Rapport

Monitor Open standaarden 2019

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

Van Jaap Korpel

Versie Versie 1.11_DT

Datum 1-12-2021

Revisietabel

Datum	Versie	Auteur	Opmerking
14-11-2019	0.85	Jaap Korpel	Eerste versie in DigiToegankelijk format
19-11-2019	0.99	Jaap Korpel	Definitieve cijfers en teksten toegevoegd
27-11-2019	1.0	Jaap Korpel	Laatste correcties, en twee IV-metingen en rapport PBLQ als bijlagen ingevoegd
19-2-2020	1.1	Jaap Korpel	Enkele nagekomen correcties, en plaat met standaarden naar lagen (bijlage).
27-3-2020	1.11	Jaap Korpel	Laatste correcties, en bijlage Rijksinstructie aangevuld met Toelichting.
1-12-2021	**1.11_DT**	**Jaap Korpel**	**Document meer Digitoegankelijk gemaakt zonder inhoudelijke wijzigingen in de tekst.**

Inhoudsopgave

1. Managementsamenvatting

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* en de verplichting geldt ook voor mede-overheden (gemeenten, provincies en waterschappen).

De kernvraag van de Monitor Open standaarden is: passen overheden de verplichte open standaarden daadwerkelijk toe, 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 de afgelopen jaren geleidelijk toegenomen. Maar het einddoel dat alle overheden de relevante open standaarden toepassen is ook in 2019 nog niet bereikt, en de ontwikkeling lijkt te stagneren.
- Bij 89% 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 als vorig jaar (85%). Van de 736 keer dat een open standaard voor een aanbesteding relevant was werd daar in 50 % van de gevallen om gevraagd.
- Voor de meeste van de 36 onderzochte overheidsbrede voorzieningen is inmiddels een behoorlijk niveau van toepassing bereikt: van alle 417 gevallen waarin een standaard voor een voorziening relevant is wordt daar in 84 % van de gevallen aan voldaan of deels voldaan of zijn er concrete plannen om daaraan te voldoen. Van volledige compliancy is nog geen sprake, en de ontwikkeling lijkt enigszins te stagneren.

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

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. Voor de Nederlandse overheid zijn open standaarden de norm: voor de gehele (semi-)publieke sector geldt sinds 2009 een 'pas toe of leg uit'-regime.

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[1]. 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 (zomer 2019 waren dit er 41) is het 'pas toe of leg uit'-regime van toepassing.

Meer informatie over deze standaarden is te vinden in Bijlage B1. Meer informatie over de beleidscontext en het juridisch kader staat in hoofdstuk 2 en Bijlage B3.

[1] 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 al gangbaar zijn of die pril zijn en veelbelovend. Dit onderzoek beperkt zich tot de standaarden op de 'pas toe of leg uit'-lijst.

1.2. Over de Monitor Open standaarden 2019 (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 door ministeries, uitvoeringsorganisaties, gemeenten, provincies en waterschappen toegepast?

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

- onderzoek van feitelijke aanbestedingen in de periode juli 2018 t/m juni 2019,
- onderzoek van de toepassing van open standaarden bij overheidsbrede voorzieningen (situatie in de zomer van 2019),
- onderzoek naar gebruiksgegevens van een aantal open standaarden (zomer 2019).

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 ICT-aanbestedingen van € 50.000 of meer de relevante open standaarden van de lijst toepassen ('pas toe'), of verantwoording afleggen in hun jaarverslag ('leg uit'). Doen zij dat ook in de praktijk?

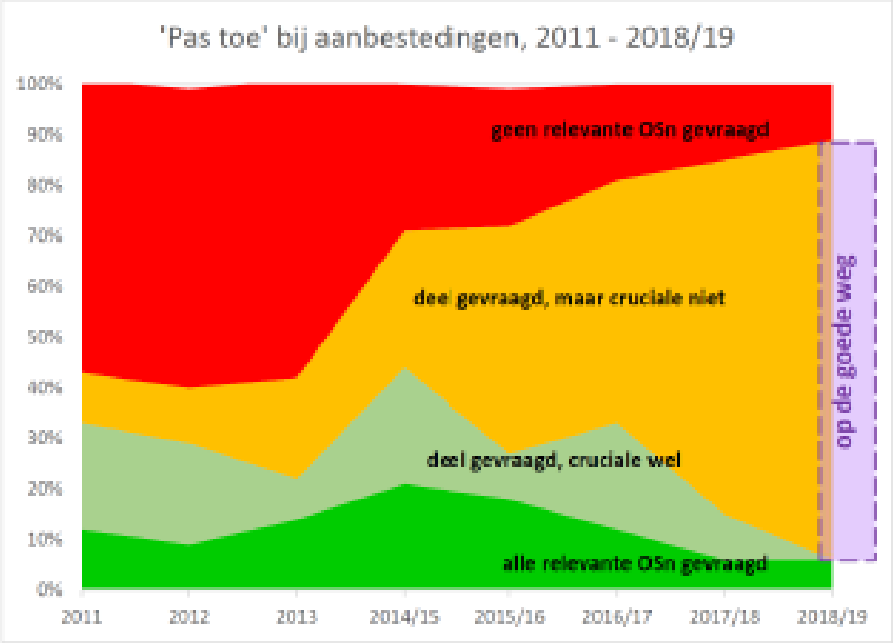
'Pas toe' bij feitelijke aanbestedingen
Voor de monitor is, net als vorig jaar, een groot aantal aanbestedingen onderzocht. Dit keer zijn 35 aanbestedingen van de rijksoverheid en uitvoeringsorganisaties en 37 aanbestedingen van mede-overheden onderzocht, in totaal 72 aanbestedingen (uit het 3e en 4e kwartaal van 2018 en 1e en 2e kwartaal van 2019). De resultaten worden beschreven in hoofdstuk 3.

In 6% van de aanbestedingen is gevraagd om alle relevante open standaarden, eenzelfde score als vorig jaar. Het percentage aanbestedingen waarbij om een deel van de open standaarden is gevraagd – de grote middencategorie – is licht toegenomen, van 79% vorig jaar naar 83% 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 enigszins teruggelopen van 15% naar 11%. Daarbij moet wel worden opgemerkt dat in tegenstelling tot vorig jaar nu wel een aantal aanbestedingen (5, 7% van het totaal) strijdig is met het open standaardenbeleid (vorig jaar geen enkele).

Rijk en uitvoeringsorganisaties deden het in 2018/2019 beter dan de mede-overheden: bij 9% van de aanbestedingen werd om alle relevante standaarden gevraagd (mede-overheden: 3%) en bij 89% om een deel van de relevante standaarden (mede-overheden: 78%). Bij 3% van de Rijks-aanbestedingen werd om geen enkele standaard gevraagd of was sprake van strijdigheid met het open standaardenbeleid, de mede-overheden deden dat slechter: 19%.

Het overall beeld voor aanbestedingen is weliswaar redelijk positief, maar de ontwikkeling lijkt een beetje in het midden te blijven steken: de meeste aanbestedingen vallen in de middengroep (niet heel goed, niet slecht) en zelfs in het middengedeelte van die

middengroep (heeft om 34 tot 66 % van de relevante standaarden gevraagd), en van alle gevallen waarin een open standaard voor een aanbesteding relevant was werd daar in 50 % van de gevallen om gevraagd (en om de andere 50 % dus niet).



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

goed nieuws	Bij 4 aanbestedingen (6%) is om alle relevante standaarden gevraagd. Hierbij gaat het om aanbestedingen van het Ministerie van BZK, Zorginstituut Nederland en Stichting NWO-I en de provincie Groningen. Ook vorig jaar was deze score 6%.
goed nieuws	Daarnaast werd bij 60 aanbestedingen (83%) om een deel van de relevante open standaarden gevraagd. Dat is procentueel iets hoger als vorig jaar (toen: 79%).
minder goed	Bij 8 aanbestedingen (11%, vorig jaar 15%) is om geen enkele relevante standaard gevraagd of is sprake van strijdigheid met het open standaardenbeleid. Dit jaar waren 5 aanbestedingen strijdig met het open standaardenbeleid (vorig jaar: geen).
goed nieuws	Van de 736 keer dat een open standaard voor een aanbesteding relevant was werd daar in 50 % van de gevallen door de aanbesteder om gevraagd. Vorig jaar lag dit percentage nog op 43%.
goed nieuws	Sommige standaarden (vooral NEN-ISO/IEC 27001 en 27002, HTTPS & HSTS en TLS en – iets minder – PDF zijn beduidend vaker relevant bij een aanbesteding dan andere.
goed nieuws	Om een aantal vaak relevante standaarden wordt, als ze voor een aanbesteding relevant zijn, in de meeste gevallen ook inderdaad gevraagd: NEN-ISO/IEC 27001, NEN-ISO/IEC 27002, HTTPS & HSTS, TLS, SAML, PDF, StUF, Digitoegankelijk en CMIS).
minder goed	Drie standaarden werden relatief weinig gevraagd: IPv4 & IPv6, ODF en Digikoppeling zijn vaak als relevant aangemerkt, maar in respectievelijk slechts 23%, 11% en 26% van die gevallen werd om de standaard gevraagd. Voor IPv4 & IPv6 is dat overigens wel een verbetering in vergelijking met vorig jaar.

Een aantal aanbestedingen onderscheidde zich in positieve zin (zie ook paragraaf 3.2.2):
Ministerie van BZK (Diginetwerk/Koppelnet Publieke Sector): voldoet aan alle 6 de relevante standaarden, terwijl het Diginetwerk een goeddeels besloten netwerk is dat niet bedoeld is om (via internet) met andere systemen interoperabel te zijn.
Zorginstituut Nederland (schaalbare Infrastructure as a Service): voldoet aan alle 10 de relevante standaarden.

Provincie Groningen (beheer van ICT-infrastructuur inclusief telefonie): voldoet aan alle drie de relevante standaarden.
Stichting Nederlandse Wetenschappelijk Onderzoekinstituten (computercluster, lokale opslagruimte, snelle netwerkverbindingen): de enige relevante geachte open standaard is uitgevraagd.
Gemeente Maastricht (corporate website en multi-site oplossing voor beheer van veertig andere websites): voldoet bijna aan alle 11 relevante standaarden (er is alleen om IPv6 gevraagd en niet ook om IPv4, anders zou deze aanbesteding in de categorie 'perfect' zijn ingedeeld).
Ministerie van AZ (e-mailmanagementvoorziening voor het Platform Rijksoverheid Online): om 10 van de 12 open standaarden is gevraagd en om een elfde gedeeltelijk (IPv6).

'Leg uit' in jaarverslagen
Wie bij een aanbesteding om een relevante open standaard niet vraagt, moet daar een legitieme (zwaarwegende) reden voor hebben en daarvan verantwoording afleggen in het jaarverslag. Is dat misschien de verklaring van een deel van de gevallen waarin niet om een relevante standaard werd gevraagd?

Of er sprake is geweest van 'Leg uit' is na te gaan voor een deel van de dit jaar onderzochte aanbestedingen: alleen voor de aanbestedingen in het 3e en 4e kwartaal van 2018 (over 2019 zal door overheden pas verantwoording afgelegd worden in het jaarverslag dat in het voorjaar van 2020 verschijnt). Voor 33 van de aanbestedingen in het 3e en 4e kwartaal van 2018 was 'Leg uit' zonder twijfel vereist, omdat hierbij om één of meer relevante open standaarden niet gevraagd werd.

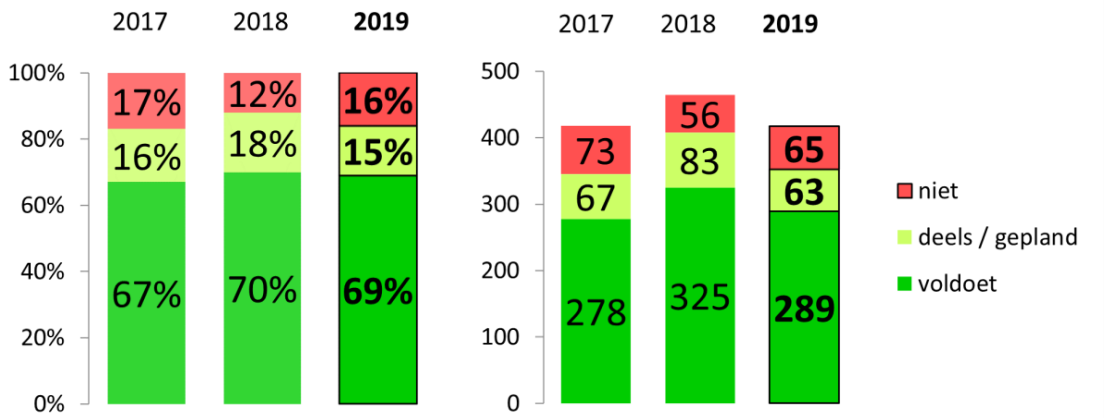
minder goed	Van expliciete 'Leg uit' voor met name genoemde aanbestedingen was in de jaarverslagen van de betreffende overheidsorganisaties (waaronder 7 ministeries) geen sprake: nergens wordt een concrete afwijking van de 'pas toe of leg uit'-lijst genoemd, laat staan verantwoord.
minder goed	Bij 33 aanbestedingen was 'Leg uit' noodzakelijk. Bij 15% hiervan (vorig jaar: 9%) was sprake van een beperkte verantwoording in het jaarverslag. Bij de overige 85% was geen sprake van enige vorm van 'Leg uit' (vorig jaar 91%).
goed nieuws	In het jaarverslag over 2018 hebben 5 van de 11 ministeries een alinea over 'pas toe of leg uit' opgenomen (vorig jaar waren dit er 4).
goed nieuws	Het ministerie van BZK heeft een alinea over 'pas toe of leg uit' opgenomen, en verwijst bovendien (net als vorig jaar) naar het overzicht dat Logius jaarlijks publiceert met afwijkingen van de lijst voor 'pas toe of leg uit' in haar ICT-producten en -diensten en bedrijfsvoering.

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 dat 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?

Ook dit jaar is onderzocht in hoeverre de belangrijkste voorzieningen (36 in totaal) voldoen aan de relevante open standaarden. Er zijn 27 voorzieningen van de Basisinfrastructuur (voorheen GDI) onderzocht. Daarnaast zijn dit jaar opnieuw 9 andere voorzieningen[2] onderzocht die vorig jaar ook onderzocht zijn.

Een belangrijk deel van alle voorzieningen blijkt te voldoen aan relevante open standaarden. Van alle 417 gevallen waarbij een open standaard voor een voorziening relevant was, voldoet in 69% de voorziening daar aan (vorig jaar 70%). Het aantal gevallen waarin de voorziening deels aan de standaard voldoet of daarvoor concrete plannen heeft is iets afgenomen: van 18% vorig jaar naar 15% dit jaar. Samen is dat 84%. De totaalcijfers laten dus zien dat een heel behoorlijk niveau van toepassing bereikt is. Maar er is nog geen sprake van volledige compliancy, en de ontwikkeling lijkt enigszins te stagneren.



In absolute aantallen (zie vierde tot en met zesde kolom) lijkt het aantal gevallen waarin aan open standaarden wordt voldaan gedaald te zijn van 325 vorig jaar naar 289 dit jaar. Dit beeld wordt echter vertekend doordat met ingang van dit jaar PDF als één standaard op de lijst staat en niet meer als drie aparte standaarden en doordat dit jaar niet op DigiToegankelijk is getoetst (zie paragraaf 4.1.4 voor een toelichting). Gezien de scores van vorig jaar voor PDF en DigiToegankelijk zou het totaal aantal gevallen waarin aan een standaard wordt voldaan dit jaar juist hóger zijn dan vorig jaar.

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

goed nieuws	Voor veel voorzieningen is een flink aantal open standaarden relevant: gemiddeld 11,6 standaarden per voorziening. Van de 41 standaarden op de lijst voor 'pas toe of leg uit' zijn er 28 relevant voor één of meer overheidsbrede voorzieningen.
goed nieuws	Voor 14 van deze 28 standaarden geldt dat minstens 80% van de voorzieningen aan die standaard – indien relevant – voldoet. Van deze standaarden vallen er 6 in het domein 'Internet & beveiliging'.
minder goed	Vijf standaarden scoren relatief laag: van de voorzieningen waarvoor deze relevant zijn voldoet er geen enkele aan NLCIUS, en voldoet 20% aan CMIS, 27% aan IPv4 & IPv6, 38% aan STARTTLS & DANE en 40% aan SKOS.
minder goed	Vooral standaarden uit het domein Internet & Beveiliging zijn vaak relevant (72% van alle gevallen). De domeinen Document & Webcontent (15%) en Stelselstandaarden (8%) volgen op grote afstand. De standaarden uit de zes andere domeinen zijn zelden relevant (samen slechts 5%).

[2] ODC Noord, Digi-Inkoop, Doc-Direct, DWR, P-Direct, Rijksoverheid.nl, Rijkspas, Rijksportaal en TenderNed.

goed nieuws	In de meeste gevallen voldoen de onderzochte voorzieningen aan de meeste ervoor relevante standaarden: aan 69% wordt voldaan, aan 15% voldoet de voorziening deels of dit is gepland en in 16% van de gevallen wordt op dit moment (nog) niet voldaan aan een relevante open standaard.
goed nieuws	Ook dit jaar voldoen 10 van de 36 voorzieningen geheel of gedeeltelijk aan alle relevante open standaarden en/of hebben concrete plannen om daaraan op korte termijn te voldoen. Alle tien zijn voorzieningen van de Basisinfrastructuur.
minder goed	Enkele voorzieningen voldoen niet aan een relatief groot deel van de voor hen relevante open standaarden: e-Factureren, Rijksportaal, Berichtenbox Bedrijven en BSN Beheervoorziening & GBA-V.
goed nieuws	Veel voorzieningen hebben ten opzichte van de vorige meting vooruitgang geboekt, met als meest positieve voorbeelden P-Direct, Samenwerkende Catalogi en daarnaast ook Digitale Werkomgeving Rijk en Digilevering.

Verschillende voorzieningen onderscheiden zich dit jaar in positieve zin:

- de nieuwe voorziening BRO (ondergrond) voldoet meteen al aan 11 van de 13 relevante standaarden, voldoet deels aan de 12e standaard en voor de 13e zijn concrete plannen;
- Mijn overheid voldoet aan 14 van de 15 relevante standaarden en deels aan de 15e;
- DigiD voldoet aan 10 van de 11 relevant standaarden (net als vorig jaar);
- Digilevering voldoet aan 7 van de 8 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. Dit jaar is dat opnieuw gedaan door de accountmanagers van het Bureau Forum Standaardisatie, in de zomer van 2019, 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 daarin ten onrechte onvoldoende 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	Uitzonderingen zijn IPv4&IPv6 (48%, maar wel stijgend), DANE (41%, ook stijgend) en STARTTLS (67%, ook stijgend).
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 B7)

Uit de '*Meting Informatieveiligheidstandaarden maart 2019*' blijkt dat het streefbeeld voor eind 2018 op het moment van de meting – maart 2019 – nog niet was gerealiseerd.

goed nieuws	Van de webstandaarden wordt DNSSEC het meest toegepast (93%), gevolgd door HTTPS conform NCSC (90%) en TLS conform NCSC (89%). HSTS conform NCSC is iets minder ver gevorderd (79%).
goed nieuws	Van de mailstandaarden wordt SPF (95%) het meest toegepast, gevolgd door DKIM (89%) en DMARC (82%).

minder goed	De andere mailstandaarden worden op dit moment nog minder vaak gebruikt en hebben nog een flink eind te gaan: STARTTLS conform NCSC (67%) en DANE (41%).

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 zijn respectievelijk afkomstig uit Tabel 5 (aanbestedingen), gebaseerd op een telling van scores in Tabel 8a/b (voorzieningen) en uit Tabel 9 (gebruiksgegevens). 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 lager dan 25%. Als het absolute aantal erg klein is (1, 2 of 3), dan hebben we het percentage tussen haakjes gezet.

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.

Voor negen van de twaalf standaarden uit het domein *Internet & beveiliging* is het overall beeld positief, en voor STARTTLS & DANE is het redelijk. Twee standaarden blijven nog wat achter: het overall beeld is wisselend voor IPv4&IPv6 en voor WPA2 Enterprise.
Ook in het domein *Stelselstandaarden* gaat het goed: voor Digikoppeling en StUF is het overall beeld positief en voor de Geo-standaarden redelijk.

In het domein *Document & (web)content* scoren twee van de acht standaarden positief (PDF en SKOS) en twee scoren redelijk (CMIS en OWMS). Het overall beeld voor Open API Specification is wisselend en twee standaarden scoren matig: Ades Baseline Profiles en ODF. (Over Digitoegankelijk zijn dit jaar te weinig gegevens beschikbaar.)

Van de vier standaarden in het domein *E-facturatie & administratie* is het overall beeld voor twee standaarden redelijk (SETU en XBRL). Voor WDO Datamodel is het beeld wisselend en voor NLCIUS matig.

Het overall beeld voor alle drie de standaarden in het domein *Juridische verwijzingen* is wisselend. Dat geldt ook voor de enige 'overige' standaard: EML_NL.

Over de in totaal zeven standaarden in de andere drie domeinen (*Water & bodem, Bouw en Onderwijs & loopbaan*) is onvoldoende informatie beschikbaar.

	Aanbestedingen	Voorzieningen	Gebruiksgegevens	Overall beeld
indicator:	*# aanbestedingen gevraagd in % van # aanbestedingen waarbij OS relevant is*	*# voorzieningen dat voldoet + deels + gepland in % van # waarvoor relevant is*	*# overheidsorganisaties dat de standaard gebruikt in % van alle overheidsorganisaties*	
Internet & beveiliging:				
DKIM	31 %	88%	van 84% naar 89%	positief
DMARC	31 %	81%	van 73% naar 82%	positief
DNSSEC	40 %	90%	van 90% naar 93%	positief
HTTPS en HSTS	61 %	97%	van 89% naar 90%	positief
IPv6 en IPv4	23 %	61%	van 29% naar 48%	wisselend
NEN-ISO\IEC 27001:2005nl	83 %	100%	*[?]*	positief
NEN-ISO\IEC 27002:2007nl	83 %	100%	*[?]*	positief
SAML	58 %	100%	(van 757 naar 868)	positief
SPF	31 %	92%	van 93% naar 95%	positief
STARTTLS en DANE	54 %	48%	cf: van 55% naar 67%	redelijk
TLS	61 %	93%	cf: van 87% naar 89%	positief
WPA2 Enterprise	20 %	(100%)	(van 459 naar 529)	wisselend
Document & (web)content:				
Ades Baseline Profiles	(0 %)	50%	*[?]*	matig
CMIS	71 %	40%	*NIET ONDERZOCHT*	redelijk
Digitoegankelijk *)	40 %	*NIET ONDERZOCHT*	*NIET ONDERZOCHT*	[?]
ODF	11 %	60%	nulmeting: 6,7%	matig
OpenAPI Specification	25 %	90%	*[?]*	wisselend
OWMS	(50 %)	75%	nulmeting: 38%	redelijk
PDF	60 %	100%	nulmeting: 99,9%	positief
SKOS		80%	nulmeting: 74%	positief
E-facturatie & administratie:				
NLCIUS	36 %	0%	nulmeting: 15%	matig
SETU	(33 %)	(100%)	(veel toegepast)	redelijk
WDO Datamodel	(0 %)		(veel toegepast)	wisselend
XBRL	33 %	(100%)	(veel toegepast)	redelijk
Stelselstandaarden:				
Digikoppeling	26 %	85%	van 96% naar 100%	positief
Geo−standaarden	29 %	100%	(veel toegepast)	redelijk
StUF	81 %	78%	(veel toegepast)	positief
Water & Bodem:				
Aquo Standaard		(100%)	*[?]*	[?]
SIKB 0101	(100 %)		*[?]*	[?]
SIKB 0102			*[?]*	[?]
Bouw:				
IFC			*[?]*	[?]
Visi			*[?]*	[?]
Juridische verwijzingen:				
BWB	0 %	100%	(LiDO: 40.000 /mnd)	wisselend
ECLI	(0 %)	(100%)	(LiDO: 40.000 /mnd)	wisselend
JCDR	0 %		(LiDO: 40.000 /mnd)	wisselend
Onderwijs & loopbaan:				
E−portfolio	0 %		*NIET ONDERZOCHT*	[?]
NL LOM	(0 %)		*NIET ONDERZOCHT*	[?]
Overig:				
EML_NL	(0 %)		(veel toegepast)	wisselend

2. Inleiding en beleidscontext

2.1. Waarom open standaarden?

Sinds 2009 moet een aantal standaarden overheidsbreed verplicht toegepast worden: de open standaarden van de 'pas toe of leg uit'-lijst. Deze lijst wordt beheerd door het Forum Standaardisatie. 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 (door leveranciersafhankelijkheid te beperken)
- en om te zorgen voor veiligheid en betrouwbaarheid in het digitale verkeer: onder andere om cybercriminaliteit tegen te gaan en persoonsgegevens te beschermen.

Om deze redenen is voor veel overheden het gebruik van deze standaarden verplicht. Niet bij wet in formele zin (hoewel deze verplichting met de komst van de wet Digitale Overheid wel op handen is), maar via het 'pas toe of leg uit'-beleid dat onder meer vorm heeft gekregen in de Instructie Rijksdienst voor aanschaf van ICT -diensten en ICT-producten en via diverse bestuursakkoorden. Hierover meer in paragraaf 2.3 over het juridisch kader.

Voor *niet-overheidsorganisaties* is het gebruik van de standaarden van de lijst niet verplicht, maar om dezelfde redenen als hierboven vermeld wel verstandig.

2.2. Het open standaardenbeleid in jaartallen

2008
Besluit van de staatssecretaris van Economische Zaken van 8 november 2008 tot vaststelling van de *Instructie rijksdienst inzake aanschaf ICT-diensten en ICT-producten*. Hiermee is het gebruik van open standaarden voor de Nederlandse overheid de norm.

Pas toe:
Overheden zijn verplicht om bij de aanbesteding, inkoop of ontwikkeling van ICT-systemen en -diensten de relevante standaarden te eisen van de 'pas toe of leg uit'-lijst van het College Standaardisatie. Voor elke open standaard is in deze lijst een functioneel toepassingsgebied en een organisatorisch werkingsgebied bepaald, aan de hand waarvan de overheids-organisatie kan bepalen of de open standaard in een specifiek aanschaftraject relevant is.

Leg uit:
Overheden mogen alleen afwijken (d.w.z. 'niet toepassen') ingeval van redenen van bijzonder gewicht[3]. Overheden zijn verplicht om afwijkingen gemotiveerd vast te leggen in de administratie en om zich over de mate van naleving te verantwoorden in het jaarverslag.

Zie Bijlage B3 voor een stroomschema.

[3] "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."

2011
Het kabinet kondigt aan dat het 'pas toe of leg uit'-regime minder vrijblijvend wordt. Eén van de maatregelen om dat te bereiken is het opnemen van de 'leg uit'-verplichting in de Rijksbegrotingsvoorschriften.

2014
Eén van de aanbevelingen in het rapport van de commissie Elias luidt: De rijksoverheid ziet daadwerkelijk toe op naleving van haar pas-toe-of-leg-uit-beleid rondom opensource software en open standaarden.

2015
De Tweede Kamer neemt de motie Oosenbrug/Gesthuizen (14 april 2015) aan, waarin de regering ondermeer gevraagd werd *"(…) ervoor te zorgen dat voor eind 2015 bij alle aanbestedingen correct omgegaan wordt met de relevante open standaarden (…)"*.

Het Nationaal Beraad Digitale Overheid herbevestigt in mei 2015 de reeds bestaande overheidsbrede verplichting voor het toepassen van open standaarden en verlengt deze tot eind 2017.

2016
De Tweede Kamer neemt de motie Oosenbrug (11 oktober 2016) aan, waarin de regering ondermeer gevraagd wordt *"(…) het gebruik van open standaarden te verplichten bij wet"*.

2018
In maart 2018 komt het nieuwe Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) voor het eerst bijeen. Het OBDO heeft de bestuurlijke afspraken van het Nationaal Beraad overgenomen cq. verlengd. Het OBDO heeft op 18 april 2018 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 zijn in het OBDO specifieke afspraken gemaakt voor de adoptie van een aantal internet-veiligheidsstandaarden.
Streefbeeld eind 2017:
- TLS wordt toegepast bij alle overheidswebsites waarbij burgers en/of bedrijven gegevens moeten invoeren, of waarbij gegevens vooringevuld zijn;
- DNSSEC wordt gebruikt voor elke domeinnaam waarmee een overheidsorganisatie met burgers en/of bedrijven communiceert;
- de 'e-mail'-standaarden DMARC, SPF en DKIM worden toegepast voor alle overheids-domeinnamen of deze nu wel of niet gebruik maken van mail.

Streefbeeld eind 2018:
- alle overheidswebsites hebben HTTPS, HSTS en TLS inclusief de veilige configuratie conform NCSC ingevoerd (aanvulling op bestaande adoptie-impuls Nationaal Beraad). Dit is herbevestigd in het Digiprogramma 2018.

Streefbeeld eind 2019:
- adoptie en configuratie van STARTTLS & DANE (beveiliging van emailverkeer middels encryptie) en het instellen van strikte policies voor emailstandaarden SPF en DMARC.

2.3. Juridisch kader

De volgende verplichtingen en afspraken gelden op dit moment voor overheidsorganisaties.

2.3.1. Ministeries en uitvoeringsorganisaties: Rijksinstructie en Rijksbegrotingsvoorschriften

Voor de rijksoverheid (zowel ministeries als uitvoeringsorganisaties) is sinds november 2008 de Rijksinstructie[4] van kracht:

> *Bij de aanschaf van een ICT-dienst of ICT-product voor een toepassingsgebied dat voorkomt op de lijst die op de website 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.*

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. In Bijlage B3 is een schema opgenomen waarin het 'pas toe of leg uit'-principe in het kort wordt toegelicht.

Een open standaard van de lijst is altijd relevant als het betreffende ICT-product of -dienst valt binnen het functionele toepassingsgebied van die open standaard, als de organisatie bovendien valt binnen het organisatorische werkingsgebied van de betreffende standaard[5]. Er kunnen redenen zijn om de open standaard toch niet toe te passen. De aanbesteder kan echter niet zelf besluiten dat een open standaard 'in dit geval niet relevant is': of een standaard relevant is, hangt uitsluitend af van functioneel toepassingsgebied en organisatorisch werkingsgebied. Wanneer besloten wordt 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 bovendien verantwoording afgelegd worden in het jaarverslag. Afwijkingen zijn overigens alleen mogelijk bij redenen van bijzonder gewicht (zie daarover ook de toelichting van de Instructie rijksdienst).

Daarnaast is sinds vele jaren in de RijksBegrotingsVoorschriften[6] 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.*

---

[4] *Besluit van de staatssecretaris van Economische Zaken van 8 november 2008 tot vaststelling van de Instructie rijksdienst inzake aanschaf ICT-diensten en ICT-producten (artikel 3, lid 1).*

[5] Het functionele toepassingsgebied en het organisatorische werkingsgebied van elke standaard zijn vermeld in de lijst voor 'pas toe of leg uit'.

[6] De Rijksbegrotingsvoorschriften zijn opgesteld door het Ministerie van Financiën en bevatten de voorschriften voor de verantwoording over de begroting, uitvoering van de begroting en de begroting.

2.3.2. *Mede-overheden: iNUP-Resultaatafspraak 20 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. 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.*

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.

2.4. Over de Monitor Open standaarden 2019

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 door ministeries, uitvoeringsorganisaties, gemeenten, provincies en waterschappen toegepast?

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

- onderzoek van feitelijke aanbestedingen in 2018/2019,
- 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 feitelijke aanbestedingen in 2018/2019

Dit jaar zijn aanbestedingen onderzocht van de rijksoverheid (en uitvoeringsorganisaties) en van mede-overheden uit de periode juli 2018 tot en met juni 2019. 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 is een onderzoek uitgevoerd naar de mate waarin 36 voorzieningen voldoen aan de open standaarden die daarvoor relevant zijn: 27 voorzieningen van de GDI (Generieke Digitale Infrastructuur) en 9 andere voorzieningen die in de voorgaande jaren ook onderzocht zijn. Hiervoor zijn de betreffende beheerorganisaties benaderd.

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: overheden moeten bij ICT-aanbestedingen de relevante open standaarden van de lijst met verplichte standaarden toepassen, of verantwoording afleggen in hun jaarverslag als zij deze standaarden (ondanks dat zij relevant zijn) niet toepassen.

In het kader van de Monitor Open standaarden 2019 is voor het achtste achtereenvolgende 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').

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 feitelijke aanbestedingen

Dit jaar is, net als in de voorgaande jaren, onderzoek gedaan naar de aanbestedingen door het Rijk (met inbegrip van de uitvoeringsorganisaties, agentschappen en ZBO's) en door de decentrale overheden (voor de periode Q3 en Q4 2018 en Q1 en Q2 2019). Dit jaar is de rol van eerste en tweede expert dezelfde als vorig jaar: de beoordeling van aanbestedingen is uitgevoerd door TNO (Wouter van den Berg en Robin de Veer), en vanuit ICTrecht hebben mr. dr. Mathieu Paapst en mr. Arend-Jan Wiersma de second opinion op de Rijks-aanbestedingen geleverd.

Onderzocht zijn aanbestedingen die op tenderned.nl zijn gepubliceerd. Het betreft daardoor voornamelijk Europese aanbestedingen (drempelwaarden voor Europese aanbestedingen[7]: voor rijksoverheid > € 144.000 en voor decentrale overheden > € 221.000). 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 wederom dat deze grens niet altijd even duidelijk is te trekken. Voor een goede beoordeling moeten de aanbestedingsdocumenten bestudeerd kunnen worden, die moeten dus (nog) voor de beoordelaars beschikbaar zijn.

[7] Deze drempelwaarden worden telkens voor een periode van twee jaar door de Europese Commissie vastgesteld. De huidige drempelwaarden zijn van kracht tot en met 31 december 2019.

In principe worden elk jaar alle gevonden relevante aanbestedingen van Rijksoverheid en uitvoeringsorganisaties beoordeeld. Dit jaar ligt het aantal beoordeelde aanbestedingen van de Rijksoverheid (35) 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:

- een aanbesteding die bestaat uit een marktscan om vervolgens overheden te helpen bij het maken van een keuze voor een leverancier;
- er wordt alleen gevraagd naar commerciële standaardsoftware licenties;
- in de aanbesteding gaat het om niet meer dan de inhuur van personeel;
- de aanbesteding betreft een raamovereenkomst;
- de aanbestedende partij valt bij nadere beschouwing buiten de doelgroep 'Rijk' zoals omschreven voor deze monitor.

Voor de mede-overheden wordt elk jaar een steekproef getrokken uit de gevonden aanbestedingen. Dit jaar zijn 37 aanbestedingen van mede-overheden beoordeeld (vorig jaar 33). Let wel: met ingang van de vorige monitor is gekozen voor een verdubbeling van het aantal aanbestedingen door mede-overheden om zo beter zicht te krijgen op de aanbestedingen door diezelfde mede-overheden.

De beoordeling heeft plaatsgevonden in twee tranches: aanbestedingen uit de periode juli tot en met december 2018 en uit de periode januari tot en met juni 2019. Uiteindelijk zijn in totaal 72 aanbestedingen beoordeeld: 35 van het Rijk (departementen en uitvoerings-organisaties, agentschappen, ZBO's) en een steekproef van 37 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-DMARC-SPF (e-mail standaarden), HTTPS&HSTS-TLS en ISO-27001-ISO-27002.

De variatie in de aard van de ICT-producten en -diensten die werden aanbesteed is net als in de voorgaande jaren groot. Enkele willekeurige voorbeelden van aanbestedingen:

- met de aanbesteding beoogt (…) de veiligstelling van de informatie die zij onder haar beheer heeft. Men wil een eenmalige inrichting voor het monitoren van het netwerk (…) en daarnaast een aantal ondersteunende diensten (ministerie / Rijk);
- de aanbesteding betreft een SaaS catalogus van Producten en Diensten gericht aan medewerkers van de opdrachtgever, alsmede het technisch beheer en onderhoud daarop, hosting en additionele diensten. De scope beperkt zich tot opleidingen, trainingen en andere leer-interventies (ministerie / Rijk);
- opdrachtgever wil maximaal ontzorgd worden met betrekking tot het beheer van de IT-Infrastructuur en wenst daarvoor het hosten, ontsluiten en beheren van de ICT-omgeving als dienst af te nemen. De dienstverlener wordt hierbij verantwoordelijk voor het beheren van de volledige IT-infrastructuur (ZBO / Rijk);
- men zoekt een partij die actuele data vergaart, verifieert, waar nodig verrijkt, opslaat en ontsluit. Binnen de scope vallen o.a. geordende verwerking en ontsluiting van data, inrichting van een database, verstrekking van de data als Open Data en beschikbaar stellen van een databestand dat kan worden bijgewerkt door gebruikers (ministerie / Rijk);
- een aanbesteding voor een applicatie ten behoeve van het automatiseren van het aanvraag-, meldings- en vergunningenproces rondom werkzaamheden in de openbare ruimte (waaronder en met name kabels en leidingen) (SSC regio);
- een systeem, op basis van SaaS, dat minimaal de volgende functionaliteit biedt: een cliëntvolgsysteem, een online omgeving voor kandidaten om hun loopbaantraject te volgen en waar de kandidaat loopbaantesten kan maken, en het genereren van managementinformatie (gemeente);
- een raadsinformatiesysteem: een integraal digitaal vergadersysteem waarmee de raad bediend kan worden ten aanzien van de vergaderagenda's, vergaderstukken, dat kan dienen als naslagwerk, (…) de mogelijkheid van live uitzendingen van vergaderingen van raad en commissies en andere bijeenkomsten, die gekoppeld worden aan de agenda en die achteraf teruggekeken kunnen worden (gemeente).

Toetsingskader

Het onderzoek is gebaseerd op de gepubliceerde, openbare informatie over de aanbestedingen. Dit sluit aan bij de transparantie die ten grondslag ligt aan het open standaardenbeleid. Bovendien is dat 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[8].

Daarnaast is onderzocht op welke wijze de verantwoording ('leg uit') over 2018 heeft plaatsgevonden[9].

Het onderzoek toetst op basis van deze openbare documenten in hoeverre de aanbestedingen voldoen aan het 'pas toe of leg uit'-beginsel, zoals dat (voor de Rijksoverheid) is vastgelegd in de Instructie Rijksdienst. Andere (beleids)overwegingen en argumenten, die mogelijk een rol hebben gespeeld bij de aanbestedingen, vallen buiten de scope van dit onderzoek.

[8] Voor de volgende monitor in 2020 zullen wij over dit uitgangspunt nog een nadere discussie hebben.
[9] Zie paragraaf 3.4.

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, en als de aanbestedende organisatie bovendien valt binnen het organisatorische werkingsgebied van de standaard. Voor één aanbesteding kunnen uiteraard meerdere open standaarden relevant zijn.

Of een standaard van toepassing is, hangt dus uitsluitend af van het functioneel toepassingsgebied en het organisatorisch werkingsgebied. 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 bovendien verantwoording afgelegd worden in het jaarverslag. Afwijkingen zijn overigens alleen mogelijk bij redenen van bijzonder gewicht.

Het toepassen van een open standaard vereist, dat bij de aanbesteding expliciet gevraagd wordt om deze standaard. In plaats van expliciet om de relevante open standaard(en) te vragen, wordt soms alleen in algemene zin verwezen naar de lijst voor 'pas toe of leg uit'. De aanbieder krijgt daarmee de verantwoordelijkheid voor het correct toepassen ervan. In de praktijk levert dat echter niet het beoogde (beleids)effect op. Immers, de aanbiedingen zijn 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. Het beoogde (beleids)effect is er dus alleen indien één of meer aanbieders (toch) de relevante open standaard(en) toepassen.

3.2. 'Pas toe' bij feitelijke aanbestedingen in 2018/2019

In totaal had in de 72 aanbestedingen die dit jaar zijn beoordeeld om 738 open standaarden gevraagd moeten worden, feitelijk werd er echter 368 keer om een open standaard gevraagd - dat is dus 50% daarvan (zie de groene rijen midden in Tabel 1). Dit percentage ligt hoger dan de overeenkomstige percentages van de afgelopen jaren (van 2014 tot 2018 fluctuerend tussen 43% en 45%). In de jaren daarvoor (2012 en 2013) lag dit percentage beduidend lager, op respectievelijk 30% en 25%.

'Pas toe' per aanbesteding

Bij 4 van de 72 aanbestedingen (6%; vorig jaar ook 6%, de grijze kolommen in Tabel 1) werd om alle relevante open standaarden gevraagd, dat is 'pas toe' in strikte zin: 1 aanbesteding door een ministerie, 2 aanbestedingen door een ZBO en 1 door een provincie. Daarnaast werd bij 60 aanbestedingen (83%; vorig jaar 79%) gevraagd om een deel van de voor die aanbesteding relevante standaarden. Bij de resterende 8 aanbestedingen (11%; vorig jaar 15%) - waarbij één of meer open standaarden relevant waren - werd om geen enkele open standaard gevraagd (bij 3 aanbestedingen) of was sprake van strijdigheid met het open standaardenbeleid (in 5 gevallen, er werd gevraagd om licenties voor standaard software).

In de monitor van vorig jaar werd voor de aanbestedingen waarbij om een deel van de relevante standaarden was gevraagd nog een onderscheid gemaakt tussen cruciale en niet-cruciale standaarden (net als in eerdere jaren)[10]. Dit onderscheid (al dan niet cruciaal) is met ingang van dit jaar komen te vervallen.

[10] En beperkte het onderzoek naar het leg-uit-principe zich tot aanbestedingen waarbij om minimaal één cruciale standaard niet werd gevraagd.

Tabel 1: 'Pas toe' en 'leg uit' bij feitelijke aanbestedingen 2018/2019

(Bron: onderzoek feitelijke aanbestedingen juli 2018 t/m juni 2019, uitgevoerd zomer 2019)

	Rijksoverheid		Mede-overheden		**Totaal 2018/2019**		Totaal 2017/2018	
	#	%	#	%	#	%	#	%
totaal aantal beoordeelde aanbestedingen waarbij OSn relevant waren	**35**	100%	**37**	100%	**72**	**100%**	67	100%
* **perfect**: aantal aanbestedingen met alle relevante OSn gevraagd	3	9 %	1	3 %	**4**	**6 %**	4	6 %
* **op de goede weg**: aantal aanbestedingen met een deel van relevante OSn gevraagd	31	89 %	29	78 %	**60**	**83 %**	53	79 %
Aantal aanbestedingen met geen relevante OSn gevraagd, waarvan:	0	0 %	3	8 %	**3**	**4 %**	10	15 %
* **matig**: er is wel algemene aandacht voor architectuur-kaders en/of OSn-beleid	0	0 %	1	3 %	**1**	**1 %**	2	3 %
* **slecht**: geen aandacht voor OSn-beleid	0	0 %	2	5 %	**2**	**3 %**	8	12 %
* **heel slecht**: strijdig met OSn-beleid	1	3 %	4	11 %	**5**	**7 %**	0	0 %
totaal aantal relevante OSn	336	100%	402	100%	**738**	**100%**	555	100%
totaal aantal gevraagde relevante OSn	167	50 %	201	50 %	**368**	**50 %**	240	43 %
Aantal aanbestedingen met niet alle OSn gevraagd => Leg Uit vereist	32		36		**68**		63 *)	
idem, maar beperkt tot Q3+Q4 2018 [11]	*16*	*100%*	*17*	*100%*	***33***	***100%***	*23*	*100%*
- concrete verantwoording in jaarverslag	*0*	*0 %*	*0*	*0 %*	***0***	***0 %***	*0*	*0 %*
- beperkte verantwoording in jaarverslag	*5*	*31 %*	*0*	*0 %*	***5***	***15 %***	*2*	*9 %*
- geen Leg Uit in jaarverslag	*11*	*69 %*	*17*	*100%*	***28***	***85 %***	*21*	*91 %*

*) De cijfers over 'Leg uit' voor 2017/2018 zijn niet helemaal vergelijkbaar. Vorig jaar is 'Leg uit' namelijk alleen onderzocht voor de 57 aanbestedingen waarbij minimaal één cruciale standaard niet was gevraagd, en dus niet bij de (6) aanbestedingen waarbij alle cruciale standaarden gevraagd waren.

De onderverdeling van de categorie 'geen relevante open standaarden gevraagd' is wel gehandhaafd, maar in een iets aangepaste vorm:

- matig: er is algemene aandacht voor architectuur-kaders en/of open standaardenbeleid (1%, vorig jaar 3%),
- slecht: er is geen aandacht voor open standaardenbeleid (3%, vorig jaar nog 12%).

Tenslotte is er nog een vierde categorie: 'heel slecht': de aanbesteding is strijdig met het open standaardenbeleid (7% tegen 0% vorig jaar). Bijvoorbeeld omdat er gevraagd wordt om standaardsoftware. Bij deze laatste categorie uit de eerder genoemde vierdeling is dus sprake van een verslechtering. Daar staat tegenover dat de kwalificaties 'matig' en 'slecht' dit jaar minder vaak voor komen.

[11] Controle op de toepassing van 'leg uit' heeft alleen kunnen plaatsvinden over de aanbestedingen uit 2018, waarover verantwoording had moeten worden afgelegd in het Jaarverslag 2018.

Ook dit jaar is sprake van verschillen tussen Rijk en uitvoeringsorganisaties enerzijds en de mede-overheden (gemeenten, provincies, waterschappen) anderzijds maar per saldo zijn deze verschillen tussen beide groepen kleiner geworden.
Bij 9% van de aanbestedingen door Rijk en uitvoeringsorganisaties werd om alle relevante standaarden gevraagd (vorig jaar nog 11%). Bij de decentrale overheden is bij één onderzochte aanbesteding om alle relevante standaarden gevraagd (3%, vorig jaar geen). Bij 89% van de Rijks-aanbestedingen (vorig jaar nog 71%) is om een deel van de relevante open standaarden gevraagd, tegen 78% voor de decentrale overheden (vorig jaar 88%). De twee middengroepen laten dus een tegengestelde ontwikkeling zien: bij de Rijksoverheid een behoorlijke toename, bij de mede-overheden een (wat minder grote) afname.

Deze tegengestelde beweging komen we – uiteraard andersom – ook tegen bij de laatste twee categorieën: 'geen relevante standaarden gevraagd' of 'strijdig met het open standaarden beleid'. Dit jaar is de categorie 'geen relevante standaarden gevraagd' leeg bij Rijk (vorig jaar: 18%). Bij één Rijks-aanbesteding (3%) is dit jaar sprake van strijdigheid met het open standaarden beleid; vorig jaar bij geen enkele aanbesteding. Voor wat betreft de mede-overheden ziet het beeld er als volgt uit. Bij 3 aanbestedingen (8%) wordt om geen enkele relevante standaard gevraagd (vorig jaar nog 12%). Dit jaar krijgt een viertal aanbestedingen door mede-overheden het predikaat 'heel slecht' (11%), omdat gevraagd werd om licenties voor standaard software. Vorig jaar was dit bij geen enkele aanbesteding door mede-overheden het geval.

Uit het horizontaal met groen gemarkeerde blok in de tabel valt op dat het aantal standaarden dat per aanbesteding relevant wordt geacht dit jaar duidelijk hoger ligt dan vorig jaar (gemiddeld ruim 10 standaarden per aanbesteding, vergeleken met gemiddeld ruim 8 standaarden vorig jaar en ongeveer 6 per aanbesteding in de twee jaren daarvoor). Deze stijging manifesteert zich zowel bij het Rijk als bij de mede-overheden.

Tot slot is opvallend aan Tabel 1 dat het aandeel bevraagde standaarden voor het Rijk en mede-overheden meer naar elkaar toe is gegroeid en nu (weer) gelijk is (50% tegen 50%). Drie jaar geleden scoorden Rijk en mede-overheden ook gelijk (44%), twee jaar geleden was de score van het Rijk bijna tweemaal zo hoog als van de mede-overheden (54% tegenover 28%) en vorig jaar was het verschil weer teruggelopen: 50% voor Rijk en 37% voor mede-overheden. Met betrekking tot deze variabele zien we derhalve behoorlijke fluctuaties zonder dat sprake is van een eenduidige ontwikkelingsrichting.

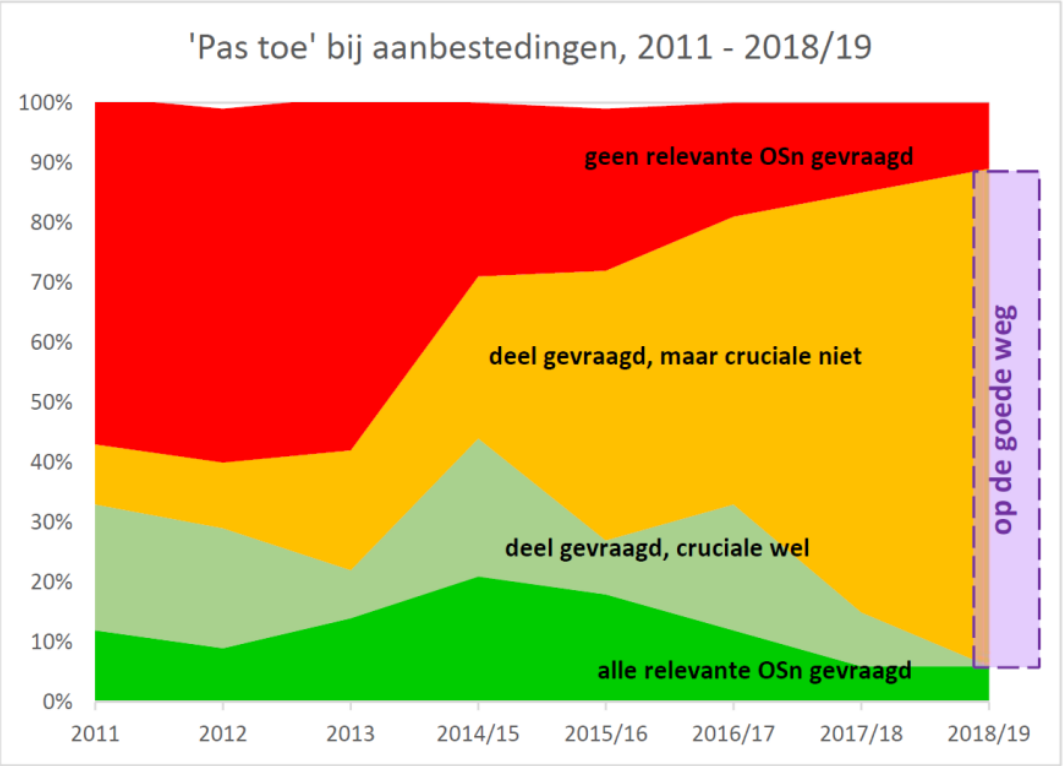
Op basis van Tabel 1 en de cijfers van de voorgaande jaren is de ontwikkeling als volgt:

- Het aantal aanbestedingen waarbij om alle relevante standaarden is gevraagd is gelijk gebleven (6%). Deze stabilisatie volgt op een periode waarin drie jaren op rij sprake is van een afname (vier jaar geleden lag dit percentage nog op 21%). Bij de Rijksoverheid is ten opzichte van vorig jaar sprake van een lichte afname van 11% naar 9%; de score voor mede-overheden lag vorig jaar op 0% en nu op 3%.
- De midden-categorie – dit jaar gekwalificeerd als 'op de goede weg' – is ook bij deze monitor weer zeer dominant met 83% tegen 79% vorig jaar.
- Het aantal aanbestedingen waarbij om geen enkele standaard is gevraagd is behoorlijk teruggelopen, van 15% vorig jaar naar 4% dit jaar.

- Deze gunstige ontwikkeling wordt voor een deel teniet gedaan door het feit dat dit jaar een vijftal aanbestedingen (7%) strijdig is met het open standaardenbeleid. Vorig jaar was hiervan in het geheel geen sprake.

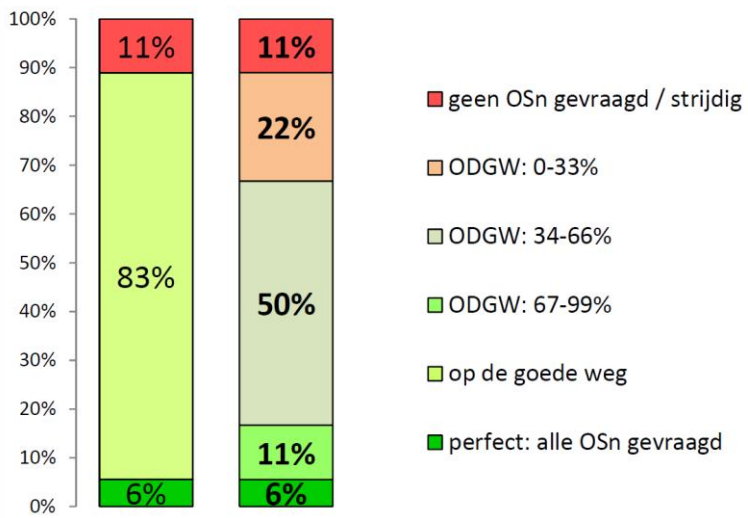
In Figuur 2 is de ontwikkeling in een breder tijdsperspectief geplaatst, vanaf het jaar 2011.

Figuur 2: 'Pas toe' bij aanbestedingen, 2011 - 2018/19



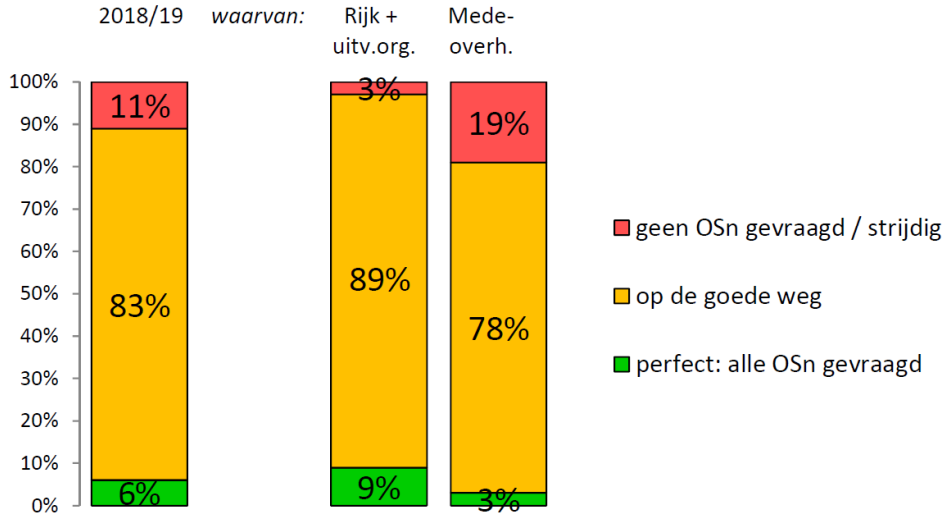
De middengroep 'op de goede weg', bestaande uit aanbestedingen waarbij wel om één of meer van de relevante open standaarden gevraagd werd maar niet om alle, is inmiddels gegroeid tot 83% van alle aanbestedingen. We hebben daarbinnen nog een nadere onderverdeling gemaakt tussen aanbestedingen waarbij maar om een klein deel (0-33%) van de relevante standaarden werd gevraagd, een middensegment (34-66%) en de groep die om een wat groter deel van de relevante standaarden heeft gevraagd. In Figuur 3 is te zien, dat het middensegment van de middengroep het grootst is.

Figuur 3: 'Pas toe' bij aanbestedingen 2018/2019: nadere uitsplitsing 'op de goede weg'



In Figuur 4 (tweede en derde kolom) is duidelijk te zien dat de verschillen tussen enerzijds Rijk en uitvoerings-organisaties en anderzijds mede-overheden groot zijn: bij 89% van de Rijks-aanbestedingen werd om een deel van de relevante standaarden gevraagd (mede-overheden: 78%), bij 9% werd om alle relevante standaarden gevraagd (mede-overheden: 3%), bij geen van de Rijks-aanbestedingen werd om geen enkele relevante standaard (mede-overheden: 8%) en bij 3% is sprake van strijdigheid met het open standaarden beleid (mede-overheden: 11%).

Figuur 4: 'Pas toe' bij aanbestedingen: uitsplitsing Rijk vs. mede-overheden 2018/2019



Alle cijfers over 'pas toe' bij aanbestedingen overziend is het beeld weliswaar redelijk positief, maar lijkt de ontwikkeling ook een beetje in het midden te blijven steken: veruit de meeste aanbestedingen vallen in de middengroep (niet heel goed, niet slecht) en zelfs in het middengedeelte van die middengroep (heeft om 34 tot 66 % van de relevante standaarden gevraagd), en van de 736 keer dat een open standaard voor een aanbesteding relevant was werd daar in 50 % van de gevallen om gevraagd (en om de andere 50 % dus niet).

Enkele goede voorbeelden

Net als in de vorige monitors brengen we ook nu weer enkele goede voorbeelden van aanbestedingen die in lijn zijn met het open standaardenbeleid voor het voetlicht. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties is net als de afgelopen twee jaren terug te vinden in dit rijtje, met de hoogste score (alle relevante standaarden uitgevraagd). Om dezelfde reden staat ook Zorginstituut Nederland (ZIN) erbij, net als vorig jaar met een heel complex aan relevante open standaarden. Ook de provincie Groningen en de stichting Nederlandse Wetenschappelijk Onderzoeksinstituten (NWO-I) zijn 'taart-kandidaat', ook al is het relevant geachte standaarden bij die twee casus duidelijk minder in aantal.

Ministerie van BZK. Het Diginetwerk is een stelsel van besloten netwerken, zonder afhankelijkheid van internet. Het Koppelnet Publieke Sector (KPS) is de centrale verbinder van het Diginetwerk. De beoordelaars van de aanbestedingen hebben bij deze casus de volgende kanttekening gemaakt. "Een uitzonderlijke aanbesteding als het gaat om de pas-toe-of-leg-uit lijst, aangezien het Diginetwerk een goeddeels besloten netwerk is dat niet bedoeld is om (via internet) met andere systemen interoperabel te zijn."

De volgende standaarden worden relevant geacht: Digikoppeling, HTTPS/HSTS, TLS, IPv4 en IPv6 en de beide ISO-standaarden ISO 27001 en 27002. Deze standaarden zijn alle uitgevraagd.

Zorginstituut Nederland. Dit betreft een aanbesteding voor een schaalbare Infrastructure as a Service (IaaS). ZiN wenst de diensten af te nemen tot en met het technisch beheer van de applicaties. De inschrijver zal verantwoordelijk worden voor datacenter, datacenter LAN, benodigde verbindingen, hardware, virtualisatielaag, server operating systems, etc. Met name in het beheer wenst ZiN ontzorgd te worden, wat bijvoorbeeld betekent dat zij zich niet meer druk wil maken over keuze van hardware, keuze van virtualisatieplatform, de installaties van de applicaties, hardware refreshments, applicatie en server operating system patches en updates, etc.
Er wordt heel complex aan open standaarden relevant geacht: DNSSEC, HTTPS/HSTS, TLS, IPv4 en IPv6, ISO 27001 en 27002, SAML, SPF, DKIM en DMARC en STARTTLS en DANE. Des te fraaier is het dat deze standaarden alle zijn uitgevraagd.

Provincie Groningen. Het doel van de aanbesteding is ten eerste het in huis halen van een leverancier die kwalitatief goed ICT-beheer kan aanbieden van de ICT-infrastructuur inclusief telefonie met bijbehorende ICT-netwerk infrastructuur. In de tweede plaats verwacht men dat deze leverancier op een proactieve manier meedenkt met de verdere ontwikkeling van een moderne, betrouwbare en kosteneffectieve ICT-infrastructuur. Actuele vraagstukken zijn het verstevigen van de (hybride) cloud werkomgeving, de beveiliging en de werkplekconcepten (mobiel).
Ook hier: alle relevant geachte standaarden (HTTPS/HSTS, TLS en ISO 27001 en /27002) zijn uitgevraagd.

Stichting Nederlandse Wetenschappelijk Onderzoekinstituten (NWO-I). De aanbestedende dienst ASTRON, het Nederlands instituut voor radioastronomie, verzoekt tot levering, installatie en oplevering van het COBALT2.0 computercluster voorzien van CPU en GPU rekenkracht, lokale opslagruimte, en snelle onderlinge netwerkverbindingen.
De enige relevante geachte open standaard (IPv4-6) is uitgevraagd.

Gemeente Maastricht. Het realiseren van een nieuwe corporate website op gemeentemaastricht.nl en een multi-site oplossing voor het beheren en creëren van veertig andere websites binnen het gemeentelijk domein. Daarnaast wil men intensief gaan samenwerken om toekomstbestendig te zijn.
De experts die de aanbestedingen hebben beoordeeld, zijn van mening dat het volgende complex van standaarden relevant is: Digitoegankelijk, DNSSEC, HTTPS en HSTS, TLS, IPv4 en IPv6, ISO 27001/27002, SAML, SPF, DKIM, DMARC en STARTTLS en DANE. In hun beoordeling zijn zij streng geweest door geen genoegen te nemen met de uitvraag van alleen IPv6 en niet ook IPv4. Anders zou deze aanbesteding zonder meer in aanmerking zijn gekomen voor de perfect-score.

Ministerie van AZ. Het leveren en beheren van een e-mailmanagementvoorziening voor het Platform Rijksoverheid Online (PRO), inclusief facultatieve dienstverlening rond optimalisatie van het e-mail-kanaal. PRO is een tool waarmee overheidsorganisaties gemakkelijk een (platform)website kunnen laten aanmaken inclusief hosting, beheer en ondersteuning. DPC faciliteert een e-maildienstverlening die content van de websites ook per e-mail aanbiedt voor gebruikers (burgers, bedrijven, professionals) van het platform.
De volgende 12 standaarden zijn in deze casus relevant: DNSSEC, HTTPS en HSTS, TLS, IPv4 en IPv6, ISO 27001/27002, SPF, DKIM, DMARC, STARTTLS en DANE, ODF, Open API Specification en PDF. Alleen om PDF is niet gevraagd (en er is niet gevraagd om IPv4 maar alleen om IPv6, zie ook de casus Maastricht). Om alle 10 de andere standaarden is gevraagd. Uit de bijlagen blijkt bovendien dat Min AZ streng is op het gebruik van de vereiste standaarden.

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 738 keer een open standaard relevant, en in 368 gevallen (50%) 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 beduidend hoger dan vorig jaar (10,3 dit jaar tegen 8,3 standaarden per aanbesteding vorig jaar, nadat vorig jaar ook al sprake was van een dergelijke stijging[12]);
- het percentage standaarden dat is uitgevraagd is 50%, dat is hoger dan vorig jaar (43%);
- de combinatie van bovenstaande twee punten betekent enerzijds dat er dit jaar per aanbesteding meer standaarden zijn uitgevraagd dan vorig jaar (5,1 versus 3,6);
- maar er zijn ook meer relevant geachte standaarden NIET uitgevraagd: het gemiddelde aantal niet-gevraagde standaarden per aanbesteding is dit jaar 5,2 (vorig jaar: 4,7); de relatieve winst is evenwel het grootst bij 'uitgevraagd'.

Dit is ook terug te zien in de scores voor 'Pas toe' per afzonderlijke standaard (zie Tabel 5, zie volgende pagina). Het aantal standaarden dat beter is uitgevraagd dan vorig jaar is groter dan het aantal standaarden die juist minder goed uitgevraagd is (procentueel gezien).

Andere zaken die opvallen bij nadere beschouwing van Tabel 5:

- Negen standaarden zijn vaker dan gemiddeld (meer dan 50%) gevraagd: HTTPS & HSTS, ISO 27001/02, SAML, STARTTLS en DANE, TLS, CMIS, PDF en StUF. In vergelijking met vorig jaar is Digitoegankelijk (voorheen: Webrichtlijnen) uit dit rijtje verdwenen. Nieuwkomers zijn STARTTLS & DANE, TLS en CMIS.
- Bij SIKB 0101 staat in de tabel weliswaar een uitvraag-percentage van 100% maar deze standaard was slechts éénmaal als relevant aangemerkt.
- Vier van de standaarden die behoorlijk vaak relevant waren (> 10 keer) laten een duidelijke stijging van de uitvraag laten zien: ISO 27001/02, XBRL, TLS en DNSSEC.
- Bij de andere standaarden die vaak relevant waren, is geen sprake flinke dalingen: als sprake is van een daling dan is die marginaal.

[12] Het aantal standaarden op de lijst voor 'pas toe of leg uit' is min of meer vergelijkbaar met vorig jaar.

Tabel 5: 'Pas toe' bij feitelijke aanbestedingen in 2018 / 2019, per standaard

(Bron: onderzoek feitelijke aanbestedingen juli 2018 t/m juni 2019, uitgevoerd zomer 2019)

	Rijksoverheid		Mede-overheden		**Totaal 2018/2019**		2017/2018
aantal aanbestedingen:	*35*		*37*		*72*		*67*
	relevant	gevraagd in % relevant	relevant	gevraagd in % relevant	relevant	gevraagd in % relevant	gevraagd in % relevant
Internet & beveiliging:							
DKIM	17	29 %	19	32 %	36	31 %	35 %
DMARC	17	29 %	19	32 %	36	31 %	35 %
DNSSEC	19	47 %	29	34 %	48	40 %	22 %
HTTPS en HSTS	32	63 %	35	60 %	67	61 %	47 %
IPv6 en IPv4	24	25 %	19	21 %	43	23 %	16 %
NEN-ISO\IEC 27001:2005nl	33	88 %	36	78 %	69	83 %	68 %
NEN-ISO\IEC 27002:2007nl	33	88 %	36	78 %	69	83 %	53 %
SAML	12	67 %	14	50 %	26	58 %	52 %
SPF	17	29 %	19	32 %	36	31 %	35 %
STARTTLS en DANE	8	50 %	5	60 %	13	54 %	0 %
TLS	32	63 %	35	60 %	67	61 %	42 %
WPA2 Enterprise	4	25 %	1	0 %	5	20 %	33 %
Document & (web)content:							
Ades Baseline Profiles	1	0 %	2	0 %	3	0 %	100 %
CMIS	3	67 %	4	75 %	7	71 %	20 %
Digitoegankelijk *)	10	30%	15	47 %	25	40 %	48 %
ODF	13	8 %	25	12 %	38	11 %	14 %
OpenAPI Specification	7	29 %	1	0 %	8	25 %	
OWMS	1	100 %	1	0 %	2	50 %	0 %
PDF	25	48 %	25	72 %	50	60 %	59 %
SKOS							
E-facturatie & administratie:							
NLCIUS	5	20 %	6	50 %	11	36 %	
SETU	1	0 %	2	50 %	3	33 %	100 %
WDO Datamodel	1	0 %			1	0 %	
XBRL	3	33 %	9	33 %	12	33 %	13 %
Stelselstandaarden:							
Digikoppeling	4	25 %	15	27 %	19	26 %	25 %
Geo−standaarden	2	100 %	5	0 %	7	29 %	0 %
StUF	1	0 %	15	87 %	16	81 %	75 %
Water & Bodem:							
Aquo Standaard							50 %
SIKB 0101			1	100 %	1	100 %	100 %
SIKB 0102							
Bouw:							
IFC							
Visi							
Juridische verwijzingen:							
BWB	2	0 %	3	0 %	5	0 %	
ECLI	2	0 %	1	0 %	3	0 %	
JCDR	2	0 %	2	0 %	4	0 %	
Onderwijs & loopbaan:							
E−portfolio	4	0 %	2	0 %	6	0 %	0 %
NL LOM	1	0 %			1	0 %	0 %
Overig:							
EML_NL			1	0 %	1	0 %	
Totaal	**336**	**50 %**	**402**	**50 %**	**738**	**50 %**	**43 %**

**) Voorheen: Webrichtlijnen. Net als voorgaande jaren alleen beoordeeld voor externe webapplicaties.*

3.4. 'Leg uit' bij feitelijke aanbestedingen

Voor twee sets van beoordeelde aanbestedingen is nagegaan in hoeverre inmiddels 'leg uit' plaatsgevonden heeft in jaarverslagen over 2018: de aanbestedingen uit Q3 en Q4 2018 die in deze Monitor 2019 zijn beoordeeld èn de set aanbestedingen uit Q1 en Q2 2018 die vorig jaar zijn beoordeeld (in het kader van de Monitor 2018).

Bij vier aanbestedingen die in het kader van deze monitor 2019 zijn beoordeeld, is om alle relevante standaarden gevraagd. Bij de andere 68 aanbestedingen had dus in het jaarverslag verantwoording afgelegd moeten worden ('Leg uit') voor het niet toepassen van de betreffende relevante standaard(en). Voor 33 van deze aanbestedingen (door 31 overheidsorganisaties, waarvan dit jaar 7 ministeries[13]) is het op dit moment mogelijk om in het Jaarverslag 2018 te controleren of 'leg-uit' is toegepast; deze 33 aanbestedingen dateren uit Q3 – Q4 2018. Voor de resterende 35 aanbestedingen kan dat pas na het verschijnen van de jaarverslagen over 2019. Van 'Leg uit' was in de jaarverslagen van deze 31 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 geen enkele verwijzing naar het standaardenbeleid teruggevonden[14].

Bij de departementen ligt dat genuanceerder. Er is naar de jaarverslagen van alle 11 ministeries gekeken, hoewel strikt genomen alleen de volgende departementen onderwerp van onderzoek zijn: Algemene Zaken, Binnenlandse Zaken, Defensie, Economische Zaken, Financiën (lees: Belastingdienst), Infrastructuur en waterstaat en VWS. Van deze zeven departementen zijn namelijk aanbestedingen beoordeeld uit Q3+Q4 2018, met een beoordeling die noodzaakt tot 'leg uit'.

Het overall-beeld voor 'Leg uit' is als volgt:

- Vijf ministeries (vorig jaar vier) hebben een vorm van verantwoording opgenomen in het jaarverslag 2018. De enige nieuwkomer in dit rijtje is het ministerie van VWS met een korte verklaring omtrent 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' (ten onrechte: dat overzicht heeft Logius dit jaar niet gepubliceerd).
- 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

[13] Te weten de ministeries van AZ, BZK, Defensie, EZ, Financiën, (lees: Belastingdienst), I&W en VWS.
[14] Ook in de gehanteerde (lokale / regionale) beleidskaders met betrekking tot inkoop en aanbesteding is geen verwijzing gevonden naar het hier bedoelde onderliggende beleid.

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	Het Ministerie van Algemene Zaken heeft geen grote ICT-projecten van meer dan € 5 miljoen uitgevoerd of gestart in 2018. Gebruik open standaarden en open source software. 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	Gebruik open standaarden en open source software Het Ministerie van BZK heeft in 2018 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. 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	[Geen]
EZ[15]	[Geen]
FIN	[Geen]
I&W	Gebruik open standaarden en open source software I & W stuurt op de door het College Standaardisatie vastgestelde open standaarden door toepassing daarvan in Project Start Architecturen (PSA). Deze worden voor zover dat mogelijk is gevolgd bij elke nieuwe ICT-toepassing. RWS heeft een standaardenlijst waarop staat welke open standaarden worden gevolgd. Op die lijst zijn ook de standaarden van het Forum Standaardisatie opgenomen. RWS beoogt op deze wijze transparant de vastgestelde open standaarden daar waar mogelijk toe te passen bij het ontwikkelen van ICT-diensten. Verder zijn er geen afwijkingen te melden ten aanzien van het gebruik van vastgestelde open standaarden. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf, onderdeel 2)*
VWS	Gebruik open standaarden Er zijn geen gevallen bekend binnen het concern VWS waarbij is afgeweken van het gebruik van open standaarden.
Geen aanbestedingen beoordeeld waarvoor 'Leg uit' noodzakelijk is	
BUZA	[Geen]
J&V	[Geen]
OCW	[Geen, maar in ROSA is wel enige aandacht voor open standaarden]
SZW	In 2017 zijn geen afwijkingen gebleken aan de eis van voldoen aan de open standaarden. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf onder 2)*

***'Leg uit'* voor aanbestedingen uit Q1+Q2 2018 (vorig jaar beoordeeld)**

In de vorig jaar verschenen Monitor 2018 zijn onder andere aanbestedingen beoordeeld uit Q1+Q2 2018. Voor 29 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 2018 nu wèl beschikbaar zijn.

Deze 29 aanbestedingen (door 25 overheidsorganisaties, waarvan 4 ministeries[16]) zijn als volgt verdeeld: 12 aanbestedingen 'Rijk' en 17 aanbestedingen 'mede-overheden'. Van 'Leg uit' in

[15] Het ministerie van LNV zal voor het eerst over 2019 een jaarverslag uitbrengen.

[16] Te weten de ministeries van BZK, Buitenlandse Zaken, I&W en SZW.

strikte zin was in de jaarverslagen van deze 25 overheidsorganisaties evenmin sprake. In geen van de jaarverslagen wordt een concrete aanbesteding genoemd waarbij volgens het onderzoek van vorig jaar van de lijst voor 'pas toe of leg uit' werd afgeweken.

Evenals in voorgaande jaren kan worden vastgesteld dat de regels met betrekking tot 'leg uit' er nog niet toe hebben geleid, dat overheden zich in jaarverslagen over specifieke aanbestedingen (en daarvoor relevante open standaarden) verantwoorden voor het niet toepassen van relevante open standaarden. In vergelijking met de verslaglegging over 2017 in de monitor 2018 valt op dat dit jaar bij één departement een verwijzing naar het beleid rond de toepassing van open standaarden is verschenen in het jaarverslag 2018 (het ministerie van VWS). Afgezien daarvan zijn de bevindingen met betrekking tot het 'Leg uit' principe over 2018 min of meer gelijk aan de voorgaande jaren (2011 tot en met 2017).

3.5. Welke open standaarden waren relevant bij feitelijke 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 (in 2017: 28 van de 39), de andere 8 waren dus voor geen van de 72 onderzochte aanbestedingen relevant. Daarvan was er vier ook vorig jaar voor geen enkele onderzochte aanbesteding relevant: Aquo, SIKB 0102, IFC en Visi. Voor de overige vier standaarden[17] geldt dat zij dit jaar voor het eerst zijn meegenomen bij de beoordeling waardoor een vergelijking met de vorige monitor niet aan de orde is.

Een vijftal standaarden steekt er met kop en schouders bovenuit als het gaat om de mate waarin zij relevant worden geacht: ISO 27001/02 zijn bijna altijd relevant (96%) en ook TLS (93%), HTTPS & HSTS (93%) en in iets mindere mate PDF (69%) scoren hoog. Deze standaarden vormden ook vorig jaar de kopgroep. Als we als criterium aanhouden 'bij meer dan 50% van de 72 aanbestedingen relevant', dan kunnen aan dit rijtje nog drie standaarden worden toegevoegd: DNSSEC (67%), IPv4 & IPv6 (60%) en ODF (53%).

Daarna volgt een groep van zes standaarden die bij 25 tot 50% van de aanbestedingen relevant was: DKIM, DMARC en SPF (elk met 50%), SAML (36%), Digitoegankelijk (35%) en Digikoppeling (26%). Het geheel overziend is sprake van een constante groep standaarden die relatief hoge percentages scoort.

[17] Dit betreft COINS, NLCS, OpenAPI specification en STIX & TAXII. Voor NLCIUS geldt dat niet, omdat deze standaard het Semantisch model e-factureren vervangt en daarmee wordt vergeleken.

Tabel 6: Open standaarden relevant / gevraagd bij feitelijke aanbestedingen in 2018/2019

(Bron: onderzoek feitelijke aanbestedingen juli 2018 t/m juni 2019, uitgevoerd zomer 2019)

	Rijksoverheid		Mede-overheden		**Totaal 2018/2019**	
aantal aanbestedingen:	*35*		*37*		*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	49 %	14 %	51 %	16 %	**50 %**	**15 %**
DMARC	49 %	14 %	51 %	16 %	**50 %**	**15 %**
DNSSEC	54 %	26 %	78 %	27 %	**67 %**	**26 %**
HTTPS en HSTS	91 %	57 %	95 %	57 %	**93 %**	**57 %**
IPv6 en IPv4	69 %	17 %	51 %	11 %	**60 %**	**14 %**
NEN-ISO\IEC 27001:2005nl	94 %	83 %	97 %	76 %	**96 %**	**79 %**
NEN-ISO\IEC 27002:2007nl	94 %	83 %	97 %	76 %	**96 %**	**79 %**
SAML	34 %	23 %	38 %	20 %	**36 %**	**21 %**
SPF	49 %	14 %	51 %	16 %	**50 %**	**15 %**
STARTTLS en DANE	23 %	11 %	14 %	8 %	**18 %**	**10 %**
TLS	91 %	57 %	95 %	57 %	**93 %**	**57 %**
WPA2 Enterprise	11 %	3 %	3 %	0 %	**7 %**	**1 %**
Document & (web)content:						
Ades Baseline Profiles	3 %	0 %	5 %	0 %	**4 %**	**0 %**
CMIS	9 %	6 %	11%	8 %	**10 %**	**7 %**
Digitoegankelijk *)	29 %	9 %	41 %	19 %	**35 %**	**14 %**
ODF	37 %	3 %	68 %	8 %	**53 %**	**6 %**
OpenAPI Specification	20 %	3 %	3 %	0 %	**11 %**	**1 %**
OWMS	3 %	3 %	3 %	0 %	**3 %**	**1 %**
PDF	71 %	34 %	68 %	49 %	**69 %**	**42 %**
SKOS						
E-facturatie & administratie:						
NLCIUS	14 %	3 %	16 %	8 %	**15 %**	**6 %**
SETU	3 %	0 %	5 %	3 %	**4 %**	**1 %**
WDO Datamodel	3 %	0 %			**1 %**	**0 %**
XBRL	9 %	3 %	24 %	8 %	**17 %**	**6 %**
Stelselstandaarden:						
Digikoppeling	11 %	3 %	41 %	11 %	**26 %**	**7 %**
Geo−standaarden	6 %	6 %	14 %	0 %	**10 %**	**3 %**
StUF	3 %	0 %	41 %	35 %	**22 %**	**18 %**
Water & Bodem:						
Aquo Standaard						
SIKB 0101			3 %	3 %	**1 %**	**1 %**
SIKB 0102						
Bouw:						
IFC						
Visi						
Juridische verwijzingen:						
BWB	6 %	0 %	8 %	0 %	**7 %**	**0 %**
ECLI	6 %	0 %	3 %	0 %	**4 %**	**0 %**
JCDR	6 %	0 %	5 %	0 %	**6 %**	**0 %**
Onderwijs & loopbaan:						
E−portfolio	11 %	0 %	5 %	0 %	**8 %**	**0 %**
NL LOM	3 %	0 %			**1 %**	**0 %**
Overig:						
EML_NL			3 %	0 %	**1 %**	**0 %**

**) Voorheen: Webrichtlijnen. Net als voorgaande jaren alleen beoordeeld voor externe webapplicaties.*

Aan de andere kant: van de 33 standaarden die bij de beoordeelde aanbestedingen relevant werden geacht, zijn er dit jaar 5 slechts incidenteel (1 of 2 keer) als relevant aangemerkt (vorig jaar waren dat er 7): OWMS twee keer, en EMN_NL, NL LOM, SIKB 0101 en WDO Datamodel elk één keer. In vergelijking met vorig jaar beperkt de overlap zich tot OWMS en SIKB 0101. Vijf standaarden zijn uit deze opsomming verdwenen; ofwel omdat ze dit jaar bij geen enkele aanbesteding relevant zijn (Aquo), ofwel omdat ze bij meer dan 2 aanbestedingen relevant zijn (Ades, Geo-standaarden, STARTTLS & DANE en SETU).

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, de combinatie DKIM, DMARC en SPF en STARTTLS & DANE. Echte uitschieters de andere kant op – veel minder vaak 'relevant' dan vorig jaar – zijn er niet. ODF was de voorgaande twee jaren de meest in het oog springende daler. Dit jaar loopt de score van ODF weer op (van 43% naar 53% relevant).

In vergelijking met de vorige monitor is er één standaard deze keer bij geen enkele aanbesteding relevant gebleken en vorig jaar wel: de Aquo-standaard. Daarbij moet wel worden aangetekend dat de relevantie van deze standaard vorig jaar ook al niet groot was. Andersom zijn er zes standaarden dit jaar wel relevant en vorig jaar niet (afgezien van de standaarden die vorig jaar vanwege recente plaatsing op de lijst niet waren meegenomen). Hierbij gaat het om de drie juridische standaarden (BWB, ECLI en JCDR) en verder NL LOM, EMN_NL en WDO Datamodel.

Voor de feitelijke adoptie is uiteraard niet alleen van belang hoe vaak de standaard relevant bleek te zijn, maar vooral hoe vaak er daadwerkelijk om is gevraagd. Zoals al bleek in paragraaf 3.2 is er dit jaar bij aanbestedingen vaker dan vorig jaar om de relevante standaarden gevraagd: 50% dit jaar tegen 43% 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 (57%) TLS (57%) en PDF (42%). Vorig jaar stonden dezelfde vijf standaarden op dit punt bovenaan.

Na dit rijtje koplopers volgt nog een achttal standaarden met een score van boven de 10%: DNSSEC (26%), SAML (21%), StUF (18%), de combinatie DKIM, DMARC en SPF (15%), Digitoegankelijk (voorheen: Webrichtlijnen) met 14% en IPv4 & IPv6, eveneens met 14%.

Om de andere standaarden is slechts bij enkele aanbestedingen gevraagd of zelfs in het geheel niet. Dit laatste is het geval bij Ades, de drie juridische standaarden (BWB, ECLI 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 juridische standaarden en E-portfolio.

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 (GDI-voorzieningen, shared services etc.). Sommige daarvan worden overheidsbreed toegepast, andere vooral door de Rijksoverheid of juist door mede-overheden. Als daarin de relevante open standaarden zijn toegepast, dan leidt ook dat tot een breder gebruik van open standaarden.

Daarom is ook dit jaar onderzocht in hoeverre de belangrijkste overheidsbrede voorzieningen (36 in totaal) voldoen aan de relevante open standaarden[18]. Hiervoor zijn 27 voorzieningen onderzocht die samen de Basisinfrastructuur (voorheen GDI) vormen[19]. Dit jaar voor het eerst inclusief de nieuwe Basisregistratie Ondergrond (BRO). Anderzijds zijn ook de 9 andere voorzieningen die vorige jaren zijn onderzocht nogmaals onderzocht.

Dit deel-onderzoek is uitgevoerd door Piet Hein Minnecré en Anne Graas (PBLQ). In Bijlage B9 is de rapportage opgenomen met alle gedetailleerde informatie per voorziening.

4.1.2. Welke voorzieningen zijn onderzocht?

Het gaat om de volgende 27 + 9 voorzieningen:

Basisinfrastructuur:		**Andere voorzieningen:**
BAG, BRK, WOZ en BGT	DigiPoort	Digi-Inkoop
Berichtenbox bedrijven	Afsprakenstelsel ETD	Digitale Werkomgeving Rijk
BRI (inkomen)	e-Factureren	Doc-Direct
BRO (ondergrond)	MijnOverheid	ODC Noord
BRT (topografie)	NHR (Nieuw HandelsRegister)	P-Direct
BRV (voertuigen)	Ondernemersplein	Rijksoverheid.nl
BSN Beheervoorz. + GBA-V	Overheid.nl	Rijkspas
DigiD	PKI Overheid	Rijksportaal
DigiD Machtigen	Samenwerkende Catalogi	TenderNed
Digilevering	SBR (Standard Business Rep.)	
Digimelding	Stelselcatalogus	
Diginetwerk		

[18] Zie ook EAR Online, voor een overzicht van voorzieningen geordend naar informatiseringsdomeinen.
[19] Niet onderzocht zijn: het eID-stelsel (moet nog worden ontwikkeld), BLAU (nog niet gerealiseerd) en NORA, en daarnaast de Standaardenlijst en de Standaarden incl. die van de Pas toe of leg uit-lijst.

4.1.3. Werkwijze

Voor dit onderzoek is gebruik gemaakt van de 'pas toe of leg uit'-lijst van 1 mei 2019. Per voorziening is gekeken of de standaarden op deze lijst relevant zijn. Daarbij is telkens uitgegaan van de eindgebruiker. Dat is diegene die in de keten baat zou moet hebben bij het gebruik van open standaarden. Dit is expliciet zo gekozen, omdat het beleid gericht is op het stimuleren van interoperabiliteit. In eerdere onderzoeken is gebleken dat beheerders van voorzieningen soms termen gebruiken als 'voorbereid' zijn op een standaard, een standaard 'deels geïmplementeerd' hebben of 'standaard XYZ-ready' zijn. Hiermee bedoelen zij dat ze zelf voldoen aan de standaard of bezig zijn deze 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[20]. Daarnaast is nagegaan – voor zover mogelijk – of vorig jaar 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.

Dit leidt tot een eerste overzicht per voorziening. Dat overzicht wordt met enkele expliciete vragen toegestuurd aan de vertegenwoordigers van de voorzieningen. Op basis van hun reactie wordt de verzamelde informatie aangescherpt. Het resultaat wordt voorgelegd aan de opdrachtgever, waarna 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. Daar waar verschillen ook na de gesprekken bleven bestaan, is dit duidelijk opgenomen in de rapportage.

4.1.4. Aandachtspunten voor de lezer

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

[20] Deze toets is bruikbaar voor een groot deel van de voorzieningen. Er zijn enkele uitzonderingen, vaak betreft dat 'besloten' voorzieningen die niet publiek via internet toegankelijk zijn.

Relevant of niet relevant
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. 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 is lastig om te toetsen wanneer een voorziening aan een standaard voldoet. Het vereist een heldere afbakening van de voorziening en heldere voorwaarden voor wanneer voldaan wordt aan een standaard. Daarnaast zou het toetsen 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 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 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
Voor een groot aantal standaarden hebben we gebruik gemaakt van de website internet.nl. De website is een initiatief van het Platform Internetstandaarden en maakt het mogelijk om het gebruik van standaarden te toetsen op basis van een specifiek domein. Het betreft de volgende standaarden:

- IPv4 en IPv6
- HTTPS & HSTS
- DMARC
- DKIM
- SPF
- STARTTLS & 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.

Het besluit verplicht overheidsinstanties om te zorgen dat hun websites en/of mobiele applicaties toegankelijk zijn conform de geldende standaard EN 301 549, en daarover een actuele toegankelijkheidsverklaring af te geven. Er geldt een gefaseerde toepassing. Nieuwe websites gepubliceerd vanaf 23 september 2018 moesten uiterlijk op 23 september 2019 voldoen. Bestaande website gepubliceerd vóór 23 september 2018 moeten een jaar later voldoen. Mobiele applicaties moeten uiterlijk 23 juni 2021 voldoen.

Ten tijde van dit onderzoek wordt een nulmeting uitgevoerd naar het gebruik van de standaard Digitoegankelijk door overheden op basis van een Europees vastgestelde methodiek. Deze resultaten worden in de loop van 2019 verwacht en worden toegezonden aan de Tweede Kamer. In dat licht is in overleg met het Forum Standaardisatie en het Centrum voor Standaarden besloten de standaard niet nogmaals apart te onderzoeken voor deze monitor en wordt volstaan om hier te verwijzen naar de conclusies van dit rapport.

ISO 27001/2, BIR en BIO
Binnen de rijksoverheid dient elke organisatie een eigen implementatie van de BIR te hebben. De BIR is gebaseerd op ISO 27001. Indien een organisatie voldoet aan de BIR, 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.

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. Veel partijen zijn momenteel al bezig met de transitie naar de BIO. Hier is in de beoordeling rekening mee gehouden.

4.2. Overzicht: open standaarden in overheidsbrede voorzieningen

In Tabel 8a + 8b zijn de bevindingen over de 36 onderzochte overheidsbrede voorzieningen in één overzicht samengebracht. In de rapportage van PBLQ, opgenomen in Bijlage B9, wordt het beeld van de mate waarin elke voorziening aan de relevante open standaarden

voldoet gedetailleerd besproken. Het gaat om de 27 onderzochte voorzieningen van de Basisinfrastructuur (voorheen GDI), plus de 9 andere onderzochte voorzieningen.

4.2.1. Per standaard beschouwd

Van alle 41 open standaarden op de 'pas toe of leg uit'-lijst zijn er 28 relevant voor één of meer overheidsbrede voorzieningen. Er zijn 12 open standaarden die voor meer dan 20 voorzieningen relevant zijn:

- IPv6+IPv4 (relevant voor 33 van de 36 voorzieningen),
- DMARC en HTTPS+HSTS (beide relevant voor 31 voorzieningen),
- TLS (relevant voor 30),
- en verder DNSSEC (29), NEN-ISO\IEC 27001 en NEN-ISO\IEC 27002 (28), SPF (26), DKIM (25), PDF (22), STARTTLS+DANE (21) en Digikoppeling (20).

De mate waarin voorzieningen aan de standaard (als die relevant is) voldoen is hoog: voor 14 van de 28 open standaarden geldt dat tenminste 80% van de voorzieningen aan die standaard voldoet. Het gaat om de volgende 14 open standaarden:

- TLS (25 van de 30 voorzieningen voldoet daaraan),
- NEN-ISO\IEC 27001 en 27002 (alle 28 voorzieningen),
- SPF (21 van de 26),
- en verder PDF (20 van de 22), SAML (13 van de 15), OpenAPI Specification (8 van de 10), Geo-standaarden (alle 6 de voorzieningen), BWB (5 van de 6), WPA2 Enterprise, SETU en XBRL (alle 2), en tenslotte Aquo standaarden en JCDR (relevant voor één voorziening en die voldoet er aan).

Van deze 14 standaarden vallen er 6 in het domein 'Internet & beveiliging'.

Vijf standaarden scoren relatief laag: van de voorzieningen waarvoor deze relevant zijn voldoet er geen enkele aan NLCIUS, en voldoet 20% van de voorzieningen aan CMIS, 27% aan IPv4+IPv6, 38% aan STARTTLS & DANE en 40% aan SKOS. Daarvan is alleen NLCIUS relatief nieuw op de lijst (sinds 2018), de andere staan al langer op de lijst (IPv4+IPv6 zelfs al 9 jaar).

De verschillen tussen de domeinen zijn groot: in totaal was 417 keer een standaard relevant, en daarbij ging het 299 keer (72%) om een standaard van het domein Internet & Beveiliging. Daarnaast ging het 64 keer (15%) om een standaard van Document en Webcontent, 35 keer (8%) om Stelselstandaarden en 19 keer (5%) om standaarden van de 6 andere domeinen.

4.2.2. Per voorziening beschouwd

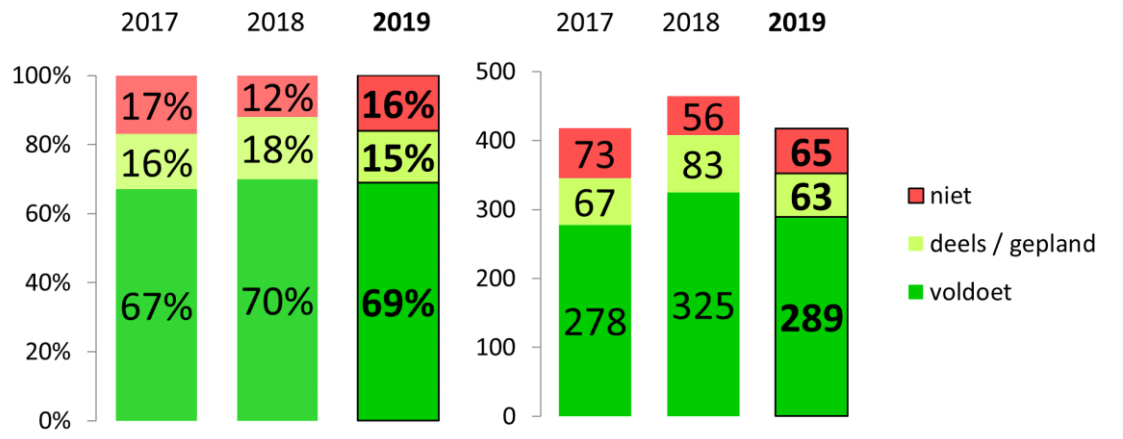
Voor een deel van de voorzieningen zijn relatief veel open standaarden relevant, zoals voor:

- de NHR (Basisregistratie Handelsregister: 19 standaarden),
- de basisregistraties BAG, BRK, WOZ, BGT en BRV (17 standaarden),
- P-Direct (16), Digitale Werkomgeving Rijk, Doc-Direct en MijnOverheid (15),
- BSN Beheervoorziening+GBA-V, ODC Noord, Overheid.nl en Rijksoverheid.nl (14) en
- BRO, Ondernemersplein en TenderNed (13).

Voor andere voorzieningen zijn slechts enkele open standaarden relevant, zoals voor BRI (5), Diginetwerk (4) en e-Factureren (1).

Gemiddeld zijn voor een voorziening 11,6 open standaarden relevant. Vorig jaar waren dat er nog ruim 13 per voorziening (maar toen stonden de drie PDF-varianten nog ieder apart op de lijst, bovendien is dit jaar DigiToegankelijk niet getoetst) en het jaar daarvoor waren het er gemiddeld 12 per voorziening.

Figuur 7: Toepassing open standaarden in 36 voorzieningen: in % en absolute aantallen



In de meeste gevallen voldoen deze voorzieningen ook aan de relevante open standaarden (zie Figuur 7): in 417 gevallen (combinaties van voorziening en relevante standaard) is een standaard van de lijst relevant, in 289 gevallen (69%, vorig jaar 70%) voldoet de voorziening daar aan en in 63 gevallen (15%, vorig jaar was dat 18%) voldoet de voorziening daar deels aan of is dat gepland. In 65 gevallen (16%, vorig jaar 12%) voldoet de voorziening op dit moment nog niet aan een relevante open standaard.

In absolute aantallen (zie vierde tot en met zesde kolom in Figuur 7) lijkt het aantal gevallen waarin aan open standaarden wordt voldaan gedaald van 325 vorig jaar tot 289 dit jaar. Het beeld wordt echter vertekend doordat (a) met ingang van dit jaar PDF als één standaard op de lijst staat en niet meer als drie aparte standaarden en (b) doordat dit jaar niet op DigiToegankelijk is getoetst (zie paragraaf 4.1.4 voor een toelichting). Gezien de scores van vorig jaar voor PDF en DigiToegankelijk zou dat 66 gevallen schelen waarin door een voorziening aan een open standaard wordt voldaan, en zou het totaal dit jaar zonder deze veranderingen met 289 + 66 = 355 juist iets hóger zijn dan vorig jaar.

De totaalcijfers over de toepassing van open standaarden bij voorzieningen laten dus zien dat een heel behoorlijk niveau van toepassing bereikt is: van alle 417 gevallen waarin een standaard voor een voorziening relevant is wordt daar in 84 % van de gevallen aan voldaan of deels voldaan of zijn er concrete plannen om daaraan te voldoen. Maar er is nog geen sprake van volledige compliancy, en de ontwikkeling lijkt enigszins te stagneren.

Bekijken we de voorzieningen apart, dan blijkt dat slechts één voorziening voldoet aan alle relevante standaarden: BasisRegistratie Inkomen (5 standaarden, op basis van gegevens van vorig jaar). Daarnaast zijn er negen voorzieningen die aan alle standaarden ofwel voldoen, danwel deels voldoen danwel concrete plannen hebben om daar op korte termijn aan te gaan voldoen (ook vorig jaar waren dat er negen). Voor 10 van de 36 onderzochte

voorzieningen geldt dus, dat zij aan alle standaarden ofwel voldoen, danwel deels voldoen danwel gepland hebben om daar op korte termijn aan te gaan voldoen. Al deze tien voorzieningen maken deel uit van de Basisinfrastructuur (voorheen GDI).

Omgekeerd: als we kijken naar het aantal relevante standaarden waaraan een voorziening niet voldoet, ook niet deels en ook niet gepland, dan scoren de volgende voorzieningen relatief slecht:

- e-Factureren (voldoet niet aan de enige relevante standaard NLCIUS = 100%),
- Rijksportaal (voldoet niet aan 4 van de 8 relevante standaarden = 50%),
- Berichtenbox Bedrijven (5 van de 11 relevante standaarden niet = 45%),
- BSN Beheervoorziening+GBA-V (6 van de 14 relevante standaarden niet = 43%).

Hierbij moet in gedachten gehouden worden, dat het 'pas toe of leg uit'-principe betrekking heeft op aanbesteding, inkoop of ontwikkeling van ICT-systemen en daarmee dus alleen op nieuwe voorzieningen en op de vernieuwing van bestaande voorzieningen. Het (gaan) voldoen aan open standaarden vindt dus plaats op het moment dat een bestaande voorziening aan vernieuwing toe is (anders zou een – mogelijk omvangrijke – des-investering nodig kunnen zijn om aan open standaarden te voldoen).

Vergeleken bij vorig jaar heeft vooral P-Direct zich sterk verbeterd: vorig jaar voldeden zij aan 39% (7 van de 18 relevante standaarden), dit jaar aan 69% (11 van de 16). Dat geldt ook voor Samenwerkende Catalogi: van vorig jaar 25% (1 van de 4 relevante standaarden) naar dit jaar aan 43% (3 van de 7). Ook een duidelijke verbetering is er bij: Digitale Werkomgeving Rijk (van 56% naar 80% voldoet, 12 van de 15 relevante standaarden) en bij Digilevering (van 63% naar 88% voldoet, 7 van de 8 relevante standaarden).

Tabel 8a: Toepassing open standaarden in 36 voorzieningen

		Identificeren & authenticeren						Dienstverlening & informatieverstrekken									
	V = voldoet *D = voldoet deels* *G = gepland* *N = voldoet niet* *(leeg = n.v.t.)*	DigiD	DigiD Machtigen	PKI Overheid	BSN Beheervz + GBA-V (x2)	Stelsel ETD	Rijkspas	MijnOverheid	Berichtenbox bedrijven	Overheid.nl	Ondernemersplein	Samenwerkende Catalogi	Rijksportaal	ODC Noord	Doc-Direct	Rijksoverheid.nl	*aantal keer relevant*
	aantal relevante OSn	*11*	*11*	*9*	*14*	*12*	*11*	*15*	*11*	*14*	*13*	*7*	*8*	*14*	*15*	*14*	*179*
Internet & beveiliging	DKIM	V				V	G	V	N	V	D		N	V	V	V	*11*
	DMARC	V	V	V		G	N	V	N	V	V	G	V	V	V	N	*14*
	DNSSEC	V	V	V		V	G	V	V	V	D		N	V		V	*12*
	HTTPS & HSTS	V	V	D	V	V		V	V	G	D	G		D	D	V	*14*
	IPv4 & IPv6	V	V	G	N	D	N	D	N	V	D	V	N	G	V	D	*16*
	NEN-ISO\IEC 27001	V	V	V	V	V	V	V		V	V			V	V	V	*13*
	NEN-ISO\IEC 27002	V	V	V	V	V	V	V		V	V			V	V	V	*13*
	SAML	V	D			V	V	V	V				V	G	V		*9*
	SPF	V	V			V	V	V	N		D	G	N	V	V	V	*12*
	STARTTLS & DANE	G				V	N	V		V	N			N		V	*8*
	STIX en TAXII																*0*
	TLS	V	V	V	V	V	V	V	N	G	V	G		D	N	V	*15*
	WPA2 Enterprise													V			*1*
Document & (web)content	AdES Baseline Prof.														N		*1*
	CMIS										N				N		*2*
	Digitoegankelijk																*0*
	ODF 1.2												V		N	V	*3*
	OpenAPI Specific.							V				V					*2*
	OWMS			V						V	N	V		G		V	*6*
	PDF (NEN)		V	V		V		V	V	V			V	D	V	D	*10*
	SKOS									V					N		*2*
E-facturatie & administratie	NLCIUS																*0*
	SETU																*0*
	WDO Datamodel																*0*
	XBRL																*0*
Stelselstandaarden	Digikoppeling		D		N		V	V	V						N		*7*
	Geo-standaarden																*0*
	StUF				N			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									V							*1*
	JCDR																*0*
Onderwijs & erkenning	e-Portfolio																*0*
	NL_LOM																*0*
	EML_NL																*0*

Tabel 8b: Toepassing open standaarden in 36 voorzieningen

		Gegevens & registreren										Dienstverlening & verbinden							
	V = voldoet *D = voldoet deels* *G = gepland* *N = voldoet niet* *(leeg = n.v.t.)*	NHR (Nieuw HandelsReg.)	BAG, BRK, WOZ en BGT (x4)	BRO (ondergrond)	BRT (topografie)	BRV (voertuigen)	BRI (inkomen)	Digilevering	Digimelding	Stelselcatalogus	P-Direct	e-Factureren	SBR (Standard Bus. Rep.)	DigiPoort	Diginetwerk	TenderNed	Dig. Werkomgeving Rijk	Digi-Inkoop	*antal keer relevant*
	aantal relevante OSn	*19*	*68*	*13*	*9*	*17*	*5*	*8*	*8*	*7*	*16*	*1*	*11*	*12*	*4*	*13*	*15*	*12*	238
Internet & beveiliging	DKIM	V	V			V		V	G		V		N	V		V	V	V	*14*
	DMARC	V	V		V	D	V	V	V	V	V		N	G		N	N	V	*17*
	DNSSEC	N	V	V		D		V	V	V	N		V	G	G	V	V	V	*17*
	HTTPS & HSTS	V	D	V	D	D		V	V	G	V		V	V		N	G	V	*17*
	IPv4 & IPv6	D	V	D		N		N	N	N	N		D	N	G	N	G	N	*17*
	NEN-ISO\IEC 27001	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	*15*
	SAML	V		V		V					V					V	V		*6*
	SPF	V	V			V		V	V		V		V	G		V	V	V	*14*
	STARTTLS & DANE	D	N		N	V		V	N		N		N			V	V		*13*
	STIX en TAXII																		*0*
	TLS	V	V	V	V	V	V				V		V	V		V	V	V	*15*
	WPA2 Enterprise																V		*1*
Document & (web)content	AdES Baseline Prof.	V									N		V						*3*
	CMIS	D		V		N													*3*
	Digitoegankelijk																		*0*
	ODF 1.2										N						V		*2*
	OpenAPI Specific.	D	V	V		V										N			*8*
	OWMS				N	V													*2*
	PDF (NEN)	V	V			V				V	V		V			V	V	V	*12*
	SKOS	N	D		V	V				V									*8*
E-facturatie & administratie	NLCIUS	N	N									N						N	*7*
	SETU													V				V	*2*
	WDO Datamodel																		*0*
	XBRL												V	V					*2*
Stelselsta ndaarden	Digikoppeling	V	D	V		D	V	V	V		V			V			V		*13*
	Geo-standaarden		V	V	V														*6*
	StUF	V	V																*5*
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 & leerloopbg	e-Portfolio																		*0*
	NL_LOM																		*0*
Overig	EML_NL																		*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.

Dit deel-onderzoek is dit jaar uitgevoerd door de accountmanagers van BFS. Dit heeft geleid tot de notitie *'Inventarisatie gebruiksgegevens 2019 door BFS'* (zie bijlage B6).

Daarnaast doet BFS elk halfjaar onderzoek naar internet-veiligheids-standaarden, een deel van de gebruiksgegevens is afkomstig uit de *'Meting Informatieveiligheidstandaarden maart 2019'* (zie bijlage B7).

5.1. Gebruiksgegevens 2019: inventarisatie door accountmanagers BFS

In de notitie *'Inventarisatie gebruiksgegevens 2019 door BFS'* (zie bijlage B6) 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 9 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.

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 (48%, maar wel stijgend), DANE (41%, ook stijgend) en STARTTLS (67%, ook stijgend).
Voor verschillende standaarden uit het domein ***Document & (web)content*** is dit jaar een begin gemaakt met een nulmeting van gebruiksgegevens. Voor de meeste andere domeinen en standaarden zijn nauwelijks cijfers beschikbaar.

Tabel 9: Gebruiksgegevens 2019, per standaard

	Beeld BFS		Resultaten IV-meting
	ontwikkeling t.o.v. 2018	gebruiksgegevens	OBDO: eind 2018 100% conform NCSC
Internet & beveiliging:			
DKIM	toegenomen	van 84% naar 89%	89 %
DMARC	toegenomen	van 73% naar 82%	82 %
DNSSEC	toegenomen	van 90% naar 93%	93 %
HTTPS	licht toegenomen	van 89% naar 90%	HTTPS cf 90 %
en HSTS		was 79% blijft 79%	HSTS cf 79 %
IPv6 en IPv4	toegenomen	van 29% naar 48%	
NEN-ISO\IEC 27001:2005nl		*[geen cijfers]*	
NEN-ISO\IEC 27002:2007nl		*[geen cijfers]*	
SAML	toegenomen	van 757 naar 868	
SPF	toegenomen	van 93% naar 95%	95 %
STARTTLS	toegenomen	cf: van 55% naar 67%	STARTTLS cf 67 %
en DANE		van 25% naar 41%	DANE 41 %
STIX & TAXII		*[geen cijfers]*	
TLS	licht toegenomen	cf: van 87% naar 89%	TLS cf 89 %
WPA2 Enterprise	toegenomen	van 459 naar 529	
Document & (web)content:			
Ades Baseline Profiles	toegenomen	*[geen cijfers]*	
CMIS		*NIET ONDERZOCHT*	
Digitoegankelijk		*NIET ONDERZOCHT*	
ODF	onbekend	(nulmeting: 6,7%)	
OpenAPI Specification		*[geen cijfers]*	
OWMS	onbekend	(nulmeting: 38%)	
PDF	onbekend	(nulmeting: 99,9%)	
SKOS	onbekend	(nulmeting: 74% ?)	
E-facturatie & administratie:			
NLCIUS	onbekend	(nulmeting: 15%)	
SETU	wsch. licht gestegen	*(wsch. veel toegepast)*	
WDO Datamodel	toegenomen	*(wsch. veel toegepast)*	
XBRL	toegenomen	*(wsch. veel toegepast)*	
Stelselstandaarden:			
Digikoppeling	toegenomen	van 96% naar 100%	
Geo−standaarden	toegenomen	*(wsch. veel toegepast)*	
StUF	toegenomen	*(wsch. veel toegepast)*	
Water & Bodem:			
Aquo Standaard		*[geen cijfers]*	
SIKB 0101		*[geen cijfers]*	
SIKB 0102		*[geen cijfers]*	
Bouw:			
COINS		GEEN REACTIE	
IFC		*[geen cijfers]*	
NLCS		GEEN REACTIE	
Visi		GEEN REACTIE	
Juridische verwijzingen:			
BWB	gelijk gebleven	LiDO: 40.000 /maand	
ECLI	gelijk gebleven	LiDO: 40.000 /maand	
JCDR	gelijk gebleven	LiDO: 40.000 /maand	
Onderwijs & loopbaan:			
E−portfolio		*NIET ONDERZOCHT*	
NL LOM		*NIET ONDERZOCHT*	
Overig:			
EML_NL		*(wsch. veel toegepast)*	

5.2. Gebruiksgegevens 2019: resultaten IV-meting

In het OBDO hebben de overheden afgesproken dat volledige adoptie 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).

Uit de '*Meting Informatieveiligheidstandaarden maart 2019*' (zie bijlage B7, de uitkomsten zijn opgenomen in de kolom 'Resultaten IV-meting' van Tabel 9) blijkt dat het streefbeeld voor eind 2018 (100%) op het moment van de meting – maart 2019 – nog niet was gerealiseerd.

Van de webstandaarden wordt DNSSEC het meest toegepast (93%), gevolgd door HTTPS conform NCSC (90%) en TLS conform NCSC (89%). HSTS conform NCSC is iets minder ver gevorderd (79%). De afspraken voor eind 2018 zijn dus nog niet helemaal gerealiseerd.

Van de mailstandaarden wordt SPF (95%) het meest toegepast, gevolgd door DKIM (89%) en DMARC (82%). De afspraken voor eind 2018 zijn voor deze drie standaarden dus 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 (67%) en DANE (41%).

Meest recente IV-meting

De voorgaande cijfers zijn gebaseerd op de meting uit maart 2019 (die de basis vormde voor een deel van de gebruiksgegevens in Hoofdstuk 5 en Bijlage B7). In Bijlage B8 is de meeste recente IV-meting opgenomen, uit september 2019.

Uit deze meting blijkt enerzijds, dat de adoptie voor de betreffende standaarden verder is toegenomen. Maar niet voldoende om het streefbeeld voor eind 2018 (100%) helemaal te bereiken. Niet voor de webstandaarden: de adoptie van DNSSEC steeg van 93% naar 94%, HTTPS conform NCSC van 90% naar 94% en TLS conform NCSC van 89% naar 92%. Het sterkst steeg HSTS conform NCSC: van 79% naar 85%. Ook voor de mailstandaarden is het streefbeeld voor eind 2018 nog niet bereikt: de adoptie van SPF steeg van 95% naar 96%, DKIM van 89% naar 90%, DMARC van 82% naar 87% en STARTTLS conform NCSC van 67% naar 76%. Vooral DANE heeft nog een eind te gaan, de adoptie is gestegen van 41% naar 45%.

BIJLAGEN

B1. Flyer: Lijst verplichte open standaarden (september 2018)

B2. Standaarden gerangschikt naar lagen

B3. Stroomschema: Pas toe of leg uit in het kort

B4. Instructie Rijksdienst (inclusief toelichting)

B5. Overzicht van de beoordeelde aanbestedingen 2018/2019

B6. Inventarisatie gebruiksgegevens 2019 door BFS

B7. Rapportage IV-meting maart 2019

B8. Rapportage IV-meting maart 2019

B9. Rapportage Open standaarden en voorzieningen (PBLQ)

B1. Flyer: Lijst verplichte open standaarden (september 2018)

Lijst **verplichte open standaarden**

PAS TOE OF LEG UIT

VERSIE SEPTEMBER 2018

Internet en beveiliging	
DKIM	Preventie van mailspoofing/phishing
DMARC	Anti-phishing
DNSSEC	Beveiligde domeinnamen
HTTPS en HSTS	Beveiligd, versleuteld webverkeer
IPv4 & IPv6	Internetnummers
ISO 27001	Managementsysteem informatiebeveiliging
ISO 27002	Richtlijnen en principes informatie-beveiliging
SAML	Authenticatie
SPF	Preventie van mailspoofing/phishing
STARTTLS en DANE	Beveiligd, versleuteld mailverkeer
STIX / TAXII	Uitwisseling van dreigingsinformatie
TLS	Beveiligde, versleutelde verbindingen
WPA 2 Enterprise	Toegang tot een WiFi-netwerk met account

Document en (web/app)content	
AdES Baseline Profiles	Digitaal ondertekenen van documenten
CMIS	Content-uitwisseling tussen CMS-/DMS-systemen
Digitoegankelijk	Toegankelijkheid web content
OpenAPI Specification	Beschrijven van REST APIs
ODF	Documentbewerkingen
OWMS	Metadata overheidsinformatie
PDF 1.7/A1/A2	Documentpublicatie/archivering
SKOS	Thesauri en begrippenwoordenboeken

E-facturatie en administratie	
NLCIUS	Elektronisch factureren
SETU	Informatie flexibele arbeidskrachten
WDO Datamodel	Douane-informatie
XBRL	Bedrijfsrapportages

Stelselstandaarden	
Digikoppeling	Veilige berichtenuitwisselingen
Geo-standaarden	Geografische informatie
StUF	Uitwisseling administratieve overheids-gegevens

Water en bodem	
Aquo-standaarden	Waterbeheer
SIKB0101	Milieutechnische bodeminformatie
SIKB0102	Archeologische bodeminformatie

Bouw	
COINS	BIM uitwisselingsstandaard
IFC	Bouwwerkinformatiemodellen
NLCS	2D tekenstandaard
VISI	Bouwprocesinformatie

Juridische identificatie en verwijzing	
BWB	Wet- en regelgeving
ECLI	Rechterlijke uitspraken
JCDR	Decentrale regelgeving

Onderwijs en loopbaan	
e-Portfolio	Uitwisseling werkervaring en competenties
NL_LOM	Metadata onderwijscontent

Overig	
EML_NL	Verkiezingsgegevens
STOSAG	Afvalinzameling en -verwerkingen

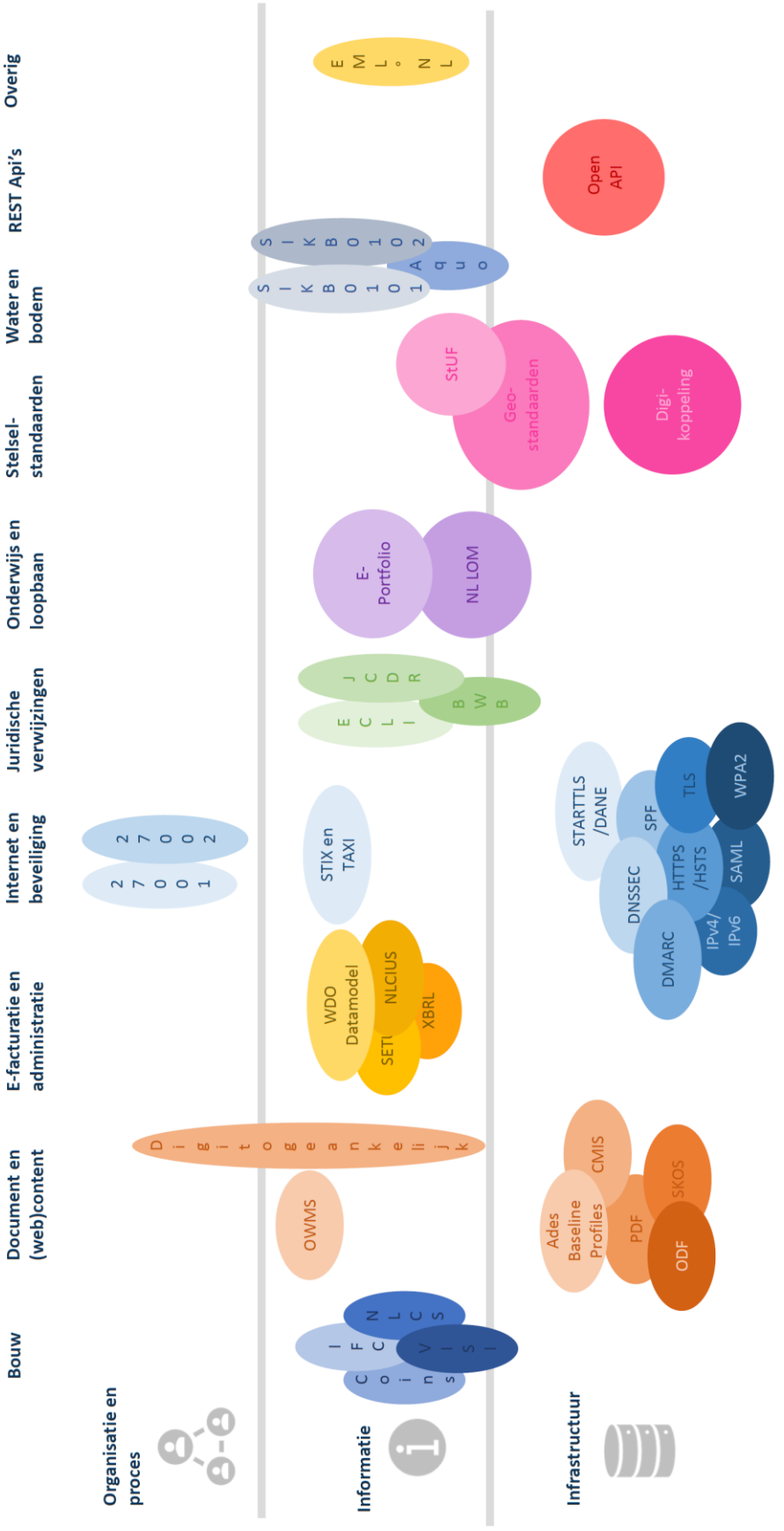
Een open overheid werkt met open standaarden. Gebruik van open standaarden zorgt voor interoperabiliteit, kostenbesparingen, digitale duurzaamheid, flexibiliteit, innovatie en meer vrijheid in de keuze voor leveranciers.

Forum Standaardisatie beheert de lijst met verplichte open standaarden voor digitale gegevensuitwisseling. Overheden en organisaties in de publieke sector zijn verplicht de relevante open standaarden uit deze lijst te kiezen bij aanschaf van ICT-producten en -diensten vanaf € 50.000. Afwijken van deze verplichte open standaarden mag, maar alleen met een zwaarwegende reden die terug te vinden is in het jaarverslag. Pas toe of leg uit.

Kijk op www.forumstandaardisatie.nl voor de meest actuele versie van de lijst verplichte open standaarden. Neem contact op met het Bureau Forum Standaardisatie voor hulp bij de beoordeling of een open standaard relevant is in een aanbesteding, het aanmelden van een nieuwe standaard of overige vragen: info@forumstandaardisatie.nl. Bellen kan ook: 070 888 77 76

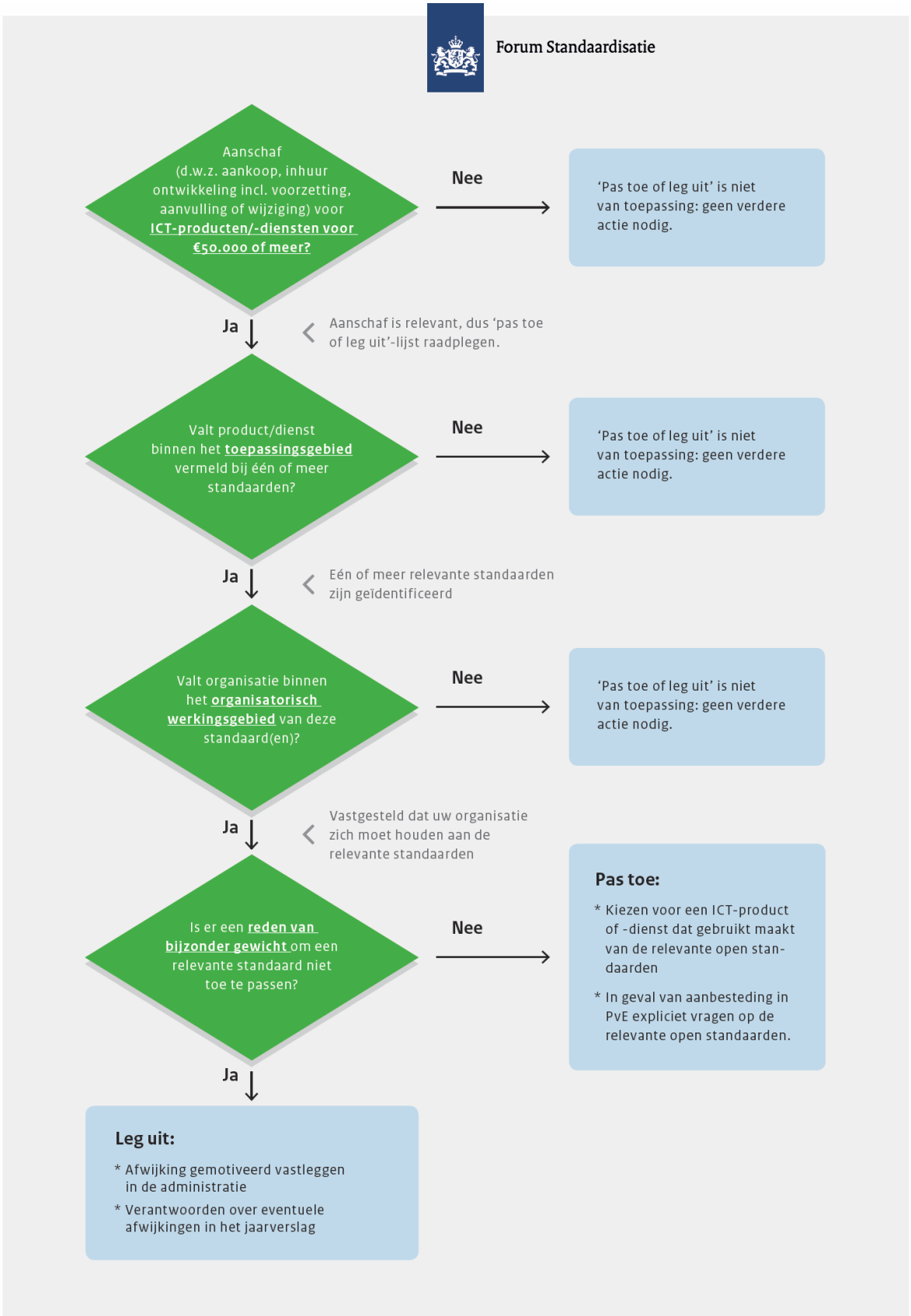
Forum Standaardisatie
voor digitaal samenwerken

B2. Standaarden gerangschikt naar lagen



Deze figuur is speciaal gemaakt voor de monitor open standaarden.
Het is een grafisch overzicht van de standaarden op de pas-toe-of-leg-uit lijst van december 2019.
Horizontaal staat de indeling in domeinen die het Forum hanteert. Verticaal zijn de standaarden ingedeeld op basis van een vereenvoudiging van verschillende bekende lagen-modellen (zoals het OSI-referentiemodel voor communicatiestandaarden en het vijf-lagenmodel dat in de zorg gehanteerd wordt).
De infrastructuur-laag bevat de standaarden die op technisch niveau eisen stellen aan de uitwisseling van gegevens. Deze laag bevat geen standaarden die eisen stellen aan de uit te wisselen informatie. De informatie-laag bevat standaarden die zien op de vraag welke informatie (in het kader van de samenwerking) vastgelegd en gedeeld wordt. De bovenste laag bevat tot slot de standaarden die eisen stellen aan de organisatie en de processen.

B3. Stroomschema: Pas toe of leg uit in het kort



B4. 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.

B5. Overzicht van de beoordeelde aanbestedingen 2018/2019

De 35 aanbestedingen van Rijk en uitvoeringsorganisaties en de 37 van mede-overheden die dit jaar zijn beoordeeld zijn in Tabel B5.1 en Tabel B5.2 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

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 B5.1 Overzicht van beoordeelde aanbestedingen Rijk en uitvoeringsorganisaties

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel
Stichting NWO-I	levering, installatie en oplevering van het COBALT2.0 computercluster voorzien van CPU en GPU rekenkracht, lokale opslagruimte, en snelle onderlinge netwerkverbindingen.	IPv4 en IPv6		**perfect (100%)**
Min. BZK	het Diginetwerk is een stelsel van besloten netwerken, zonder afhankelijkheid van internet. Het KPS is de centrale verbinder van het Diginetwerk.	Digikoppeling IPv4 en IPv6 ISO 27001/27002 HTTPS en HSTS TLS		**perfect (100%)**
Zorginst. Nl.	een schaalbare Infrastructure as a Service (IaaS). Aanbestedende dienst wenst de diensten af te nemen tot en met het technisch beheer van de applicaties. Dit betekent dat de aanbieder verantwoordelijk zal worden voor het benodigde datacenter, het datacenter LAN, benodigde verbindingen, hardware, virtualisatielaag, server operating systems, etc.	DNSSEC HTTPS en HSTS TLS IPv4 en IPv6 ISO 27001/27002 SAML SPF DKIM DMARC STARTTLS & DANE		**perfect (100%)**
Min. AZ	het leveren en beheren van een e-mailmanagementvoorziening voor het Platform Rijksoverheid Online (PRO), inclusief facultatieve dienstverlening rondom optimalisatie van het e-mailkanaal.	DNSSEC ISO 27001/27002 IPv4 en IPv6 ODF HTTPS en HSTS TLS DKIM DMARC SPF STARTTLS & DANE Open API spec.	PDF	**op de goede weg (92%)**

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel
LVNL	het gaat om de overstap van SIDN naar SIP trunking (valt dus onder telefonie). Er wordt ook een webportaal geëist waarmee LVNL zelf wat configuratie kan instellen.	HTTPS en HSTS TLS IPv4 en IPv6 PDF	ISO 27001/27002	**op de goede weg (80%)**
Min. SZW	de housing en hosting plus het technische beheer van de infrastructuur van Directie Dienstverlening Samenwerkingsverbanden en Uitvoering (DSU).	ISO 27001/27002 HTTPS en HSTS TLS DNSSEC	IPv4 en IPv6 Digikoppeling	**op de goede weg (67%)**
Min.BZK	het vervangen van de applicatie (database, frontend + tools) die nu te vinden is op www.financiengemeenten.nl.	ISO 27001/27002 HTTPS en HSTS TLS IPv4 en IPv6 DNSSEC Digitoegankelijk PDF	ODF DKIM DMARC SPF	**op de goede weg (64%)**
KB	de aanschaf en implementatie van een e-*lending solution*, inclusief configuratie, technische applicatiebeheer, hosting en onderhoud.	ISO 27001/27002 HTTPS en HSTS TLS Digitoegankelijk SAML	IPv4 en IPv6 DNSSEC OpenAPI spec.	**op de goede weg (63%)**
Min. AZ.	het gaat om het overnemen van het beheer van het Platform Rijksoverheid Online (PRO) van de huidige leverancier naar opdrachtnemer.	ISO 27001/27002 DNSSEC Digitoegankelijk OWMS DKIM DMARC SPF STARTTLS & DANE OpenAPI spec.	HTTPS en HSTS TLS IPv4 en IPv6 BWB ECLI JCDR CMIS	**op de goede weg (57%)**
Min. BZK	de Nederlandse Zorgautoriteit zoekt een integrale SaaS oplossing voor de HRM en F&C processen en waarbij de salaris administratie/-verwerking als dienstverlening wordt aangeboden.	ISO 27001/27002 HTTPS en HSTS TLS DNSSEC PDF DKIM DMARC SPF	IPv4 en IPv6 E-portfolio NLCIUS SAML XBRL ODF	**op de goede weg (57%)**
SBB	er wordt gevraagd om het leveren van een geautomatiseerde abonneeadministratie voor meerdere achterliggende functies	ISO 27001/27002 HTTPS en HSTS TLS DNSSEC SPF DKIM DMARC STARTTLS & DANE	Digitoegankelijk SAML IPv4 en IPv6 ODF PDF OpenAPI spec.	**op de goede weg (57%)**
Min. Fin.	een HR-SaaS-oplossing plus uitbesteding van personeels- en salarisadministratie.	ISO 27001/27002 HTTPS en HSTS TLS PDF SAML	IPv4 en IPv6 DNSSEC ODF E-portfolio	**op de goede weg (56%)**
Bel.dst.	programmatuur en diensten voor een EOMS-Oplossing (EOMS = Enterprise Output Management Solution). De EOMS-Oplossing dient te bestaan uit programmatuur (software) voor documentopmaak (inclusief technisch beheerdiensten), migratiediensten van bestaande documentstromen, en procesbesturing inclusief monitoring.	ISO 27001/27002 HTTPS en HSTS TLS PDF XBRL CMIS	ODF Digikoppeling DKIM DMARC SPF Open API spec.	**op de goede weg (50%)**

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel
Min. Def.	Het ontwikkelen van Offline Worldwide Imagery Basemap en het jaarlijks doorontwikkelen daarvan.	ISO 27001/27002 Geo	HTTPS en HSTS TLS	**op de goede weg (50%)**
IUC-Noord	het leveren, installeren en onderhouden van een fullcolour hoogvolume rolprintoplossing en bijbehorende randapparatuur.	ISO 27001/27002 PDF	HTTPS en HSTS TLS	**op de goede weg (50%)**
Min. EZK	toeleveranciers aan decentrale overheden 'onboarden' op het SimplerInvoicing netwerk zodat deze in staat zijn een eveneens op het netwerk aangesloten decentrale overheid een e-factuur te sturen.	NLCIUS	PDF	**op de goede weg (50%)**
RvS	op zoek naar een leverancier die de monitoring, technisch beheer, logging, signalering en terugkoppeling in periodieke rapportages van 'Mijn Zaak' biedt.	ISO 27001/27002	PDF	**op de goede weg (50%)**
Min. Fin.	outsourcing van kantoorautomatisering.	ISO 27001/27002 TLS HTTPS en HSTS DNSSEC PDF SAML	IPv4 en IPv6 ODF DKIM DMARC SPF STARTTLS & DANE WPA2 Enterprise NB: In de NvI zijn open standaarden naderhand alsnog uitgevraagd.	**op de goede weg (46%)**
AFM	op zoek naar een leverancier die kan voorzien in een Digitale Nieuwsvoorziening. De nieuws-voorziening bestaat uit de levering van nieuwsartikelen en een dashboard, digitaal archief, en het ontsluiten van al gecontracteerde titels.	ISO 27001/27002 HTTPS en HSTS TLS	PDF DKIM DMARC SPF	**op de goede weg (43%)**
Bel.dst.	het leveren, implementeren en gebruiksklaar opleveren van een Laboratorium Informatie Management Systeem (LIMS), inclusief beheer en onderhoud en het verrichten van diensten t.b.v. het Douane Laboratorium te Amsterdam. Het doel van het LIMS is het ondersteunen van het Laboratorium proces door onder andere het registreren van data van en rapporteren over laboratorium onderzoeken ten behoeve van uitgevoerde / uit te voeren controles.	ISO 27001/27002 TLS PDF HTTPS en HSTS	Ades baseline pr. NLCIUS Open API spec. DKIM DMARC SPF	**op de goede weg (40%)**
Zorginst. Nl	telefonie en verwante diensten o.b.v. SIP trunk, inclusief Front Office applicatie.	IPv4/IPv6 ISO 27001/27002	HTTPS en HSTS TLS PDF	**op de goede weg (40%)**
SVB	een Software oplossing met de domeinen FIN+ voor de financiële processen (Purchase2Pay, contactmanagement en beheer, projectaccounting, urenregistratie), en HR+ voor de HR-processen.	ISO 27001/27002 HTTPS en HSTS TLS SAML PDF	DNSSEC IPv4 en IPv6 NLCIUS SETU XBRL E-portfolio DKIM DMARC SPF	**op de goede weg (36%)**

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel
DJI	elektronisch via een portal beschikbaar stellen van een ruim aanbod van digitaal psychologische tests/vragenlijsten en het genereren van rapportages over de uitslag van de tests ten behoeve van selectie, doorstroom en mobiliteit van personeel en potentiële kandidaten.	ISO 27001/27002 HTTPS en HSTS TLS SAML PDF	DNSSEC IPv4 en IPv6 Digitoegankelijk Digikoppeling E-portfolio Open API spec. DKIM DMARC SPF	**op de goede weg (36%)**
Bel.dst.	een SaaS catalogus van Producten en Diensten gericht aan medewerkers van de Belastingdienst (opleidingen, trainingen e.d.), alsmede het Technisch beheer en onderhoud daarop, hosting en additionele diensten.	ISO 27001/27002 HTTPS en HSTS TLS DNSSEC SAML	Digitoegankelijk NL LOM PDF ODF IPv4 en IPv6 STARTTLS & DANE DKIM DMARC SPF	**op de goede weg (36%)**
RDW	de complete Wifi dienstverlening extern afnemen zodanig dat Wifi op alle RDW-locaties in Nederland als een managed service wordt aangeboden. Onderdeel van deze aanbesteding is een volledige dienst die end-2-end de gewenste functionaliteit levert, inclusief de complete installatie, implementatie en onderhoud & support.	ISO 27001/27002 WPA2 Enterprise	DNSSEC IPv4 en IPv6 HTTPS en HSTS TLS	**op de goede weg (33%)**
Jur.loket	de levering van een ICT-infrastructuur en een passende ICT-dienstverlening ter ondersteuning van de bedrijfsprocessen van Het Juridisch Loket (HJL, een initiatief van de Raad voor Rechtsbijstand en het ministerie van Justitie en Veiligheid).	HTTPS en HSTS TLS	ISO 27001/27002 IPv4 en IPv6 WPA2 Enterprise SAML	**op de goede weg (33%)**
IFV	een Dynamisch Aankoop Systeem inrichten als elektronische inhuuromgeving middels een SaaS applicatie. De applicatie dient het IFV in staat te stellen op een rechtmatige wijze personeel in te kunnen huren door gebruik te maken van het DAS als inkoopprocedure voor de inhuur van personeel.	ISO 27001/27002 HTTPS en HSTS TLS	DNSSEC IPv4 en IPv6 SAML PDF DKIM DMARC SPF	**op de goede weg (30%)**
Min. Def	een PoC en pilot voor de beproeving van een Enterprise Content Management (ECM) concept.	SAML CMIS	ISO 27001/27002 HTTPS en HSTS TLS ODF PDF	**op de goede weg (29%)**
Min. I&W	op zoek naar een partij die actuele data met betrekking tot RVV Verkeersborden op alle wegen in Nederland vergaart, verifieert, waar nodig verrijkt, opslaat en ontsluit. Binnen de scope vallen o.a. geordende verwerking en ontsluiting van data, inrichting van een database, verstrekking van de data als Open Data en beschikbaar stellen van een databestand dat kan worden bijgewerkt door gebruikers.	ISO 27001/27002 Geo	HTTPS en HSTS TLS PDF ODF JCDR	**op de goede weg (29%)**

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel
KvK	een ATA-carnet kun je gebruiken bij tijdelijke uitvoer van bijvoorbeeld tentoonstellingsmateriaal of gereedschappen. De KVK heeft een dedicated platform in gebruik voor aanvragen en leveringen van dit document en zoekt een leverancier voor een nieuwe oplossing.	ISO 27001/27002 PDF	HTTPS en HSTS Digitoegankelijk DNSSEC IPv4 en IPv6 WDO Datamodel	**op de goede weg (29%)**
Min. VWS	het Ministerie zoekt een nieuwe exploitant voor de Zorg Trust Service Provider (TSP).	ISO 27001/27002 HTTPS en HSTS TLS	Digitoegankelijk DNSSEC IPv4 en IPv6 NLCIUS PDF STARTTLS & DANE DKIM DMARC SPF STUF	**op de goede weg (23%)**
Min. VWS	het College ter Beoordeling van Geneesmiddelen beoogt de veiligstelling van de informatie die zij onder haar beheer heeft. Men wil een eenmalige inrichting voor het monitoren van het netwerk van het CBG, en daarnaast een aantal ondersteunende diensten.	ISO27001/27002	HTTPS en HSTS TLS DKIM DMARC SPF	**op de goede weg (17%)**
St. Nidos	het ontwikkelen, beschikbaar stellen en beheren van software en een platform, waarop die software beschikbaar wordt gesteld, inclusief de daarbij behorende ondersteunende diensten. Onder 'platform' wordt verstaan het gehele onderliggende platform waarop de software kan draaien, inclusief hosting.	PDF	ISO 27001/27002 IPv4 en IPv6 HTTPS en HSTS TLS Digitoegankelijk DNSSEC BWB ECLI ODF	**op de goede weg (10%)**
RvA	de Raad voor Accreditatie wil met betrekking tot het beheer van de IT-Infrastructuur maximaal ontzorgd worden en wenst daarvoor het hosten, ontsluiten en beheren van zijn ICT-omgeving als dienst af te nemen.	ISO 27001/27002	HTTPS en HSTS TLS IPv4 en IPv6 DNSSEC ODF PDF DKIM DMARC SPF STARTTLS & DANE WPA2 Enterprise	**op de goede weg (8%)**
LVNL	grotendeels een beheeropdracht voor Office 365 en gerelateerde applicaties en ontwikkelplatform (Azure).	ISO 27001/27002	HTTPS en HSTS TLS ODF PDF	**heel slecht *) n.v.t.**

*) Om licenties voor standaard software gevraagd, dat is strijdig met open standaardenbeleid.

Tabel B5.2 Overzicht van beoordeelde aanbestedingen Mede-overheden

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel
Provincie Groningen	een leverancier die kwalitatief goed ICT-beheer kan aanbieden van de ICT-infrastructuur inclusief telefonie met bijbehorende ICT-netwerk infrastructuur. In de tweede plaats verwacht men dat deze leverancier op een proactieve manier meedenkt met de verdere ontwikkeling van een moderne, betrouwbare en kosteneffectieve ICT-infrastructuur.	ISO 27001/27002 HTTPS en HSTS TLS		**perfect (100%)**
Gemeente Maastricht	het realiseren van een nieuwe corporate website op gemeentemaastricht.nl en een multisite oplossing voor het beheren en creëren van veertig (40) andere websites binnen het gemeentelijk domein.	Digitoegankelijk DNSSEC HTTPS en HSTS TLS ISO 27001/27002 SAML SPF DKIM DMARC STARTTLS & DANE	IPv4 en IPv6	**op de goede weg (91%)**
Gemeente Breda	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 HTTPS en HSTS TLS IPv4 en IPv6 ISO 27001/27002 SPF DKIM DMARC	PDF	**op de goede weg (89%)**
Waterschap De Dommel	het realiseren van verschillende WAN verbindingen en managed VPN dienst.	DNSSEC HTTPS en HSTS TLS IPv4 en IPv6 ISO 27001/27002	PDF	**op de goede weg (83%)**
Provincie Zeeland	de aanschaf, implementatie en onderhoud van een systeem voor zaakgericht werken en document management in de vorm van een Software as a Service oplossing (SaaS).	Digikoppeling Digitoegankelijk DNSSEC HTTPS en HSTS TLS IPv4 en IPv6 ISO 27001/27002 StUF ODF PDF SAML DKIM DMARC SPF	STARTTLS & DANE AdES baseline Geo	**op de goede weg (82%)**
Gemeente Apeldoorn	een loopbaanportal dat medewerkers in staat stelt regie te nemen over hun loopbaan.	DNSSEC HTTPS en HSTS TLS ISO 27001/27002 SPF DKIM DMARC STARTTLS & DANE	Digitoegankelijk E-Portfolio IPv4 en IPv6	**op de goede weg (73%)**

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel
Gemeente Edam-Volendam	Het leveren en hosten van een nieuwe, goed functionerende, veilige en gebruiksvriendelijke website en het converteren van de opgeschoonde content van de huidige website en het verder met de contentmanager van de gemeente inrichten van de nieuwe website.	DNSSEC HTTPS en HSTS TLS ISO 27001/27002 StUF	BWB Digitoegankelijk IPv4 en IPv6	**op de goede weg (63%)**
Hoogheem-raadschap. Rijnland	het aanschaffen, implementeren en onderhouden van een nieuwe zoekmachine.	Digitoegankelijk PDF HTTPS en HSTS TLS SAML	ISO 27001/27002 ODF DNSSEC	**op de goede weg (63%)**
Gemeente Lelystad	het beschikbaar stellen, implementeren, beheren en onderhouden van een zaaksysteem (ZS) met een geïntegreerd documentmanagementsysteem (DMS).	HTTPS en HSTS TLS ISO 27001/27002 StUF PDF SAML DKIM DMARC SPF	Digikoppeling DNSSEC IPv4 en IPv6 CMIS ODF STARTTLS & DANE	**op de goede weg (60%)**
Veiligheids-regio Kenne-merland	het leveren, realiseren, implementeren en onderhouden van een 'Generiek Zaaksysteem' inclusief DMS en een sjabloongenerator. De applicatie is voor intern gebruik.	Digikoppeling HTTPS en HSTS TLS ISO 27001/27002 StUF CMIS ODF PDF	DNSSEC IPv4 en IPv6 SAML SPF DKIM DMARC	**op de goede weg (57%)**
Regio Westfrieslan d	Een gebruiksvriendelijk AVG-beheer systeem dat gestructureerd, eenvoudig en overzichtelijk ondersteuning biedt bij de wettelijke verplichtingen, te weten: het register van verwerkingsactiviteiten, en Privacy Impact Analyses. Ook biedt het beheersysteem mogelijkheid voor de registratie van inbreuken, de registratie van verzoeken van betrokkenen om hun rechten uit te oefenen, en monitoring op verbeteringen en maatregelen.	HTTPS en HSTS ISO 27001/27002 PDF TLS	DNSSEC IPv4 en IPv6 ODF	**op de goede weg (57%)**
SSC Zuid-Limburg	een applicatie ten behoeve van het automatiseren van het aanvraag-, meldings- en vergunningenproces rondom werkzaamheden in de openbare ruimte (waaronder en met name kabels en leidingen).	DNSSEC HTTPS en HSTS TLS ISO 27001/27002 StUF SPF DKIM DMARC STARTTLS & DANE	Digikoppeling Digitoegankelijk Geo AdES baseline NLCIUS ODF PDF	**op de goede weg (56%)**
Gemeente Den Helder	het vervangen van haar financieel systeem. Onderdeel is het leveren van een SaaS oplossing on-premise, het implementeren en migreren naar het nieuwe systeem, en support.	HTTPS en HSTS ISO 27001/27002 NLCIUS StUF PDF TLS	Digikoppeling DNSSEC IPv4 en IPv6 XBRL ODF SAML	**op de goede weg (50%)**

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel
BAR-organisatie	levering, implementatie en onderhoud van een applicatie voor de gemeenten Barendrecht, Albrandswaard en Ridderkerk met de benodigde koppelingen voor het digitaliseren de Planning en Control cyclus, het digitaal publiceren van de begroting, digitaal inzichtelijk maken van uitvoering van de (beleids)doelstellingen en ontwikkeling van de budgetbestedingen.	HTTPS en HSTS IPv4 en IPv6 ISO 27001/27002 PDF TLS	ODF DNSSEC SPF DKIM DMARC	**op de goede weg (50%)**
Meerinzicht	een aanbesteding om te voorzien in een mobiele communicatie voorziening.	ISO 27001/27002	PDF	**op de goede weg (50%)**
Gem. regeling Veiligheids-regio Brabant-Noord	de levering van een financieel systeem. De opdracht omvat het realiseren, implementeren, beheren en onderhouden van een SaaS oplossing die de processen op het gebied van Financiën en de informatiebehoefte ondersteunt.	HTTPS en HSTS TLS ISO 27001/27002 XBRL CMIS PDF	IPv4 en IPv6 NLCIUS StUF ODF Digikoppeling DNSSEC SAML	**op de goede weg (46%)**
Waterschap Hollandse Delta	het leveren, implementeren, inrichten, onderhouden en beheren van een SaaS Purchase 2 Pay oplossing.	DNSSEC HTTPS en HSTS TLS ISO 27001/27002 NLCIUS PDF	IPv4 en IPv6 XBRL ODF OpenAPI spec. SPF DKIM DMARC	**op de goede weg (46%)**
Gemeente Gooise Meren	de levering, installatie, implementatie en onderhoud van een online applicatie voor de ondersteuning van de Planning en Control (P&C) cyclus.	Digitoegankelijk HTTPS en HSTS TLS ISO 27001/27002 PDF	XBRL DNSSEC SAML SPF DKIM DMARC	**op de goede weg (45%)**
Gemeente Amsterdam	een aanbesteding voor de verwerving van een nieuw personeels- en salarissysteem voor de gemeente Amsterdam in de vorm van een SaaS-oplossing.	ISO 27001/27002 DNSSEC HTTPS en HSTS TLS SETU CMIS SAML	ODF PDF XBRL SPF DKIM DMARC Digikoppeling Digitoegankelijk E-portfolio	**op de goede weg (44%)**
Gemeente Achtkarspelen	de levering, implementatie, instandhouding en beheer van de IC-applicaties Belastingen, Financiën (optioneel) BAG, Burgerzaken (inclusief BRP), GBA-V en VOA en het bijbehorende gegevensdistributiecentrum.	ISO 27001/27002 StUF NLCIUS ODF PDF XBRL	SPF DKIM DMARC Digikoppeling Digitoegankelijk DNSSEC HTTPS en HSTS TLS	**op de goede weg (43%)**
Gemeente Heerlen	op basis van een modulaire SaaS-oplossing leveren, implementeren, onderhouden en beheren (updates) van een digitaal systeem voor parkeerproducten.	Digitoegankelijk DNSSEC HTTPS en HSTS TLS ISO 27001/27002 StUF	IPv4 en IPv6 Geo ODF PDF SPF DKIM DMARC Digikoppeling	**op de goede weg (43%)**

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel
Gemeente Utrecht	het leveren, implementeren, configureren en onderhouden van een BuurtteamOrganisaties en KlantSysteem (BOKS).	HTTPS en HSTS ISO 27001/27002 StUF PDF SAML TLS	IPv4 en IPv6 ODF Digikoppeling Digitoegankelijk DNSSEC SPF DKIM DMARC	**op de goede weg (43%)**
Gem. bel. kantoor Locosensus - Tricijn	een systeem voor de ondersteuning van het proces van heffen en innen van de waterschaps- en gemeentebelastingen (inclusief gecombineerde belastingaanslagen) door de GBLT, inclusief het gegevensbeheer.	Digikoppeling ISO 27001/27002 StUF	HTTPS en HSTS TLS PDF SAML	**op de goede weg (43%)**
gem. regeling DCMR	de levering, implementatie en support van een nieuw Bodeminformatiesysteem (BIS). Voor acht gemeenten beheert de DCMR alle bodeminformatie.	ISO 27001/27002 SIKB0101 PDF SAML	StUF ODF Digikoppeling Geo HTTPS en HSTS TLS	**op de goede weg (40%)**
IJssel-gemeenten	het inrichten, implementeren, gebruiken (middels gebruikersrecht e.d.) en onderhouden van het financieel administratiesysteem als SaaS oplossing.	Digitoegankelijk ISO 27001/27002 StUF XBRL PDF	Digikoppeling DNSSEC HTTPS en HSTS TLS IPv4 en IPv6 NLCIUS ODF SAML SPF DKIM DMARC	**op de goede weg (31%)**
Provincie Utrecht	de (door)ontwikkeling van, het onderhoud aan en ondersteuning bij het gebruik van een toekomstbestendige Distributiefunctie (reizigersinformatiesysteem). Onderdeel is het opstellen van een hostingplan.	HTTPS en HSTS TLS PDF	DNSSEC IPv4 en IPv6 ISO 27001/27002 ODF SPF DKIM DMARC	**op de goede weg (30%)**
Regio Rivierenland	het opleveren van een Enterprise Service Bus (ESB) On-Premise. De ESB speelt een centrale rol in de grondplaat binnen het toekomstige applicatielandschap en de architectuur van de aanbestedende dienst.	Digikoppeling ISO 27001/27002 StUF	DNSSEC HTTPS en HSTS TLS ODF SPF DKIM DMARC	**op de goede weg (30%)**
IJsselgemeenten	het leveren, implementeren, gebruiken en onderhouden van een applicatie voor het opstellen ('workflow') van de Planning en control producten, inclusief de financiële koppelingen, de publicatie van de financiële documenten via een website ('publicatie') voor de gemeente Capelle aan den IJssel en optioneel IJsselgemeenten.	Digitoegankelijk ISO 27001/27002 PDF	DNSSEC HTTPS en HSTS TLS IPv4 en IPv6 XBRL ODF SPF DKIM DMARC	**op de goede weg (25%)**

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel
Gemeente Groningen	een raadsinformatiesysteem: een integraal digitaal vergadersysteem waarmee de raad bediend kan worden ten aanzien van de vergaderagenda's, vergaderstukken, dat kan dienen als naslagwerk, dat de mogelijkheid biedt om diverse modules in onder te brengen etc.	ISO 27001/27002 StUF PDF	Digikoppeling Digitoegankelijk DNSSEC EML_NL HTTPS en HSTS TLS BWB JCDR ODF OWMS SAML	**op de goede weg (21%)**
Gemeente Oldambt	de levering d.m.v. hosting van gebruiksrechten voor een E-HRM systeem (inclusief documentatie, onderhoud en ondersteuning) en de dienstverlening rond de verwerking van salaris en loonstroken van medewerkers.	ISO 27001/27002 PDF	DNSSEC HTTPS en HSTS TLS IPv4 en IPv6 SETU ODF SPF DKIM DMARC	**op de goede weg (18%)**
SSC Zuid-Limburg	het middels een abonnementsvorm verkrijgen van toegang tot een kennisbank m.b.t. actuele wet- en regelgeving en werkinstructies op het gebied van Jeugdwet, Wmo, Participatiewet (incl ioaw/z en BBZ), Wet gemeentelijke Schuldhulp-verlening en aanverwante wet- en regelgeving welke digitaal aangeboden wordt ten behoeve van de medewerkers binnen het Sociaal domein.		BWB, DNSSEC, ECLI, HTTPS en HSTS TLS JCDR ISO 27001/27002	**matig (0%)**
Provincie Overijssel	samenwerkende partners Provincie Overijssel, Gemeenschappelijk Havenbedrijf Twente en Rijkswaterstaat zijn op zoek naar een oplossing die leidt tot betere benutting van de Twentekanalen door vlottere doorstroming van de scheepvaart en een hogere beladingsgraad en zoekt daarom een partij voor het ontwikkelen en lanceren van een ICT oplossing informatieplatform Blauwe Golf Twentekanalen.		Digitoegankelijk DNSSEC HTTPS en HSTS TLS ISO 27001/27002 Geo WPA2 Enterprise	**slecht (0%)**
GGD Drenthe	de aanschaf van o.a. desktops, monitoren, laptops, chromebooks en bijbehorende accessoires als toetsenborden, muis, dockingstations, tassen e.d. voor Veiligheidsregio Drenthe.		DNSSEC HTTPS en HSTS TLS	**slecht (0%)**
ISHW	de vernieuwing van de huidige Microsoft licenties inclusief de bijbehorende ondersteunende dienstverlening (Microsoft Software Assurance).		PDF ISO 27001/27002	**heel slecht *) n.v.t.**
Gemeente Loppersum	het leveren van software licenties van Microsoft. Gedurende de looptijd van de overeenkomst wil het Gemeenschappelijk Computer Centrum de overstap maken naar Exchange online en waarschijnlijk te zijner tijd ook naar Office 365.		HTTPS en HSTS TLS ODF ISO 27001/27002	**heel slecht *) n.v.t.**
Gemeente Vijfheeren-landen	de aanschaf van licenties van o.a. Microsoft.		HTTPS en HSTS TLS ODF ISO 27001/27002	**heel slecht *) n.v.t.**
Gemeente Meierijstad	de levering van licenties voor Microsoft.		HTTPS en HSTS TLS ODF ISO 27001/27002	**heel slecht *) n.v.t.**

*) Om licenties voor standaard software gevraagd, dat is strijdig met open standaardenbeleid.

B6. Inventarisatie gebruiksgegevens 2019 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 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 het Bureau Forum Standaardisatie (BFS) hebben hiervoor contact opgenomen met beheerders van standaarden en sommige specifiek voor de standaard relevante voorzieningen. Voor een aantal standaarden zijn de gebruiksgegevens uit het halfjaarlijkse onderzoek naar internet-veiligheids-standaarden (zie *Meting informatieveiligheidstandaarden maart 2019*).

B6.1. Domein Internet en beveiliging

DKIM, DMARC en SPF

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaarden kijken we naar de ondersteuning van DMARC, DKIM en SPF op 563 domeinen van de overheid. Zie hiervoor de IV-meting van begin 2019 (Bijlage B7).

Voor DMARC en SPF is m.i.v. 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.

	begin 2018 (januari)	**medio 2018** (september)	**begin 2019** (maart)
DMARC	65 %	73 %	82 %
DMARC policy	(niet gemeten)	28 %	37 %
DKIM	76 %	84 %	89 %
SPF	85 %	93 %	95 %
SPF Policy	(niet gemeten)	85 %	88 %

Duiding

Vergeleken met vorig jaar is het **gebruik: toegenomen**. Het meeste groeipotentieel zit bij DMARC-policy.

Mogelijke verklaringen voor de toename: stimulering door Platform Internetstandaarden (Internet.nl); daarnaast IV-metingen door Forum Standaardisatie (geldt ook voor andere IV-standaarden); incentive-regeling SIDN; journalistieke aandacht.

Het gebruik van deze standaarden door overheden is groter dan daarbuiten. Zie voor adoptie op .nl-domeinen: stats.sidnlabs.nl/nl/mail.html. Mogelijke verklaring: het stimuleringsbeleid van de overheid.

DNSSEC

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaard kijken we naar het gebruik van DNSSEC-handtekeningen op 563 kern-domeinen van de overheid. Zie hiervoor de IV-meting van begin 2019 (Bijlage B7).

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

	begin 2018 (januari)	**medio 2018** (september)	**begin 2019** (maart)
DNSSEC	80 %	90 %	93 %
op mailserver-domeinen	(niet gemeten)	69 %	71 %

Duiding

Vergeleken met vorig jaar is het **gebruik: toegenomen**.

Mogelijke verklaringen voor de toename: dienstverleners zoals DPC en DICTU bieden het default aan; stimulering door SIDN via incentive-regeling; stimulering door Platform Internetstandaarden (Internet.nl).

Het gebruik van deze standaard door overheden is meer dan daarbuiten: circa 55% van .nl-domeinnamen is ondertekend met DNSSEC. Zie: https://stats.sidnlabs.nl/nl/dnssec.html#gesigneerde%20domeinnamen. Mogelijke verklaring: Niet helemaal duidelijk.

HTTPS & HSTS en TLS

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaarden kijken we naar het gebruik van HTTPS op 563 kern-domeinen van de overheid. Zie hiervoor de IV-meting van begin 2019 (Bijlage B7).

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

	begin 2018 (januari)	**medio 2018** (september)	**begin 2019** (maart)
HTTPS	82 %	89 %	90 %
HSTS	69 %	79 %	79 %
TLS	95 %	96 %	96 %
TLS cf. NCSC	83 %	87 %	89 %

Duiding

Vergeleken met vorig jaar is het **gebruik: licht toegenomen**.

Mogelijke verklaringen voor de toename: door hoge score nog maar weinig verbeterruimte (behalve bij HSTS); stimulering door Platform Internetstandaarden (Internet.nl); journalistieke aandacht voor HTTPS.

Het gebruik van deze standaarden door overheden is licht meer dan daarbuiten. Firefox meet dat ongeveer 78% van de webpagina's over HTTPS wordt bezocht:

https://letsencrypt.org/stats/#percent-pageloads. Mogelijke verklaring: niet helemaal duidelijk.

IPv6 & IPv4

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaarden kijken we naar het gebruik van IPv6 op 563 kern-domeinen van de overheid.

	medio 2017	**medio 2018** (september)	**begin 2019** (maart)
Rijk & Uitvoering	33 % (98)	45 % (127)	51 % (127)
Gemeenten	11 % (396)	25 % (388)	49 % (388)
Provincies	25 % (16)	17 % (18)	33 % (18)
Waterschappen	9 % (34)	13 % (30)	27 % (30)
Totaal	15 % (544)	29 % (563)	48 % (563)

Duiding

Vergeleken met vorig jaar is het **gebruik: toegenomen**.

Mogelijke verklaringen voor de toename: actieve campagne door VNG; dienstverleners zoals DPC en DICTU die het default aanbieden; stimulering door SIDN via incentive-regeling; stimulering door Platform Internetstandaarden (Internet.nl).

Het gebruik van deze standaarden door overheden is licht meer dan daarbuiten. Voor .nl ligt het op ongeveer 40%. Zie: https://stats.sidnlabs.nl/nl/dns.html#.nl-domeinnamen%20bereikbaar%20via%20ipv6 . Mogelijke verklaring: niet helemaal duidelijk.

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

Feitelijk gebruik

Voor de Monitor 2019 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.

Baseline Informatiebeveiliging Overheid (BIO)

Om de veiligheid verder te vergroten, is sinds 1 januari 2019 de Baseline Informatiebeveiliging Overheid van kracht, afgekort BIO. 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. Meer informatie: bio-overheid.nl/over-de-bio

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.

Rijksoverheid

De BIO is in december 2018 vastgesteld door de Ministerraad voor de Rijksoverheid. Daarvoor was door gemeenten, waterschappen en provincie reeds besloten tot invoering van de BIO. In 2019 en 2020 wordt de BIO geïmplementeerd binnen alle overheidslagen. De overheidslagen zijn zelf verantwoordelijk voor implementatie van de BIO. De Algemene Rekenkamer en de Auditdienst Rijk onderzoeken de staat van informatiebeveiliging van het Rijk. Hierover zijn afgelopen jaar relevante stukken gepubliceerd:

- https://www.rekenkamer.nl/onderwerpen/verantwoordingsonderzoek/documenten/rapporten/2019/05/15/staat-van-de-rijksverantwoording-2018
- https://www.rijksoverheid.nl/documenten/kamerstukken/2019/07/02/kamerbrief-aanpak-bevindingen-algemene-rekenkamer-t.a.v.-informatiebeveiliging-en-ict-binnen-de-rijksoverheid
- https://www.rijksoverheid.nl/documenten/rapporten/2019/04/22/onderzoeksrapport-rijksbreed-onderzoek-beheersing-informatiebeveiliging-2018

Provincies

Geen aanvullende informatie beschikbaar.

Gemeenten

De BIO gaat op 1 januari 2020 van kracht. In 2019 kunnen gemeenten zich voorbereiden op de overgang van de BIG naar de BIO. De informatiebeveiligingsdienst (IBD) ondersteunt gemeenten daarbij met producten en regionale bijeenkomsten. De verantwoordingssystematiek ENSIA zal ook worden bijgewerkt naar de BIO.
De Informatiebeveiligingsdienst van de VNG licht toe dat de implementatie van de BIG een cyclisch proces is volgens de plan-do-check-act-cyclus. Er is derhalve geen uniforme trend te destilleren uit de verantwoording van de verschillende gemeenten. Gemeenten maken ieder een eigen afweging van de mate waarin zijn BIG implementeren en het tempo dat daarin voor hen passend is. Deze afweging ligt bij de diverse colleges. Gemeenten hanteren het uitgangspunt dat zij aan de BIG/BIO moeten kunnen voldoen in de relatie met toeleveranciers en verwerkers. Dit betekent dat leveranciers voor zover van toepassing vergelijkbare normen hanteren als de gemeentelijke opdrachtgever.
(Bron: Informatiebeveiligingsdienst VNG)

Waterschappen

In de ledenvergadering van de Unie van Waterschappen van 29 juni 2018 hebben de waterschappen het minimale ambitieniveau voor digitalisering vastgesteld, de 'baseline' Basis op orde. Afspraak 18 in de baseline gaat over de BIWA / BIO en luidt als volgt: 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.

SAML

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaard kijken we naar het aantal aansluitingen bij eHerkenning en DigiD, gebaseerd op SAML.

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 in identificeren bij overheden. Het aantal aansluitingen op deze voorzieningen is dan ook in voorgaande jaren als indicator genomen om het gebruik van SAML te meten.

	2016	**2017**	**2018**	**2019** (vanaf 1 juli)
eHerkenning: SAML	168	203	359	439
DigiD: SAML	128	290	398	429
eHerkenning + DigiD	296	493	757	868

Bron: navraag bij de beheerders van eHerkenning en DigiD bij Logius, en Monitor Open Standaarden 2017, p. 122

Duiding

Vergeleken met vorig jaar is het **gebruik: toegenomen**.
Het aantal SAML aansluitingen voor eHerkenning en DigiD stijgt en daarmee het gebruik van SAML.

STARTTLS & DANE

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 563 domeinen van de overheid. Zie hiervoor de IV-meting van begin 2019 (Bijlage B7).

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

	begin 2018 (januari)	**medio 2018** (september)	**begin 2019** (maart)
STARTTLS		94 %	94 %
STARTTLS cf. NCSC		55 %	67 %
DANE		25 %	41 %
DNSSEC MX *)		69 %	71 %

**) DNSSEC MX is randvoorwaardelijk voor DANE*

Duiding

Vergeleken met vorig jaar is het **gebruik: toegenomen**. De adoptie van STARTTLS is niet gegroeid maar is al hoog. Met name DANE is flink gestegen. Daar zit ook nog steeds het grootste verbeterpotentieel. DNSSEC MX toont het directe potentieel voor DANE.

Mogelijke verklaringen voor de toename: door hoge score nog maar weinig verbeterruimte voor STARTTLS; stimulering door Platform Internetstandaarden (Internet.nl) en IV-metingen door Forum Standaardisatie (geldt ook voor andere IV-standaarden).

Het gebruik van deze standaarden door overheden is groter dan daarbuiten. Zie voor adoptie op .nl-domeinen: stats.sidnlabs.nl/nl/mail.html#dane. Mogelijke verklaring: het stimuleringsbeleid van de overheid.

STIX & TAXII

De standaarden STIX en TAXII worden onder meer gebruikt door het Nationaal Cyber Security Centrum (NCSC), die de standaard zelf ook gebruikt. Het NCSC doet dit in het Nationaal Detectie Netwerk (NDN), een stelsel van samenwerkingsverbanden tussen het NCSC en organisaties uit de Rijksoverheid en andere vitale sectoren. Binnen dit netwerk wordt gestructureerd informatie uitgewisseld over digitale dreigingen. Een NDN-deelnemer is een organisatie die deelneemt aan dit netwerk.

Van vier van de in totaal veertien NDN-deelnemers is bekend dat zij gebruik maken van STIX/TAXII. Het NCSC vermeldt hierbij dat het daarbij gaat om relatief grote spelers. Het is zeer wel mogelijk dat andere deelnemers STIX/TAXII gebruiken, het NCSC heeft hier echter geen zicht op.

VNG Realisatie gaat met het product GGI-Veilig managed SIEM/SOC dienstverlening aanbieden. De verwachting is dat de meeste gemeenten hier op zullen aansluiten. Hiermee zal het gebruik van STIX/TAXII binnen het gemeentelijk domein in de toekomst stijgen.

WPA2 Enterprise

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: govroam.nl/over- govroam/deelnemende-organisaties resp. https://eduroam.nl/instellingen)

	2016 (september)	**2017** (september)	**2018** (september)	**2019** (september)
Govroam	49	132	244	307
Eduroam	157	199	215	222
samen	206	331	459	529

Duiding

Vergeleken met vorig jaar is het **gebruik: toegenomen** (als we kijken naar aangesloten organisaties op Govroam en Eduroam). Het aantal gekoppelde instellingen aan Eduroam is hoog en zit tegen het saturatiepunt aan. Het aantal gekoppelde organisaties aan Govroam stijgt gestaag. Eduroam is er al sinds 2003 en Govroam is in 2013 gelanceerd.

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.

Naast gekoppelde instellingen zou ook gekeken kunnen worden naar het aantal authenticaties of gebruikers per dag. Eduroam heeft anno 2019 ca. 3-4 miljoen authenticaties per dag en 250.000 gebruikers per dag. Voor deze monitor zijn geen absolute cijfers van

Govroam bekend. Govroam zou wel meer gebruikt kunnen worden. Het wordt nog niet ten volle benut, deels door onbekendheid met het netwerk, deels omdat WiFi netwerken met een vooraf gedeelde sleutel (Pre-Shared-Key) gemakkelijker in gebruik zijn, mensen de risico's niet zien, of grote moeite hebben met het koppelen van de authenticatie. Het gebruiksgemak van WPA2-Enterprise wordt bemoeilijkt door de password change policies die de overheden vaak nog hanteren. Wachtwoorden moeten een aantal keer per jaar worden gewijzigd. Dit werk door op de manier waarop gebruikers zich wireless authenticeren. Dat remt behoorlijk in de deployment van WPA2-Enterprise. Uiteraard zijn daar oplossingen voor, waaronder pseudo-accounts (TLS-certificaten als client, of een applicatie-specifiek-password), en daar zijn verschillende vormen en implementaties van.

B6.2. Domein Document en (web/app)content

Ades Baseline Profiles

Feitelijk gebruik

Over de toepassing van de Ades profielen zijn geen feitelijke cijfers beschikbaar. Onderstaande informatie is een momentopname van zomer 2019.

Er zijn enkele grootschalige toepassingen bekend in de interactie tussen overheden en bedrijven/ particulieren. O.a. de Kamer van Koophandel (KvK) vraagt in toenemende mate van organisaties om officiële documenten, zoals jaarrekeningen, met Xades te ondertekenen. Je kunt bij de KvK ook diverse documenten bestellen die digitaal gewaarmerkt zijn, zoals een uittreksel of een jaarrekening. Deze pdf-documenten zijn met een digitale handtekening gewaarmerkt wat garandeert dat het document van KVK is. De digitale handtekening is gemaakt met PAdes.

Daarnaast zijn via de eIDAS-regulation over elektronische identificatie de Ades-profielen verplicht gesteld voor grensoverschrijdend verkeer. Ook daarvan zijn geen cijfers bekend, maar aangenomen mag worden dat onder invloed van de voortschrijdende ontwikkeling van de European Digital Single Market het gebruik van de Ades profielen ook zal toenemen.

Duiding

Vergeleken met vorig jaar is het **gebruik: toegenomen**.

Mogelijke verklaringen voor de toename: onder andere doordat de (KvK) vanaf de boekjaren die beginnen op of na 1 januari 2017 bedrijven in de klasse middelgroot verplicht om de jaarrekening bij de KvK te deponeren via SBR en de digitale handtekening die daarbij hoort wordt in XAdes gemaakt. Ook de controleverklaring van de accountant wordt digitaal opgesteld voorzien van een Xades handtekening.

Feitelijke cijfers over het gebruik van deze standaard buiten de overheid zijn niet bekend, maar gebruik van XAdes is in een aantal gevallen voorgeschreven. De KvK uitwisselingen betreffen verkeer tussen de overheid en het bedrijfsleven. D.w.z. dat bedrijven de ondertekenaars zijn die Xades gebruiken, gedwongen door de overheid (verplicht wijze van deponeren). SBR wordt inmiddels ook ingezet in de bancaire sector, SBR Nexus verzorgt dit. Aangenomen mag worden dat hier ook digitale handtekeningen cf. XAdes profiles worden gebruikt.

CMIS

Omdat CMIS op dit moment de evaluatie-procedure doorloopt hebben wij niet apart informatie verzameld over het gebruik van CMIS.

Digitoegankelijk

Over Digitoegankelijk zijn dit jaar niet apart gegevens verzameld, omdat er een onderzoek door Stichting Accessibility wordt uitgevoerd. De gegevens uit dat onderzoek waren echter niet op tijd beschikbaar om voor de Monitor Open standaarden 2019 te gebruiken.

ODF en PDF

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaard kijken we naar een nulmeting van het gebruik van ODF en PDF bij de overheid. Deze nulmeting is gedaan 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 93 websites:

- de 30 meest bezochte websites van de overheid (volgens Communicatie Rijk),
- de 30 grootste gemeenten,
- de 12 provincies,
- de 21 waterschappen.

Bij deze meting zoeken we op elke onderzochte website de documenten en bepalen van welk type de documenten zijn. Daarbij onderscheiden we PDF, ODF en Microsoft Office bestanden (.docx, .xlsx, .pptx, .doc, .xls, .ppt). Ook onderscheiden we verschillende typen PDF en stellen we vast of een PDF voldoet aan de standaarden (PDF/A, PDF 1.7) die op de pas-toe-of-leg-uit lijst staan.

Omdat verschillende zoekmachines verschillende resultaten kunnen opleveren, doen wij per website twee peilingen:

1. Met Google zoeken wij het totaal aantal documenten in PDF, ODF en Microsoft Office format. De datum van de documenten speelt hierbij geen rol. Dit geeft een globaal beeld van alle documenten die op een website te vinden zijn, ook oudere documenten.
2. Met Bing zoeken wij gerichter naar documenten die vanaf 23 september 2018 zijn gepubliceerd, en onderscheiden daarbij tussen PDF/A, PDF 1.7 en PDF formats die geen open standaard zijn. Dit geeft een gedetailleerder beeld van recent gepubliceerde documenten.

We moeten hierbij aantekenen 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. Dit heeft te maken met de manier waarop zoekmachines crawlen, indexeren en hun resultaten filteren. De getoonde statistieken geven dus niet meer dan een indicatie van trends op basis van een steekproef.

In de volgende tabel geven wij de resultaten geaggregeerd weer, dus geen cijfers voor individuele websites.

	Top 30 overheid	G30 gemeenten	Provincies	*Water-schappen*
Aantal gevonden PDF	381.849	197.482	173.860	34.268
Aantal gevonden ODF	15	2	4	2
Aantal gevonden MS Office	123	98	51	52
percentage PDF	99 %	> 99 %	> 99 %	> 99 %
percentage ODF	11 %	2 %	7 %	4 %
Aantal gevonden PDF na 23 – 9 - 2018	1306	1673	1158	818
Groei van aantal PDF sinds 23 – 9 - 2018	0,3 %	0,8 %	0,7 %	2,4 %
%age ISO-PDF van aantal PDF na 23 – 9 - 2018	36 %	47 %	57 %	41 %

Duiding

Omdat het hier gaat om een nulmeting, is de ontwikkeling in het **gebruik dit jaar nog onbekend**.

- In totaal zijn de documenten op 93 websites van verschillende overheden (Rijksoverheid, gemeenten, provincies en waterschappen) onderzocht.
- PDF is veruit het meest gebruikte format voor de publicatie van documenten. Over alle gemeten websites heeft meer dan 99,9% van de documenten een PDF format.
- Op vrijwel alle onderzochte websites werden minder dan 10 Microsoft Office documenten gevonden.
- Twee onderzochte websites hadden meer dan 100 Microsoft Office documenten op hun websites staan.
- In totaal werd maar een handjevol documenten gevonden in ODF format. ODF vormt 6,7% van de bewerkbare documenten op de onderzochte websites.
- Het aantal documenten op websites van overheidsorganisaties groeit langzaam. Over alle gemeten websites is er 0,6% aan nieuwe PDF documenten bijgekomen na 23 september 2018. Het aantal bewerkbare documenten (MS Office, OOXML, ODF) is na 23 september 2018 vrijwel niet gegroeid.

OpenAPI Specification

Er zijn op dit moment nog **geen gegevens over het feitelijk gebruik** van OpenAPI Specification beschikbaar.

Open API Specification (OAS) is een standaard voor de documentatie van Application Programming Interfaces (APIs). Een API is een koppelvlak waarmee applicaties over het Internet toegang kunnen krijgen tot gegevens en diensten (zie docs.geostandaarden.nl/api/API-Strategie/).

OAS staat sinds mei 2018 op de pas-toe-of-leg-uit lijst. In 2019 worden dus voor het eerst gebruiksgegevens over deze standard verzameld. BFS heeft de nulmeting van het feitelijk gebruik van OAS uitbesteed aan ICTU. De nulmeting zal worden uitgevoerd in twee stappen:

1. Maak een inventaris van APIs die door overheidsorganisaties worden gepubliceerd.
2. Kijk per API of deze OAS documentatie heeft.

De eerste stap is de meest arbeidsintensieve. Uitgangspunt is developer.overheid.nl, maar hier staan nog lang niet alle APIs die door overheidsorganisaties worden aangeboden. Er zal

dus een dosis zoekwerk gedaan moeten worden. De tweede stap is relatief eenvoudig uit te voeren.

In 2019 heeft het ministerie van BZK in samenwerking met VNG Realisatie het portal developer.overheid.nl opgezet. De ambitie is dat dit portal in de toekomst alle APIs 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 developer.overheid.nl echter nog maar een fractie van alle APIs die bij de overheid beschikbaar zijn.

De resultaten van het onderzoek van ICTU over het feitelijk gebruik van OAS komen vermoedelijk te laat om nog opgenomen te worden in de Monitor 2019. De onderzochte APIs wel worden aangemeld bij developer.overheid.nl zodat hier later in het jaar betrouwbaarder informatie te vinden is over het gebruik van OAS.

OWMS

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaard kijken we naar een nulmeting van het gebruik van OWMS bij de overheid. Deze nulmeting is gedaan 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 93 websites:

- de 30 meest bezochte websites van de overheid (volgens Communicatie Rijk),
- de 30 grootste gemeenten,
- de 12 provincies,
- de 21 waterschappen.

We hebben bij iedere website gekeken of er metadatering plaatsvindt, en of de volgens OWMS verplichte metadata aanwezig is. Conform het functioneel toepassingsgebied van OWMS beoordelen wij alleen organisaties die metadatering toepassen op hun website. Een website voldoet alleen als alle volgens OWMS verplichte metadata aanwezig is.

Sommige websites hebben wel Dublin Core elementen maar missen één of meer elementen die verplicht zijn volgens OWMS. Deze gevallen worden apart vermeld in de onderstaande tabel met resultaten.

	Top 30 overheid	**G30 gemeenten**	**Provincies**	***Water-schappen***
Voldoet aan OWMS	48 %	17 %	55 %	42 %
Voldoet helemaal niet: gebruikt andere metadata	42 %	50 %	12 %	15 %
Voldoet niet, heeft wel enkele DC elementen	7 %	13 %	33 %	32 %
Geen metadata	3 %	20 %	0 %	11 %

Duiding

Omdat het hier gaat om een nulmeting, is de ontwikkeling in het **gebruik dit jaar nog onbekend**.

- In totaal (gewogen gemiddelde voor de 93 websites) voldoet dit jaar 38% aan OWMS.
- Veel websites hebben wel Open Graph en Twitter metadata maar passen geen OWMS toe. Deze organisaties lijken dus meer te sturen op vindbaarheid in commerciële zoekmachines en sociale media.
- Er zijn nogal wat websites die wel Dublin Core metadata bevatten maar niet volledig voldoen aan OWMS. Van 5 waterschappen (van de in totaal 21) misten de websites alleen het dcterms.title element.
- Het komt regelmatig voor dat een organisatie niet bewust meta-dateert, maar het CMS een aantal metadata tags automatisch op de website plaatst. Deze websites voldoen uiteraard niet aan OWMS.
- Op vrijwel alle onderzochte websites is de metadata identiek op alle pagina's. Organisaties geven dus zelden specifieke metadata voor elke pagina op de website. Volgens de beheerder van OWMS heeft deze manier van metadateren maar beperkte waarde. Het geven van specifieke metadata bij elke pagina te geven vergemakkelijkt namelijk het zoeken naar specifieke informatie op de website.
- De koepelorganisaties VNG, VNG Realisatie en IPO publiceren geen metadata op hun websites. Deze organisaties zijn niet meegeteld in de bovenstaande tabel.

SKOS

Feitelijk gebruik

Voor het feitelijk gebruik van deze open standaard kijken we naar een nulmeting van het gebruik van de standaard SKOS bij de overheid.

In principe kan het gebruik van SKOS vrijwel automatisch worden gemeten via de LOD Laundromat (http://lodlaundromat.org/) die toegang biedt tot alle linked data wereldwijd. De LOD Laundromat echter al enkele maanden buiten dienst en het is niet duidelijk of en wanneer deze weer beschikbaar zal komen. Een alternatieve bron is 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.

Daarom hebben wij in overleg met het Platform Linked Data Nederland besloten om het feitelijk gebruik van SKOS voor deze Monitor te onderzoeken met een enquête. De enquête is uitgezet bij ruim 70 overheden en semi-overheden waaronder de G4 en 10 kleinere gemeenten. De vragen van de enquête zijn te zien op nl.surveymonkey.com/r/VHTTW6D

In totaal reageerden 42 organisaties (58% van de ondervraagden). Dit waren vooral uitvoeringsorganisaties, maar er waren ook 4 gemeenten en 1 waterschap onder de respondenten.

Van de 42 respondenten geeft 64% (27 organisaties) aan Linked Data te gebruiken. Hiervan publiceert 85% Linked Data online (23 organisaties). De overige 15% gebruikt Linked Data alleen voor interne processen (4 organisaties). Van de organisaties die Linked Data publiek ontsluiten gebruikt 74% SKOS (17 organisaties).

Duiding

Omdat het hier gaat om een nulmeting, is de ontwikkeling in het **gebruik dit jaar nog onbekend**.

- Er valt niet eenvoudig te concluderen of de 74% toepassing van SKOS bij externe ontsluiting van Linked Data een 'goed' of 'slecht' feitelijk gebruik representeert. Dit wordt

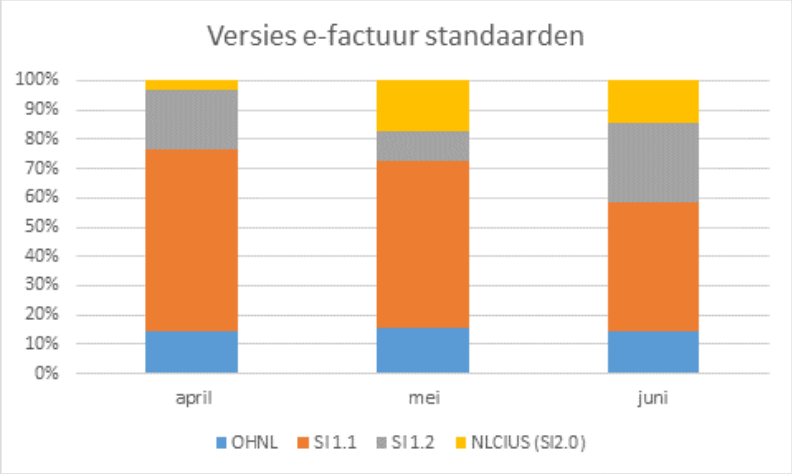
hieronder toegelicht onder ‘Ambities’. De enquête geeft wel de indruk dat SKOS meestal wordt toegepast waar het functioneel toepassingsgebied dat vereist.
- Uit de enquête ontstaat een algemeen beeld dat Linked Data en SKOS nog vooral experimenteel worden toegepast. Slechts een handvol organisaties heeft Linked Data sets van ‘productiekwaliteit’.
- Bij de overheid passen vooral uitvoeringsorganisaties Linked Data en SKOS toe. Bij gemeenten, provincies en waterschappen lijkt het gebruik van Linked Data (en daarmee van SKOS) vooralsnog vrijwel nihil.

B6.3. Domein E-facturatie en administratie

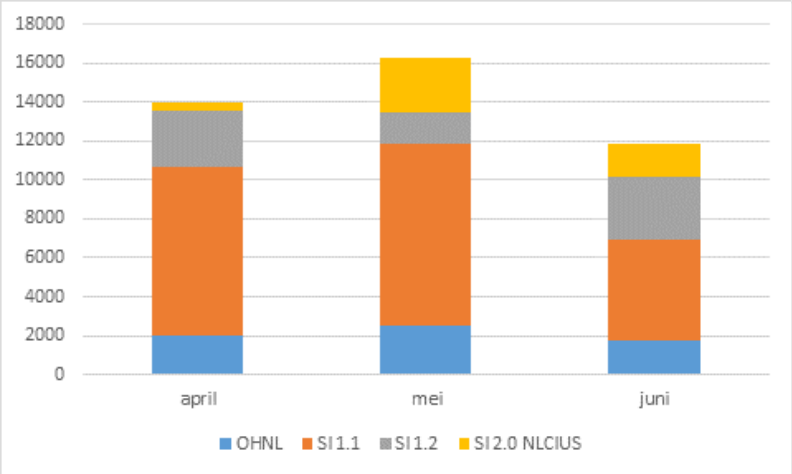
NLCIUS

Feitelijk gebruik

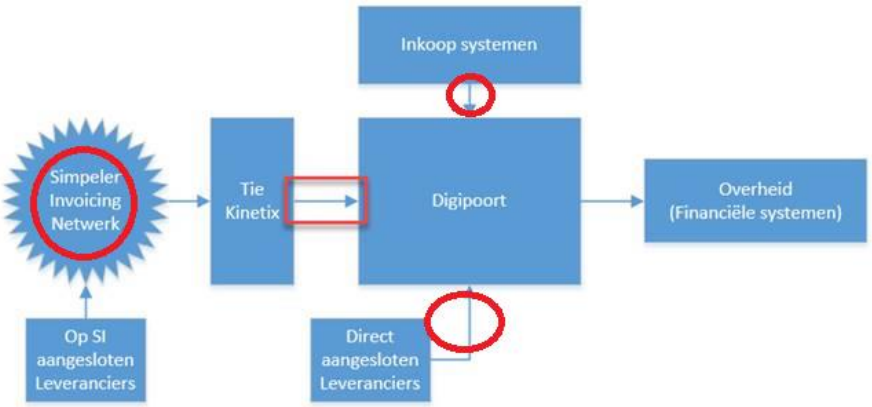
Beheer en bevordering van het gebruik van NL CIUS is belegd bij het Standaardisatieplatform e-factureren waar in drie partijen samenwerken: NEN, Simplerinvoicing en TNO. Het initiatief wordt ondersteund door het Ministerie van Economische Zaken en Klimaat vanwege het maatschappelijke belang. De meting van gebruikscijfers van NL CIUS is pas in april 2019 gestart. Gebruikscijfers van e-factuurstandaarden over april/mei/juni 2019 zijn als volgt (OHNL = de voormalige overheidsstandaard, SI = Simpler Invoicing):



Dezelfde gegevens in absolute aantallen:



Belangrijk: deze cijfers gaan over een beperkt stuk van het e-facturatie landschap, namelijk de rode rechthoek in onderstaande figuur, het verkeer dat via Tie Kinetix naar Digipoort gaat.



De andere toegangen tot Digipoort, de cirkels rondom Digipoort, doen nu alleen nog maar OHNL (dus dat verlaagt het totale NLCIUS percentage. De cijfers van gebruik in het Simpeler Invoicing Netwerk (grote rode cirkel) zijn niet beschikbaar.

Duiding
Omdat het hier gaat om een eerste meting, is de ontwikkeling in het **gebruik dit jaar nog onbekend**.

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.

Feitelijk gebruik
Onderstaande informatie is een momentopname van zomer 2019. De SETU-standaarden worden ontwikkeld en beheerd door de stichting SETU waarin alle grote uitzendorganisaties in Nederland betrokken zijn. SETU beschikt, in lijn met voorgaande jaren, niet over kwantitatieve gegevens over het feitelijke gebruik van de standaarden. De gebruiksgegevens zijn lastig te bepalen, aangezien het berichtenverkeer niet via een centraal platform geregeld wordt en er recent ook geen metingen of enquêtes zijn uitgevoerd.

TNO onderzocht in 2014 de adoptie van SETU en ontwikkelt de standaard in opdracht van de beheerder. Zij meldden dat alle grote spelers in de markt voor flexibele arbeid zijn aangesloten bij SETU en de SETU-standaarden gebruiken voor hun berichtuitwisseling. Deze spelers vertegenwoordigen 85% van de markt. Uit informele uitvraag bij werkgroepen blijkt dat deze spelers gestaag nieuwe koppelingen ontwikkelen met behulp van de SETU-standaarden. Voor de kleinere spelers in deze markt geldt dat zij afhankelijk zijn van hun softwareleveranciers.

Duiding
Vergeleken met vorig jaar is het **gebruik: waarschijnlijk licht gestegen**.

Concreet is in 2019 bekend dat 19 softwareleveranciers één of meerdere van de SETU-standaarden ondersteunen. In 2018 waren dit er 18.

Verder is in 2018 de 2.1 versie van de SETU Standard for Invoicing gepubliceerd, die volledig in lijn is met het Nederlandse gebruiksprofiel van de Europese norm (NLCIUS). In 2019 zijn de eerste partijen aan de slag met het implementeren van deze 2.1 versie. Ook merkt TNO als beheerder van de SETU standaarden dat er vragen en dus partijen concreet aan de slag zijn met de implementatie van de SETU Standard for Vacancies. Uit bovenstaande kan dus worden geconcludeerd dat er sprake is van een lichte toename in gebruik. Gezien de verplichting die op het gebied van e-facturatie in april 2019 is ingegaan, voorziet TNO in ieder geval een verdere toename in het gebruik van de SETU Standard for Invoicing.

WDO Datamodel

WDO Datamodel komt van *World Customs* (Douane) *Organization Data Model*. Het WDO Datamodel is een wereldwijde gegevensstandaard die als basis dient voor het elektronisch uitwisselen van gegevens en berichten (in EDIFACT en XML) wanneer goederen, personen en vervoermiddelen de grens over gaan. De gegevensstroom verloopt tussen bedrijven en overheden en tussen overheden onderling. In veel landen wordt de douaneaangifte (ook) 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 vaak een eigen standaard voorschrijven. Ook binnen de Europese Unie.

Door het gebruik van deze standaard kunnen de diverse overheidsorganisaties dezelfde taal spreken en eenvoudig informatie uitwisselen. Voor de administratie van import en export bevat het WDO Datamodel namelijk zogenaamde 'informatiepakketten' voor gegevensuitwisseling. Een informatiepakket beschrijft de semantiek van de uitgewisselde informatie: gegevens- en procesmodellen en hiervan afgeleide berichtspecificaties (Message Implementation Guidelines). Het doel van het gebruik van de standaard is een efficiënt verloop van de aankomst, het vertrek, de doorvoer en de vrijgave van goederen, vervoersmiddelen en personen in de internationale handel. Het WDO Datamodel wordt daarom gebruikt door de Douane, Rijkswaterstaat, Zeehavenpolitie/Koninklijke Marechaussee en de Nederlandse Voedsel en Warenautoriteit en door havenautoriteiten. Voor Douane betreft het gebruik van de standaard de goederenstromen, maar daarnaast biedt het WDO Datamodel ook informatie over personen (voor bijvoorbeeld marechaussee) en informatie over vervoermiddelen (voor bijvoorbeeld Rijkswaterstaat).

De Douane (beheerder van de standaard) meldt dat het gebruik het WDO Datamodel in principe op twee manieren kan worden afgelezen:

- Toepassing van de MIG (Message Implementation Guidelines) in ontwerpdocumenten van berichten. Hierbij dient wel te worden opgemerkt dat een MIG voor meerdere berichtstromen gebruikt kan worden of juist gesplitst. Dat maakt het tellen van de toepassing wat lastig.
- Vaststellen hoeveel berichten er op basis van de ontwerpdocumentatie worden uitgewisseld.

In de monitor zijn vorig jaar geen gegevens opgenomen over het gebruik van de standaard, dus een vergelijking in de tijd is niet op basis van concrete cijfers te maken. Volgens de Douane is het gebruik is toegenomen. Er zijn meer partijen aangesloten en hierdoor is er sprake van meer berichtstromen met meer berichten.

Douane streeft ernaar in al haar samenwerkingsverbanden met andere overheden, waarbij gegevensuitwisseling tot stand komt, het WDO datamodel in te zetten. Of dit streven gerealiseerd wordt kan worden bepaald door periodiek te meten of het aantal verheden dat deelneemt is toegenomen.

Conclusie van BFS
Het feitelijk gebruik zou wellicht indirect afgelezen kunnen worden door de aantallen toepassingen van de MIG's van het WDO Datamodel. Of door het aantal gedane aangiften en verzonden retourberichten te tellen, want deze zijn namelijk allemaal in de vorm van het WDO Datamodel. Maar of dit zin heeft met het oog op het meten van de adoptie de vraag.

XBRL

eXtensible Business Reporting Language (XBRL) is de internationale open standaard om bedrijfsinformatie te verzamelen, elektronisch uit te wisselen, te analyseren en zo nodig nader te bewerken.

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 2016	**Realisatie 2017**	**Realisatie 2018**	**Realisatie 2019** t/m juni
Belastingdienst				
Aangifte IB + VPB	13.550.654	15.353.253	17.167.811	10.135.398
Loonheffingen (incl. UZGB)	2.533.906	7.642.968	8.481.840	4.431.362
Erfbelasting + Schenkbelasting	-	-	231	1.907
Aangifte OB + Intercomm. prestaties	4.077.407	4.448.085	4.921.431	2.686.708
Toeslagen	1.044.417	1.141.882	1.242.836	697.410
KvK – Reporting Services (SBR)				
Jaarrekeningen	277.410	716.754	866.497	532.664
DUO – Reporting Services (SBR)				
Jaarrekeningen		2.415	1.838	190
SBR Wonen - Reporting Services (SBR)				
DPI (prognose informatie)			852	126
DVI (verantwoordingsinformatie)				1.169
SBRWonen Jaarrekening 2018				34

Duiding

Vergeleken met vorig jaar is het **gebruik: toegenomen**.

Bij domein BD is sprake van een toename in de berichtaantallen. Mede veroorzaakt door toename in het aantal aanleverende partijen. Bij domein KVK is toename te verklaren door verplichting van deponering van de jaarrekening door rechtspersonen in de bedrijfsklasse Middelgroot. Bij domein DUO is sprake van een afname. Het gaat daarbij om beperkte aantallen. Reden (nog) niet bekend. Bij domein SBR Wonen is in 2018 de DPI (prognose informatie) gestart.

Het is onduidelijk of het gebruik van deze standaard door overheden groter of kleiner is dan daarbuiten. XBRL wordt op grote schaal gebruikt door Standard Business Reporting, waarbij de 'Business' voor het overgrote deel private partijen zijn die aan de overheden rapporteren. Ook zijn private intermediairs in deze keten actief. SBR wordt ook gebruikt door Banken, dat betreft uitwisselingen tussen private partijen onderling. Sinds 1 december 2018 is SBR Banken overgegaan in SBR Nexus (= een initiatief van ABN Amro, ING en Rabobank). SBR Nexus meldt dat gebruiksinformatie vertrouwelijk is. Zonder toestemming van deze eigenaren mogen zij deze informatie niet delen.

B6.4. Domein Stelselstandaarden

Digikoppeling

Feitelijk gebruik

Het meten van de toepassing van de Digikoppeling-standaard is lastig omdat het gebruik van dit transport-protocol in veel gevallen buiten het zicht van de beheerder (Logius) omgaat. Digikoppeling kent geen centrale component waarlangs berichten worden gevoerd en inzicht in het gebruik kan dus niet op basis van kwantitatieve metingen worden gedaan. Verder zet de trend steeds meer door dat overheidsorganisaties gebruikmaken van cloudoplossingen aangeboden door zowel publieke als private dienstverleners waardoor de vraag "organisatie gebruikt Digikoppeling" een complex antwoord kan hebben. Er bestaat echter een objectief meetinstrument om te bepalen of een organisatie Digikoppeling toepast in één van haar ketens van elektronische gegevensuitwisseling, Digikoppeling vereist 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.

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 % ****)

**) 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%.*

De categorie “Rijk…” is zeer lastig te bepalen omdat het niet duidelijk is welke organisaties onder deze categorie vallen. Vandaar dat vanaf zomer 2019 deze categorie is vervangen door een nieuwe invulling: Rijk hebben we als volgt gedocumenteerd: Rijk = Alle Ministeries + Basisregistraties + Gemeenschappelijke Regelingen + ZBO’s + Hoge Colleges van Staat + Adviescolleges + Rechterlijke Organisaties. De reden voor deze nieuwe invullingen is dat voor deze lijsten stabiele bronnen bestaan zodat vergelijkingen met volgende jaren mogelijk wordt.

Duiding
Vergeleken met vorig jaar is het **gebruik: toegenomen**.

Het percentage ‘totaal’ in bovenstaande tabel is lager dan vorig jaar omdat in 2019 hierin ook het percentage van de nieuwe gedefinieerde categorie “Rijk” is opgeteld. Als we deze categorie niet zouden meewegen dan was de score op 100% uitgekomen. Een groei van 4 procentpunt t.o.v. van 2018.

Geo-Standaarden

Feitelijk gebruik
Als indicator voor het feitelijk gebruik van deze open standaarden kijken we naar de gebruikscijfers van Publieke Dienstverlening Op de Kaart (PDOK), het open geodata portaal van de Nederlandse overheid.

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. 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. PDOK laat elk jaar aanzienlijke groeicijfers zien, zo is het aantal hits van 6,3 miljard in 2017 verder gegroeid naar 10,5 miljard hits in 2018. Het aantal hits is de beste indicator van het gebruik van de standaarden aan de afname kant, 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. Daarnaast kan specifiek voor NEN3610 nog geteld worden hoeveel informatiemodellen (afgeleide domeinstandaarden) er op gebaseerd zijn.

Kwantitatieve gegevens
Aan de afnamekant is er een groei van 6,3 naar 10,5 (+66%) miljard hits op PDOK. Aan aanbodzijde is het aantal datasets gegroeid van 126 naar 157 (+25%) en het aantal services van 344 naar 415 (+21%). Specifiek voor NEN3610 (één van de Geo-standaarden) is de ontwikkeling gestart voor IMGeluid (Informatiemodel Geluid, waarmee er weer een extra domein conform NEN3610 ontsloten zal gaan worden). De bovengenoemde cijfers zijn een vergelijking van 2018 met 2017.

Duiding
Vergeleken met vorig jaar is het **gebruik: toegenomen**.

De groei houdt aan, zowel qua afnemers die dankzij open standaarden van data kunnen profiteren, als qua aanbieders die data conform open standaarden willen 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 zijn de meerwaarde nu makkelijker in, doordat er voldoende voorbeelden zijn van andere organisaties waarin dit effect optreedt.

Ontwikkeling binnen de overheid en daarbuiten

Binnen overheidsorganisaties is het sterker dan erbuiten. Tegelijk zien we de interessante case dat ESRI (de marktleider in geografische software) zelf niet actief het gebruik van open standaarden promoot, maar wel alle relevante open datasets van de overheid actief inleest en vervolgens uitserveert in de eigen, leverancier-specifieke formaten. Enerzijds kun je dat zien als het niet-gebruiken van open standaarden door hun klanten, anderzijds kun je dat ook zien als dat de juiste, officiële overheidsdata wel degelijk gebruikt wordt door hun klanten, juist omdat de leverancier deze in kan lezen dankzij open standaarden.

StUF

De StUF-standaard is een familie van samenhangende gegevens- en berichtenstandaarden. 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.

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. Zo is ook het convenant samenwerking WOZ-ICT vanuit de waarderingskamer net vernieuwd.

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

- Zwaardere inbedding van standaarden in architectuur en binnen grootschalige (landelijke) ontwikkelingen;
- Leveranciersmanagement;
- Instrumentarium voor preventief testen, model gedreven ontwikkeling;
- Landelijke softwarecatalogus voor markttransparantie en applicatiemanagement;
- Periodieke Monitoring over digitalisering en compliance van softwareproducten;
- Uniforme inkoopvoorwaarden en contractgenerator;
- Bestekteksten, opleidingen en communicatie, enz.

Feitelijk gebruik

Het gebruik van de StUF wordt voornamelijk uitgelezen via de applicaties. Dit is het aantal berichten dat heen en weer gaan 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 miljoenen berichten per jaar.

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.

	Totaal		StUF-BG 3.10 & 3.20		StUF-ZKN 3.10 & 3.20	
Aantal leveranciers	223	(208)	69	(74)	63	(52)
Aantal softwareproducten (incl. versies)	2879	(2760)	1083	(993)	745	(745)
wv. beschikbaar/in gebruik	1374	(1334)	366	(350)	234	(213)
wv. gepland/in ontwikkeling	111	(133)	56	(64)	33	(29)

Peildatum augustus 2019 (tussen haakjes de cijfers van de vorige monitor)
(bron VNG-Realisatie: softwarecatalogus.nl/)

Duiding
Vergeleken met vorig jaar is het **gebruik: toegenomen**.

B6.5. Domein Water en bodem

Aquo-standaard

Feitelijk gebruik
Alle waterschappen en provincies en Rijkswaterstaat leveren hun rapportages middels de Aquo-standaard aan bij het ministerie van Infrastructuur & Waterstaat en bij het European Environment Agency (EEA). Gebruikers van de Aquo-standaard zijn ook middels het indienen van wijzigingsverzoeken en het stellen van vragen betrokken bij de ontwikkeling van de standaard.

Er zijn **geen gegevens over het feitelijk gebruik** van de Aquo-standaard beschikbaar.

Wel is bekend hoeveel vragen gesteld worden en hoe vaak wijzigingsvoorstellen worden ingediend. In de periode 1 juni 2018 - 1 juni 2019 werden door 42 verschillende instanties in totaal 106 vragen gesteld. Dat is een daling (-19%) ten opzichte van de periode 1 juni 2017 - 1 juni 2018, toen nog 143 vragen werden gesteld.

Ook het aantal wijzigingsvoorstellen is gedaald (met 8%): in 2017/2018 waren dit er 158 (ingediend door 28 verschillende instanties), in 2018/2019 waren het er 146 (ingediend door 31 verschillende instanties).

SIKB0101 en SIKB0102

Feitelijk gebruik
Er zijn **geen gegevens over het feitelijk gebruik** van de datastandaarden SIKB0101 en SIKB0102 beschikbaar.

Wel is bekend dat belangrijke partijen de standaard gebruiken.

SIKB0101
Alle gemeenten, omgevingsdiensten en provincies werken met software die gebruik maakt van de datastandaard SIKB0101. Dit blijkt uit de contacten 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) vertegenwoordigd, waar besluitvorming plaatsvindt. 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 bestaande (digitale) bodeminformatie.

De drinkwatersector (publiek/privaat) is in 2018/2019 gestart met de implementatie van SIKB0101. Tevens worden (verkennende) gesprekken gevoerd over de harmonisatie van de standaarden van de Basisregistratie Ondergrond (BRO) met SIKB0101.

SIKB0102

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

- Het 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)
- Opgravende bedrijven (markt en overheid circa 30% van de partijen / 50% qua volume) groeiend.

De depots van gemeenten (veelal historische steden) gebruiken nu nog hoofdzakelijk eigen systemen. Ze bereiden zich voor op een transitie waarbij zij ook gegevens gaan uitwisselen met andere partijen.

Het gebruik van SIKB0102 is groeiende. 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.

B6.6. Domein Bouw

COINS

Over COINS zijn **geen gebruiksgegevens ontvangen**.

IFC

Feitelijk gebruik

Er zijn **geen gegevens over het feitelijk gebruik** van de standaarden IFC beschikbaar.

Wel is op te merken dat vanaf 2011 het beleid van het Rijksvastgoedbedrijf (RVB) is om IFC toe te passen door het voorschrijven van de RVB BIM Specificatie (RBS) bij PPS-contracten. RBS beschrijft de specificaties waaraan bouwwerkinformatieproducten in de vorm van 3D-modellen in het open standaard formaat IFC moeten voldoen. Verder is het sterk de vraag op welke wijze de mate van het feitelijke gebruik überhaupt op een betekenisvolle manier afgelezen kan worden. Zuiver op basis van het aantal geproduceerde IFC's geeft dit een vertekend beeld, omdat in één groot project, waar modellen opgesplitst zijn in deelmodellen, dit kan resulteren in een groot aantal IFC-bestanden, terwijl een bescheiden project slechts een handvol modellen oplevert, terwijl eigenlijk beide projecten evenwaardig en met dezelfde intenties (ook) gebruik maken van het IFC-formaat.

Omdat er geen kwantitatieve gegevens beschikbaar zijn, is een op cijfers onderbouwde vergelijking niet mogelijk. Het is wel zo dat in de praktijk het merkbaar is dat het gebruik van het IFC-formaat in de markt over het algemeen geaccepteerd en ingeburgerd is geraakt. Ook binnen een overheidsorganisatie als het Rijksvastgoedbedrijf krijgt het IFC-formaat vaste voet aan wal. Ondanks het ontbreken van harde cijfers, kan toch gesteld worden dat zowel binnen een overheidsorganisatie, als daarbuiten (in de markt) er 'meer' gebruikt gemaakt wordt van modellen in het IFC-formaat.

NLCS

Over NLCS zijn **geen gebruiksgegevens ontvangen**.

VISI

Over VISI zijn **geen gebruiksgegevens ontvangen**.

B6.7. Domein Juridische identificatie en verwijzing

BWB, ECLI en JCDR

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

Feitelijk gebruik

Het gebruik van LiDO is sinds de Monitor Open standaarden 2018 aangemerkt als graadmeter voor het gebruik van de standaarden BWB, JCDR en ECLI samen. Het gebruik is in juni 2019 gelijk gebleven aan het jaar ervoor: ongeveer 40.000 bezoekers per maand.

BWB

BWB, de Juriconnect-standaard voor identificatie van en verwijzing naar wet- en regelgeving, staat op de 'pas toe of leg uit'-lijst sinds 2 januari 2016. Deze standaard wordt ook wel "logische links naar wetgeving" genoemd. De standaard is een URI, een Uniform Resource Identifier, een unieke computerleesbare 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[21].

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.

[21] Zie ook art. 13 Bekendmakingsbesluit: wetten.overheid.nl/BWBR0025257/2009-07-01/#Hoofdstuk4_Artikel13

In wetten.nl wordt de BWB-URI, zichtbaar in de URL, achter de domeinnaam. Dat is te zien in de link in bovenstaande voetnoot. Met de URI kan overigens ook op een meer granulair niveau worden verwezen, bijvoorbeeld naar een artikel.

Ontwikkelingen
De BWB standaard heeft tekortkomingen die mogelijk opgelost kunnen worden door toepassing van de Akoma Ntoso standaard van OASIS. 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 op de 'pas toe of leg uit'- lijst sinds 28 november 2013. De JCDR standaard, eveneens een URI , werd aanvankelijk ontwikkeld binnen de Centrale Voorziening voor Decentrale Regelgeving (CVDR), in 2018 overgegaan in DROP, de voorziening voor Decentrale Regelgeving en Officiële Publicaties. In DROP kunnen decentrale overheidsorganisaties zorgen voor consolidatie en publicatie van hun regelgeving.
In de zomer van 2019 werden 517 diverse overheidsorganisaties geteld[22], die waren aangesloten op DROP. Dit waren er 471 in 2018.

Regelingen in DROP hebben een iets aangepaste URI, maar de JCDR wordt nog steeds ondersteund. JCDR is ook beschikbaar in de open data van Overheid.nl. Het is niet bekend hoe JCDR hergebruikt wordt in de open data van Overheid.nl en Rechtspraak.nl.

Ontwikkelingen
Waarschijnlijk zal de Akoma Ntoso standaard van Oasis op termijn ook toegepast worden als het gaat om identificatie van en verwijzing naar decentrale regelgeving omdat deze gebruikt zal worden voor de nieuwe STOP standaard, de Standaard voor Officiële Publicaties.

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

Ontwikkelingen
De beheerder heeft een nieuwe versie van de ECLI-standaard aangekondigd in een presentatie aan het Forum Standaardisatie in maart 2019. Definitieve vaststelling wordt zomer 2019 verwacht.

[22] koopoverheid.nl/voor-overheden/gemeenten-provincies-en-waterschappen/drop/deelnemende-organisaties-drop

B6.8. Domein Onderwijs en loopbaan

E-Portfolio NL

De standaard ePortfolio is in 2018 in opdracht van het Forum Standaardisatie geëvalueerd. De evaluatie heeft tot doel om informatie te verschaffen over de huidige relevantie van de standaard, het toepassingsgebied en de stand van zaken rond het gebruik van de standaard. De onderzoekers concluderen dat standaard nuttig is voor overheden en instellingen uit de (semi-)publieke sector en voor het lerende individu. Mede door conflicterende belangen van leveranciers wordt de standaard maar beperkt gebruikt. Er zijn geen harde cijfers beschikbaar over gebruik.

Het Forum Standaardisatie besloot de standaard E-Portfolio op de 'Pas toe of leg uit'-lijst te handhaven maar stelt als voorwaarde dat de beheerder vóór eind 2019 een implementatiestrategie opstelt om de adoptie en het gebruik van de standaard te verhogen. Als de standaard op de 'Pas toe of leg uit'-lijst blijft staan, zal de ontwikkeling van het gebruik door de tijd heen gemonitord worden.

NL LOM

De standaard NL LOM is in 2018/19 in opdracht van het Forum Standaardisatie geëvalueerd. De evaluatie heeft tot doel om informatie te verschaffen over de huidige relevantie van de standaard, het toepassingsgebied en de stand van zaken rond het gebruik van de standaard. NL LOM wordt breed toegepast door met name universiteiten. NL LOM is opgenomen als randvoorwaarde in de stimuleringsregeling Open Leermaterialen. De standaard wordt echter beperkt gebruikt door private partijen. Dat betekent dat de zoekmachines voor lesmateriaal geen volledig beeld schetsen van beschikbaar materiaal, maar met name de publieke leermaterialen tonen. Dat is een groot gemis voor de eindgebruikers, veelal docenten.

Het Forum Standaardisatie besloot de standaard NL LOM op de 'Pas toe of leg uit'-lijst te handhaven maar adviseert de beheerder Bureau EDUstandaard om te kijken hoe gebruik vereenvoudigd kan worden en internationale ontwikkelingen op dit gebied te volgen (m.n. IEEE LOM). Een jaar na de evaluatie wordt over de voortgang en/of resultaten gerapporteerd aan het Forum. Als de standaard op de 'Pas toe of leg uit'-lijst blijft staan, zal de ontwikkeling van het gebruik door de tijd heen gemonitord worden.

B6.9. Domein Overig

EML_NL

EML_NL is het Nederlands toepassingsprofiel op de Election Markup Language standaard. Met EML_NL wordt gedefinieerd welke gegevens en in welke vorm de uitwisseling van digitale gegevens bij verkiezingen (die vallen onder de Nederlandse Kieswet) dient plaats te vinden (zoals gegevens over kandidaten of deeluitslagen) om de verkiezingsuitslag en zetelverdeling vast te kunnen stellen. EML_NL draagt ertoe bij dat het verkiezingsproces transparant plaatsvindt en met minder kans op overname- en optelfouten. De standaard staat op de 'pas toe of leg uit'-lijst sinds 28 november 2013.

Feitelijk gebruik

De EML_NL standaard is opgenomen in de Ondersteunende Software Verkiezingen, hierna "OSV". Het gebruik van OSV is daarmee een indicator voor het gebruik van de EML_NL standaard. OSV wordt toegepast bij verkiezingen die onder de Kieswet vallen en is derhalve in de periode 2018-2019 beschikbaar gesteld bij onderstaande verkiezingen en aan de volgende overheidsorganisaties.

Reguliere gemeenteraadsverkiezingen op 21 maart 2018: OSV beschikbaar gesteld aan

- ongeveer 2.200 politieke partijen die lokaal deelnamen aan de gemeenteraadsverkiezingen;
- 335 gemeenten.

Gemeentelijke herindelingsverkiezingen op 21 november 2018: OSV beschikbaar gesteld aan

- ongeveer 80 politieke partijen die lokaal deelnamen aan de herindelingsverkiezingen;
- 12 gemeenten.

Provinciale statenverkiezingen en leden van het algemeen bestuur van de waterschappen op 20 maart 2019: OSV beschikbaar gesteld aan

- ongeveer 180 politieke partijen;
- 355 gemeenten (waarbij tevens 20 gemeenten de rol van hoofdstembureau en 12 gemeenten tevens de rol van centraal stembureau vervullen)
- 21 waterschappen (in hun rol als hoofd en centraal stembureau).

Verkiezing voor de Nederlandse leden van het Europees Parlement op 23 mei 2019 en verkiezing voor de Eerste Kamer op 27 mei 2019: OSV beschikbaar gesteld aan

- ongeveer 20 politieke partijen;
- 355 gemeenten (waarbij tevens 19 gemeenten de rol van hoofdstembureau vervullen) en aan de Kiesraad als centraal stembureau.

Na afloop van alle hierboven genoemde verkiezingen zijn EML_NL bestanden aan de Kiesraad verstrekt en als dataset beschikbaar gesteld op data.overheid.nl.

B7. Rapportage IV-meting maart 2019

Forum Standaardisatie

Meting informatieveiligheidstandaarden maart 2019

Datum 24 april 2019
Status Versie 1.01

Inleiding

Burgers en ondernemers moeten erop kunnen vertrouwen dat gegevensuitwisseling met de overheid en tussen overheden veilig verloopt. Hiervoor dienen overheden meerdere informatieveiligheidstandaarden te implementeren. Recente phishing-incidenten waarin e-mails en websites van de overheid werden nagemaakt onderstrepen nogmaals het belang van overheidsbrede adoptie van deze standaarden. Binnen de overheid zijn daarom implementatieafspraken gemaakt over standaarden voor het beveiligen van mail en websites.

Om de voortgang van deze afspraken bij te houden voert het Forum twee keer per jaar een meting uit op de implementatie van informatieveiligheidstandaarden bij overheidsorganisaties. Voorliggende meting dateert van maart 2019, waarbij 563 domeinnamen zijn getoetst. Uit deze meting blijkt dat het stijgende gebruik van de standaarden doorzet.

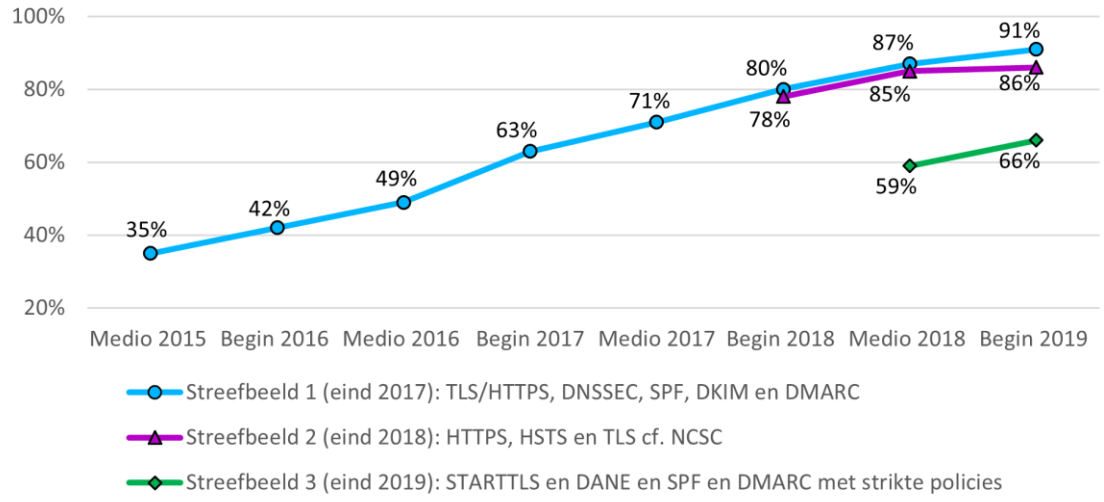
1. Samenvatting

Het gebruik van de informatieveiligheidstandaarden is afgelopen jaar wederom gegroeid. De webstandaarden doen het gemiddeld beter dan de mailstandaarden (89% vs 74%). De adoptie van mailstandaarden groeit echter harder door dan die van de webstandaarden. We zien dat voor sommige standaarden de individuele overheidslagen 100% scoren. Alle provincies maken gebruik van de anti-phishing standaard SPF en passen bovendien de juiste policy toe. Daarnaast maken alle waterschappen gebruik van de standaarden voor beveiligde verbindingen van websites HTTPS en TLS.

De adoptiegraad van de webstandaard HSTS (79%) is in het afgelopen halfjaar niet gestegen. Ook de relatief lage adoptiegraden van de mailstandaarden DMARC met strikte policy (37%) en DANE (41%) vragen bijzondere aandacht.

Eind 2018 is de tweede streefbeeldafspraak afgelopen. De streefbeeldafspraak heeft nog niet geleid tot 100% adoptie van de betreffende standaarden (HTTPS, HSTS en TLS inclusief de veilige configuratie conform NCSC). Tot eind 2019 loopt er een derde streefbeeldafspraak voor de adoptie en configuratie van een aantal mailstandaarden (STARTTLS en DANE, en SPF en DMARC met strikte policies).

Gemiddelde adoptiegroei per streefbeeldafspraak



Hoewel de gemiddelde adoptie van informatieveiligheidstandaarden in de afgelopen 3 jaar sterk is gegroeid zijn we er nog niet. Zonder aanvullende inspanningen zal zo goed als volledige adoptie van de informatieveiligheidstandaarden lastig te realiseren zijn. Door de inspanningen te concentreren op grotere dienstverleners en een ‘één op één’ benadering voor achterblijvers te hanteren, kan de adoptie mogelijk verder worden gebracht. Ook het wettelijke verplichten van informatieveiligheidstandaarden kan helpen om de achterblijvers zo ver te krijgen dat ze de standaarden ondersteunen.

2. Achtergrond

Sinds 2015 biedt het Platform Internetstandaarden[23] de mogelijkheid om via de website Internet.nl domeinen te toetsen op het gebruik van een aantal moderne internet-standaarden, 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.

Voorliggende rapportage bevat tevens de eindmeting van de tweede streefbeeldafspraak die eind 2018 afliep.

2.1 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

[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/iv-meting-en-afspraken

2.2 Om welke domeinnamen gaat het

In totaal zijn in deze meting 563 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.

Ten opzichte van de vorige meting is de lijst geactualiseerd. Hierdoor zijn er nieuwe domeinnamen bijgekomen en zijn niet-relevante domeinnamen verwijderd. De reden hiervoor kan verschillen, bijvoorbeeld omdat er een gemeentelijke herindeling heeft plaatsgevonden of dat er waterschappen zijn samengevoegd. Ook is de lijst met best bezochte domeinnamen aangepast en zijn alle organisaties uit de Manifestgroep en Klein Lef toegevoegd.

Het betreft echter nog steeds een selectie van domeinnamen. 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 deze domeinen garandeert geenszins dat hiermee *alle* overheidsdomeinen beschermd zijn tegen bijvoorbeeld phishing. Mocht uwer inziens een relevante domeinnaam ontbreken dan verzoeken we om deze aan ons door te geven.

2.3 Hoe wordt gemeten

De meting geeft de stand van zaken weer op de peildatum 21 maart 2019. De meting laat zien of op een domeinnaam de standaarden worden toegepast.

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. Overigens heeft de score die een domeinnaam op Internet.nl kan halen (namelijk max. 100%) geen relatie met het resultaat uit deze meting aangezien wij toetsen op een subset van de standaarden. De website Internet.nl is een initiatief van het Platform Internetstandaarden. In het platform participeren verschillende partners uit de internetgemeenschap (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.

In de meting wordt alleen gekeken naar de toepassing van standaarden op domeinnamen. Er wordt in de meting (nog) niet gekeken naar de andere ontvangende kant, bijvoorbeeld de controle op DMARC door bijvoorbeeld e-mailproviders van consumenten, en validatie van DNSSEC en DANE.

2.4 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.

2.4.1 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 voor 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)[27]. 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	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 voor 2019 aan te voldoen.

2.4.2 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 is om hier voor 2020 aan te voldoen
DKIM	Met DKIM kunnen e-mailberichten worden gewaarmerkt. De ontvanger van een e-mail kan op die manier controleren of een e-mailbericht écht van de afzender afkomstig is en of het bericht onderweg ongewijzigd is gebleven.

[27] Zie https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html. Een wijziging ten opzichte van de vorige meting is dat in de huidige meting ook de vertrouwensketen van het certificaat wordt meegenomen in de test voor TLS conform NCSC.

	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 is 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[28]	Net zoals bij HTTPS kan er bij STARTTLS gebruik worden gemaakt van verschillende versies van het TLS en verschillende versleutelingsstandaarden (ciphers). Aangezien niet alle versies en combinaties als voldoende veilig worden beschouwd, is het belangrijk om hierin de juiste keuze te maken en ook regelmatig te controleren of de gebruikte instellingen nog veilig zijn. Getest wordt of STARTTLS is geconfigureerd zoals door het NCSC is aanbevolen. De streefbeeldafspraak is om hier voor 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 is 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.

[28] https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html

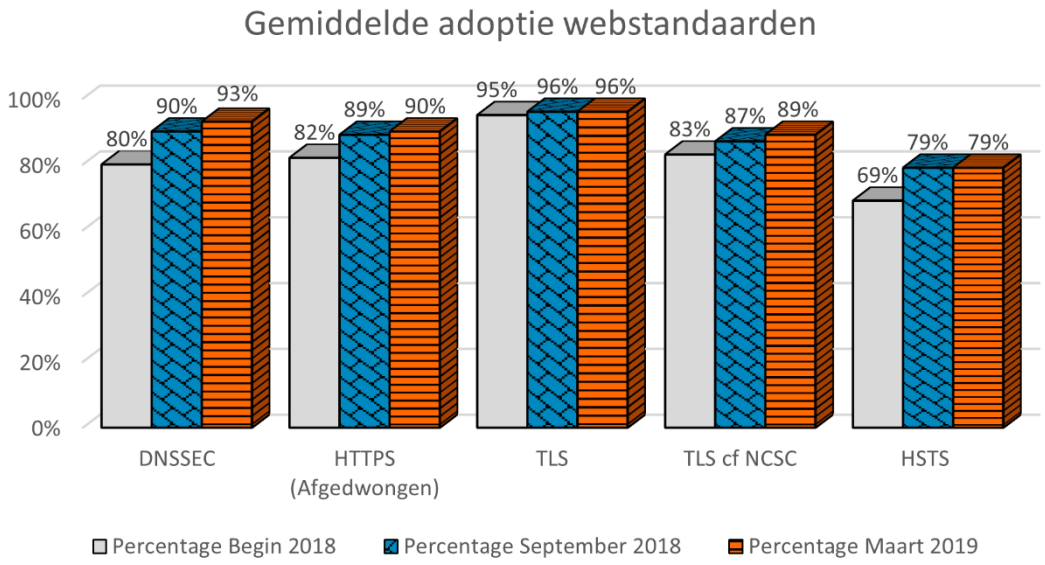
3. Resultaten meting maart 2019

Op 21 maart heeft het Bureau Forum Standaardisatie de meting uitgevoerd. De resultaten zijn voorgelegd aan een aantal koepelorganisaties en stakeholders en geactualiseerd indien nodig. Naast de resultaten per standaard en per "overheidslaag" zoals bij voorgaande metingen, bevat deze meting tevens het perspectief van de verschillende streefbeelden. Dit laat duidelijk zien hoe het met de adoptie van de standaarden per streefbeeld is gesteld.

3.1 Per standaard

De onderstaande grafiek toont de adoptiestatus van de individuele standaarden voor zowel de webstandaarden als de mailstandaarden. Daar waar mogelijk is er een vergelijking gemaakt met de voorgaande metingen van 2018.

Gemiddelde adoptie webstandaarden

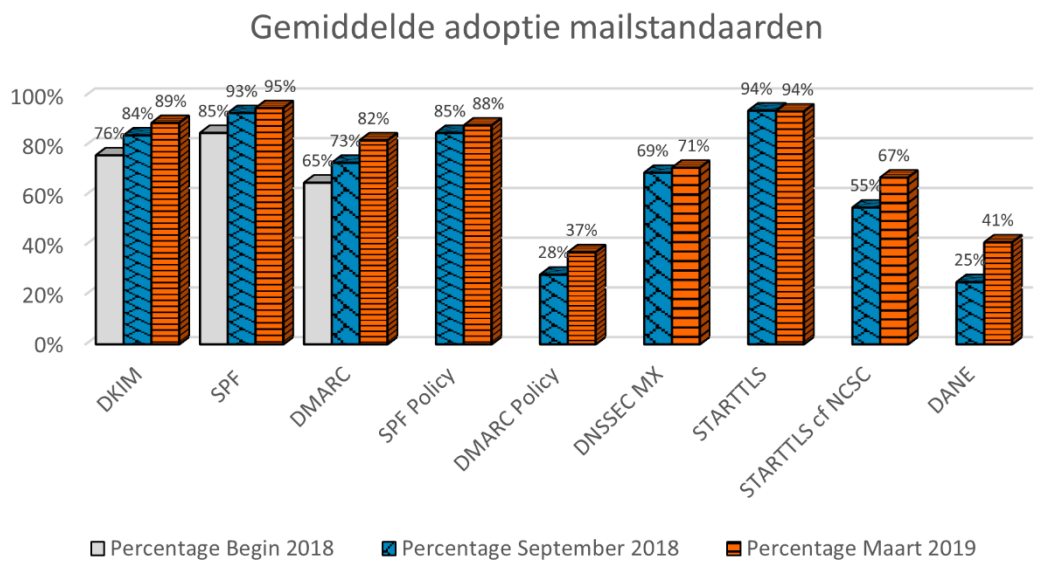


Allereerst is de gemiddelde adoptie van deze standaarden hoog. Het gemiddelde van alle webstandaarden samen is inmiddels 89% HSTS trekt dit gemiddelde iets omlaag en blijft steken op 79%. Voor TLS en HSTS geldt bovendien dat het afgelopen halve jaar de groei is gestagneerd. Voor de overige standaarden geldt dat de groei nog wel aanwezig is, hetzij beperkt. Om de adoptie van deze standaarden verder te stimuleren is een 'één op één' benadering nodig om de 100% te halen.

De gemiddelde adoptie van de mailstandaarden (visualisatie op de volgende pagina) ligt met 73% lager dan de webstandaarden. Dit is enerzijds te verklaren door de grotere hoeveelheid standaarden waaraan voldaan moet worden en anderzijds geldt voor een deel van de standaarden pas sinds begin 2018 een streefbeeldafspraak die loopt tot eind 2019. Waar de gemiddelde adoptiegraad hier lager ligt dan bij de webstandaarden is de groei gemiddeld groter. Hoewel de groei van DANE het afgelopen halfjaar het grootst is, met een sprong van 25% naar 41%, is de adoptiegraad relatief laag en vraagt de implementatie aandacht. Ook de adoptiegraad van DMARC met strikte configuratie (DMARC policy) is

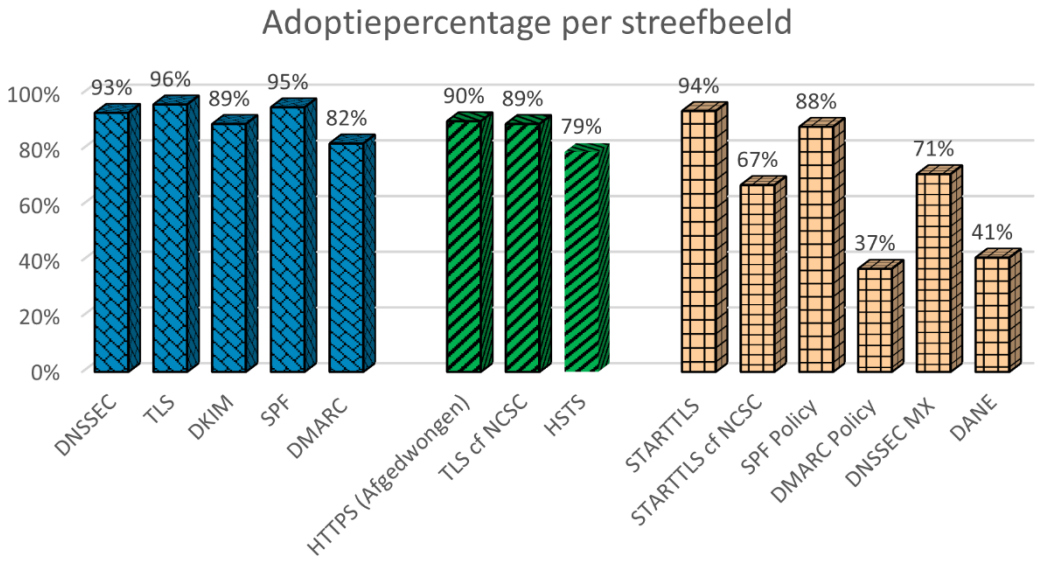
relatief gezien laag en vraagt aandacht. De streefbeeldafspraken rond DANE en DMARC policy lopen eind 2019 af.

Gemiddelde adoptie mailstandaarden



3.2. Per streefbeeldafspraak

Adoptiepercentage per streefbeeld



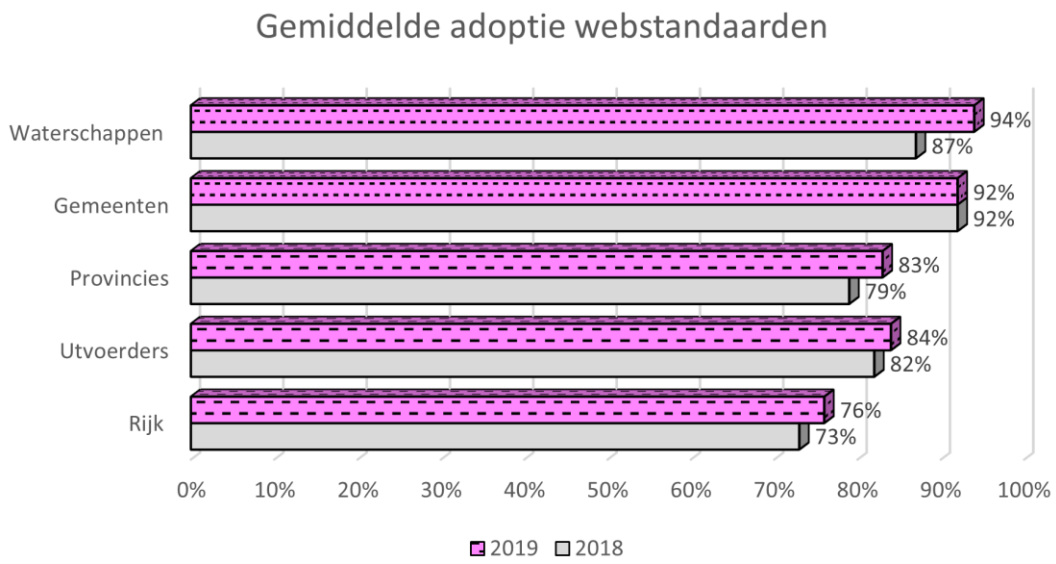
Bovenstaande grafiek verdeelt de standaarden over de drie streefbeeldafspraken van het OBDO. De eerste set standaarden (blauw) uit het streefbeeld dat eind 2017 afliep worden gemiddeld het meest toegepast, maar ook begin 2019 is voor deze standaarden de gewenste 100% adoptie nog niet gehaald.

De deadline voor tweede streefbeeldafspraak (oranje) was eind 2018. Ook voor deze standaarden geldt dat de gemiddelde adoptie hoog is, maar de 100% nog niet is behaald. Voor deze standaarden: HTTPS, 'TLS conform NSCS' en HSTS is er het voornemen een Algemene Maatregel van Bestuur (AMvB) op te stellen[29]. Deze AMvB is naar verwachting in 2020 van kracht en dwingt partijen die ondanks de streefbeeldafspraken de standaarden nog steeds niet toepassen, dat alsnog te doen.

De gemiddelde adoptie van de standaarden uit de derde streefbeeldafspraak (groen) is het laagst. Deze streefbeeldafspraak loopt tot eind 2019. Zonder extra inspanning van alle betrokken partijen is het onwaarschijnlijk dat dit streefbeeld wel wordt gehaald.

3.3 Per overheidslaag

Gemiddelde adoptie webstandaarden

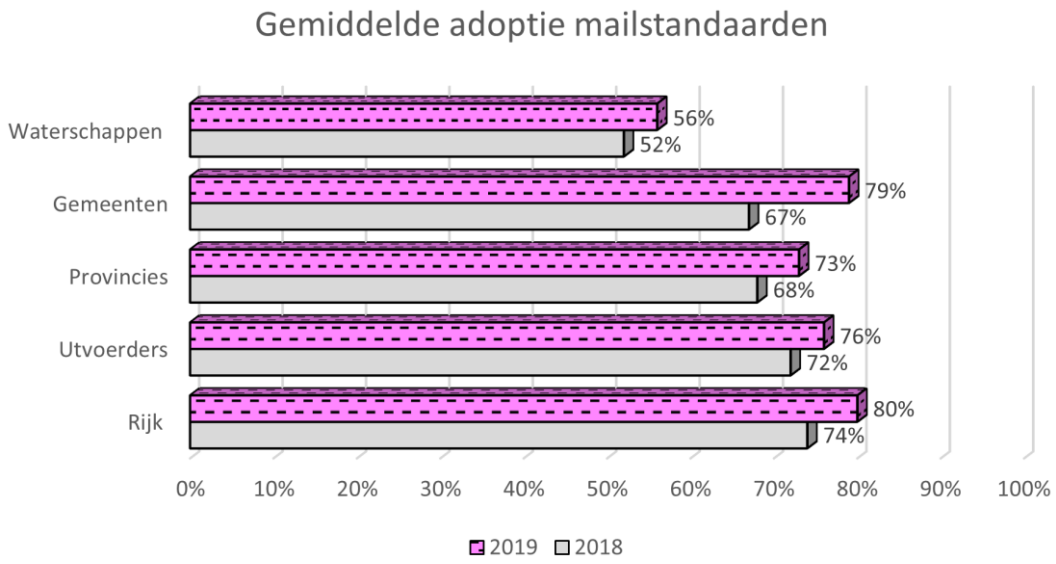


Een uitsplitsing van de resultaten van de webstandaarden naar overheidslaag laat zien dat in iedere overheidslaag de adoptie groeit. De waterschappen en gemeenten scoren gemiddeld respectievelijk 94 en 92%. Het Rijk blijft iets achter met een score van 76%. De mate van groei verschilt wel sterk, met name de waterschappen zijn sterk gegroeid met gemiddeld 7 procentpunt over het afgelopen halve jaar.

Het beeld is anders bij de mailstandaarden (visualisatie op de volgende pagina). Hier blijven de waterschappen gemiddeld juist iets achter op de andere overheidslagen. Het Rijk heeft bij de mailstandaarden gemiddeld de hoogste adoptiegraad. Verderop in de rapportage wordt per overheidslaag toegelicht welke standaarden gemiddeld veel worden toegepast en welke minder.

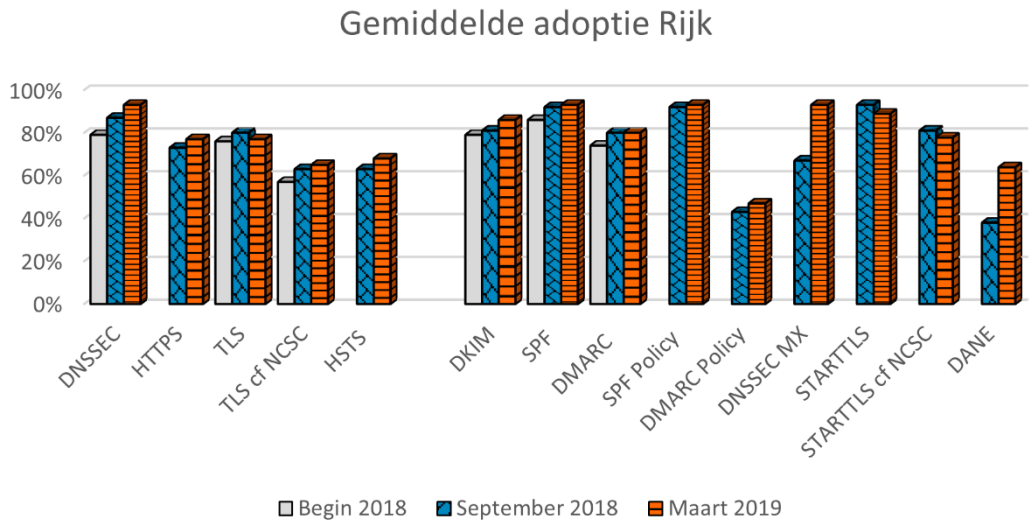
[29] Op basis van artikel 2 van het wetsvoorstel Wet digitale overheid.

Gemiddelde adoptie mailstandaarden



3.2.1 Het Rijk

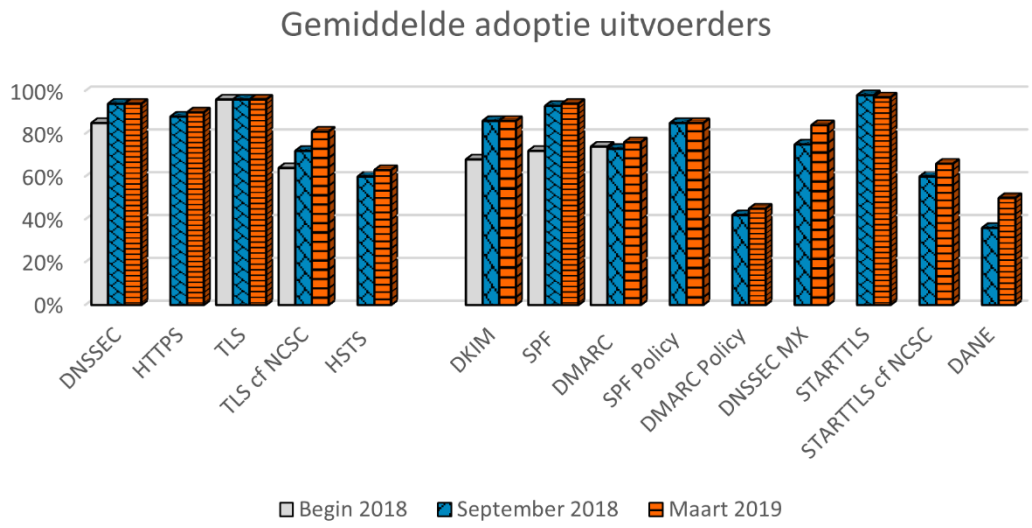
Gemiddelde adoptie Rijk



Het Rijk scoort gemiddeld goed als het gaat om de mailstandaarden. Met name DMARC en DANE scoren hier hoog t.o.v. de andere overheidslagen. Dit komt waarschijnlijk doordat het beheer van de mailservers bij een relatief klein aantal partijen belegd is. Een aanpassing bij die partijen heeft daarom grote impact op de score van het rijk. TLS en HTTPS blijven t.o.v. de andere overheidslagen achter. Dit komt deels door het relatief grote aantal redirect domeinen dat nog niet voorzien is van de standaarden. Redirect domeinen zijn domeinen waar geen website op gehost wordt, maar die doorverwijzen naar een ander domein. Bijvoorbeeld minbzk.nl (en vele andere departementale domeinen die vooral gebruikt worden voor de mailextensie) verwijst door naar rijksoverheid.nl.

3.2.2 Uitvoering

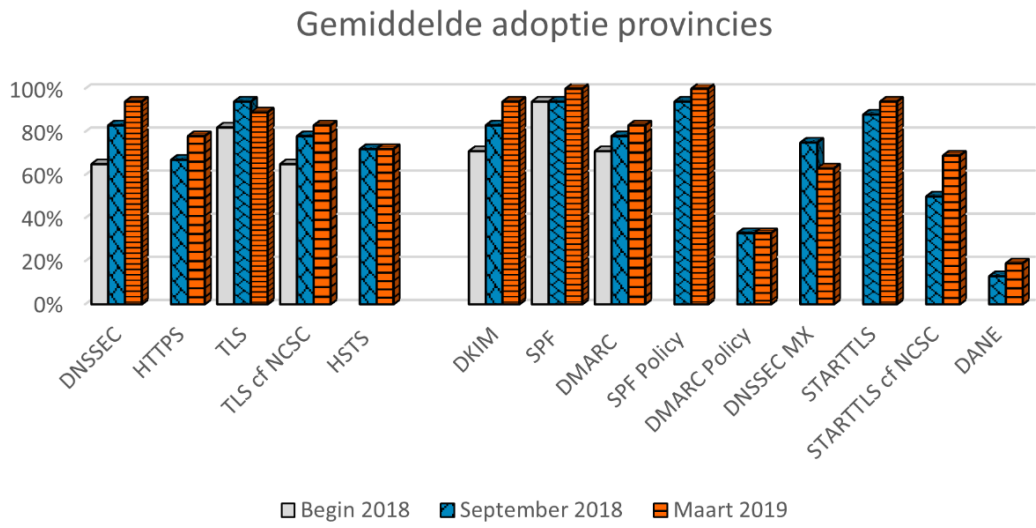
Gemiddelde adoptie uitvoerders



De uitvoerders vormen een degelijke middenmoter. Met name op het vlak van de mailstandaarden was het afgelopen half jaar de groei t.o.v. de andere overheidslagen groot. Opvallend is de score voor STARTTLS, deze is afgelopen half jaar 1 procentpunt gedaald.

3.2.3 Provincies

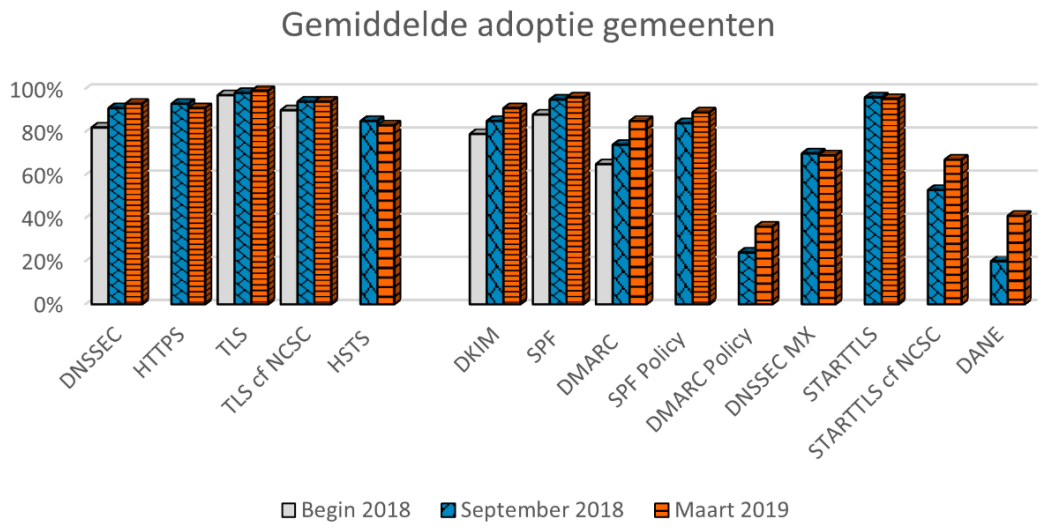
Gemiddelde adoptie provincies



Hoewel niet goed zichtbaar in bovenstaande grafiek, hebben de provincies samen met de waterschappen de afgelopen 2 jaar een enorme inhaalslag gemaakt. Meest opvallende is dat **alle** provincies gebruik maken van SPF en bovendien de juiste policy toepassen. Ze scoren op beide items 100%. De score van DNSSEC op mailservers (DNSSEC MX) lijkt vreemd genoeg te zijn gedaald. Hier is momenteel geen eenduidige verklaring voor.

3.2.4 Gemeenten

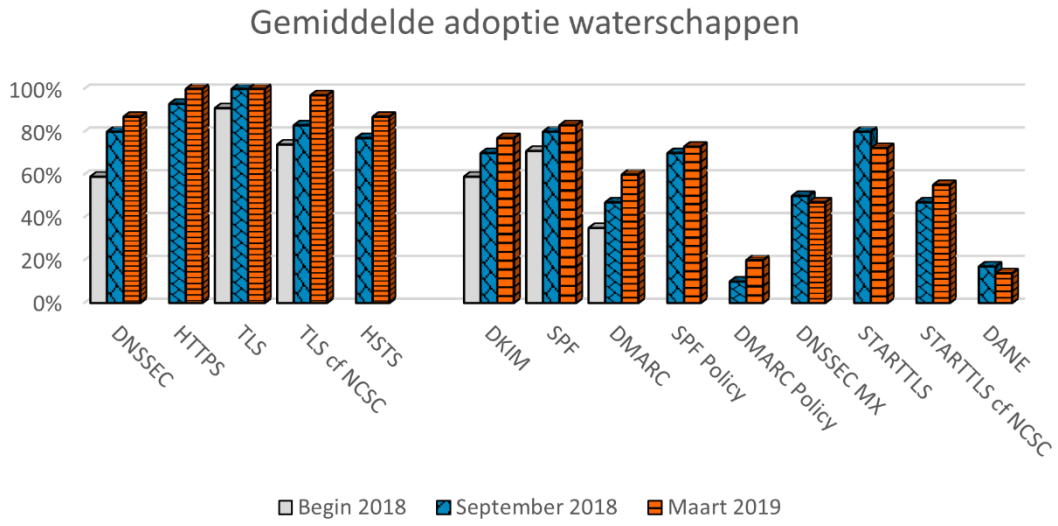
Gemiddelde adoptie gemeenten



Als we web- en mailstandaarden samen bekijken, scoren de gemeenten gemiddeld het best van alle overheidslagen. 99% van alle gemeentedomeinen in deze meting zijn voorzien van TLS. 94% is bovendien optimaal veilig geconfigureerd volgens de aanbevelingen van het NSCS. Het feit dat de gemeenten met afstand de meeste domeinen bezitten in onze test (388 van de 563) maakt de hoge scores nog indrukwekkender.

3.2.5 Waterschappen

Gemiddelde adoptie waterschappen



Naast dat de Waterschappen de afgelopen twee jaar zijn verschoven van de achterhoede naar de voorlopers als het gaat om de gemiddelde adoptie van de standaarden, scoren zij

ook nog eens 100% op HTTPS en TLS adoptie. Ook de score voor de optimale configuratie van TLS (TLS conform NCSC) is erg hoog met 97%. Wat betreft de mailstandaarden blijven de waterschappen gemiddeld wat achter op de andere overheidslagen. Met name het toepassen van DMARC met de juiste strikte policy en DANE blijft achter.

4. Conclusie

Het gebruik van de informatieveiligheidstandaarden is afgelopen jaar wederom gegroeid. De webstandaarden doen het gemiddeld beter dan de mailstandaarden (89% vs 74%). De adoptie van mailstandaarden groeit echter harder door dan die van de webstandaarden. We zien dat voor sommige standaarden de individuele overheidslagen 100% scoren. Alle provincies maken gebruik van de anti-phishing standaard SPF en passen bovendien de juiste policy toe. Daarnaast maken alle waterschappen gebruik van de standaarden voor beveiligde verbindingen van websites HTTPS en TLS.

4.1 Webstandaarden

De gemiddelde adoptie van alle webstandaarden is inmiddels **89%**. HSTS trekt dit gemiddelde iets omlaag en blijft steken op 79%. Voor TLS (96%) en HSTS (79%) geldt bovendien dat de groei het afgelopen half jaar is gestagneerd. Voor de overige standaarden geldt dat de groei nog wel aanwezig is, hetzij beperkt. Om de adoptie van deze standaarden verder te stimuleren is een meer gerichte benadering nodig om de 100% te halen.

4.2 E-mailstandaarden

De gemiddelde adoptie van de mailstandaarden ligt met **74%** lager dan de webstandaarden. Dit is niet vreemd aangezien er meer mailstandaarden zijn, en voor een deel van de standaarden pas sinds begin 2018 een streefbeeldafspraak is die loopt tot eind 2019. Waar de gemiddelde adoptiegraad hier lager ligt dan bij de webstandaarden is de groei gemiddeld groter. De adoptiegraden van DMARC met strikte policy (37%) en DANE (41%) zijn relatief gezien laag en vragen bijzondere aandacht.

4.3 Streefbeeldafspraken

Eind 2018 is de tweede streefbeeldafspraak afgelopen. De streefbeeldafspraak heeft nog niet geleid tot 100% adoptie van de betreffende standaarden. De afspraak was dat ALLE overheidswebsites HTTPS, HSTS en TLS inclusief de veilige configuratie conform NCSC uiterlijk eind 2018 hebben ingevoerd. De adoptiepercentages zijn 90% voor HTTPS, 89% voor TLS conform NCSC richtlijn en 79% voor HSTS.

Tot eind 2019 loopt er een derde streefbeeldafspraak voor de adoptie en configuratie van een aantal mailstandaarden (STARTTLS en DANE, en SPF en DMARC met strikte policies).

4.4 Handelingsperspectief

Hoewel de gemiddelde adoptie van informatieveiligheidstandaarden in de afgelopen 3 jaar sterk is gegroeid zijn we er nog niet. Zonder aanvullende inspanningen zal zo goed als volledige adoptie van de mailstandaarden uit de derde streefbeeldafspraak eind 2019 lastig te realiseren zijn. Dit geldt in minder mate ook voor de web- en mailstandaarden uit de eerste en tweede streefbeeldafspraken. Belangrijk is om per doelgroep te kijken welke standaarden extra aandacht nodig hebben en of er 'quick wins' te behalen zijn. Om voor de webstandaarden toch 100% te halen, is het misschien mogelijk om organisaties individueel aan te spreken en te helpen. Dit bij voorkeur via de koepelorganisaties. Om de adoptie van mailstandaarden verder te brengen is het een optie om de grotere mailleveranciers in beweging te krijgen. Daarnaast kan een wettelijke verplichting helpen om de achterblijvers zo ver te krijgen dat ze de standaarden ondersteunen. Voor HTTPS, TLS geconfigureerd volgens de aanbevelingen van het NCSC en HSTS, is het ministerie van BZK voornemens de standaard te verplichten door middel van een algemene maatregel van bestuur (AMvB) op basis van het wetsvoorstel Wet digitale overheid. Of dit ook voor andere informatieveiligheid-standaarden een goede optie is, wordt door het ministerie van Binnenlandse Zaken bekeken na het verlopen van de laatste streefbeeldafspraak eind dit jaar.

B8. Rapportage IV-meting september 2019

Forum Standaardisatie

Meting informatieveiligheidstandaarden september 2019

Datum 1 november 2019
Status Definitief t.b.v. OBDO

Managementsamenvatting

De Meting Informatieveiligheidstandaarden heeft betrekking op een aantal informatie-veiligheidsstandaarden waarvoor, in aanvulling op pas-toe-of-leg-uit, overheidsbrede streefbeeldafspraken met uiterlijke implementatiedata zijn gemaakt door het Nationaal Beraad en door het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO).

Eind 2019 loopt de deadline van de derde overheidsbrede streefbeeldafspraak af. Deze streefbeeldafspraak gaat over het implementeren van STARTTS en DANE (om vertrouwelijkheid van mailverkeer te borgen) en het voldoende strikt configureren van SPF en DMARC (om mailspoofing tegen te gaan). In het afgelopen half jaar is de adoptiegraad van deze standaarden met gemiddeld 5% gegroeid. Daarmee ligt het groeitempo iets lager dan dat van de vorige meting, waar we nog 7% groei zagen.

Specifiek ten aanzien van de derde streefbeeldafspraak is het gebruik van STARTTLS voor beveiligde mailverbindingen gegroeid met 3% naar 97%. Het gebruik van STARTTLS conform de NCSC richtlijnen is gegroeid met 9% naar 76%. Het faciliteren van DANE voor het afdwingen van met STARTTLS beveiligde mailverbindingen bij het ontvangen van mail is gegroeid met 4% naar 45%. En tot slot is het toepassen van DMARC met strikte policy om mailspoofing tegen te gaan gegroeid met 12% naar 49%.
In algemene zin is gebruik van de informatieveiligheidstandaarden het afgelopen jaar wederom gegroeid. De webstandaarden worden gemiddeld beter toegepast dan de mailstandaarden (92% vs 77%). Waar de gemiddelde groei in gebruik van mailstandaarden in de vorige meting nog hoger was dan dat van de webstandaarden, is deze inmiddels gelijk met ongeveer 3% ten opzichte van een half jaar geleden.

Meest opvallende resultaten uit deze meting zijn de groei in gebruik van webstandaarden bij het Rijk, en de achteruitgang in toepassing van DNSSEC op mailservers.

Het Rijk heeft een flinke inhaalslag gemaakt met betrekking tot de standaarden voor het versleutelen van webverkeer (HTTPS en HSTS). Dit komt doordat een aantal doorverwijzende domeinen (redirects) van de ministeries recent voorzien zijn van HTTPS. Het gaat om domeinen die voornamelijk voor mail worden gebruikt, waar geen website op gehost wordt, maar die doorverwijzen naar een ander domein. Bijvoorbeeld minbzk.nl dat doorverwijst naar www.rijksoverheid.nl.

De oorzaak van de neerwaartse trend in toepassing van DNSSEC op mailservers (een randvoorwaarde voor DANE) is dat een aantal provincies en gemeenten de overstap naar Microsoft Office 365 Exchange Online heeft gemaakt, dit product biedt vooralsnog geen ondersteuning voor DNSSEC en DANE. Dit is een duidelijk zorgpunt voor de vertrouwelijkheid van overheidsmail, omdat deze overheidsorganisaties niet altijd een versleuteld mailtransport kunnen afdwingen en tevens niet aan de streefbeeldafspraak omtrent het gebruik van DANE kunnen voldoen. Desondanks groeit het gebruik van DANE overheidsbreed nog steeds, en zien we bij het Rijk al een adoptiegraad van 75%.

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.

Om de voortgang van deze afspraken bij te houden voert het Forum twee keer per jaar een meting uit op de implementatie van informatieveiligheidstandaarden bij overheidsorganisaties. Voorliggende meting dateert van september 2019, waarbij 548 domeinnamen zijn getoetst. Uit deze meting blijkt dat het stijgende gebruik van de standaarden doorzet. Tegelijkertijd resteren er nog wel uitdagingen om het niveau van informatieveiligheid rondom domeinen, websites en e-mail naar een hoger plan te tillen.

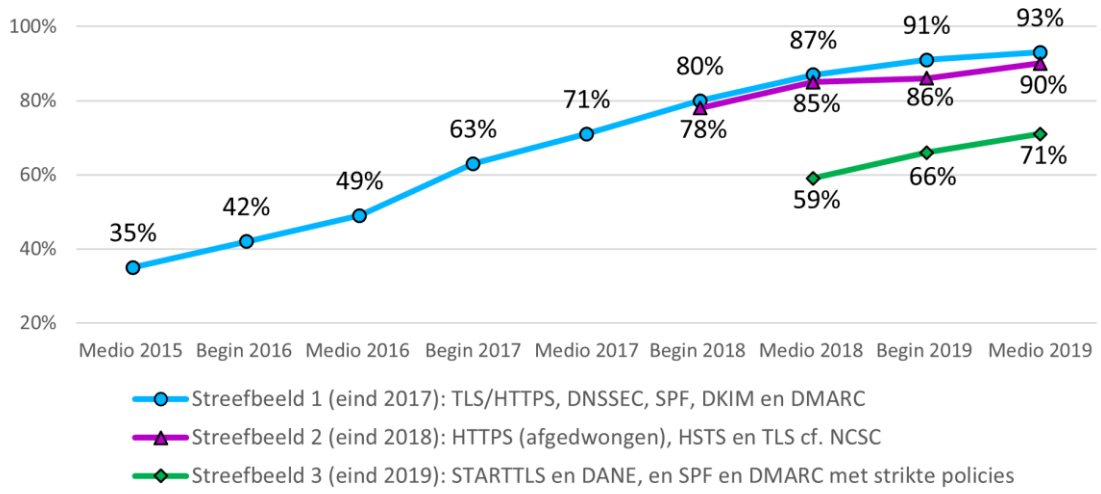
2. Conclusie

Het gebruik van de informatieveiligheidstandaarden is afgelopen half jaar wederom gegroeid. De webstandaarden worden gemiddeld beter toegepast dan de mailstandaarden (92% vs 77%). Waar de gemiddelde groei in gebruik van mailstandaarden in de vorige meting nog hoger was dan dat van de webstandaarden, is deze inmiddels gelijk met ongeveer 3% ten opzichte van een half jaar geleden.

2.1 Streefbeeldafspraken

Eind 2019 loopt de deadline van de derde overheidsbrede streefbeeldafspraak af. Deze streefbeeldafspraak gaat over het implementeren van STARTTS en DANE (om vertrouwelijkheid van mailverkeer te borgen) en het voldoende strikt configureren van SPF en DMARC (om mailspoofing tegen te gaan). In het afgelopen half jaar is de adoptiegraad van deze standaarden met gemiddeld 5% gegroeid. Daarmee ligt het groeitempo iets lager dan dat van de vorige meting, waar we nog 7% groei zagen. Onderstaande grafiek toont de overheidsbrede voortgang in het voldoen aan deze en eerdere streefbeeldafspraken.

Gemiddelde adoptiegroei per streefbeeldafspraak



Specifiek ten aanzien van de derde streefbeeldafspraak is het gebruik van STARTTLS voor beveiligde mailverbindingen gegroeid met 3% naar 97%. Het gebruik van STARTTLS conform de NCSC richtlijnen is gegroeid met 9% naar 76%. Het faciliteren van DANE voor het afdwingen van met STARTTLS beveiligde mailverbindingen bij het ontvangen van mail is gegroeid met 4% naar 45%. En tot slot is het toepassen van DMARC met strikte policy om mailspoofing tegen te gaan gegroeid met 12% naar 49%.

2.2 Webstandaarden

De gemiddelde adoptie van alle webstandaarden is inmiddels **92%**.

De gemeenten scoren het beste op het gebruik van de webstandaarden met gemiddeld 95% adoptie van de webstandaarden. Positief is dat ondanks de al hoge statistieken uit de vorige meting er wederom een zichtbare groei is. Het feit dat de gemeenten met afstand de

meeste domeinen bezitten in onze test (365 van de 548) maakt de hoge scores nog indrukwekkender.

Het Rijk heeft een flinke inhaalslag gemaakt met betrekking tot de standaarden voor het versleutelen van webverkeer (HTTPS en HSTS). Dit komt doordat een aantal doorverwijzende domeinen (redirects) van de ministeries recent voorzien zijn van HTTPS. Het gaat om domeinen waar geen website op gehost wordt, maar die doorverwijzen naar een ander domein. Bijvoorbeeld minbzk.nl (en vele andere departementale domeinen die vooral gebruikt worden voor de mailextensie) verwijst door naar rijksoverheid.nl. Als gevolg hiervan zien we bij het Rijk 17% groei in de implementatie van TLS voor het web (HTTPS) naar 94%.

Overheidsbreed zien we een groei van 6% in de toepassing van HSTS, waar dat in de vorige meting nog volledig was gestagneerd. In algemene zin is er nog wel ruimte voor groei bij het toepassen van HSTS (85%) en het veilig configureren van TLS (krap 92%).

Met name de uitvoerders en provincies zullen meer aandacht moeten geven aan het toepassen van de webstandaarden, omdat we bij beide overheidslagen een algehele stagnatie zien.

2.3 E-mailstandaarden

De gemiddelde adoptie van de mailstandaarden ligt met **77%** lager dan de webstandaarden. Dit is niet vreemd aangezien er meer mailstandaarden zijn, en voor een deel van de standaarden pas sinds begin 2018 een streefbeeldafspraak is die loopt tot eind 2019. Wel valt op dat het groeitempo lager is dan het voorgaande half jaar; in de vorige meting zagen we nog 7% groei, waar dit nu 3% is.

De waterschappen hebben de grootste groei in gebruik van mailstandaarden doorgemaakt met 12%. Toch blijven de waterschappen met een gemiddelde adoptie van 66% flink achter lopen op de andere overheidslagen.

Hoewel de uitvoerders in de vorige meting nog een grote groei in het gebruik van mailstandaarden toonden, zien we nu een lichte terugval. Specifiek valt de achteruitgang in het gebruik van DKIM op bij zowel de uitvoerders, het Rijk, en de provincies.

In algemene zin ligt de uitdaging met name bij het strikt configureren van de DMARC policy (49%), het toepassen van DANE (45%), en het veilig configureren van STARTTLS (76%).

In relatie tot DANE valt de neerwaartse trend van DNSSEC op de mailservers (MX) op, van 71% naar 67%. DNSSEC is een randvoorwaarde voor de betrouwbaarheid van DANE. De oorzaak van de neerwaartse trend is dat een aantal gemeenten en provincies de overstap naar Microsoft Office 365 Exchange Online hebben gemaakt, dit product biedt vooralsnog geen ondersteuning voor DNSSEC, en daarmee ook geen ondersteuning voor DANE. Dit is een duidelijk zorgpunt voor de betrouwbaarheid van overheidsmail, omdat deze gemeenten en provincies niet altijd een versleuteld mailtransport kunnen afdwingen en tevens niet aan de streefbeeldafspraak omtrent het gebruik van DANE kunnen voldoen. Desondanks is het gebruik van DANE overheidsbreed met 4% gegroeid, en zien we bij het Rijk al een

adoptiegraad van 75%. Er is nog extra groeipotentieel voor DANE, gezien de adoptiegraad van DNSSEC op de mailservers met 67% nog wel hoger ligt dan dat van DANE (45%).

Strategisch Leveranciersmanagement Rijk (onderdeel van het Ministerie van Justitie en Veiligheid) is in samenwerking met Forum Standaardisatie in gesprek met Microsoft om ondersteuning van DANE hoger op de roadmap van Microsoft te krijgen.

2.4 Handelingsperspectief

Hoewel de gemiddelde adoptie van informatieveiligheidstandaarden in de afgelopen 3 jaar sterk is gegroeid zijn we er nog niet. Tot eind 2019 loopt de derde streefbeeldafspraak voor de adoptie en configuratie van een aantal mailstandaarden (STARTTLS en DANE, en SPF en DMARC met strikte policies). Zonder aanvullende inspanningen zal zo goed als volledige adoptie van de mailstandaarden uit de derde streefbeeldafspraak eind 2019 lastig te realiseren zijn. Dit geldt in minder mate ook voor de web- en mailstandaarden uit de eerste en tweede streefbeeldafspraken.

Allereerst is het van belang dat overheidsorganisaties hun verantwoordelijkheid nemen en domeinen, websites en e-mail adequaat beveiligen en daarin de informatieveiligheidstandaarden meenemen.

Voor het Forum Standaardisatie is het van belang om per doelgroep te kijken welke standaarden extra aandacht nodig hebben en of er 'quick wins' te behalen zijn. Om voor de webstandaarden dichter bij de 100% te komen, zal het Bureau Forum Standaardisatie organisaties individueel aanspreken en helpen. Dit bij voorkeur via de koepelorganisaties.

Om de adoptie van mailstandaarden verder te brengen is het een optie om de grotere mailleveranciers in beweging te krijgen. Daarnaast kan een wettelijke verplichting helpen om de achterblijvers zo ver te krijgen dat ze de standaarden ondersteunen. Voor HTTPS, TLS geconfigureerd volgens de aanbevelingen van het NCSC en HSTS, is het ministerie van BZK voornemens de standaard te verplichten door middel van een algemene maatregel van bestuur (AMvB) op basis van het wetsvoorstel Wet digitale overheid. Deze AMvB is tussen 2 september 2019 en 20 oktober 2019 in openbare consultatie geweest[30]. Of dit ook voor andere informatieveiligheidstandaarden een goede optie is, wordt door het ministerie van Binnenlandse Zaken bekeken na het verlopen van de laatste streefbeeldafspraak eind 2019.

3. Achtergrond

Sinds 2015 biedt het Platform Internetstandaarden[31] de mogelijkheid om via de website Internet.nl domeinen te toetsen op het gebruik van een aantal 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

[30] internetconsultatie.nl/overheidswebsites/
[31] 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 internet.nl/about/

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[32]. 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[33].

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[34]:

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.

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);

[32] http://www.binnenlandsbestuur.nl/digitaal/nieuws/nationaal-beraad-wil-sneller-moderne-e.9540822.lynkx

[33] 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.

[34] Voor meer informatie ga naar: https://www.forumstandaardisatie.nl/thema/iv-meting-en-afspraken

- 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.

Ten opzichte van de vorige meting is de lijst geactualiseerd. Hierdoor zijn er nieuwe domeinnamen bijgekomen en zijn niet-relevante domeinnamen verwijderd. De reden hiervoor kan verschillen, bijvoorbeeld omdat er een gemeentelijke herindeling heeft plaatsgevonden of dat er waterschappen zijn samengevoegd. Ook is de lijst met best bezochte domeinnamen aangepast en zijn alle organisaties uit de Manifestgroep en Klein Lef toegevoegd.

Het betreft echter nog steeds een selectie van domeinnamen. 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 deze domeinen garandeert geenszins dat hiermee *alle* overheidsdomeinen beschermd zijn tegen bijvoorbeeld phishing. Mocht uwer inziens een relevante domeinnaam ontbreken dan verzoeken we om deze aan ons door te geven.

3.3 Hoe wordt gemeten

De meting geeft de stand van zaken weer op de peildatum 13 september 2019. De meting laat zien of op een domeinnaam de standaarden worden toegepast.

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. Overigens heeft de score die een domeinnaam op Internet.nl kan halen (namelijk max. 100%) geen relatie met het resultaat uit deze meting aangezien wij toetsen op een subset van de standaarden. De website Internet.nl is een initiatief van het Platform Internetstandaarden. In het platform participeren verschillende partners uit de internetgemeenschap (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:

- validatie van DNSSEC door de DNS-resolver van een overheidsorganisatie, burger of bedrijf;
- validatie van de DMARC, DKIM en SPF kenmerken door ontvangende mailservers van een overheidsorganisatie, burger of bedrijf;
- validatie van DANE kenmerken door verzendende mailservers.

In de loop van 2020 zal de functionaliteit van Internet.nl worden aangepast zodat het mogelijk zal zijn om te controleren of DMARC, DKIM, SPF en DANE validatie wordt toegepast. Dat betekent dat we vanaf dat moment kunnen gaan controleren of:

- ontvangende mailservers van een overheidsorganisatie DMARC+DKIM+SPF-validatie uitvoeren.
- verzendende mailservers van een overheidsorganisatie DANE-validatie uitvoeren.

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 voor 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)[35]. 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	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 voor 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.

[35] Zie https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html. Een wijziging ten opzichte van de vorige meting is dat in de huidige meting ook de vertrouwensketen van het certificaat wordt meegenomen in de test voor TLS conform NCSC.

	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 is om hier voor 2020 aan te voldoen
DKIM	Met DKIM kunnen e-mailberichten worden gewaarmerkt. De ontvanger van een e-mail kan op die manier controleren of een e-mailbericht écht van de afzender afkomstig is en of het bericht onderweg ongewijzigd is gebleven. Getest wordt of de domeinnaam DKIM ondersteunt. Voor non-mail domeinen waar dit goed is ingesteld heeft DKIM verder geen toegevoegde waarde. In de meting wordt dit weergegeven middels de score “NVT” (niet van toepassing) voor DKIM. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
SPF	SPF heeft als doel spam te verminderen. SPF controleert of een verzendende mailserver die e-mail namens een domein wil versturen, ook daadwerkelijk gerechtigd is om dit te mogen doen. Getest wordt of de domeinnaam een SPF-record heeft. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
SPF Policy	Aanvullend op bovenstaande test wordt gecontroleerd of de syntax van de SPF-record geldig is en of deze een voldoende strikte policy bevat om misbruik van het domein door phishers en spammers tegen te gaan. De streefbeeldafspraak is 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[36]	Net zoals bij HTTPS kan er bij STARTTLS gebruik worden gemaakt van verschillende versies van het TLS en verschillende versleutelingsstandaarden (ciphers). Aangezien niet alle versies en combinaties als voldoende veilig worden beschouwd, is het belangrijk om hierin de juiste keuze te maken en ook regelmatig te controleren of de gebruikte instellingen nog veilig zijn. Getest wordt of STARTTLS is geconfigureerd zoals door het NCSC is aanbevolen. De streefbeeldafspraak is om hier voor 2020 aan te voldoen.

[36] https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls.html

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 is om hier voor 2020 aan te voldoen
DNSSEC MX	DNSSEC is een randvoorwaarde voor het instellen van DANE. Daarom wordt getest of de domeinnamen van de mailservers (MX) ondertekend zijn met DNSSEC. Dit in het kader van de streefbeeldafspraak om voor 2020 STARTTLS en DANE te ondersteunen.

4. Resultaten meting september 2019

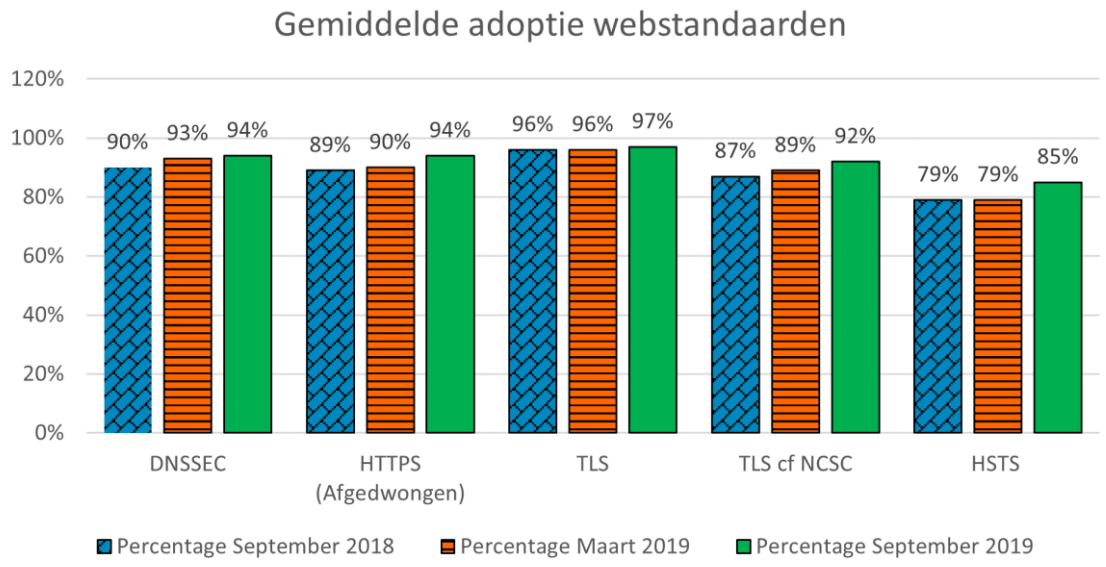
Op 13 september 2019 heeft het Bureau Forum Standaardisatie de meting uitgevoerd. De resultaten worden voorgelegd aan een aantal koepelorganisaties en stakeholders en geactualiseerd indien nodig. Naast de resultaten per standaard en per "overheidslaag" zoals bij voorgaande metingen, bevat deze meting tevens het perspectief van de verschillende streefbeelden. Dit laat duidelijk zien hoe het met de adoptie van de standaarden per streefbeeld is gesteld.

4.1 Per standaard

De onderstaande grafiek toont de adoptiestatus van de individuele standaarden voor zowel de webstandaarden als de mailstandaarden. Daar waar mogelijk is er een vergelijking gemaakt met de voorgaande metingen.

De gemiddelde adoptie van de webstandaarden is hoog. Het gemiddelde van alle webstandaarden samen is inmiddels 92% HSTS trekt dit gemiddelde iets omlaag en blijft steken op 85%. Positief is dat we deze meting weer een hogere groei in toepassing van webstandaarden zien ten opzichte van het voorgaande halfjaar. Om de adoptie van deze standaarden verder te stimuleren is een 'één op één' benadering nodig om dichter bij de 100% te komen.

Gemiddelde adoptie webstandaarden

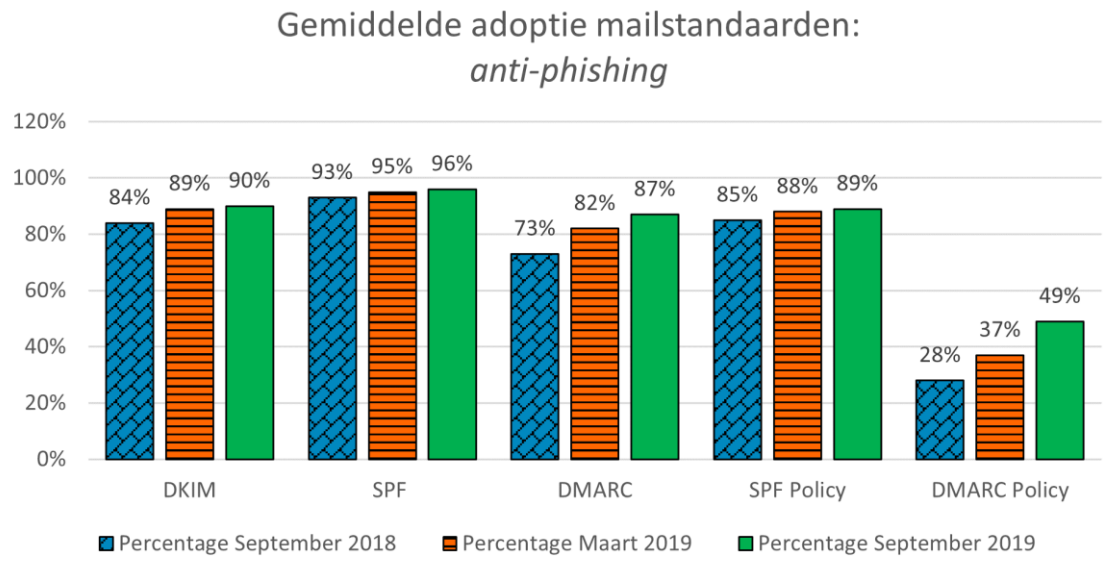


De gemiddelde adoptie van de mailstandaarden (visualisatie op de volgende pagina) ligt met 77% lager dan de webstandaarden. Dit is enerzijds te verklaren door de grotere hoeveelheid standaarden waaraan voldaan moet worden en anderzijds geldt voor een deel van de standaarden pas sinds begin 2018 een streefbeeldafspraak die loopt tot eind 2019. Het groeitempo is licht gedaald, dit was de vorige meting 7% en was afgelopen half jaar gelijk aan dat van de webstandaarden met circa 3%. Analoog hieraan is het groeitempo van DANE flink lager, de adoptie blijft steken op 45%, en de implementatie vraagt extra aandacht. Ook de adoptiegraad van DMARC met strikte configuratie (DMARC policy) is

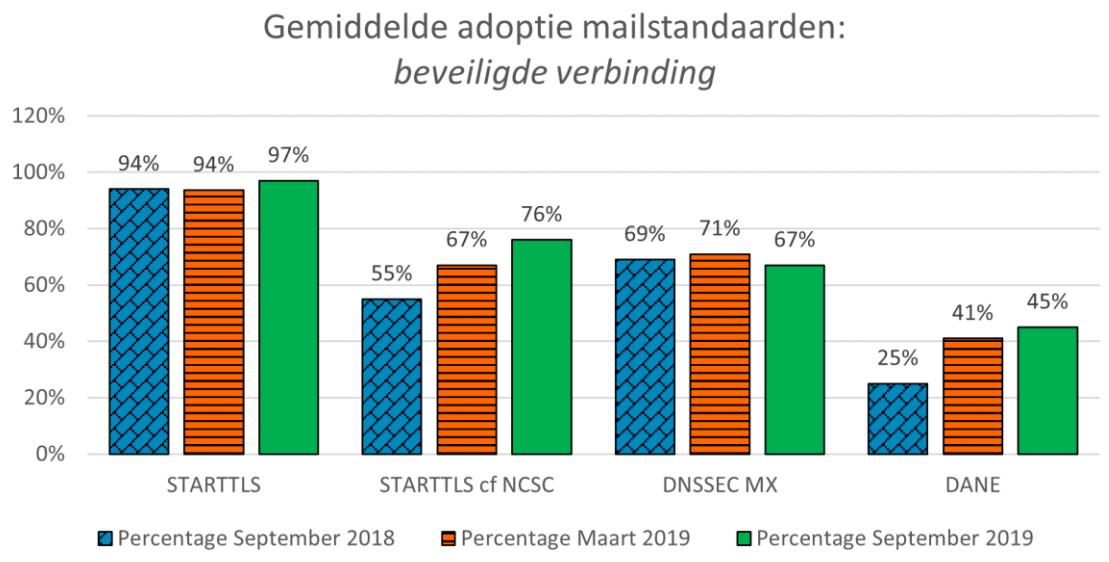
ondanks flinke groei nog relatief gezien laag en vraagt aandacht. De streefbeeldafspraken rond DANE en DMARC policy lopen eind 2019 af.

Opvallend is de neerwaartse trend van DNSSEC op de mailservers (MX). DNSSEC is een randvoorwaarde voor de betrouwbaarheid van DANE. De oorzaak van de neerwaartse trend is dat een aantal gemeenten en provincies de overstap naar Microsoft Office 365 Exchange Online hebben gemaakt, dit product biedt vooralsnog geen ondersteuning voor DNSSEC, en daarmee ook geen ondersteuning voor DANE. Dit is een duidelijk zorgpunt voor de betrouwbaarheid van overheidsmail, omdat deze gemeenten en provincies niet altijd een versleuteld mailtransport kunnen afdwingen en tevens niet aan de streefbeeldafspraak omtrent het gebruik van DANE kunnen voldoen.

Gemiddelde adoptie mailstandaarden: anti-phishing

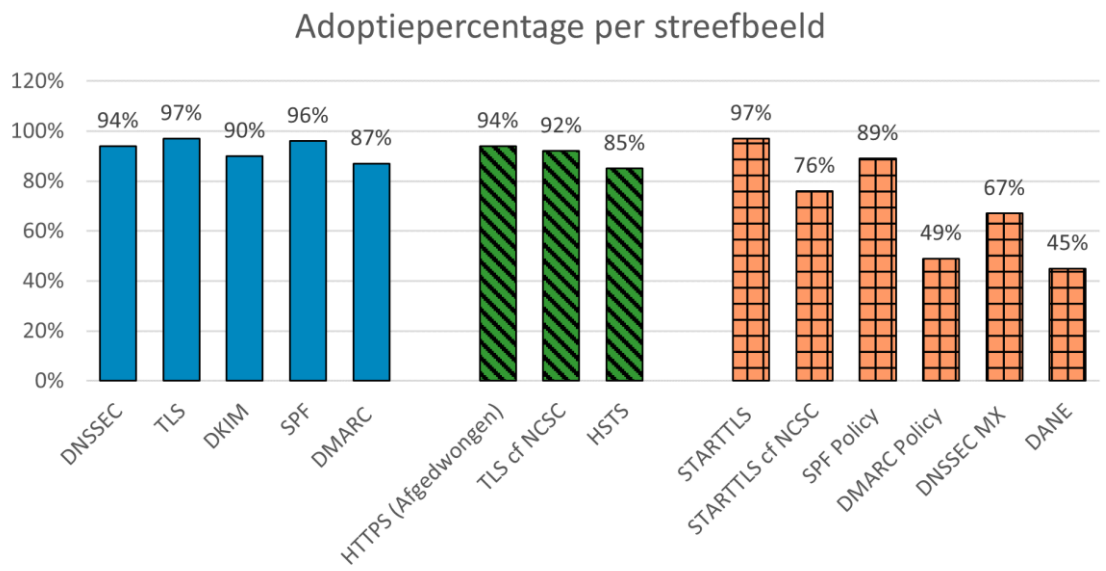


Gemiddelde adoptie mailstandaarden: beveiligde verbinding



4.2 Per streefbeeldafspraak

Adoptiepercentage per streefbeeld



Bovenstaande grafiek verdeelt de standaarden over de drie streefbeeldafspraken van het OBDO. De eerste set standaarden (blauw) uit het streefbeeld dat eind 2017 afliep worden gemiddeld het meest toegepast, maar ook begin 2019 is voor deze standaarden de gewenste 100% adoptie nog niet gehaald.

De deadline voor tweede streefbeeldafspraak (oranje) was eind 2018. Ook voor deze standaarden geldt dat de gemiddelde adoptie hoog is, maar de 100% nog niet is behaald.

Voor deze standaarden: HTTPS, 'TLS conform NSCS' en HSTS is er het voornemen een Algemene Maatregel van Bestuur (AMvB) op te stellen[37]. Deze AMvB is naar verwachting in 2020 van kracht en dwingt partijen die ondanks de streefbeeldafspraken de standaarden nog steeds niet toepassen, dat alsnog te doen.

De gemiddelde adoptie van de standaarden uit de derde streefbeeldafspraak (groen) is het laagst. Deze streefbeeldafspraak loopt tot eind 2019. Zonder extra inspanning van alle betrokken partijen is het onwaarschijnlijk dat dit streefbeeld wel wordt gehaald.

4.3 Per overheidslaag

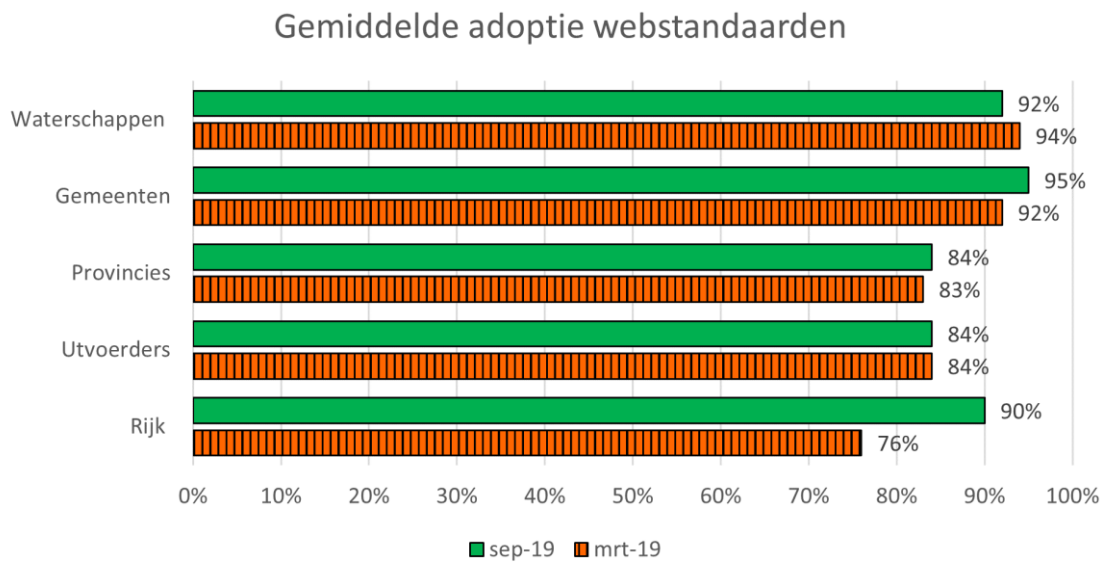
Een uitsplitsing van de resultaten van de webstandaarden naar overheidslaag laat zien dat in iedere overheidslaag de adoptie groeit. De waterschappen en gemeenten scoren gemiddeld respectievelijk 94 en 92%. Het Rijk blijft iets achter met een score van 76%. De mate van groei verschilt wel sterk, met name de waterschappen zijn sterk gegroeid met gemiddeld 7 procentpunt over het afgelopen halve jaar.

Het beeld is anders bij de mailstandaarden (visualisatie op de volgende pagina). Hier blijven de waterschappen gemiddeld juist iets achter op de andere overheidslagen. Het Rijk heeft

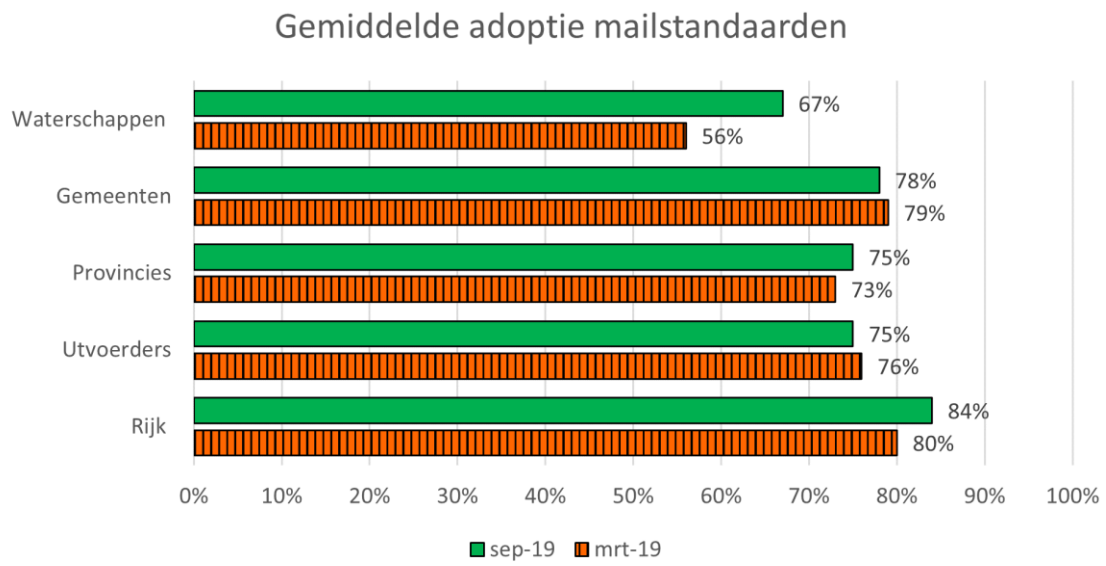
[37] Op basis van artikel 2 van het wetsvoorstel Wet digitale overheid.

bij de mailstandaarden gemiddeld de hoogste adoptiegraad. Verderop in de rapportage wordt per overheidslaag toegelicht welke standaarden gemiddeld veel worden toegepast en welke minder.

Gemiddelde adoptie webstandaarden



Gemiddelde adoptie mailstandaarden

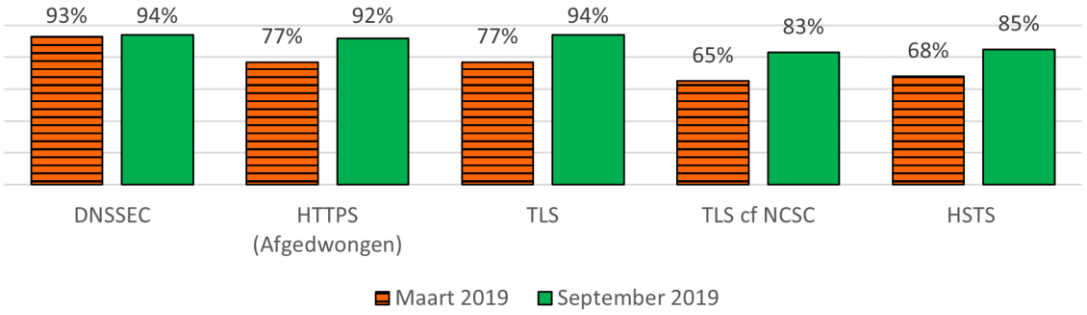


4.3.1 Het Rijk

Het Rijk heeft een flinke inhaalslag gemaakt met betrekking tot de standaarden voor het versleutelen van webverkeer (HTTPS en HSTS). Dit komt omdat een aantal doorverwijzende domeinen (redirects) van de ministeries recent voorzien zijn van HTTPS. Het gaat om domeinen waar geen website op gehost wordt, maar die doorverwijzen naar een ander domein. Bijvoorbeeld minbzk.nl (en vele andere departementale domeinen die vooral gebruikt worden voor de mailextensie) verwijst door naar www.rijksoverheid.nl.

Er valt nog winst te behalen bij het veilig configureren van TLS en het toepassen van HSTS.

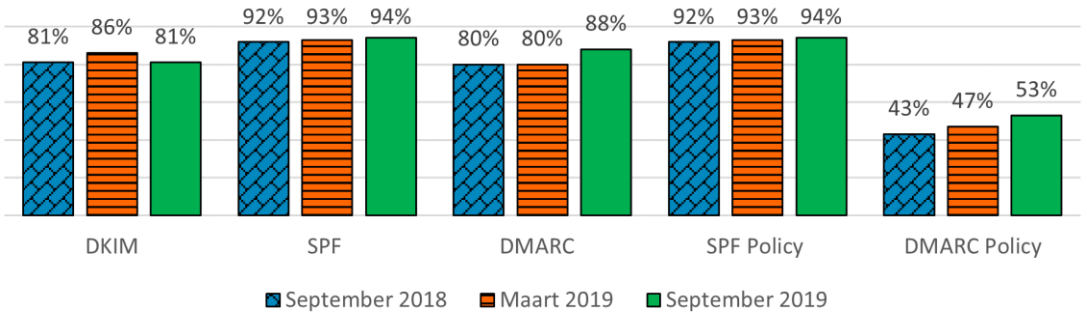
Gemiddelde adoptie Rijk: webstandaarden



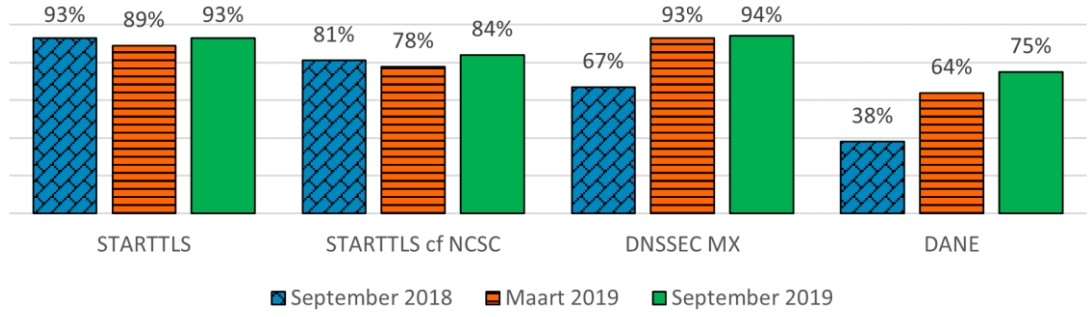
Het Rijk scoort goed als het gaat om de mailstandaarden. Met name DMARC en DANE scoren hier hoog t.o.v. de andere overheidslagen. Dit komt waarschijnlijk doordat het beheer van de mailservers bij een relatief klein aantal partijen belegd is. Een aanpassing bij die partijen heeft daarom grote impact op de score van het Rijk.

DKIM toont een achteruitgang. Er valt nog winst te behalen bij het strikt configureren van de DMARC policy, het toepassen van DANE, en het veilig configureren van STARTTLS

Gemiddelde adoptie Rijk: mailstandaarden - anti-phishing



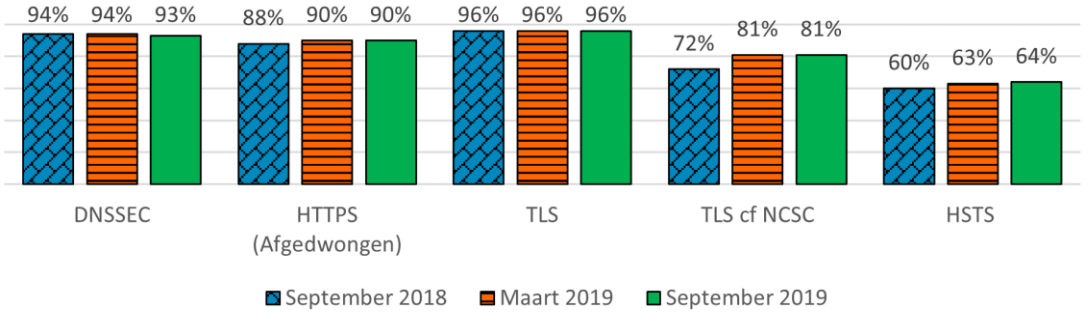
Gemiddelde adoptie Rijk: mailstandaarden - beveiligde verbinding



4.3.2 Uitvoering

De uitvoerders vormen een middenmoter. Bij de webstandaarden zien we een algehele stagnatie ten opzichte van de vorige meting. Er valt nog winst te behalen bij het veilig configureren van TLS en het toepassen van HSTS.

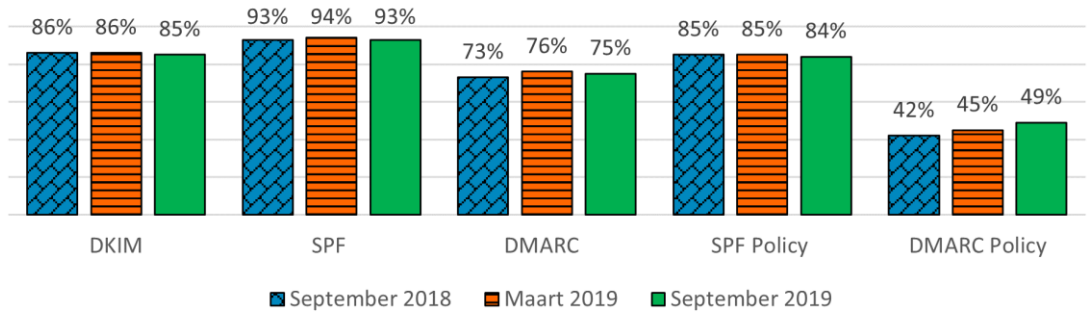
Gemiddelde adoptie uitvoerders: webstandaarden



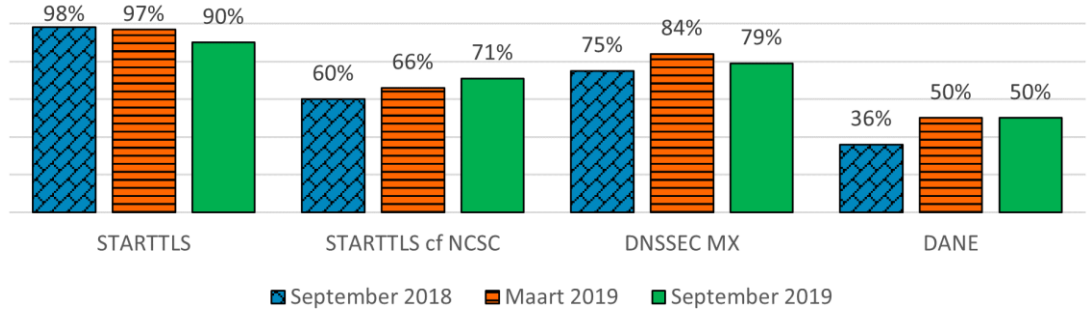
Waar de uitvoerders in de vorige meting nog een grote groei in het gebruik van mailstandaarden toonden, zien we nu een gemiddelde achteruitgang. Alleen het strenger afstellen van de DMARC policy en het veilig configureren van STARTTLS is gegroeid.

Er is over de hele linie nog genoeg ruimte voor verbetering.

Gemiddelde adoptie uitvoerders: mailstandaarden - anti-phishing



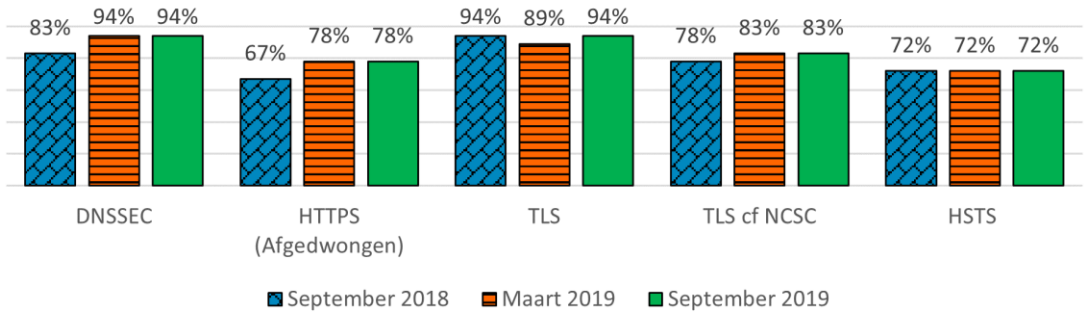
Gemiddelde adoptie uitvoerders: mailstandaarden - beveiligde verbinding



4.3.3 Provincies

De provincies laten ten aanzien van de webstandaarden een stagnatie zien. Enkel de toepassing van TLS is gestegen. Er valt nog winst te behalen bij het veilig configureren van TLS, het afdwingen van HTTPS, en het toepassen van HSTS.

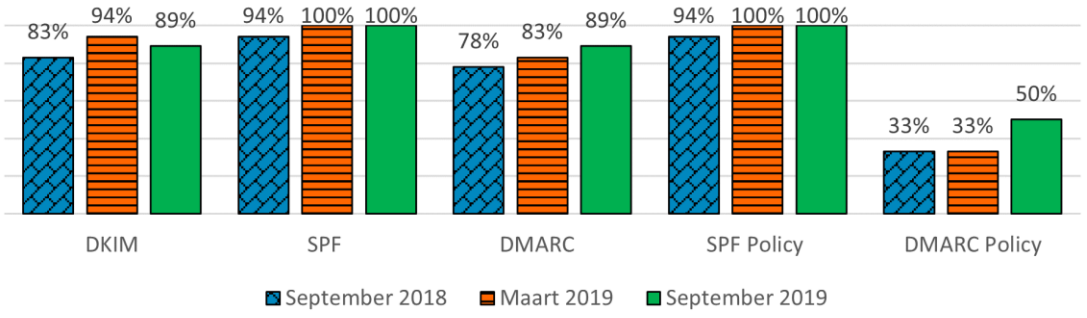
Gemiddelde adoptie provincies: webstandaarden



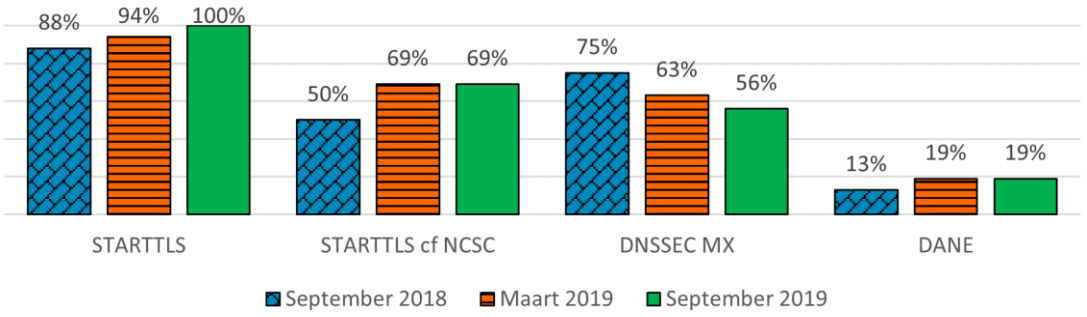
Ten aanzien van de mailstandaarden zien we een groei in het strikt afstellen van de DMARC policy, maar er is nog genoeg ruimte voor extra groei. Het gebruik van DKIM is licht gedaald. Positief is dat alle provincies gebruik maken van SPF en bovendien de juiste policy toepassen, daarnaast passen zij ook allen STARTTLS toe, hoewel niet altijd voldoende veilig geconfigureerd.

Daarnaast valt de neerwaartse trend van DNSSEC op de mailservers (MX) op. De oorzaak hiervan is dat een aantal provincies de overstap naar Microsoft Office 365 Exchange Online hebben gemaakt, dit product biedt vooralsnog geen ondersteuning voor DNSSEC, en daarmee ook geen ondersteuning voor DANE. Dit is een duidelijk zorgpunt voor de provincies, omdat zij zo niet aan de streefbeeldafspraak omtrent het gebruik van DANE kunnen voldoen.

Gemiddelde adoptie provincies: mailstandaarden - anti-phishing



Gemiddelde adoptie provincies: mailstandaarden - beveiligde verbinding

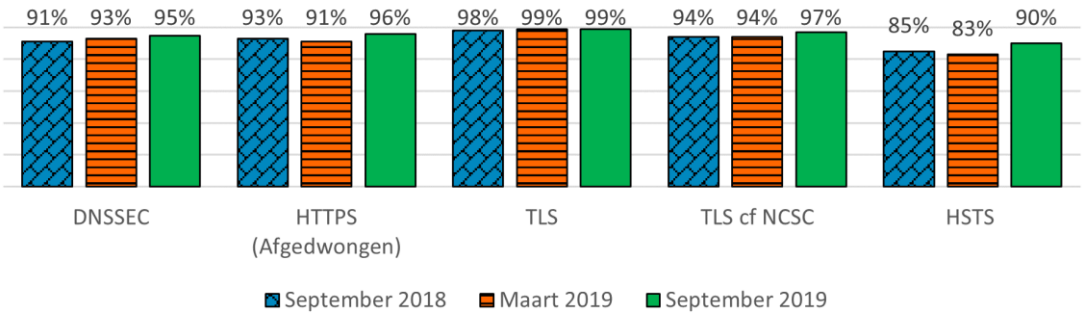


4.3.4 Gemeenten

De gemeenten scoren het beste op het gebruik van de webstandaarden. Positief is dat we ondanks de al hoge statistieken uit de vorige meting er wederom een zichtbare groei is. Met name het afdwingen van de HTTPS verbinding met onder meer HSTS wordt beter toegepast.

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

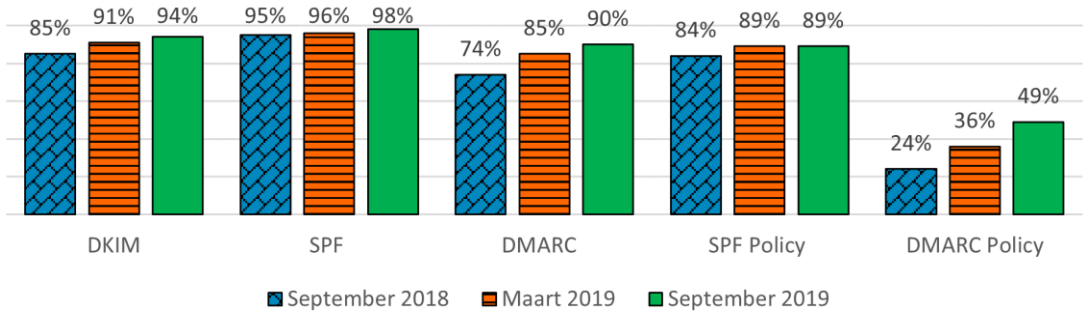
Gemiddelde adoptie gemeenten: webstandaarden



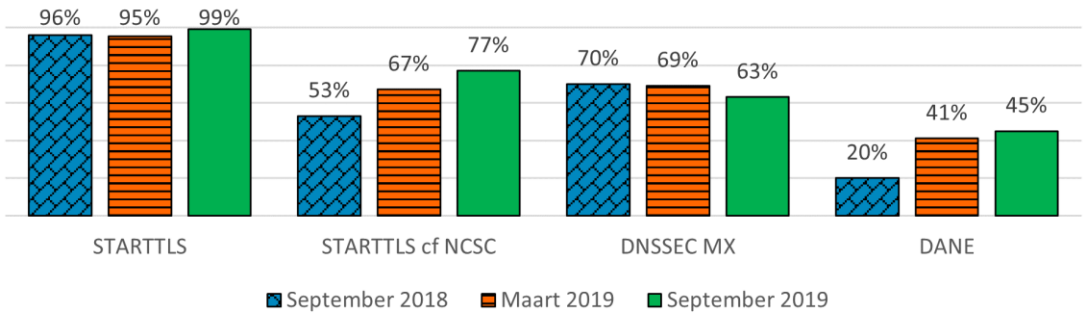
Ten aanzien van de mailstandaarden zien we over het algemeen ook groei. Het strikt afstellen van de DMARC policy is flink gegroeid, hoewel er ruimte is voor meer groei.

Analoog aan de provincies zien we ten aanzien van DNSSEC op de mailservers (MX) een neerwaartse trend. Ook hier is de oorzaak dat een aantal gemeenten de overstap naar Microsoft Office 365 Exchange Online hebben gemaakt. Dit is een duidelijk zorgpunt voor de gemeenten, omdat zij zo niet aan de streefbeeldafspraak omtrent het gebruik van DANE kunnen voldoen.

Gemiddelde adoptie gemeenten: mailstandaarden - anti-phishing



Gemiddelde adoptie gemeenten: mailstandaarden - beveiligde verbinding

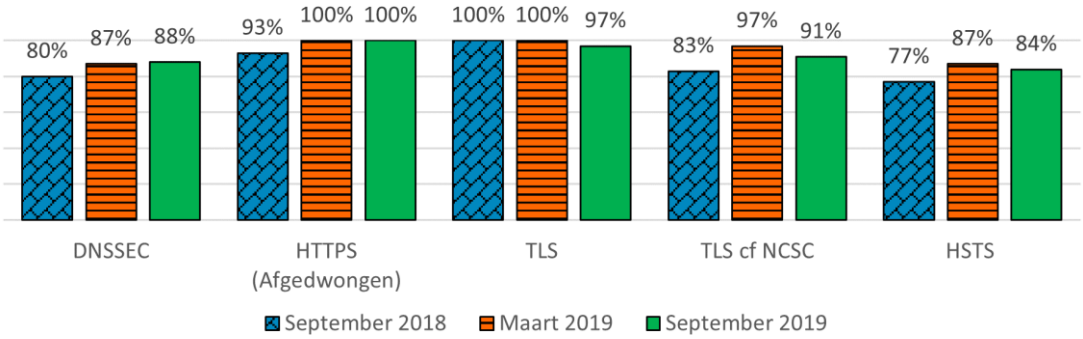


4.3.5 Waterschappen

De waterschappen scoren al enkele metingen achter elkaar relatief hoog op het toepassen van webstandaarden. Ook dit keer scoren zij in verhouding nog redelijk hoog. Helaas zien we voor een aantal standaarden een achteruitgang, wat een zorgpunt is voor de

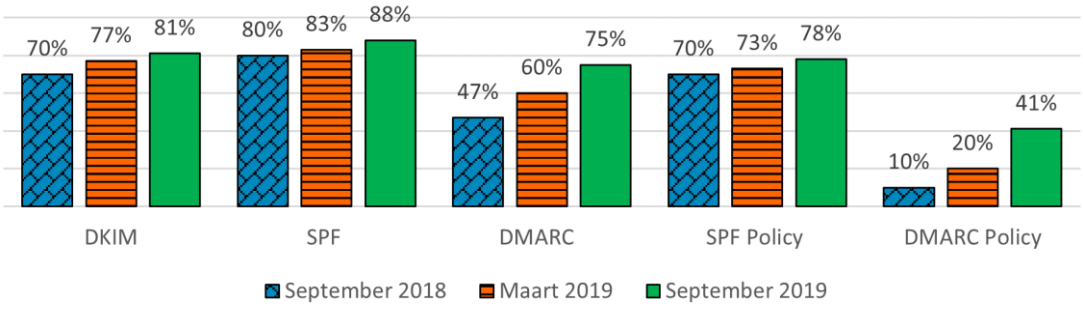
waterschappen. De achteruitgang lijkt fors, maar valt mee in de wetenschap dat het gaat om 32 domeinen, waar 1 domein al voor meer dan 3% meetelt.

Gemiddelde adoptie waterschappen: webstandaarden

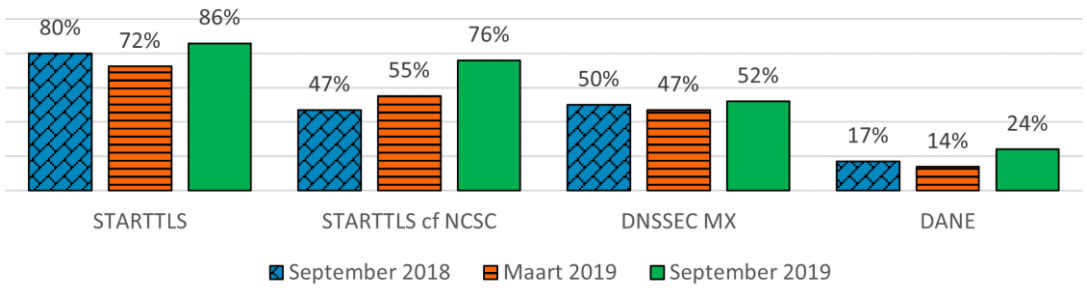


Ten aanzien van de mailstandaarden hebben de waterschappen een gemiddelde groei van 12% doorgemaakt, de grootste groei in verhouding met andere overheidslagen. Toch blijven de waterschappen met een gemiddelde adoptie van 66% flink achter lopen op de andere overheidslagen. Met name het toepassen van DMARC met de juiste strikte policy en DANE blijft achter.

Gemiddelde adoptie waterschappen: mailstandaarden - anti-phishing



Gemiddelde adoptie waterschappen: mailstandaarden - beveiligde verbinding



B9. Rapportage Open standaarden en voorzieningen (PBLQ)

PBLQ

Monitor Open Standaarden Voorzieningen 2019

Versie 1.10
21-12-2021

PBLQ
verbinders in de informatiesamenleving

Inhoudsopgave

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 Generieke Digitale Infrastructuur (GDI), plus een aantal voorzieningen die niet bij de GDI behoren.

1.3 Werkwijze

Voor dit onderzoek is gebruik gemaakt van de 'pas toe of leg uit'-lijst van 1 mei 2019. Per voorziening is gekeken of de standaarden op deze lijst relevant zijn.
Daarbij is telkens uitgegaan van de eindgebruiker. Dat is diegene die in de keten baat zou moet 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

[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.

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.

1.4.2 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.

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

[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

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 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
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.
Het besluit verplicht overheidsinstanties om te zorgen dat hun websites en/of mobiele applicaties toegankelijk zijn conform de geldende standaard EN 301 549, en daarover een actuele toegankelijkheidsverklaring af te geven.

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

Er geldt een gefaseerde toepassing. Nieuwe websites gepubliceerd vanaf 23 september 2018 moesten uiterlijk op 23 september 2019 voldoen. Bestaande website gepubliceerd vóór 23 september 2018 moeten een jaar later voldoen. Mobiele applicaties moeten uiterlijk 23 juni 2021 voldoen.

Ten tijde van dit onderzoek wordt een nul-meting uitgevoerd naar het gebruik van de standaard Digitoegankelijk door overheden op basis van een Europees vastgestelde methodiek. Deze resultaten worden in de loop van 2019 verwacht en worden toegezonden aan de Tweede Kamer. In dat licht is in overleg met het Forum Standaardisatie en het Centrum voor Standaarden besloten de standaard niet nogmaals apart te onderzoeken voor deze monitor en wordt volstaan om hier te verwijzen naar de conclusies van dit rapport.

ISO 27001/2, BIR en BIO

Binnen de rijksoverheid dient elke organisatie een eigen implementatie van de BIR te hebben. De BIR is gebaseerd op ISO 27001. Indien een organisatie voldoet aan de BIR, 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.
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. Veel partijen zijn momenteel al bezig met de transitie naar de BIO. Hier is in de beoordeling rekening mee gehouden.

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/).
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)	Gepland	De mailserver van DigiD past STARTTLS/DANE toe (zie https://internet.nl/mail/digid.nl/). Er is nog een aandachtspunt voor de gebruikte ciphersuites, hiervoor is een wijziging onderweg die in Q3/4 2019 wordt doorgevoerd.
TLS (Beveiligde, versleutelde verbindingen)	Ja	DigiD ondersteunt voor de gebruikersdomeinen alleen TLS v1.2. Voor de afnemersdomeinen is een wijziging onderweg (Q3/4 2019) om TLS v1.0 ook uit te faseren, zodat ook alleen TLS v1.2 overblijft. De mailserver ondersteunt nog TLS v1.0 en v1.1; omdat deze ook voor andere voorzieningen gebruikt wordt, is de impact nog in onderzoek.

Ten opzichte van 2018 zijn er geen wijzingen in de statussen. Wel is de planning voor implementatie van STARTTLS/DANE verschoven.

Concluderend, moet DigiD nog enkele aandachtspunten oplossen om de volgende standaard (volledig) te implementeren: STARTTLS/DANE.

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 verstuurd 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)	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Rijk (BIR) 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).

(Richtlijnen en principes informatiebeveiliging)		
SAML v2.0 (Inloggegevens)	Deels	Het authenticatie koppelvlak met eHerkenning voldoet aan de SAML standaard. Het authenticatie koppelvlak met DigiD maakt geen gebruik van SAML. Dit koppelvlak is door DigiD Machtigen gerealiseerd toen DigiD nog geen SAML koppelvlak bood. Overgang naar een SAML koppelvlak is voorzien bij de realisatie van de nieuwe website voor het DigiD Machtigen (publieke machtigingenregister), mogelijk al in het 4e kwartaal 2019. 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 verstuurd 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)	Ja	TLS is geïmplementeerd. DigiD Machtigen ondersteunt TLS v1.0, TLS v1.1 en TLS v1.2. Voor brede comptabiliteit worden TLS 1.0 en 1.1 nog ondersteund.
		Document en (web/app)content
PDF/A en PDF 1.7 (Document-publicatie/ archivering)	Ja	De voorziening voldoet aan deze standaard.
		Overig
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). 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 2018 zijn er geen veranderingen.

Concluderend, moet DigiD Machtigen nog de volgende standaarden (volledig) implementeren: SAML 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 TSP's die PKIoverheidscertificaten verstrek- ken. 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.
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".
IPv4 en IPV6 (Internetnummers)	Gepland	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/). Dit was gepland voor Q4 2019. De implementatiedatum is gekoppeld aan gunning van een nieuw contract aan applicatieleverancier. Dit is uitgesteld naar Q1 2020.
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 BIR 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/).

		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 2018 gaat de status van HTTPS/HSTS van ja naar deels.

Concluderend, moet PKIoverheid nog de volgende standaarden (volledig) implementeren: HTTPS en HSTS, IPv4 en IPv6.

2.4 Beheervoorziening BSN en GBA-V

Beheerorganisatie: Rijksdienst voor Identiteitsgegevens (RvIG), Ministerie BZK

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
HTTPS/HSTS (Beveiligd, Versleuteld Webverkeer)	Ja	Alle aangeboden webservices draaien HTTPS en HSTS.
IPv4 en IPV6 (Bereikbaarheid nieuwe Internetnummers)	Nee	Het publiceren van de diensten op IPv6 wordt in 2020 op de backlog van infrastructuur wijzigingen gezet. Wanneer de diensten beschikbaar zijn op IPv6 is nog niet bekend. Er wordt al wel met de ODC leverancier gekeken hoe IPv6 publicatie van diensten zou moeten plaatsvinden.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De Rijksdienst voor Identiteitsgegevens heeft een beveiligingsplan op basis van de BIR. Hier worden externe audits op gedaan. Er is een In Control Verklaring (ICV) aanwezig.
TLS (Beveiligd Versleuteld emailverkeer)	Ja	De voorziening ondersteunt zowel TLS 1.2, 1.1 als 1.0.
		Stelstelstandaarden
Digikoppeling 2.0 (Veilige berichtuitwisseling)	Nee	Er zijn plannen om voor de BRP (basisregistratie personen) gebruik te gaan maken van Digikoppeling. Gezien het lopende

		BRP bezinningsproces is de planning onduidelijk. Ontsluiting van BV-BSN middels Digikoppeling zal niet plaatsvinden.
StUF (Uitwisseling administratieve overheidsgegevens)	Nee	De voorziening spreekt de WSI standaard XML/SOAP met haar gebruikers. Er is geen concrete planning voor de invoering van StUF.

Ten opzichte van 2018 zijn er geen veranderingen.

Concluderend moeten voor de beheervoorziening BSN en GBA-V nog de volgende standaarden (volledig) worden geïmplementeerd: IPv4 en IPV6, Digikoppeling 2.0, StUF.

2.5 Rijkspas

Beheerorganisatie: Ministerie van BZK

Werking en inhoud van Rijkspas
Rijkspas is de voorziening waarmee (een groot deel van) de rijksambtenaren toegang krijgt tot de gebouwen van de rijksoverheid. Het is een multifunctionele smartcard en onderdeel van een veilig en flexibel toegangsconcept voor fysieke toegang tot rijksoverheidspanden en logische toegang tot systemen en netwerken. Het is opgezet als een federatief systeem, waarbij ieder departement een eigen Identity management oplossing heeft, die via de infrastructuur van de Rijkspas gezamenlijk worden ontsloten.

Het strategisch opdrachtgever- en eigenaarschap voor de Rijkspas is belegd bij DGOO/CIO Rijk/ICT Voorzieningen en Infrastructuur Rijk, die meer van dergelijke rijksbrede voorzieningen in het portfolio heeft. De tactische en operationele regie is in 2018 ondergebracht bij P-Direkt. SSC-ICT is in opdracht van CIO Rijk verantwoordelijk voor de housing en hosting van de Rijkspas Verkeershub en het Generiek Cardmanagement Systeem (GCMS). De Certificate Authority is ondergebracht onder de bestaande infrastructuur van DICTU. De departementen zijn eigenaar van de Identity management- en toegangscontrolesystemen.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Gepland	Voor Rijkspas worden mails verstuurd vanaf de applicatie voor Interdepartementale Toegang (IDT). In de huidige infrastructuur is dit niet toegepast. De eerdere planningen van Q3 2018 en Q4 2018 voor verhuizing van de Rijkspassystemen naar een nieuw datacenter waar DKIM wel toegepast zal worden zijn door SSC-ICT uitgesteld naar Q3 2019. De email server die gebruikt wordt is inmiddels wel verhuisd naar het ODC. Onderdeel van de totale applicatiemigratie (inclusief nieuwe email verzendadressen) is het mogelijk maken van DKIM.
DMARC (Anti-phishing)	Nee	P-direkt is afhankelijk van SSC-ICT voor implementatie van de standaard. De status hiervan is onbekend.
DNSSEC (Beveiligde domeinnamen)	Gepland	Rijkspas communiceert momenteel nog niet via het publieke internet. De verbinding die daarvoor voorzien is, maakt wel gebruik van DNSSEC. Voor communicatie binnen de Rijksoverheid wordt

		momenteel gebruik gemaakt van de Haagse Ring. Deze ondersteunt nog geen DNSSEC. De planning van 2017 is niet gehaald en is afhankelijk van de verhuizing naar het nieuwe data center. De verhuizing stond gepland voor Q1 2019 en staat nu gepland voor Q3 2019.
IPv4 en IPV6 (Internetnummers)	Nee	IPv4 wordt toegepast. De Haagse ring, waarover eigenlijk al het verkeer naar de Rijkspas voorzieningen loopt, ondersteunt geen IPv6. Deze dienst wordt door Logius geleverd, en is onderdeel van de 'connectiviteitsdiensten' waarvan I&I gebruik maakt.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De Rijkspas heeft een eigen normen- en beveiligingskader gebaseerd op ISO-9001 en 27001/2. Jaarlijks worden hier ook audits op gedaan, onder andere door de Audit Dienst Rijk.
SAML (Inloggegevens)	Ja	De Interdepartementale Toegang applicatie (IDT) is per 2015 aangesloten op de Single Sign On voorziening via SAML.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd.
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Nee	Rijkspas neemt email dienstverlening af van SSC-ICT, en vanuit deze leverancier is aangegeven dat nog niet alle randvoorwaarden in plaats zijn voor deze standaard. Eén van deze randvoorwaarden is DNSSEC, waarvan de implementatie afhankelijk is van de verhuizing naar het nieuwe data center. Na deze implementatie zal SSC-ICT opnieuw de mogelijkheden van STARTTLS en DANE analyseren.
TLS (Beveiligde, versleutelde verbindingen)	Ja	TLS wordt gebruikt voor het veilig ontsluiten van de website voor IdT.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Rijkspas maakt gebruik van het WUS-gedeelte van de Digikoppeling. De deelnemers kunnen zelf de keuze maken welk protocol ze hanteren, de standaard koppeling Rijkspas of de Digikoppeling.

Ten opzichte van 2018 is de planning voor implementatie van DKIM verplaatst van Q4 2018 naar Q3 2019 en de implementatie van DNSSEC is verplaatst van Q1 naar Q3 2019.

Concluderend moeten voor de voorziening Rijkspas nog de volgende standaarden (volledig) worden geïmplementeerd: DKIM, DMARC, DNSSEC, IPv4 en IPV6, STARTTLS/DANE.

2.6 Stelsel elektronische toegangsdiensten

Beheerorganisatie: Logius

Werking en inhoud van het Stelsel Elektronische Toegangsdiensten
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 zowel Idensys als eHerkenning. Momenteel zijn de wijze waarop deze voorzieningen geclusterd zijn en de eisen die eraan gesteld worden sterk aan verandering onderhevig.

Het Afsprakenstelsel Elektronische Toegangsdiensten is een set van technische, functionele, juridische en organisatorische afspraken op basis waarvan het netwerk van eHerkenning en Idensys worden geleverd. 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.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	Bij verstuurde email wordt DKIM toegepast, bij ontvangst gebeurd dit door de centrale email voorzieningen van Logius (SSC-ICT).
DMARC (Anti-phishing)	Gepland	Stelsel Elektronische toegangsdiensten voldoet aan DMARC, maar de policy is niet voor Q1 2019 aangescherpt. Er zijn nog enkele problemen waardoor het nog te vroeg is om van volledige implementatie te spreken. De planning is uiterlijk Q4 2019 volledig compliant te zijn. (Zie: https://internet.nl/mail/eherkenning.nl/ en https://internet.nl/mail/idensys.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.
IPv4 en IPv6 (Internetnummers)	Deels	Niet alle voorzieningen voldoen aan IPv4 en IPv6. (Zie: https://internet.nl/mail/eherkenning.nl/ en https://internet.nl/mail/idensys.nl/). De webservers voldoen wel aan IPv6, maar niet alle mailservers voldoen. Voor onze inkomende mail zijn we als kleine voorziening van Logius afhankelijk van de dienstverlening van het Shared Service Centrum van het Rijk (SSC-ICT). We zijn als Logius wel in gesprek met SSC-ICT.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De BIR is van toepassing op Logius, in het stelsel wordt certificering tegen ISO27001 geëist voor de deelnemers. De beheerorganisatie zelf is als 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	Ja	SPF wordt toegepast bij de voorziening, maar wordt vooralsnog niet vereist als toe te passen techniek voor deelnemers.

(Preventie van mailspoofing/phishing)		
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 KA-leverancier SSC-ICT.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Het afsprakenstelsel stelt het gebruik van TLS1.x verplicht.
		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 office software 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 2018 is de geplande datum voor (volledige) implementatie van DMARC verschoven van Q1 2019 naar Q4 2019. Inmiddels voldoet de voorziening aan DANE, waardoor de status van STARTTLS en DANE van nee naar ja gaat. De status van IPv4 en IPv6 is veranderd van ja naar deels.

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

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	Deze standaard wordt toegepast (zie: https://internet.nl/mail/mijnoverheid.nl/ en https://internet.nl/mail/mijn.overheid.nl/). 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)	Deels	MijnOverheid gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik. 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. Dit is ook minder urgent dan IPv6 op de website, waar we dit wel op ingeschakeld hebben.
NEN-ISO/IEC 27001/27002	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Rijk (BIR) van toepassing die is gebaseerd op NEN-ISO27001. Logius heeft zich over toepassing van deze norm verantwoord

(Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)		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.
		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 2018 is de status van IPv4 en IPv6 van nee naar deels gegaan.

Concluderend, moet mijnOverheid nog de volgende standaarden (volledig) implementeren: IPv6.

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)	Nee	DKIM is niet geïmplementeerd (zie: https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/).
DMARC (Anti-phishing)	Nee	De BerichtenBox voor Bedrijven voldoet niet aan DMARC. Deze standaard is mede afhankelijk van SPF en DKIM, welke niet ondersteund worden door de BerichtenBox voor Bedrijven.
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)	Ja	HTTPS en HSTS zijn geïmplementeerd (zie: https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/).
IPv4 en IPv6 (Internetnummers)	Nee	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 Berichtenbox is wel IPv6 ready, maar nog niet de hele keten. E-ovb (beheerder van de Berichtenbox) is daarbij ook afhankelijk van leveranciers die hun IPv6 implementatie nog niet op orde hebben. De implementatie moet DICTU-breed gebeuren voordat dit voor de Berichtenbox gedaan zal worden. Een datum voor de implementatie is zowel in 2018 als in 2019 niet bekend.
SAML (Inloggegevens)	Ja	eHerkenning is SAML-based en wordt toegepast voor het inloggen op de Berichtenbox.
SPF	Nee	SPF is niet geïmplementeerd (zie https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/).

(Preventie van mailspoofing/phishing)		
TLS (Beveiligde, versleutelde verbindingen)	Nee	De Berichtenbox maakt gebruik van TLS 1.2 (zie: https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/). Maar de webserver staat client-initiated renegotiation toe, wat niet veilig is.
		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 2018 voldoet de voorziening niet meer aan TLS, de status gaat van ja naar nee.

Concluderend moeten voor Berichtenbox voor bedrijven nog de volgende standaarden (volledig) worden geïmplementeerd: DKIM, DMARC, IPv4 en IPv6, SPF, 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 wordt toegepast op overheid.nl (Zie: https://internet.nl/mail/overheid.nl/).
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)	Gepland	HTTPS en HSTS zijn doorgevoerd op overheid.nl (zie https://internet.nl/site/www.overheid.nl/). Op een aantal sub-domeinen is HTTPS wel ingesteld, maar de configuratie voor HSTS-policy nog niet helemaal correct. Dit wordt in de zomer van 2019 hersteld.
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 BIR 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	STARTTLS en DANE zijn geheel geïmplementeerd (zie: https://internet.nl/mail/overheid.nl/).
TLS (Beveiligde, versleutelde verbindingen)	Gepland	Deze standaard is doorgevoerd op overheid.nl (zie: https://internet.nl/site/www.overheid.nl/). Op een aantal sub-domeinen is TLS wel ingesteld, maar de configuratie voor client initiated renegotiation nog niet helemaal correct. Dit wordt in de zomer van 2019 hersteld.
		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 2018 zijn er geen veranderingen in de statussen van de relevante standaarden. De planningen voor implementatie van HSTS en TLS zijn verschoven.

Concluderend, moet overheid.nl op een aantal subdomeinen nog de volgende standaarden (volledig) implementeren: HSTS en TLS.

3.4 Ondernemersplein

Beheerorganisatie: Kamer van Koophandel

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. Sinds dit jaar is ondernemersplein.kvk.nl nieuw, ondernemersplein.nl verwijst vanaf dit jaar door naar ondernemersplein.kvk.nl.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Deels	DKIM is geïmplementeerd voor de domeinen kvk.nl en ondernemersplein.nl (zie: https://internet.nl/mail/kvk.nl/249076/, https://internet.nl/mail/ondernemersplein.nl/) maar niet voor het domein ondernemersplein.kvk.nl (zie: https://internet.nl/mail/ondernemersplein.kvk.nl/246411/).
DMARC (Anti-phishing)	Ja	Ondernemersplein voldoet aan DMARC (zie: https://internet.nl/mail/ondernemersplein.nl/, https://internet.nl/mail/kvk.nl/249076/, https://internet.nl/mail/ondernemersplein.kvk.nl/246411/).
DNSSEC (Beveiligde domeinnamen)	Deels	De standaard is geïmplementeerd op de nieuwe DNS omgeving voor de webdomeinen en voor het maildomein ondernemersplein.kvk.nl. Voor de mailserverdomeinen kvk.nl en ondernemersplein.nl geldt dat DNSSEC niet is geïmplementeerd (zie: https://internet.nl/mail/kvk.nl/249076/# en https://internet.nl/mail/ondernemersplein.nl/249075/#). Ondernemersplein maakt geen gebruik van ondernemersplein.kvk.nl als mail adres. Alle mailadressen die worden gebruikt zijn @ondernemersplein.nl of @kvk.nl, waar DMARC, DKIM, SPF en STARTTTLS wel geïmplementeerd zijn. Desondanks is het verzoek wel neergelegd bij IT beheer om dit op te lossen. Naar verwachting gebeurt dit niet op korte termijn.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels	Aan deze standaard wordt voldaan voor het domein ondernemersplein.nl (zie: https://internet.nl/site/www.ondernemersplein.nl/), maar voor het domein ondernemersplein.kvk.nl geldt dat HSTS niet is geïmplementeerd (zie: https://internet.nl/site/ondernemersplein.kvk.nl/577753/#). – De HSTS Policy komt naar verwachting eind november 2019 live.
IPv4 en IPV6 (Internetnummers)	Deels	De website ondersteunt IPv4 en is toegankelijk via IPv6 (zie: https://internet.nl/site/www.ondernemersplein.nl/ en

		https://internet.nl/site/ondernemersplein.kvk.nl/577753/#). Voor het maildomein ondernemersplein.nl en kvk.nl is IPv6 niet geïmplementeerd (zie: https://internet.nl/mail/ondernemersplein.nl/249075/# en https://internet.nl/mail/kvk.nl/249076/). Implementatie van IPv6 voor de mailservers is niet mogelijk.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Ondernemersplein is gehost bij de Kamer van Koophandel. Daar liep een ISO 27001 certificeringstraject en Ondernemersplein heeft dit inmiddels toegepast en is door een audit in april 2016 gecertificeerd hierop. Toetsing vond plaats in februari 2019 met goed resultaat.
SPF (Preventie van mailspoofing/phishing)	Deels	Er wordt aan deze standaard voldaan op de domeinen kvk.nl en ondernemersplein.nl (zie: https://internet.nl/mail/kvk.nl/249076/# en https://internet.nl/mail/ondernemersplein.nl/). SPF is niet geïmplementeerd voor het domein ondernemersplein.kvk.nl (zie: https://internet.nl/mail/ondernemersplein.kvk.nl/246411/#)
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Nee	Aan STARTTLS wordt voldaan, maar aan DANE wordt nog niet voldaan. De KvK geeft zowel in 2018 als in 2019 aan nog te moeten onderzoeken of hieraan voldaan zal worden. Er is nog geen concreet onderzoekstraject gedefinieerd.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Er is een migratie uitgevoerd naar TLS 1.2 en op verzoek van de product owner wordt TLS 1.0 nog ondersteund.
		Document en (web/app)content
CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)	Nee	De tooling (CMS/ESB) ondersteunt de standaard wel, maar deze wordt niet actief gebruikt. Er zijn geen content leveranciers die hun CMS in CMIS vorm aan het Ondernemersplein.nl 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 2018 is naast ondernemersplein.kvk.nl gekeken naar de domeinen ondernemersplein.nl en kvk.nl, omdat daarvandaan wordt gemaild. De status van de standaarden DKIM, HTTPS/HSTS en SPF is daarmee van ja naar deels gegaan, omdat niet alle domeinen voldoen. De status van de standaarden DNSSEC en IPv4 en IPv6 is van ja naar deels gegaan.

Concluderend moeten voor de voorziening ondernemersplein nog de volgende standaarden (volledig) worden geïmplementeerd: DKIM, DNSSEC, HTTPS/HSTS, IPv4 en IPV6, SPF, STARTTLS/DANE, CMIS, 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 data is voor iedereen doorzoekbaar door middel van de Zoekdienst van KOOP op basis van een API. De eindgebruiker ziet de zoekdienst niet, maar gebruikt de portalen Overheid.nl en Ondernemersplein.nl. Zowel Overheid.nl als het Digitaal Ondernemersplein haalt de productinformatie uit de zoekdienst. Daarnaast kan de eindgebruiker via de desbetreffende overheidswebsites informatie via Samenwerkende Catalogi opvragen.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DMARC (Anti-phishing)	Gepland	Samenwerkende Catalogi wordt beheerd door Logius waarmee DMARC valt onder het organisatorisch werkingsgebied. De validator is benaderbaar via een subdomein van Logius (scvalidator.logius.nl) waarvoor geldt dat dit een overheidsdomein is waarvandaan niet wordt gemaild. Daarmee valt dit onder het functioneel toepassingsgebied. Het DMARC-compliant maken van de validator stond gepland voor 2018. De validator van Samenwerkende Catalogi is in de tweede helft van juli 2019 gemigreerd naar een ander platform. Op dit moment worden alle relevante standaarden geïmplementeerd: HTTPS en HSTS, SPF, DMARC, TLS. Verwachting is dat dit Q3 2019 gereed is.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Gepland	De validator van Samenwerkende Catalogi is in de tweede helft van juli 2019 gemigreerd naar een ander platform. Op dit moment worden alle relevante standaarden geïmplementeerd: HTTPS en HSTS, SPF, DMARC, TLS. Verwachting is dat dit Q3 2019 gereed is.
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)	Gepland	De validator van Samenwerkende Catalogi is in de tweede helft van juli 2019 gemigreerd naar een ander platform. Op dit moment worden alle relevante standaarden geïmplementeerd: HTTPS en HSTS, SPF, DMARC, TLS. Verwachting is dat dit Q3 2019 gereed is.
TLS (Beveiligde, versleutelde verbindingen)	Gepland	De validator van Samenwerkende Catalogi is in de tweede helft van juli 2019 gemigreerd naar een ander platform. Op dit moment worden alle relevante standaarden geïmplementeerd: HTTPS en HSTS, SPF, DMARC, TLS. Verwachting is dat dit Q3 2019 gereed is.
		Document en (web/app)content
Open Api Specification	Ja	Samenwerkende catalogi voldoet aan deze standaard.

(Beschrijven van REST API's)		
OWMS (Metadata overheidsinformatie)	Ja	Samenwerkende catalogi is volledig gebaseerd op OWMS.

Ten opzichte van 2018 voldoet Samenwerkende catalogi aan de standaard Open Api Specification en is het (volledig) implementeren van DMARC uitgesteld van 2018 naar Q3 2019. Ten opzichte van vorig jaar zijn verder de standaarden HTTPS en HSTS, IPv4 en IPv6, SPF en TLS toegevoegd.

Concluderend moet Samenwerkende catalogi nog de volgende standaarden (volledig) implementeren: DMARC, HTTPS en HSTS, SPF en TLS.

3.6 Rijksportaal

Beheer organisatie: SSC-ICT

Werking en inhoud van Rijksportaal
Het Rijksportaal is het (Rijksbrede) raamwerk voor intranettoepassing voor alle (kern)departementen en verschillende uitvoeringsinstanties. Hiermee is het merendeel van de oorspronkelijke intranetten van de(kern)departementen vervangen. Het Rijksportaal geeft de rijksambtenaar toegang tot Rijksbrede en departementspecifieke informatie, bronnen en toepassingen. Ook is vanuit het Rijksportaal mogelijk om nieuws van andere departementen te volgen en personeels- en facilitaire zaken te regelen. SSC-ICT voert het technisch beheer en (technisch) applicatiebeheer over het Rijksportaal in opdracht van de Dienst Publiek en Communicatie (DPC) van het Ministerie van Algemene Zaken en van CIO Rijk.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/ phishing)	Nee	Onderbouwing beheerder ontbreekt.
DMARC (Anti-phishing)	Ja	Er wordt in enkele situaties gebruik gemaakt van email. Bijvoorbeeld om te reageren naar een redactie. Hierbij wordt gebruik gemaakt van de generieke e-mailvoorziening van SSC-ICT, die de DMARC standaard ondersteunt.
DNSSEC (Beveiligde domeinnamen)	Nee	Bij transitie Rijksportaal wordt deze bouwsteen opnieuw ingebracht.
IPv6 en IPv4 (Internet-nummers)	Nee	Het huidige Rijksportaal (versie 1.6.5) is alleen ingericht voor IPv4. Om performanceredenen wordt IPv6 momenteel nog niet toegepast. Als gevolg van de transitie naar het overheidsdatacenter (ODC), het beëindigen van de realisatie van release 1.7 en een lopende verkenning op een nieuwe omgeving is er zowel in 2018 als in 2019 geen doorontwikkeling t.a.v. nieuwe functionaliteit voor het Rijksportaal.

SAML (Inloggegevens)	Ja	Eind februari 2019 is de dienst SAML SSO voor Rijksportaal officieel door SSC-ICT opgeleverd en in beheer genomen. Begin december 2018 is de SAML-acceptatie omgeving opgeleverd. In december 2018 en begin januari 2019 is er getest door de kerndepartementen. Daarnaast is een pilot gedraaid met EZK/LNV. Inmiddels gebruiken EZK, LNV, Tweede Kamer, AZ en de belastingdienst deze manier van authenticatie voor het Rijksportaal.
SPF (Preventie van mailspoofing/phishing)	Nee	SPF is minder relevant voor deze oplossing. Echter, het gebruik van DKIM/DMARC (want maillinks) en het gebruik van mailservers laat onverlet dat SPF ook een (mogelijk) te gebruiken standaard dient te zijn.
		Document en (web/app)content
ODF (Document-bewerkingen)	Ja	ODF wordt ondersteund: ODF-bestanden kunnen geüpload en gedownload worden en de inhoud van ODF-bestanden kan door de zoekmachine worden geïndexeerd. Naast ODF worden op het Rijksportaal ook andere documentformaten gebruikt; het gebruik van ODF wordt niet afgedwongen.
PDF 1.7 PDF/A-1, PDF/A-2 (Documentpublicatie/ archivering)	Ja	PDF wordt ondersteund: PDF-bestanden kunnen geüpload en gedownload worden en de inhoud van PDF-bestanden kan door de zoekmachine worden geïndexeerd. Naast PDF 1.7, PDF/A-1 en PDF/A-2 worden op het Rijksportaal ook andere PDF-versies gebruikt; het gebruik van PDF 1.7, PDF/A-1 en PDF/A-2 wordt niet afgedwongen.

Ten opzichte van vorig jaar voldoet Rijksportaal aan SAML, waarmee de status van nee naar ja is gegaan. Ten opzichte van vorig jaar zijn verder de standaarden DKIM, DNSSEC en SPF opgenomen als relevant.

Concluderend moet voor Rijksportaal nog de volgende standaard (volledig) worden geïmplementeerd: DKIM, DNSSEC, IPv6, SPF.

3.7 ODC Noord

Beheerorganisatie: Dienst Uitvoering Onderwijs (DUO)

Werking en inhoud van ODC-Noord
ODC-Noord is één van de datacentra die ingericht is voor de (Rijks)overheid en andere overheden. ODC-Noord is sinds 2015 operationeel.

ODC-Noord maakt enerzijds gebruik van de DUO mailomgeving (odc-noord.nl en sso-noord.nl) en anderzijds van een eigen mailomgeving (rijkscloud.nl)

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM	Ja	DKIM is voor odc-noord.nl, sso-noord.nl en rijkscloud.nl geïmplementeerd voor ODC-Noord.

(Preventie van mailspoofing/phishing)		
DMARC (Anti-phishing)	Ja	DMARC is voor de betreffende domeinen geïmplementeerd. https://internet.nl/mail/odc-noord.nl/247561/#; https://internet.nl/mail/sso-noord.nl/247564/#control-panel-9
DNSSEC (Beveiligde domeinnamen)	Ja	ODC-Noord heeft sinds het onderzoek uit 2015 een eigen DNS ingericht, die DNSSEC gebruikt.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels	De cloud dashboards zijn allemaal uitsluitend via HTTPS benaderbaar, een aantal websites draaien op HSTS. Alle sites, met uitzondering van sso-noord.nl zijn voorzien van een SSL-certificaat. Het domein sso-noord.nl wordt voor 1 januari 2020 opgeheven. https://internet.nl/site/odc-noord.nl/574389/#control-panel-21; https://internet.nl/site/sso-noord.nl/574393/#control-panel-11 https://internet.nl/site/rijkscloud.nl/574696/#sitetls.
IPv6 en IPv4 (Internetnummers)	Gepland	Intern wordt IPv6 gebruikt op een specifiek netwerk. Nog niet alle benodigde producten worden met IPv6 aangeboden. Zodra de markt alles op het juiste niveau kan aanbieden zal dit geïmplementeerd worden en zullen de systemen die vanaf het internet benaderbaar zijn, ook worden ontsloten via IPv6. Planning is eind 2019 geïmplementeerd. https://internet.nl/site/odc-noord.nl/574389/#control-panel-21; https://internet.nl/site/rijkscloud.nl/574392/#control-panel-21; https://internet.nl/site/sso-noord.nl/574393/#control-panel-11; Nb. De mailomgeving van DUO waarop odc-noord.nl en sso-noord wordt gehost is daarentegen wel via IPv6 bereikbaar. https://internet.nl/mail/rijkscloud.nl/247562/#control-panel-16 Zodra ipv6 beschikbaar komt in Openstack kan rijkscloud.nl domein via ipv6 mail ontvangen en versturen.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Op 15 februari 2019 is door ODC-Noord een BIR in Control Verklaring voor 2018 afgegeven, ondersteund door een Assurance verklaring van de ADR. De onderliggende leveranciers voldoen aan de ISO. ODC-Noord voldoet aan de BIR.
SAML (Inloggegevens)	Gepland	ODC-Noord maakt voor het interne systeem geen gebruik van SAML. Bij het ontwikkelen van diensten ten bate van klanten (SaaS) wordt SAML onderzocht en waar mogelijk toegepast. Eerder stond SAML federatie, wat onderdeel uitmaakt van de multifactor implementatie voor de SAAS dienstverlening van ODC-Noord, op de roadmap voor eind 2018. SAML is doorgeschoven naar 2019 en wordt na de zomervakantie opgepakt. De PoC welke eerder dit jaar heeft plaatsgevonden, heeft uitgewezen dat de oplossing gaat werken.
SPF (Bescherming tegen e-mailphishing)	Ja	SPF is geïmplementeerd voor alle drie de domeinen.
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Nee	STARTTLS/DANE is voor de mailomgeving rijkscloud.nl onvoldoende veilig geïmplementeerd (niet conform de NCSC richtlijnen). De mailomgeving van DUO, waarop odc-noord.nl

		en sso-noord.nl worden gehost, is STARTTLS ingericht, maar DANE niet. https://internet.nl/mail/odc-noord.nl/247561/#; https://internet.nl/mail/rijkscloud.nl/247562/#control-panel-16; https://internet.nl/mail/sso-noord.nl/247564/#control-panel-9
TLS (Beveiligde, versleutelde verbindingen)	Deels	Het beleid van ODC-Noord voor internet-gekoppelde systemen is dat TLS (in volgorde) van TLS1.2, TLS1.1 wordt aangeboden. TLS 1.0 wordt niet toegepast tenzij er een explain komt van de site-eigenaar. https://internet.nl/site/sso-noord.nl/574393/#control-panel-11; sso-noord.nl voldoet niet aan de standaard. Het domein sso-noord.nl wordt voor 1 januari 2020 opgeheven.
WPA2 Enterprise (Toegang tot een WiFi-netwerk met account)	Ja	Deze standaard is toegepast waar ODC-Noord wifi gebruikt.
		Document en (web/app)content
OWMS (Metadata overheidsinformatie)	Gepland	Oorspronkelijk stond de implementatie van OWMS gepland voor Q4 2018. De website van ODC-Noord is in een eerste fase herbouwd, maar nog niet op het gewenste platform. Begin september start hiervoor de tweede fase waarbij naast de webrichtlijnen ook aan OWMS standaard zal worden voldaan. Volledige implementatie is gepland voor Q4 2019.
PDF 1.7, PDF A/1, PDF A/2 (Document-publicatie/ archivering)	Deels	V.w.b. uitwisseling van (definitieve) documenten met externe partijen wordt gebruik gemaakt van PDF. PDFCreator van Windows wordt als printoptie in de kantoorautomatiseringsomgeving aangeboden. De standaardinstelling is PDF versie 1.4, optioneel is 1.5. Vooralsnog wordt er bij DUO nog voor gekozen om de gratis variant van PDF-creator beschikbaar te stellen. Deze biedt maximaal PDF 1.5. Gebruikers van LibreOffice (dat is het meest gebruikte Office-pakket binnen de operationele omgeving van ODC-Noord) kunnen documenten exporteren naar PDF/A-1. Op dit moment is dat nog geen standaard werkwijze. PDF/A is beschikbaar en wordt gebruikt voor formele documenten

Ten opzichte van 2018 voldoet ODC Noord aan DMARC en SPF. In 2018 voldeed ODC Noord aan HTTPS/HSTS, in 2019 voldoet de voorziening nog deels. De status van STARTTLS/DANE gaat van gepland naar nee. IPv4 en IPv6 was deels wordt gepland. TLS was gepland en wordt deels. ODF is niet meer relevant. De planningen voor implementatie van SAML en OWMS zijn verschoven.

Concluderend, moet ODC Noord nog de volgende standaarden (volledig) implementeren: HTTPS en HSTS, IPv6 en IPv4, SAML, STARTTLS/DANE, OWMS, PDF 1.7, PDF A/1, PDF A/2 en TLS.

3.8 Doc-Direkt

Beheerorganisatie: Doc-Direkt

Werking en inhoud van Doc-Direkt
Doc-Direkt levert diensten aan departementen en notarissen voor archiefbewerking, -beheer, opslag en digitale documenthuishouding. Statische archieven worden aan Doc-Direkt in beheer gegeven door diverse onderdelen van de rijksoverheid. Doc-Direkt beheert ook een Document Management Systeem (DMS) voor o.a. BZK, waarin een levend archief wordt ontsloten.

Standaard	Status	Toelichting beheerder

		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	Volgens SSC-ICT maakt Doc-Direkt gebruik van de mailservers van SSC-ICT, deze zijn onderdeel van het BZK domein, waarvoor DKIM actief is.
DMARC (Anti-phishing)	Ja	Doc-Direkt voldoet aan DMARC.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels	De standaard wordt toegepast. De laatste open realisatie is de website www.handelingenbank.nl. De certificaat aanvraag loopt en realisatie in 4e kwartaal 2018 is niet gehaald. Nieuwe planning voor implementatie is 4e kwartaal 2019.
IPv4 en IPv6 (Internetnummers)	Ja	Doc-Direkt voldoet aan IPv4 en IPv6.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Voor de informatiesystemen waarvan Doc-Direkt eigenaar is, is in 2016 een 'in controle verklaring' opgesteld. Op de punten waar Doc-Direkt afwijkt is een uitleg gegeven (explains) en er is een verbeterplan opgesteld. Verbeteringen worden inmiddels uitgevoerd.
SAML (Inloggegevens)	Ja	Via de werkplek DWR kunnen medewerkers via SSO inloggen op de door Doc-Direkt beheerde DMS applicatie.
SPF (Preventie van mailspoofing/phishing)	Ja	Ook SPF wordt inmiddels toegepast.
TLS (Beveiligde, versleutelde verbindingen)	Nee	TLS v 1.2 is van toepassing en behoort tot de dienstverlening van SSC-ICT. Er wordt gewerkt aan TLS 1.3.
		Document en (web/app)content
Ades Baseline Profiles (Digitaal ondertekenen van documenten)	Nee	Er wordt op dit moment een productiepilot gedraaid. Het is een gezamenlijk dienst van Doc-Direkt en SSC-ICT. De verwachting is dat we in 2020 deze dienst in onze PDC kunnen opnemen.
CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)	Nee	De mogelijkheid en noodzakelijkheid van het toepassen van deze standaard werd in 2016 nader onderzocht, maar dit heeft nog niet tot een besluit geleid. Er zijn in 2018 proof of concepts uitgevoerd.
ODF (Documentbewerkingen)	Nee	Voor bewerkbare documenten wordt alleen .doc-formaat gebruikt. Er zijn geen plannen ODF te gebruiken.
PDF 1.7 – PDF A/1 of PDF A/2 (Documentpublicatie/ archivering)	Ja	Doc-Direkt ondersteunt in haar archieven vooral PDF/A. Alles wat gescand wordt gaat naar PDF/A. Daarnaast wordt ook 1.7 veel gebruikt.
SKOS (Thesauri en begrippen-woordenboeken)	Nee	SKOS wordt op dit moment niet toegepast. Er waren in 2018 en er zijn in 2019 nog geen plannen bekend of en wanneer SKOS geïmplementeerd zal worden.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Nee	Sinds 2018 wordt door SSC-ICT gewerkt aan operationalisering van Digikoppeling voor het gebruik binnen de dienstverlening van Doc-Direkt.

Ten opzichte van 2018 is de planning voor implementatie van HTTPS en HSTS verschoven van 4e kwartaal 2018 naar 4e kwartaal 2019. Voor TLS is geen concrete planning afgegeven.

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

3.9 Rijksoverheid.nl

Beheerorganisatie: Ministerie van AZ (DPC)

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 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.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/ phishing)	Ja	DKIM is geïmplementeerd.
DMARC (Anti-phishing)	Nee	DMARC is geïmplementeerd maar de policy is onvoldoende strikt (zie: https://internet.nl/mail/rijksoverheid.nl/249091/#). SSC-ICT beheert technisch het maildomein en het aanzetten van de dmarc policy op quarantaine of reject is voor de SSC-ICT geen probleem. Het gevolg van het aanzetten van de stricte dmarc policy is dat partijen die mail mogen versturen als rijksoverheid.nl worden aangemerkt als SPAM. Dit komt omdat de echtheidskenmerken die de partijen toepassen niet overeenkomen met de echtheidskenmerken die SSC-ICT toepast op rijksoverheid.nl. Om er voor te zorgen dat de partijen mail kunnen versturen als rijksoverheid.nl zijn er meerdere oplossingen. In overleg met de eigenaar van het maildomein moet dan bepaald worden welke partijen gebruikt mogen maken van rijksoverheid.nl en welke niet.
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)	Deels	De website rijksoverheid.nl ondersteunt zowel IPv6 als IPv4 (zie: https://internet.nl/site/www.rijksoverheid.nl/). 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 eind 2019 ondersteunen.
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 audit heeft plaatsgevonden in 2019.

SPF (Preventie van mailspoofing/phishing)	Ja	Het e-maildomein @rijksoverheid.nl is integraal van SPF voorzien (zie: https://internet.nl/mail/rijksoverheid.nl/). Vanwege ontbreken van een aanspreekpunt van het maildomein, heeft geen verdere afstemming plaats gevonden met een beheerder na toetsing van de standaard. Deze statustoekenning is van PBLQ en is niet gevalideerd.
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/). Vanwege ontbreken van een aanspreekpunt van het maildomein, heeft geen verdere afstemming plaats gevonden met een beheerder na toetsing van de standaard. Deze statustoekenning is van PBLQ en is niet gevalideerd.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Rijksoverheid.nl is onderdeel van het Platform Rijksoverheid Online en geheel voorzien van https door middel van QWAC PKIo EV certificaten (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 PDFs op rijksoverheid.nl kunnen plaatsen. Het is daardoor simpelweg niet helemaal onder controle welke soorten PDF worden toegepast.
		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 2018 is STARTTLS/DANE geïmplementeerd. De standaard DMARC is sinds 2018 onvoldoende geïmplementeerd. De status gaat van ja naar nee. Voor het maildomein geldt dat rijksoverheid.nl niet voldoet aan IPv6, waardoor de status van ja naar deels is gegaan. De status van de standaard PDF 1.7 / PDF A/1 en PDF A/2 is van nee naar deels gegaan. Verder is de applicatie die gebruik maakte van de standaard SAML komen te vervallen. Deze standaard is daardoor niet meer van toepassing. De statussen ten aanzien van de standaarden STARTTLS-DANE en SPF, gebruikt voor het emaildomein, zijn toegekend door PBLQ en niet gevalideerd. Ondanks herhaalde pogingen de verantwoordelijke te vinden, is dit niet gelukt.

Concluderend moeten voor de voorziening rijksoverheid.nl nog de volgende standaarden (volledig) worden geïmplementeerd: DMARC, IPv4 en IPV6, PDF1.7 / PDF A/1 en PDF A/2.

4. Gegevens en registreren

4.1 Basisregistraties

4.1.1 NHR (Handelsregister)

Beheerorganisatie: Kamer van Koophandel

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

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)	Nee	De ondertekening in de emailomgeving van kvk.nl vindt momenteel niet goed plaats. Dit wordt z.s.m. hersteld, in ieder geval in 2019. Er is samenhang met de HSTS melding hierna vanwege afspraken met de provider van kvk.nl.zie: https://en.internet.nl/site/kvk.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening gebruikt zowel HTTPS als HSTS. Alleen voor kvk.nl werkt hsts niet, dit wordt in 2019 hersteld. Was nog niet gebeurd om 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)	Deels	Mailservers e.d. zijn bereikbaar via zowel IPv4 als IPv6 maar de website van KvK nog niet, De website kvk.nl ondersteunt IPv4, maar is niet toegankelijk via IPv6 (zie: https://internet.nl/site/www.kvk.nl/). Het project om over te stappen naar IPv6 voor de website hangt samen met de wisseling van provider die KvK wil gaan doen, die wisseling gaat niet voor 2020 plaatsvinden.
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)	Deels	De voorziening past STARTTLS toe, DANE nog niet (zie: https://internet.nl/mail/kvk.nl/). Op DNS-servers is dit uitgerold maar op de emailservers onder Microsoft niet omdat Microsoft DANE niet ondersteunt.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De KvK gebruikt TLS op de verbindingen waar voorheen SSL werd gebruikt. De KvK gebruikt versie TLS1.2 (zie: https://internet.nl/site/www.kvk.nl/).
		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)	Deels	De bij de KvK in gebruik zijnde content management 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 upgrade van Tridion vindt in 2019 plaats, daarna worden de koppelingen daarmee aangepakt (2020 e.v.). 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. Er zijn nog documenten in PDF A/1 die nog in 2019 worden omgezet.
SKOS (Thesauri en begrippen-woordenboeken)	Nee	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. Implementatie van SKOS in de Gegevenscatalogus HR is nog niet ingepland vanwege andere prioriteiten.
		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 2018 is de status van STARTTLS/DANE en Open API Specification van gepland naar deels gegaan. De status van DNSSEC is gegaan van ja naar nee. De status van HSTS is van deels naar ja gegaan. Daarnaast is de planning van IPv4 en IPv6 verschoven.

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

4.1.2 BAG (Basisregistraties Adressen en Gebouwen), BRK (Basisregistratie Kadaster), BGT (Basisregistratie Grootschalige Topografie), WOZ (Basisregistratie Waarde Onroerende Zaken)

Beheerorganisatie: Kadaster

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

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

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

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

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

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

Standaard	Status	Toelichting beheerder
Internet en beveiliging		

DKIM (Preventie van mailspoofing/ phishing)	Ja	Het Kadaster voldoet aan DKIM.
DMARC (Anti-phishing)	Ja	Deze standaard is geïmplementeerd.
DNSSEC (Beveiligde domeinnamen)	Ja	De website www.kadaster.nl ondersteunt DNSSEC (zie: https://internet.nl/domain/www.kadaster.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels	HTTPS en HSTS zijn deels geïmplementeerd. (zie: https://internet.nl/domain/www.kadaster.nl/) Eerdere planningen voor volledige implementatie in Q1 en Q4 2018 zijn niet gehaald. HSTS is inmiddels op de meeste Kadaster endpoints geïmplementeerd. Er is een beperkte set aan Digikoppeling gerelateerde content (schema's) die nog niet over kunnen naar HTTPS en HSTS. Er is nog geen duidelijke planning voor.
IPv4 en IPv6 (Internetnummers)	Ja	Zowel IPv4 als IPv6 worden ondersteund door het Kadaster (zie: https://internet.nl/domain/www.kadaster.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Het Kadaster is gecertificeerd voor NEN-ISO/IEC 27001 en hanteert 27002. Het Handboek Beveiliging Kadaster is volledig op de 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/kadaster.nl/).
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Nee	STARTTLS is geïmplementeerd (zie: https://internet.nl/domain/www.kadaster.nl/). Eerdere planningen voor implementatie van DANE per Q1 2018 en later Q1 2019 zijn niet gehaald. De verhuizing van het mail domein is vertraagd, waarbij opgemerkt moet worden dat de bestemming, in dit geval Microsoft, geen planning heeft voor de implementatie van DANE.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Deze standaard wordt volledig door het Kadaster ondersteund (zie: https://internet.nl/domain/www.kadaster.nl/).
		Document en (web/app)content
Open API Specification (Beschrijven van REST API's)	Ja	Deze standaard is geïmplementeerd.
PDF 1.7, PDF/A-1 en PDF/A-2 (Documentpublicatie/ archivering)	Ja	Uittreksels worden verstrekt in PDF 1.4-formaat. Databestanden worden vooral in GML uitgewisseld. GML is een standaard XML-formaat voor Geo-data, gebaseerd op de Geo-standaarden. Afnemers melden geen problemen met het huidige PDF formaat. Daarom geeft het Kadaster

		geen prioriteit aan het vervangen van PDF 1.4. Voor het archiveren van kennisgevingen wordt gebruik gemaakt van PDF/A-1.
SKOS (Thesauri en begrippen-woordenboeken)	Deels	Het Kadaster hanteert SKOS voor de beschikbaarstelling van begrippenkaders van basisregistraties. De begrippenkaders voor de BRK zoals gepubliceerd op brk.basisregistraties.nl, de BAG zoals gepubliceerd op bag.basisregistraties.nl en de BGT (IMgeo) en BRT op definities.geostandaarden.nl zijn allemaal conform SKOS. Voor de WOZ moet deze slag nog worden gemaakt. (4 van de 5 BR's). Hiervoor is nog geen planning. Het Kadaster is alleen verantwoordelijk voor de hosting en het technisch beheer van de LV-WOZ de verantwoordelijkheid voor de implementatie van SKOS ligt bij de Waarderingskamer. Voor zover bij het Kadaster bekend is er geen planning voor de implementatie van SKOS voor de LV-WOZ.
		E-facturatie en administratie
NLCIUS (Elektronisch factureren)	Nee	Invoering van elektronisch factureren is zowel 2018 als in 2019 onderhanden en daarop zal gebruik gemaakt gaan worden van de NLCIUS standaard.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichten-uitwisselingen)	Deels	Vrijwel alle koppelingen met afnemers, andere basisregistraties en evt. front-office systemen worden gelegd op basis van Digikoppeling: - de koppelingen voor het aanleveren van gegevens aan LV-BAG, LV-WOZ en LV-BGT zijn gebaseerd op Digikoppeling standaarden; - het aanleveren door bronhouders (o.a. notariaat) van gegevens aan de BRK is niet gebaseerd op Digikoppeling; - de koppelingen voor het verkrijgen van informatie van gegevens uit LV BAG en LV WOZ en BRK zijn gebaseerd op Digikoppeling. Daarnaast kan informatie uit LV's worden verkregen via PDOK (Publieke Dienstverlening op de Kaart) die gebruik maakt van de Open GEO-standaarden. Ook de informatie uit de BRT wordt op deze wijze geleverd. Gegevens uit de BGT zijn beschikbaar via PDOK.
Geo-Standaarden (Geografische informatie)	Ja	Naast de INSPIRE richtlijnen, maakt het Kadaster gebruik van NEN3610 en de meest gangbare Geo standaarden voor de betreffende basisregistraties.
StUF (Uitwisseling administratieve overheidsgegevens)	Ja	Het Kadaster maakt deels gebruik van StUF en is deels volgens de Geo-standaarden (GML) opgemaakt. StUF wordt gebruikt voor aanlevering van bronhouder naar LV-BAG, LV-WOZ en LV-BGT. WOZ en BGT worden ook geleverd in StUF.

Ten opzichte van 2018 is de status van HTTPS/HSTS veranderd van gepland naar deels. Er is een beperkte set aan Digikoppeling gerelateerde content (schema's) die nog niet over kunnen naar HTTPS en HSTS. Er is nog geen duidelijke planning voor. De status van STARTTLS/DANE is veranderd van gepland naar nee. De verhuizing van het mail domein is vertraagd.

Concluderend moeten voor de BAG, BRK, BGT en WOZ nog de volgende standaarden (volledig) worden geïmplementeerd: HTTPS/HSTS, STARTTLS/DANE, SKOS, NLCIUS, Digikoppeling 2.0.

4.1.3 BRT (Basisregistratie Topografie)

Beheerorganisatie: Kadaster

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	DMARC is geïmplementeerd.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels	HTTPS en HSTS zijn deels geïmplementeerd (zie: https://internet.nl/domain/www.kadaster.nl/). Eerdere planningen voor (volledige) implementatie in Q1 en in Q4 2018 zijn niet gehaald. HSTS is inmiddels op de meeste Kadaster endpoints geïmplementeerd. Er is een beperkte set aan Digikoppeling gerelateerde content (schema's) die nog niet over kunnen naar HTTPS en HSTS. Er is hier nog geen duidelijke planning voor.
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.
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Nee	STARTTLS is geïmplementeerd (zie: https://internet.nl/domain/www.kadaster.nl/). Eerdere planningen voor implementatie van DANE per Q1 2018 en later Q1 2019 zijn niet gehaald. De verhuizing van het mail domein is vertraagd, waarbij opgemerkt moet worden dat de bestemming, in dit geval Microsoft, geen planning heeft voor de implementatie van DANE.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Deze standaard wordt volledig door het Kadaster ondersteund (zie: https://internet.nl/domain/www.kadaster.nl/).
		Document en (web/app)content
OWMS (Metadata overheidsinformatie)	Nee	OWMS is wel van toepassing, maar PDOK hanteert via het Nationaal GEO Register de wettelijk vastgelegde standaarden, gebaseerd op Inspire en ISO volgens het zogenaamde NL profiel. Data.overheid.nl harvest het NGR met behulp van de CSW standaard (Catalogue Services for the Web' een OGC-Geostandaard (Open Geospatial Consortium), ook onderdeel van INSPIRE). De BRT voldoet dus niet aan de standaard maar voldoet

		wel aan alternatieve internationale standaarden. Er zijn geen interoperabiliteitsproblemen hierdoor.
SKOS (Thesauri en begrippen-woordenboeken)	Ja	Het Kadaster hanteert SKOS voor de beschikbaarstelling van begrippenkaders van basisregistraties. De begrippenkaders voor de BRK zoals gepubliceerd op brk.kadaster.nl, de BAG zoals gepubliceerd op bag.kadaster.nl en de BGT (IMgeo) en BRT op definities.geostandaarden.nl zijn allemaal conform SKOS.
		Stelselstandaarden
Geo-Standaarden (Geografische informatie)	Ja	De BRT wordt zowel geleverd via PDOK (Wat biedt Publieke Dienstverlening Op de Kaart) in GML (Objectdata), als via internationale Geo-standaarden. Daarnaast wordt de BRT geleverd via PDOK in rasterformaat in GEO, tiff formaat en WMTS (Web Map Tile Service).

Ten opzichte van 2018 is de status van HTTPS/HSTS veranderd van gepland naar deels. Er is een beperkte set aan Digikoppeling gerelateerde content (schema's) die nog niet over kunnen naar HTTPS en HSTS. Er is nog geen duidelijke planning voor. De status van STARTTLS/DANE is veranderd van gepland naar nee. De verhuizing van het mail domein is vertraagd.

Concluderend moeten voor de BRT nog de volgende standaarden (volledig) worden geïmplementeerd: HTTPS/HSTS, STARTTLS/DANE, OWMS.

4.1.4 BRO (Basisregistratie Ondergrond)

Beheer organisatie: Programmabureau BRO van het Ministerie BZK (afdeling DG BRW – RO)

Werking en inhoud BRO
De Basisregistratie Ondergrond (BRO) brengt alle informatie over de Nederlandse ondergrond op één plek bij elkaar en stelt deze via één loket digitaal beschikbaar. Per 1 januari 2018 is de wet BRO in werking getreden voor de eerste tranche van registratieobjecten (Geotechnisch sondeeronderzoek, Booronderzoek, Grondwatermonitoringput). De ketenprocessen van de BRO zijn ingericht en de bronhouders zijn in staat om aan te (laten) leveren via het Bronhouderportaal aan de Landelijke Voorziening (LV). Er is een gebruiksplicht inwerking getreden voor overheidsorganisaties en iedereen die in opdracht van hen werkzaamheden verricht. Op 1 februari 2018 waren er bijna 50 bronhouders aangesloten op het Bronhouderportaal. Het gaat om 28 gemeenten, acht provincies, negen waterschappen en vier overige overheidsorganisaties.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DNSSEC (Beveiligde domeinnamen)	Ja	Toegepast door alle hostingpartijen die BRO systemen hosten.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	BRO website (https://www.basisregistratieondergrond.nl), BRO web applicaties (DINO|BRO Loket https://www.dinoloket.nl) en APIs ondersteunen HTTPS en HSTS.
IPv4 en IPv6 (Internetnummers)	Deels	Hosting Landelijke Voorziening BRO door TNO bij Solvinity > Hoewel alle gebruikte componenten IPv6 capabel zijn, wordt het interne netwerk ingericht op basis van IPv4. Initieel is de internetverbinding

		ook alleen op basis van IPv4 ingericht. In een later stadium zal de internetverbinding doormiddel van een IPv4/IPv6 proxy ook via IPv6 beschikbaar worden gesteld. Hosting Bronhouderportaal BRO bij Standaard Platform (ODC Noord) > Zie status (d.d. maart 2018) in de monitor open standaardenbeleid https://www.noraonline.nl/wiki/Monitor_Open_Standaardenbeleid_2016/ODC-Noord-IPv6_en_IPv4 basisregistratieondergrond.nl is via IPv4 en IPv6 bereikbaar, voor dinoloket.nl geldt dat het domein nog alleen via IPv4 bereikbaar is.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	TNO (en hosting partij Solvinity) zijn ISO 27001/27002 compliant ICTU (en hosting partij SP|ODC-Noord) zijn ISO 27001/27002 compliant PDOK (en hosting partij CapGemini) zijn ISO 27001/27002 compliant
SAML (Inloggegevens)	Ja	Het Bronhouderportaal BRO maakt gebruik van eHerkenning voor authenticatie van gebruikers. eHerkenning ondersteunt SAML. Zie ook evaluatierapport SAML 2.0 Forum Standaardisatie https://www.forumstandaardisatie.nl/sites/bfs/files/proceedings/FS%20180314.3C%20Evaluatie%20SAML%202.0.pdf
TLS (Beveiligde, versleutelde verbindingen)	Ja	De BRO gebruikt SSL (TLS) certificaten voor inname en uitgifte APIs en voor beveiligde gegevensuitwisseling met PDOK.
		Document en (web/app)content
CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)	Ja	DIGIDOC2 > Interne opslag van formele documenten programma BRO vindt plaats in het DMS systeem van het Ministerie BZK Digidoc2 v7.0.1. Zie voor CMIS compliancy van Digidoc2 het onderzoek Forum uit 2014 (https://www.forumstandaardisatie.nl/sites/bfs/files/Aanvullend%20onderzoek%20CMIS.pdf). Inmiddels zijn de compliancy issues waarover in het 2014 rapport wordt gesproken mogelijk opgelost
	Ja	SAMENWERKINGSRUIMTEN RIJK (https://sts.dwr.rijksdienst.nl) > Samenwerkingsruimte BRO (externe uitwisseling o.a. met BIT) gebaseerd op Sharepoint.. Sharepoint ondersteunt CMIS https://docs.microsoft.com/en-us/sharepoint/dev/general-development/content-management-interoperability-services-cmis-in-sharepoint
	Ja	CONFLUENCE > Confluence omgeving BRO is een WIKI omgeving voor alle operationele content management BRO programma. Confluence ondersteunt CMIS, zie https://community.atlassian.com/t5/Answers-Developer-

		Questions/How-do-I-set-up-a-CMIS-Repository-within-Confluence/qaq-p/518301
	Ja	ALFRESCO DMS > Alfresco wordt door LV BRO en Bronhouderportaal BRO gebruikt voor opslag van IMBRO XML documenten registratie authentieke brondocumenten). Alfresco ondersteunt CMIS https://docs.alfresco.com/5.0/pra/1/topics/cmis-welcome.html
Open API Specification (Beschrijven van REST API's)	Ja	Het Bronhouderportaal BRO (voorportaal voor validatie van BRO gegevens voordat deze worden door geleverd naar de Landelijke Voorziening BRO) voldoet aan de open API specificatie https://www.bronhouderportaal-bro.nl/bpbro-frontend/documentation/api.html. De Landelijke Voorziening BRO voldoet aan de PTOLU Digikoppeling standaard (SOAP-XML).
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Landelijke Voorziening BRO inname en uitgifte APIs zijn gebaseerd op Digikoppeling 2.0.
Geo-standaarden	Ja	BRO is een geo-basisregistratie. Geografische BRO gegevens worden o.a. beschikbaar gesteld via het GDI geo-knooppunt PDOK (www.pdok.nl). De PDOK APIs zijn gebaseerd op Open Geospatial Consortium standaarden (www.opengeospatial.org), waaronder OGC:WMS, OGC:WFS, OGC:WCS. Geografische gegevens worden uitgeleverd in open bestandsformaten (OGC:GML, OGC:Geopackage, OGC:GeoTIFF). BRO metadata wordt via het Nationaal Georegister (www.nationaalgeoregister.nl) ontsloten. Het Nationaal Georegister is gekoppeld met (wordt geharvest door) data.overheid.nl Het NGR is gebaseerd op de geo-standaarden CS-W 2.0 (discovery service), ISO 19115 NL profiel (metadata voor geografische datasets), en ISO 19119 NL profiel (metadata voor geografische web services)
		Water en bodem
Aquo-standaard	Ja	Relevante onderdelen worden meegenomen in de BRO standaardisatie van het grondwaterdomein (de aquo standaard omvat ook oppervlaktewater hetgeen buiten scope is voor de BRO).
		Juridische verwijzingen
BWB (Identificatie van en verwijzing naar wet- en regelgeving)	Gepland	Zou gebruikt kunnen (en moeten) worden voor verwijzingen naar BRO gerelateerde wetsartikelen vanuit de BRO website en in overige BRO documenten zoals programmaplan, GAS, PSA, etc. (zie voorbeeld https://www.overheid.nl/help/wet-en-regelgeving/verwijzen-naar-wet-en-regelgeving). De standaard wordt 3e kwartaal 2019 geïmplementeerd.

De BRO is dit jaar voor eerst opgenomen in het onderzoek. Voor SKOS, SIKB0101, SIKB0102 geldt dat deze standaarden (mogelijk) in de toekomst relevant zijn. I.v.m. SKOS: De BRO begrippen (o.a. registratieobjecten) worden binnenkort opgenomen in de Stelselcatalogus (gebaseerd op SKOS, zie

https://www.noraonline.nl/wiki/Stelselcatalogus ondersteunde standaarden Stelselcatalogus). Het BRO standaardisatieteam o.l.v. Geonovum heeft hierover reeds contact met Logius. I.v.m. SIKB0101: Mogelijk op termijn van belang voor BRO (opname van onderzoeksgegevens over de milieu-hygiënische kwaliteit van de bodem in de BRO wordt op dit moment onderzocht). I.v.m. SIKB0102: Archeologische informatie is geen onderdeel van de BRO > In een mogelijk vervolgprogramma “BRO II” zullen archeologische gegevens mogelijk onderdeel gaan uitmaken van de BRO.

Concluderend moeten voor de BRO nog de volgende standaarden (volledig) worden geïmplementeerd: IPv4 en IPv6 en BWB.

4.1.5 BRV (Basisregistratie Voertuigen)

Beheerorganisatie: RDW (Rijksdienst Wegverkeer)

Werking en inhoud van BRV
In de Basisregistratie Voertuigen (BRV) staan gegevens van voertuigen, kentekenbewijzen en personen aan wie het kentekenbewijs is afgegeven. Een organisatie is aangesloten op de Basisregistratie Voertuigen wanneer op een gestructureerde wijze (niet incidenteel) informatie wordt afgenomen uit het Kentekenregister. Alle gemeenten, provincies, waterschappen, (relevante) departementen, manifestpartijen en andere overheidsorganisaties in de voertuigenketen zijn aan gesloten op de BRV.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	De BRV voldoet aan DKIM.
DMARC (Anti-phishing)	Deels	De BRV voldoet aan DMARC. Rdw.nl voldoet niet aan de standaard, zie: https://internet.nl/mail/rdw.nl/253063/. De RDW is in 2017 gestart met een nieuwe leverancier die ook maatregelen voor het aanscherpen van DANE, DKIM, SPF, etc. zou meenemen. 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. De onderwerpen zoals DANE, DKIM, SPF, etc. zijn ook onderdeel van deze verbeteringen en de verwachting is dat RDW dit komende jaar de verbeteringen heeft 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)	Deels	Implementatie zou medio 2018 gerealiseerd worden. Rdw.nl voldoet niet aan de standaard, zie: https://internet.nl/mail/rdw.nl/253063/. De RDW is in 2017 gestart met een nieuwe leverancier die ook maatregelen voor het aanscherpen van DANE, DKIM, SPF, etc. zou meenemen. 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. De

		onderwerpen zoals DANE, DKIM, SPF, etc. zijn ook onderdeel van deze verbeteringen en de verwachting is dat RDW dit komende jaar de verbeteringen heeft 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)	Ja	De BRV voldoet aan STARTTLS, DANE, DKIM en SPF
TLS (Beveiligde, versleutelde verbindingen)	Ja	RDW ondersteunt en gebruikt de TLS protocollen op de e-mail servers en Digikoppeling.
		Document en (web/app)content
CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)	Nee	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.
OWMS (Metadata overheidsinformatie)	Ja	De toegang tot BRV-data is op data.overheid.nl in overeenstemming met OWMS gemetadateerd beschikbaar.
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/archivering)	Ja	Bij digitale dienstverlening worden uittreksels en informatie uit de BRV in PDF/A vorm verstrekt.
SKOS (Thesauri en begrippenwoordenboeken)	Ja	De BRV voldoet aan SKOS.
		Stelselstandaarden

Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Deels	RDW maakt voor alle nieuwe uitwisselingen gebruik van Digikoppeling. Dat is onder meer het geval in de uitwisseling met MijnOverheid (Berichtenbox), CJIB, Politie, ILT, CBR, de Belastingdienst, etc. De intentie is uitgesproken om ook bestaande koppelingen pro-actief te migreren om de voordelen van het diginetwerk te benutten. Een planning hiervoor is nog niet vastgesteld.

Ten opzichte van 2018 voldoet de voorziening nog deels aan DMARC. De status is van ja naar deels gegaan. De status van HTTPS/HSTS ging van gepland naar deels.. De status van DNSSEC is van ja naar deels gegaan.

Concluderend moeten voor de BRV nog de volgende standaarden (volledig) worden geïmplementeerd: DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, CMIS, Digikoppeling 2.0.

4.1.6 BRI (Basisregistratie Inkomen)

Ondanks herhaalde verzoeken en gesprekken met verschillende contactpersonen om dit jaar informatie aan te leveren ten aanzien van gebruik van standaarden bij de BRI, is het dit jaar niet gelukt een reactie te krijgen van de belastingdienst.

Beheerorganisatie: Belastingdienst

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	De voorziening voldoet aan de DMARC standaard.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De BRI voldoet aan de standaard beveiligingseisen van de Belastingdienst. Deze eisen zijn conform VIR met classificatie departementaal vertrouwelijk. Voor opsporingsgegevens (FIOD) geldt een strakker regime. Aangezien het beveiligingskader voor de gehele Belastingdienst geldt, is er geen apart in control statement voor de BRI.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De actuele versies van TLS maken deel uit van de standaard beveiligingsrichtlijnen van de Belastingdienst.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Digikoppeling wordt toegepast in de rol van afnemer van berichten van basisregistraties(HR). De ebMS-koppeling met Digilevering is operationeel in de productie-omgeving. De aansluiting op Digilevering wordt nu alleen gebruikt in de rol van afnemer van het stelsel van basisregistraties. Het aansluiten van

	de BRI als Basisregistratie/leverancier op Digilevering was niet eerder dan 2017-2018 gepland.

Ten opzichte van 2018 zijn er geen wijzigingen opgenomen in de tekst.

4.2 Digilevering

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM[7] (Preventie van mailspoofing/phishing)	Ja	Digilevering draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. DKIM is geïmplementeerd op de centrale voorziening mail relay.
DMARC (Anti-phishing)	Ja	DMARC is inmiddels geïmplementeerd en doorgevoerd in de DNS instellingen.
DNSSEC[8] (Beveiligde domeinnamen)	Ja	DNSSEC is geïmplementeerd op de centrale voorziening DNS.
HTTPS/HSTS[9] (Beveiligd, versleuteld webverkeer)	Ja	Digilevering voldoet aan de HTTPS standaard. Voor Digilevering is een PKIO certificaat verplicht om te kunnen aanloggen op de applicatie. Zonder dit certificaat kan de https doorverwijzing niet slagen en biedt www.internet.nl geen toetsing. HSTS wordt aangeboden.

[7] Digimelding en Digilevering zijn op het Equinix platform geïmplementeerd, de applicaties kunnen alleen via de mail-relay server van het platform e-mail versturen. Deze mail –relay server is niet van buitenaf benaderbaar, daarom kan dit met internet.nl niet getoetst worden.

[8] idem

[9] idem

IPv4 en IPv6 (Internetnummers)	Nee	IPv6 kan niet worden aangeboden, omdat de infrastructuur van Logius dit nog niet voldoende ondersteunt. Dit is een Logius breed vraagstuk. De vraag hoe IPv6 geïmplementeerd dient te worden is wederom bij onze architecten ingediend.
SPF[10] (Preventie van mailspoofing/phishing)	Ja	Digilevering draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. SPF is geïmplementeerd op de centrale voorziening mail relay.
STARTTLS/DANE[11] (Beveiligd, versleuteld mailverkeer)	Ja	Digilevering draait op het Logius Managed Services platform. Vanuit de clouddienst is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Digilevering maakt gebruik van Digikoppeling.

Ten opzichte van 2018 is DMARC volgens planning geïmplementeerd. De status van IPv4 en IPv6 ging van gepland naar nee.

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

4.3 Digimelding

Beheerorganisatie: Logius

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

[10] idem

[11] idem

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Gepland	DKIM draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. Gepland Q3 2019.
DMARC (Anti-phishing)	Ja	DMARC is geïmplementeerd.
DNSSEC[12] (Beveiligde domeinnamen)	Ja	DNSSEC is geïmplementeerd.
HTTPS/HSTS[13] (Beveiligd, versleuteld webverkeer)	Ja	De url portaal.digimelding.nl voldoet aan HTTPS en HSTS.
IPv4 en IPv6 (Internetnummers)	Nee	Digimelding gebruikt het Logius infrastructuurplatform. IPv6 kan niet worden aangeboden, omdat de infrastructuur van Logius dit nog niet voldoende ondersteunt. Dit is een Logius breed vraagstuk. De vraag hoe IPv6 geïmplementeerd dient te worden is wederom bij onze architecten ingediend. Digimelding ondersteunt op dit moment alleen IPv4.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd.
STARTTLS/DANE[14] (Beveiligd, versleuteld mailverkeer)	Nee	Digimelding draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Digimelding maakt gebruik van Digikoppeling.

[12] [12] Digimelding en Digilevering zijn op het Equinix platform geïmplementeerd, de applicaties kunnen alleen via de mail-relay server van het platform e-mail versturen. Deze mail –relay server is niet van buitenaf benaderbaar, daarom kan dit met internet.nl niet getoetst worden.

[13] Digimelding portaal is alleen benaderbaar via de url portaal.digimelding.nl

[14] Digimelding en Digilevering zijn op het Equinix platform geïmplementeerd, de applicaties kunnen alleen via de mail-relay server van het platform e-mail versturen. Deze mail –relay server is niet van buitenaf benaderbaar, daarom kan dit met internet.nl niet getoetst worden.

Ten opzichte van 2018 voldoet Digimelding niet meer aan de standaard DKIM, de status is veranderd van ja naar gepland. Verder voldoet de voorziening inmiddels aan de standaarden DMARC en HTTPS en HSTS.

Concluderend moet Digimelding de volgende standaarden nog (volledig) implementeren: DKIM, IPv4 en IPv6 en STARTTLS/DANE.

4.4 Stelselcatalogus

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	De Stelselcatalogus voldoet aan DMARC (zie: https://internet.nl/mail/stelselcatalogus.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC is geïmplementeerd op de centrale voorziening DNS (zie: https://internet.nl/site/www.stelselcatalogus.nl/).
HTTPS/ HSTS (Beveiligd, versleuteld webverkeer)	Gepland	De voorziening voldoet niet meer aan HTTPS (zie: https://internet.nl/site/www.stelselcatalogus.nl/). De website www.stelselcatalogus.nl zal voor eind 2019 worden voorzien van een certificaat.
IPv4 en IPv6 (Internetnummers)	Nee	De Stelselcatalogus gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt niet de open standaard IPv4 en IPv6 voor internet gebruik. Stelselcatalogus ondersteunt geen IPv6 (zie: https://internet.nl/site/www.stelselcatalogus.nl/).
		Document en (web/app)content
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/ archivering)	Ja	Documenten worden als PDF-A/1 aangeboden via de website.
SKOS (Thesauri en begrippen-woordenboeken)	Ja	SKOS wordt toegepast door de voorziening.
		Juridische identificatie en verwijzing

BWB (Wet- en regelgeving)	Ja	De Stelselcatalogus gebruikt het Basis Wetten Bestand (BWB) via Juriconnect als open standaard voor de link naar de wetgeving als bron. De Juriconnect Id's worden gebruikt om per gegeven of begrip in de Stelselcatalogus de link te leggen naar de wet en het artikel in het Basis Wetten Bestand.

Ten opzichte van 2018 is een planning afgegeven voor implementatie van HTTPS/HSTS (status van nee naar gepland) en voldoet de stelselcatalogus niet langer aan IPv4 en IPv6 (status van ja naar nee).

Concluderend, moet stelselcatalogus nog de volgende standaarden (volledig) implementeren: HTTPS/HSTS en IPv4 en IPv6.

4.5 P-Direkt

Beheerorganisatie: P-Direkt

Werking en inhoud van P-Direkt
P-Direkt is de administratieve dienstverlener van en voor de Rijksdienst, op het gebied van personeelszaken. De salarisbetaling en personele informatievoorziening zijn de belangrijkste eindproducten. De voorziening P-Direkt wordt geleverd door de organisatie P-Direkt.

Medewerkers van het Rijk, loggen bij P-Direkt in via het Rijksportaal, en komen dan op een eigen P-Direkt portal. Daar vinden ze intranetachtige functionaliteit (met onder andere alle relevante regelgeving) maar ook een zogenaamd mijn-domein, waar ze eigen gegevens kunnen opgeven/wijzigen, informatie kunnen opvragen (loonstroken, vakantiesaldo etc.) en zaken kunnen regelen.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	P-Direkt maakt gebruik van de mailservers van SSC-ICT, onder andere voor het versturen van de loonstroken aan de medewerkers. Het initiatief voor de adoptie van dit soort standaarden ligt dan ook bij SSC-ICT. Navraag bij SSC-ICT leert dat DKIM actief gemaakt is voor deze mailservice van P-Direkt.
DMARC (Anti-phishing)	Ja	De Rijksbrede mail voorziening waarvan P-Direkt gebruik maakt, ondersteunt DMARC.
DNSSEC (Beveiligde domeinnamen	Nee	Op de Haagse ring maakt het netwerk van SSC-ICT, waar P-Direkt gebruik van maakt, geen gebruik van DNSSEC. Ook hier geldt dat P-Direkt een afnemer is van een Rijksbrede dienstverlening en het initiatief voor het implementeren van DNSSEC bij de SSC-ICT ligt. DNSSEC is nog niet geïmplementeerd binnen SSC-ICT en dus ook niet op het P-Direkt Self Service portaal. Op de externe website www.p-direkt.nl is DNSSEC wel geïmplementeerd.

HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	HTTPS is 100% doorgevoerd voor alle communicatie met klanten. HSTS is volledig geïmplementeerd op de interne en externe site van P-Direkt.
IPv4 en IPv6 (Internetnummers)	Nee	De P-Direkt omgeving, draaiend in de ODC Rijswijk omgeving en beheert door SSC-ICT, is gebaseerd op IPv4. ODC Rijswijk en Haagse Ring (het koppelnetwerk waar P-Direkt gebruik van maakt) ondersteunt geen IPv6.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De hosting van de dienstverleningssystemen van P-Direkt voldoet aan de BIR (BIR compliancy is integraal onderdeel van de inrichting van het Overheids Data Center, en als zodanig daarmee ook voor P-Direkt). Daarmee wordt indirect voldaan aan NEN-ISO/IEC 27001/27002, de BIR is immers gebaseerd op NEN-ISO/IEC 27001/27002, aangevuld met overheidsspecifieke maatregelen. In Q2 2019 is in samenwerking met het Ministerie van Infrastructuur en Waterstaat een project gestart om volledig Baseline Informatiebeveiliging Overheid (BIO), en daarmee NEN-ISO/IEC 27001/27002 compliant te zijn. Verwachtte afronding is eind 2019, begin 2020. Een aantal P-Direkt systemen, inclusief beheerorganisatie voldoet inmiddels aan de BIO.
SAML (Inloggegevens)	Ja	P-Direkt gebruikt SAML om Single Sign-On in te vullen. Verbinding naar de kerndepartementen is gelegd, maar een gedeelte van de rijksambtenaren van onderliggende organisatieonderdelen, moeten nog handmatig inloggen. P-Direkt heeft met de kerndepartementen de afspraak gemaakt dat de kerndepartementen verantwoordelijk zijn voor het implementeren van de Single Sign-on functie bij de onderliggende organisatieonderdelen.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd door de beheerder van de maildienst (in het geval van P-Direkt is dat SSC-ICT).
STARTTLS/DANE	Nee	STARTTLS en DANE zijn van toepassing. STARTTLS is wel geïmplementeerd op de Rijks Mail Relay, DANE niet.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Alle diensten van P-Direkt die door middel van HTTP worden ontsloten, worden aangeboden via TLS v1.0, v1.1 en v1.2.
		Document en (web/app)content
Ades Baseline Profiles (Digitaal ondertekenen van documenten)	Nee	De implementatie van deze standaard is nog niet gestart en hiervoor is nog geen concrete planning.
ODF (Document-bewerkingen)	Nee	Veel brieven die automatisch gegenereerd worden, worden in Word gemaakt en naar managers verstuurd, die deze dan zelf nog aanpassen. P-Direkt gebruikt .doc(x), omdat dit voor de doelgroep het meest gangbaar is. De ontvanger van de brieven zou dit zelf moeten omzetten met de aanwezige KA software die ODF ondersteunt. In het proces dat brieven genereert is het niet mogelijk ODF bestanden te genereren.
PDF 1.7 – PDF A/1 of PDF A/2 (Documentpublicatie/ archivering)	Ja	De meeste zaken die het digitale personeelsdossier ingaan zijn PFDA/1. Sinds de ingebruikname van de nieuwe versie van het Document/Record Management Systeem worden ook de loonstroken opgeslagen in PDF A/1 formaat.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	P-Direkt heeft vele interfaces met partijen binnen de overheid, Identity management, hr-data, arbo-diensten, ziekmeldingen, koppelingen met BD. Het salarisverwerkingssysteem werkt op basis van Digikoppeling. Alle nieuwe koppelingen die P-Direkt ontwikkelt,

		worden gebouwd op basis van Digikoppeling. Richting 2018 migreert de voorziening naar de rijksdatacenters, Digikoppeling krijgt dan een nog belangrijkere rol. Nieuwe interfaces zoals TEM2W, IDM2 en de ARBO interface zijn conform Digikoppeling 2.0.
		Juridische identificatie en verwijzing
BWB (Wet- en regelgeving)	Ja	Alle verwijzingen naar wetten worden conform de BWB-standaard gemaakt. De redactie heeft de richtlijn dat ze altijd op deze manier handelt bij verwijzingen naar wetsteksten of andere regels en richtlijnen die op wetten.overheid.nl te vinden zijn.

Ten opzichte van 2018 is HTTPS/HSTS van gepland naar ja gegaan. Implementatie van NEN-ISO/IEC 27001/27002 en PDF is van deels naar ja gegaan. STARTTLS/DANE is nieuw opgenomen.

Concluderend moeten voor P-direkt nog de volgende standaarden (volledig) worden geïmplementeerd: DNSSEC, IPv6, Ades Baseline Profiles, ODF en STARTTLS/DANE.

5. Dienstverlening en verbinden

5.1 eFactureren

Beheerorganisatie: Logius

Werking en inhoud van eFactureren
Voor de uitwisseling van digitale bestanden sluiten verzenders en ontvangers van de facturen aan op een centrale infrastructuur. Bedrijven leveren hun facturen voor de overheid elektronisch aan bij Digipoort. Digipoort controleert of de e-factuur betrouwbaar, leesbaar en verwerkbaar is. Dit overlapt buiten Digikoppeling verder volledig met de andere onderdelen van Digipoort (Digipoort wordt gebruikt als e-factuur postbode richting de overheid). En zorgt dat de e-factuur snel bij de juiste overheidsorganisatie terechtkomt. Alle Rijksdiensten kunnen conform het MR-besluit 'Digipoort voor e-facturen', facturen ontvangen, verwerken en betalen. Naast Rijksdiensten zijn er nog meer overheden aangesloten.

Standaard	Status	Toelichting beheerder
		E-facturatie en administratie
NLCIUS (Elektronisch factureren)	Nee	De SMEF 2.0 standaard was nog niet geïmplementeerd maar wordt opgevolgd door de NLCIUS. Per 19 april 2019 is de NLCIUS verplicht voor overheden, volgens Europese richtlijn 2014/55. Implementatie van NLCIUS stond gepland voor Q2 2019. Implementatie staat niet meer concreet gepland. De verwachting is dat implementatie Q2 2020 gereed is.

Ten opzichte van 2018 is de implementatiedatum van de standaard NLCIUS verplaatst van Q2 2019 naar Q2 2020 (naar verwachting).

Concluderend moet voor de voorziening eFactureren nog de volgende standaard (volledig) worden geïmplementeerd: NLCIUS.

5.2 SBR

Beheerorganisatie: Logius

Werking en inhoud van SBR
Standard Business Reporting (SBR) is de nationale standaard voor digitale uitwisseling van bedrijfsmatige rapportages. SBR wordt gebruikt voor het samenstellen, uitwisselen en verwerken van (financiële) rapportages in de publieke en private sector. Als basis voor het versturen van SBR-berichten wordt de internationale standaard XBRL gebruikt. In de afgelopen jaren zijn belangrijke vorderingen geboekt en is een breed draagvlak gecreëerd voor SBR als rapportagestandaard voor gestructureerd digitaal gegevensverkeer. SBR is daarmee een (grootschalig) werkende oplossing en “proven technology”. Binnen het (semi)overheidsdomein wordt gebruik gemaakt van SBR bij de Belastingdienst, de Kamer van

Koophandel (KvK), het Centraal Bureau voor de Statistiek (CBS) en de Dienst Uitvoering Onderwijs (DUO)[15]. De voorziening voor de e-dienstverlening is Digipoort. SBR heeft een eigen website.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/ phishing)	Nee	De website van SBR (http://www.sbr-nl.nl) heeft ook een mailserver die niet voldoet aan DKIM. Zie: https://internet.nl/mail/sbr-nl.nl/249059/De website is overgezet naar het Ministerie van AZ.
DMARC (Anti-phishing)	Nee	SBR voldoet niet aan DMARC. Dit stond gepland voor Q1 2019 en nieuwe planning volgt in Q4 2019.
DNSSEC (Beveiligde domeinnamen)	Ja	De website van SBR (http://www.sbr-nl.nl) Voldoet zowel op het web als het maildomein aan DNSSEC.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening voldoet aan HTTPS en HSTS. Zie: https://internet.nl/site/sbr-nl.nl/563965/
IPv4 en IPv6 (Internetnummers)	Deels	De website van SBR wordt bij een derde partij gehost en is bereikbaar met IPv6. Er zijn mailservers die niet voldoen aan IPv6. IPv6 kan niet worden aangeboden, omdat de infrastructuur van Logius dit nog niet voldoende ondersteunt. Dit is een Logius breed vraagstuk. De vraag hoe IPv6 geïmplementeerd dient te worden is wederom bij onze architecten ingediend.
SPF (Preventie van mailspoofing/phishing)	Ja	De website van SBR (http://www.sbr-nl.nl) heeft ook een mailserver. Deze voldoet aan SPF (zie: https://internet.nl/mail/sbr-nl.nl/).
STARTTLS/ DANE (Beveiligd, versleuteld mailverkeer)	Nee	Aan STARTTLS en DANE wordt nog niet voldaan. Dit stond gepland voor Q1 2019 en nieuwe planning volgt in Q4 2019.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De verbinding alleen mogelijk voor voldoende veilige TLS-versies (zie: https://internet.nl/site/www.sbr-nl.nl/#). In geval van Digipoort geldt voor de markt bij koppelvlak WUS en ebMS dat TLS 1.2 de standaard is. TLS 1.0 (en mogelijk ook 1.1) is uitgefaseerd. SSL v3 en v3.1 zijn in 2015 uitgefaseerd. Het koppelvlak Grote Berichten 3.0 worden op TLS 1.0 en TLS 1.1 aangeboden. TLS 1.0 en TLS 1.1 worden nog uitgefaseerd.

[15] Naast deze (semi)overheidsinstellingen wordt nog een categorie gebruikers onderscheiden: een drietal grootbanken, specifiek gericht op het digitaliseren van de processen rond aanvragen en het beheer van zakelijke kredieten. Deze banken zijn naar verluidt klaar voor het ontvangen van kredietrapportages via SBR.

		Document en (web/app)content
Ades Baseline Profiles (Digitaal ondertekenen van documenten)	Ja	Binnen SBR (Assurance) waarbij bijvoorbeeld jaarverslagen worden ondertekend door een accountant, wordt binnen DigiPoort gebruik gemaakt van XAdES als EU standaard.
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/archivering)	Ja	Bij het publiceren van documenten houdt Logius voor SBR PDF/A aan bij publicatie.
		E-facturatie en administratie
XBRL (Bedrijfs-rapportages)	Ja	SBR maakt gebruik van XBRL.

Ten opzichte van 2018 is de status van DKIM, DMARC en STARTTLS/DANEvan gepland naar nee gegaan. De status van IPv4 en IPv6 ging van ja naar deels. De voorziening voldoet aan HTTPS en HSTS. Deze standaard is nieuw opgenomen.

Concluderend moet SBR de volgende standaarden nog (volledig) implementeren: DKIM, DMARC, IPv4 en IPv6, STARTTLS/DANE.

5.3 Digipoort

Beheerorganisatie: Logius

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

Omdat Digipoort slechts machine-naar-machine koppelingen levert en niet toegankelijk is vanaf het openbare internet, is deze voorziening niet getoetst met de toetsen van internet.nl.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	Digipoort maakt gebruik van de e-mailserver uit de centrale voorziening EASI. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. DKIM is geïmplementeerd op de centrale voorziening mail relay.
DMARC (Anti-phishing)	Gepland	Planning voor de implementatie van DMARC was Q1 2019, als onderdeel van een Logius breed project voor Domein verhuizing. Deze planning is niet gehaald, nu is deze wijziging ingepland voor Q3 2019.
DNSSEC	Gepland	Implementatie van DNSSEC zou plaatsvinden in Q1 2019 en is nu deels aanwezig en wordt deels ingepland voor Q3 2019.

(Beveiligde domeinnamen)		
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening voldoet aan HTTPS. Formeel wordt niet aan HSTS voldaan, maar de standaard HTTP (poort 80) is bij de voorziening helemaal niet ontsloten, zodat feitelijk alleen via HTTPS een verbinding gemaakt kan worden. In de geest voldoet de voorziening dus impliciet wel aan HSTS.
IPv4 en IPV6 (Internetnummers)	Nee	Digipoort gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik niet. IPv6 kan niet worden aangeboden, omdat de infrastructuur van Logius dit nog niet voldoende ondersteund. Dit is een Logius breed vraagstuk. De vraag hoe IPv6 geïmplementeerd dient te worden is wederom bij onze architecten ingediend. Digipoort ondersteunt IPv4. Implementatie van IPv6 stond gepland voor Q1 2019 maar dient opnieuw te worden ingepland.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	DigiPoort voldoet aan de BIR. Leveranciers voldoen aan ISO 27001 of een vergelijkbare standaard.
SPF (Preventie van mailspoofing/phishing)	Gepland	DigiPoort heeft geen SPF-records. Er wordt niet gemaild vanuit dit domein, maar SPF zou wel ingericht moeten worden. De planning van Q1 2019 is niet gehaald en de standaard wordt ingericht in Q3/Q4 2019.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Digipoort ondersteunt TLS v1.2, maar niet meer de verouderde versies.
		Stelselstandaarden
Digikoppeling (Veilige berichten-uitwisselingen)	Ja	Digipoort voldoet aan deze standaard. Zie de koppelvlakspecificaties op http://www.logius.nl/producten/gegevensuitwisseling/digitpoort/koppelvlakken.
		E-facturatie en administratie
SETU (Informatie flexibele arbeidskrachten)	Ja	DigiPoort ondersteunt de uitwisseling van SETU-hr-XML berichten.
XBRL en Dimensions (Bedrijfsrapportages)	Ja	De standaard wordt ondersteund door Digipoort.

De situatie ten opzichte van 2018 is gewijzigd, vanwege een belangrijke migratie is er sprake van een ‘Freeze’ periode geweest. Hierdoor zijn de noodzakelijke wijzigingen na deze migratie opnieuw gepland en delen hiervan recent opgeleverd dit betreft DMARC, DNSSEC en SPF. Wijzigingen worden momenteel op de verschillende domeinen uitgevoerd. Verder ging IPv4 en IPV6 ging van gepland naar nee.

Concluderend moeten voor de voorziening Digipoort nog de volgende standaarden (volledig) worden geïmplementeerd: DMARC, DNSSEC, IPv4 en IPV6, SPF.

5.4 Diginetwerk

Beheerorganisatie: Logius

Werking en inhoud van Diginetwerk
Diginetwerk is een afsprakenstelsel en bestaat uit een beschreven samenwerking, normenkaders, handhavingsmechanismen, toetredingseisen en een set van standaarden. Diginetwerk is opgebouwd uit een aantal aan elkaar gekoppelde besloten overheidsnetwerken, waarover overheden gegevens veiliger (vertrouwelijkheid en beschikbaarheid) met andere overheden kunnen uitwisselen dan via het internet. Een belangrijk onderdeel van Diginetwerk is de Koppelnet Publieke Sector (KPS) voorziening, welke de fysieke koppeling tussen de diverse deelnemers verzorgt.

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

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DNSSEC (Beveiligde domeinnamen)	Gepland	DNSSEC valt voor het besloten netwerk buiten het afsprakenstelsel. Een aantal deelnemers maakt echter gebruik van de diginetwerk domeinnamen om ook op het openbare internet hun dienst ter beschikking te stellen. Hiervoor is besloten wel gebruik te maken van DNSSEC. Gepland voor 2020.
IPv4 en IPV6 (Internetnummers)	Gepland	IPv4 is geïmplementeerd door de deelnemers aan Diginetwerk. De implementatie van IPv6 stond gepland voor Q4 2018 en wordt 2020. Vanwege aanbesteding KPS (koppelpunt van Diginetwerk) is ondersteuning van IPv6 gepland als onderdeel van de migratie naar de nieuwe KPS leverancier.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Deze standaard is onderdeel van het algemene beveiligingsbeleid van Logius. Logius voldoet aan deze standaard en Diginetwerk is ook gebaseerd op deze standaard.

Ten opzichte van 2018 is de standaard DMARC afgevoerd i.v.m. relevantie. Diginetwerkdomein gebruik op internet voldeed in 2018 aan DNSSEC, maar voldoet in 2019 niet aan DNSSEC. De dns leverancier is verzocht dit verder te onderzoeken en op te lossen. Gepland voor 2020. De planning van IPv4 en IPv6 is verschoven.

Concluderend, moeten voor het besloten Diginetwerk nog de volgende standaarden (volledig) worden geïmplementeerd: IPv6. Voor het gebruik van diginetwerk domeinnamen op internet moeten de volgende standaarden (volledig) worden geïmplementeerd: DNSSEC.

5.5 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)	Nee	Tenderned voldoet niet aan DMARC.
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, maar niet met HSTS (zie: https://internet.nl/site/www.tenderned.nl/).
IPv4 en IPV6 (Internetnummers)	Nee	Tenderned.nl is zowel in 2018 als in 2019 niet voorbereid op IPv6 (zie: https://internet.nl/site/www.tenderned.nl/). TenderNed is afhankelijk van de hostingpartij. Wanneer deze een transitie door maakt naar IPv6 zal TenderNed daarin mee gaan.
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. (Bron: http://www.tenderned.nl/eherkenning-en-tenderned-0)
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	Ja	STARTTLS en DANE worden ondersteund.

(Beveiligd, versleuteld mailverkeer)		
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 vorig jaar voldoet Tenderned aan DKIM en STARTTLS/DANE. De statussen zijn gegaan van nee naar ja. Verder voldoet de voorziening niet meer aan HSTS waardoor de status van de standaard HTTPS/HSTS van ja naar nee gaat.

Concluderend moeten voor Tenderned nog de volgende standaarden (volledig) worden geïmplementeerd: DMARC, HTTPS en HSTS, IPv4 en IPV6, Open API Specification.

5.6 DWR

Beheerorganisatie: Ministerie BZK

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	De implementatie van DKIM is voor SSC-ICT zelf geheel afgerond.
DMARC (Anti-phishing)	Nee	De technische implementatie van DMARC is afgerond. Het doorvoeren van de DMARC *reject policy* moet nog worden uitgevoerd, maar dit kan nog niet voor (een aantal) externe applicaties die mailen of klanten die gebruik maken van externe mailingdiensten. Open staat derhalve nog het

		aanbieden van een dienst hiervoor. SSC-ICT is voor realisatie van deze dienst afhankelijk van de betreffende klanten. De inrichting van deze dienst wordt projectmatig opgepakt; dit project bevindt zich op dit moment in de initiatiefase.
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC is geïmplementeerd en alle domeinnamen die bij SSC-ICT gehost worden voldoen aan DNSSEC.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Gepland	HTTPS wordt gebruikt, maar HSTS wordt nog niet standaard aangezet voor websites die SSC-ICT host voor klanten. Andere webgebaseerde voorzieningen maken wel gebruik van HSTS. Implementatie van deze standaarden is voor eind 2019 voorzien.
IPv4 en IPV6 (Internetnummers)	Gepland	IPv4 is in gebruik. De gebruikte technische componenten van DWR ondersteunen wel IPv6. IPv6 is een onderdeel van de infrastructuur en IPv6 reeksen worden uitgedeeld door Logius. De internet facing kant van de DMZ gaat IPv6 eind 2019 ondersteunen.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	SSC-ICT werkt via deze standaard en wordt hier ook op geaudit. De laatste audit heeft plaatsgevonden in 2019.
SAML (Inloggegevens)	Ja	Single Sign-on (SSO) op basis van SAML 2.0 wordt aangeboden als dienst in de Servicecatalogus van SSC-ICT. Het SSO-koppelvlak is een generieke dienst. Het project DOorontwikkeling Single Sign-On (DOrSSOn) voorziet internet facing aanvulling van de huidige oplossing met open source componenten gebaseerd op de standaarden SAML 2.0 en OAuth 2.0 in opdracht van de CIO Rijk.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF wordt op alle domeinen toegepast.
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Ja	STARTTLS en DANE zijn geïmplementeerd.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De op de werkplek aangeboden browsers ondersteunen TLS. De internet mailvoorziening werkt met STARTTLS. Voor webservers met applicaties van klanten wordt dit toegepast voor de klanten die dit hebben aangevraagd.
WPA2 Enterprise (Toegang tot een WiFi-netwerk met account)	Ja	Op de wifivoorziening wordt deze standaard toegepast. Wifi wordt door SSC-ICT als voorziening geleverd in de kantoorpanden waar SSC-ICT IT-dienstverlener voor het pand is (IDV-P).
		Document en (web/app)content
ODF 1.2 (Documentbewerkingen)	Ja	De DWR Next client wordt geleverd met zowel Libreoffice als Office 2016. Beide softwaresuites ondersteunen het lezen en schrijven van ODF-bestanden.
PDF 1.7 / PDF A/1 en PDF A/2 (Documentpublicatie/ archivering)	Ja	De DWR Next client kan alle types PDF lezen. Schrijven van PDF kan op meerdere manieren. Alle types worden ondersteund, al is daarvoor soms wel het installeren van Adobe Acrobat Professional benodigd. PDF A/2 is mogelijk

		voor klanten die Adobe Acrobat Pro afnemen. De regulier verstrekte Adobe Acrobat Standard ondersteunt PDF A/2 niet, maar wel PDF 1.7 en PDF A/1. De scanfunctionaliteit in het reguliere multifunctional printplatform voor de werkomgeving ondersteunt PDF 1.7 en PDF A/1.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Binnen JenV vindt elektronisch berichtenverkeer interdepartementaal plaats via de Justitie Berichten Service (JUBES). JUBES is vanuit JenV het koppelvlak voor de Digikoppelingdienst van Logius. De open standaarden eBMS en WUS zijn de daarbij gebruikte protocollen om de berichten veilig te versturen. Binnen BZ wordt deze standaard gebruikt voor de Mule koppeling. Verder nemen alle departementen uit het verzorgingsgebied van SSC-ICT deel aan eFacturatie. Op deze standaard wordt waar van toepassing aangesloten bij nieuwe koppelingen.

Ten opzichte van 2018 is de status van DMARC van deels naar nee gegaan en is de status van DKIM, DNSSEC en Digikoppeling 2.0 van deels naar ja gegaan. Verder is de status van STARTTLS/DANE van gepland naar ja gegaan. De planning van HTTPS/HSTS en IPv4 en IPv6 is verschoven.

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

5.7 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 Leverancierssportaal voor Leveranciers van de Rijksoverheid. Hiermee kunnen deze leverancier 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/).
DMARC (Anti-phishing)	Ja	De standaard DMARC is geïmplementeerd (zie: https://internet.nl/mail/digiinkoop.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	DigiInkoop voldoet aan DNSSEC (zie: https://internet.nl/mail/digiinkoop.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening voldoet aan HTTPS/HSTS. Zie https://internet.nl/site/digiinkoop.nl/)
IPv4 en IPV6 (Internet-nummers)	Nee	IPv6 werd in 2016, 2017 en 2018 niet ondersteund door de hoster van DigiInkoop. Er zijn geen plannen dit te realiseren, en er is geen opdracht om dit aan te passen. (zie: https://internet.nl/mail/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/).
		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)	Nee	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 stond gepland voor Q2 2019. Er is gekozen voor een tijdelijke tussenoplossing om aan de Europese richtlijn te voldoen, er zijn geen concrete plannen voor implementatie, de verwachting is dat het Q2 2020 gereed is.
SETU (Informatie flexibele arbeidskrachten)	Ja	DigiInkoop ondersteunt de uitwisseling van SETU-hr-XML berichten.

Ten opzichte van 2018 zijn de DKIM, DMARC en SPF standaard geïmplementeerd, de status is van gepland naar ja gegaan. De status van de standaard NLCIUS is van gepland naar de status nee gegaan.

Concluderend, moet DigiInkoop nog de volgende standaarden (volledig) implementeren: IPv4 en IPV6 , NLCIUS.

Bijlage A Geïnterviewde personen

Naam voorziening	Contactpersoon
BAG, WOZ, BGT, BRK	Koen Huisstede
Berichtenbox voor bedrijven	Dick Bruinsma, Laura Ouwehand
BRI	Henk Heerink, Harry Roumen
BRO	Erik van der Zee, Marjan Bevelander
BRT	Koen Huisstede
BRV	Gert Stel, Walter Huberts
BSN en GBA-V	Bob te Riele, Hans van laar
DigiInkoop	Güldeniz Özdemir Isik, Erwin Kaats
DigiD	Evert-Jan van der Marck
DigiD Machtigen	Güldeniz Özdemir Isik, Erwin Kaats
Digilevering	Güldeniz Özdemir Isik, Erwin Kaats
Digimelding	Güldeniz Özdemir Isik, Erwin Kaats
Diginetwerk	Glenn Lutke Schipholt
DigiPoort	Güldeniz Özdemir Isik, Erwin Kaats
Doc-Direkt	Ali Amin Shahidi
DWR	Rein Hennen, Cees Vaes, Paul Slats, Jan Pothof
eFactureren	Güldeniz Özdemir Isik, Erwin Kaats
Stelsel elektronische toegangsdiensten	Güldeniz Özdemir Isik, Erwin Kaats
MijnOverheid	Güldeniz Özdemir Isik, Erwin Kaats
NHR	Rob Spoelstra
ODC Noord	Jaap Jansma
Ondernemersplein	Elie Mokheiber
Overheid.nl	Lucien de Moor, Hans Overbeek
P-Direkt	Richard Schop, Eric van der Ende
PKI Overheid	Güldeniz Özdemir Isik, Erwin Kaats
Rijksoverheid.nl	Cees den Heijer, Gerrit Berkouwer, Cees Vaes
Rijkspas	Jacqueline Vlietland
Rijksportaal	Marvin Kramer, Marc van Hilvoorde
Samenwerkende Catalogi	Güldeniz Özdemir Isik, Erwin Kaats
SBR	Güldeniz Özdemir Isik, Erwin Kaats
Stelselcatalogus	Gerben Stevens
Tenderned	Rudi van Eijk

Bijlage B Lijst verplichte open standaarden

Standaard
Ades Baseline Profiles
Aquo-standaard
BWB
CMIS
COINS
Digikoppeling
DKIM
DMARC
DNSSEC
E-Portfolio NL
ECLI
EML_NL
Geo-Standaarden
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)
SAML
SETU
SIKB0101
SIKB0102
SKOS
SPF
STARTTLS en DANE
STIX en TAXII
StUF
TLS
VISI
WDO Datamodel
WPA2 Enterprise
XBRL