM	**0 %**			0 %		
Overig:						
EML_NL	**0 %**			0 %		

5. Gebruiksgegevens over 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 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 2020'* (zie Bijlage B3).

Daarnaast doet BFS elk halfjaar onderzoek naar internet-veiligheids-standaarden, een deel van de gebruiksgegevens is afkomstig uit de *'Meting Informatieveiligheidstandaarden overheid - september 2020'* (zie Bijlage B4).

5.1. Gebruiksgegevens 2020: inventarisatie door accountmanagers BFS

In de notitie *'Inventarisatie gebruiksgegevens 2020'* (zie Bijlage B3) 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 meer dan de helft van de 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 2020, per standaard

	Beeld BFS		Resultaten IV-meting
	ontwikkeling t.o.v. 2019	gebruiksgegevens	
Internet & beveiliging:			
DKIM	toegenomen	van 89% naar 96%	96 %
DMARC	toegenomen	van 82% naar 92%	DMARC 92 %
en DMARC policy	toegenomen	van 37% naar 66%	DMARC policy 66 %
DNSSEC	stabiel	van 93% naar 94%	94 %
HTTPS	toegenomen	van 90% naar 98%	HTTPS cf 98 %
en HSTS	toegenomen	van 79% naar 92%	HSTS cf 92 %
IPv6 en IPv4	toegenomen	van 48% naar 69%	
NEN-ISO\IEC 27001:2005nl	niet duidelijk	*[geen cijfers]*	
NEN-ISO\IEC 27002:2007nl	niet duidelijk	*[geen cijfers]*	
RKPI	n.v.t. (nieuw op lijst)	globale cijfers	
SAML	toegenomen	van 868 naar 1016	
SPF	licht toegenomen	van 95% naar 97%	SPF 97 %
en SPF policy	toegenomen	van 88% naar 91%	SPF policy 91 %
SPF	licht toegenomen	van 95% naar 97%	97 %
STARTTLS	afname	cf: van 67% naar 42%	STARTTLS cf 42 %
en DANE	toegenomen	van 41% naar 53%	DANE 53 %
STIX & TAXII	onduidelijk	*[geen cijfers]*	
TLS	afname	cf: van 89% naar 78%	TLS cf 78 %
WPA2 Enterprise	toegenomen	van 529 naar 563	
Document & (web)content:			
Ades Baseline Profiles		*NIET ONDERZOCHT*	
CMIS		*NIET ONDERZOCHT*	
Digitoegankelijk	n.v.t. (eerste meting)	diverse indicatoren	
ODF	toegenomen	van 8% naar 24%	
OpenAPI Specification	n.v.t. (eerste meting)	diverse indicatoren	
OWMS	afname	van 36% naar 28%	
PDF	stabiel	bijna 100%	
SKOS	onduidelijk	globale cijfers	
E-facturatie & administratie:			
NLCIUS	toegenomen	*[geen cijfers]*	
SETU	stabiel	*[geen cijfers]*	
WDO Datamodel	toegenomen	*[geen cijfers]*	
XBRL	toegenomen	diverse indicatoren	
Stelselstandaarden:			
Digikoppeling	licht toegenomen	van 90% naar 91%	
Geo−standaarden	toegenomen	diverse indicatoren	
StUF	licht toegenomen	diverse indicatoren	
Water & Bodem:			
Aquo Standaard	stabiel	diverse indicatoren	
SIKB 0101	toename	*[geen cijfers]*	
SIKB 0102	toename	*[geen cijfers]*	
Bouw:			
COINS	n.v.t. (eerste meting)	*[geen cijfers]*	
IFC		*NIET ONDERZOCHT*	
NLCS	toegenomen	in 2019 geen cijfers	
Visi	toegenomen	in 2019 geen cijfers	
Juridische verwijzingen:			
BWB	toegenomen	*[nauwelijks cijfers]*	
ECLI	toegenomen	*[nauwelijks cijfers]*	
JCDR	toegenomen	*[nauwelijks cijfers]*	
Onderwijs & loopbaan:			
E−portfolio	stabiel	*[nauwelijks cijfers]*	
NL LOM	toegenomen	*[geen cijfers]*	
Overig:			
EML_NL	stabiel	*(veel 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 nog niet de door het OBDO nagestreefde 100%). Uitzonderingen zijn IPv4&IPv6 (69%, stijgend), DANE (53%, ook stijgend), STARTTLS (42%, dalend) en TLS (78%, dalend). Bij de daling van STARTTLS en TLS past een kanttekening. Deze daling is een gevolg van een andere manier van meten dan bij de vorige meting met als gevolg dat de lat om te voldoen aan de criteria hoger is komen te liggen.

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 2020: 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 september 2020*' (zie Bijlage B4, de uitkomsten zijn opgenomen in de rechterkolom van Tabel 10) blijkt dat het streefbeeld voor eind 2019 op het moment van de meting – september 2020 – nog niet was gerealiseerd. Het gebruik van een aantal standaarden is in vergelijking met de vorige monitor wel doorgegroeid naar meer dan 90%. Dit betreft DKIM, DMARC en HTTPS & HSTS. Daartegenover staat een lagere score voor STARTTLS en voor TLS.

Van de webstandaarden wordt HTTPS conform NCSC het meest toegepast (98%), gevolgd door DNSSEC (94%) en HSTS (92%). TLS conform NCSC is zoals eerder al opgemerkt wat terugvallen (78%). De afspraken voor eind 2019 zijn dus nog niet helemaal gerealiseerd.

Van de emailstandaarden wordt SPF het meest toegepast (97%), gevolgd door DKIM (96%) en DMARC (92%). De afspraken voor eind 2019 zijn voor deze drie standaarden dus ook nog niet helemaal gerealiseerd. De andere mailstandaarden worden op dit moment nog minder vaak gebruikt en hebben echt nog een flink eind te gaan: STARTTLS conform NCSC (42%) en DANE (53%).

Ontwikkeling van de adoptie

Uit deze meting blijkt enerzijds, dat de adoptie voor de betreffende standaarden verder is toegenomen. Maar niet voldoende om het streefbeeld voor eind 2019 (100%) helemaal te bereiken. Niet voor de webstandaarden: de adoptie van DNSSEC steeg van 93% naar 94%, HTTPS conform NCSC van 90% naar 98% en HSTS van 79% naar 92%. TLS conform NCSC zakt om eerder beschreven redenen van 89% naar 78%. Ook voor de mailstandaarden is het

streefbeeld voor eind 2019 nog niet bereikt: de adoptie van SPF steeg van 95% naar 97%, DKIM van 89% naar 96%, DMARC van 82% naar 92%. STARTTLS conform NCSC is gedaald van 67% naar 42%, daar is nog een eind te gaan. Diezelfde boodschap geldt ook voor het gebruik van DANE, ook al is de adoptie gestegen van 41% naar 53%.

Aanvullend op de standaard-meting (548 domeinnamen) is voor het eerst een vergelijking gemaakt met een bredere selectie van bijna 1.790 overheidsdomeinen. Die extra meting bevestigt, dat er nog een flinke stap gezet zal moeten worden. De scores voor de bredere selectie zijn in de meeste gevallen lager dan voor de kerngroep van 548 domeinnamen.

BIJLAGEN

B1. Instructie Rijksdienst (inclusief toelichting)

B2. Overzicht van de beoordeelde aanbestedingen 2019/2020

B3. Inventarisatie gebruiksgegevens 2020 door BFS

B4. Rapportage IV-meting september 2020

B5. Rapportage Open standaarden en voorzieningen (PBLQ)

B1. Instructie Rijksdienst (inclusief toelichting)

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

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 2019/2020

De 37 aanbestedingen van Rijk en uitvoeringsorganisaties en de 35 van mede-overheden die dit jaar zijn beoordeeld zijn in 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 en de uiteindelijke beoordeling. Hiervoor is de volgende indeling gehanteerd (conform 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 procent 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 kolom daarnaast in rood.

Tabel B2.1 Overzicht van beoordeelde aanbestedingen Rijk en uitvoeringsorganisaties

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
Raad van State	Data-uitwisseling mogelijk maken, via één koppeldienst, tussen hun SaaS- en "On Premise"-oplossingen. Om dergelijke data-uitwisseling mogelijk te maken is een koppelfunctionaliteit en/of een berichtenmakelaar nodig.	ISO 27001 ISO 27002 HTTPS en HSTS TLS Digikoppeling IPv4 en IPv6 CMIS DNSSEC ECLI Open API SAML COINS Digitoegankelijk PDF StUF		perfect	(100%)
Rijksdienst voor Ondernemend Nederland	Het verwerken van onbewerkte satellietdata tot bruikbare producten, die via het Satelliet-dataportaal beschikbaar worden gesteld.	Geo		perfect	(100%)
Belasting-dienst	Het waarborgen van de continuïteit van het AIX-platform (AIX is een besturingssysteem van IBM gebaseerd op Unix), na afloop van de huidige raamovereenkomsten voor dit platform. Bestaat uit het leveren van onderhoud en support op de Installed Base van het AIX platform en/of additionele diensten.	ISO 27001 ISO 27002		perfect	(100%)

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
Ministerie van Binnenlandse Zaken en Koninkrijks-relaties	Levering, implementatie (waaronder tenminste: ontsluiting, integratie, configuratie, migratie, conversie), beheer, onderhoud, doorontwikkeling en hosting van een facilitair managementinformatiesysteem (FMIS), inclusief een gebruiksvriendelijk gebruikersportaal en mobiele app's, geleverd op basis van SaaS dienstverlening.	ISO 27001 ISO 27002 HTTPS en HSTS TLS DNSSEC IPv4 en IPv6 ODF PDF SAML SPF DKIM DMARC STARTTLS & DANE Digitoegankelijk Open API		**perfect**	**(100%)**
Rijks-waterstaat	Ontwikkeling van een bouwblok audio welke de huidige audiosystemen- en toepassingen in de verkeerscentrales voor wegverkeer en objectbediening, bediencentrales, verkeersposten en objecten moet gaan vervangen.	ISO 27001 ISO 27002 HTTPS en HSTS TLS	IPv4 en IPv6	**op de goede weg:** op weg naar perfect	**(80%)**
RIVM (Rijksinstituut voor Volks-gezondheid en Milieu)	Een applicatie die het digitaliseren van het analoge proces gegevensregistratie hielprikafname mogelijk maakt. Het continu aanpassen van de applicatie op basis van de optimalisatie in het ketenproces; Realiseren van een koppeling van en naar Praeventis.	ISO 27001 ISO 27002 HTTPS en HSTS TLS SAML	DNSSEC IPv4 en IPv6	**op de goede weg:** op weg naar perfect	**(71%)**
Belasting-dienst	Vervangen van de huidige SAP infrastructuur door een nieuwe SAP gecertificeerde oplossing welke geschikt is voor in eerste instantie de HANA database en later voor S/4HANA.	ISO 27001 ISO 27002 HTTPS en HSTS TLS DNSSEC	IPv4 en IPv6 OpenAPI spec.	**op de goede weg:** op weg naar perfect	**(71%)**
Rijks-waterstaat	Uitbesteden technisch beheer van het specialistisch platform en (kort cyclische) ontwikkeling van het specialistisch platform Service Management Systeem TOPdesk.	ISO 27001 ISO 27002 HTTPS en HSTS TLS	PDF ODF	**op de goede weg:** op weg naar perfect	**(67%)**
CBR	Correctief, preventief en adaptief onderhoud van hun RGahS systeem (Rijgeschiktheid aan het Stuur, ook wel OPUS).	ISO 27001 ISO 27002	PDF ODF	**op de goede weg:** midden-moot	**(50%)**
Ministerie van Financiën	Een informatiesysteem dat het achterliggende proces van schatkistbankieren ondersteunt, inclusief de schatkistadministratie, de procesondersteuning en de portalen voor de deelnemers en de medewerkers die met het informatiesysteem werken.	ISO 27001 ISO 27002 CMIS Digikoppeling XBRL Ades Baseline pr. SAML	HTTPS & HSTS TLS ODF DNSSEC SPF DKIM DMARC STARTTLS & DANE	**op de goede weg:** midden-moot	**(47%)**

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
Politie	Een MultiMedia Service ("MMS"): een online dienst, waar multimediabestanden (audio-, beeld- en videomateriaal, en combinaties daarvan) kunnen worden geüpload, opgeslagen, afgespeeld, bewerkt, gedeeld en ontsloten.	ISO 27001 ISO 27002 ODF PDF Digitoegankelijk SAML OpenAPI spec.	DNSSEC HTTPS & HSTS TLS IPv4 en IPv6 SPF DKIM DMARC STARTTLS & DANE	**op de goede weg:** midden -moot	**(47%)**
Kamer van Koophandel	In 2019 is de KVK gestart met het inrichten van een Intelligence Platform (IP), dat bestaat uit: BI-datastore (datawarehouse); Datavisualisatietool; Analyse-omgeving (tools, w.o. al aangeschafte Python, KNIME, R). Het gaat in deze aanbesteding enkel om de Datavisualisatietool.	ISO 27001 ISO 27002 HTTPS en HSTS TLS SAML PDF	ODF SPF DKIM DMARC DNSSEC IPv4 en IPv6 STARTTLS & DANE	**op de goede weg:** midden -moot	**(46%)**
Belasting-dienst	Het leveren van een Facilitair Management Informatie Systeem (FMIS) oplossing en/of additionele diensten aan de Belastingdienst.	ISO 27001 ISO 27002 IHTTPS en HSTS TLS SAML IFC	ODF SPF DKIM DMARC IPv4 en IPv6 DNSSEC PDF STARTTLS & DANE	**op de goede weg:** midden -moot	**(43%)**
DUO (Dienst Uitvoering Onderwijs)	Examenafnamesoftware (SAAS) ten behoeve van de afname van inburgeringsexamens en de Naturalisatietoets in Nederland en het buitenland. De logistiek en administratie van deze examens voert DUO uit met behulp van een informatiesysteem. In dit geval betreft dat een specifiek voor DUO ingerichte SAP-omgeving.	ISO 27001 ISO 27002 HTTPS en HSTS TLS Digitoegankelijk	PDF SPF DMARC DKIM IPv4 en IPv6 DNSSEC STARTTLS & DANE	**op de goede weg:** midden -moot	**(42%)**
Belasting-dienst	De levering van een Bezoeker Verwijs Systeem (BVS) oplossing met additionele en product-specifieke diensten.	ISO 27001 ISO 27002 HTTPS en HSTS TLS Digitoegankelijk	ODF DNSSEC IPv4 en IPv6 SPF DMARC DKIM STARTTLS & DANE	**op de goede weg:** midden -moot	**(42%)**
NWO (Nederlandse Organisatie voor Weten-schappelijk Onderzoek)	Perceel 1: Ontwerp, bouw en beheer van nwo.nl en nro.nl en kennisrotonde.nl. Perceel 2: De Opdracht richt zich op het ontwikkelen en bouwen van een nieuwe website en daarnaast het hosten en technisch onderhouden en beheren van de website.	ISO 27001 ISO 27002 HTTPS en HSTS TLS Digitoegankelijk	SPF DMARC DKIM DNSSEC IPv4 en IPv6 ODF SAML CMIS STARTTLS & DANE	**op de goede weg:** midden -moot	**(36%)**

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
Ministerie van Buitenlandse Zaken	Het sluiten van een overeenkomst met één dienstverlener voor het leveren van een Cloud dienstverlening ten behoeve van het 24/7 BZ ContactCenter.	ISO 27001 ISO 27002 HTTPS en HSTS TLS PDF	ODF DKIM DMARC SPF Open API DNSSEC IPv4 en IPv6 CMIS SAML STARTTLS & DANE	**op de goede weg:** nog een heel eind te gaan	**(33%)**
NZa (Nederlandse Zorgautoriteit)	De scope van de opdracht is de ondersteuning van alle fases in het Electronic Discovery Reference Model (EDRM) middels een SaaS-oplossing. Dit moet een totaaloplossing zijn inclusief hosting, software, processing, beheer, support en onderhoud.	ISO 27001 ISO 27002 HTTPS en HSTS TLS	IPv4 en IPv6 DNSSEC ODF PDF SPF DKIM DMARC STARTTLS & DANE	**op de goede weg:** nog een heel eind te gaan	**(33%)**
ZonMW	Het ter beschikking stellen, implementeren, onderhoud en support van een nieuwe specifieke op sociale intranetten ontwikkelde technologie en bijbehorende nieuwe functionaliteiten via SaaS.	ISO 27001 ISO 27002 HTTPS en HSTS TLS	IPv4 en IPv6 DNSSEC SAML SPF DMARC DKIM PDF STARTTLS & DANE	**op de goede weg:** nog een heel eind te gaan	**(33%)**
EBN bv (Energie Beheer Nederland)	Op zoek naar een leverancier die de monitoring, technisch beheer, logging, signalering en terugkoppeling in periodieke rapportages van 'Mijn Zaak' biedt.	ISO 27001 ISO 27002	HTTPS en HSTS TLS SAML IPv4 en IPv6	**op de goede weg:** nog een heel eind te gaan	**(33%)**
LVNL (Lucht-verkeers-leiding Nederland)	Het beheer en de ontwikkeling van het portalen domein websites. Dit omvat o.a. de LVNL verder uit kunnen bouwen (met inzet Umbraco platform), gebruikers (o.a. potentiele sollicitanten) van de website een betere gebruikerservaring geven (prettig, makkelijk en snel gebruik), en het sparren en meedenken over het realiseren van nieuwe voorgestelde functionaliteiten.	ISO 27001 ISO 27002	HTTPS en HSTS TLS Digitoegankelijk DNSSEC	**op de goede weg:** nog een heel eind te gaan	**(33%)**
Ministerie van Binnenlandse Zaken en Koninkrijks-relaties	Onderdeel Financiële Dienstverlening (FD) van Uitvoeringsorganisatie Bedrijfsvoering Rijk (UBR) wil haar Exact landschap uitbesteden aan een marktpartij die komende jaren als integrale partner fungeert. Drie delen: managed hosting van het Exact landschap, doorontwikkeling van de hoofdapplicaties en de transitie en migratie.	ISO 27001 ISO 27002	HTTPS en HSTS TLS DNSSEC IPv4 en IPv6 NLCIUS SAML	**op de goede weg:** nog een heel eind te gaan	**(25%)**
IFV (Instituut Fysieke Veiligheid)	Het ontwikkelen van een applicatie op basis van de code van Farsite en Rothermel met de huidige en aanvullende functionaliteiten. De omvang is het ontwerp van zowel front-end, middleware en back-end plus daarna het applicatiebeheer, functioneel beheer (2e lijn), hosting en technisch beheer van de applicatie voor het NBVM.	ISO 27001 ISO 27002	SAML DNSSEC Geo HTTPS en HSTS TLS IPv4 en IPv6	**op de goede weg:** nog een heel eind te gaan	**(25%)**

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
LDCR (Landelijk Diensten-centrum voor de Rechtspraak)	Revitaliseren van primaire processystemen van de Rechtspraak. De gemigreerde applicatie dient de eindgebruiker de mogelijkheid te geven te werken in een GUI die gebaseerd is op web technologie.	HTTPS en HSTS TLS Digitoegankelijk OpenAPI spec.	ISO 27001 ISO 27002 PDF SAML IPv4 en IPv6 DNSSEC SPF DKIM DMARC ECLI BWB JCDR STARTTLS & DANE	**op de goede weg:** nog een heel eind te gaan	**(24%)**
Schiphol	Een extern gehost informatiesysteem (SaaS). Het systeem dient ter ondersteuning van de activiteiten die erop gericht zijn Schiphol ijs- en sneeuwvrij te maken en te houden.	HTTPS en HSTS TLS PDF	Geo DNSSEC ISO 27001 ISO 27002 IPv4 enIPv6 Open API SPF DMARC DKIM STARTTLS & DANE	**op de goede weg:** nog een heel eind te gaan	**(23%)**
LVNL (Lucht-verkeers-leiding Nederland)	De aanschaf en implementatie van een *e-lending solution*, inclusief configuratie, technische applicatiebeheer, hosting en onderhoud.	ISO 27001 ISO 27002 PDF	IPv4 en IPv6 DNSSEC Digitoegankelijk HTTPS en HSTS TLS SPF DMARC DKIM Geo STARTTLS & DANE	**op de goede weg:** nog een heel eind te gaan	**(23%)**
Belasting-dienst	Een Maritieme Informatie voor Douane (MID) oplossing in de vorm van een SAAS. Het is opgedeeld in twee percelen, maar die zijn inhoudelijk identiek: beschikbaar stellen van een MID systeem. Voor perceel 1 is dat voor douane-afdeling Onbekende Sub- en Objecten Douane Toezicht (OSODT), voor perceel 2 is dat Douane Landelijk Tactisch Centrum (DLTC).	ISO 27001 ISO 27002 PDF	HTTPS & HSTS TLS DNSSEC IPv4 en IPv6 SPF DKIM DMARC ODF Geo STARTTLS & DANE	**op de goede weg:** nog een heel eind te gaan	**(23%)**
LVNL (Lucht-verkeers-leiding Nederland)	Op zoek naar een gecertificeerde Zabbix-reseller of -partner. Zabbis is open-source enterprise monitoring software die vaker in het luchtvaartdomein wordt toegepast. In scope zijn meerdere diensten.	HTTPS en HSTS TLS	ISO 27001 ISO 27002 DNSSEC DKIM DMARC SPF STARTTLS& DANE	**op de goede weg:** nog een heel eind te gaan	**(22%)**

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
KB (Koninklijke Biblioheek)	De 2e lijns IT-ondersteuning (UEM) voor circa 550 wps. Inbegrepen in de gevraagde dienstverlening is het verzorgen van tweedelijns support door Opdrachtnemer. De tweedelijns (remote) servicedesk handelt meldingen af die niet door de eerstelijns Servicedesk van KB uitgevoerd kunnen worden.	ISO 27001 ISO 27002	HTTPS & HSTS TLS SPF DKIM DMARC STARTTLS & DANE PDF ODF	**op de goede weg:** nog een heel eind te gaan	**(20%)**
RIVM (Rijksinstituut voor Volks-gezondheid en Milieu)	Serialisatie software (ook wel decommisioning software genoemd) met compatible hardware voor het afmelden van geleverde geneesmiddelen in de NMVS database.	ISO 27001 ISO 27002	IPv4 en IPv6 HTTPS en HSTS TLS DNSSEC PDF SPF DKIM DMARC STARTTLS & DANE	**op de goede weg:** nog een heel eind te gaan	**(18%)**
Ministerie van Binnenlandse Zaken en Koninkrijks-relaties	Komen tot een nieuwe overeenkomst voor het onderhoud, beheer en support van Exact software, modules en maatwerk.	ISO 27001 ISO 27002	Digikoppeling DNSSEC PDF HTTPS & HSTS TLS SPF DKIM DMARC STARTTLS & DANE	**op de goede weg:** nog een heel eind te gaan	**(18%)**
Kansspel-autoriteit	CRUKS (Centraal Register voor de Uitsluiting van KansSpelen) wordt online ter beschikking gesteld en moet worden beheerd (zowel Functioneel als Technisch (Applicatie)beheer) en in de toekomst aangepast ofwel verder ontwikkeld kunnen worden.	ISO 27001 ISO 27002	HTTPS & HSTS TLS Digitoegankelijk DNSSEC IPv4 en IPv6 SAML SPF DKIM DMARC STARTTLS & DANE	**op de goede weg:** nog een heel eind te gaan	**(17%)**
RvA (Raad voor Accreditatie)	Digitaliseren van het primaire proces 'Beoordelen en rapporteren auditbevindingen'. Hiertoe wordt op de korte termijn een Audit-rapportagetool, een Normentool en bijbehorend Toegangsbeheer (Identity and Access management) ingericht. Op de middellange termijn uitbreiden met aanvullende functionaliteit, zoals een Planningstool en Onboarding (accreditatie-aanvraagproces) tool.	ISO 27001 ISO 27002	HTTPS en HSTS TLS DNSSEC PDF SAML SPF DMARC DKIM IPv4 en IPv6 STARTTLS & DANE	**op de goede weg:** nog een heel eind te gaan	**(17%)**
Ministerie van Buitenlandse Zaken	De levering inclusief bijbehorende dienstverlening van zo'n 14 MultiFunctional Printers (MFPs) voor de ambassade van Nederland in Brussel. Onder bijbehorende dienstverlening wordt vooral onderhoud en ondersteuning verstaan.	PDF	ISO 27001 ISO 27002 HTTPS en HSTS TLS IPv4 en IPv6	**op de goede weg:** nog een heel eind te gaan	**(17%)**

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
Kamer van Koophandel	Het converteren/omzetten van bij KVK gedeponeerde originele 'papieren' jaarrekeningen, in pdf, volgens een voorgeschreven richtlijn, naar een formaat van standaard jaarrekeningen (CSV bestand).	*(geen)*	ISO 27001 ISO 27002	**slecht**	**n.v.t.**
Rijks-waterstaat	Een opdracht voor 'het beheer en onderhoud, actualisatie en verdere ontwikkeling van het tijpoortadviseringssysteem PROTIDE (Probabilistic Tidal Window Determination)'.	*(geen)*	ISO 27001 ISO 27002 Geo	**slecht**	**n.v.t.**
Belasting-dienst	Het leveren van Onderhoud en Support en Additionele Diensten van Programmatuur die, op moment van publicatie van deze aanbesteding, onderdeel van de Installed Base zijn.	*(geen)*	ISO 27001 ISO 27002	**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	
Gemeente Gorinchem	Het leveren, implementeren en onderhoud/ondersteuning van een standaard on-premise ICT-applicatie ten behoeve van de vergunningverlening, toezicht en handhaving.	ISO 27001 ISO 27002 HTTPS en HSTS TLS DNSSEC Digikoppeling Geo OpenAPI spec. DKIM DMARC SPF STARTTLS & DANE StUF SAML		**perfect**	**(100%)**
Bizob (35 gemeenten en organisaties)	Werkend opleveren en vervolgens ter beschikking stellen van een burgerzaken-applicatie, inclusief onderhoud en ondersteuning. De burgerzaken-applicatie draait off-premise, waarbij de verantwoordelijkheid voor de hosting en onderhoud van de burgerzakenapplicatie bij de inschrijver ligt (SAAS).	Digitoegankelijk Digikoppeling DNSSEC HTTPS en HSTS TLS ISO 27001 ISO 27002 SAML SPF DKIM DMARC STARTTLS & DANE OpenAPI spec. PDF StUF	IPv4 en IPv6 ODF	**op de goede weg:** op weg naar perfect	**(88%)**
Gemeente Purmerend	Een vastgoedbeheersysteem. In het systeem is het gemeentelijke vastgoed, gebouwen en gronden met bijbehorende kadastrale percelen geregistreerd, met uitzondering van de openbare ruimte, en wordt het vastgoedbeheersysteem ingezet voor het beheer ervan.	DNSSEC Digitoegankelijk HTTPS en HSTS TLS IPv4 en IPv6 ISO 27001 ISO 27002 CMIS StUF PDF SAML SPF DKIM DMARC STARTTLS & DANE	ODF Digikoppeling	**op de goede weg:** op weg naar perfect	**(88%)**
Veiligheids-regio Groningen	Een technisch platform voor de ondersteuning van de beheerprocessen van de teams Techniek & Ondersteuning (T&O), Facilitaire Zaken (FZ) en Informatiemanagement (IM) realiseren.	DNSSEC HTTPS en HSTS TLS ISO 27001 ISO 27002 PDF SAML SPF DKIM DMARC STARTTLS & DANE	ODF IPv4 en IPv6	**op de goede weg:** op weg naar perfect	**(85%)**

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
Gemeente Amsterdam	Beschikbaar stellen, inrichten, hosten en in beheer nemen van een systeem dat voorziet in de ondersteuning van P&O processen zoals "Werving, Selectie & Matching", op basis van een SaaS oplossing.	DNSSEC HTTPS en HSTS TLS ISO 27001 ISO 27002 SAML DKIM DMARC SPF	STARTTLS & DANE IPv4 en IPv6	**op de goede weg:** op weg naar perfect	**(82%)**
Gemeente Langedijk	Het leveren, onderhouden en ondersteunen van een zaaksysteem/DMS/RMA o.b.v. SaaS. De opdracht omvat het leveren van software inclusief koppelingen en het leveren van verschillende diensten.	DNSSEC Digitoegankelijk HTTPS en HSTS TLS ISO 27001 ISO 27002 SPF DKIM DMARC STARTTLS & DANE SAML StUF	Digikoppeling PDF IPv4 en IPv6	**op de goede weg:** op weg naar perfect	**(80%)**
Gemeente Maastricht	De aanschaf van een nieuw zaaksysteem inclusief implementatie, hosting, beheer en onderhoud ten behoeve van de gemeente Maastricht en mogelijk de gemeente Meerssen (optie).	DNSSEC HTTPS en HSTS TLS ISO 27001 ISO 27002 StUF Geo SAML SPF DKIM DMARC STARTTLS & DANE	Digikoppeling PDF IPv4 en IPv6	**op de goede weg:** op weg naar perfect	**(80%)**
Veiligheids-regio R'dam Rijnmond[8]	Volledig werkende Wifi-voorziening, inclusief ontwerpen, leveren, implementeren en configureren.	ISO 27001 ISO 27002 WPA2 Enterprise	IPv4 en IPv6	**op de goede weg:** op weg naar perfect	**(75%)**
Veiligheids- en gezondheids regio Midden-Gelderland	Een oplossing ter ondersteuning van het documentmanagement (DMS) volgens de Archiefwet en van de werkprocessen.	Digitoegankelijk PDF ODF HTTPS en HSTS TLS ISO 27001 ISO 27002 SAML StUF SPF DKIM DMARC CMIS	IPv4 en IPv6 Digikoppeling DNSSEC Ades baseline pr. STARTTLS & DANE	**op de goede weg:** op weg naar perfect	**(72%)**

[8] Deze aanbesteding is naderhand ingetrokken.

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
Gemeente Midden Groningen	Een zaaksysteem; een systeem waarmee de processen van dienstverlening en de bedrijfsvoering door middel van zaakgericht werken ondersteund worden.	ISO 27001 ISO 27002 DNSSEC Digitoegankelijk CMIS StUF PDF SAML DKIM DMARC SPF STARTTLS & DANE	HTTPS en HSTS TLS Digikoppeling IPv4 en IPv6 ODF Geo	**op de goede weg:** op weg naar perfect	**(67%)**
Werk-organisatie De BUCH (gemeenten Bergen, Uitgeest, Castricum, Heiloo)	De huidige burgerzaken-oplossing (bestaande uit twee systemen) te vervangen (met één systeem). De gemeenten vragen "een Cloud, bij voorkeur SaaS oplossing".	DNSSEC HTTPS en HSTS TLS ISO 27001 ISO 27002 StUF SAML CMIS PDF SPF DKIM DMARC WPA2 Enterprise	Digikoppeling Digitoegankelijk IPv4 en IPv6 ODF OpenAPI spec. EML_NL STARTTLS & DANE	**op de goede weg:** midden-moot	**(65%)**
Gemeente Soest	Het betreft een aanbesteding voor het leveren, implementeren en onderhouden van een zaaksysteem voor de gemeente Soest.	HTTPS en HSTS ISO 27001 ISO 27002 PDF TLS SAML StUF SPF DKIM DMARC	DNSSEC Digikoppeling Digitoegankelijk IPv4 en IPv6 Geo STARTTLS & DANE	**op de goede weg:** midden-moot	**(63%)**
Gemeente Oss	De aanschaf, implementatie en onderhoud van een leerlingvolgsysteem ten behoeve van het Regionaal Bureau Leerplicht en voortijdig schoolverlaten Brabant Noordoost (RBL BNO) en de aanschaf, implementatie en onderhoud van een module leerlingenvervoer.	DNSSEC Digikoppeling CMIS HTTPS en HSTS TLS ISO 27001 ISO 27002 StUF PDF	IPv4 en IPv6 SPF DKIM DMARC STARTTLS & DANE ODF SAML	**op de goede weg:** midden-moot	**(56%)**
Gemeente Moerdijk	Een beheersysteem voor de openbare ruimten waarmee de gemeente de gehele openbare ruimte integraal kan beheren en waarmee lopende en toekomstige ontwikkelingen kunnen worden ondersteund.	HTTPS en HSTS ISO 27001 ISO 27002 SAML StUF PDF TLS Geo	ODF DNSSEC SPF DKIM DMARC STARTTLS & DANE Digikoppeling IPv4 en IPv6	**op de goede weg:** midden-moot	**(50%)**

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
Gemeente Venlo	Een pakket aan diensten waaronder: openbaar vervoer mogelijkheden, elektrische deelauto's en - fietsen plus de laadinfra, de applicaties om dit alles te bedienen, service en onderhoud. Kortom een compleet pakket wat ook wel Mobility as a Service wordt genoemd. De ICT component bevat de reserverings- en gebruikssoftware en de monitoring, data en rapportages.	ISO 27001 ISO 27002 Digitoegankelijk	HTTPS en HSTS TLS ODF	**op de goede weg:** midden -moot	**(50%)**
Provincie Gelderland	Aanvragen, onderhouden en beheren van dataverbindingen welke nu ingezet voor het ontsluiten van verkeersregelinstallaties (VRI's) en steeds meer camera's. Provincie Gelderland ziet kansen om in de toekomst deze verbindingen voor meerdere doeleinden in te zetten, zoals verbindingen naar bijvoorbeeld kleine buitenkantoren of objecten (sensoren).	HTTPS en HSTS TLS IPv4 en IPv6	ISO 27001 ISO 27002 SAML	**op de goede weg:** midden -moot	**(50%)**
Veiligheids-regio Zeeland	Het realiseren, implementeren, beheren en onderhouden van een geïntegreerde softwarematige SAAS oplossing die binnen de organisatie van de opdrachtgever de processen op het gebied van HRM en Financiën, waaronder salarisverwerking ondersteunt.	HTTPS en HSTS TLS ISO 27001 ISO 27002 XBRL PDF NLCIUS SAML Digitoegankelijk	IPv4 en IPv6 ODF Digikoppeling DNSSEC CMIS SETU SPF DKIM DMARC STARTTLS &DANE	**op de goede weg:** midden -moot	**(47%)**
De Connectie (gemeenten Arnhem, Renkum, Rheden)	Een VMS-inhuursysteem: een softwarematig systeem dat alle voorkomende organisatorische en administratieve aspecten bij het registreren en verwerken van gegevens die samenhangen met de inzet, inhuur, van flexibel personeel invult.	DNSSEC Digitoegankelijk HTTPS en HSTS TLS ISO 27001 ISO 27002 CMIS StUF	IPv4 en IPv6 Ades baseline pr. SPF DKIM DMARC STARTTLS & DANE PDF NLCIUS SAML SETU	**op de goede weg:** midden -moot	**(44%)**
Gemeente Amsterdam	Het Sport Accommodatie Verhuur Systeem faciliteert op een efficiënte en gebruiksvriendelijke voor zowel gemeente medewerkers als burgers van Amsterdam voor de verhuur van sport accommodaties in Amsterdam. Het betreft een SaaS-oplossing inclusief hosting.	HTTPS en HSTS TLS SAML ISO 27001 ISO 27002	Digikoppeling Digitoegankelijk DNSSEC SPF DKIM DMARC STARTTLS & DANE IPv4 en IPv6	**op de goede weg:** midden -moot	**(38%)**
Gemeente Kerkrade	Een all-in-one oplossing voor het sociaal domein.	ISO 27001 ISO 27002 CMIS Digikoppeling PDF StUF	ODF Digitoegankelijk DNSSEC SPF DKIM DMARC STARTTLS & DANE HTTPS en HSTS TLS IPv4 en IPv6	**op de goede weg:** midden -moot	**(38%)**

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
Gemeente Delft	Het leveren van een oplossing voor het publiceren van beleidsregels in de beleidsinstrumenten die de Omgevingswet voorschrijft voor gemeenten.	ISO 27001 ISO 27002 HTTPS en HSTS TLS PDF SAML	SPF DKIM DMARC Digikoppeling DNSSEC NLCS BWB JCDR IPv4 en IPv6 STARTTLS & DANE	**op de goede weg:** midden -moot	**(38%)**
Provincie Limburg	De levering, implementatie en onderhoud van een leerplatform; een systeem waarin medewerkers kunnen zoeken naar in-company en extern leeraanbod.	DNSSEC HTTPS en HSTS TLS ISO 27001 ISO 27002	IPv4 en IPv6 SPF DKIM DMARC STARTTLS & DANE CMIS E-portfolio NL LOM SAML	**op de goede weg:** midden -moot	**(36%)**
Veiligheids-regio Brabant-Noord	Het implementeren, beheren en onderhouden van een materieelbeheersysteem (SaaS), die de volgende functionaliteiten omvat: • Gebouwen en middelen beheer • Materieel- en materiaalbeheer • Rapportage en monitoring • Onderhoudswerkzaamheden • onderhouds-/keuringagenda	HTTPS en HSTS ISO 27001 ISO 27002 PDF TLS	IPv4 en IPv6 ODF SAML SPF DKIM DMARC STARTTLS & DANE DNSSEC IFC	**op de goede weg:** midden -moot	**(36%)**
Gemeente Noordenveld	ICT oplossing voor de uitvoeringsondersteuning van het Fysiek Domein, specifiek de processen van "Vergunning verlenen", "Toezicht houden" en "Handhaven"(VTH) in verband met het invoeren van de Omgevingswet.	ISO 27001 ISO 27002 StUF PDF SAML Digikoppeling	HTTPS en HSTS TLS SPF DKIM DMARC STARTTLS & DANE CMIS DNSSEC Geo IPv4 en IPv6 ODF	**op de goede weg:** midden -moot	**(35%)**
Gemeente Beverwijk	Het plaatsen en richten van verschillende hardware, zoals servers, storage en back-ups, migratie van data, installatie van een virtualisatieplatform vSphere, on-the-job training, testen van verschillende omgevingen, licenties die voor het functioneren van de nieuwe ICT-infrastructuur nodig zijn en (periodiek) onderhoud op alle geleverde hardware.	ISO 27001 ISO 27002	HTTPS en HSTS TLS IPv4 en IPv6 PDF	**op de goede weg:** nog een heel eind te gaan	**(33%)**

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
Gemeente Haarlemmermeer	Een handhaafsysteem om haar handhavingstaken zoveel als mogelijk digitaal en informatie gestuurd uit te voeren, te registreren en te ondersteunen. In ieder geval op een wijze die het mobiel digitaal handhaven mogelijk maakt, zodanig dat handhavers op straat direct beschikking hebben over alle voor hun werk relevante informatie (input) en dat handhavers een zo groot mogelijk deel van de administratieve afhandeling en rapportages op straat kunnen uitvoeren (output).	HTTPS en HSTS TLS CMIS StUF	Digikoppeling DNSSEC ISO 27001 ISO 27002 SPF DKIM DMARC STARTTLS & DANE IPv4 en IPv6	**op de goede weg:** nog een heel eind te gaan	**(31%)**
Gemeente Rotterdam	Software waarmee meerdere nieuwsoverzichten (op verschillende onderwerpen / thema's / gebieden) kunnen worden opgezet en geredigeerd. De beoogde partij moet digitale content kunnen leveren uit voor de gemeente relevante bronnen en regelt de auteursrechten die daaraan zijn verbonden.	HTTPS en HSTS TLS PDF	DNSSEC SPF DKIM DMARC STARTTLS & DANE ISO 27001 ISO 27002 IPv4 en IPv6	**op de goede weg:** nog een heel eind te gaan	**(27%)**
Werk-organisatie CGM (gemeenten Cuijk, Grave, Mill & Sint Hubert)	Levering, installatie, bedrijfsklaar opleveren, beheren en servicen van een integrale telecommunicatievoorziening. De nieuwe infrastructuur bevat de volgende onderdelen binnen één omgeving: telecommunicatiesysteem, contactcenteromgeving en rapportagetools, Mobiele telefonie, Vaste telefonie (netlijnen en verbindingen), en Vast - mobiel integratie (noodzakelijke integratie mobiele telefonie).	ISO 27001 ISO 27002	HTTPS en HSTS TLS IPv4 en IPv6 SPF DKIM DMARC STARTTLS & DANE	**op de goede weg:** nog een heel eind te gaan	**(22%)**
GBTwente (10 gemeenten)	Een PSA/HRM-systeem en aanverwante dienstverlening ten behoeve van de verbetering van de organisatieprocessen met betrekking tot Personeel-salaris en HRM.	ISO 27001 ISO 27002	DNSSEC IPv4 en IPv6 PDF HTTPS en HSTS TLS E-portfolio SETU NLCIUS	**op de goede weg:** nog een heel eind te gaan	**(20%)**
Veiligheids-regio R'dam Rijnmond	E-HRM-, Salarisadministratiesoftware en de bijhorende Salarisdienstverlening ter vervanging van het huidige contract. Doel van de dienst/het platform is ondersteuning te bieden voor: • Verwerken, bijhouden en wijzigen van personeelsgegevens door HRM • Inzicht in personeelsgegevens voor HRM, leidinggevenden en medewerkers • Medewerkers-/Managers Selfservice voor het aanvragen van verlof, declaraties, etc.	ISO 27001 ISO 27002 PDF	DNSSEC Digitoegankelijk IPv4 en IPv6 E-portfolio HTTPS en HSTS TLS SAML SETU ODF SPF DKIM DMARC STARTTLS & DANE	**op de goede weg:** nog een heel eind te gaan	**(19%)**

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
Gemeente Delft	De vervanging VTH vergunningensoftware i.v.m. invoering Omgevingswet om te komen tot het leveren van een oplossing welke tot doel heeft de processen voor het ontvangen en afhandelen van (omgevings)vergunningen en het uitvoeren van toezicht en handhaving op deze vergunningen uit te kunnen voeren.	ISO 27001 ISO 27002 StUF	DNSSEC Digikoppeling COINS HTTPS en HSTS TLS IPv4 en IPv6 IFC PDF ODF SPF DKIM DMARC STARTTLS & DANE	**op de goede weg:** nog een heel eind te gaan	**(19%)**
Provincie Groningen	Een flexibele, doch betrouwbare personeels-registratie die de (maandelijkse) verloning juist uit kan voeren, maar vooral op ieder moment inzicht kan geven in de actuele stand van het personeels-bestand, niet alleen in kwantiteiten, maar vooral ook in kwaliteiten en van daaruit de medewerker en het management het juiste inzicht kan verschaffen om de goede keuzes te maken als het gaat om inzet van het belangrijke instrument: het menselijk kapitaal van de provincie.	ISO 27001 ISO 27002	DNSSEC E-portfolio HTTPS en HSTS TLS IPv4 en IPv6 PDF SPF DKIM DMARC STARTTLS & DANE	**op de goede weg:** nog een heel eind te gaan	**(17%)**
Empatec (sociaal werkbedrijf) (gemeenten De Fryske Marren, Harlingen, Waadhoeke, Súdwest Fryslân, Terschelling, Vlieland)	Het werken met HR en salarisgegevens veranderen van een centrale administratie (waarmee informatie via papieren formulieren, mails en gesproken communicatie wordt uitgewisseld) naar een decentraal proces (in de gehele organisatie waarbij alle betrokkenen direct inzicht in hun eigen informatie hebben en daarin direct mutaties kunnen doen).	ISO 27001 ISO 27002	Digitoegankelijk DNSSEC E-portfolio HTTPS en HSTS TLS IPv4 en IPv6 SPF DKIM DMARC STARTTLS & DANE	**op de goede weg:** nog een heel eind te gaan	**(17%)**
Gemeente Delfzijl	Voor de nieuwe gemeente Eemsdelta een gebruiksklaar Human Resource Management, “welke vanuit de cloud wordt beheerd en onderhouden”. Het betreft dus een SaaS. In scope vallen o.a. de volgende functionaliteiten: personeelsadministratie, salarisadministratie, digitale personeelsdossiers (met daarin portfolio, bekwaamheid, gespreksverslagen en opleidingen), Management- en signaalrapportages, en Medewerker- en managementselfservice.	PDF	HTTPS en HSTS TLS ISO 27001 ISO 27002 DNSSEC IPv4 en IPv6 E-portfolio SAML SETU ODF SPF DKIM DMARC STARTTLS & DANE Ades baseline pr.	**op de goede weg:** nog een heel eind te gaan	**(6%)**
Gemeente Berkelland	Het ontwikkelen van een mobile website en de bouw van een drietalige app (DU-EN-NL) ten behoeven van het Duits-Nederlandse grensgebied van de Berkel. Het gaat om de ontwikkeling van de zogeheten BerkelGame.		HTTPS en HSTS TLS ISO 27001 ISO 27002 DNSSEC Digitoegankelijk	**slecht**	**n.v.t.**

B3. Inventarisatie gebruiksgegevens 2020 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, september 2020,* opgenomen in Bijlage B4).

Van het gebruik van de volgende standaarden is dit jaar geen actuele informatie beschikbaar: Ades Baseline Profiles, CMIS en IFC. De volgende drie standaarden staan pas sinds dit jaar op de 'pas toe of leg uit' lijst: GWSW, NL GOV Assurance profile for OAuth 2.0 en REST-API Design Rules. Met ingang van volgend jaar worden deze standaarden voor het eerst meegenomen in het onderdeel 'gebruiksgegevens'.

B3.1. 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 (september 2020) zijn 548 domeinnamen getoetst die ook in eerdere metingen centraal stonden. In deze september-meting is daarnaast voor het eerst een vergelijking gemaakt met de meetresultaten van een bredere selectie van bijna 1.800 overheidsdomeinnamen. 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 548 primaire (veelgebruikte) internetdomeinen waarop in de IV-meting de focus ligt. In die zin is er nog de nodige winst te boeken.

DKIM, DMARC en SPF

Algemeen

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[9]);
- *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);

[9] Hier vermeld (evenals verderop) is de oorspronkelijke plaatsing op de 'pas toe of leg uit'-lijst.

- *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 548 domeinen van de overheid. Zie hiervoor de IV-meting van medio 2020 (Bijlage B4).
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)
DMARC	73 %	82 %	87 %	88 %	92 %
DMARC policy	28 %	37 %	49 %	58 %	66 %
DKIM	84 %	89 %	90%	92 %	96%
SPF	93 %	95 %	96 %	96 %	97 %
SPF Policy	85 %	88 %	89 %	91 %	91 %

Vergeleken met de vorige monitor is **over de volle breedte** sprake van een **toename van het gebruik**. Let wel: in de monitor 2019 is voor de bijlage 'gebruiksgegevens' gebruik gemaakt van de IV-meting uit maart 2019. 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 66% medio 2020 nog steeds het grootste groeipotentieel. Uit de IV-meting blijkt tot slot dat de hier gemelde stijging zich voordoet bij elke overheidslaag.

Als kanttekening bij dit gunstige beeld moet worden opgemerkt dat een vergelijking met de bredere selectie van bijna 1.800 domeinnamen uitwijst dat de score van het gebruik van deze standaarden daar substantieel lager ligt (15 a 20 procentpunten lager). Dat impliceert dat de focus op de (primaire groep van) 548 domeinen een wat vertekend beeld geeft.

DNSSEC

Algemeen
Een domeinnaamhouder kan met DNSSEC een digitale handtekening toevoegen aan DNS-informatie. Met DNSSEC kan de ontvanger vervolgens de echtheid van de domeinnaaminformatie (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 548 kern-domeinen van de overheid. Zie hiervoor de IV-meting van medio 2020 (Bijlage B4).

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

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

Vergeleken met de meting begin maart 2019 is het gebruik **min of meer stabiel**. Voor web is sprake van een marginale stijging (1%) en voor zowel voor email-verkeer van een daling van 5%. Inzoomend op de verschillende overheidslagen komen een paar opmerkelijke verschillen aan het licht (vergeleken met een jaar terug):

- de categorie 'Rijk' laat als enige een lichte stijging zien, zowel voor web als e-mail, waarbij een 100% score in zicht komt (97% voor web, 98 % voor e-mail);
- het verschil tussen de scores van het gebruik van DNSSEC voor web zijn niet heel groot bij een vergelijking tussen de verschillende overheidslagen (variërend van 88% tot 97%). 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% terwijl zowel provincies als waterschappen een score van onder de 50% laten zien (44% respectievelijk 48%).

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 blijvende aandacht. Dit geldt temeer als de vergelijking wordt gemaakt met het gebruik van deze standaard onder de bredere groep van bijna 1.800 domeinen van de overheid. Voor die grotere groep liggen de procentuele scores van het gebruik lager: 14 procentpunten lager voor wat betreft het web (80% in plaats van 94%) en 12 procentpunten lager voor email (54% in plaats van 66%). De groeipotentie is daar dus nog behoorlijk aanwezig.

HTTPS & HSTS en TLS

Algemeen

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 548 kern-domeinen van de overheid. Zie ook de IV-meting van medio 2020 (Bijlage B4).

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)
HTTPS	89 %	90 %	94 %	95 %	98 %
HSTS	79 %	79 %	85 %	88 %	92 %
TLS	96 %	96 %	97 %	98 %	100 %
TLS cf. NCSC	87 %	89 %	92%	93 %	78 %

Vergeleken met de cijfers uit de monitor van 2019 is het gebruik van de standaarden **HTTPS & HSTS** (overigens net als vorig jaar) **toegenomen**. De grenzen van de groei komen in zicht met percentages van 100% of net daaronder. Het gebruik van **TLS conform NCSC** laat een afwijkend beeld zien, in het bijzonder voor de periode tussen de meting van maart 2020 en september 2020. De hier gesignaleerde **terugval** is 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 hoger komen te liggen bij de toetsing met een lager percentage gebruik als resultaat.

Ook voor deze standaarden is weer een vergelijking gemaakt met de meting onder de breder samengestelde groep van bijna 1.800 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 548 domeinen). Voor HSTS is de score wel duidelijk lager: 65% gebruik bij de breed samengestelde groep, 92% 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 548 domeinen: 60% tegen 78%.

De 5 overheidslagen die in de IV-monitor worden onderscheiden (Rijk, uitvoeringsorganisaties, provincies, gemeenten, waterschappen) laten op een enkel detail na alle een soortgelijke ontwikkeling zien op de standaarden die in bovenstaande tabel zijn onderscheiden.

IPv6 & IPv4

Algemeen

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 548 kern-domeinen van de overheid.

Vergeleken met de uitkomsten in de monitor 2019 is het gebruik **toegenomen**. Dat geldt overigens niet voor elk van de overheidslagen in dezelfde mate. Bij Rijk en uitvoerings-organisaties is sprake van een lichte stijging, vergeleken met de grotere progressie die te zien is bij de drie andere overheidslagen.

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

* 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: na een stabilisatie van ruim een jaar op 17% is uit de meest recente meting gebleken dat de bereikbaarheid van overheidsmail (algemeen) nu (september 2020) ligt op 20%.

Relevante ontwikkeling
Onlangs, 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. In het tempo waarmee de laatste twee jaar voortgang wordt geboekt op de bereikbaarheid van overheidswebsites via IPv6 gaat deze doelstelling niet gehaald worden. Het beeld voor wat betreft e-maildomeinnamen van de overheid is nog minder rooskleurig.

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

Algemeen
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 mei 2008.

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 2020 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
Afhankelijk van de organisatie specifieke risico's en eisen worden passende maatregelen genomen volgens het pas toe of leg uit-principe. Dit betreft overigens ook maatregelen aanvullend op de BIO op basis van NAVO- en EU-kaders. Bij vaststelling van de (inhoudelijke identieke) BIR2017 is afgesproken dat deze per 1-1-2018 geldt voor alle nieuwe informatiesystemen en dat de departementen voor 1-1-2019 plannen hebben opgesteld voor de implementatie van de BIR2017 voor de overige informatiesystemen. In 2019 hebben de departementen gewerkt aan de implementatie van de BIR2017 voor nieuwe systemen. Zodra een rijksoverheidsorganisatie de BIR2017 conform de PDCA-cyclus heeft ingevoerd, heeft zij daarmee ook de BIO 1.0 ingevoerd. De voortgang wordt door CIO Rijk gemonitord in de jaarlijkse CISO- en CIO-gesprekken en gerapporteerd aan ADR en Algemene Rekenkamer.

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.
Inmiddels is 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 zijn ook bezig met een ISO 27001 certificeertraject en nemen daar de BIO ook expliciet in mee. De andere provincies zijn 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.

Waterschappen
In de monitor van vorig jaar 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.

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 rijksoverheid en de gemeenten beperken zich tot een procedurele insteek, met betrekking tot de waterschappen is geen actuele informatie ontvangen. Ten aanzien van de provincies is wel een beknopt actueel beeld beschikbaar.
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.

RPKI

Algemeen
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 het gevolg zijn 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 pas recent op de 'pas toe of leg uit'-lijst, sinds november 2019.

Feitelijk gebruik
Het feitelijk gebruik van RPKI moet nog gestalte gaan krijgen. Op zich is dat niet vreemd gezien de recente datum van plaatsing van deze standaard op de 'pas toe of leg uit' lijst.

Aan zeven deelnemers aan verdiepingssessies overheidsnetwerken (namelijk SSC-ICT, VNG, Belastingdienst, Rijkswaterstaat, ministeries van Defensie en Justitie en Veiligheid en Logius) zijn twee vragen gesteld om een eerste globale indruk te krijgen van het gebruik van RPKI:

- ondertekent uw organisatie routes met RPKI?
- valideert uw organisatie RPKI-ondertekende routes?

De eerste vraag wordt door twee van de zeven respondenten bevestigend beantwoord; de overige vijf antwoorden ontkennend. De tweede vraag wordt vanuit alle zeven organisaties met "nee" beantwoord.
De algemene teneur uit de toelichting bij de beantwoording is dat men nog afwachtend is om over te gaan tot implementatie van de standaard. Daarbij kan onder andere een rol spelen dat men intern nog geen intrinsieke behoefte heeft aan deze standaard, dat de technologie nog nieuw is en dat men eerst meer kennis wil verwerven (het komt te vroeg) of dat men meer zicht wil krijgen op eventuele risico's die kleven aan het gebruik van RPKI. Daarnaast is in deze een belangrijke rol weggelegd voor de upstream providers. De (eventuele wijziging in de) aansluitvoorwaarden die deze providers hanteren kan bepalend zijn voor het moment om over te gaan tot implementatie van RPKI.

Aanvullend op het bovenstaande is met als invalshoek het gebruik van RPKI bij voorzieningen gekeken naar RPKI-ondertekening op zowel IPv4 als IPv6. Daarbij kan worden beschikt over twee meetmomenten: 24 juli en 8 oktober 2020. Bij een vergelijking tussen die beide peildata blijkt het volgende (n= 23 webadressen, verdeeld over 16 voorzieningen):

- RPKI-ondertekening op IPv4 neemt toe van 7 naar 15 webadressen;
- RPKI-ondertekening op IPv6 blijft stabiel op 9 webadressen.

Relevante ontwikkeling
Als follow-up op dit eerste beeld van het gebruik van RPKI is het de ambitie om bij volgende monitors een uitgebreider beeld van het gebruik te kunnen presenteren. Een belangrijke stap daarbij 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 2020

Algemeen
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**
eHerkenning: SAML	168	203	359	439	458
DigiD: SAML	128	290	398	429	558
eHerkenning + DigiD	296	493	757	868	1.016

Bron: navraag bij de beheerders van eHerkenning en DigiD bij Logius.

Uit bovenstaand overzicht kan worden opgemaakt dat voor het vierde achtereenvolgende jaar sprake is van een toename van het aantal aansluitingen op de genoemde voorzieningen en daarmee een **toename** van het gebruik van SAML (+ 17%). Het grootste aandeel van de groei zit bij DigiD (+30%) tegen een groei van 4% bij eHerkenning. Het feit dat het aantal afnemers van de voorzieningen toeneemt is hierbij de verklarende factor.

Bij de voorziening DigiD zijn aansluitingen mogelijk via SAML en het legacy A-select koppelvlak. Van 689 aangesloten organisaties zijn er 558 met een SAML-koppelvlak (140 van deze 558 organisaties hebben beide: niet alleen een SAML maar ook een A-select koppelvlak). De overige 131 organisaties maken uitsluitend gebruik van het A-select koppelvlak. Hier zit derhalve nog potentiële groei voor wat betreft het gebruik van SAML bij DigiD.

STARTTLS & DANE

Algemeen
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 548 domeinen van de overheid. Zie hiervoor de IV-meting van medio 2020 (Bijlage B4).

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)
STARTTLS	94 %	94 %	97 %	98 %	99 %
STARTTLS cf. NCSC	55 %	67 %	76 %	87 %	42 %
DANE	25 %	41 %	45 %	50 %	53 %

Vergeleken met vorig jaar is het gebruik van **STARTTLS toegenomen**. Met een percentage van 99% is op het eerste gezicht nauwelijks nog sprake van enige groeipotentie. Het beeld van dezelfde standaard maar dan conform de aanbevolen configuratie volgens het NCSC laat echter een ander beeld zien. Tot en met de meting van maart 2020 is sprake van een gestage groei, maar inclusief de laatste meting (september 2020) is sprake van een forse **terugval bij STARTTLS cf. NCSC**, van 87% naar 42%. Dit heeft te maken met een aangepaste norm waardoor de lat hoger is komen te liggen.
Het gebruik van **DANE neemt gestaag toe**. Daar zit ook nog steeds verbeterpotentieel. DNSSEC MX toont het directe potentieel voor DANE.

Een vergelijking met de meting onder de breder samengestelde groep van bijna 1.800 domeinnamen van de overheid wijst uit dat het gebruik van STARTTLS ook daar zeer hoog scoort, met 98%. Voor DANE geldt dat echter in mindere mate; de score valt voor die standaard met 34% lager uit dan voor de kerngroep van 548 domeinen (53%).

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 96% voor uitvoeringsorganisaties);
- de terugval in de meest recente meting (september 2020) van STARTTLS conform NCSC is te vinden bij elk van de overheidslagen, maar de onderlinge verschillen waar het de terugval betreft zijn groot. Zo valt de score bij Rijk in de periode van een jaar terug van 84% naar 77% (-7%) terwijl de terugval bij gemeenten veel groter is: van 77% naar 36% (-41%). De scores in terugval bij de andere overheidslagen liggen tussen deze uitersten in;

- het Rijk scoort op het gebruik van DANE beduidend beter (84%) dan de andere overheidslagen. Met name provincies en waterschappen blijven achter met scores van respectievelijk 20% en 28%. Gemeenten en uitvoeringsorganisaties scoren gemiddeld, rond de 53%.

STIX & TAXII

Algemeen

STIX en TAXII maken het mogelijk om dreigingsinformatie over een cyberdreiging of -aanval op een gestructureerde en automatisch verwerkbare manier te beschrijven en in real-time te delen met belanghebbende organisaties. Op basis van de dreigingsinformatie kunnen de betreffende organisaties indien nodig beveiligingsmaatregelen treffen. De standaarden STIX en TAXII staan op de 'pas toe of leg uit' lijst sinds november 2017.

Feitelijk gebruik

Er is geen meetmethode voorhanden om het gebruik van STIX en TAXII inzichtelijk te maken. Daarbij komt dat de adoptiegraad moeilijk is te bepalen omdat producten van leveranciers STIX en TAXII niet standaard ondersteunen (worden derhalve niet vendor-onafhankelijk aangeboden). De vraag naar gebruiksgegevens heeft wel de nodige kwalitatieve informatie opgeleverd, waarbij moet worden onderscheiden naar het nationale niveau en dat van de gemeenten.

Nationaal niveau

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 stelsel van samenwerkingsverbanden tussen het NCSC en organisaties uit de Rijksoverheid en andere vitale sectoren. Bij de Rijksoverheid zijn 134 van de 186 organisaties aangesloten bij het NDN en van de vitale partijen is het merendeel aangesloten; exacte aantallen hiervan worden niet vrijgegeven. Bij het NCSC is onbekend in hoeverre ook provincies en waterschappen gebruik maken van STICX en TAXII. Wanneer een partij is aangesloten bij het NDN worden er sensoren geplaats om de dreigingsinformatie centraal te kunnen verwerken. Het NDN richt zich op het onderling delen van dreigingsinformatie om cybersecurityrisico's en -gevaren sneller waar te nemen. Deelnemers kunnen dan maatregelen nemen om schade te voorkomen of te beperken.

In de monitor van vorig jaar stond het volgende vermeld over het gebruik van STIX en TAXII:

- vier van de in totaal veertien NDN-deelnemers maken gebruik van STIX/TAXII;
- daarbij gaat het om relatief grote spelers;
- het is zeer wel mogelijk dat ook andere deelnemers STIX/TAXII gebruiken (het NCSC heeft hierop geen zicht).

Recente vergelijkbare cijfers zijn niet voorhanden: "met de huidige aantallen deelnemers is dat moeilijk te zeggen".

Een viertal Cyber Emergency Response Teams gaat op korte termijn aangesloten worden bij het NDN om gestructureerd informatie te delen over digitale dreigingen en zijn aangewezen door de minister. Dit zijn GGI-Veilig[10] vanuit de gemeenten, SurfCERT[11] vanuit alle universiteiten, ZorgCERT[12] vanuit de zorgsector en CERT-WM[13] vanuit het Waterschapshuis.

[10] https://www.vngrealisatie.nl/producten/ggi-veilig
[11] https://www.hetwaterschapshuis.nl/cert-wm
[12] https://www.z-cert.nl
[13] https://www.hetwaterschapshuis.nl/cert-wm

Over techniek het volgende. Hierbij wordt gebruik gemaakt van het threat intelligence platform "Open Source Threat Intelligence Platform & Open Standards For Threat Information Sharing" (MISP). In dit platform 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. Ook wordt gebruik gemaakt van het threat intelligence platform "EclecticIQ". De dreigingsinformatie die binnenkomt bij het NDN wordt grotendeels niet aangeleverd in STIX-formaat omdat organisaties weinig STIX dreigingsinformatie ontvangen. Een grote groep van de overheid Security Operations Centers (SOC's), die een Threat Intelligence Platform hebben, maken gebruik van TAXII. De dreigingsinformatie die hierin uitgewisseld wordt gebeurt volgens een STIX-gebaseerd formaat, maar niet volgens de STIX-definitie. De vitale partijen delen hun dreigingsinformatie niet middels STIX.

Gemeentelijk niveau
De Informatiebeveiligingsdienst (IBD) van VNG Realisatie regelt de threat intelligence capabiliteit van de gemeenten in de vorm van GGI-Veilig. Het is niet inzichtelijk welke gemeenten gebruik maken van STIX en TAXII. Het platform van GGI-veilig gaat aangesloten worden (binnen een maand) bij het NDN van het NCSC. Het overgrote deel van de gemeenten heeft niet het 'volwassenheidsniveau' om zelf het proces van threat intelligence uit te voeren waarbij GGI-Veilig dit over kan nemen.
In de aanbesteding van GGI-veilig zijn eisen aan het SIEM-platform[14] gesteld. Hierin staat dat de dreiging informatie bi-directioneel via een koppeling wordt gedeeld. Dit gebeurt op basis van STIX/TAXII en/of XML. Producten/diensten die bij deelnemers in de lokale ICT-infrastructuur geïmplementeerd worden, moeten gemonitord kunnen worden vanuit de centrale SIEM-oplossing. Dit betekent dat geboden oplossingen als logbron moeten kunnen dienen en te koppelen moeten zijn met een logcollector van de gangbare SIEM-systemen. Voor wat betreft het kunnen uitwisselen van dreigingsinformatie geldt dat dit dient te gebeuren middels open standaarden (bijvoorbeeld 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. De aanbesteding is inmiddels achter de rug.

Relevante ontwikkeling
Een nieuwe versie van STIX gaat getest worden en er wordt gekeken of deze praktisch toegepast kan worden. De nieuwe versie moet meer praktische mogelijkheden gaan bieden dan de huidige versie. Het ligt in de lijn der verwachting dat een dergelijke verbetering het gebruik van de standaard bevordert.
Voorts maken de gemeenten een grote stap richting beveiliging van hun netwerkverkeer door middel van het GGI-Veilig programma dat zoals eerder vermeld wordt aangeboden door VNG Realisatie. In de monitor van 2019 werd dit traject aangekondigd, inmiddels is de aansluiting van alle gemeenten op dit platform in volle gang.

WPA2 Enterprise

Algemeen
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

[14] https://www.vngrealisatie.nl/sites/default/files/2018-09/Beschrijvend%20Document%20GGI%20Veilig%201.3%20definitief.pdf

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 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)** *)
Govroam	49	132	244	307	332
Eduroam	157 (mei)	199	215	222	231
samen	206	331	459	529	563

**) Op de website van Govroam zijn de meest actuele gegevens bijgewerkt tot juni 2020. Bij Eduroam is wel een opgave te vinden over september (inmiddels 237).*

Uit bovenstaand overzicht blijkt dat het gebruik van WPA2 Enterprise vergeleken met vorig jaar is **toegenomen** met ruim 6%. Deze stijging vinden we terug bij beide bronnen: zowel bij Govroam als bij Eduroam. Bij beide voorzieningen is het aantal klanten toegenomen.

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
Binnen de Rijksoverheid wordt naast Govroam ook gebruik gemaakt van Rijk2Air. Rijk2Air is de WiFi-voorziening voor toegang tot Internet voor Rijksambtenaren binnen het verzorgingsgebied van SSC-ICT. Rijk2Air maakt gebruik van de WPA2 Enterprise standaard. Rijk2Air wordt echter uitgefaseerd en zal vervangen worden door Govroam. Govroam biedt vergelijkbare functionaliteit, die breder gebruikt kan worden door alle ambtenaren in de aangesloten kantoorpanden.

B3.2. Domein Document en (web/app)content

Digitoegankelijk

Algemeen
Digitoegankelijk is de Nederlandse naam voor de Europese norm 301 549 die voorziet in toegankelijkheidsrichtlijnen voor overheidswebsites en de documenten die daarop gepubliceerd zijn. EN 301 549 verwijst naar de technische standaard WCAG 2.1 van W3C die specificeert hoe content op websites, in webapplicaties en in documenten toegankelijk kunnen worden gemaakt. Daarnaast beschrijft EN 301 549 instructies voor het inkopen van toegankelijke producten en diensten. Door toepassing van Digitoegankelijk

worden websites en webapplicaties voor iedereen toegankelijk, ook voor mensen met functiebeperkingen. Zo krijgt iedereen (dus ook dyslectici, kleurenblinden, slechtzienden, blinden, slechthorende, doven, en mensen met cognitieve of motorische beperkingen) dezelfde toegang tot overheidsinformatie. Vanaf 23 september 2020 is toepassing van deze standaard wettelijk verplicht. De standaard staat op de 'pas toe of leg uit' lijst sinds oktober 2016.

Feitelijk gebruik

De Stichting Accessibility, ondergebracht bij het ministerie van BZK, heeft vorig jaar een vernieuwde onderzoeksaanpak in gang gezet om zicht te krijgen op de toegankelijkheid van websites en mobiele applicaties van Nederlandse overheidsorganisaties. De benodigde eisen die daaraan worden gesteld, zijn vastgelegd in de internationale norm WCAG 2.1 niveau AA die zijn opgenomen in de Europese norm EN 301 549. In de vorige monitor (2019) zijn echter geen gegevens opgenomen over het gebruik van de standaard Digitoegankelijk. De gegevens uit het betreffende onderzoek waren indertijd niet op tijd beschikbaar om in de vorm van een nulmeting opgenomen te worden in de Monitor Open standaarden 2019. Deze gegevens zijn nu wel beschikbaar (*Nulmeting toegankelijkheid 2019,* Stichting Accessibility, oktober 2019).

De nulmeting kent een gelaagde onderzoeksopzet waaruit onder meer de volgende inzichten naar voren komen:

- Globaal beeld: met behulp van testsoftware zijn 1.814 Nederlandse overheidswebsites automatisch onderzocht op toegankelijkheid. Van het totale aantal van 50 succes-criteria kan 5-15% automatisch worden gemeten. De (semi-)automatische tool vond bij 23% van de onderzochte websites geen afwijkingen. Die websites zouden dus potentieel goed toegankelijk zijn. Om te bepalen of dat echt zo is, is echter nog handmatig onderzoek nodig van de succescriteria die niet door de tool worden getoetst.
- Een aanvullende handmatige toetsing van 435 websites (uit de groep van 1.814) op 4 succescriteria per website, specifiek gericht op problemen die het voor mensen met een beperking lastig maken om op een website te navigeren (4-criteria-onderzoek). De resultaten van deze aanvullende toetsing:
    - aanwezigheid van skiplink op de website: bij 76% aanwezig;
    - zichtbaarheid van de focus bij het tabben op de website: bij 70%;
    - logische toetsenbord-volgorde op de website: bij 93% in orde;
    - toetsenbord-toegankelijkheid van de website: 88% positief.
- Meer in de diepte, een aanvullend onderzoek op 60 geselecteerde overheidswebsites. Bij deze 60 websites zijn alle succescriteria handmatig onderzocht. De uitkomst daarvan is dat websites gemiddeld op 12,4 van de 50 getoetste criteria een afwijking vertonen. Geen van de onderzochte websites voldeed aan alle succescriteria.
- Een onderzoek naar 23 mobiele applicaties waarbij deze zijn getoetst op 11 succescriteria. Geen van de mobiele applicaties voldoet volledig aan alle getoetste succescriteria.
- Naast het testen van websites en apps is er ook een enquête gehouden onder betrokken medewerkers bij overheidsinstanties. Meer dan 80% van de respondenten geeft in de enquête aan dat de website voldoende of goed geschikt is (toegankelijk) voor mensen met een beperking. Uit het onderzoek van de websites en mobiele applicaties blijkt echter dat zij nog niet volledig aan alle succescriteria voldoen.

Vanwege het karakter van deze meting - een nulmeting - is een **vergelijking met eerdere metingen niet aan de orde**.

Relevante ontwikkeling
Het ministerie van BZK zal de in het bovenstaande besproken meting jaarlijks herhalen. Dat impliceert dat de hier gepresenteerde resultaten van de nulmeting het referentiekader gaan vormen voor volgende jaarlijkse metingen. Een publicatie over een vervolgmeting was ten tijde van het schrijven van dit onderdeel van het deelonderzoek 'gebruiksgegevens' nog niet beschikbaar.

ODF en PDF

Algemeen
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 mei 2008.

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 november 2008. (Inmiddels wordt in de monitor geen onderscheid meer gemaakt tussen de varianten PDF A-1, A-2 en 1.7. PDF A-1 stond het eerst op de lijst.)

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[15]:

- 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. Voor het zoeken van documenten op websites is Google search gebruikt (https://www.google.com). Vorig jaar gebruikten wij daarnaast ook de Bing API van Microsoft, maar die gaf onvolledige resultaten. Daarom hebben wij Bing dit jaar niet meer ingezet. Bij deze meetmethode moet worden aangetekend dat geen enkele zoekmachine gegarandeerd alle documenten vindt die op een website gepubliceerd zijn. Ook zijn de zoekopdrachten maar beperkt reproduceerbaar: als je dezelfde zoekopdracht op dezelfde zoekmachine herhaalt kan er een ander resultaat uit komen. 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).

[15] Bij de vorige meting zijn de 5 koepelorganisaties niet in de steekproef meegenomen.

	Top 30 overheid	G30 gemeenten	Provincies	Waterschappen	Totaal
Aantal gevonden PDF	325.008 (381.849)	168.005 (197.482)	116.886 (173.860)	22.951 (34.268)	632.850 (787.459)
Aantal gevonden ODF	17 (15)	4 (2)	8 (4)	1 (2)	30 (23)
Aantal gevonden MS Office	39 (123)	30 (98)	25 (51)	6 (52)	100 (324)
Percentage PDF van alle gevonden documenten	99,99% (99,13%)	99,98 (99,95%)	99,97% (99,87%)	99,97 (99,72%)	99,98% 99,52%
Percentage ODF van de gevonden bewerkbare documenten	30% (11%)	12% (2%)	24% (7%)	14% (4%)	24% (8%)
Percentage ISO PDF	47% (36%)	43% (47%)	33% (57%)	29% (41%)	43% (44%)
Percentage digitaal toegankelijke PDF	23%	17%	25%	0%	21%

De belangrijkste observaties naar aanleiding van dit overzicht:

- 20% minder PDF-documenten op websites van overheden dan vorig jaar. De daling van het aantal documenten op websites is zowel bij de rijksoverheid als bij gemeenten, provincies en waterschappen te zien. Deze trend zagen we al in de meting voor de Monitor 2019 en lijkt zich dit jaar voort te zetten;
- PDF blijft veruit het meest gebruikte format voor de publicatie van documenten. Over alle gemeten websites heeft 99,98% van de documenten een PDF format;
- ODF vormt 24% van de bewerkbare documenten op de onderzochte websites. Dit percentage is aanzienlijk meer dan de 8% in 2019. Dat komt omdat er meer in ODF wordt gepubliceerd en we tegelijk ook minder Microsoft Office bestanden vinden.
- 43% van alle gevonden PDF-bestanden voldoet aan de ISO standaard PDF 1.7 of PDF/A. Deze score is vergelijkbaar met vorig jaar: toen 44%. Wat opvalt is dat het percentage bij gemeenten, provincies en waterschappen terugloopt. Dit kan te maken hebben met de iets andere wijze van meten;
- slechts 21**%** van de gevonden PDF van na september 2018 is digitaal toegankelijk volgens de WCAG 2.1 specificatie (en voldoet dus aan de wettelijke verplichting). Zie ook de paragraaf gebruiksgegevens van de Digitoegankelijk-standaard.

De sterke terugloop van het aantal Microsoft Office bestanden en de stijging van het percentage ODF van de gevonden bewerkbare documenten lijkt erop te wijzen dat **overheden zich beter houden aan het 'pas toe of leg uit' beleid**. Deze trend was in 2019 al te zien en zet in 2020 versterkt door. Het aantal digitaal toegankelijke PDF-bestanden met een open ISO format schiet nog flink tekort, zeker gezien de wettelijke verplichting die sinds juli 2018 geldt.

OpenAPI Specification

Algemeen

Open API Specification (OAS) is een standaard voor de documentatie van Application Programming Interfaces (API's). Een API is een koppelvlak waarmee applicaties over het Internet toegang kunnen krijgen tot gegevens en diensten. Zo'n API is in de praktijk zo

effectief als z'n documentatie. De documentatie van een API moet voor machines leesbaar en voor mensen begrijpelijk zijn. OAS 3.0 geeft ontwikkelaars van applicaties een eenduidige en leesbare beschrijving van een REST API waarmee zij de API kunnen gebruiken zonder te hoeven weten hoe deze geïmplementeerd is. OAS 3.0 zorgt voor gemakkelijker (her)gebruik van APIs en minder leveranciersafhankelijkheid. De standaard OpenAPI Specification staat op de 'pas toe of leg uit' ijst sinds mei 2018.

Feitelijk gebruik
Vorig jaar waren nog geen gegevens over het gebruik van OAS beschikbaar. Wel werd in de monitor 2019 al aangekondigd dat Bureau Forum Standaardisatie een nulmeting van het feitelijk gebruik van OAS3 had uitbesteed aan ICTU. Deze nulmeting naar het gebruik is in de afgelopen periode uitgevoerd. Met deze meting is in kaart gebracht:

- welke API's door overheidsorganisaties worden aangeboden;
- en in hoeverre OAS3 wordt gebruikt om de documentatie te specificeren.

In 2019 heeft het ministerie van BZK in samenwerking met VNG Realisatie het portal https://developer.overheid.nl/ opgezet. De ambitie is dat dit portal in de toekomst alle API's ontsluit die door de overheid worden gepubliceerd. Als dit lukt, dan komt hiermee continu up-to-date informatie beschikbaar over het feitelijk gebruik van OAS. Op dit moment ontsluit https://developer.overheid.nl/ echter nog maar een fractie van alle APIs die bij de overheid beschikbaar zijn. Daarom zijn om een zo compleet mogelijk beeld te krijgen nog enkele aanvullende zoekacties uitgevoerd. Een en ander heeft geleid tot de volgende inventarisatie:

- 90 potentiële API's gevonden in de publieke sector;
- uitval: 16 (geen informatie te vinden of geen verdere documentatie beschikbaar).

Met betrekking tot de resterende 74 API's kon de tweede vraag worden beantwoord: al dan niet gebruik van OAS3 om de documentatie te specificeren. Daaruit blijkt het volgende:

- bij 13 API's wordt niet gedocumenteerd met gebruikmaking van een standaard;
- bij 25 API's wordt gedocumenteerd op basis van Swagger;
- bij 36 API's wordt gebruik gemaakt van de OAS-standaard.

Gegeven het feit dat sprake is van een nulmeting is over een ontwikkeling van het gebruik van OAS3 in dit stadium nog niets te zeggen. Bovenstaande gegevens dienen als referentiekader voor eventuele vervolgmetingen.

OWMS

Algemeen
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 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 een totaal van 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.

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 2019. Deze percentages over 2019 zijn gecorrigeerd omdat in de tabel van vorig jaar nu ook - met terugwerkende kracht - de 5 koepelorganisaties zijn meegenomen.

	Top 30 overheid	**G30 gemeenten**	**Provincies**	**Waterschappen**	**Totaal**
Voldoet aan OWMS	13 (43%) *(47%)*	2 (6%) *(16%)*	5 (38%) *(54%)*	7 (30%) *(39%)*	27 (28%) *(36%)*
Voldoet helemaal niet: gebruikt andere metadata	14 (47%) *(43%)*	17 (53%) *(47%)*	3 (23%) *(8%)*	7 (30%) *(22%)*	41 (42%) *(35%)*
Voldoet niet, heeft wel enkele DC elementen	3 (10%) *(7%)*	7 (22%) *(13%)*	5 (39%) *(31%)*	8 (35%) *(30%)*	23 (23%) *(17%)*
Geen metadata	0% *(3%)*	6 (19%) *(25%)*	0% *(8%)*	1 (4%) *(9%)*	7 (7%) *(12%)*
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: 88%);
- in totaal voldoen 27 van deze 91 organisaties (28**%** van het totaal van 98) aan OWMS;
- dat is **minder dan in 2019**, toen was dit nog 36%. Deze daling vinden we terug bij elk van de groepen overheden;
- nog eens 23 van deze 91 organisaties (23% van 98) heeft een deel van de door OWMS verplichte metadata maar voldoet formeel niet aan de standaard;
- dat is meer dan in 2019, toen was dit 17%. De stijging vinden we terug bij elk van de groepen overheden.

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. Hoewel de resultaten van het onderzoek laten zien dat OWMS wel gebruikt wordt bij de overheid, lijkt het correcte gebruik van OWMS af te

nemen. KOOP, de beheerder van OWMS plaatst zelf kanttekeningen bij de meerwaarde van metadatering. Moderne zoektechnologie zoals toegepast in de grote zoekmachines (Google, Bing, enz.) maakt metadatering steeds overbodiger, aldus de beheerder. Deze trend is terug te zien in de resultaten van dit jaar.

SKOS

Algemeen

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 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.
Daarom is in overleg met het Platform Linked Data Nederland (PLDN) besloten om het feitelijk gebruik van SKOS voor de Monitor net als vorig jaar ook dit jaar te onderzoeken met een enquête. De enquête is uitgezet bij ruim 70 overheden en semi-overheden. De steekproef van 2020 is vrijwel gelijk aan de steekproef gebruikt bij de meting van 2019 en bestaat voornamelijk uit gebruikers van de LOD Nederland groep op LinkedIn.

In totaal reageerden dit jaar slechts 18 organisaties (26% van de ondervraagden, vorig jaar 58%). De meeste respondenten zijn uitvoeringsorganisaties, net als in 2019. Verder antwoordden er 2 ZBO's, 1 gemeente en 1 provincie. Deze lage respons biedt niet meer dan een smalle basis voor een vergelijking met de uitkomsten van de enquête ten tijde van de monitor 2019. Met die nuance in het achterhoofd zijn de volgende gegevens met betrekking tot het gebruik verzameld:

- 50% van de respondenten (9 organisaties) geeft aan een begrippenlijst, woordenboek of taxonomie op het internet te publiceren. Vorig jaar lag ligt aantal beduidend hoger, op 23 organisaties (55% van de respons toen);
- 6 organisaties geven dit jaar expliciet aan geen begrippenlijst, woordenboek of taxonomie op het internet te publiceren. De overige 3 respondenten kunnen deze vraag niet beantwoorden;
- van de 9 organisaties die een begrippenlijst, woordenboek of taxonomie op het internet ontsluiten, gebruiken er 5 SKOS (56%). Vorig jaar lag dat aantal hoger (74% van 23).

Een basis voor een goede vergelijking met de gegevens uit de vorige monitor ontbreekt evenwel. Nog afgezien van de zeer beperkte respons, spelen daarbij de volgende overwegingen:

- de vraagstelling in beide jaren is niet volledig vergelijkbaar en richtte zich dit jaar iets directer op het toepassingsgebied van SKOS;

- bij het aantal van 9 organisaties die een begrippenlijst, woordenboek of taxonomie op het internet publiceren vallen ook de nodige kanttekeningen te plaatsen.

Op basis van het bovenstaande kan **geen duidelijke uitspraak** worden gedaan over de **ontwikkeling** van het gebruik van SKOS. De aantallen zijn daarvoor te laag.

Desalniettemin enkele aanvullende observaties:
- De resultaten laten zien dat SKOS meestal gebruikt wordt waar het 'pas toe of leg uit' beleid dat verplicht. Ondanks de (te) beperkte steekproef past dit beeld in de trend die in 2019 ook al viel waar te nemen.
- Ook het beeld uit 2019 dat vooral uitvoeringsorganisaties SKOS en linked data toepassen, wordt dit jaar bevestigd. De gemeente en provincie die antwoordden op de enquête gaven aan geen linked data te gebruiken.
- 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 Web Ontology Language (OWL). 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 resultaten van de enquête lijken te wijzen op een 'alles of niets' trend: óf een organisatie doet helemaal niet aan linked data, óf een organisatie pakt het meteen serieus aan.

Relevante ontwikkeling
SKOS is een standaard die eigenlijk thuishoort in een set linked data standaarden. Op dit moment staan deze standaarden verspreid over de 'pas toe of leg uit' lijst (SKOS) en de lijst aanbevolen standaarden (RDF, OWL en SHACL). 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.

B3.3. Domein E-facturatie en administratie

NLCIUS

Algemeen
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 waarin drie partijen samenwerken: NEN, SimplerInvoicing en TNO. Het initiatief wordt ondersteund door het Ministerie van Economische Zaken en Klimaat vanwege het maatschappelijke belang. Meting van gebruikscijfers van NLCIUS is pas in april 2019 gestart.

Een inzichtelijk overzicht om actuele gebruiksgegevens te vergelijken met die uit de vorige monitor is niet beschikbaar. Met als bron een intern memo aan de stuurgroep STPE is wel een volgend beeld te schetsen:

- Het aantal registraties van NLCIUS endpoints is nu bijna gelijk aan het aantal registraties van SI-UBL 1.2 endpoints. (SI-UBL 1.2 is de andere factuurstandaard die in Nederland door Simplerinvoicing wordt ondersteund.) De SI-UBL 1.2 registraties zijn niet minder geworden. Dat impliceert dat sprake is van een stijging van het aantal gebruikers die via het SI-netwerk NLCIUS-facturen kunnen verwerken;
- Sinds dit jaar ligt het aantal serviceverzoeken (vragen) met betrekking tot NLCIUS zeven keer hoger dan de serviceverzoeken over SI-UBL 1.2. Hiermee zien we ook dat het gebruik enorm is toegenomen. Ook dit duidt op groeiende adoptie;
- Als we kijken naar het totale volume van verzonden en ontvangen e-facturen binnen het SI/PEPPOL-netwerk zitten we tot en met augustus 2020 al op een verdubbeling van de e-factuur volumes ten opzichte van geheel 2019. In cijfers: de teller voor 2020 stond eind augustus op ruim 4 miljoen facturen, terwijl in 2019 totaal het aantal rond de 2.1 miljoen lag. Kanttekening hierbij: dit gaat om meer factuurformaten dan alleen NLCIUS. Het lijkt er echter sterk op dat die stijging wel degelijk door grotere volumes van NLCIUS-facturen komt, aangezien die gelijk loopt met de verplichtstelling van NLCIUS voor overheden in april 2019 en de strengere handhaving van efacturatie-beleid door het Rijk in de maand augustus van hetzelfde jaar. Dezelfde conclusie blijkt uit een recente analyse van Tradeinterop2: die stelt dat 50% van het totale volume om Business-to-Government (B2G) facturen gaat, en van B2G facturen mogen we aannemen dat dit NLCIUS-facturen betreft.

Mede op basis van bovenstaande invalshoeken komt TNO tot de conclusie dat sprake is van **stijging van het gebruik** van NLCIUS.

Relevante ontwikkeling
Er is het voornemen om in de volgende periode (2021 – 2023) meer structureel het gebruik van de standaard te gaan monitoren.

SETU

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. 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 mei 2009.

Feitelijk gebruik
In lijn met vorige jaren blijkt het erg lastig om een inschatting te maken van het feitelijke gebruik van de SETU-standaarden aangezien het berichtenverkeer niet via een centraal platform geregeld wordt. Uit ervaring van in de stichting participerende partijen komt naar voren dat daar waar de relaties tussen leverancier en de organisatie binnen de publieke sector meer dan incidenteel is, de standaard in vrijwel alle gevallen wordt toegepast. Er bestaan echter grote verschillen 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.
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 zouden hebben gegeven tot wijziging in het gebruik.

Relevante ontwikkeling
Er zijn dit jaar nieuwe versies van een aantal SETU-standaarden uitgebracht, met name om wijzigingsverzoeken in het kader van de Wet Arbeidsmarkt in Balans te verwerken. Daarnaast is er een nieuwe versie van de factuur uitgebracht om deze in lijn te brengen met NLCIUS.

Voor de zomer 2020 heeft een gebruikerspeiling plaatsgevonden. De uitkomst daarvan was niet tijdig beschikbaar om opgenomen te worden in de monitor. In een volgende monitor kan worden gerapporteerd over deze (kwantitatieve) gegevens aangaande het gebruik van de SETU-standaarden.

WDO Datamodel

Algemeen
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.

In veel landen wordt de douaneaangifte nog steeds (gedeeltelijk) op papier ingediend. Daarnaast moeten ook 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 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. 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 april 2014.

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, gebaseerd op EU CDM (subset van WDO Datamodel), 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, noch in de vorige monitor harde gegevens over het feitelijke 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 in de toekomst en op de korte termijn gaan manifesteren als eCommerce (DECO) daadwerkelijk in gebruik wordt genomen. Hierover meer bij 'relevante ontwikkeling'.

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:

- eCommerce (DECO): dit betreft 2 binnenkomende en 1 uitgaand berichttype, gebaseerd op EU CDM;
- Presentation Notification ICS2: dit betreft 1 binnenkomend en 1 uitgaand berichttype, gebaseerd op het WDO Datamodel.

Voor deze twee laatste onderdelen geldt dat de Douane als enige toekomstige gebruiker wordt 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

Algemeen
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 zonodig nader te bewerken. Deze XBRL-standaard staat op de 'pas toe of leg uit' lijst sinds 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 het aantal XBRL-berichten van 2018 en de eerste helft van 2019. Onderstaande cijfers zijn in het kader van SBR gerapporteerd zijn t.b.v. de monitor GDI. De cijfers van SBR zijn totalen inclusief machtigen en de cijfers zijn afgerond.

	Realisatie 2017	**Realisatie 2018**	**Realisatie 2019**	**Realisatie 2020** t/m juni
Belastingdienst				
Aangifte IB + VPB	15.353.253	17.167.811	16.557.481	9.492.853
Loonheffingen (incl. UZGB)	7.642.968	8.481.840	8.650.532	4.493.456
Erfbelasting + Schenkbelasting	-	231	4.073	7.359
Aangifte OB + Intercomm. prestaties	4.448.085	4.921.431	5.429.106	2.854.704
Toeslagen	1.141.882	1.242.836	1.325.719	689.877
KvK – Reporting Services (SBR)				
Jaarrekeningen	716.754	866.497	1.020.452	358.007
DUO – Reporting Services (SBR)				
Jaarrekeningen	2.415	1.838	1.950	170
SBR Wonen - Reporting Services (SBR)				
DPI (prognose informatie)		852	1.112	267
DVI (verantwoordingsinformatie)			1.363	1.016
SBR Wonen Jaarrekening 2018			0	1.046

Ook over 2019 zijn cijfers beschikbaar tot en met juni. Dat zou een basis kunnen vormen om te vergelijken met de meest actuele cijfers, tot en met juni 2020. De verwachting bij de beheerorganisatie (Logius) is echter dat de cijfers over de eerste helft 2020 als gevolg van corona een incidenteel-afwijkend beeld laten zien waardoor een vergelijking met 2019 niet zinvol is. Daarvoor in de plaats een vergelijking van de cijfers over heel 2019 met die over 2018. Daaruit blijkt dat op vrijwel alle genoemde variabelen in het overzicht sprake is van **een stijging** van het gebruik. De enige uitzondering vormt 'Aangifte IB en VPB'.

Er is nog potentie voor verdere groei van het gebruik van XBRL. Immers, als er van uit wordt gegaan dat bij financiële verantwoordingsrapportages SBR gebruikt zou moeten worden dan volgt daaruit dat alle ministeries, provincies, waterschappen, gemeenten, uitvoerings-instanties en ZBO's gebruik moeten maken van SBR. Dit is echter nog niet het geval.

B3.4. Domein Stelselstandaarden

Digikoppeling

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

- Bevragingen: 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.
- Meldingen: 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 24 mei 2018.

Feitelijk gebruik

Logius (Stelselvoorzieningen) heeft op verschillende peilmomenten (maart 2013, augustus 2013 t/m 2015, zomer 2016 t/m 2020) lijsten aangeleverd waarop (onderdelen van) overheden en uitvoeringsorganisaties stonden die op Digikoppeling zeggen te zijn aangesloten. Daaruit is het onderstaande overzicht af te leiden.

Overheden aangesloten op 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 % *)		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 **)		98 %	75 %	59 %	95 % ***)
Zomer 2019		60 % ****)	100 %	100 %	100 %	90 % ****)
Zomer 2020		65 % *****)	100 %	100 %	100 %	91 % *****)

**) 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.*

***) In deze berekening in 2018 konden de overheidsorganisaties die zijn betrokken bij 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%.*

****) Hierin zijn voor 2018 alleen de aantallen voor gemeenten, provincies en waterschappen opgenomen*

*****) Dit percentage is als volgt samengesteld: Ministeries: 100%, Basisregistraties: 100%, ZBO's: 28%, Gemeenschappelijke Regelingen: 28%, Hoge colleges van Staat: 67%, Adviescolleges: 7% en Rechtelijke Organisaties: 89%.*

******) Dit percentage is als volgt samengesteld: Ministeries: 100%, Basisregistraties: 100%, ZBO's: 33%, Gemeenschappelijke Regelingen: 24%, Hoge colleges van Staat: 100%, Adviescolleges: 33% en Rechtelijke Organisaties: 100%.*

Het overzicht wijst uit dat gedurende een reeks van jaren sprake is van een gestage groei van het gebruik van Digikoppeling.

De ontwikkeling in de tijd bij de categorie 'Rijk' is een moeilijk te definiëren factor en moet met het nodige voorbehoud worden bekeken. Deze categorie is gevoelig voor veranderingen in de samenstelling van de populatie. Zo is in 2016 het percentage gedaald doordat er veel organisaties zijn toegevoegd uit de OOV-sector die niet zijn aangesloten op Digikoppeling. Vandaar dat vanaf zomer 2019 deze categorie is vervangen door gebruik te maken van beter te verifiëren data. Rijk is sindsdien als volgt gedocumenteerd: Rijk = Alle Ministeries + Basisregistraties + Gemeenschappelijke Regelingen + ZBO's + Hoge Colleges van Staat + Adviescolleges + Rechterlijke Organisaties. De reden voor deze nieuwe invulling is dat

voor deze lijsten stabiele bronnen bestaan zodat vergelijkingen met volgende jaren mogelijk wordt.

De conclusie voor de categorieën gemeenten, provincies en waterschappen is dat de dekking inmiddels volledig is.

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 cloud-oplossingen 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.

Relevante ontwikkeling
De Digikoppeling standaard is een levende standaard. Het nieuwe Pushprofiel voor de Digikoppeling Grote Berichtenstandaard, is dit jaar aan de standaard toegevoegd. Het Digikoppeling OIN-register kent sinds 2019 ook een API, zodat systemen het register automatisch kunnen raadplegen. In 2019 en 2020 zijn hieraan extra identificerende gegevens toegevoegd, zodat organisaties naast hun OIN ook op andere kenmerken, zoals KvK-nummer en BG-Code kunnen worden bevraagd. De Digikoppeling Beveiligingsvoorschriften zijn in lijn gebracht met de nieuwe richtlijnen voor TLS van NCSC. Op dit moment wordt gewerkt aan een Digikoppeling Profiel voor REST-API's, gebaseerd op de API Design Rules, die dit jaar op de lijst van verplichte standaarden van het Forum Standaardisatie zijn geplaatst.

Geo-Standaarden

Algemeen
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 maken het mogelijk om op een eenduidige manier gegevens met een geografische component uit te wisselen. De Geo-standaarden staan op de 'pas toe of leg uit' lijst sinds maart 2011.

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 vorige monitor 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 2019 versie 1.0). Voor verschillende variabelen ziet de ontwikkeling er als volgt uit:

- aan de afnamekant is er een groei van 10,5 miljard hits op PDOK over 2018 naar 14,4 miljard hits over 2019, een groei van 37%;
- aan de aanbodzijde is het aantal datasets gegroeid van 157 (2018) naar 192 in 2019, een groei van 22%;
- het aantal services is gestegen van 415 in 2018 naar 505 in 2019, eveneens een toename van 22%;
- het aantal daadwerkelijke gebruikers lijkt licht te groeien, van 450 instanties in 2018 naar ruim 450 instanties geregistreerd in 2019.

Het geheel overziend is wederom sprake van **substantiële groei van het gebruik**. De groei houdt aan, zowel aan de afnamekant waar men dankzij open standaarden van data kan profiteren, als aan de aanbodzijde waar men data conform open standaarden wil ontsluiten. Enerzijds is dit het gevolg van actief beleid vanuit de overheid (stimuleren om data conform open standaarden te ontsluiten), anderzijds is dit het gevolg van het succes van eerdere jaren: data-aanbieders zien de meerwaarde nu makkelijker in, doordat er voldoende voorbeelden zijn van andere organisaties waarin dit effect optreedt. Er lijkt daarbij sprake van een vliegwieleffect: omdat er meer gebruik is, komt er meer aanbod, waardoor er meer gebruik komt, etc.

Bij dit beeld van groei wordt wel een kanttekening geplaatst door de beheerorganisatie van de Geo-standaarden, Geonovum. Er is namelijk één categorie overheidsinstellingen die de standaarden onvoldoende gebruiken. Dit betreft gemeenten die ieder hun eigen open data portaal optuigen. Er is een aantal commerciële aanbieders van portalen actief, die redelijk rekening houden met standaarden rond algemene open data, maar die geen rekening houden met de standaarden die specifiek voor geo-informatie gelden. Soms geven die aanbieders (ten onrechte) aan dat gemeenten met hun product alle relevante standaarden volgen, maar in veel gevallen worden relevante standaarden genoemd noch gevraagd. De versplintering bij gemeenten en de beperkte bereidheid tot samenwerken leidt ertoe dat er nauwelijks aandacht is voor relevante standaarden op dit vlak.

Relevante ontwikkeling
Specifiek voor NEN3610 (het gemeenschappelijke basismodel Geo-informatie voor de verschillende onderliggende sectorale informatiemodellen) werd in de vorige monitor gemeld dat de ontwikkeling was gestart van Informatiemodel Geluid (IMG) als nieuw domein. Dat is in de tussentijd gerealiseerd. Inmiddels is gestart met de ontwikkeling van het Informatiemodel Externe Veiligheid waarmee een volgend domein conform NEN3610 gemodelleerd gaat worden.
Verder zien we dat het Informatiemodel Basisregistratie Ondergrond (IMBRO) steeds verder ontwikkeld wordt en deze relatief nieuwe basisregistratie scoort ook direct zeer hoog op compliance met de PTOLU-standaarden. Meer in zijn algemeenheid geldt dat het potentiële gebruik toeneemt naarmate meer domeinen

Algemeen

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 staat sinds eind 2008 op de 'pas toe of leg uit' lijst en 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, CORV, 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.

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.

	Totaal		**StUF-BG 3.10 & 3.20**		**StUF-ZKN 3.10 & 3.20**	
Aantal leveranciers	231	(223)	74	(69)	62	(63)
Aantal softwareproducten (incl. versies)	3229	(2879)	1211	(1083)	713	(745)
wv. beschikbaar/in gebruik	1530	(1374)	402	(366)	241	(234)
wv. gepland/in ontwikkeling	122	(111)	47	(56)	25	(33)

Peildatum juni 2020 (tussen haakjes de cijfers van de vorige monitor)
(bron VNG-Realisatie: www.softwarecatalogus.nl)

Uit de cijfers blijkt dat gemeenten, ketenpartners en hun leveranciers StUF dan ook 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.

Uit het overzicht valt af te lezen dat het aantal leveranciers **licht is gestegen** (overall een stijging van 4%) en ook het aantal softwarepakketten stijgt (overall een stijging van 12%). 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.

Bij de beheerorganisatie zijn geen bijzonderheden bekend over specifieke organisaties die de standaarden wel zouden moeten gebruiken, maar deze niet gebruiken. Wat wel opvalt is dat de modernisering via REST/JSON en/of het gebruik van API-standaarden enorm traag verloopt. Mede-overheden beschikken, zo lijkt het, niet over het vermogen, de tijd en de middelen om vergaande modernisering te prioriteren.

Aanvullend op de gegevens uit het overzicht meldt de beheersorganisatie dat de GIBIT-inkoopvoorwaarden inmiddels door 97% van de gemeenten in de praktijk wordt toegepast of heeft opgenomen in hun inkoopbeleid. De overeenkomstengenerator wordt bij 18% van de gemeenten gebruikt.

Relevante ontwikkeling
In de loop van 2020 wordt een implementatie- en communicatiecampagne gestart om gebruik van de documentengenerator te stimuleren. De voorwaarden zijn ge-update en de kwaliteitsnormen (met onder andere een verwijzing naar standaarden waaronder StUF) zijn geactualiseerd.

B3.5. Domein Water en bodem

Aquo-standaard

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

Feitelijk gebruik
Het gebruik van de Aquo-standaard binnen het waterbeheer is groot. Zo hebben de 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.
Gebruikers van de Aquo-standaard zijn ook middels het indienen van wijzigingsverzoeken en het stellen van vragen betrokken bij de ontwikkeling van de standaard. Een deel van de

door IHW verstrekte gegevens over het gebruik van de Aquo-standaard haakt op dit laatste in en kan worden vergeleken met de opgave van vorig jaar:

- aantal ingediende wijzigingsvoorstellen[16]: 118 (vorig jaar: 150)
- daarbij betrokken instanties: 43 (vorig jaar: 42)
- aantal gestelde vragen: 96 (vorig jaar: 106).

Deze gegevens geven slechts een zeer beperkt beeld van het gebruik van de Aquo-standaard. Dit jaar zijn aanvullende gegevens beschikbaar die een beter en completer beeld geven van het daadwerkelijk gebruik[17]:

- Aquo-Domeintabellen Service (raadplegen): ca. 5.000.000 X per jaar
- IM Metingen (uitwisselen): ca. 10.000.000 X per jaar
- Aquo-kit:
  - webservice: meer dan 480.000 X per jaar
  - importeren meetwaarden meer dan 6000 X per jaar
  - toetsen waterkwaliteitsgegevens meer dan 2400 X per jaar
  - toetsen bodemkwaliteitsgegevens meer dan 2400 X per jaar
  - KRW-beoordelen meer dan 600 X per jaar.
- Zwemwaterregister (importeren): meer dan 100 X per jaar.
- Database Grondwaterkwaliteit: meer dan 100 X per jaar
- Waterveiligheidsportaal (op orde krijgen en verzamelen van basisgegevens): meer dan 5.000 X per jaar
- Z-info: ca. 1.000.000 X per jaar
- Centrale Distributielaag (bron PDOK): ca. 40.000 X per jaar
- Stelsel Catalogus Digitaal Stelsel Omgevingswet (geen gegevens, gebruik ontwikkelt zich momenteel sterk).

Achter dit geheel van gebruikscijfers is sprake van meer dan 1000 actieve gebruikers van de genoemde applicaties. Daaronder zitten o.a. de waterschappen, de provincies, Rijkswaterstaat, de Inspectie voor Leefomgeving & Transport en het ministerie van Infrastructuur en Waterstaat.

Omdat deze gegevens in de vorige monitor niet voorhanden waren, ontbreekt een inzichtelijke basis om te vergelijken. Het IHW voegt hieraan toe dat voor de meeste onderdelen geldt dat het gebruik in 2020 **ongeveer hetzelfde** is als in 2019. Een belangrijke **uitschieter** hierin is het gebruik van de Webservice Aquo-kit. Het gebruik hiervan is sinds augustus 2019 explosief gestegen. Deze webservice wordt veelal gebruikt door kennisinstituten die werken in opdracht van waterbeheerders. In de eerste helft van 2019 werd deze webservice amper gebruikt, maar sinds augustus 2019 gemiddeld meer dan 40.000 keer maand. Dit resulteert in een enorme toename van het gebruik van de Aquo-standaard.

Bovenstaande gegevens zijn ook volgend jaar weer beschikbaar (bron: IHW). Dat maakt het mogelijk om tegen die tijd inzichtelijk te maken hoe een en ander zich in de loop van de tijd ontwikkelt.

SIKB0101 en SIKB0102

Algemeen

SIKB0101 is een standaard voor de uitwisseling van bodemkwaliteitsgegevens, inclusief geografische en administratieve gegevens. Op basis daarvan kan worden vastgesteld of

[16] Periode: 1 juni 2019 – 1 juni 2020. Vorig jaar een vergelijkbare periode.
[17] Ook deze gegevens betreffen de periode 1 juni 2019 – 1 juni 2020.

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. SIKB 0101 staat op de 'pas toe of leg uit' lijst sinds juni 2012, SIKB 0102 sinds februari 2016.

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 een aantal depots (landelijk, provinciaal en/of gemeentelijk).

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. 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 dat 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).

Relevante ontwikkeling
De drinkwatersector (publiek/privaat) is sinds 2019 gestart met de implementatie van SIKB0101. In nauw overleg met Geonovum worden gesprekken gevoerd over de harmonisatie van de standaarden van de Basisregistratie Ondergrond (BRO) met SIKB0101. De groeipotentie voor wat betreft het aantal gebruikers uit de overheidssector is overigens niet (meer) zo groot.

Voor de komende jaren zal Archeodepot ook open worden gesteld voor gemeentelijke depots waarmee de standaard SIKB0102 ook binnen de gemeenten een steeds belangrijkere rol gaat spelen. Enkele pilots zijn 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.

B3.6. Domein Bouw

COINS

Algemeen
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 Rijkswaterstaat en provincie Gelderland. Een **vergelijking met eerdere monitor-metingen is niet te maken**. De standaard staat pas kort op de lijst en voor de monitor 2019 waren nog geen gebruiksgegevens over COINS beschikbaar.

Relevante ontwikkeling
Alle provincies en de gemeenten Amsterdam en Rotterdam zijn in een programma bij CROW (BIM Pro) aan het onderzoeken met welk uitwisselingsformaat zij dataleveringen willen gaan uitvragen. Hierbij is ICDD, het eerste onderdeel van COINS zoals hierboven beschreven, genoemd als potentieel geschikt middel. Er is nog geen advies over vastgesteld.

NLCS

Algemeen
Organisaties hanteren vaak een eigen tekenstandaard voor de opbouw van 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
Voor zicht op het feitelijk gebruik door overheidsorganisaties is de beheerorganisatie (BIM-loket) te rade gegaan bij de 5 leveranciers. Dat levert het volgende beeld op.

Soort overheid	**# gebruikers**
Gemeenten	140
Waterschappen/Hoogheemraadschappen	8
Provincies	12
Ministeries	2

Omdat van vier van de vijf bevraagde leveranciers een opgave is ontvangen van gebruik door overheidsorganisaties, mag worden aangenomen dat het werkelijke aantal gebruikers hoger ligt dan het beeld uit de tabel. Overigens is het gebruik buiten de overheid ook aanzienlijk.

Een vergelijking met de uitkomst van de vorige monitor (2019) is niet mogelijk; er waren toen nog geen gebruiksgegevens over NLCS beschikbaar. De beheerorganisatie geeft evenwel aan dat plaatsing op de 'pas toe of leg uit' lijst zeker in de gemeentelijke markt en bij beheerders van ondergrondse infrastructuur heeft geleid tot meer bekendheid, bewustwording en ook **meer gebruik** van de NLCS-standaard. Ook heeft opname van NLCS op de lijst geleid tot toetreding van een nieuwe leverancier, wat het totaal aantal leveranciers op vijf heeft gebracht.

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 en stedelijk spoor nog een stuk lager dan zou kunnen. Diverse organisaties gebruiken nog eigen tekenstandaarden. Dat is wel aan het veranderen, voor beide sectoren zijn namelijk projecten gestart om de NLCS uit te breiden met domein specifieke onderdelen. De adoptie van de NLCS zal in deze sectoren naar verwachting snel gaan zodra de projectenresultaten opgenomen zijn in de standaard.

VISI

Algemeen
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 juni 2012.

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), met als peildatum eind juli 2020:

- overheidsorganisaties: 86 gemeenten
  11 provincies
  15 waterschappen
  2 nutsbedrijven
  overig: RWS, TenneT, Prorail en Rijksvastgoedbedrijf
- individuele gebruikers bij overheden 11.480
- overheidsprojecten 5.747

De beheerorganisatie geeft aan dat sprake is van **toename van het gebruik**. Zo zijn enkele gemeenten in het afgelopen jaar begonnen met het toepassen van de open standaard VISI bij een eerste project. Tevens is bij bijna alle overheidsorganisaties de inzet van VISI vergroot. Dit is zichtbaar en meetbaar door meer projecten en meer gebruikers. Naast de rijksoverheid gebruiken steeds meer andere opdrachtgevers de VISI-standaard. Zo wordt VISI steeds meer toegepast binnen de energiesector en ook havenbedrijven (Port of Rotterdam, Groningen Seaports, Havenbedrijf Moerdijk) en luchthavens (Schiphol, Rotterdam The Hague Airport) omarmen de VISI-standaard.
Een vergelijking met de monitor 2019 is niet te maken; voor die monitor waren geen gegevens over VISI beschikbaar. Voor een vergelijking moeten we terug naar de monitor 2017. Toen werd melding gemaakt van 90 publieke opdrachtgevers die VISI hebben gebruikt (gemeenten, provincies, waterschappen en landelijke overheid samen). Inmiddels ligt dit aantal dus net onder de 120. Een basis voor een vergelijking met de andere hierboven genoemde variabelen ontbreekt.

Relevante ontwikkeling
Om de openheid en implementatie van de standaard te vergroten wordt dit jaar een analyse gemaakt van eventuele drempels die de standaard momenteel oproept voor succesvolle implementatie. Er is nog groeipotentie want iedere organisatie die bouwprojecten doet, moet VISI gebruiken. Eigenlijk alle gemeenten en provincies dus.

B3.7. Domein Juridische identificatie en verwijzing

BWB, ECLI en JCDR

Algemeen
BWB
BWB, de Juriconnect-standaard voor identificatie van en verwijzing naar wet- en regelgeving, staat op de ‘pas toe of leg uit’-lijst sinds november 2013. 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[18].
Met betrekking tot de te verwachten ontwikkeling het volgende.
De BWB-standaard heeft tekortkomingen waarvoor mogelijke oplossingsrichtingen thans 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.

JCDR
JCDR is de Juriconnect standaard voor identificatie van en verwijzing naar decentrale regelgeving en staat eveneens op de 'pas toe of leg uit'- lijst sinds 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.
Met betrekking tot de te verwachten ontwikkeling het volgende.
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 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 maart 2019 waren dat 17 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.
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

[18] Zie ook art. 13 Bekendmakingsbesluit: https://wetten.overheid.nl/BWBR0025257/2009-07-01/#Hoofdstuk4_Artikel13. Wetten.overheid.nl wordt beheerd door KOOP (Kennis- en exploitatiecentrum Officiële Overheidspublicaties), onderdeel van het Ministerie van BZK. De website heeft meer dan een miljoen bezoeken per maand. In wetten.overheid.nl wordt de BWB-URI, zichtbaar in de URL, achter de domeinnaam. Dat is te zien in de link bovenin deze voetnoot.

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 in 2020 op ongeveer 35.000 bezoeken / bezoekers en 310.000 page-views per maand (peilmoment: juni 2020).
Twee kanttekeningen hierbij. Ten eerste is onbekend welk deel van de 35.000 bezoekers vanuit de overheid afkomstig is. Ten tweede: op het eerste oog is sprake van een terugloop ten opzichte van vorig jaar (in 2019: circa 40.000 bezoeken per maand). Echter, in 2020 is overgeschakeld op andere software voor het meten van websiteverkeer waardoor een vergelijking met voorgaande jaren niet goed mogelijk is.

Dat neemt niet weg dat vanuit de beheerorganisatie de inschatting wordt 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 et 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. en wet- en regelgeving die het gebruik van deze normen voorschrijven.

B3.8. Domein Onderwijs en loopbaan

E-Portfolio NL NEN 2035

Algemeen
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 2019 en de eerste 3 maanden van 2020 38 keer aangeschaft of ingezien via NEN Connect (het licentiesysteem van NEN). In 30 van deze gevallen ging het om publieke organisaties. 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.
In de vorige monitor waren geen gegevens beschikbaar over het feitelijke gebruik van E-portfolio NL. Dat neemt niet weg dat de beheerorganisatie de inschatting kan maken dat het feitelijke gebruik **stabiel is gebleven** in vergelijking met vorig jaar.

Relevante ontwikkeling
In de vorige monitor is melding gemaakt van het feit dat Forum Standaardisatie enkele voorwaarden heeft verbonden aan continuering van een plaats op de 'pas toe of leg uit' lijst voor E-portfolio NL:

- monitoring van het gebruik van de standaard door overheidsinstellingen;
- opstellen van een implementatiestrategie om de adoptie en het gebruik van de standaard te verhogen.

Bovenstaande cijfers zijn een eerste stap voor wat betreft monitoring en geven een eerste kwantitatieve indruk van het gebruik van de standaard.
Voor wat betreft de tweede afspraak het volgende. De inschatting is dat een groot aantal organisaties de standaard nog niet gebruiken, maar dit wel zouden moeten doen. Om hier meer inzicht in te krijgen wordt in 2020 een uitgebreide analyse gemaakt door NEN. Daarbij wordt eerst inzichtelijk gemaakt welke stakeholders belang hebben bij NEN 2035 en de ISO-standaarden en wordt daarna met hen bepaald of er behoefte is aan een herziening van E-portfolio NEN 2035. Hierbij wordt ook in ogenschouw genomen dat de ISO-norm voor e-Portfolio, ISO 20033, momenteel wordt herzien. Samen met de belanghebbenden zal bepaald moeten worden of er in Nederland nog steeds behoefte is aan een eigen, nationale norm, of dat gebruik kan worden gemaakt van ISO 20033, mogelijk met een nationale aanvulling.

NL LOM

Algemeen
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 mei 2011.

Feitelijk gebruik
NL-LOM wordt gebruikt door verschillende organisatie in de onderwijs- en publieke sector. In de publieke Edurep leermaterialen zoekmachine krijgt de beheerorganisatie (Edustandaard, ondergebracht bij Kennisnet NL-LOM records aangeboden vanuit hoger onderwijs, waaronder Groen Kennisnet. Repositories voor PO en VO worden vanuit Kennisnet onderhouden onder de Wikiwijs naam. Maar ook partijen als SchoolTV, NEMO, Freudenthal Instituut en Beeld en Geluid zijn aanbieders. Onze bron heeft geen zicht op gebruik van NL-LOM buiten de Edurep aansluitingen.
In de vorige monitor (2019) zijn bij gebrek aan input geen gebruiksgegevens met betrekking tot het gebruik van NL LOM openomen. Dat neemt niet weg dat vanuit de beheerorganisatie van de standaard dit jaar melding wordt gemaakt van **stijging** van het gebruik van NL LOM.

Relevante ontwikkeling

Op dit moment loopt er een project om educatief materiaal van erfgoed-instellingen beter te ontsluiten voor het onderwijs. Veel van de betrokken organisaties kunnen hun data nu nog niet in NL-LOM uitvoeren. De toekomst zal moeten uitwijzen of dit leidt tot meer gebruik van de standaard. Als kanttekening hierbij wordt opgemerkt dat het lastig is voor partijen om NL LOM uit te voeren. Het is niet de meest makkelijke standaard en over het gebruik van de mogelijke waardensets is veel inhoudelijke discussie. Daarbij komt dat dit technisch complex blijkt.

B3.9. Domein Overig

EML_NL

Algemeen
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 november 2013.

Feitelijk gebruik
De EML_NL-standaard is opgenomen in de Ondersteunende Software Verkiezingen, hierna "OSV". Het gebruik van de OSV is daarmee een indicator voor het gebruik van de EML_NL standaard. Deze OSV wordt beschikbaar gesteld bij verkiezingen die onder de Kieswet vallen.

Tijdens de vorige monitor (2019) is vastgesteld dat alle bij het verkiezingsproces betrokken overheden gebruik hebben gemaakt van de OSV en daarmee EML_NL hebben toegepast. Dit is het meest actuele inzicht in het gebruik van deze standaard. Na het afronden van de vorige monitor hebben in Nederland immers geen verkiezingen meer plaatsgevonden, vallend onder de Nederlandse Kieswet. Daarmee is meteen aangegeven dat het daadwerkelijke en feitelijk gebruik van de EML_NL standaard samenhangt met het feit of sprake is van dergelijke verkiezingen.

Relevante ontwikkeling
Het gegeven dat inmiddels alle overheden in geval van verkiezingen gebruik maken van de OSV maakt dat met deze standaard in de huidige vorm een 100% doelbereik wordt gerealiseerd. Het dossier ten aanzien van verkiezingssoftware 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 OSV 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 'pas toe of leg uit'-lijst staan.

Meting Informatieveiligheidstandaarden overheid september 2020

Inclusief IPv6-meting overheid

Datum	30 oktober 2020
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-maildomeinen 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 september 2020. In de meting zijn 548 domeinnamen die ook in eerdere metingen centraal stonden getoetst. Bovendien is voor de eerste keer een vergelijking gemaakt met de meetresultaten van een bredere selectie van bijna 1800 overheidsdomeinen. Uit deze meting blijkt dat het stijgende gebruik van de standaarden doorzet, maar dat nieuwe dreigingen de stand der techniek voortstuwen, en dat ook de eisen aan de techniek – in dit geval internetstandaarden – verlegd kunnen worden. Voldoen aan standaarden is daarmee geen eenmalige actie, maar een voortdurend proces van continue verbetering.

2. Samenvatting

2.1. Hoofdzakelijke bevindingen

Het gebruik van de meeste informatieveiligheidstandaarden is afgelopen halfjaar wederom gegroeid. Het individueel aanschrijven van overheidsorganisaties, wat Forum Standaardisatie in het tweede kwartaal van 2020 heeft gedaan, lijkt zichtbaar in groei bij de meeste standaarden uit deze meting. De voornaamste uitzonderingen hierop zijn TLS (web) en STARTTLS (e-mail) conform de aanbevolen configuratie volgens het NCSC, waar we een forse daling zien als gevolg van een aangepaste norm. De terugval bij TLS is ontstaan doordat in deze meting voor het eerst conform de tweede versie van de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS)[19] (uit april 2019) is getoetst. Hiermee is de lat hoger gelegd t.o.v. de voorgaande meting, toen nog conform de eerste versie van deze richtlijnen (uit 2014)

[19] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls

werd getoetst. De stand der techniek schrijdt voort, en periodieke controle op compliance is daarmee een vereiste.

Om phishingmails uit naam van overheidsorganisaties (inclusief bewindspersonen) te voorkomen, moet meer dan 1/3e 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 bijna de helft van de overheidsdomeinen nog niet voldoet.

Daarnaast zien we bij DNSSEC, voor zowel web als e-mail, een daling van 1%-punt, wat illustreert dat toepassen van standaarden een voortdurende activiteit is waar blijvende aandacht voor nodig is.

Uit een vergelijking met een bredere set overheidsdomeinen blijkt 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. We constateren een extreme wildgroei aan overheidsdomeinnamen, wat een groeiende beheerlast met zich meebrengt. Het is moeilijk overzicht houden en ook lastig om ervoor te zorgen dat informatieveiligheidstandaarden goed op iedere domeinnaam worden toegepast. Meer regie is nodig om grip te krijgen.

Tot slot zien we dat er nog onvoldoende aandacht is voor IPv6. IPv6 adoptie voor websites beweegt langzaam de goede kant op, maar het groeitempo lijkt te kort te komen om het nieuwe streefbeeld, dat in april 2020 in het OBDO is afgesproken, te gaan halen. Met het huidige groeitempo van IPv6 voor e-maildomeinen is het nog slechter gesteld, en als dit tempo doorzet wordt de adoptiegraad van 100% eind 2021 zeker niet gehaald.

2.2. Webstandaarden

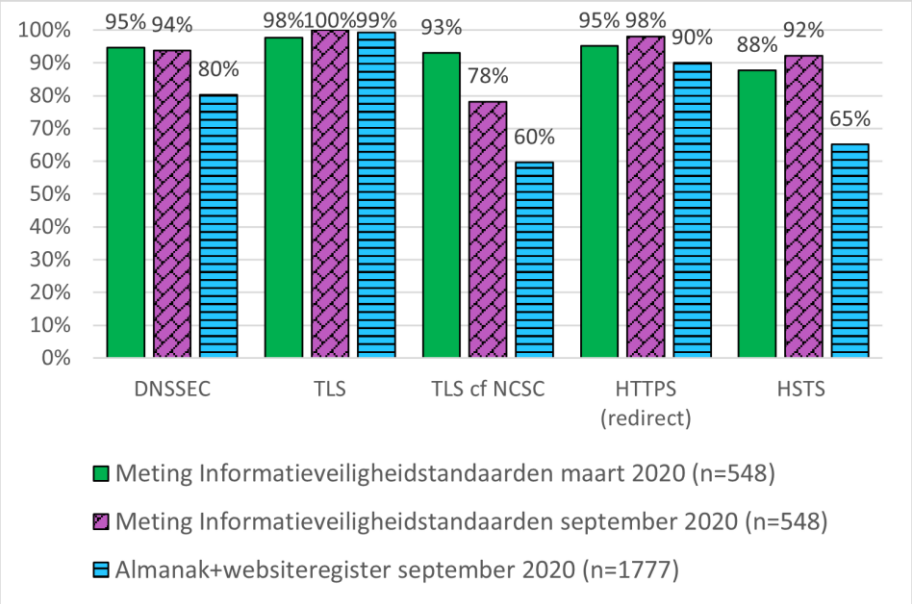
Positief is dat alle webdomeinen uit de originele meting inmiddels HTTPS gebruiken en dat het afdwingen van HTTPS steeds beter wordt toegepast door op de juiste manier door te verwijzen en HSTS vaker toe te passen.

De terugval in toepassing van een veilige TLS configuratie en de lichte daling op DNSSEC laten zien dat constante aandacht voor internetstandaarden nodig blijft. DNSSEC is een belangrijke waarborg voor de integriteit van internetverkeer, en inmiddels wordt bij meer dan de helft van het Nederlandse DNS-verkeer DNSSEC-handtekeningen gecontroleerd[20].

De vergelijking met een bredere selectie van internetdomeinen toont dat hoewel TLS in de basis gemeengoed lijkt met 99% adoptiegraad, dat dit nog lang niet even veilig geconfigureerd is en ook niet altijd goed wordt afgedwongen door op de juiste manier door te verwijzen en HSTS toe te passen.

[20] https://stats.labs.apnic.net/dnssec/NL

Adoptie webbeveiligingsstandaarden - originele metingen t.o.v. bredere selectie



2.3. E-mailstandaarden voor bestrijding van phishing

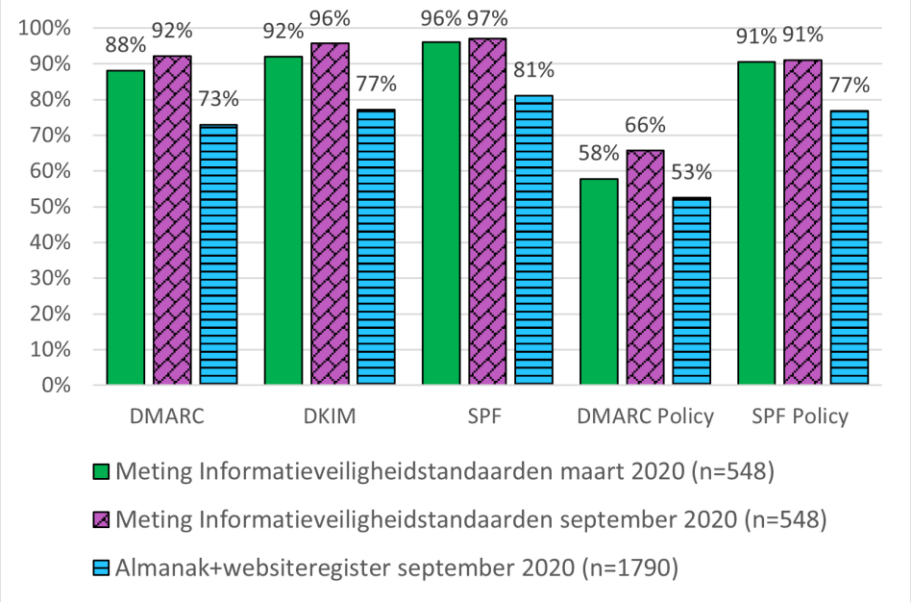
Phishing is aan de orde van de dag. Ook phishing uit naam van de overheid, waarbij overheidsdomeinnamen worden misbruikt[21]. Met de implementatie en juiste strikte configuratie van anti-e-mailvervalsingstandaarden kan phishing worden bestreden. De OBDO streefbeeldafspraak om dat eind 2019 bij 100% van de gemeten e-maildomeinen op orde te hebben is nog niet gehaald. Meer dan 34% 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.

[21] https://www.nu.nl/tech/6042430/lek-maakte-het-mogelijk-om-te-e-mailen-uit-naam-van-rijksoverheid-en-rivm.html

Adoptie e-mailstandaarden anti-phishing - originele metingen t.o.v. bredere selectie

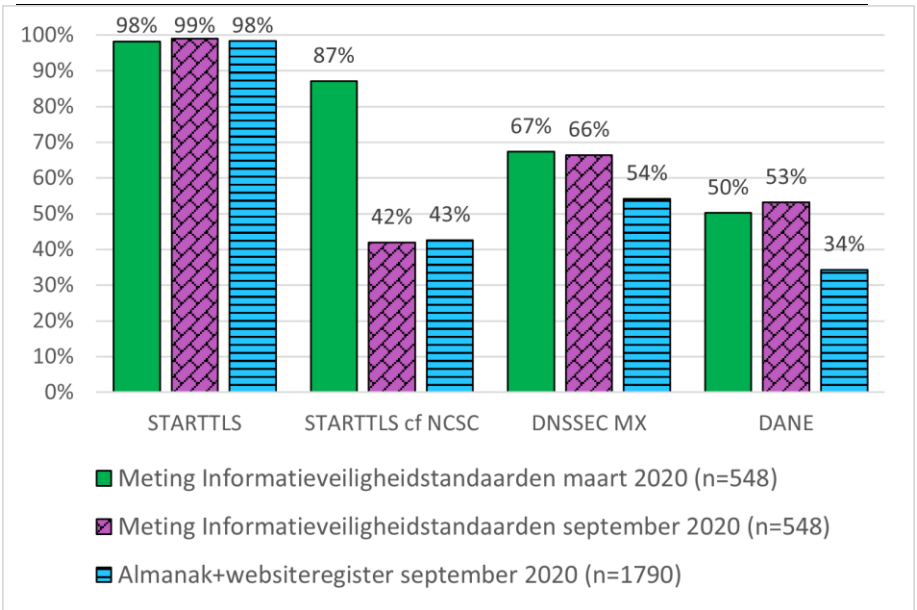


2.4. E-mailstandaarden voor vertrouwelijkheid e-mailverkeer

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.

De terugval in toepassing van een veilige STARTTLS configuratie en de lichte daling op DNSSEC laten zien dat constante aandacht voor internetstandaarden nodig blijft. 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

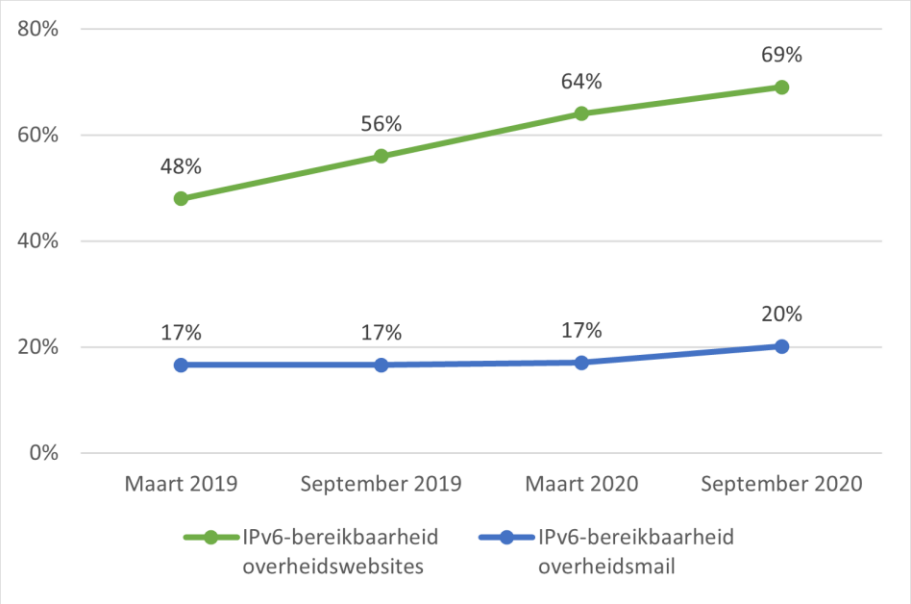


2.5. Bereikbaarheid via IPv6

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 1,5 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 howto's[22] 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 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, met name ook voor overheden die achteruit zijn gegaan op DNSSEC.

[22] Voor how-to's over DANE en DMARC+DKIM+SPF zie: https://github.com/internetstandards/toolbox-wiki

5. Forum Standaardisatie zal in overleg met het NCSC kijken op welke wijze overheidsorganisaties kunnen worden geholpen om de ICT-beveiligingsrichtlijnen voor TLS beter toe te passen, bijvoorbeeld met een aanvullende handreiking ten aanzien van de bevindingen op cipher-volgorde en sleuteluitwisselingsparameters.

Meer specifiek met betrekking tot de mailstandaarden:

6. 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 90% van de domeinen). Er ligt dus een duidelijk groeipotentieel voor DMARC-policy.
7. 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 66% 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.
8. Forum Standaardisatie zal in contact treden 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.

Meer specifiek met betrekking tot IPv6:

9. Forum Standaardisatie gaat in gesprek met VNG Realisatie hoe hun (succesvolle) aanpak kan worden voortgezet, en kan worden verbreed naar andere overheidslagen.
10. Adoptiegroei binnen de categorieën Rijk en uitvoering is met name te behalen als shared service providers, zoals DICTU en SSC-ICT, ook stappen zetten om de servers via IPv6 bereikbaar te maken. Partijen als DPC en SSC-I doen dit al. Met name SSC-ICT kan nog flinke stappen zetten, hun name-, web- en mailservers zijn bijvoorbeeld nog niet per IPv6 bereikbaar.
11. 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.

Tot slot constateren we een wildgroei aan internetdomeinen van de overheid. Slecht geconfigureerde internetdomeinen komen met allerlei risico's. De wildgroei vraagt om meer regie en daarmee grip op de aanwezigheid van de overheid op het Internet. Overheidsorganisaties hebben overzicht op het bredere domeinnaamportfolio nodig om alle risico's te kunnen beheersen, en basishygiënemaatregelen zoals standaarden consequent toe te passen. Daarom roepen wij overheidsorganisaties op actief te werken aan goed domeinnaambeheer. Forum Standaardisatie zal het komende halfjaar verkennen hoe de overheid hier een stap vooruit in kan zetten.

3. Achtergrond

Sinds 2015 biedt het Platform Internetstandaarden[23] 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[24]. 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[25].

De eerste streefbeeldafspraak is eind 2017 afgelopen. Begin 2018 is een eindmeting voor deze afspraak gepubliceerd. Ondanks een grote stijging de afgelopen twee jaar was volledige adoptie nog niet bereikt. Daarom zijn deze afspraken in april 2018 herbevestigd en aangevuld door het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO), de opvolger van het Nationaal Beraad. De metingen vanaf 2018 zijn daarom uitgebreider (meer standaarden) dan voorgaande metingen. Daarnaast was het een goed moment om de lijst met de te toetsen domeinnamen te herijken en is besloten om het tijdstip van meten beter te laten aansluiten op de bestaande overlegcycli.

3.1. Om welke standaarden gaat het

Het Nationaal Beraad en het OBDO hebben streefbeeldafspraken gemaakt met betrekking tot de volgende standaarden[26]:

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

[23] Platform Internet Standaarden is een gezamenlijk initiatief van de Internetgemeenschap en de Nederlandse overheid (Forum Standaardisatie, het Ministerie van Economische Zaken en Klimaat, en NCSC). Zie https://internet.nl/about/
[24] http://www.binnenlandsbestuur.nl/digitaal/nieuws/nationaal-beraad-wil-sneller-moderne-e.9540822.lynkx
[25] Onderdeel van deze afspraak is dat Forum Standaardisatie de voortgang van de adoptie meet en inzichtelijk maakt. De halfjaarlijkse IV-meting is ook onderdeel van de jaarlijkse Monitor Open standaarden beleid.
[26] Voor meer informatie ga naar: https://www.forumstandaardisatie.nl/thema/veilig-internet/streefbeeldafspraken

3.2. Om welke domeinnamen gaat het

In totaal zijn in deze meting 548 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 6000 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 1800 internetdomeinen die zijn ontleend aan het Register van Overheidsorganisaties en het Websiteregister Rijksoverheid[27]. 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 4 augustus 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

[27] https://almanak.overheid.nl en https://websiteregisterrijksoverheid.nl

(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 de loop van 2021 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)[28]. 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.

[28] Zie https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls. Een wijziging ten opzichte van de vorige meting is dat nu wordt getest tegen ICT-beveiligingsrichtlijn voor TLS versie 2.0 (uit 2019) in plaats van versie 1.0 (uit 2014).

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[29]	Net zoals bij HTTPS kan er bij STARTTLS gebruik worden gemaakt van verschillende versies van het TLS en verschillende versleutelings-standaarden (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.

[29] https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls

4. Resultaten meting september 2020

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".

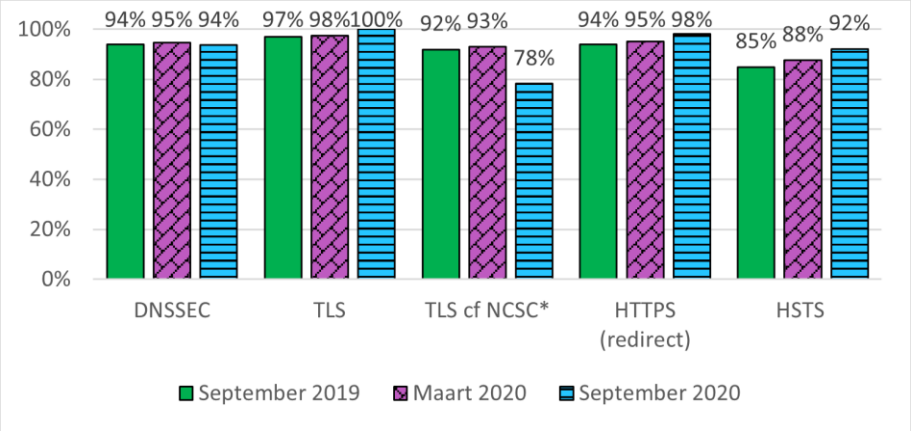
4.1. Per standaard

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

Bij de webstandaarden vallen in eerste instantie de achteruitgang bij zowel DNSSEC als TLS conform de TLS-beveiligingsrichtlijnen van het NCSC op. Dat laatste is te verklaren doordat de bulkmeettool van Internet.nl – waar deze meting mee is uitgevoerd – nu net als de publieke interface van Internet.nl toetst conform de laatste ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) (v2.0 uit april 2019). Hiermee is de lat hoger gelegd t.o.v. de voorgaande meting. De terugval wordt met name veroorzaakt door de testelementen cipher-volgorde en sleuteluitwisselingsparameters.

Gemiddelde adoptie webstandaarden



De lichte daling op DNSSEC laat zien dat constante aandacht voor internetstandaarden nodig blijft, het betreft enkele gemeenten en waterschappen die na de laatste meting geen DNSSEC meer toepassen.

Positief is dat alle webdomeinen uit de meting inmiddels HTTPS gebruiken en dat het afdwingen van HTTPS steeds beter wordt toegepast door op de juiste manier door te verwijzen en HSTS vaker toe te passen.

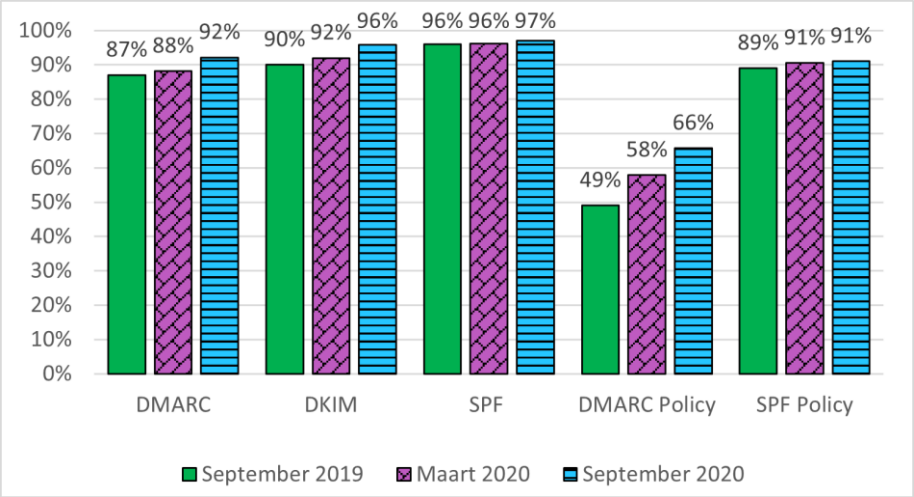
Het Bureau Forum Standaardisatie zal in overleg met het NCSC onderzoeken hoe middels voorlichting de adoptiegraad van de veilige configuratie van TLS conform de beveiligingsrichtlijnen van het NCSC kan worden vergroot.

Om de adoptie van de overige standaarden verder te stimuleren is een 'één-op-één' benadering nodig om dichter bij de 100% te komen.

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 gemiddeld een iets hoger groeitempo dan de vorige meting. Wel blijft aandacht nodig voor het toepassen van strikte DMARC policies om vervalste e-mails ook echt tegen te houden.

Gemiddelde adoptie mailstandaarden - Voorkomen e-mailspoofing (anti-phishing)



Hoewel het percentage vrij hoog is, zien we een stagnatie in het strikter instellen van de SPF policies. Met SPF kan een organisatie aangeven welke partijen namens een domein e-mail mogen verzenden.

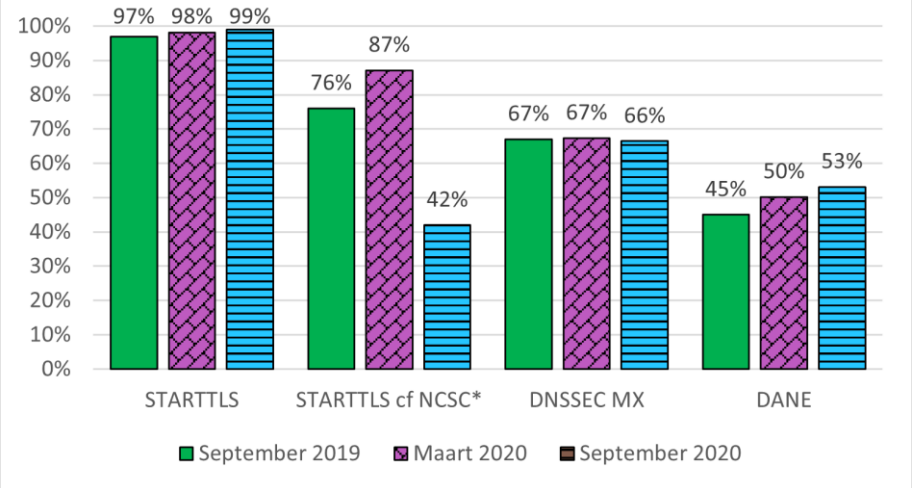
Het Bureau Forum Standaardisatie spreekt reeds actief partijen aan op de noodzaak om actieve, strikte policies voor zowel DMARC en SPF in te stellen, en zal hier blijvend aandacht aan schenken.

4.1.3. E-mailstandaarden voor vertrouwelijkheid e-mailverkeer

Bij de set e-mailstandaarden die de vertrouwelijkheid van het transport van e-mail tussen mailservers kunnen waarborgen valt in eerste instantie de terugval van STARTTLS conform de beveiligingsrichtlijnen van het NCSC op. Ook dit wordt veroorzaakt door de hogere lat als gevolg van de update van de bulkmeettool van Internet.nl, die nu toetst conform de laatste ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) (v2.0 uit april 2019).

Daarnaast valt de lichte daling van DNSSEC op mailservers (MX) op, nadat we de vorige meting al een stagnatie constateerden. Enerzijds is dit veroorzaakt door een paar partijen die over zijn op cloudmailproducten die geen DNSSEC ondersteunen, anderzijds door partijen die om andere redenen geen DNSSEC meer ondersteunen. We zien tevens dat het groeitempo van DANE aan het afzwakken is. Wel zien we aan de hand van het adoptiepercentage van DNSSEC voor de mailserver nog een direct groeipotentieel van 13% 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 2020 outbound DANE support te kunnen bieden, en eind 2021 inbound DANE support. 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 zal in contact treden met andere 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.

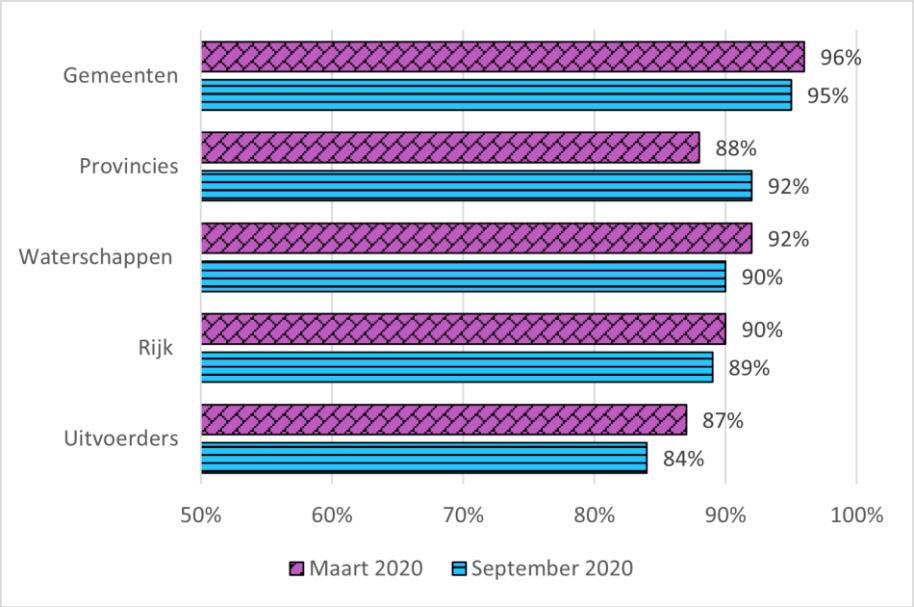
4.2. Per overheidslaag

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 provincies hebben gemiddeld gezien alsnog een groei doorgemaakt, zij scoren nu een nette tweede plaats met 92% na de gemeenten 95%. De uitvoerders zijn sterkste daler en hekkensluiter met een gemiddeld adoptiepercentage van 84%, zij scoren dan ook het slechtst op STARTTLS conform de TLS-beveiligingsrichtlijnen van het NCSC.

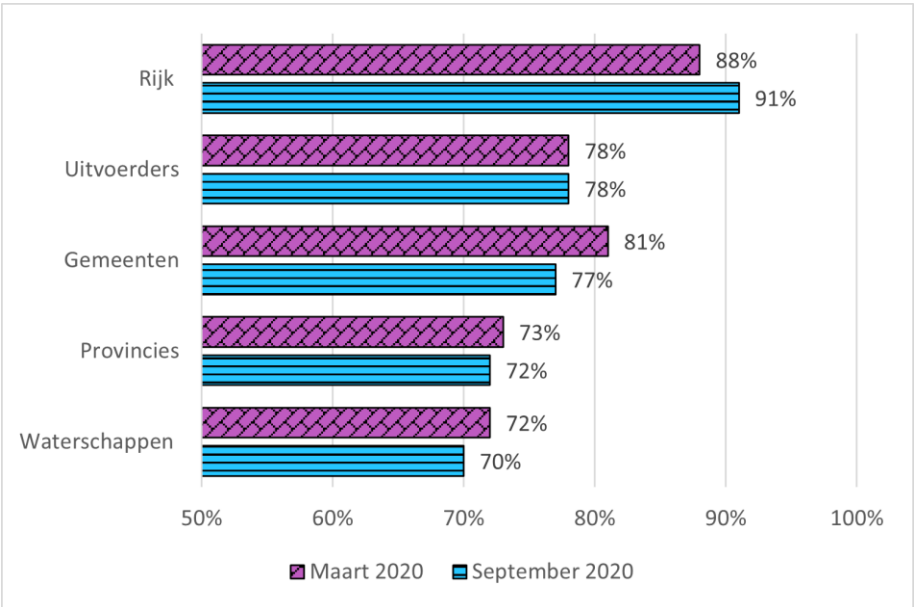
Gemiddelde adoptiegraad webstandaarden per overheidslaag (van hoog naar laag)



4.2.2. E-mailstandaarden

Het Rijk is koploper en toont als enige overheidslaag groei t.o.v. de vorige meting van de e-mailstandaarden. Het Rijk kon de terugval voor STARTTLS conform de beveiligingsrichtlijnen van het NCSC goedmaken met een significante groei in de toepassing van strikte DMARC policies. De waterschappen en provincies gemiddeld iets achter op de andere overheidslagen.

Gemiddelde adoptiegraad e-mailstandaarden per overheidslaag (van hoog naar laag)



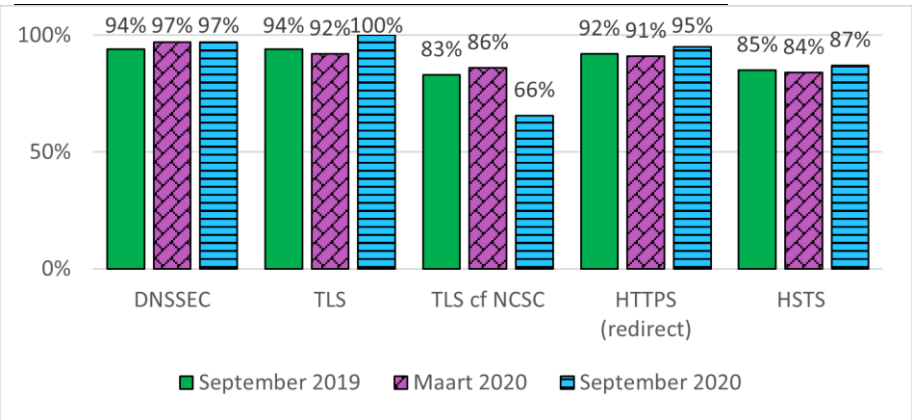
In het vervolg van de rapportage wordt per overheidslaag toegelicht welke standaarden gemiddeld veel worden toegepast en welke minder.

4.2.3. Het Rijk

Het Rijk lijkt zich te hebben herpakt na een lichte terugval in de voorgaande meting. Alleen op TLS conform de TLS-beveiligingsrichtlijnen van het NCSC scoort het Rijk – conform

verwachting – slechter, vanwege de strengere norm. Inmiddels wordt op alle webdomeinen TLS toegepast. Er is nog voldoende ruimte voor groei voor het vaker toepassen van HSTS.

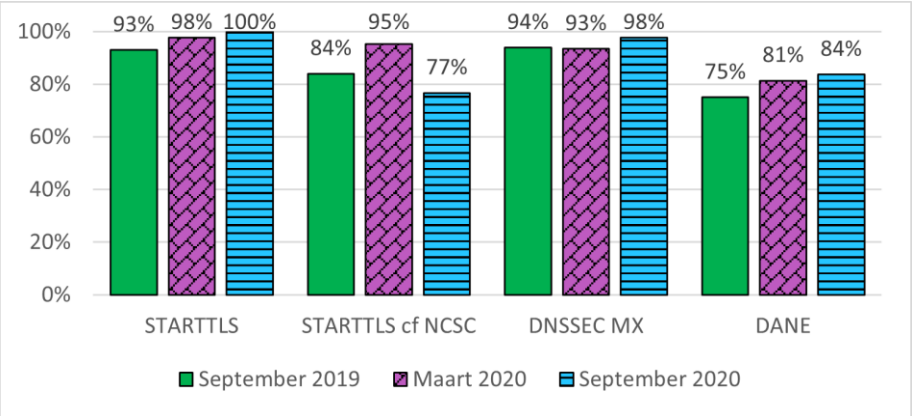
Gemiddelde adoptie Rijk: webstandaarden



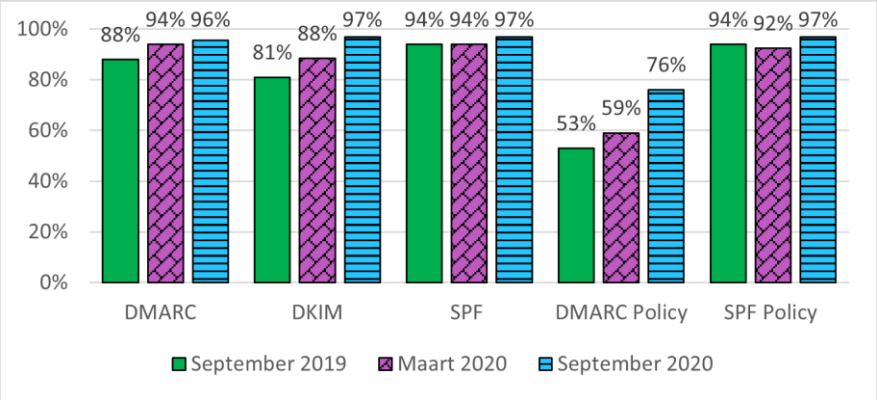
Hoewel het Rijk relatief beter scoort dan andere overheidslagen als het gaat om de mailstandaarden is het streefbeeld om 100% van de gemeten e-maildomeinen op orde te hebben nog niet gehaald. Met name bij STARTTLS conform de TLS-beveiligingsrichtlijnen van het NCSC, een strikt DMARC policy en DANE vragen 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.

Inmiddels wordt op alle relevante domeinen STARTTLS toegepast. STARTTLS conform de TLS-beveiligingsrichtlijnen van het NCSC laat zoals verwacht een terugval zien vanwege de strengere norm die hier voor geldt. Hier is dus weer werk aan de winkel. De toepassing van DMARC met strikte policy heeft een grote sprong voorwaarts gemaakt, 17% adoptiegroei t.o.v. 8% overheidsbreed. Toch voldoet ongeveer een kwart van de e-maildomeinen van het Rijk nog niet aan de afspraken en komen phishingmails namens de achterblijvende rijks-organisaties (inclusief bewindspersonen) daardoor nog steeds bij burgers en bedrijven aan.

Gemiddelde adoptie Rijk: mailstandaarden - beveiligde verbinding



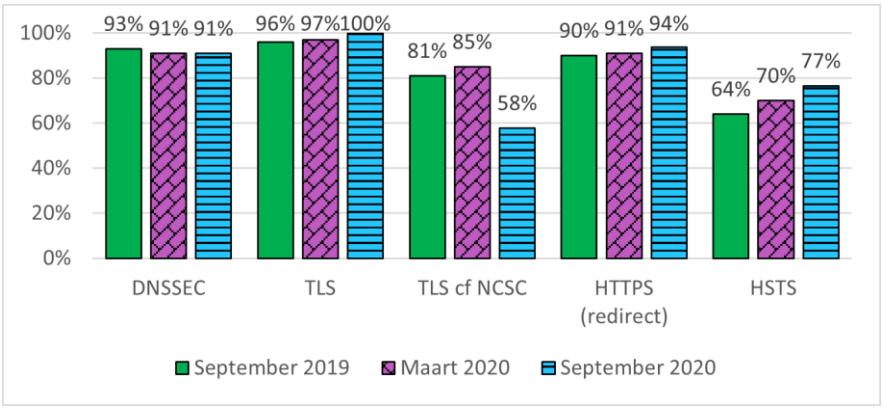
Gemiddelde adoptie Rijk: mailstandaarden - anti-phishing



4.2.4. Uitvoering

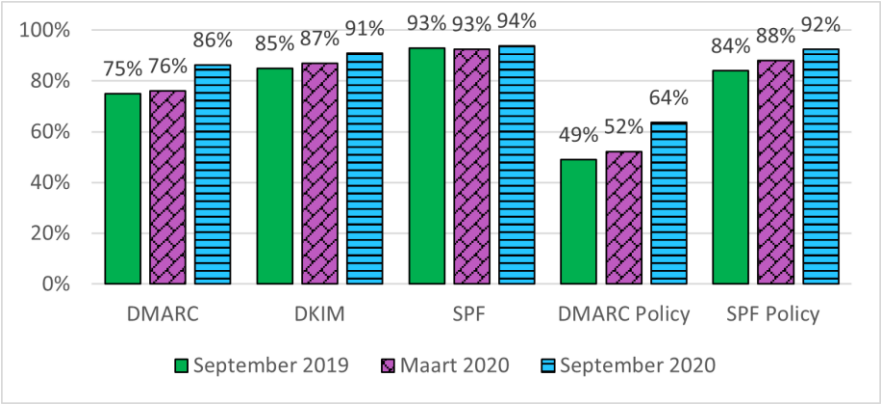
Bij de uitvoeringsorganisaties zien we dat er nog steeds onvoldoende aandacht is voor DNSSEC, deze staat op een adoptiegraad van 91% t.o.v. 94% overheidsbreed. Hoewel ook alle uitvoeringsorganisaties nu TLS toepassen, scoren zij gemiddeld het slechtst op TLS conform de TLS-beveiligingsrichtlijnen. Ondanks significante groei bij HSTS, wordt ook deze standaard gemiddeld gezien het slechtst toegepast met een adoptiegraad van 77%.

Gemiddelde adoptie uitvoerders: webstandaarden

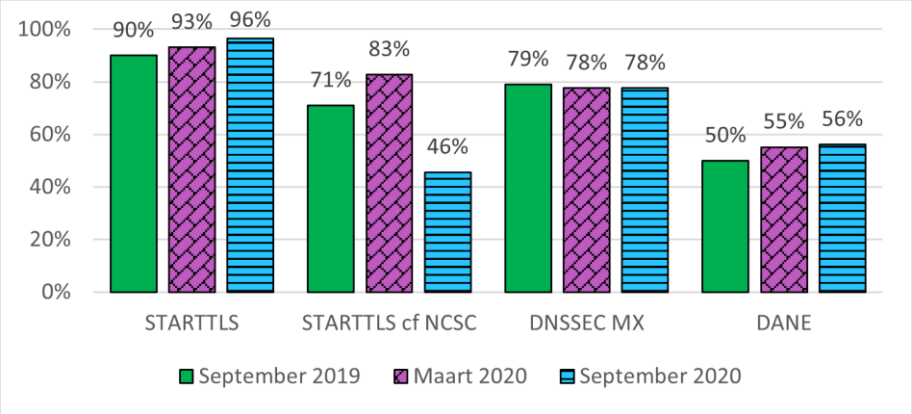


De stagnatie bij e-mailstandaarden, die we bij de uitvoeringsorganisaties in de vorige meting constateerden, is over het algemeen omgezet in groei. Met name DMARC, mét en zonder strikte policy, wordt vaker toegepast, hoewel er nog meer ruimte is voor groei. De adoptiecijfers voor DNSSEC bij mailservers, en DANE voor het afdwingen van een versleutelde verbinding, blijven zorgelijk. Afgeleid van het adoptiepercentage van DNSSEC MX, is er een groeipotentieel van 22% om DANE voor inkomend verkeer mogelijk te maken.

Gemiddelde adoptie uitvoerders: mailstandaarden - anti-phishing



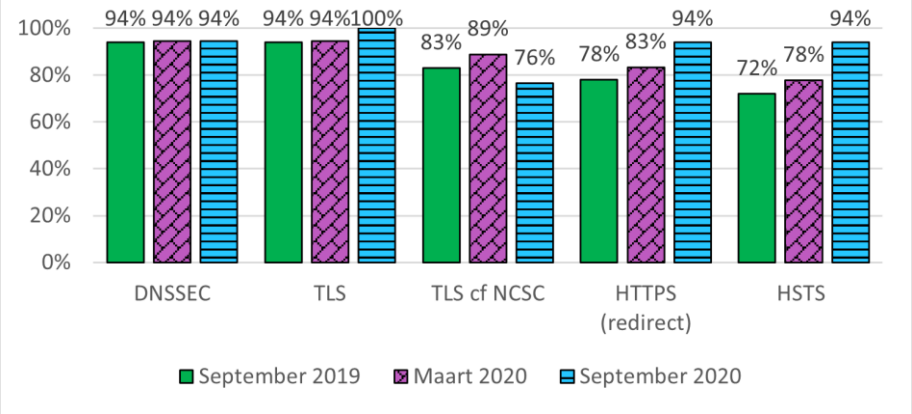
Gemiddelde adoptie uitvoerders: mailstandaarden - beveiligde verbinding



4.2.5. Provincies

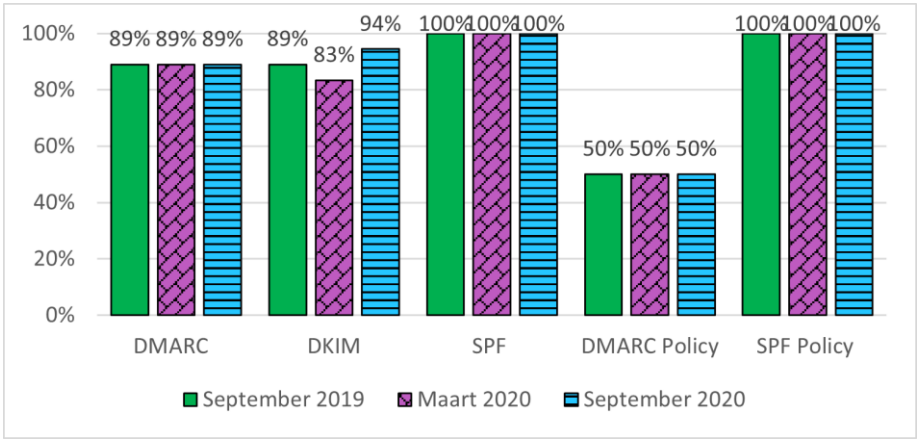
De provincies scoren inmiddels ook 100% op TLS. Het afdwingen van de TLS-verbinding wordt gemiddeld veel beter gedaan, en de 100% is ook voor HTTPS-redirect en HSTS binnen handbereik. Ook hier zien we een terugval bij TLS conform de TLS-beveiligingsrichtlijnen door de strengere norm.

Gemiddelde adoptie provincies: webstandaarden



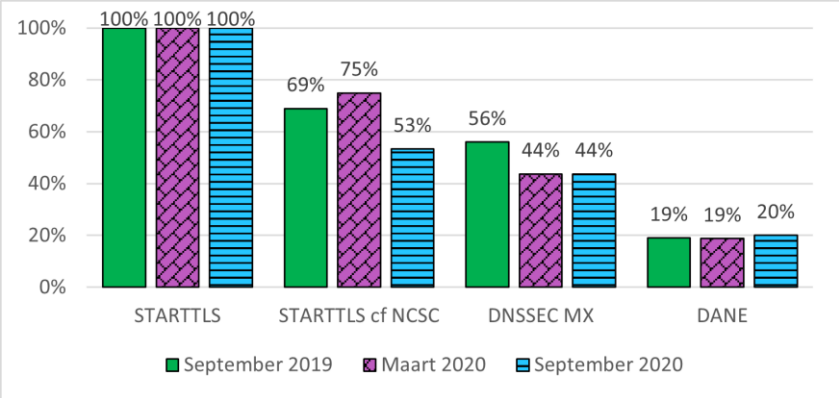
Ten aanzien van e-mail zien we helaas dat de stagnatie uit de voorgaande meting heeft doorgezet. Niet verrassend is de terugval bij STARTTLS conform de TLS-richtlijnen vanwege de strengere norm. DKIM wordt inmiddels weer wat betere toegepast, en 100% ligt binnen bereik. De provincies zijn helaas wel de meest 'spoofbare' overheidslaag, met de laagste adoptiegraad van een strikte DMARC policy (50%).

Gemiddelde adoptie provincies: mailstandaarden - anti-phishing



Ook de adoptiegraad van DNSSEC en DANE is met respectievelijk 44% en 20% het laagste van alle overheidslagen.

Gemiddelde adoptie provincies: mailstandaarden - beveiligde verbinding

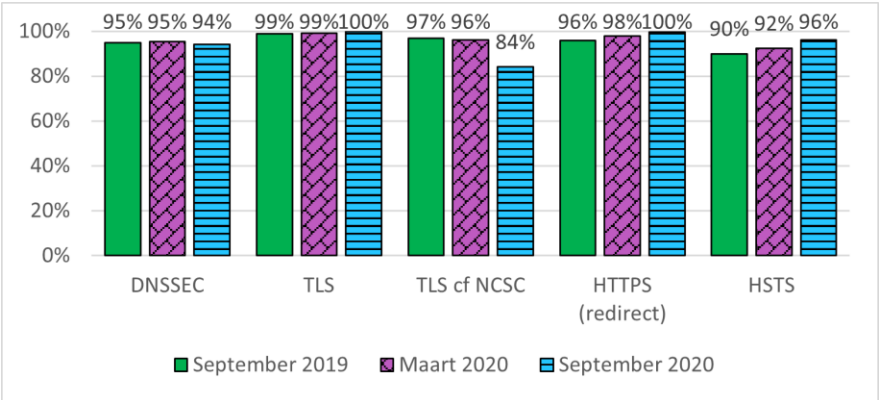


4.2.6. Gemeenten

De gemeenten scoren wederom het beste op het gebruik van de webstandaarden. De voornaamste uitdaging is om TLS conform de TLS-beveiligingsrichtlijnen weer boven het oude niveau te krijgen.

Het feit dat de gemeenten met afstand de meeste domeinen bezitten in onze test (365 van de 548) maakt de hoge scores nog indrukwekkender.

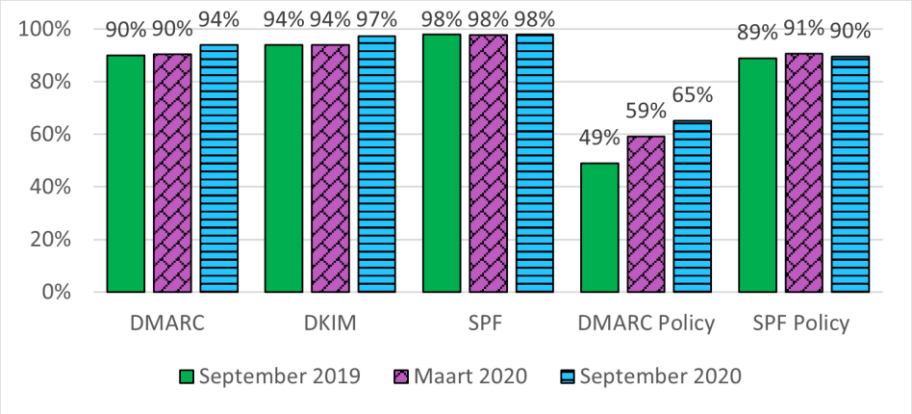
Gemiddelde adoptie gemeenten: webstandaarden



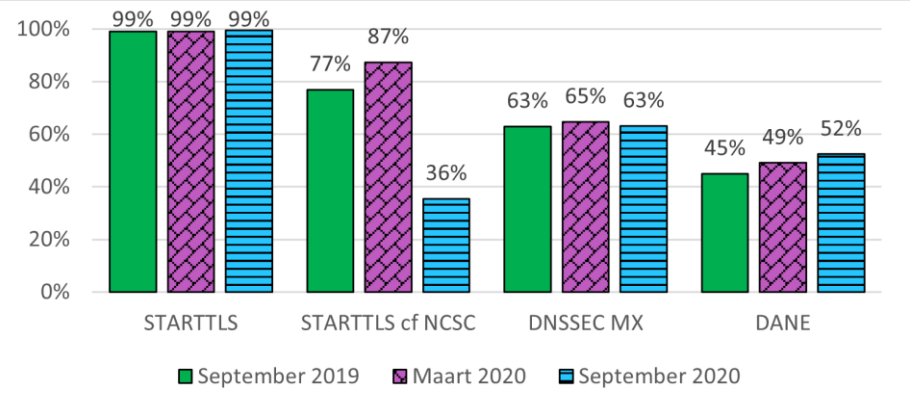
Bij de mailstandaarden zien we dat er nog aandacht nodig is voor het strikt afstellen van DMARC policy (65%) en SPF policy (90%).

Ook is de enorme terugval bij STARTTLS conform de TLS-beveiligingsrichtlijnen opvallend, de gemeenten scoren hier nu met afstand het slechtst. 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



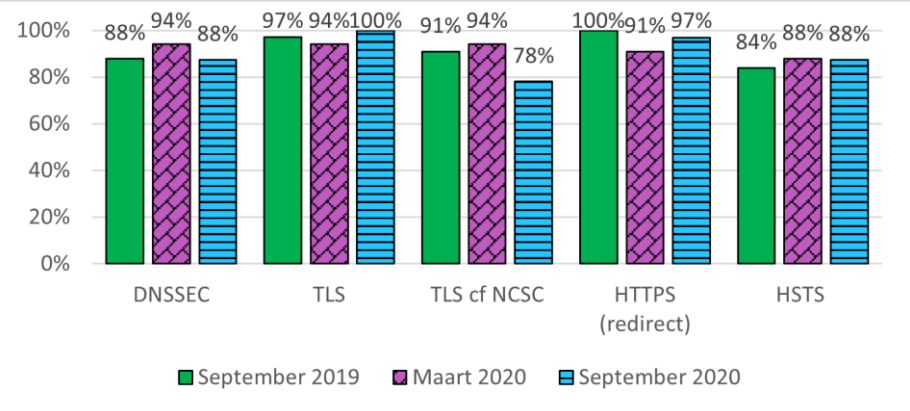
Gemiddelde adoptie gemeenten: mailstandaarden - beveiligde verbinding



4.2.7. Waterschappen

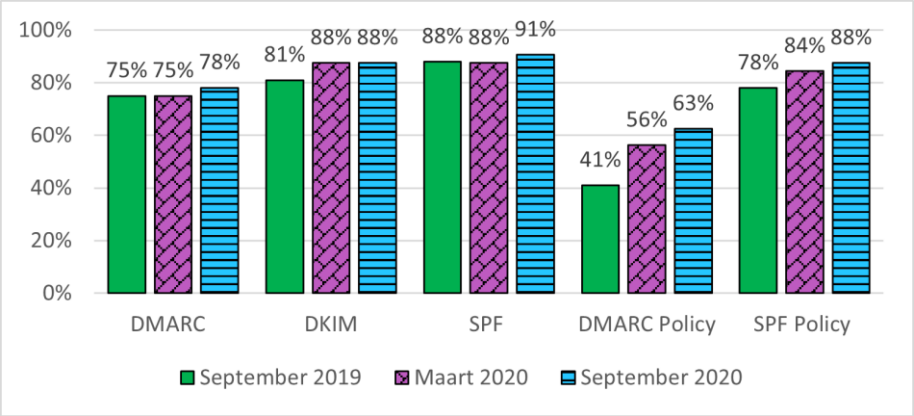
De waterschappen zijn een middenmotor in het toepassen van webstandaarden. Naast de verwachte achteruitgang bij TLS conform de TLS-beveiligingsrichtlijnen zien we een achteruitgang van 6% bij DNSSEC. De achteruitgang lijkt procentueel fors, maar valt mee in de wetenschap dat het gaat om 32 domeinen, waar één domein al voor meer dan 3% meetelt.

Gemiddelde adoptie waterschappen: webstandaarden

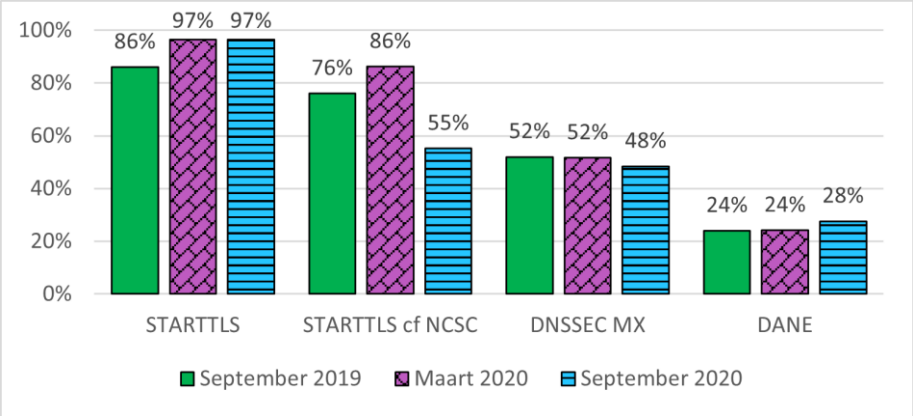


Op het vlak van e-mailbeveiligingsstandaarden beginnen de waterschappen gemiddeld gezien echt achter te lopen op de overige overheidslagen. Met name verbindingsbeveiliging vergt aandacht, maar ook de DMARC policies kunnen strikter worden ingesteld.

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 vanaf deze meting 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.

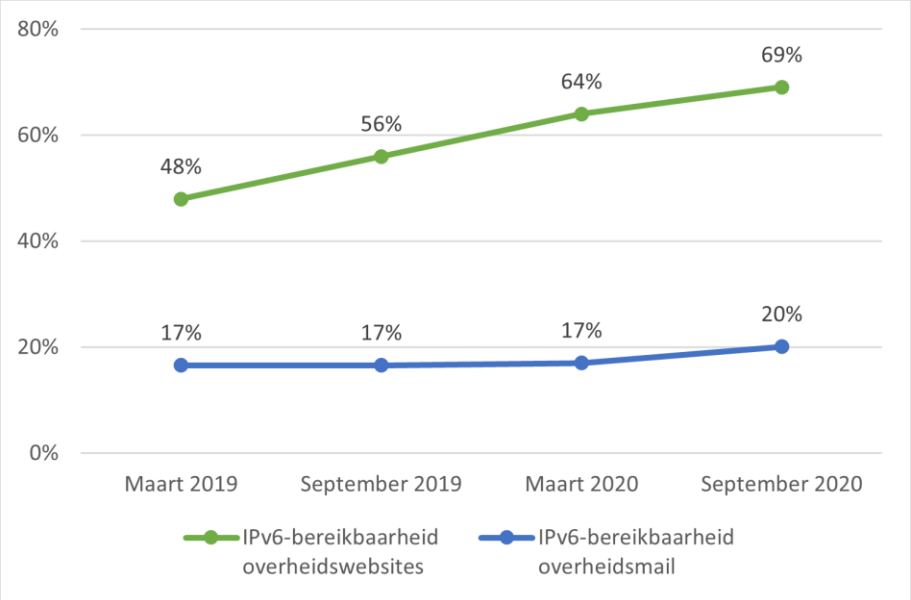
De volgende tabel geeft aan wat is getest.

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. De historische gegevens zijn bijvangst uit eerdere metingen. 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 1,5 jaar in de buurt van de 100% komen.

Trend bereikbaarheid van websites en e-maildomeinen overheid via internetstandaard IPv6

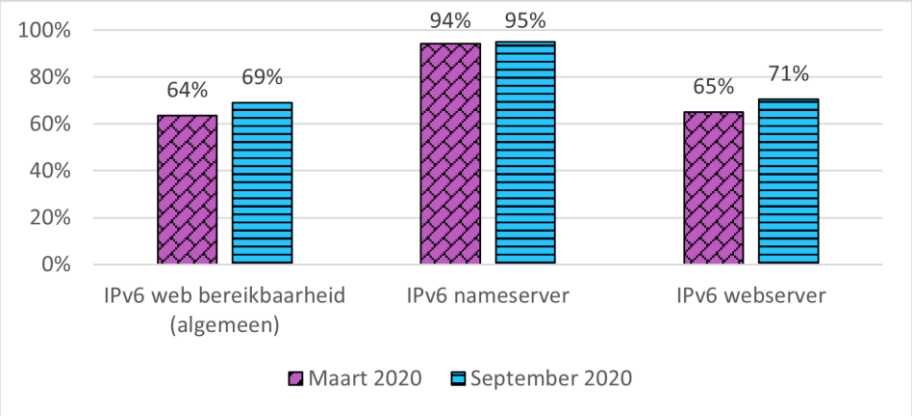


5.4. Bereikbaarheid overheidswebsites via IPv6

5.4.1. Gemiddelde bereikbaarheid

De gemiddelde bereikbaarheid van websites wordt met name geremd door de adoptie van IPv6 op webservers. De adoptiegraad is 71%. De adoptiegraad op nameservers is al relatief hoog, en dat illustreert dat het streefbeeld van 100% adoptie op dat aspect binnen bereik ligt.

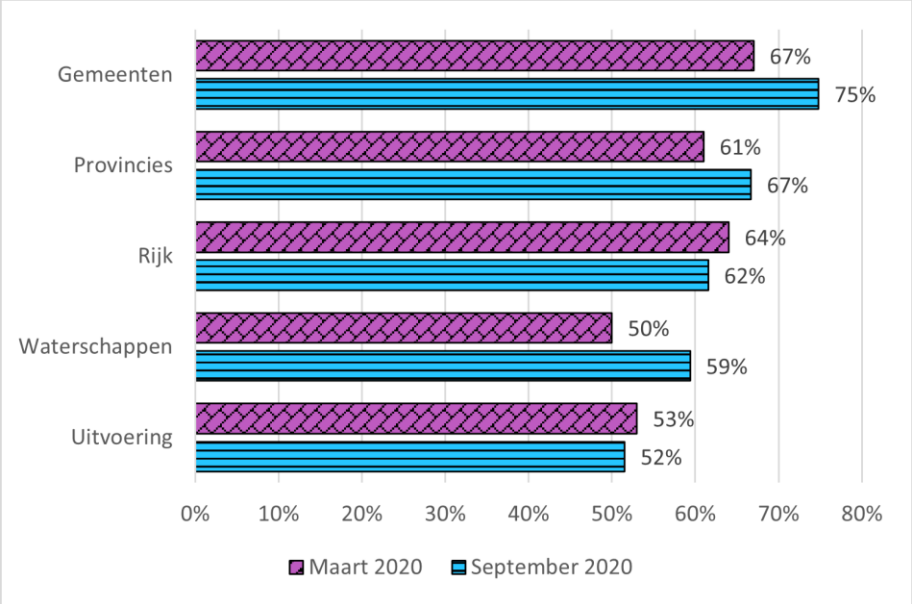
Bereikbaarheid overheidswebsites via IPv6



5.4.2. Per overheidslaag

De gemeenten scoren het beste op de bereikbaarheid van websites via IPv6. Dit komt waarschijnlijk met name door het programma van VNG Realisatie waarmee gemeenten worden ondersteund bij de implementatie van IPv6.

Bereikbaarheid websites via IPv6 per overheidslaag (van hoog naar laag)

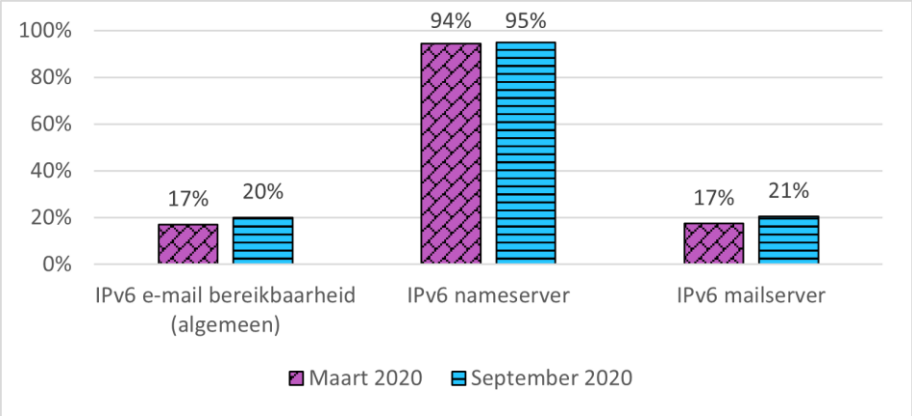


5.5. Bereikbaarheid e-maildomeinen via IPv6

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 slechts 21%. De adoptiegraad op nameservers is al relatief hoog, en dat illustreert dat het streefbeeld van 100% adoptie op dat aspect binnen bereik ligt.

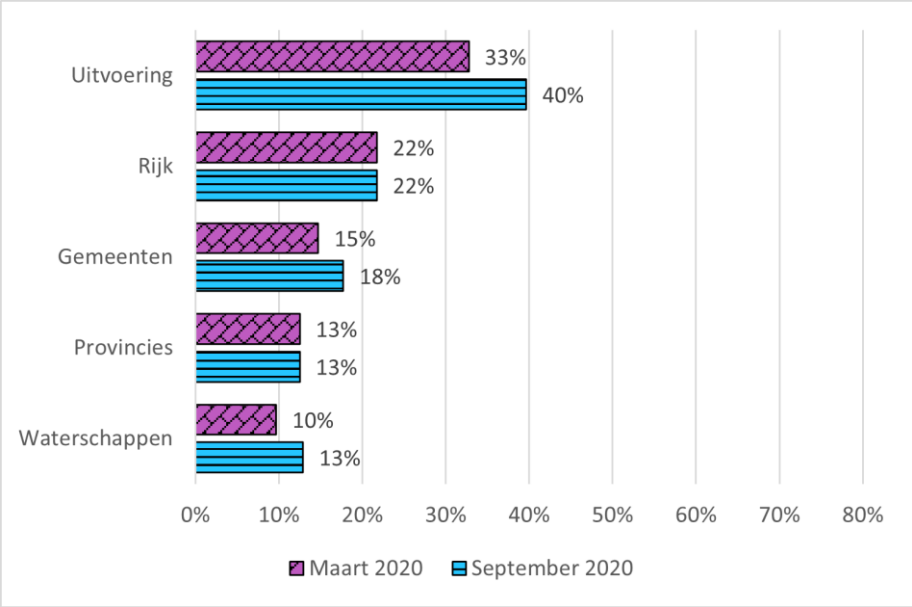
Bereikbaarheid e-maildomeinen overheid via IPv6



5.5.2. Per overheidslaag

Uitvoeringsorganisaties scoren gemiddeld het hoogst op IPv6. Dit komt onder meer doordat een aantal domeinen zijn aangesloten op de centrale mailvoorziening van Justitie en Veiligheid die IPv6 ondersteund.

Bereikbaarheid e-maildomeinen via IPv6 per overheidslaag (van hoog naar laag)



Adoptiegroei binnen de categorieën Rijk en uitvoering is met name te behalen als shared service providers, zoals DICTU en SSC-ICT, ook stappen zetten om de servers via IPv6 bereikbaar te maken. Met name SSC-ICT kan nog flinke stappen zetten, hun nameservers zijn nog niet per IPv6 bereikbaar.

Bij decentrale overheden zien we over het algemeen vaker gebruik van cloudmailoplossingen. Hierbij is het zaak de leverancier 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.

B5. Rapportage Open standaarden en voorzieningen (PBLQ)

PBLQ

Monitor Open Standaarden Voorzieningen 2020

Versie 0.99
12-2-2021

PBLQ
verbinders in de informatiesamenleving

Inhoudsopgave

PBLQ
verbinders in de informatiesamenleving

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 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 direct raken aan de communicatie en gegevensuitwisseling met burgers en bedrijven.

1.3 Werkwijze

Voor dit onderzoek is gebruik gemaakt van de 'pas toe of leg uit'-lijst van 1 april 2020. Voor elke voorziening is 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 vorig jaar. Waar

mogelijk zijn de standaarden opnieuw getoetst. Daarbij maken we onder meer gebruik van de testen die beschikbaar zijn via https://internet.nl. Hiermee kan voor een groot deel van de standaarden getoetst worden of eraan voldaan wordt[1]. Daarnaast kijken we – voor zover mogelijk – of de geplande activiteiten inmiddels uitgevoerd zijn. Voor nieuwe voorzieningen maken we een inschatting welke standaarden relevant zijn. Voor nieuwe standaarden op de lijst maken we 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 vertegenwoordigers 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 vertegenwoordigers 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

Voor de volgorde van het overzicht van standaarden is de volgorde van de flyer[2] met standaarden van het Forum Standaardisatie aangehouden.

[1] Deze toetst in bruikbaar voor een groot deel van de voorzieningen. Er zijn enkele uitzonderingen. Vaak betreft het ‘besloten’ voorzieningen die niet publiek via internet toegankelijk zijn.

[2] https://www.forumstandaardisatie.nl/sites/bfs/files/Lijst_verplichte_open_standaarden_sept-2018_0.pdf

1.4.2 Status

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

- Ja: De voorziening is conform[3] de standaard,
- Nee: De voorziening is niet conform de standaard,
- Deels: Onderdelen van de voorziening zijn conform aan, maar niet alle onderdelen[4],
- 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 toepassingsgebied en van het organisatorisch toepassingsgebied, zoals vermeld op de pas-toe-of-leg-uit lijst van het Forum Standaardisatie gehanteerd.[5] 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 van wanneer een voorziening aan een standaard voldoet is lastig. Het vereist een heldere afbakening van de voorziening en heldere voorwaarden voor 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 afwijken van elkaar 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

[3] Met “conform” wordt in dit onderzoek bedoeld dat de standaard door de eindgebruiker te gebruiken is.

[4] De bedoeling hiervan is dus niet dat een voorziening gedeeltelijk aan een standaard voldoet, maar dat *een onderdeel van* de voorziening helemaal aan de standaard voldoet. Voor dit onderdeel is dan in feite de status “Ja” van toepassing, maar niet voor de overige onderdelen. Idealiter zouden op termijn alle onderdelen van een voorziening aan de relevante standaard moeten voldoen.

[5] Zie: https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht

Voor een groot aantal standaarden hebben we gebruik gemaakt van de website internet.nl. De website is een initiatief van het Platform Internetstandaarden[6] 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 & 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.

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 dat een inclusieve benadering van digitale overheidsdienstverlening moet realiseren. 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 en binnen een redelijk haalbare termijn, toewerken naar volledig 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.
Momenteel is de wijze waarop overheden omspringen met de verplichting nog zeer divers. Gelet daarop en gelet op het feit dat 23 september 2020 bij de start van dit onderzoek nog een half jaar verder lag, is in overleg met de opdrachtgever besloten pas volgend jaar te toetsen op het al dan niet hebben van een toegankelijkheidsverklaring. We zullen dan ook (in overleg met de beheerder van de standaard) kijken of er een verdere objectivering van de beoordeling van het al dan niet voldoen aan de standaard mogelijk en wenselijk is.

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 27001/2 standaard. Indien een organisatie voldoet aan de BIO, dan voldoen zij binnen de context van dit rapport ook aan de verplichting om de ISO 27001/2 standaard te gebruiken. Waar er een aparte certificering op het gebied van ISO 27001 is toegekend, geven wij dit apart aan.

RPKI

[6] https://internet.nl/about/

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.
In het onderzoek is gebleken dat er onduidelijkheid was bij een groot aantal beheerders van voorzieningen over de vraag of de standaard voor hen van toepassing is.

- 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 gaat men ervan uit dat de netwerkleverancier dit regelt.
- 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.

Vanwege de verwarring is in overleg met Bureau Forum Standaardisatie besloten de standaard dit jaar nog niet in de tabel op te nemen. We hebben in het kader van dit onderzoek wel getoetst[7] of de standaard wordt toegepast en naar aanleiding van het onderzoek hebben ook een aantal voorzieningen de standaard alsnog geadopteerd. Uit het onderzoek blijkt dat 3 voorzieningen inmiddels wel voldoen aan de standaard, en dat nog 13 voorzieningen de standaard moeten adopteren. Alle voorzieningen die niet voldoen hebben daarnaast een mail ontvangen met deze boodschap. In een volgende monitor wordt de standaard wel in de tabel opgenomen.

2. Identificeren en authenticeren

2.1 DigiD

Beheerorganisatie: Logius

Werking en inhoud van DigiD
Met hun persoonlijke DigiD kunnen burgers inloggen op websites van de overheid en van private organisaties met een publieke taak (zoals pensioenfondsen en zorgverzekeraars). Diensten die met DigiD geregeld kunnen worden zijn o.a. het doen van belastingaangifte, het regelen van toeslagen, het aanvragen van uitkeringen, het aanvragen van studiefinanciering, het inzien van het landelijk diplomaregister, het aanvragen van een omgevingsvergunning, het registreren van donorschap, het inzien van pensioenoverzichten en zorgverzekeringen en het aanvragen van het rijexamen.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	DigiD mail wordt verstuurd met een DKIM signature (zie: https://internet.nl/mail/digid.nl/).

[7] De toetsing van RPKI is in samenwerking met het Bureau Forum Standaardisatie uitgevoerd. Voor de toetsing zijn de relevantie ip-adressen van de voorzieningen gecontroleerd via https://stat.ripe.net/46.22.185.32#tabId=routing

DMARC (Anti-phishing)	Ja	DMARC is voor DigiD geconfigureerd als een van de anti-phishing maatregelen (zie: https://internet.nl/mail/digid.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC is doorgevoerd in de domeinen (DNS-zones) van DigiD en operationeel. Ook de mailservers voldoen aan de standaard (zie: https://internet.nl/site/digid.nl/ en https://internet.nl/mail/digid.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	DigiD maakt gebruik van HTTPS voor de communicatie tussen clients (zoals browsers) en servers. Verder ondersteunt de DigiD website HSTS-policy met een geldigheidsduur van 1 jaar (zie: https://internet.nl/site/digid.nl/).
IPv4 en IPv6 (Internetnummers)	Ja	De website DigiD.nl is via IPv6 toegankelijk. Inmiddels verlopen ook de mailstromen via IPv6 (zie https://internet.nl/mail/digid.nl/ en https://internet.nl/site/digid.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Overheid (BIO) van toepassing die is gebaseerd op NEN-ISO27001/2. Logius heeft zich over toepassing van deze norm verantwoord door het afgeven van In Control Verklaringen (ICV's) aan de eigenaar (BZK/DGOBR).
SAML (Inloggegevens)	Ja	DigiD biedt aan afnemers een SAML-koppelvlak om authenticaties uit te kunnen voeren. Wanneer de afnemer “single sign on” wil gebruiken is dit alleen mogelijk via het SAML koppelvlak. De SAML koppelvlak-specificaties van DigiD zijn gepubliceerd op de website van Logius (zie: https://www.logius.nl/sites/default/files/public/bestanden/diensten/DigiD/Koppelvlakspecificatie-SAML-DigiD.pdf)
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is relevant voor DigiD bij alle mails vanuit de DigiD applicatie, en DigiD voldoet ook aan deze standaard (zie: https://internet.nl/mail/digid.nl/).
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Ja	De mailservers van DigiD passen STARTTLS/DANE toe (zie: https://internet.nl/mail/digid.nl/). Vanwege ondersteuning van oudere e-mailservers is een risicoafweging gemaakt om de TLS-versies 1.0 en 1.1 te blijven aanbieden.
TLS (Beveiligde, versleutelde verbindingen)	Ja	DigiD ondersteunt voor de website-domeinen alleen TLS v1.2. Voor het backend-domein digid.nl is vanwege ondersteuning van afnemers met oudere backend-systemen een risicoafweging gemaakt om nog een aantal “uit te faseren” ciphersuites te handhaven.

Ten opzichte van 2019 voldoet de voorziening aan STARTTLS/DANE.

Concluderend zijn er geen standaarden die DigiD nog (volledig) dient te implementeren.

2.2 DigiD Machtigen

Beheerorganisatie: Logius

Werking en inhoud van DigiD Machtigen
DigiD Machtigen stelt burgers in staat anderen namens hen te machtigen om DigiD te gebruiken.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	DigiD Machtigen ontvangt en verstuurt geen email op het domein machtigen.digid.nl. Er is een DMARC record (zie: https://internet.nl/mail/machtigen.digid.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	Het domein https://machtigen.digid.nl voldoet aan DNSSEC (zie: https://internet.nl/site/machtigen.digid.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	Deze standaarden zijn geïmplementeerd (zie: https://internet.nl/site/machtigen.digid.nl/).
IPv4 en IPV6 (Internetnummers)	Ja	Zowel IPv6 als IPv4 worden ondersteund (zie: https://internet.nl/site/machtigen.digid.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Op de Rijksoverheid is de BIO van toepassing die is gebaseerd op NEN-ISO27001. Logius heeft zich over toepassing van de BIR norm verantwoord door het afgeven van In Control Verklaringen (ICV's) aan de eigenaar (BZK/DGOBR).
SAML v2.0 (Inloggegevens)	Ja	Het authenticatiekoppelvlak met eHerkenning voldoet aan de SAML standaard. Het authenticatiekoppelvlak met DigiD maakt gebruik van SAML. Overgang naar een SAML koppelvlak is gerealiseerd met de livegang van de nieuwe website voor het DigiD Machtigen (publieke machtigingenregister), 10 juni 2020. Naast authenticatie gebruikt DigiD Machtigen de SAML standaard ook om een getekend machtigingsbewijs af te geven, namelijk als een SAML assertion.
SPF (Preventie van mailspoofing/ phishing)	Ja	DigiD Machtigen verstuurt geen email aan gebruikers. Er is wel een SPF record aangemaakt voor het domein: machtigen.digid.nl welke aangeeft dat er vanaf dit domein geen email wordt verstuurd.
TLS (Beveiligde, versleutelde verbindingen)	Gepland	TLS is geïmplementeerd. DigiD Machtigen ondersteunt TLS v1.2. TLS 1.0 en 1.1 worden niet meer ondersteund. We hebben nog een waarschuwing voor cypher volgorde en we ondersteunen onvoldoende veilige parameters voor Diffie-Hellman-sleuteluitwisseling. Dit staat op de planning voor de patchronde van juli 2020.
		Document en (web/app)content
PDF/A en PDF 1.7	Ja	De voorziening voldoet aan deze standaard.

(Document-publicatie/ archivering)		
		Stelselstandaarden
Digikoppeling 2.0	Deels	Recent ontwikkelde koppelvlakken en/of nieuwe versies van bestaande koppelvlakken zijn Digikoppeling compliant (bijvoorbeeld DVS 2017). Er zijn echter nog koppelvlakken waarvan geen Digikoppeling compliant versie is gemaakt en/of koppelvlakken waar nog diensten afnemers op aangesloten zitten (bijvoorbeeld PBS (Een koppelvlak waarover een aangesloten dienstaanbieder kan controleren of iemand daadwerkelijk gemachtigd is om te handelen namens een vertegenwoordigde)). Deze koppelvlakken bestaan uit de tijd dat de Digikoppeling standaard in ontwikkeling was en voldoen deels aan de uiteindelijk ontstane Digikoppeling standaard. Het is de bedoeling dat bestaande dienst afnemers overgaan naar de nieuwe koppelvlakken. Hier wordt niet actief op gestuurd. Door ontwikkelingen rondom eID, eIDAS en DigiD Machtigen moeten afnemers in de toekomst gebruik maken van andere koppelvlakken, waardoor gebruik van de niet compliant koppelvlakken zal afnemen. Bij nieuwe koppelvlakontwikkelingen zal meer naar de REST-API standaard worden gekeken dan naar Digikoppeling 2.0.

Ten opzichte van 2019 voldoet DigiD Machtigen aan SAML. De voorziening voldoet niet aan TLS, waardoor de status van ja naar gepland gaat.

Concluderend, moet DigiD Machtigen nog de volgende standaarden (volledig) implementeren: TLS en Digikoppeling 2.0.

2.3 PKIoverheid

Beheerorganisatie: Logius

Werking en inhoud van PKIoverheid
Met PKIoverheid wordt de betrouwbaarheid van informatie-uitwisseling via e-mail en websites op basis van Nederlandse (en Europese) wetgeving geborgd. Er zijn acht Toegetreden vertrouwensdienstverleners (TSP's) die PKIoverheidscertificaten verstrekken. Dit zijn: KPN, ESG, QuoVadis, Digidentity, Cleverbase, CIBG, het Ministerie van Infrastructuur en Waterstaat en het Ministerie van Defensie.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	Pkioverheid.nl voldoet aan DMARC (zie: https://internet.nl/mail/pkioverheid.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	Het PKIoverheid-deel van de website van Logius en de website van PKIoverheid maken gebruik van DNSSEC (zie: https://internet.nl/domain/crl.pkioverheid.nl/ en https://internet.nl/domain/www.logius.nl/).

HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels	Deze standaard wordt toegepast door de voorziening (zie: https://internet.nl/domain/crl.pkioverheid.nl/ en https://internet.nl/domain/www.logius.nl/). Voor logius.nl, crl.pkioverheid.nl en cert.pkioverheid.nl is HTTPS goed geconfigureerd. pkioverheid.nl en www.pkioverheid.nl verwijzen door (oftewel 'redirecten') naar cert.overheid.nl. Alleen voor deze domeinen faalt de test op het punt "HTTPS-doorverwijzing". Met het ingaan van het nieuwe contract is het compliant maken aan de open standaarden van de website pkioverheid.nl een van de projecten die hierin is opgenomen.
IPv4 en IPV6 (Internetnummers)	Nee	IPv6 is geïmplementeerd voor de informatiepagina's van PKIoverheid op de Logius website (zie: https://internet.nl/domain/www.logius.nl/). De PKIoverheid specifieke applicatiepagina's zijn op dit moment nog niet geschikt voor IPv6 (zie: https://internet.nl/domain/crl.pkioverheid.nl/). De implementatiedatum is gekoppeld aan gunning van een nieuw contract aan applicatieleverancier. Gunning heeft inmiddels plaatsgevonden. Implementatie van IPV6 is een van de projecten die in dit contract is opgenomen. Planning hiervan heeft nog niet plaatsgevonden.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Primair is het Webtrust normenkader van toepassing op PKIoverheid. Dit kader kent strengere eisen dan deze ISO standaarden vereisen. Implementatie van de BIO is daarnaast uitgevoerd op basis van best effort.
TLS	Ja	Het PKIoverheid deel van de website van Logius maakt gebruik van TLS 1.1 en 1.2 en de website van PKIoverheid zelf maakt gebruik van TLS 1.2 (zie: https://internet.nl/domain/crl.pkioverheid.nl/ en https://internet.nl/domain/www.logius.nl/). Uit te faseren ciphers voor pkioverheid.nl worden opgepakt bij vernieuwing van website.
		Document en (web/app)content
OWMS (Metadata overheidsinformatie)	Ja	Het PKIoverheid deel van de website van Logius voldoet aan de standaard, maar niet op de website van PKIoverheid (deze informatie is niet bedoeld voor hergebruik van overheidsinformatie).
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie /archivering)	Ja	Documenten die via de websites beschikbaar worden gesteld worden volgens PDF/A opgesteld.

Ten opzichte van 2019 is de planning voor implementatie van IPv4 en IPv6 niet gehaald. Er is geen nieuwe planning afgegeven. De status gaat van gepland naar nee.

Concluderend moeten voor PKIoverheid nog de volgende standaarden (volledig) worden geïmplementeerd: HTTPS/HSTS, IPv4 en IPv6.

2.4 Afsprakenstelsel elektronische toegangsdiensten

Beheerorganisatie: Logius

Werking en inhoud van het Afsprakenstelsel Elektronische Toegangsdiensten
Het Afsprakenstelsel Elektronische Toegangsdiensten is een set van technische, functionele, juridische en organisatorische afspraken op basis waarvan het netwerk van eHerkenning wordt geleverd in een publiek-private samenwerking. Dat betekent dat het netwerk wordt geleverd door private dienstverleners, waarbij er publieke ondersteunende diensten zijn (in beheer bij de 'Beheerorganisatie eHerkenning'). De afspraken hebben als doel om samenwerking en zekerheid in het netwerk te garanderen. Tegelijkertijd bieden de afspraken ook vrijheid aan de deelnemers om competitieve proposities te leveren aan hun klanten.

Sinds 2016 is het Afsprakenstelsel Elektronische Toegangsdiensten in het onderzoek opgenomen in plaats van eHerkenning. Het afsprakenstelsel bevat de voor dit onderzoek relevante eisen voor eHerkenning en is in beheer bij de 'Beheerorganisatie eHerkenning', die is ondergebracht bij Logius. Het afsprakenstelsel is sterk aan veranderingen onderhevig. Zo was Idensys tot voor kort nog onderdeel van het stelsel, wordt het inloggen vanuit Europa bij overheidsinstellingen in Nederland sinds begin 2019 ondersteund (eIDAS) en kan men vanaf eind 2020 via het stelsel inloggen in Europa met een Nederlands inlogmiddel (eIDAS).

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	Bij verstuurde e-mail wordt DKIM toegepast, bij ontvangst gebeurt dit door de centrale e-mailvoorziening, die Logius als dienst afneemt van het Shared Service Centrum van het Rijk (SSC-ICT).
DMARC (Anti-phishing)	Gepland	Het Afsprakenstelsel Elektronische Toegangsdiensten maakt geen gebruik van e-mailfunctionaliteit, maar de policy voor ondersteunende e-maildiensten is niet voor Q1 2020 aangescherpt. Door een scopewijziging bij een aanbesteding wordt een oude component later dan voorzien uit productie genomen, waardoor de policy nog niet aangescherpt kon worden. De nieuwe planning is uiterlijk Q4 2020 volledig compliant te zijn. (Zie: https://internet.nl/mail/eherkenning.nl/)
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC werd in 2015 in de productieomgeving opgenomen.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	HTTPS en HSTS wordt toegepast op alle websites en webapplicaties onder beheer van de beheerorganisatie en deelnemers in het stelsel.
IPv4 en IPv6 (Internetnummers)	Deels	Het Afsprakenstelsel Elektronische Toegangsdiensten voldoet aan IPv4 en IPv6. Ondersteunende e-mailservers, die geen onderdeel uitmaken van het netwerk, voldoen niet volledig. (Zie: https://internet.nl/mail/eherkenning.nl/). Voor inkomende e-mail wordt door Logius gebruik gemaakt van de dienstverlening van het Shared Service Centrum van het Rijk (SSC-ICT).
NEN-ISO/IEC 27001/27002	Ja	In het afsprakenstelsel wordt certificering tegen ISO27001 geëist voor de deelnemers. De beheerorganisatie eHerkenning is als

(Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)		stelselbeheerder ook gecertificeerd volgens ISO 27001. Daarvoor is ook een in control statement beschikbaar.
SAML (Inloggegevens)	Ja	SAML is een verplichte eis vanuit het stelsel.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF wordt toegepast bij de voorziening, maar wordt vooralsnog niet vereist als toe te passen techniek voor deelnemers.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	STARTTLS is geïmplementeerd voor eherkenning.nl en idensys.nl. DANE voor SMTP is voor de maildomeinen geïmplementeerd bij de centrale e-mailvoorziening, die Logius als dienst afneemt van het Shared Service Centrum van het Rijk (SSC-ICT).
TLS (Beveiligde, versleutelde verbindingen)	Deels	Het Afsprakenstelsel Elektronische Toegangsdiensten stelt het gebruik van TLS volgens de richtlijnen van het NCSC verplicht. Ondersteunde e-mailservers, die geen onderdeel uitmaken van het netwerk, voldoen niet volledig (zie: https://internet.nl/mail/eherkenning.nl/). Voor inkomende e-mail wordt door Logius gebruik gemaakt van de dienstverlening van het Shared Service Centrum van het Rijk (SSC-ICT).
		Document en (web/app)content
PDF 1.7, PDF/A-1 of PDF/A-2 (Documentpublicatie/ archivering)	Ja	Primair wordt de stelseldocumentatie via HTML op eherkenning.nl gepubliceerd. Stelseldocumentatie wordt met behulp van officesoftware gepubliceerd in PDF/A-formaat. Overige documenten worden met een aparte tool in PDF/A formaat geconverteerd, omdat het gehanteerde DMS dit niet ondersteunt.

Ten opzichte van 2019 voldoet de voorziening nog deels aan TLS. De status van deze standaard is van ja naar deels gegaan. De planning voor het implementeren van DMARC is niet gehaald, de status blijft gelijk.

Concluderend moeten voor Afsprakenstelsel Elektronische Toegangsdiensten nog de volgende standaarden (volledig) worden geïmplementeerd: DMARC, IPv4 en IPv6, TLS.

3. Dienstverlening en informatieverstrekken

3.1 MijnOverheid

Beheerorganisatie: Logius

Werking en inhoud van MijnOverheid
MijnOverheid is een persoonlijk toegangsportaal waarin verschillende diensten van de overheid ontsloten worden. MijnOverheid gaat over persoonlijke, en om die reden met DigiD beveiligde, diensten en informatie. Binnen MijnOverheid heeft de burger toegang tot de Berichtenbox, Lopende Zaken en Persoonlijke Gegevens. De Berichtenbox is de persoonlijke brievenbus waarin burgers post van onder meer de

Belastingdienst, RDW, SVB, UWV, gemeenten en pensioenfondsen kunnen ontvangen. Lopende Zaken geeft weer wat de stand is van bijvoorbeeld aanvragen of vergunningen. Inzage Persoonlijke Gegevens maakt het mogelijk om te controleren of de eigen gegevens correct zijn opgeslagen bij de overheid. Logius is verantwoordelijk voor het portaal, de aangesloten partijen zijn verantwoordelijk voor hun eigen dienstverlening die via MijnOverheid benaderd kan worden.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/ phishing)	Ja	MijnOverheid voldoet aan DKIM (zie: https://internet.nl/mail/mijnoverheid.nl/ en https://internet.nl/mail/mijn.overheid.nl/).
DMARC (Anti-phishing)	Ja	Deze standaard wordt toegepast.
DNSSEC (Beveiligde domeinnamen)	Ja	MijnOverheid voldoet aan DNSSEC (zie: https://internet.nl/site/mijnoverheid.nl/ en https://internet.nl/site/mijn.overheid.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	HTTPS wordt toegepast voor zowel het domein mijn.overheid.nl, als mijnoverheid.nl. HSTS wordt toegepast voor het domein mijn.overheid.nl. HSTS voor mijnoverheid.nl is niet van toepassing, omdat die enkel redirect naar mijn.overheid.nl.
IPv4 en IPV6 (Internetnummers)	Ja	MijnOverheid gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internetgebruik. MijnOverheid ondersteunt op dit moment IPv4 en IPv6. Mijn.overheid.nl voldoet aan de standaard. IPv6 staat niet op de inkomende mailservers er bestaat ook geen planning voor om dit wel te doen.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Op de Rijksoverheid is de BIO van toepassing die is gebaseerd op NEN-ISO27001. Logius heeft zich over toepassing van deze norm verantwoord door het afgeven van In Control Verklaringen (ICV'en) aan de eigenaar (BZK/DGOBR). De ICV's zijn nog up-to-date.
SAML (Inloggegevens)	Ja	Authenticatie loopt via SAML.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is relevant en geïmplementeerd.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	Deze standaard wordt toegepast.
TLS (Beveiligde, versleutelde verbindingen)	Ja	In de dienstverlening aan burgers maakt MijnOverheid gebruik van een TLS 1.2-verbinding (zie: https://internet.nl/site/mijn.overheid.nl). De koppelingen met afnemers (overheidsorganisaties) lopen ook via TLS op basis van PKIoverheid-certificaten. MijnOverheid gebruikt TLS 1.2 en veilige

		cipher suites. Een aantal oude ciphers wordt nog ondersteund omdat er anders problemen ontstaan bij afnemers, burgers e.d. TLS 1.3 moet nog geïmplementeerd worden. Oudere versies worden niet meer geaccepteerd.
		Document en (web/app)content
Open API Specification (Beschrijven van REST API's)	Ja	Deze standaard wordt gebruikt voor de REST-API's van MijnOverheid.
PDF 1.7, PDF/A-1 of PDF/A-2 (Documentpublicatie/archivering)	Ja	MijnOverheid genereert zelf PDF-bestanden welke voldoen aan de PDF/A-1a standaard. MijnOverheid neemt concrete stappen om te gaan controleren op de toegankelijkheid en veiligheid van PDF-bestanden die aangeleverd worden door afnemers via de Berichtenbox.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Zowel nieuwe als oude koppelingen worden conform Digikoppeling 2.0 ingericht.
StUF (Uitwisseling administratieve overheidsgegevens)	Ja	MijnOverheid heeft waar relevant de koppeling op basis van StUF. Dit is alleen relevant voor WOZ en Lopende Zaken.

Ten opzichte van 2019 is de status van IPv4 en IPv6 van deels naar ja gegaan. HTTPS/HSTS is – ondanks negatieve score op internet.nl - goedgekeurd naar aanleiding van handmatige analyse door onderzoekers van het Bureau Forum Standaardisatie.

Concluderend zijn er geen standaarden die mijnOverheid nog (volledig) moet implementeren.

3.2 Berichtenbox voor bedrijven

Beheerorganisatie: Rijksdienst voor Ondernemend Nederland (RVO).

Inhoud en werking Berichtenbox voor bedrijven
De Berichtenbox voor bedrijven is het beveiligde e-mailsysteem tussen ondernemers en de overheid. De Berichtenbox voor bedrijven is vergelijkbaar met de Berichtenbox voor burgers (zie MijnOverheid.nl), met als belangrijkste verschil dat de Berichtenbox voor bedrijven tweerichtingsverkeer tussen ondernemers en de overheid mogelijk maakt. Via de Berichtenbox wordt (bedrijfs)gevoelige informatie veilig uitgewisseld met overheden, bijvoorbeeld voor vergunningaanvragen aan gemeente of provincie, meldingen, inschrijvingen en registraties.

De Berichtenbox is speciaal gemaakt voor de Dienstenwet. Voor alle procedures die onder de Dienstenwet vallen, hebben ondernemers het recht om de Berichtenbox te gebruiken. Overheidsorganisaties zijn verplicht berichten via de Berichtenbox te beantwoorden.

BZK heeft het voornemen uitgesproken om de Berichtenbox voor bedrijven op termijn uit te faseren. Er dient dan wel een vervangend systeem te zijn voor berichtenverkeer naar ondernemingen én voor de loketfunctie in het kader van de Dienstenwet. Naar het zich nu laat aanzien, zal uitfasering eind 2022 zijn.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	@antwoordvoorbedrijven.nl en @berichtenbox.antwoordvoorbedrijven.nl voldoen hieraan. Dit kan gecontroleerd worden op https://internet.nl/mail/antwoordvoorbedrijven.nl en https://internet.nl/mail/berichtenbox.antwoordvoorbedrijven.nl N.B. De notificaties de we sturen hebben als afzender noreply-berichtenbox@antwoordvoorbedrijven.nl
DMARC (Anti-phishing)	Ja	@antwoordvoorbedrijven.nl en @berichtenbox.antwoordvoorbedrijven.nl voldoen hieraan. Dit kan gecontroleerd worden op https://internet.nl/mail/antwoordvoorbedrijven.nl en https://internet.nl/mail/berichtenbox.antwoordvoorbedrijven.nl N.B. De notificaties de we sturen hebben als afzender noreply-berichtenbox@antwoordvoorbedrijven.nl
DNSSEC (Beveiligde domeinnamen)	Ja	Volgens internet.nl voldoet het domein berichtenbox.antwoordvoorbedrijven.nl (zie: https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Gepland	HTTPS/HSTS is al operationeel op de Berichtenbox maar is nog niet volledig geïmplementeerd. HTTPS/HSTS wordt RvO breed gerealiseerd (overgang naar nieuwe SOAP versie; zogenaamde cloud migratie), staat gepland voor realisatie uiterlijk medio 2021.
IPv4 en IPv6 (Internetnummers)	Gepland	De website van de Berichtenbox ondersteunt IPv4 maar is volgens internet.nl niet toegankelijk via IPv6 (zie: https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/). De implementatie moet DICTU-breed gebeuren voordat dit voor de Berichtenbox gedaan zal worden. IPv6 wordt RvO breed gerealiseerd en is onderdeel van de toegangsverleningsservice (TVS) voorziening en moet ultimo 2021 zijn gerealiseerd.
SAML (Inloggegevens)	Ja	eHerkenning is SAML-based en wordt toegepast voor het inloggen op de Berichtenbox.
SPF (Preventie van mailspoofing/phishing)	Ja	@antwoordvoorbedrijven.nl en @berichtenbox.antwoordvoorbedrijven.nl voldoen hieraan. Dit kan gecontroleerd worden op https://internet.nl/mail/antwoordvoorbedrijven.nl en https://internet.nl/mail/berichtenbox.antwoordvoorbedrijven.nl N.B. De notificaties de we sturen hebben als afzender noreply-berichtenbox@antwoordvoorbedrijven.nl
TLS (Beveiligde, versleutelde verbindingen)	Nee	De Berichtenbox maakt gebruik van TLS 1.2 (zie: https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/). Client-initiated renegotiation komt niet door de test. Client-initiated renegotiation (CIR) heeft impact op de beschikbaarheid en niet op de vertrouwelijkheid. Kort samengevat: wij zien CIR niet als een

		beveiligingsissue en is ook niet als zodanig in de Pentest naar voren gekomen.
		Document en (web/app)content
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/ archivering)	Ja	Alle berichten kunnen worden gedownload (vanaf de Berichtenbox website) in PDF/A formaat. PDF-documenten worden gegenereerd in PDF A/1.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Overheden kunnen via Digikoppeling geautomatiseerd berichten verzenden en ontvangen. Ondernemers kunnen alleen handmatig (via de website) hun Berichtenbox gegevens opvragen.
StUF (Uitwisseling administratieve overheidsgegevens)	Ja	StUF wordt in combinatie met Digikoppeling gebruikt voor de uitwisseling met alle partijen die via digikoppeling op de Berichtenbox zijn aangesloten.

Ten opzichte van 2019 voldoet de voorziening aan DMARC, DKIM en SPF, de status van HTTPS/HSTS is van ‘ja’ naar ‘gepland’ gegaan en de status van IPv4 en IPv6 is van ‘nee’ naar ‘gepland’ gegaan.

Concluderend moeten voor Berichtenbox voor bedrijven nog de volgende standaarden (volledig) worden geïmplementeerd: HTTPS/HSTS, IPv4 en IPv6 en TLS.

3.3 Overheid.nl

Beheerorganisatie: Kennis- en Exploitatiecentrum Officiële Overheidspublicaties (KOOP)

Werking en inhoud van Overheid.nl
De website Overheid.nl biedt centrale internettoegang voor informatie en diensten van de Nederlandse overheid. Overheid.nl is bestemd voor burgers, bedrijven en ondernemers en andere overheden. Overheid.nl bevat naast informatie en diensten ook de contactgegevens van Nederlandse overheidsorganisaties. Ook het domein wetten.overheid.nl valt onder deze voorziening.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	DKIM is geïmplementeerd (zie: https://internet.nl/mail/overheid.nl/).
DMARC (Anti-phishing)	Ja	DMARC is volledig doorgevoerd.
DNSSEC (Beveiligde domeinnamen)	Ja	Overheid.nl voldoet sinds Q2 2015 aan DNSSEC (zie: https://internet.nl/site/www.overheid.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	Overheid.nl voldoet aan HTTPS en HSTS (zie: https://internet.nl/site/overheid.nl/).

IPv4 en IPV6 (Internetnummers)	Ja	Er wordt voldaan aan IPv4 en IPv6 (zie: https://internet.nl/domain/www.overheid.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Vanaf 2015 staat overheid.nl niet meer op de risicokaart van BZK en hoeft hiervoor geen ICV (In Control Verklaring) meer te worden afgegeven. Voor OEB, de applicatie die centraal staat in het publiceren van overheidsinformatie en richtinggevend is voor alle KOOP-dienstverlening, wordt wel jaarlijks een ICV afgegeven; deze is gebaseerd op de BIO die weer is gebaseerd op NEN-ISO/IEC 27001/27002. Alle dienstverlening van KOOP is ondergebracht bij een hostingpartij die jaarlijks een ISAE3402 Type II verklaring laat opstellen; deze verklaring baseert zich mede op de certificering met NEN-ISO/IEC 27001/27002.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	Overheid.nl voldoet hieraan (zie: https://internet.nl/mail/overheid.nl/).
TLS (Beveiligde, versleutelde verbindingen)	Gepland	Op de website is het volledig doorgevoerd. De mailomgeving geeft een melding. Deze wordt opgelost in oktober 2020.
		Document en (web/app)content
OWMS (Metadata overheidsinformatie)	Ja	Overheid.nl is gemetadateerd conform OWMS.
PDF 1.7 PDF/A-1 PDF/A-2 (Documentpublicatie/ archivering)	Ja	Alle PDF's van officiële bekendmakingen zijn PDF/A-1a zoals wettelijk bepaald is.
SKOS (Thesauri en begrippenwoordenboeken)	Ja	SKOS is geïmplementeerd voor de waardelijsten van OWMS.
		Juridische identificatie en verwijzing
BWB (Wet- en regelgeving)	Ja	Overheid.nl is zelfs de bron van de BWB identificatie (zie: wetten.overheid.nl).
JCDR (Decentrale regelgeving)	Ja	Overheid.nl is zelfs de bron van de JCDR identifiers (zie: https://zoek.overheid.nl/lokale_wet_en_regelgeving).

Ten opzichte van 2019 voldoet de voorziening aan HTTPS en HSTS, maar niet langer (volledig) aan TLS.

Concluderend moeten voor Overheid.nl nog de volgende standaarden (volledig) worden geïmplementeerd: TLS.

3.4 Ondernemersplein

Beheerorganisatie: Kamer van Koophandel

Ondernemersplein is een onderdeel van de website van de Kamer van Koophandel. Dat heeft geleid tot een effect ten aanzien van het gebruik van standaarden en de wijze van rapporteren daarvan namelijk in het jaarverslag (miv 2020). KVK heeft op kwartaalbasis een interne WDO scan ingericht waarmee haar business owners kunnen sturen op compliancy aan de WDO. WDO is een superset van de standaarden die via de Monitor gedekt worden.

Werking en inhoud van Ondernemersplein

Het Ondernemersplein is de centrale plek (website) waar overheden gezamenlijke informatie en hulpmiddelen aanbieden voor ondernemers, variërend van praktische stappenplannen en webinars tot informatie over regelgeving en geldzaken. Daarnaast bestaat de mogelijkheid voor overheden de content van Ondernemersplein via hun eigen kanalen te ontsluiten. Ondernemersplein.kvk.nl is de vervanger van ondernemersplein.nl, die sinds 2019 slechts doorverwijst.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Deels	DKIM is geïmplementeerd voor domein kvk.nl maar niet specifiek voor het subdomein ondernemersplein.kvk.nl.
DMARC (Anti-phishing)	Ja	Ondernemersplein als onderdeel van kvk.nl voldoet aan DMARC.
DNSSEC (Beveiligde domeinnamen)	Ja	Ondernemersplein voldoet aan DNSSEC voor de website. Er wordt niet gemaild vanuit mail subdomein maar van kvk.nl.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	Aan deze standaard wordt voldaan voor het domein kvk.nl
IPv4 en IPV6 (Internetnummers)	Nee	IPv4 klaar, IPv6 target : eind 2021 conform overheidsbrede afspraken
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Ondernemersplein is onderdeel van de website van de Kamer van Koophandel. KVK is ISO 27001 gecertificeerd vanaf 2016. KVK is in 2019 opnieuw succesvol gecertificeerd.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd voor kvk.nl.
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Nee	Aan STARTTLS wordt voldaan, maar aan DANE wordt nog niet voldaan. De KvK vindt de relevantie van DANE voor mail laag: er zijn geen mailservers die DANE geïmplementeerd hebben.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De websites ondernemersplein.kvk.nl en www.kvk.nl zijn TLS 1.2 of beter beveiligd.
		Document en (web/app)content
CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)	Nee	De tooling (CMS/ESB) ondersteunt de standaard, maar deze wordt niet actief gebruikt. Er zijn geen content leveranciers die hun CMS in CMIS vorm aan het Ondernemersplein beschikbaar

		stellen. Concreet is er dus nog geen toepassing op dit moment en er zijn ook nog geen plannen om dit te doen.
OWMS (Metadata overheidsinformatie)	Nee	De informatie op de website is gemetadateerd volgens een eigen model die past bij de metadatering van de partners.
		Juridische identificatie en verwijzing
BWB (Wet- en regelgeving)	Ja	Binnen de website, de content van AvB, wordt verwezen naar wetgeving conform de BWB standaard.

Ten opzichte van 2019 voldoet Ondernemersplein aan DNSSEC, HTTP/HTTPS en SPF.

Concluderend, moet Ondernemersplein nog de volgende standaarden (volledig) implementeren: DKIM, IPv6, DANE, CMIS en OWMS.

3.5 Samenwerkende catalogi

Beheerorganisatie: Logius

Inhoud en werking van Samenwerkende Catalogi
Samenwerkende Catalogi koppelt de productcatalogi van verschillende overheidsorganisaties. De koppeling van productcatalogi door Samenwerkende Catalogi maakt het ‘no wrong door’- principe mogelijk. Dit bekent dat over organisatiegrenzen heen gezocht kan worden naar producten en diensten. Het is de standaard (specificatie) voor het publiceren en uitwisselen van metadata over producten en diensten binnen de overheid, zoals bijvoorbeeld het aanvragen van een vergunning of het aanvragen van een reisdocument. Deze productinformatie is voor iedereen doorzoekbaar door middel van een API. De eindgebruiker gebruikt de portalen Overheid.nl en Ondernemersplein.nl. Zowel Overheid.nl als het Digitaal Ondernemersplein haalt de productinformatie uit de SC API.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	De online validatieservice controleert of Samenwerkende Catalogi XML-bestanden op de juiste wijze zijn opgemaakt en de metadata voldoen aan de technische specificaties van Samenwerkende Catalogi en de Overheid.nl Web Metadata Standaard OWMS. De validator is benaderbaar via een subdomein van Logius (scvalidator.logius.nl). De validator voldoet aan deze standaard.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	nee	De validator van Samenwerkende Catalogi voldoet niet meer aan HTTPS. Gepland is om dit mee te nemen in de migratie naar een andere provider. De verwachting is dat dit in 2020 gaat plaatsvinden.
IPv4 en IPv6 (Adressering van ICT-systemen binnen een netwerk)	Ja	Zowel de informatieve pagina’s op logius.nl als de validator zelf zijn voorzien van IPv4 en IPv6 adressen. Dit na een migratie van beide omgevingen.
SPF (Preventie van mailspoofing/phishing)	Ja	De validator van Samenwerkende Catalogi voldoet aan deze standaard.

TLS (Beveiligde, versleutelde verbindingen)	Nee	De validator van Samenwerkende Catalogi voldoet niet meer aan deze standaard. Gepland is om dit mee te nemen in de migratie naar een andere provider. De verwachting is dat dit in 2020 gaat plaatsvinden.
		Document en (web/app)content
Open API Specification (Beschrijven van REST API's)	Ja	Samenwerkende catalogi voldoet aan deze standaard.
OWMS (Metadata overheidsinformatie)	Ja	Samenwerkende catalogi is volledig gebaseerd op OWMS.

Ten opzichte van 2019 voldoet de voorziening aan DMARC en SPF. De statussen van deze standaarden gaan van gepland naar ja. De status van HTTPS en HSTS en TLS gaat van gepland naar nee.

Concluderend moeten voor samenwerkende catalogi nog de volgende standaarden (volledig) worden geïmplementeerd: HTTPS/HSTS, TLS.

3.6 RDW.nl

Beheerorganisatie: RDW (Rijksdienst Wegverkeer)

Werking en inhoud van RDW.nl
De website RDW.nl biedt informatie over de dienst wegverkeer (RDW). De RDW beheert onder andere het kentekenregister. De website kent specifieke functies voor particulier- en zakelijk gebruik. Particulieren kunnen via RDW.nl bijvoorbeeld digitaal een keuringsafspraak voor hun auto maken of een kentekenbewijs voor de brommer of scooter aanvragen. Bedrijven kunnen via RDW.nl bijvoorbeeld kentekenbewijzen voor bedrijfsvoertuigen aanvragen en ontheffingen voor transporteurs regelen. Voor digitale diensten en producten verwijst RDW.nl naar onderliggende domeinen. Het is daarnaast voor particulieren mogelijk om via DigiD in te loggen op RDW.nl om eigen gegevens te raadplegen.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	De BRV (basisregistratie voertuigen) voldoet aan DKIM.
DMARC (Anti-phishing)	Gepland	De BRV voldoet aan DMARC. Rdw.nl voldoet niet aan de standaard, zie: https://internet.nl/mail/rdw.nl/. De RDW is in 2017 gestart met een nieuwe leverancier. Doordat de implementatie van de digitale werkomgeving langer heeft geduurd dan beoogd, is dit tot op heden nog niet uitgevoerd. Augustus 2019 is RDW gestart om privacy en security verder te gaan verbeteren. Medio 2020 is deze verbetering doorgevoerd.
DNSSEC (Beveiligde domeinnamen)	Deels	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.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Gepland	Implementatie zou medio 2018 gerealiseerd worden. Rdw.nl voldoet niet aan de standaard, zie: https://internet.nl/site/rdw.nl/. De RDW is in 2017 gestart met een nieuwe leverancier. Doordat de implementatie van de digitale werkomgeving langer heeft geduurd dan beoogd, is dit tot op heden nog niet uitgevoerd. Augustus 2019 is RDW gestart om privacy en security verder te gaan verbeteren. Medio 2020 is deze verbetering doorgevoerd. De diensten op (voertuig)gegevens, die als microservices in de Azure cloud draaien, voldoen wel aan HTTPS/HSTS.
IPv4 en IPv6 (Internetnummers)	Nee	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.
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	Deze zullen uiterlijk Q3 2020 geconfigureerd zijn overeenkomstig de overheidsstandaarden (zie: https://internet.nl/mail/rdw.nl/).
TLS (Beveiligde, versleutelde verbindingen)	Nee	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
CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)	Nee	Inmiddels relevant doordat de RDW bezig is met de ontwikkeling van een centraal Document Management Systeem voor de geautomatiseerde processen. Dit systeem wordt ontsloten via CMIS. In de loop van 2019/2020 zal het document management systeem voor de primaire processen geschikt worden gemaakt voor aansluiting door geautomatiseerde processen. CMIS zal als standaard voor de ontsluiting worden gehanteerd.
Open API Specification (Beschrijven van REST API's)	Ja	De BRV voldoet aan Open API Specification.

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 begrippenwoordenboeken)	Ja	De BRV voldoet aan SKOS.
		E-facturatie en administratie
NLCIUS (Elektronisch factureren)	Nee	De huidige SAP implementatie voldoet hier niet aan. Er zal in de komende periode een aanbesteding plaatsvinden voor het Finance domein waarin deze standaard zal worden meegenomen.
Ades Baseline Profiles	Nee	De RDW voldoet niet aan deze standaard. De RDW heeft een aantal PDF-documenten die op een andere manier worden ondertekend. Er liggen op dit moment geen plannen om deze Ades compatible te maken.

Dit jaar worden alleen de set voorzieningen onderzocht die direct raken aan de communicatie en gegevensuitwisseling met burgers en bedrijven. RDW.nl staat “nieuw” op de lijst. Voor de monitor open standaarden 2021 wordt de set voorzieningen onderzocht die vooral gericht is op de communicatie en gegevensuitwisseling tussen overheden dan wel op de onderliggende infrastructuur. Hieronder valt de BRV. Die wordt volgend jaar separaat onderzocht. Zoals is te zien zijn deze voorzieningen met elkaar verweven.

Concluderend moeten voor RDW.nl nog de volgende standaarden (volledig) worden geïmplementeerd: DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, STARTTLS en DANE, TLS, CMIS, NLCIUS, Ades Baseline Profiles.

3.7 Rijksoverheid.nl

Beheerorganisatie webdomein: Ministerie van AZ (DPC)
Beheerorganisatie maildomein: Onbekend

Werking en inhoud van rijksoverheid.nl
De website Rijksoverheid.nl is de publiekswebsite met informatie van en over alle ministeries. De website wordt verzorgd door de Dienst Publiek en Communicatie (DPC). DPC is een baten-lastendienst van het ministerie van AZ en biedt shared servicediensten aan de rijksoverheid op het gebied van Communicatie. Het e-mail domein @rijksoverheid.nl is in technisch beheer bij SSC-ICT van het ministerie van BZK. Het is niet helder wie zich verantwoordelijk voelt voor het emaildomein. Van het webdomein is AZ eigenaar en beheerder. Voor het maildomein is SSC-ICT de technisch beheerder. Kantekening hierbij is dat AZ/DPC de beheerder is voor de DNS. Vanuit het Bureau Forum Standaardisatie zijn gesprekken gevoerd met betrokken partijen. Daarbij is aangegeven dat er gezocht wordt naar een verantwoordelijke voor het emaildomein.

3.7.1 Maildomein

Standaard	Status	Toelichting beheerder
		Internet en beveiliging

DKIM (Preventie van mailspoofing/ phishing)	Ja	DKIM is geïmplementeerd (zie: https://internet.nl/mail/rijksoverheid.nl/).
DMARC (Anti-phishing)	Ja	DMARC policy staat op reject, de meest strikte policy (zie: https://internet.nl/mail/rijksoverheid.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	Rijksoverheid.nl is ondertekend met DNSSEC (zie: https://internet.nl/mail/www.rijksoverheid.nl/). DPC biedt DNSSEC ook aan al haar klanten die domeinen via haar registrar-functie afnemen (zie: https://internet.nl/mail/rijksoverheid.nl/).
IPv4 en IPV6 (Internetnummers)	Gepland	IPv6 is niet voor (alle) mailservers geïmplementeerd (zie: https://internet.nl/mail/rijksoverheid.nl/249091/#). Het technisch beheer van een aantal maildomeinen wordt uitgevoerd door SSC-ICT. De internet facing kant van de DMZ gaat IPv6 in 2020/2021.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De leveranciers hebben een NEN 27001/2 implementatie waarin de beveiliging van rijksoverheid.nl meegaat. DPC zelf valt onder de VIR/BIO-implementatie van het moederdepartement AZ. SSC-ICT werkt via deze standaard en wordt hier ook op geaudit. De laatste audits hebben plaatsgevonden in 2019 en 2020.
SPF (Preventie van mailspoofing/phishing)	Ja	Het e-maildomein @rijksoverheid.nl is integraal van SPF voorzien (zie: https://internet.nl/mail/rijksoverheid.nl/). Deze wordt door SSC-ICT beheerd in samenwerking met AZ. Technisch gezien is SSC-ICT het aanspreekpunt.
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Ja	Verzendende mailservers die STARTTLS ondersteunen, kunnen met ontvangende mailserver(s) een beveiligde verbinding opzetten. Rijksoverheid.nl voldoet aan DANE (zie: https://internet.nl/mail/rijksoverheid.nl/). Deze wordt door SSC-ICT beheerd in samenwerking met AZ. Technisch gezien is SSC-ICT het aanspreekpunt.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De nieuwe versies en oude worden ondersteund. Best practice is de oude TLS versies aan laten staan op de mailservers i.v.m. interoperabiliteit. Het uitzetten kan tot gevolg hebben dat er onvercijferd wordt gecommuniceerd.

3.7.2 Webdomein

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DNSSEC (Beveiligde domeinnamen)	Ja	Rijksoverheid.nl is ondertekend met DNSSEC (zie: https://internet.nl/site/www.rijksoverheid.nl/). DPC biedt DNSSEC ook aan al haar klanten die domeinen via haar registrar-functie afnemen.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening voldoet aan deze standaard (zie: https://internet.nl/site/www.rijksoverheid.nl/).
IPv4 en IPV6 (Internetnummers)	Ja	De website rijksoverheid.nl ondersteunt zowel IPv6 als IPv4 (zie: https://internet.nl/site/www.rijksoverheid.nl/).

NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De leveranciers hebben een NEN 27001/2 implementatie waarin de beveiliging van rijksoverheid.nl meegaat. DPC zelf valt onder de VIR/BIO-implementatie van het moederdepartement AZ.
RPKI (Beveiligen van de routing infrastructuur)	Nee	Het publiceren van ROA's doet Rijksoverheid.nl al langer. Het valideren en het 'droppen' van invalide routes doet Rijksoverheid.nl niet. We denken na over mogelijke toepassing.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Het webdomein van rijksoverheid.nl voldoet aan TLS (zie: https://internet.nl/site/www.rijksoverheid.nl/).
		Document en (web/app)content
ODF 1.2 (Documentbewerkingen)	Ja	Het CMS van het Platform Rijksoverheid Online accepteert slechts ODF (open standaard) formaten. Er zijn wel 'legacy'-bestanden in alleen .doc of .xls formaat.
OWMS (Metadata overheidsinformatie)	Ja	De beleidskeuzes (contentmodellen) zijn in te zien in het Informatie Publicatie Model (IPM) bij het OWMS (zie: http://standaarden.overheid.nl/rijksoverheid).
PDF 1.7 / PDF A/1 en PDF A/2 (Documentpublicatie/ archivering)	Deels	De centrale redactie van Rijksoverheid.nl stuurt op het aanbieden van de juiste typen PDF's. De centrale redactie heeft beperkt zicht op soort en type PDF's die door decentrale redacteuren van de ministeries zelfstandig op rijksoverheid.nl worden geplaatst. Er zijn veel verschillende organisaties die PDF's op rijksoverheid.nl kunnen plaatsen. Het is daardoor simpelweg niet helemaal onder controle welke soorten PDF worden toegepast. Sinds eind 2019 gebruikt Rijksoverheid.nl een nieuwe module voor invoer van een deel van de documenten. PDF-documenten uit deze module voldoen aan alle richtlijnen. Naar aanleiding van de verplichte toegankelijkheid van overheidswebsites gaat in 2020 de centrale redactie in gesprek met de ministeries over het voldoen aan de toegankelijkheidseisen bij alle documenten die externe redacties op Rijksoverheid.nl plaatsen of laten plaatsen.
		Juridische identificatie en verwijzing
BWB (Wet- en regelgeving)	Ja	Binnen de website wordt verwezen naar wetgeving conform de BWB standaard. BWB wordt toegepast.

Ten opzichte van 2019 is voor het maildomein DMARC geïmplementeerd. De status gaat van nee naar ja. Voor het maildomein geldt dat rijksoverheid.nl niet voldoet aan IPv6, de planning van 2019 is niet gehaald en doorgeschoven naar eind 2020. De status gaat naar gepland. Het webdomein voldoet net als vorig jaar aan IPv4 en IPv6. Nieuw op de lijst en relevant voor het webdomein is RPKI. De voorziening voldoet niet aan deze standaard.

Concluderend moeten voor de voorziening rijksoverheid.nl nog de volgende standaarden (volledig) worden geïmplementeerd voor het maildomein: IPv4 en IPV6.

Concluderend moeten voor de voorziening rijksoverheid.nl nog de volgende standaarden (volledig) worden geïmplementeerd voor het webdomein: RPKI, PDF 1.7 / PDF A/1 en PDF A/2 .

3.8 WOZ Waardeloket

Beheerorganisatie: Kadaster

Werking en inhoud van WOZ Waardeloket
Het WOZ Waardeloket biedt de mogelijkheid de WOZ-waarde van woningen te raadplegen. Het WOZ Waardeloket is bedoeld voor het individueel raadplegen van afzonderlijke woningen. De getoonde WOZ-waarden zijn formeel door de desbetreffende gemeente vastgestelde WOZ-waarden. De gemeente is dan ook verantwoordelijk voor deze WOZ-waarde. De getoonde objectkenmerken, zoals bouwjaar en gebruiksoppervlakte, zijn afkomstig uit de Basisregistraties adressen en gebouwen. Ook voor deze gegevens is de gemeente verantwoordelijk.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	Centraal geregeld: Het Kadaster voldoet aan DKIM. Er is geen mailserver voor het domein wozwaardeloket.nl en DKIM records worden op dit domein niet ondersteund (zie: https://internet.nl/mail/wozwaardeloket.nl).
DMARC (Anti-phishing)	Nee	Centraal geregeld: Deze standaard is geïmplementeerd. Er is geen mail server voor het domein wozwaardeloket.nl en er is geen DMARC policy quarantine of reject actief (zie: https://internet.nl/mail/wozwaardeloket.nl).
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC wordt ondersteund (zie: https://internet.nl/site/www.wozwaardeloket.nl).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	HTTPS en HSTS zijn geïmplementeerd (zie: https://internet.nl/site/www.wozwaardeloket.nl).
IPv4 en IPv6 (Internetnummers)	Ja	Exact dezelfde website is zowel over IPv4 als IPv6 bereikbaar (zie: https://internet.nl/site/www.wozwaardeloket.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 BIR gebaseerd. In het jaarverslag is een in control statement opgenomen.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd (zie: https://internet.nl/mail/wozwaardeloket.nl).
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Nee	STARTTLS is beschikbaar. Er is geen mailserver voor het domein wozwaardeloket.nl en DANE is daarom niet actief. Er is geen Null MX record (RFC 7505) ingesteld voor dit domein (zie: https://internet.nl/mail/wozwaardeloket.nl).
TLS (Beveiligde, versleutelde verbindingen)	Ja	Minimaal TLS 1.2 (zie: https://internet.nl/site/www.wozwaardeloket.nl).
		Document en (web/app)content

PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/ archivering)	Nee	Het WOZ-waardeloket biedt de mogelijkheid een schermafdruk van de gegevens in PDF-formaat te downloaden. Dit is momenteel geen PDF 1.7, PDF A/1 of PDF A/2.

Het WOZ Waardeloket is een dit jaar nieuw onderzochte voorziening. Digikoppeling is niet van toepassing, doordat de WOZ voorziening en het WOZ Waardeloket beide in uitvoering zijn bij het Kadaster. WOZ is een portal op voorzieningen waar Geo-standaarden worden toegepast (bijv. PDOK).

Concluderend moeten voor het WOZ Waardeloket nog de volgende standaarden (volledig) worden geïmplementeerd: DMARC, STARTTLS en DANE, PDF 1.7, PDF A/1, PDF A/2.

4. Gegevens en registreren

4.1 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. Bij de toetsing van NHR is dit jaar naar de website kvk.nl en de onderliggende systemen en koppelingen gekeken.

Standaard	Status	Toelichting beheerder
		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	Kvk,nl is DNSSEC beveiligd. De Microsoft Exchange 365 cloud omgeving niet. Volgens planning van Microsoft wordt DNSSEC eind 2021 ondersteund.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening gebruikt zowel HTTPS als HSTS. Alleen voor kvk.nl werkt HSTS niet, dit is in 2019 hersteld. Was nog niet gebeurd omdat kvk.nl alleen redirect naar www.kvk.nl en deze werkt wel onder HSTS. Er was en is dus geen security risico.
IPv4 en IPv6 (Internetnummers)	Nee	Netwerkprovider KPN ondersteunt geen IPv6. KvK kan in principe IPv6 verkeer aan. Intern wordt IPv4 gebruikt.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De KvK is sinds 2016 ISO 27001 gecertificeerd en hanteert ISO27002.
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/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/DANE eind 2021 ondersteund.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De mailserver kvk-nl.mail.protection.outlook.com ondersteunt nog TLS 1.1. Dit is een externe mailserver. De leverancier (Microsoft) dient de TLS versies uit te faseren. De KVK zal dit opnemen met de leverancier. Op deze mailserver wordt ook TLS 1.2 ondersteunt. 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 niet zeker is of dit in 2020 kan worden afgerond.
		Document en (web/app)content
Ades Baseline Profiles (Digitaal ondertekenen van documenten)	Ja	De NHR voldoet aan de Ades Baseline Profiles standaard.
CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)	Gepland	De bij de KvK in gebruik zijnde contentmanagement systemen, Sharepoint en Documentum zijn compliant aan de CMIS standaard, maar het webcontent platform Tridion (nog) niet vanwege een verouderde versie van de software. De KVK is bezig om Tridion uit te faseren door een nieuw CMS systeem aan te besteden. CMIS is hierin een knock out criterium. Aanbesteding en implementatie vindt in 2020/21 plaats. Koppelingen met Sharepoint worden CMIS compliant uitgevoerd.
Open API Specification (Beschrijven van REST API's)	Deels	KvK gebruikt deze specificatie actief. Reeds operationele API's worden geleidelijk aangepast.
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.
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. Eerste evaluatie van SKOS voor NHR heeft plaatsgevonden. De KVK wil dit in 2020/2021 verwezenlijken.
		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 overheids-gegevens)	Ja	Ongeveer 10% van het verkeer van het NHR gaat naar medeoverheden. Die uitwisselingen vinden allemaal plaats via Digikoppeling en StUF.
		E-facturatie en administratie
NLCIUS (Elektronisch factureren)	Nee	KvK heeft haar financiële systeem in 2018 naar AFAS gemigreerd. UBL 2.1 en SMeF 2.0 worden wel ondersteund, maar de modelfactuur nog niet.

Ten opzichte van 2019 zijn de volgende standaarden van ‘nee’ en/of ‘deels’ naar ‘gepland’ gegaan: DNSSEC, STARTTLS/DANE, CMIS en SKOS. Daarnaast voldoet de voorziening niet langer meer aan de standaard IPv4 en IPv6. Voor de Open API Specification en NLCIUS zijn er geen veranderingen opgetreden.

Concluderend moeten voor het NHR nog de volgende standaarden (volledig) worden geïmplementeerd: DNSSEC, IPv4 en IPv6, STARTTLS/DANE, CMIS, Open API Specification, SKOS en NLCIUS.

4.2 PDOK

Beheer organisatie: Kadaster

Werking en inhoud van PDOK
Bij PDOK vind je open datasets van de overheid met actuele geo-informatie. Deze datasets zijn benaderbaar via geo webservices, RESTful API's en beschikbaar als downloads en linked data. PDOK is tot stand gekomen door een samenwerking tussen het Kadaster, de ministeries van Infrastructuur en Waterstaat, Binnenlandse Zaken en Koninkrijksrelaties en Economische Zaken en Klimaat, Rijkswaterstaat en Geonovum. PDOK is een open initiatief. Elke overheidsorganisatie die zijn geodata voor hergebruik beschikbaar wil stellen, kan zich tot PDOK wenden. Het dataportaal PDOK wordt gehost door het Kadaster.

Standaard	Status	Toelichting
		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.pdok.nl ondersteunt DNSSEC (zie: https://internet.nl/domain/www.pdok.nl/).

HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Gepland	Er is een probleem met HSTS-policy via pdok.nl (zie: https://internet.nl/site/pdok.nl). Melding gemaakt om opgelost te worden. Verwachting is dat dit in juli 2020 opgelost wordt.
IPv4 en IPv6 (Internetnummers)	Ja	Zowel IPv4 als IPv6 worden ondersteund door het Kadaster (zie: https://internet.nl/domain/www.pdok.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 BIR gebaseerd en is deels door standaarden op basis van de BIO vervangen. In het jaarverslag is een in control statement opgenomen.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd (zie: https://internet.nl/mail/pdok.nl/).
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	STARTTLS en DANE zijn geïmplementeerd (zie: https://internet.nl/mail/pdok.nl/).
TLS (Beveiligde, versleutelde verbindingen)	Ja	Deze standaard wordt volledig door het Kadaster ondersteund (zie: https://internet.nl/domain/www.pdok.nl/). PDOK volgt de richtlijnen van het NCSC voor TLS. Hieruit blijkt dat mogelijke problemen met cipher-volgorde wat betreft vertrouwelijkheid geen risico vormen, omdat de data openbaar is volgens de BIV classificatie.
Document en (web/app)content		
Open API Specification (Beschrijven van REST API's)	Ja	Deze standaard is geïmplementeerd en wordt toegepast.
OWMS (Metadata overheidsinformatie)	Ja	PDOK ontsluit metadata via het NGR (www.nationaalgeoregister.nl), deze gaat in ieder geval uit van ISO en INSPIRE (en NL profielen). Data.overheid.nl harvest het NGR. v.w.b. OWMS: https://data.overheid.nl/nationaal-georegister.
Stelselstandaarden		
Geo-standaarden	Ja	PDOK maakt gebruik van OGC en INSPIRE standaarden voor haar webservices. Webservices kennen verschillende formaten qua uitlevering. Downloads worden via formaten GeoPackages en GML aangeleverd en uitgeserveerd.
StUF	Ja	Voor het uitserveren van de BGT.

PDOK.nl is een nieuw onderzochte voorziening die vanaf 2020 voor het eerst wordt getest in de Monitor. Geconcludeerd kan worden dat de voorziening nog niet (volledig) voldoet aan HTTPS/HSTS.

5. Dienstverlening en verbinden

5.1 TenderNed

Beheerorganisatie: PIANOo/DICTU

Werking en inhoud van TenderNed
TenderNed is het online marktplein voor aanbestedingen van de Nederlandse overheid. Het is een volledig digitaal aanbestedingssysteem voor alle aanbestedende diensten en ondernemingen in Nederland.

TenderNed is onderdeel van PIANOo, het Expertisecentrum Aanbesteden van het ministerie van Economische Zaken. Het beheer van de technische infrastructuur is ondergebracht bij DICTU.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	E-mails verzonden vanuit TenderNed zijn beveiligd met DKIM (zie: https://internet.nl/mail/tenderned.nl/).
DMARC (Anti-phishing)	Ja	Dienstverlener DICTU heeft DMARC aangezet.
DNSSEC (Beveiligde domeinnamen)	Ja	Het domein is gesigned met DNSSEC (zie: https://internet.nl/site/www.tenderned.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Nee	De client-server communicatie van TenderNed is beveiligd met HTTPS en niet met HSTS (zie: https://internet.nl/site/www.tenderned.nl/).
IPv4 en IPV6 (Internetnummers)	Nee	TenderNed.nl is zowel in 2018 en 2019 als in 2020 niet voorbereid op IPv6 (zie: https://internet.nl/site/www.tenderned.nl/). TenderNed is afhankelijk van de hostingpartij. Wanneer deze een transitie doormaakt naar IPv6 zal TenderNed daarin mee gaan. Er is geen planning om dat wel te doen op dit moment.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	TenderNed is ISO27001/2 gecertificeerd. Dit wordt jaarlijks geaudit.
SAML (Inloggegevens)	Ja	Per 1 juli 2014 is het mogelijk voor gebruikers om, naast de huidige registreer- en inlogmogelijkheden, gebruik te maken van inloggen via eHerkenning.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is inmiddels aangezet door de technisch dienstverlener DICTU (zie: https://internet.nl/mail/tenderned.nl/140321/#mailauth).
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	STARTTLS en DANE worden ondersteund.

TLS (Beveiligde, versleutelde verbindingen)	Ja	TenderNed past TLS 1.2 toe (zie: https://internet.nl/site/www.tenderned.nl/). Voor een aantal koppelingen wordt nog TLS 1.0 gebruikt voor compatibiliteit.
		Document en (web/app)content
Open API Specification (Beschrijven van REST API's)	Nee	De publieke API's worden beschreven door middel van Swagger. Swagger kan je zien als OAS versie 2.0. Swagger als API Specificatie bestaat niet meer en is opgegaan in OAS. TenderNed voldoet daarmee niet aan OAS 3.0. Deze versie is belangrijk omdat deze samenhang aanbrengt in de verschillende manieren om API specificaties op te stellen.
PDF 1.7, PDF/A-1, PDF/A-2 (Documentpublicatie/ archivering)	Ja	Geautomatiseerd gecreëerde PDF's (bij de aankondigingen) zijn gemaakt in versie 1.7.

Ten opzichte van 2019 is DMARC geïmplementeerd. De status gaat van nee naar ja.

Concluderend moeten voor TenderNed nog de volgende standaarden (volledig) worden geïmplementeerd: HTTPS/ HSTS, IPv4 en IPv6, Open API Specification.

5.2 DigiInkoop

Beheerorganisatie: Logius

Werking en inhoud van DigiInkoop
DigiInkoop is een rijksbreed geautomatiseerd inkoopsysteem dat het inkoopproces vereenvoudigt. DigiInkoop is er voor de inkoop van alle producten en diensten, van kantoorartikelen tot inhuur van personeel. Daarnaast biedt de voorziening DigiInkoop een leveranciersportaal voor leveranciers van de Rijksoverheid. Hiermee kunnen deze leveranciers offertes, orders en facturatie afhandelen, met één inlog voor de hele Rijksoverheid.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	De standaard DKIM is geïmplementeerd. (zie: https://internet.nl/mail/digiinkoop.nl/). Digiinkoop.nl ontvangt geen mail. Het DNS mx record mta.dc.ordina.nl is ook niet meer van toepassing. Dus alle verwijzingen hiernaar (die internet.nl gebruikt) kunnen buiten beschouwing worden gelaten. De DNS record zal verwijderd worden. Vanuit noreply@digiinkoop.nl wordt wel mail verstuurd. SPF/DKIM/DMARC zijn dus wel van toepassing.
DMARC (Anti-phishing)	Nee	De standaard is geïmplementeerd, maar de policy is onvoldoende strikt. Onderzoek loopt naar striktere policy implementatie, de verwachting is Q3 2020 hieraan te kunnen voldoen (zie: https://internet.nl/mail/digiinkoop.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	DigiInkoop voldoet aan DNSSEC (zie: https://internet.nl/mail/digiinkoop.nl/). DigiInkoop.nl ontvangt geen mail. Het DNS mx record mta.dc.ordina.nl is ook niet meer

		van toepassing. Dus alle verwijzingen hiernaar (die internet.nl gebruikt) kunnen buiten beschouwing worden gelaten. De DNS record zal verwijderd worden.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening voldoet aan HTTPS/HSTS. Opvallend is dat internet.nl dat niet goed vast kan stellen (zie https://internet.nl/site/digiinkoop.nl/). Hier wordt nog verder onderzoek naar gedaan.
IPv4 en IPV6 (Internet-nummers)	Gepland	Er loopt een migratie naar een cloudplatform. Verwachting is dat hier IPv6 beschikbaar komt Q4 2020 (zie: https://internet.nl/site/digiinkoop.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	DigiInkoop voldoet aan de BIR. Er is een in control statement afgegeven. Leveranciers voldoen aan ISO 27001.
SPF (Preventie van mailspoofing/phishing)	Ja	DigiInkoop voldoet aan deze standaard (zie: https://internet.nl/mail/digiinkoop.nl/).
TLS (Beveiligde, versleutelde verbindingen)	Ja	DigiInkoop is TLS 1.2 compliant (zie: https://internet.nl/mail/digiinkoop.nl/). mta.dc.ordina.nl is uitgefaseerd.
		Document en (web/app)content
PDF/A en PDF 1.7 (Documentpublicatie/archivering)	Ja	De DigiInkoop applicatie produceert inkooporders en facturen in PDF-formaat. Documenten die op logius.nl beschikbaar worden gesteld zijn in PDF/A-formaat (dit zijn de documenten over de berichtenverkeerstandaarden waar DigiInkoop gebruik van maakt: https://www.logius.nl/ondersteuning/gegevensuitwisseling/ubl-ohnl en https://www.logius.nl/ondersteuning/gegevensuitwisseling/setu-hr-xml-ohnl).
		E-facturatie en administratie
NLCIUS (Elektronisch factureren)	Ja	Per 19 april 2019 is de NLCIUS verplicht voor overheden, volgens Europese richtlijn 2014/55/EU. De SMEF 2.0 standaard wordt opgevolgd door de NLCIUS. Implementatie is conform planning in Q2 2019 gerealiseerd.
SETU (Informatie flexibele arbeidskrachten)	Ja	DigiInkoop ondersteunt de uitwisseling van SETU-hr-XML berichten.

Ten opzichte van 2019 voldoet de voorziening niet meer aan DMARC. Verder is de status van de IPv4 en IPv6 standaarden van nee naar gepland gegaan. De voorziening voldoet aan NLCIUS.

Concluderend, moet DigiInkoop nog de volgende standaarden (volledig) implementeren: DMARC, IPv4 en IPv6.

Bijlage A Geïnterviewde personen

Naam voorziening	Contactpersoon
Berichtenbox voor bedrijven	Erwin Sakkers
DigiInkoop	Güldeniz Özdemir Isik
DigiD	Güldeniz Özdemir Isik
DigiD Machtigen	Güldeniz Özdemir Isik
Stelsel elektronische toegangsdiensten	Güldeniz Özdemir Isik
MijnOverheid	Güldeniz Özdemir Isik
NHR	Rob Spoelstra
Ondernemersplein	Elie Mokheiber, Rienco Ligtenbarg, Gaico Aertssen
Overheid.nl	Erna Wisselaar
PDOK	Jeroen Hogeboom
PKI Overheid	Güldeniz Özdemir Isik
Rijksoverheid.nl	Gerrit Berkouwer, Cees Vaes
RDW.nl	Gert Stel,
Samenwerkende Catalogi	Güldeniz Özdemir Isik
Tenderned	Rudi van Eijk
WOZ Waardeloket	Rijk van Haaften

Bijlage B Lijst onderzochte verplichte open standaarden

Standaard
Ades Baseline Profiles
Aquo-standaard
BWB
CMIS
COINS
Digikoppeling
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 LOM
NLCIUS
NLCS
ODF
OpenAPI Specification
OWMS
PDF (NEN-ISO)
RPKI
SAML
SETU
SIKB0101
SIKB0102
SKOS
SPF
STARTTLS en DANE
STIX en TAXII
StUF
TLS
VISI
WDO Datamodel
WPA2 Enterprise
XBRL