Rapport

Monitor Open standaarden 2022

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

Van Jaap Korpel

Versie Versie 1.0

Datum 18-11-2022

Inhoudsopgave

Managementsamenvatting Monitor Open standaarden 2022

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

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

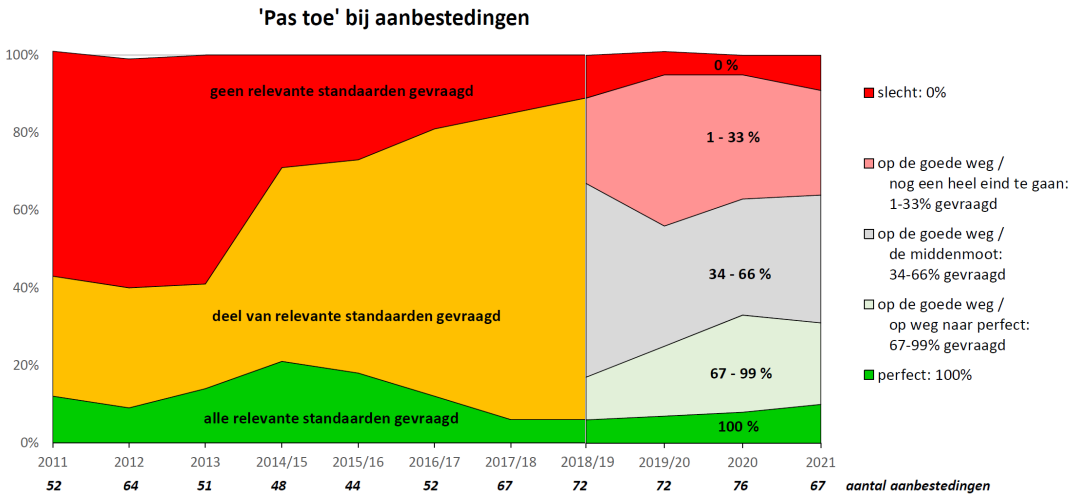
- onderzoek van aanbestedingen (in januari t/m december 2021): is daarbij om de relevante open standaarden gevraagd, en indien niet: is dat in het jaarverslag correct uitgelegd?; het glas is halfvol: om 53% van de relevante standaarden is gevraagd; dat percentage neemt langzaam toe en is de helft van een groeiend aantal standaarden; maar in dit tempo duurt het nog tot 2034 voordat – wat kabinetsbeleid is – in alle gevallen om de relevante open standaarden wordt gevraagd (zie hoofdstuk 3);
- onderzoek van de toepassing van open standaarden bij voorzieningen (zomer van 2022); die is inmiddels op een heel redelijk niveau: door de dit jaar onderzochte voorzieningen wordt aan 92% van de standaarden voldaan, of deels voldaan, of daar wordt binnenkort aan voldaan (zie hoofdstuk 4);
- onderzoek naar gebruiksgegevens van een aantal open standaarden (zomer 2022); voor veel standaarden zijn geen harde gegevens beschikbaar, de meeste standaarden waarover wèl cijfers bekend zijn worden door veel overheden gebruikt (zie hoofdstuk 5).

Voor de (semi-)publieke sector geldt sinds 2009 een 'pas toe of leg uit'-regime. Het open standaardenbeleid vergroot de interoperabiliteit en de leveranciersonafhankelijkheid van de publieke organisaties. Het maakt een kwalitatief hoogwaardige, kostenefficiënte en veilige informatie-uitwisseling mogelijk. En de open standaarden zijn een voorwaarde voor het realiseren van een veilige, inclusieve en kansrijke digitale samenleving.

Aanbestedingen

Met ingang van deze monitor worden steeds aanbestedingen per kalenderjaar onderzocht. Dat waren er dit keer 67 in totaal, waarvan 32 van Rijksoverheid en 35 van mede-overheden.

'Pas toe' bij aanbestedingen, 2011 – 2021

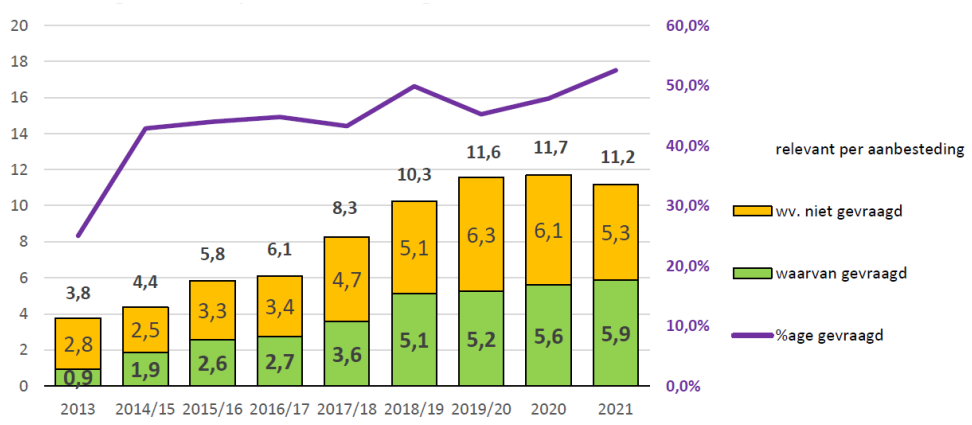


Bij deze 67 aanbestedingen was 750 keer een standaard relevant, en 394 keer is daar ook om gevraagd: dat is 53 % (was vorig jaar 48 %). Bij 10% van de 67 onderzochte aanbestedingen

uit 2021 is gevraagd om alle relevante open standaarden. Aanbestedingen waarbij om een deel van de open standaarden is gevraagd – de grote middencategorie – is iets kleiner dan vorig jaar: 81% (was 87%). Het aandeel aanbestedingen waarbij niet om een open standaard is gevraagd, is iets gestegen van 5% naar 9%.

Het gemiddelde aantal relevante standaarden per aanbesteding is inmiddels 11,2 per aanbesteding (bijna 3 keer zoveel als in 2013). Dit jaar werd zoals gezegd om 53% daarvan gevraagd, dat percentage fluctueert maar neemt geleidelijk toe. Het is bovendien een stijgend percentage van een toenemend aantal. Echter: extrapolatie van de laatste drie monitors laat zien, dat het in dit tempo nog tot 2034 zal duren voordat in alle gevallen om relevante standaarden wordt gevraagd.

Aantal relevante standaarden, gemiddeld per aanbesteding

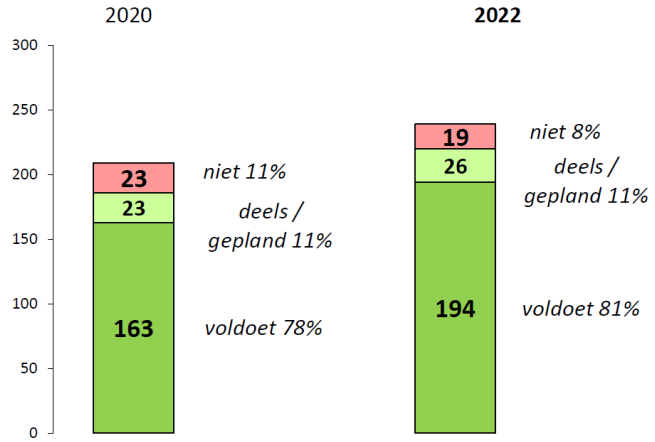


Voorzieningen

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

Figuur 8: Dit jaar onderzocht: 17 voorzieningen

Relevant voor communicatie en gegevensuitwisseling met burgers en bedrijven



Dit jaar bleek in totaal 239 keer een standaard relevant voor een voorziening (gemiddeld 14,1 keer per voorziening). De dit jaar onderzochte 17 voorzieningen blijken voor een groot deel te voldoen aan de voor hen relevante open standaarden. In 81% van de gevallen

voldoet de voorziening daaraan, en 11% voldoet de voorziening er deels aan of heeft concrete plannen daarvoor. In 8% van de gevallen voldoet een voorziening niet aan een relevante standaard (19 gevallen).

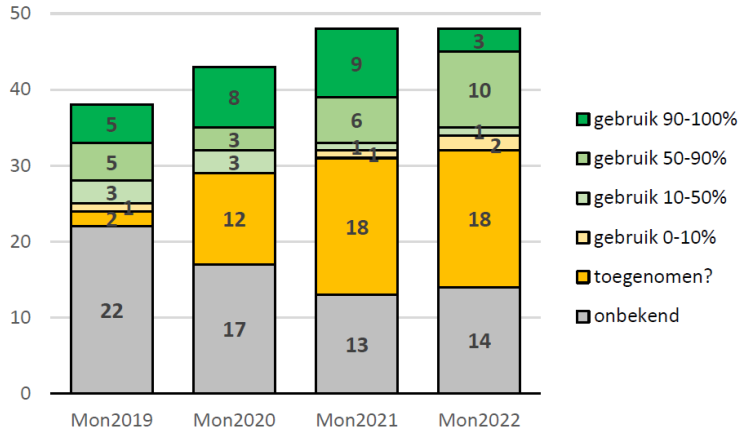
Vooral de vijftien standaarden uit het domein Internet & beveiliging waren vaak relevant voor een voorziening (samen goed voor 73 %), gevolgd door de zes standaarden uit het domein Document & (web)content (14 %) en de REST API's (6 %).

Gebruiksgegevens

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

Over de meeste standaarden uit het domein Internet & beveiliging en over enkele andere standaarden zijn wèl cijfers beschikbaar. Deze worden door redelijk veel overheden gebruikt: voor 3 standaarden is het gebruik meer dan 90% en voor 10 standaarden is het 50 tot 90%. Daarnaast is voor 18 standaarden waarover geen harde gegevens beschikbaar zijn, wel de indruk dat het gebruik toeneemt.

Gebruiksgegevens over open standaarden (aantallen)



1. Bevindingen van de Monitor Open standaarden 2022 – in het kort

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

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

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

Open standaarden voor 'pas toe of leg uit'

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

Voor een aantal open standaarden is een extra stimulans wenselijk, maar werd een wettelijke verplichting een brug te ver geacht. Het gaat daarbij om open standaarden die sterk bijdragen aan de interoperabiliteit en de leveranciersonafhankelijkheid voor de publieke sector en waarvoor breed draagvlak bestaat, maar die op dit moment nog niet breed geadopteerd zijn. Deze worden, na een zorgvuldige en open toetsingsprocedure, door het Forum Standaardisatie op de lijst voor 'pas toe of leg uit' geplaatst. Op deze open standaarden (medio 2022 waren dit er 44) is het 'pas toe of leg uit'-regime van toepassing. Meer informatie over de beleidscontext en het juridisch kader staat in hoofdstuk 2.

1.2. Over de Monitor Open standaarden 2022 (zie H2)

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

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

- onderzoek van aanbestedingen in de periode januari t/m december 2021,
- onderzoek van de toepassing van open standaarden bij overheidsbrede voorzieningen (situatie in de zomer van 2022),
- onderzoek naar gebruiksgegevens van een aantal open standaarden (zomer 2022).

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

1.3. Open standaarden bij aanbestedingen (zie H3)

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

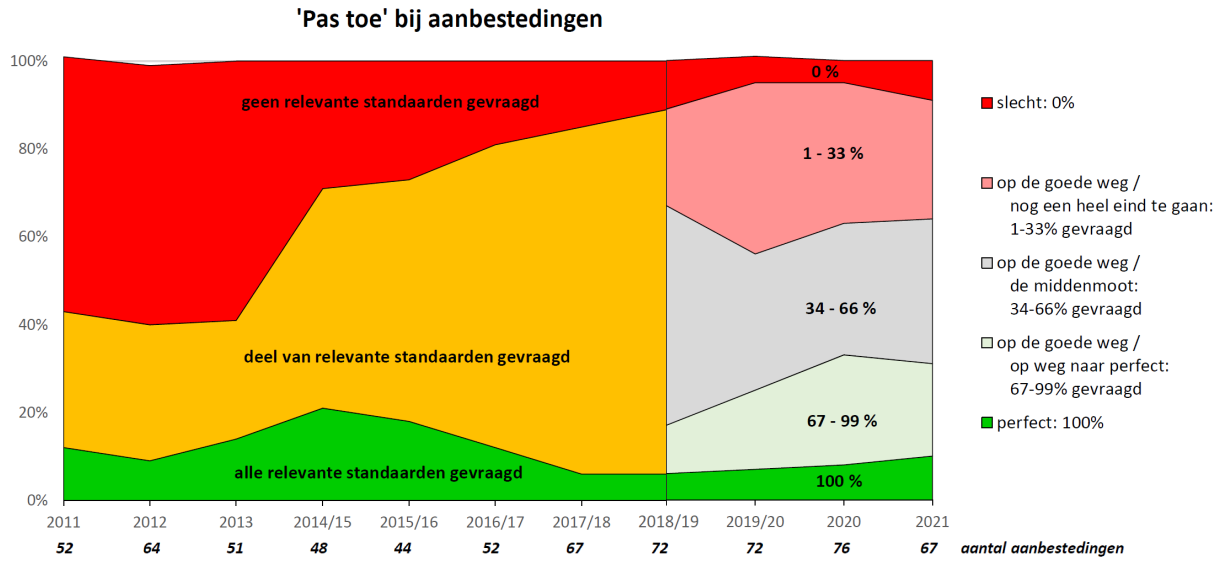
'Pas toe' bij aanbestedingen

We gaan er van uit, dat expliciet vragen om een standaard een voorwaarde is om te kunnen kiezen voor een dienst of product dat aan die standaard voldoet. Voor de monitor wordt daarom jaarlijks een groot aantal aanbestedingen hierop onderzocht. Dit jaar zijn 32 aanbestedingen van de rijksoverheid en uitvoeringsorganisaties en 35 aanbestedingen van mede-overheden onderzocht, in totaal 67 aanbestedingen. De resultaten worden beschreven in hoofdstuk 3.

Bij 10% van de 67 onderzochte aanbestedingen uit 2021 is gevraagd om alle relevante open standaarden (over heel 2020 was het 8%). Het percentage aanbestedingen waarbij om een deel van de open standaarden is gevraagd – de grote middencategorie – is iets kleiner dan vorig jaar: 81% (was 87%). Het percentage aanbestedingen waarbij niet om een open standaard is gevraagd, is iets gestegen van 5% naar 9%. En daar zijn net als vorig jaar geen aanbestedingen bij die strijdig zijn met het standaardenbeleid.

De mede-overheden deden het dit jaar beter dan de Rijksoverheid (vorig jaar was het beeld omgekeerd): bij 37% van de aanbestedingen vroegen mede-overheden om alle relevante standaarden of om tenminste tweederde daarvan (Rijksoverheid: 25%). De mede-overheden vroegen bij 40% van de aanbestedingen om geen enkele of om minder dan een derde van de relevante standaarden (Rijksoverheid: 32%).

'Pas toe' bij aanbestedingen, 2011 – 2021

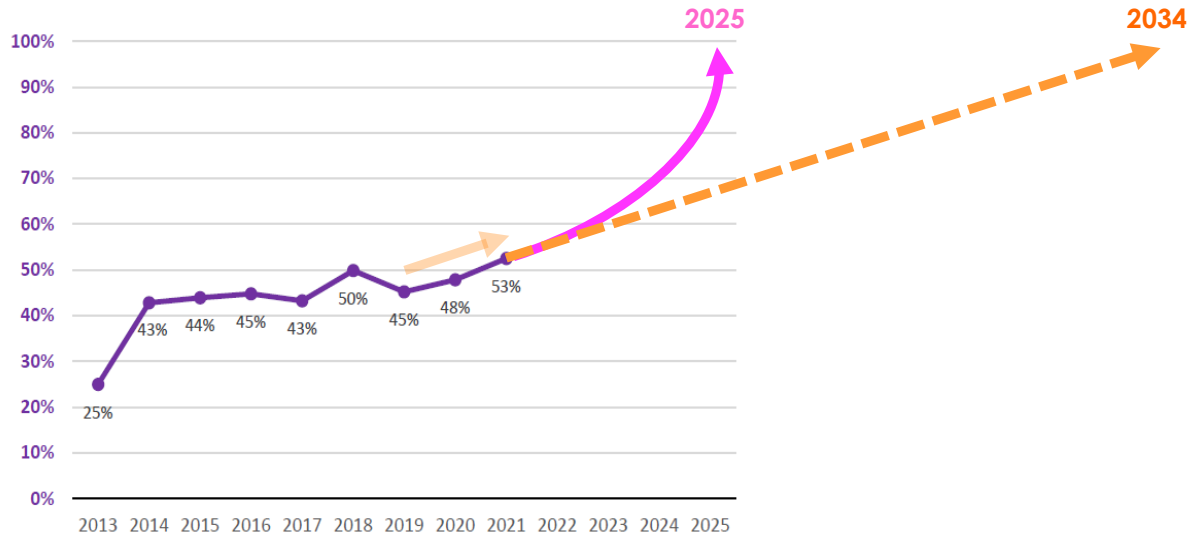


Het overall beeld voor aanbestedingen is positief, maar we zijn pas halverwege: veruit de meeste aanbestedingen (81%) vallen in de middengroep (niet heel goed, niet slecht). En van

alle keren dat een open standaard voor een aanbesteding relevant was, werd daar in 53% van de gevallen om gevraagd.

Ruim 12 jaar nadat de *Instructie Rijksdienst bij aanschaf ICT-diensten of ICT-producten* van kracht werd zijn Rijk en mede-overheden halverwege: ongeveer in de helft van de gevallen wordt – wat kabinetsbeleid is – gevraagd om de relevante open standaarden van de lijst. Deze standaarden zijn inmiddels alleen maar belangrijker geworden, en ook voor het kabinetsbeleid voor een veilige, inclusieve en kansrijke digitale samenleving zijn deze open standaarden een voorwaarde. Maar dan moeten overheden wel in 100% van de gevallen voldoen aan de relevante standaarden, en niet in 50%. Wanneer wordt die 100% bereikt? Extrapolatie van de ontwikkeling van 2019 tot 2021 leert, dat het in dit tempo nog tot 2034 zou duren voordat de 100% bereikt wordt. Om in 2025 op 100% te zitten is dus een flinke versnelling nodig, zie ook onderstaande figuur.

Extrapolatie van 'Pas toe' bij aanbestedingen: wanneer wordt 100% bereikt?



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

goed nieuws	Bij 7 aanbestedingen (10%, vorig jaar 8%) is om alle relevante standaarden gevraagd. Het gaat om aanbestedingen van de Sociale Verzekeringsbank, Kamer van Koophandel, Tweede Kamer der Staten Generaal, en de gemeenten Gorinchem, Etten-Leur, Heerde en Heerhugowaard.
goed nieuws	Daarnaast werd bij 54 aanbestedingen (81%) om een deel van de relevante open standaarden gevraagd. Dat is iets minder dan voor het jaar 2020 (toen: 87%).
minder goed	Bij 6 van de 67 aanbestedingen (9%, bijna twee keer zoveel als vorig jaar: 5%) is om geen enkele relevante standaard gevraagd.
goed nieuws	Dit jaar waren er geen aanbestedingen strijdig met het open standaardenbeleid.
goed nieuws	Van de 750 keer dat een open standaard voor een aanbesteding relevant was werd daar in 53 % van de gevallen door de aanbesteder om gevraagd. Vorig jaar lag dit percentage nog op 48%, en er tekent zich een heel geleidelijk stijgende trend af.
minder goed	Extrapolatie van de laatste drie monitors laat echter zien, dat het in dit tempo nog zal duren tot 2034 voordat in alle gevallen om relevante standaarden wordt gevraagd.

goed nieuws	Het gemiddeld aantal relevante standaarden per aanbesteding steeg van 4,4 (2015) tot 11,2 in 2021. Dit jaar is het gemiddelde aantal wel iets lager dan vorig jaar (11,7).
goed nieuws	Sommige standaarden (vooral NEN-ISO/IEC 27001 en 27002, IPv6 & IPv4, HTTPS & HSTS en TLS) zijn veel vaker (88% tot 97%) relevant bij een aanbesteding dan andere. NEN-ISO/IEC 27001 en 27002 worden bovendien – àls zij relevant zijn – het vaakst ook daadwerkelijk gevraagd (83%). Nog 6 andere IV-standaarden waren ook vaak relevant (78% tot 82%), maar deze werden minder vaak gevraagd.
goed nieuws	Dit jaar werden ook enkele andere standaarden, àls ze relevant waren, redelijk vaak gevraagd: StUF (92%), NLCIUS (100%, maar van 2x relevant) en Ades Baseline Profiles (100%, maar van 1x relevant).
minder goed	IPv4 & IPv6 was voor 91% van de aanbestedingen relevant, maar er werd er slechts in 30% van die gevallen om de standaard gevraagd. Terwijl in het OBDO (onder andere) voor IPv4 & IPv6 'streefbeeldafspraken' zijn gemaakt (zie par. 5.2).

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

- Gemeente Etten-Leur (containermanagement en afvalinformatie voor inwoners): voldoet aan alle 13 relevante open standaarden.
- Gemeente Gorinchem (e-HRM systeem en ondersteuning): voldoet aan alle 12 relevante open standaarden, volgens de beoordelaars een hoge kwaliteit aanbesteding.
- Gemeente Heerde (zaaksysteem): voldoet aan alle 14 relevante open standaarden.
- Gemeente Heerhugowaard (gegevensdistributie en servicebus): voldoet aan alle 14 relevante open standaarden, volgens de beoordelaars een voorbeeldige aanbesteding.
- Provincie Flevoland (financieel systeem): maar liefst 18 standaarden relevant, waarvan slechts twee niet gevraagd (Digikoppeling en Digitoegankelijk). Commentaar van beoordelaar: voorbeeldig, maar ook enkele standaarden gevraagd die niet relevant zijn.
- Ministerie van SoZaWe (subsidiesoftware, klantportaal, zaakmanagement): er zijn 16 standaarden relevant, waarvan er slechts één niet is uitgevraagd (Digikoppeling). Volgens de beoordelaar: een voorbeeld!

'Leg uit' in jaarverslagen

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

Voor de onderzochte aanbestedingen uit 2021 is nagegaan of er sprake is geweest van een geldige 'Leg uit'. Voor 60 van de 67 aanbestedingen was 'Leg uit' vereist, omdat hierbij om één of meer relevante open standaarden niet gevraagd werd.

minder goed	Van expliciete 'Leg uit' voor met name genoemde aanbestedingen was in de jaarverslagen van de betreffende overheidsorganisaties (waaronder 8 ministeries) geen sprake: nergens wordt een concrete afwijking van de 'pas toe of leg uit'-lijst genoemd, laat staan verantwoord.
minder goed	Bij 60 aanbestedingen was 'Leg uit' noodzakelijk. Bij 17% hiervan (vorig jaar: 19%) was sprake van een beperkte verantwoording: 7 van de 12 ministeries hebben een algemene alinea over 'pas toe of leg uit' opgenomen in het jaarverslag. Bij de overige 83% was geen sprake van enige vorm van 'Leg uit' (vorig jaar 81%).

Sinds enkele jaren informeren wij aanbesteders over de beoordeling van hun aanbesteding en interviewen wij bovendien enkele van hen. Dat leidt soms nog tot een (beperkte) aanpassing van de beoordeling. En, hoewel dit geen alternatief is voor 'Leg Uit', blijkt het wel in een behoefte te voorzien. De discussie is meestal wederzijds leerzaam en deze blijkt ook interessante inzichten op te leveren. In paragraaf 3.5.2 is daarom een bloemlezing uit deze discussies opgenomen.

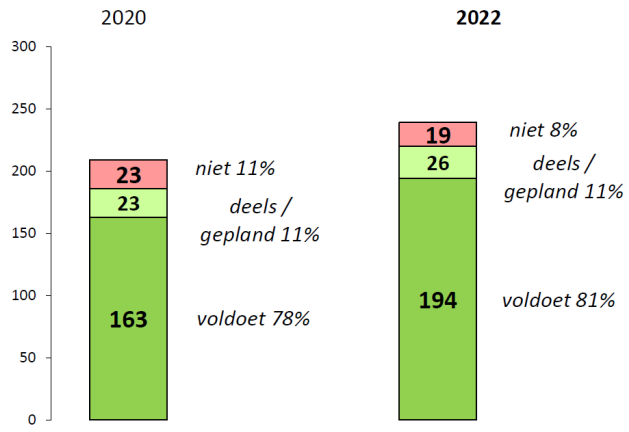
1.4. Toepassing van open standaarden via voorzieningen (zie H4)

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

Sinds 2020 onderzoeken we het ene jaar 19 voorzieningen die relevant zijn voor de gegevens-uitwisseling en de communicatie tussen overheden en de onderliggende infrastructuur. Het andere jaar (dit jaar) onderzoeken we de 17 voorzieningen die direct raken aan de communicatie en gegevensuitwisseling met burgers en bedrijven.

De dit jaar onderzochte voorzieningen blijken voor een groot deel te voldoen aan de relevante open standaarden. Er waren in totaal 239 gevallen waarbij een open standaard voor een voorziening relevant was. Het percentage 'voldoet' is toegenomen van 78% tot 81%. Het aantal gevallen waarin de voorziening deels aan de standaard voldoet of daarvoor concrete plannen heeft bleef gelijk (11%). Samen met 'voldoet' is dat dit jaar dus een stijging van 89% naar 92%.

Dit jaar onderzocht: 17 voorzieningen
Relevant voor communicatie en gegevensuitwisseling met burgers en bedrijven



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

goed nieuws	Voor veel voorzieningen is een flink aantal open standaarden relevant: voor de dit jaar onderzochte voorzieningen gemiddeld 14,1 standaarden per voorziening. Van de 44 standaarden op de lijst voor 'pas toe of leg uit' zijn er 27 relevant voor één of meer van de dit jaar onderzochte voorzieningen.

goed nieuws	Voor 18 van deze 27 standaarden geldt dat minstens 80% van de onderzochte voorzieningen aan die standaard – indien relevant – voldoet. Van deze standaarden vallen er 11 in het domein 'Internet & beveiliging'. De andere 7 zijn verdeeld over vier van de negen andere domeinen: Document & (web)content, E-facturatie & administratie, Stelselstandaarden en Juridische verwijzingen.
minder goed	Drie standaarden scoren relatief laag: van de voorzieningen waarvoor deze relevant zijn voldoet slechts 13% (volledig) aan Digitoegankelijk, 33% aan NLCIUS en 38% aan REST-API Design Rules.
goed nieuws	De voorzieningen voldoen aan redelijk veel standaarden: de 17 onderzochte voorzieningen voldoen aan 81% van de voor hen relevante standaarden.
minder goed	Vergeleken met twee jaar geleden is het percentage 'voldoet' licht gestegen van 78% tot 81%. Het aantal gevallen waarin de voorziening deels aan de standaard voldoet of daarvoor concrete plannen heeft bleef gelijk (11%). Samen met 'voldoet' is dat dit jaar dus 92%.
goed nieuws	Zeven voorzieningen voldoen geheel of gedeeltelijk aan alle relevante open standaarden of hebben concrete plannen om er op korte termijn aan te voldoen.

Opvallend is, dat vooral standaarden uit het domein Internet & Beveiliging vaak relevant zijn (73% van alle gevallen). De domeinen Document & Webcontent (14%) en REST API's (6%) volgen op grote afstand. De 21 standaarden uit de zes andere domeinen zijn zelden relevant (samen slechts 7%).

Verschillende voorzieningen onderscheiden zich dit jaar in positieve zin:

- Het emaildomein van Rijksoverheid.nl voldoet aan alle 9 relevante standaarden.
- Zes voorzieningen voldoen 'bijna' aan alle standaarden, aan een groot deel voldoen zij en aan de meeste andere voldoen zij deels, of hebben dat gepland: DigiD, DigiD Machtigen, PKI Overheid, Stelsel ETD, MijnOverheid en het webdomein Rijksoverheid.nl.

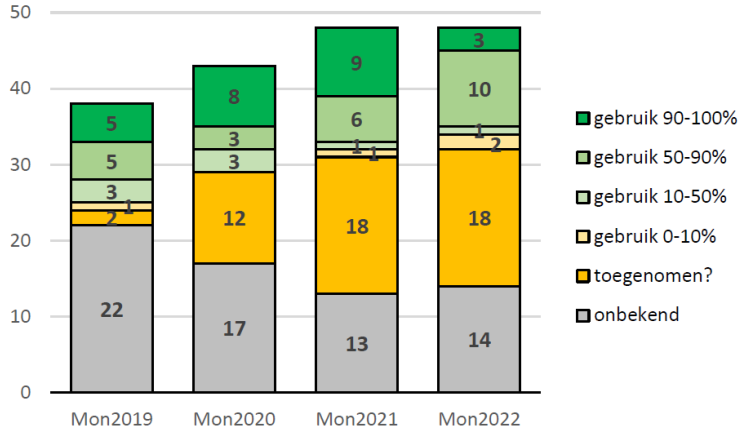
1.5. Gebruiksgegevens van een aantal open standaarden (zie H5)

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

Dergelijke gebruiksgegevens zijn niet in alle gevallen eenvoudig te verzamelen. Dat is door de accountmanagers van het Bureau Forum Standaardisatie gedaan, in de zomer van 2022, met de volgende uitkomsten:

minder goed	Over meer dan de helft van de open standaarden zijn geen gebruiksgegevens beschikbaar. Dat is in sommige gevallen begrijpelijk, maar in de andere gevallen lijken beheerorganisaties en/of initiatiefnemers daarin niet echt geïnteresseerd.
goed nieuws	Over de meeste standaarden uit het domein Internet & beveiliging zijn cijfers beschikbaar. Een deel van deze standaarden wordt veel gebruikt.
minder goed	Voor IPv4&IPv6 is het OBDO-streefbeeld, dat 100% adoptie eind 2021 bereikt moet zijn, nog niet bereikt. Het gebruik (op een andere manier gemeten dan voorheen) was voor overheidswebsites 70%, en voor overheidsemail van 50%.
goed nieuws	Op basis van soms globale cijfers en soms inschattingen van betrokkenen wordt verondersteld dat het gebruik van 18 standaarden (licht) toegenomen is.

Gebruiksgegevens over open standaarden (aantallen)



Halfjaarlijkse meting Internetveiligheidsstandaarden (zie ook Bijlage B5)

Uit de 'Meting Informatieveiligheidstandaarden overheid voorjaar 2022' blijkt dat het streefbeeld voor eind 2019 op het moment van de meting – twee jaar later – nog niet volledig was gerealiseerd. De opzet van de IV-meting is veranderd, een vergelijking met voorgaande jaren is daarom niet goed mogelijk.

1.6. De drie deel-onderzoeken naast elkaar

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

In de onderstaande tabel is dat in beeld gebracht.

- De cijfers in de kolom 'Aanbestedingen' zijn afkomstig uit Tabel 6 (hoofdstuk 3) en geven weer hoe vaak om standaard X is gevraagd, in procent van het aantal keer dat deze standaard relevant was bij een aanbesteding.
- Voor de kolom 'Voorzieningen' zijn de scores van de 17 voorzieningen die dit jaar onderzocht zijn gecombineerd met de scores van de andere 19 voorzieningen (vorig jaar onderzocht). Berekend is voor hoeveel voorzieningen standaard X relevant was en hoeveel procent daaraan voldoet, of deels voldoet of binnenkort zal voldoen.
- In de kolom 'Gebruiksgegevens' is aangegeven hoeveel procent van bijvoorbeeld alle overheidsorganisaties of van de relevante web- of email-domeinnamen voldoet aan standaard X. Soms moest worden volstaan met een kwalitatieve inschatting daarvan.
- In de rechterkolom ('Overall beeld') zijn deze drie cijfers per standaard zo goed als mogelijk samengevat tot één kwalificatie: positief, redelijk, wisselend, of matig. Een vraagteken betekent dat er onvoldoende informatie over de standaard beschikbaar is.

Het 'overall beeld' uit de drie deel-onderzoeken

Voor 11 van de 19 standaarden (incl. varianten) uit het domein Internet & beveiliging is het overall beeld positief, voor 6 standaarden is het redelijk en voor één standaard is het beeld wisselend. Voor één standaard zijn onvoldoende gegevens beschikbaar.

In het domein Document & (web)content scoren vier van de zes standaarden positief, één scoort wisselend en voor één standaard zijn onvoldoende gegevens beschikbaar.

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

Van de vier standaarden in het domein E-facturatie & administratie is het overall beeld voor twee positief, voor één is het wisselend en voor één is onvoldoende informatie beschikbaar.

In het domein Stelselstandaarden gaat het redelijk goed: voor twee standaarden is het overall beeld positief, en voor één standaard wisselend.

In het domein Water & Bodem is slechts voor één standaard voldoende informatie beschikbaar: het overall beeld daarvoor is positief.

Over de standaarden in de domeinen Bouw en Onderwijs & loopbaan is onvoldoende informatie beschikbaar.

Het overall beeld voor twee van de drie standaarden in het domein Juridische verwijzingen is redelijk. Voor de derde standaard is onvoldoende informatie beschikbaar.

De enige 'overige' standaard scoort positief.

indicator:	**Aanbestedingen** # aanbestedingen waarbij OS is gevraagd in % van # waarbij OS relevant is	**Voorzieningen** # voorzieningen dat voldoet +deels +gepland in % van relevant	**Gebruiksgegevens** # overheden dat de standaard gebruikt in % van alle overheidsorganisaties	**Overall beeld**
Internet & beveiliging:				
DKIM	31%	96%	82%	positief
DMARC	31%	97%	72%	positief
DNSSEC web	47%	97%	89%	positief
en DNSSEC email			57%	redelijk
HTTPS	59%	91%	92%	positief
en HSTS			57%	redelijk
IPv6 en IPv4 web	33%	86%	70%	redelijk
en IPv6 en IPv4 email			50%	redelijk
NEN-ISO\IEC 27001	83%	100%	[?]	positief
NEN-ISO\IEC 27002	83%	100%	[?]	positief
NL GOV Assurance	25%	15%	[?]	matig
RPKI		79%	[?]	redelijk
SAML	66%	100%	[?]	positief
SPF	31%	97%	87%	positief
STARTTLS	31%	65%	81%	positief
en DANE			46%	redelijk
STIX & TAXII	67%	100%	toegenomen	positief
TLS	59%	97%	75%	positief
WPA2 Enterprise	0%		licht toegenomen	[?]
Document & (web)content:				
Ades Baseline Profiles	100%	100%	[?]	positief
Digitoegankelijk	76%	100%	licht toegenomen	positief
ODF	27%	75%	beperkt gebruik	wisselend
OWMS		29%	[?]	[?]
PDF	68%	100%	stabiel	positief
SKOS		92%	stabiel	positief
REST API's:				
OpenAPI Specification	17%	86%	[?]	wisselend
REST_API Design Rules	17%	58%	[?]	wisselend
E-facturatie & administratie:				
NLCIUS	100%	11%	toegenomen	wisselend
SETU		100%	licht toegenomen	positief
WDO Datamodel	0%		toegenomen	[?]
XBRL	40%	100%	stabiel	positief
Stelselstandaarden:				
Digikoppeling	71%	95%	stabiel	positief
Geo-standaarden	0%	100%	toegenomen	wisselend
StUF	92%	83%	toegenomen	positief
Water & Bodem:				
Aquo Standaard		100%	stabiel	positief
GWSW			toegenomen	[?]
SIKB 0101			stabiel	[?]
SIKB 0102			toegenomen	[?]
Bouw:				
COINS			[?]	[?]
IFC			beperkt gebruik	[?]
NLCS			licht toegenomen	[?]
Visi			licht toegenomen	[?]
Juridische verwijzingen:				
BWB	50%	100%	[?]	redelijk
ECLI			[?]	[?]
JCDR		100%	[?]	redelijk
Onderwijs & loopbaan:				
E-portfolio	0%		[?]	[?]
NL LOM	0%		licht toegenomen	[?]
Overig:				
EML_NL	31%	96%	overal toegepast	positief

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

2.1. Waarom open standaarden?

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

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

Het gebruik van deze standaarden is essentieel:

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

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

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

Pas toe:

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

Leg uit:

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

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

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

2.2.1. Ministeries en uitvoeringsorganisaties: Rijksinstructie en Rijksbegrotingsvoorschriften

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

> Bij de aanschaf van een ICT-dienst of ICT-product voor een toepassingsgebied dat voorkomt op de lijst die op de website www.forumstandaardisatie.nl is gepubliceerd, wordt gekozen voor een ICT-dienst of een ICT-product dat gebruikt maakt van een bij het desbetreffende toepassingsgebied vermelde open standaard. (Art. 3, lid 1)

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

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

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

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

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

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

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

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

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

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

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

2.3. Over de Monitor Open standaarden 2022

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

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

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

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

Onderzoek van aanbestedingen in tweede helft 2021

Dit jaar zijn aanbestedingen onderzocht van de rijksoverheid (en uitvoeringsorganisaties) en van mede-overheden uit de periode januari tot en met december 2021.

Met ingang van deze monitor worden telkens de aanbestedingen van een kalenderjaar worden onderzocht (tot nu toe onderzochten wij aanbestedingen van juli voorgaande jaar tot en met juni lopende jaar). De uitkomsten worden vergeleken met de aanbestedingen uit 2020 die voor de vorige monitor zijn onderzocht (Q3+Q4) en de monitor dáárvoor (Q1+Q2).

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

Onderzoek open standaarden bij overheidsbrede voorzieningen en shared services

Dit jaar onderzoeken wij 17 voorzieningen die vooral gericht zijn op de gegevensuitwisseling en communicatie met burgers en bedrijven. Voor deze 17 voorzieningen is onderzocht in hoeverre zij voldoen aan de open standaarden die daarvoor relevant 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. Ook dit jaar zijn deze gebruiksgegevens verzameld in samenwerking met de accountmanagers van het Bureau Forum Standaardisatie.

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

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

In het kader van de Monitor Open standaarden 2022 is voor inmiddels het elfde jaar op rij onderzoek gedaan naar de toepassing van open standaarden bij aanbestedingen door overheden. Per aanbesteding is vastgesteld welke open standaarden van de lijst daarop van toepassing waren en in hoeverre daar daadwerkelijk om is gevraagd ('pas toe'). Vervolgens is nagegaan in hoeverre overheden in hun jaarverslag verantwoording hebben afgelegd, wanneer bij aanbestedingen van de lijst werd afgeweken ('leg uit').

Op het moment van rapporteren (zomer 2022) omvatte de 'pas toe of leg uit'-lijst 44 open standaarden, dezelfde standaarden als een jaar eerder. Voor dit onderzoek zijn alle 44 standaarden in beeld als het erom gaat vast te stellen of ze ook relevant zijn voor de onderzochte aanbestedingen.

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

3.1. Onderzoek van aanbestedingen

Met ingang van deze monitor zullen telkens aanbestedingen van één volledig kalenderjaar worden onderzocht. Vorig jaar is op deze nieuwe aanpak al een voorschot genomen door eenmalig alleen te kijken naar aanbestedingen uit Q3 en Q4 2020. Voorheen werden namelijk de aanbestedingen van Q3+Q4 van het voorgaande jaar en Q1+Q2 van het lopende jaar onderzocht. Dat betekent dat Q1 en Q2 2020 al waren onderzocht in de Monitor 2020. Voor deze Monitor 2022 worden derhalve aanbestedingen uit het hele kalenderjaar 2021 door het Rijk (met inbegrip van onder andere uitvoeringsorganisaties, agentschappen en ZBO's) en door de decentrale overheden onderzocht.

De resultaten van deze aanbestedingen uit 2021 worden in dit hoofdstuk gepresenteerd. Dat zijn immers de nieuw onderzochte aanbestedingen. De resultaten worden vergeleken met de opbrengst uit de vorige monitor. Ten aanzien van deze vergelijking het volgende. Normaal gesproken vindt een vergelijking plaats met de aanbestedingen die in de vorige monitor zijn onderzocht. Zoals hierboven aangegeven, waren dat in de Monitor 2021 (over 2020) alleen aanbestedingen uit Q3 en Q4 van 2020. In de vorige monitor is erop geanticipeerd om dit jaar een volwaardige vergelijking mogelijk te maken tussen de set van aanbestedingen uit volledige kalenderjaren 2020 en 2021. Daartoe zijn in de vorige monitor-rapportage de cijfers van de aanbestedingen uit Q1 en Q2 2020 (die zijn onderzocht in de Monitor 2020) toegevoegd aan de resultaten voor Q3 en Q4 2020, met als resultaat dat er ook een totaalbeeld voor het volledige kalenderjaar 2020 beschikbaar is. Dit samengevoegde overzicht over het hele kalenderjaar 2020 is in de vorige monitor verder niet geanalyseerd

maar dient nu als goede vergelijkingsbasis. Dit overzicht over het kalenderjaar 2020 is terug te vinden in bijlage B3 van de vorige monitor-rapportage.

Dit jaar is ervoor gekozen om de rolverdeling tussen de experts in vergelijking met vorig jaar om te draaien. De beoordeling van aanbestedingen is uitgevoerd door Arend-Jan Wiersma terwijl Robin de Veer en Jelte Bootsma (beiden TNO) de second opinion op de Rijks-aanbestedingen hebben geleverd. De rapportage (dit hoofdstuk) is geschreven door Joost Vreuls.

Onderzocht zijn vooral aanbestedingen die op tenderned.nl zijn gepubliceerd. Het betreft daardoor veelal Europese aanbestedingen. Drempelwaarden daarvoor waren in 2021 voor de rijksoverheid > € 139.000 en voor decentrale overheden > € 214.000. (Deze waarden worden telkens voor twee jaar door de Europese Commissie vastgesteld. Per 1 januari 2022 zijn deze drempelwaarden inmiddels opnieuw vastgesteld voor de periode van twee jaren na die datum.)

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

In principe worden elk jaar veel van de in de voorafgaande periode verzamelde relevante aanbestedingen van Rijksoverheid en uitvoeringsorganisaties beoordeeld; de speelruimte om een steekproef te trekken is beperkt. Dit jaar viel ongeveer de helft van de aanbestedingen door de Rijksoverheid buiten de steekproef. Het aantal beoordeelde aanbestedingen van de Rijksoverheid (35) ligt dit jaar op het gebruikelijke niveau voor een jaarlijkse periode. Ook dit jaar is een aantal (9) aanvankelijk geselecteerde aanbestedingen van Rijksoverheid en uitvoeringsorganisaties bij nader inzien door de experts gekwalificeerd als 'niet beoordeelbaar'. Om toch tot het streef-aantal van 35 beoordeelde aanbestedingen te komen, was de steekproef ruimer genomen. Bij de niet beoordeelbare aanbestedingen gaat het om uiteenlopende casuïstiek:

- er is in twee gevallen bij nader inzien sprake van een raamovereenkomst zonder zicht op de inhoud van onderliggende nadere overeenkomsten en daarmee buiten scope;
- drie aanbestedingen zijn naderhand alsnog ingetrokken;
- bij één aanbesteding ontbreken de documenten om tot een beoordeling te kunnen komen;
- één aanbesteding betreft de aanschaf en plaatsing van bestaande en reeds ontwikkelde hardware en software; hier is geen ruimte voor het toepassen van open standaarden;
- één niet of op zijn minst erg lastig te beoordelen aanbesteding. Het betreft wel een ICT dienst, maar het is twijfelachtig of alle standaarden betrekking hebben op het proces of de ICT dienst. Er wordt alleen gevraagd om conversie van PDF documenten naar TEI-XML;
- de laatste aanbesteding in deze opsomming had niet in de lijst terecht moeten komen. De vraag heeft weinig tot niets met IT dienstverlening te maken. Het betreft met name een financiële dienst.

Voor de medeoverheden wordt elk jaar een steekproef getrokken uit de (vele) gevonden aanbestedingen. Dit jaar zijn eveneens 35 aanbestedingen van medeoverheden beoordeeld over het jaar 2021. Nogmaals ter herinnering: met ingang van de Monitor 2018 is gekozen voor een verdubbeling van het aantal te onderzoeken aanbestedingen door medeoverheden om daar beter zicht op te krijgen.

In totaal zijn 70 aanbestedingen beoordeeld: 35 van het Rijk (departementen, uitvoerings-organisaties, agentschappen, ZBO's) en een steekproef van 35 aanbestedingen van medeoverheden. De 70 beoordeelde aanbestedingen vormen een goede afspiegeling van de overheids-ICT-aanbestedingen, voor zover die binnen de beschreven zoek-kaders vallen.

Na de beoordeling, daarbij inbegrepen de bevindingen uit de second opinion sessies voor wat betreft de aanbestedingen Rijk, zijn de resultaten in een proces van hoor en wederhoor voorgelegd aan de contactpersonen van alle beoordeelde aanbestedingen, met daarbij een expliciete uitnodiging om te reageren. Voor een drietal aanbestedingen (alle Rijks-aanbestedingen) heeft dit proces ertoe geleid dat deze aanbestedingen uiteindelijk buiten de monitor-rapportage zijn gehouden. Twee aanbestedingen bleken bij nader inzien en in een later stadium alsnog ingetrokken en bij één aanbesteding moet achteraf worden vastgesteld dat geen sprake is van een ICT-aanbesteding zoals bedoeld binnen de kaders van deze monitor. Zodoende resteren uiteindelijk 32 (van de 35) aanbestedingen Rijk als basis voor een overall-beeld.

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

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

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

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

- Met het oog op de veiligheid van haar werknemers wil de aanbestedende partij, naast het voldoen aan haar wettelijke verplichtingen, haar BHV organisatie verder

professionaliseren. Belangrijk is hierbij aandacht voor continuïteit en uniformiteit, zodat BHV-ers van verschillende locaties elkaar eenvoudig kunnen vervangen. Het betreft ook de levering en het beheer van een app.

- Deze aanbesteding betreft het vervangen van de huidige brievenboeksystemen door één gemeenschappelijke voorziening voor E-Publicatie voor de gehele organisatie die het mogelijk maakt om formele gepersonaliseerde communicatie-uitingen aan de klant (kanaalonafhankelijk) te creëren, op te maken en samen te voegen. Brievenboeksystemen zijn geautomatiseerde systemen waarmee brieven worden gemaakt en naar klanten worden gestuurd. De opdracht omvat het leveren van de voorziening E-Publicatie, implementatie van de software, en beheer en onderhoud van de software.
- Het betreft de inkoop van software en licenties voor een muziekscheduling-systeem. Dit zijn specialistische applicaties waarmee de muziekredacties van de NPO-radiozenders voor elk programma automatisch een speellijst laten samenstellen die tijdens dat programma wordt uitgezonden. Verder behoren implementatiewerkzaamheden en supportwerkzaamheden van de software binnen de scope van de aanbesteding.
- Een scanoplossing parkeerhandhaving bestaande uit de volgende onderdelen:
  - implementatie en doorontwikkeling van een scandienst binnen de parkeerketen van de gemeente;
  - het beschikbaar stellen van scanmiddelen (bestaande uit de scanoplossing en de drager (voertuig)) aan de handhavingsorganisatie;
  - het integrale beheer van de koppelingen binnen de separate onderdelen van de aangeboden scandienst en het in stand houden van de koppelvlakken met systemen van derden binnen de lokale parkeerketen;
  - het verzorgen van het communicatiesysteem middels onder andere een IT platform, waar alle scandata worden verzameld, opgeslagen en verwerkt zodat de data geanalyseerd kunnen worden ten behoeve van een meer efficiënte handhaving in de stad (inclusief het beheer en onderhoud hiervan).
- De gemeente wil het oude standskantoor omvormen naar van een nieuw HUIS van Roosendaal; een gebouw waar je op een kwalitatief goede manier kunt vergaderen, werken en elkaar kunt ontmoeten. De huidige COVID-situatie heeft e.e.a. in een versnelling gebracht. Het elkaar ontmoeten, vergaderingen, met elkaar kunnen brainstormen of kennis uitwisselen zal niet meer altijd fysiek op dezelfde plek plaatsvinden. Een hybride vorm van werken is daarmee een manier van werken geworden. Hierbij kan een deel van de mensen fysiek aanwezig zijn op kantoor en een deel online vanuit huis of elders. Daar waar het gaat om een hybride vorm van (samen) kunnen werken is een gedegen keuze van de juiste audio- en beeld technieken, als onderdeel van de AV-installaties, een zeer belangrijk aspect.

Toetsingskader

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

Het onderzoek toetst op basis van de openbare documenten in hoeverre de aanbesteding voldoet aan het 'pas toe of leg uit'-beginsel, zoals dat (voor de Rijksoverheid) is vastgelegd in de Instructie Rijksdienst. Deze verplichting geldt ook voor mede-overheden (gemeenten, provincies en waterschappen).

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

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

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

Daarnaast is onderzocht op welke wijze de verantwoording ('leg uit') over 2021 heeft plaatsgevonden (zie paragraaf 3.5). Wanneer de aanbestedende organisatie besluit om niet te vragen om één of meer open standaarden die wèl van toepassing zijn, dan moet dit worden vastgelegd in de departementale administratie en hierover moet verantwoording afgelegd worden in het jaarverslag. Afwijkingen zijn overigens alleen mogelijk bij redenen van bijzonder gewicht.

3.2. 'Pas toe' bij aanbestedingen in 2021

In de 67 aanbestedingen uit 2021 die voor deze monitor zijn beoordeeld had in totaal om 750 open standaarden gevraagd moeten worden, feitelijk is er echter 394 keer om een open standaard gevraagd. Dat is 53% daarvan (zie de groene rijen in het gestippelde kader midden in Tabel 1), en dat ligt duidelijk boven de score van vorig jaar (toen 48%, het jaar daarvoor 45% en daardoor 50%). In de vorige monitor was al sprake van een stijging en ook nu is sprake van een stijging, zelfs sterker dan vorig jaar (een plus van 5%).

Deze toename naar 53% uitgevraagd is in zijn geheel toe te schrijven aan een fors hoger uitvraag-percentage bij de aanbestedingen door mede-overheden: van 45% naar 56%. Ter vergelijking: het percentage voor de Rijks-aanbestedingen is gedaald van 51% vorig jaar naar nu 48%. Deze terugval van het uitvraag-percentage bij Rijks-aanbestedingen wordt derhalve meer dan gecompenseerd door de betere score bij de mede-overheden. Met name bij de Rijks-aanbestedingen wisselen lage en hoge uitvraagpercentages elkaar de laatste jaren af.

3.2.1. *'Pas toe' per aanbesteding*

Bij 7 van de 67 aanbestedingen (10%, zie de grijze kolommen in tabel 1; vorig jaar 8%) werd **om alle relevante open standaarden gevraagd ('perfect')**, dat is 'pas toe' in strikte zin. Dit waren 3 aanbestedingen vallend in de categorie Rijksoverheid (Kamer van Koophandel, Tweede Kamer der Staten Generaal en de Sociale Verzekeringsbank) en een viertal gemeenten: Etten Leur, Gorinchem, Heerde en Heerhugowaard.

Daarnaast werd bij 54 aanbestedingen (81%; vorig jaar 87%) gevraagd om een deel van de voor die aanbesteding relevante standaarden ('op de goede weg'). Bij de resterende aanbestedingen (9%; vorig jaar 5%) waren wel standaarden relevant, maar werd om geen enkele gevraagd en was in de aanbestedingsdocumenten in het geheel geen aandacht voor open standaardenbeleid terug te vinden ('slecht').

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

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

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

Deze nuancering leidt tot het volgende beeld:

- 21% van alle aanbestedingen is 'op weg naar perfect', 33% behoort tot de middenmoot en voor 27% geldt dat er nog een heel eind te gaan is;
- in vergelijking met de vorige monitor is het overall beeld per saldo min of meer in balans. Enerzijds is sprake van een daling bij de categorie 'op weg naar perfect': van 25% naar 21% (volledig toe te schrijven aan een terugval bij Rijk). Daar staat tegenover dat ook het aandeel achterblijvers ("nog een heel eind te gaan") is teruggelopen, van 32% naar 27%. Bij de categorie 'middenmoot' is het verschil met vorig jaar het kleinst (33% tegen 30% vorig jaar);
- inzoomend op de afzonderlijke categorieën overheid (Rijk vs. mede-overheden), vallen enkele verschillen op. Zo is de score 'op weg naar perfect' bij de rijksoverheid laag: 16% tegen 26% bij de mede-overheden. De categorie 'middenmoot' is bij Rijk juist relatief groot: 44% tegen 23% bij de mede-overheden. Bij de mede-overheden komt de score 'nog een heel eind te gaan' juist weer duidelijk meer voor: 34% tegen 19% voor het Rijk.
- In de vorige monitor werd nog gesproken van een duidelijke verbetering bij de categorie Rijk in vergelijking met de mede-overheden. Daar is dit jaar geen sprake van. Bij Rijk houden verschuivingen in de goede en minder goede kant elkaar min of meer in evenwicht. Bij de mede-overheden is per saldo wel sprake van een verschuiving de goede kant op maar de verschillen zijn te klein om daar veel gewicht aan toe te kennen.

Tabel 1: 'Pas toe' en 'leg uit' bij aanbestedingen uit 2021

(Bron: onderzoek aanbestedingen 2021, uitgevoerd zomer 2022)

	Rijksoverheid		Mede-overheden		**Totaal 2021**		Totaal 2020	
	#	%	#	%	#	%	#	%
totaal aantal beoordeelde aanbestedingen waarbij OSn relevant waren	32	100%	35	100%	**67**	**100%**	76	100%
* **perfect**: alle relevante OSn gevraagd	3	9%	4	11%	**7**	**10%**	6	8%
* **op de goede weg**: deel van relevante OSn gevraagd	25	78%	29	83%	**54**	**81%**	66	87%
- op weg naar perfect (67-99%)	5	16%	9	26%	**14**	**21%**	19	25%
- de middenmoot (34-66%)	14	44%	8	23%	**22**	**33%**	23	30%
- nog een heel eind te gaan (1-33%)	6	19%	12	34%	**18**	**27%**	24	32%
geen relevante OSn gevraagd, waarvan	4	13%	2	6%	**6**	**9%**	4	5%
* **matig**: er is wel algemene aandacht voor architectuur-kaders en/of OSn-beleid	0	0%	0	0%	**0**	**0%**	0	0%
* **slecht**: geen aandacht voor OSn-beleid	4	13%	2	6%	**6**	**9%**	4	5%
* **heel slecht**: strijdig met OSn-beleid	0	0%	0	0%	**0**	**0%**	0	0%
In aantallen standaarden:								
totaal aantal relevante OSn	*309*	*100%*	*441*	*100%*	***750***	***100%***	*888*	*100%*
totaal aantal gevraagde relevante OSn	*149*	*48%*	*245*	*56%*	***394***	***53%***	*425*	*48%*
niet alle OSn gevraagd => Leg Uit vereist (voor toelichting: zie paragraaf 3.5)	29	100%	31	100%	**60**	**100%**	70	100%
- concrete verantwoording in jaarverslag	0	0%t	0	0%	**0**	**0%**	0	0%
- beperkte verantwoording in jaarverslag	10	34%	0	0%	**10**	**17%**	11	16%
- geen Leg Uit in jaarverslag	19	66%	31	100%	**50**	**83%**	61	84%

In de categorie **'geen relevante open standaarden gevraagd'** vielen zes aanbestedingen:

- matig: er is algemene aandacht voor architectuur-kaders en/of open standaardenbeleid (0%, vorig jaar eveneens 0%),
- slecht: er is geen aandacht voor open standaardenbeleid (6 aanbestedingen = 9%, vorig jaar nog 5%);
- heel slecht: strijdig met het open standaardenbeleid: (dit jaar geen enkele aanbesteding, vorig jaar evenmin).

Alles bij elkaar genomen is deze verzamelcategorie 'geen relevante open standaarden gevraagd' dus groter geworden, na twee jaren met een daling.

Uit het groen gemarkeerde gestippelde kader midden in de tabel valt op dat het **aantal standaarden** dat per aanbesteding relevant wordt geacht dit jaar wat lager ligt dan vorig jaar (gemiddeld 11,2 standaarden per aanbesteding, vergeleken met 11,7 vorig jaar). Deze daling komt na een periode van enkele jaren achter elkaar met een per saldo oplopend aantal relevante standaarden per aanbesteding. De daling dit jaar manifesteert zich in ongeveer gelijke mate bij zowel aanbestedingen rijksoverheid als mede-overheden. Het gemiddelde bij de mede-overheden is overigens nog steeds beduidend hoger dan bij de rijksoverheid (een verschil van bijna 3 relevante standaarden per aanbesteding).

Tot slot is opvallend aan Tabel 1 dat het aandeel gevraagde standaarden voor Rijk en voor medeoverheden behoorlijk verschilt, dit keer duidelijk in het nadeel van het Rijk: 48% versus 56%. De score bij het Rijk is afgenomen (van 51% naar 48%) terwijl bij de mede-overheden sprake is van een flinke stijging: van 45% naar 56%. Hierbij moet worden opgemerkt dat deze variabele door de jaren heen behoorlijk fluctueert zonder dat sprake is van een eenduidige ontwikkeling. Met de terugval van het uitvraag-percentage bij de Rijksaanbestedingen zijn we terug bij de situatie van twee jaren terug; ook toen scoorde Rijk lager dan de mede-overheden.

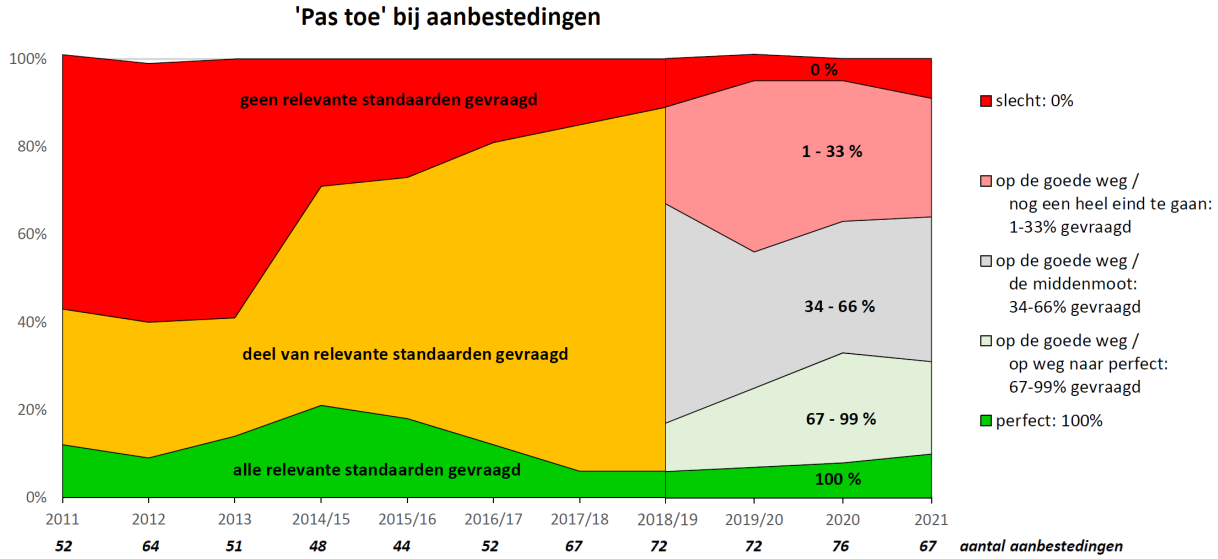
Op basis van Tabel 1 en de cijfers van voorgaande jaren is de ontwikkeling als volgt:

- Het aantal aanbestedingen waarbij om alle relevante standaarden is gevraagd ligt procentueel wat hoger dan vorig jaar; nu 10% tegen 8% vorig jaar. Voor een breder perspectief in de tijd: de vier jaren daarvoor lag de score steeds op 6% of 7% en in de jaren daarvoor was drie jaren op rij sprake van een afname (zeven jaar geleden lag dit percentage nog op 21%). De scores bij de Rijksoverheid en die van de mede-overheden ontlopen elkaar op dit punt niet veel (9% tegen 11% bij medeoverheden).
- De midden-categorie - gekwalificeerd als 'op de goede weg' - is ook bij deze monitor weer op afstand de grootste met 81% (vorig jaar 87%). Binnen deze midden-categorie is het aantal aanbestedingen met de kwalificatie 'op weg naar perfect' afgenomen, in zijn geheel toe te schrijven aan een duidelijke verslechtering bij de aanbestedingen Rijk. Vorig jaar was bij Rijk juist sprake van een duidelijke verbetering op dit punt. Hier staat als positief punt tegenover dat het aandeel van de kwalificatie 'nog een heel eind te gaan' ook is afgenomen. De ‘middenmoot’ laat een min of meer vergelijkbare score als vorig jaar zien.
- Het aantal aanbestedingen waarbij om geen enkele standaard is gevraagd (met oordelen 'matig' dan wel 'slecht') is opgelopen, van 5 % vorig jaar naar 9 % dit jaar.
- Net als vorig jaar is er dit jaar bij geen enkele aanbesteding sprake van strijdigheid met het open standaardenbeleid.

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

De middengroep ‘op de goede weg’, bestaande uit aanbestedingen waarbij wel om één of meer van de relevante standaarden gevraagd werd maar niet om alle, is in de loop der jaren flink gegroeid, inmiddels structureel tot boven de 80% van alle aanbestedingen (zie Figuur 2). Binnen die middengroep maken we nog een nadere onderverdeling tussen aanbestedingen waarbij maar om een klein deel van de relevante standaarden werd gevraagd (1-33%; ‘nog een heel eind te gaan’), een middensegment (34-66%; de middenmoot) en de groep die om een groter deel van de relevante standaarden heeft gevraagd (‘op weg naar perfect’). Zowel in Figuur 2 als in Figuur 3 is te zien, dat het segment van de middengroep met de kwalificatie ‘de middenmoot’ dit jaar het grootst is, gevolgd door wat we hier de minst goede scores noemen (‘nog een heel eind te gaan’). Vorig jaar was dat net andersom. Het segment met de kwalificatie ‘op weg naar perfect’ is relatief het kleinst. Dat was vorig jaar ook al zo, maar het verschil met de beide minder goede subcategorieën ‘middenmoot’ en ‘nog een heel eind te gaan’ is groter geworden, in het nadeel van de categorie ‘op weg naar perfect’.

Figuur 2: 'Pas toe' bij aanbestedingen, 2011 – 2021



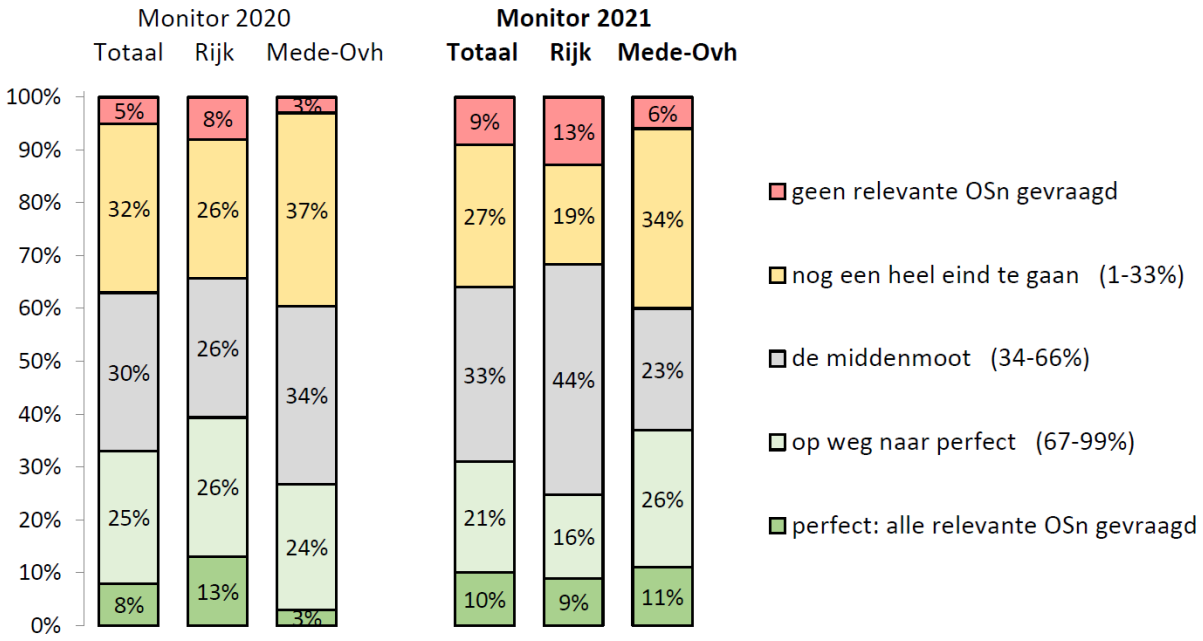
Het Rijk en uitvoeringsorganisaties doen het dit jaar, in tegenstelling tot vorig jaar, minder goed dan de mede-overheden: bij 25% van de aanbestedingen (vorig jaar nog 39%) vroegen Rijk en uitvoeringsorganisaties om alle relevante standaarden ('perfect') of om tenminste twee-derde daarvan ('op weg naar perfect'), voor de mede-overheden ligt het vergelijkbare percentage op 37% (vorig jaar 27%). Bij Rijk is derhalve sprake van een flinke terugval, daar waar bij de mede-overheden juist sprake is van flinke vooruitgang. Aan de andere kant van het spectrum: de Rijksoverheid vroeg bij 32% van de aanbestedingen om geen enkele of om minder dan een derde van de relevante standaarden (vorig jaar 34%). Bij de medeoverheden ligt dit aandeel op 40% (vorig jaar eveneens 40%). Voor zowel de Rijksoverheid als de mede-overheden is derhalve sprake van een stabilisering op deze variabele; daar waar verschillen zijn, zijn deze in vergelijking met de vorige monitor klein.

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

- bij de Rijks-aanbestedingen is het aandeel 'perfect' afgenomen ten opzichte van vorig jaar (van 13% naar 9%) en het aandeel 'geen enkele standaard gevraagd' toegenomen (van 8% naar 13%);
- bij de aanbestedingen van de medeoverheden is het aandeel 'perfect' toegenomen ten opzichte van vorig jaar (van 3% naar 11%), en ook hier is het aandeel 'geen enkele standaard gevraagd' iets toegenomen (van 3% naar 6%);
- de middencategorie 'op de goede weg' is bij de Rijks-aanbestedingen vrijwel even groot als vorig jaar (78% nu tegen 79% vorig jaar); binnen die middencategorie is bij de Rijks-aanbestedingen echter sprake van een duidelijke verschuiving de verkeerde kant op. Het aandeel 'op weg naar perfect' is namelijk flink gedaald (van 26% naar 16%). Het aandeel 'nog een heel eind te gaan' is gedaald: van 26% naar 19%. Het aandeel 'middenmoot' binnen de middencategorie van de Rijksaanbestedingen is gestegen, van 26% naar 44%;
- bij de medeoverheden is de middencategorie 'op de goede weg' geslonken in vergelijking met vorig jaar: van 95% naar 83%. Het aandeel 'op weg naar perfect' is iets toegenomen (van 24% naar 26%) en daar komt bij dat sprake is van een daling bij de

categorie ‘nog een heel eind te gaan’ (van 37% naar 34%). Het aandeel ‘middenmoot’ bij de medeoverheden is sterk gedaald, van 34% naar 23%.

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



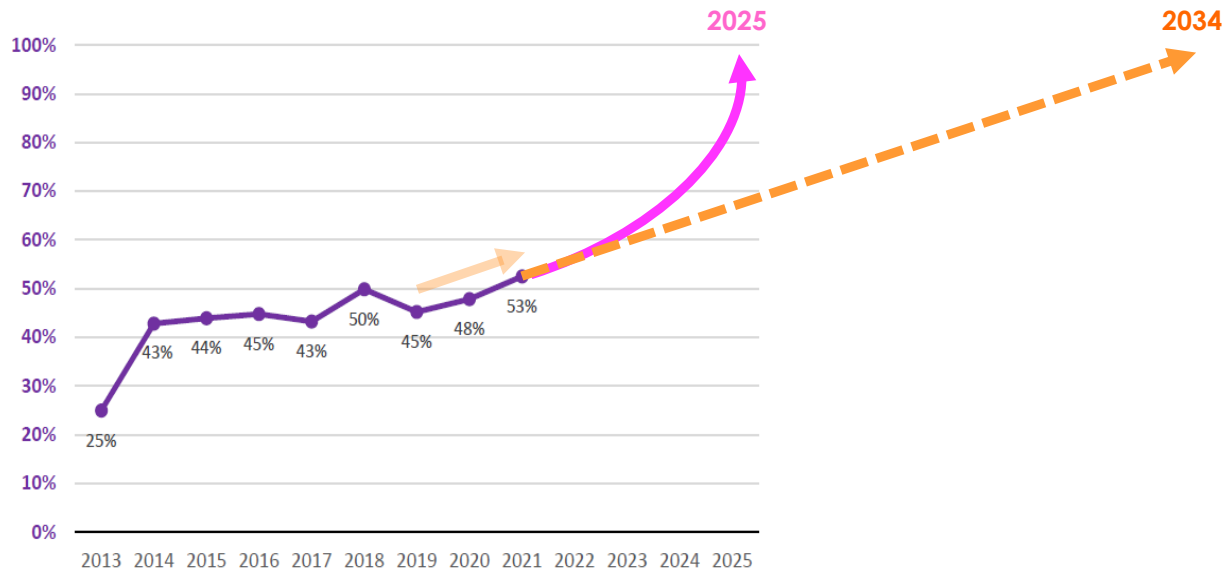
In de vorige monitor werd nog gesteld dat het totaalbeeld, alle cijfers over ‘pas toe’ bij aanbestedingen overziend, behoorlijk positief was. Dat ligt dit jaar genuanceerder.

- Het aandeel aanbestedingen dat als ‘perfect’ werd beoordeeld is beperkt toegenomen, van 8% naar 10%. Het aandeel aanbestedingen in de categorie ‘op weg naar perfect’ is echter kleiner: van 25% naar 21%. Rijk en medeoverheden laten een duidelijk ander beeld zien. Bij Rijk is binnen de hier beschreven twee categorieën sprake van een daling, bij mede-overheden juist van een stijging.
- En het aantal aanbestedingen waarbij geen enkele relevante standaard werd gevraagd is toegenomen, van 5% naar 9%. Deze toename zien we terug bij zowel Rijk als medeoverheden.
- Binnen de grote middengroep is per saldo sprake van een stabilisering. Enerzijds is sprake van een verslechtering, te weten een duidelijke lagere score voor ‘op weg naar perfect’ (van 25% naar 21%). De oorzaak hiervan ligt bij de Rijksaanbestedingen. Daar staat tegenover dat de categorie ‘nog een heel eind te gaan’ ook kleiner is geworden, met een daling van 32% vorig jaar naar 27% dit jaar.
- Van de in totaal 750 keer dat een open standaard voor een aanbesteding relevant was, werd daar in 53% van de gevallen om gevraagd (vorig jaar 48%). Deze vooruitgang komt doordat het percentage ‘gevraagd’ bij Rijks-aanbestedingen weliswaar daalde (van 51% tot 48%) maar deze daling wordt meer dan gecompenseerd door een stijging bij de medeoverheden: van 45% naar 56%.

Ruim 12 jaar nadat de *Instructie Rijksdienst bij aanschaf ICT-diensten of ICT-producten* van kracht werd zijn Rijk en mede-overheden dus halverwege: ongeveer in de helft van de gevallen wordt – wat kabinetsbeleid is – gevraagd om de relevante open standaarden van de lijst. Deze standaarden zijn inmiddels alleen maar belangrijker geworden, en ook voor het

kabinetsbeleid voor een veilige, inclusieve en kansrijke digitale samenleving zijn deze open standaarden een voorwaarde. Maar dan moeten overheden wel in 100% van de gevallen voldoen aan de relevante standaarden, en niet in 50%. Wanneer wordt die 100% bereikt? Extrapolatie van de ontwikkeling van 2019 via 2020 tot 2021 leert, dat het in dit tempo nog tot 2034 zou duren voordat de 100% bereikt wordt. Om in 2025 op 100% te zitten is dus een flinke versnelling nodig, zie ook Figuur 4.

Figuur 4: Extrapolatie van 'Pas toe' bij aanbestedingen: wanneer wordt 100% bereikt?



3.2.2. *Enkele goede voorbeelden*

Ook dit jaar brengen we weer enkele goede voorbeelden van aanbestedingen voor het voetlicht. Bij de keuze van de voorbeelden is het oordeel 'perfect' op zichzelf niet leidend geweest. Ook nu weer zijn er namelijk drie aanbestedingen met het predicaat 'perfect' met een zeer beperkt aantal relevant geachte standaarden waardoor een oordeel 'perfect' relatief makkelijk te bereiken is.

In het navolgende worden zes aanbestedingen kort belicht die alle een complex beeld van relevant geachte standaarden hebben en waar sprake is van een zeer goede uitvraag: vier aanbestedingen met een score 'perfect' (alle gemeenten, al eerder in dit hoofdstuk genoemd) en twee aanbestedingen die daar zeer dicht bij in de buurt komen, van het Ministerie van SoZaWe en van de provincie Flevoland.

- **Gemeente Etten-Leur**. Bij deze aanbesteding gaat het om het leveren van:
  - data- en servicediensten waaronder (a) een Container Management Systeem, (b) een Servicepunt Afval voor de inwoners, (c) een Afval informatiewebsite met Inwoner Portaal afvalregistraties en (d) een Afval informatie App;
  - technische servicediensten, namelijk het ter onderhoud/vervanging/reparatie innemen, afvoeren, aanvullend leveren en uitzetten minicontainers van diverse inhoudsmaten, incl. chips (Restafval, GFT-afval en OPK-afval) en identificatiesticker.
  - De volgende 13 standaarden zijn relevant en ook allemaal uitgevraagd: HTTPS en HSTS, TLS, DNSSEC, SPF, DKIM, DMARC, STARTTLS & DANE, IPv4 en IPv6, StUF, ISO 27001 en ISO 27002, Digitoegankelijk en PDF.

- **Gemeente Gorinchem**. De gemeente is voornemens om de opdracht te verstrekken voor de levering, inrichting en het beheer van een nieuw e-HRM systeem (SaaS-oplossing). Daarnaast wenst de gemeente de volledige ondersteuning bij de implementatie en de koppelingen met de omringende applicaties. Vervolgens is de opdrachtnemer verantwoordelijk voor het verzorgen van scholing, support en advies.
  - Er zijn 12 standaarden relevant: ISO 27001 en 27002, HTTPS & HSTS, TLS, SPF, DKIM, DMARC, STARTTLS & DANE, DNSSEC, SAML, PDF en StUF. Deze zijn alle uitgevraagd.
  - Commentaar van de beoordelaar: hoge kwaliteit aanbesteding.
- **Gemeente Heerde**. Met deze aanbesteding wil de gemeente een standaard (off-the-shelf) zaaksysteem en aanverwante applicatiefuncties verwerven met aanvullend een aantal specifieke koppelingen en diensten.
  - Bij deze aanbesteding waren de volgende 14 standaarden relevant: ISO 27001, ISO 27002, HTTPS en HSTS, TLS, SPF, DKIM, DMARC, STARTTLS & DANE, DNSSEC, IPv4 en IPv6, StUF, SAML, Digitoegankelijk en Digikoppeling. Deze zijn alle 14 uitgevraagd.
- **Gemeente Heerhugowaard**. De gemeente is op zoek naar een applicatie Gegevensdistributie en Servicebus.
  - Bij deze aanbesteding zijn exact dezelfde 14 open standaarden relevant als bij de vorige (van de gemeente Heerde). Ook hier zijn alle 14 standaarden uitgevraagd.
  - Commentaar van de beoordelaar: een voorbeeldige aanbesteding.
- **Provincie Flevoland**. De provincie is voornemens een langjarige overeenkomst te sluiten met een opdrachtnemer voor de vervanging van het financiële systeem inclusief koppelingen middels een software as a service oplossing (SaaS).
  - Er zijn maar liefst 18 standaarden relevant: ISO 27001 en 27002, HTTPS & HSTS, TLS, SPF, DKIM, DMARC, STARTTLS & DANE, DNSSEC, IPv4 en IPv6, SAML, ODF, PDF, NLCIUS, XBRL, Ades Baseline profiles, Digikoppeling en Digitoegankelijk. Alleen de laatste twee zijn niet in de uitvraag meegenomen.
  - Commentaar van de beoordelaar: voorbeeldig maar met een kanttekening. De aanbestedende partij heeft een (bijna) integrale lijst van de open standaarden opgenomen, waaronder ook enkele die niet relevant zijn. Toch communiceert dit wel de juiste intentie richting de inschrijvers, vandaar dat een en ander wel als uitgevraagd is beoordeeld.
- **Ministerie van SoZaWe**. De doelstelling van de aanbesteding is het contracteren van een betrouwbare, ervaren en kundige leverancier van softwarepakketten. Het contract met een leverancier moet leiden tot een geïmplementeerde en adequaat onderhouden applicatie die alle subsidie uitvoeringsvarianten ondersteunt en wordt geïntegreerd in he dan bestaande ICT-landschap. De onderdelen van de applicaties zijn het klantportaal, zaakmanagement, relatiemanagement en documentmanagement.
  - Er zijn 16 standaarden relevant: ISO 27001 en 27002, HTTPS & HSTS, TLS, SPF, DKIM, DMARC, STARTTLS & DANE, DNSSEC, IPv4 en IPv6, SAML, ODF, PDF, BWB, Digikoppeling en Digitoegankelijk. Alleen Digikoppeling is niet uitgevraagd.
  - Commentaar van de beoordelaar: een voorbeeld!

Voor de volgende drie aanbestedingen geldt: net als bij de eerste vier aanbestedingen uit bovenstaande opsomming ook 100% uitgevraagd, maar bij een veel kleiner aantal relevante standaarden (bij de twee eerstgenoemden hieronder alleen de ISO-standaarden):

- **Kamer van Koophandel**. De opdracht betreft het mogelijk maken om te 'vergelijken op NAW'. Klanten die KVK een overzicht bedrijven, stichtingen en/of rechtspersonen

aanleveren, zonder nadere identificerende gegevens (o.a. Kvk-nr, vestigingsnummer, subdossiernummer) wordt bij de Opdrachtnemer gematcht en vergeleken.

- **Tweede Kamer der Staten Generaal**. De inschrijvende partij zal zich in haar rol als (applicatie) beheer hebben kunnen zetten. In deze rol heeft zij volledige verantwoordelijkheid voor de applicatie onder haar beheer. Er is een duidelijk gedefinieerde SLA (Service level agreement). Dit laatste betekent dat beheer de volledige verantwoordelijkheid neemt voor de applicatie(s).
- **Sociale Verzekeringsbank**. Het doel van de aanbesteding is om een overeenkomst te sluiten met één dienstverlener voor de levering van WAN- en internetconnectiviteit en aanverwante dienstverlening. De WAN- en internetverbindingen moeten veilig, betrouwbaar en schaalbaar zijn en goede prestaties bieden. Bij deze aanbesteding zijn niet alleen de ISO-standaarden relevant maar ook HTTPS & HSTS, TLS, DNSSEC en IPv4 en IPv6. Deze zijn alle uitgevraagd.

3.3. 'Pas toe' per open standaard

Voor de mate waarin om een open standaard wordt gevraagd (wanneer die voor de aanbesteding relevant is) biedt Tabel 1 al een eerste indicatie. Bij 67 aanbestedingen was dit jaar in totaal 750 keer een open standaard relevant, en in 394 gevallen (53%) 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 lager dan vorig jaar (11,2 dit jaar tegen 11,7 standaarden per aanbesteding vorig jaar, nadat de vier jaren daarvoor sprake was van een flinke stijging); dit terwijl het aantal standaarden op de lijst hetzelfde is als vorig jaar;
- het percentage daarvan dat is uitgevraagd is 53%, dat is duidelijk hoger dan vorig jaar (toen 48%);
- de combinatie van bovenstaande twee constateringen betekent dat er dit jaar per aanbesteding gemiddeld iets meer standaarden zijn uitgevraagd dan vorig jaar (5,9 dit jaar, versus 5,6 vorig jaar). Hier is derhalve sprake van een gewenste vooruitgang, zij het beperkt qua omvang;
- en het betekent dat er dit jaar minder relevant geachte standaarden NIET uitgevraagd zijn: het gemiddelde aantal niet-gevraagde standaarden per aanbesteding is dit jaar 5,3 (vorig jaar: 6,1). Dit completeert het beeld van een ontwikkeling de goede kant op.

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

Andere zaken die opvallen bij nadere beschouwing van Tabel 5:

- twaalf standaarden zijn vaker gevraagd dan gemiddeld (dus meer dan 53%): HTTPS & HSTS, ISO 27001/02, SAML, STIX en TAXII, TLS, Ades Baseline Profiles, Digitoegankelijk, PDF, NLCIUS, Digikoppeling en StUF. In vergelijking met vorig jaar zijn SETU en de Geo-standaarden uit dit rijtje verdwenen. Nieuwkomers dit jaar zijn STIX en TAXII en Ades Baseline Profiles.
- Deze vier nieuwkomers komen we slechts incidenteel tegen bij aanbestedingen, variërend van 1 tot 3 keer op een totaal van dit jaar 67 onderzochte aanbestedingen.

Tabel 5: 'Pas toe' bij aanbestedingen in 2021, per standaard

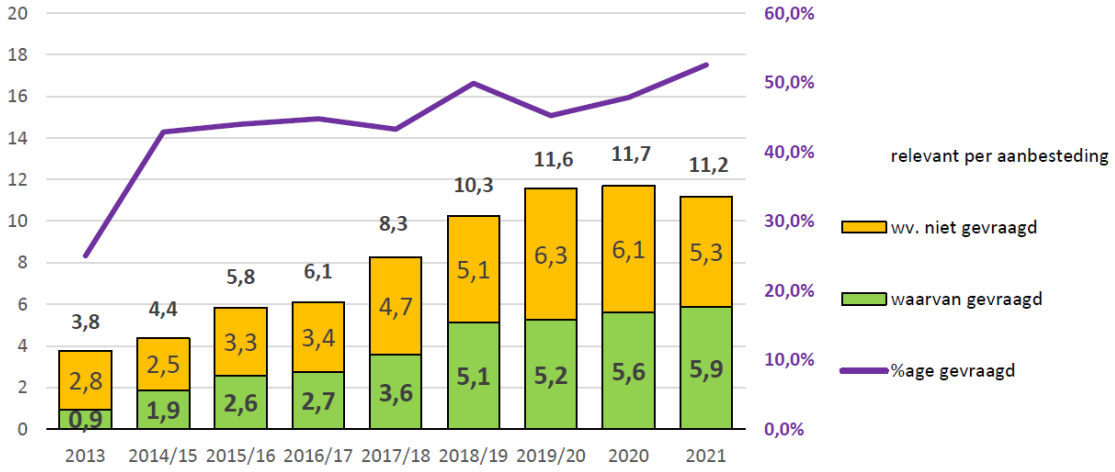
	Rijksoverheid		Mede-overheden		**Totaal 2021**		2020
	relevant	gevraagd in % relevant	relevant	gevraagd in % relevant	relevant	gevraagd in % relevant	gevraagd in % relevant
aantal aanbestedingen:	*32*		*35*		**67**		*76*
Internet & beveiliging:							
DKIM	20	10%	32	44%	**52**	**31%**	28%
DMARC	20	10%	32	44%	**52**	**31%**	28%
DNSSEC	23	43%	32	50%	**55**	**47%**	27%
HTTPS en HSTS	25	64%	34	56%	**59**	**59%**	60%
IPv6 en IPv4	26	19%	35	43%	**61**	**33%**	11%
NEN-ISO\IEC 27001:2005nl	30	90%	35	77%	**65**	**83%**	91%
NEN-ISO\IEC 27002:2007nl	30	90%	35	77%	**65**	**83%**	91%
NL GOV Assurance	4	25%	0		**4**	**25%**	0%
RPKI	0		0		**0**		
SAML	14	71%	21	62%	**35**	**66%**	55%
SPF	20	10%	32	44%	**52**	**31%**	28%
STARTTLS en DANE	20	10%	32	44%	**52**	**31%**	23%
STIX en TAXII	1	0%	2	100%	**3**	**67%**	0%
TLS	25	64%	34	56%	**59**	**59%**	60%
WPA2 Enterprise	1	0%	0		**1**	**0%**	100%
Document & (web)content:							
Ades Baseline Profiles	0		1	100%	**1**	**100%**	67%
Digitoegankelijk *)	13	77%	16	75%	**29**	**76%**	67%
ODF	9	22%	6	33%	**15**	**27%**	6%
OWMS	0		0		**0**		50%
PDF	12	100%	25	52%	**37**	**68%**	69%
SKOS	0		0		**0**		
REST API's:							
OpenAPI Specification	3	0%	3	33%	**6**	**17%**	43%
REST_API Design Rules	3	0%	3	33%	**6**	**17%**	0%
E-facturatie & administratie:							
NLCIUS	1	100%	1	100%	**2**	**100%**	71%
SETU	0		0		**0**		38%
WDO Datamodel	1	0%	0		**1**	**0%**	
XBRL	2	50%	3	33%	**5**	**40%**	60%
Stelselstandaarden:							
Digikoppeling	3	67%	11	73%	**14**	**71%**	52%
Geo−standaarden	0		3	0%	**3**	**0%**	42%
StUF	0		12	92%	**12**	**92%**	89%
Water & Bodem:							
Aquo Standaard	0		0		**0**		
GWSW	0		0		**0**		
SIKB 0101	0		0		**0**		0%
SIKB 0102	0		0		**0**		
Bouw:							
COINS	0		0		**0**		
IFC	0		0		**0**		25%
NLCS	0		0		**0**		
Visi	0		0		**0**		
Juridische verwijzingen:							
BWB	1	100%	1	0%	**2**	**50%**	
ECLI	0		0		**0**		
JCDR	0		0		**0**		
Onderwijs & loopbaan:							
E−portfolio	1	0%	0		**1**	**0%**	0%
NL LOM	1	0%	0		**1**	**0%**	
Overig:							
EML_NL	0		0		**0**		
Totaal	309	48%	441	56%	**750**	**53%**	48%

- Bij drie van de standaarden die behoorlijk vaak relevant waren (> 20 keer) is het percentage gevraagd flink gestegen (meer dan 10%), te weten bij IPv4 en IPv6, DNSSEC en SAML.
- Bij de andere standaarden die vaak relevant waren (> 20 keer), vinden we geen dalers terug als we 'meer dan 10%' als criterium aangehouden. De beide ISO-standaarden 27001 en 27002 komen evenwel dicht in de buurt (van 91% naar 83%).
- Eerder is al opgemerkt dat bij het Rijk het overall uitvraag-percentage is gedaald, van 51 % naar 48 %. Deze afname wordt voor het overgrote deel verklaard door een veel lager uitvraag-percentage bij een aantal standaarden in de hoek van Internet & beveiliging: DKIM, DMARC, SPF en STARTTLS & DANE.

Als we iets verder terugkijken in de tijd, dan blijkt het aantal standaarden dat (gemiddeld) per aanbesteding relevant is gedurende een lange periode gestaag te groeien: van 4,4 in 2015 tot 11,7 in 2020. Met de meting over 2021 erbij is sprake van een kleine daling, tot 11,2 standaard per aanbesteding (zie Figuur 6).

Het percentage dat daarvan gevraagd werd ligt sinds 2015 ruwweg rond de 45% (zie de paarse lijn en de bijbehorende percentage-schaal). Gemiddeld wordt dus om iets minder dan de helft van de relevante standaarden gevraagd, maar er zijn wel ieder jaar meer standaarden relevant. De score van deze monitor (53%) steekt hier dus boven uit.

Figuur 6: Aantal relevante standaarden bij aanbestedingen, 2013-2020



De gestage groei van het aantal relevante standaarden per aanbesteding (even afgezien van de recente correctie) is slechts voor een klein deel te verklaren doordat er meer standaarden op de lijst komen te staan: in 2013 stonden er 34 standaarden op de lijst en voor deze Monitor 2021 waren het er 44. De lijst groeide dus per saldo met 29 %. Dat is slechts een fractie van de toename van het aantal relevante standaarden (voor 2021 bijna 3 keer zoveel als in 2013). Een beperkt deel van de verklaring is, dat er enkele standaarden van de lijst afgevoerd zijn waarvan de meeste niet erg vaak relevant waren en tegelijkertijd er nieuwe standaarden op de lijst zijn gezet die vaak relevant zijn (uit het domein Internet & beveiliging). Overigens zijn er ook nieuwe standaarden op de lijst gekomen die niet bovengemiddeld vaak relevant zijn.

De voornaamste verklaring lijkt te zijn, dat een aantal standaarden de afgelopen jaren geleidelijk vaker relevant is geworden, en dat geldt het sterkste voor de standaarden uit het domein Internet & beveiliging. De 15 standaarden uit dit domein (een-derde van de lijst) zijn goed voor een belangrijk deel van het aantal keer relevant: in totaal was 750 keer een standaard relevant en daarvan betrof het 615 keer (82 %, vorig jaar 74%) een standaard uit het domein Internet & beveiliging.

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

3.4. Welke open standaarden waren relevant bij aanbestedingen?

In het onderzoek is van elke aanbesteding vastgesteld welke standaarden van de 'pas-toe-of-leg-uit'-lijst daarvoor relevant waren. Dat levert ook interessante informatie op vanuit het perspectief van de adoptie van standaarden. In Tabel 7 is weergegeven hoe vaak elk van de standaarden van de lijst relevant is gebleken bij een aanbesteding.

Van de 44 standaarden op de lijst voor 'pas toe of leg uit' zijn er net als vorig jaar 29 (dus twee-derde van de lijst) minimaal bij één aanbesteding relevant. De andere 15 standaarden op de lijst waren dus dit jaar voor geen van de 67 onderzochte aanbestedingen relevant. Daarvan waren er negen ook vorig jaar voor geen enkele onderzochte aanbesteding relevant: RPKI, SKOS, de Aquo-standaarden, GWSW, SIKB 0102, Visi, ECLI, JCDR en EML_NL. De resterende zes standaarden (OWMS, SETU, SIKB0101, COINS, NLCS en IFC) waren bij de vorige monitor wel relevant.

Een vijftal standaarden steekt er met kop en schouders bovenuit als het gaat om de mate waarin zij relevant worden geacht: ISO 27001en ISO 27002 zijn net als vorig jaar bijna altijd relevant (97%) en ook TLS en HTTPS & HSTS scoren net als vorig jaar hoog (beide 88%). Nieuw in dit rijtje van vijf is IPv4 en IPv6 met 91% (vorig jaar 82%).

Als we als criterium aanhouden ‘bij meer dan 50% van de 67 aanbestedingen relevant’, dan kunnen aan dit rijtje nog zeven standaarden worden toegevoegd: DNSSEC (82%), DKIM, DMARC, SPF en STARTTLS & DANE (alle 78%), PDF (55%) en SAML (52%).

Daarna volgt één standaard die bij 25 tot 50% van de aanbestedingen relevant was: Digitoegankelijk. Vorig jaar behoorden ODF, StUF en Digikoppeling ook nog tot deze groep; die zitten nu rond de 20%. Het geheel overziend is sprake van een behoorlijk constante groep standaarden die relatief vaak relevant zijn. Echte uitschieters zitten er niet tussen.

Aan de andere kant: van de 29 standaarden die bij de beoordeelde aanbestedingen relevant werden geacht, zijn er dit jaar 7 slechts incidenteel (1 of 2 keer) als relevant aangemerkt (vorig jaar waren dat er 3): NLCIUS en BWB elk twee keer relevant en WPA2 Enterprise, Ades Baseline Profiles, E-portfolio, NL_LOM en WDO Datamodel elk één keer. In vergelijking met vorig jaar is bij dit rijtje geen sprake van enige overlap (vorig jaar ging het om STIX en TAXII, OWMS en SIKB0101.

Tabel 7: Open standaarden relevant / gevraagd bij aanbestedingen in 2021

(Bron: onderzoek aanbestedingen 2021, uitgevoerd zomer 2022)

	Rijksoverheid		Mede-overheden		**Totaal 2021**	
	relevant in % aanbest.n	gevraagd in % aanbest.n	relevant in % aanbest.n	gevraagd in % aanbest.n	relevant in % aanbest.n	gevraagd in % aanbest.n
aantal aanbestedingen:	*32*		*35*		**67**	
Internet & beveiliging:						
DKIM	63%	6%	91%	40%	**78%**	**24%**
DMARC	63%	6%	91%	40%	**78%**	**24%**
DNSSEC	72%	29%	91%	46%	**82%**	**39%**
HTTPS en HSTS	78%	50%	97%	54%	**88%**	**52%**
IPv6 en IPv4	81%	16%	100%	43%	**91%**	**30%**
NEN-ISO\IEC 27001:2005nl	94%	84%	100%	77%	**97%**	**81%**
NEN-ISO\IEC 27002:2007nl	94%	84%	100%	77%	**97%**	**81%**
NL GOV Assurance	13%	3%	0%		**6%**	**1%**
RPKI	0%		0%		**0%**	
SAML	44%	31%	60%	37%	**52%**	**34%**
SPF	63%	6%	91%	40%	**78%**	**24%**
STARTTLS en DANE	63%	6%	91%	40%	**78%**	**24%**
STIX en TAXII	3%	0%	6%	6%	**4%**	**3%**
TLS	78%	50%	97%	54%	**88%**	**52%**
WPA2 Enterprise	3%	0%	0%		**1%**	**0%**
Document & (web)content:						
Ades Baseline Profiles	0%		3%	3%	**1%**	**1%**
Digitoegankelijk *)	41%	31%	46%	34%	**43%**	**33%**
ODF	28%	6%	17%	6%	**22%**	**6%**
OWMS	0%		0%		**0%**	
PDF	38%	38%	71%	37%	**55%**	**37%**
SKOS	0%		0%		**0%**	
REST-API's:						
OpenAPI Specification	9%	0%	9%	3%	**9%**	**1%**
REST-API Design Rules	9%	0%	9%	3%	**9%**	**1%**
E-facturatie & administratie:						
NLCIUS	3%	3%	3%	3%	**3%**	**3%**
SETU	0%		0%		**0%**	
WDO Datamodel	3%	0%	0%		**1%**	**0%**
XBRL	6%	3%	9%	3%	**7%**	**3%**
Stelselstandaarden:						
Digikoppeling	9%	6%	31%	23%	**21%**	**15%**
Geo−standaarden	0%		9%	0%	**4%**	**0%**
StUF	0%		34%	31%	**18%**	**16%**
Water & Bodem:						
Aquo Standaard	0%		0%		**0%**	
GWSW	0%		0%		**0%**	
SIKB 0101	0%		0%		**0%**	
SIKB 0102	0%		0%		**0%**	
Bouw:						
COINS	0%		0%		**0%**	
IFC	0%		0%		**0%**	
NLCS	0%		0%		**0%**	
Visi	0%		0%		**0%**	
Juridische verwijzingen:						
BWB	3%	3%	3%	0%	**3%**	**1%**
ECLI	0%		0%		**0%**	
JCDR	0%		0%		**0%**	
Onderwijs & loopbaan:						
E−portfolio	3%	0%	0%		**1%**	**0%**
NL LOM	3%	0%	0%		**1%**	**0%**
Overig:						
EML_NL	0%		0%		**0%**	

Eerder in dit hoofdstuk is al opgemerkt dat het aantal relevant geachte standaarden per aanbesteding iets lager ligt dan vorig jaar. Het verschil is evenwel klein. Dit valt ook terug te lezen in Tabel 7: het aantal stijgers en dalers ontloopt elkaar niet veel. Een paar opvallende verschillen zijn met name terug te vinden bij de dalers: ODF, en in mindere mate SETU, de Geo-standaarden en Open API specification. In de vorige monitor werden ODF en Open API specification juist genoemd als opvallende stijgers. Uitschieters de andere kant op – veel vaker 'relevant' dan vorig jaar – zijn er niet.

In vergelijking met de vorige monitor zijn er zoals eerder al opgemerkt zes standaarden deze keer bij geen enkele aanbesteding relevant gebleken en vorig jaar wel: OWMS, SETU, SIKB0101, COINS, NLCS en IFC. Daarbij moet wel worden aangetekend dat de relevantie van deze standaard vorig jaar ook al niet groot was. Andersom zijn er twee 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 WDO Datamodel en NL_LOM.

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: 53% dit jaar tegen 48% vorig jaar. In Tabel 7 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 (81% voor beide), HTTPS & HSTS (52%) TLS (52%), DNSSEC (39%) en PDF (37%). De afgelopen vier jaren stonden op DNSSEC na dezelfde vijf standaarden op dit punt bovenaan.

Na dit rijtje koplopers volgt – net als vorig jaar – nog een tiental standaarden met een score boven de 10%: SAML (34%), Digitoegankelijk (33%), IPv4 & IPv6 (30%), DKIM, DMARC, SPF en STARTTLS & DANE (24%), StUF (16%) en Digikoppeling (15%). In dit rijtje bevinden zich geen nieuwkomers.

Om de andere standaarden is slechts bij enkele aanbestedingen gevraagd of zelfs in het geheel niet. Dit laatste is het geval bij WDO Datamodel, de Geo-standaarden, E portfolio en NL_LOM. Deze 0%-score doet zich dit jaar ook voor bij één standaard die meer dan twee keer als relevant is aangemerkt: de Geo-standaarden.

3.5. 'Leg uit' bij aanbestedingen

Voor de beoordeelde aanbestedingen is nagegaan in hoeverre inmiddels 'leg uit' plaatsgevonden heeft in jaarverslagen over 2021, daar waar dat nodig was.

3.5.1. 'Leg uit' voor aanbestedingen voor aanbestedingen uit 2021

Bij zeven aanbestedingen die in het kader van deze Monitor 2022 zijn beoordeeld, is om alle relevante standaarden gevraagd. Bij de andere 60 aanbestedingen moet dus in het jaarverslag verantwoording afgelegd worden ('Leg uit') voor het niet toepassen van de relevante standaard(en). Voor deze 60 aanbestedingen (door 52 verschillende overheidsorganisaties: 22 vallend onder Rijk, waarvan dit jaar 8 ministeries, en 30 Medeoverheden) is in het Jaarverslag 2021 nagegaan of 'leg-uit' is toegepast. Van 'Leg uit' was in de jaarverslagen van deze 52 overheidsorganisaties echter geen sprake, in die zin dat

in geen van de jaarverslagen een concrete aanbesteding wordt genoemd uit het voorliggende onderzoek waarbij van de lijst voor 'pas toe of leg uit' werd afgeweken.

Bij de 30 decentrale overheden waarvan aanbestedingen zijn onderzocht is in de jaarverslagen c.q. jaarstukken 2021 (voor zover beschikbaar) geen verwijzing naar het open standaardenbeleid teruggevonden, laat staan dat er sprake is van 'Leg uit' voor een specifieke aanbesteding waarvoor dat aan de orde is.

Bij de departementen ligt dat genuanceerder. Er is naar de jaarverslagen van alle 12 ministeries gekeken, hoewel strikt genomen alleen de volgende acht departementen onderwerp van onderzoek zijn: Binnenlandse Zaken en Koninkrijksrelaties, Buitenlandse Zaken, Financiën (met inbegrip van de Belastingdienst), Defensie, Economische Zaken en Klimaat, Sociale Zaken en Werkgelegenheid, Volksgezondheid, Welzijn en Sport en Infrastructuur en Waterstaat. Van deze acht departementen zijn namelijk aanbestedingen beoordeeld uit 2021, met een beoordeling die noodzaakt tot 'leg uit'.

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

- Zeven ministeries (vorig jaar eveneens zeven) hebben een vorm van verantwoording opgenomen in het jaarverslag 2021. Er is daarbij sprake van één nieuwkomer (het ministerie van Buitenlandse Zaken) en één departement (het ministerie van Sociale Zaken en Werkgelegenheid) had vorig jaar nog wel een opmerking in het jaarverslag staan over het toepassen van open standaarden (overigens zeer summier) maar dit jaar niet meer.
- Een vijftal ministeries gaat relatief uitgebreid in op het beleid rond open standaarden, overigens zonder op 'Leg uit' bij concrete aanbestedingen in te gaan. Dit zijn de ministeries van Binnenlandse Zaken en Koninkrijksrelaties, Buitenlandse Zaken, Infrastructuur en Waterstaat, Onderwijs, Cultuur en Wetenschap en Volksgezondheid, Welzijn en Sport. Geen van deze vijf ministeries geeft overigens expliciet aan dat niet is afgeweken van de afspraken rond het gebruik van open standaarden.
- De toelichting van het ministerie van Infrastructuur en Waterstaat overstijgt het tamelijk procedurele niveau van de andere vier ministeries en gaat concreet in op de praktijk van het toepassen van open standaarden (en gebruik maken van open source software).
- De ministeries van Algemene Zaken en Defensie zijn heel summier. Zie onderstaand overzicht.
- Vier van de vijf ministeries die dit jaar niets melden over het gebruik van open standaarden deden dat vorig jaar ook niet. Uit het overzicht hieronder valt af te leiden dat het gaat om de ministeries van Economische Zaken en Klimaat, Financiën, Justitie en Veiligheid en Landbouw, Natuur en Visserij.

In onderstaand overzicht zijn de bevindingen samengebracht.

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

Ministerie	Uitvoering 'leg uit'
BZK	Open standaarden en open source software Het Ministerie van BZK handelt in overeenstemming met artikel 3, eerste lid van de 'Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten'. BZK ziet er op toe zoveel mogelijk te voldoen aan de open standaarden op de pas toe of leg uit -lijst van het Forum Standaardisatie. Het in 2020 gestarte project om de open standaarden voor beveiliging van domeinen en email te bevorderen en op orde te brengen is doorgelopen tot in 2021. BZK stimuleert rijksbreed het gebruik van open source software met inachtneming van de wetten en beleidsregels omtrent privacy, informatiebeveiliging en informatiehuishouding. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf, onder paragraaf 2)*
BUZA	Gebruik open standaarden en open source software Conform de Instructie Rijksdienst maakt BZ gebruik van de lijst van open standaarden van Forum Standaardisatie bij het verwerven en/of realiseren van nieuwe informatie-voorzieningen. Hierbij wordt in de beginfase beoordeeld welke open standaarden voor de informatievoorzieningen van toepassing zijn en als eis neergezet voor de implementatie van deze voorziening. Daarnaast wordt er bij BZ actief gestuurd op de halfjaarlijkse metingen op deze standaarden die via de CISO-Raad worden verspreid. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf, onder paragraaf 2)*
DEF	Gebruik open standaarden en open source software Het beleid inzake open standaarden en open source-software wordt zoveel mogelijk gevolgd. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf, onder paragraaf 2)*
EZK	[Geen]
FIN	[Geen]
I&W	Gebruik open standaarden en open source software In 2021 is de CoronaCheck Scanner door VWS ontwikkeld. IenW stond aan de lat voor het ondersteunen van internationale reisorganisaties bij het controleren van DCC QR codes (DCC=Digital COVID Certificate). Doordat de CoronaCheck code geheel Open Source is, heeft IenW optimaal gebruik kunnen maken van de inspanningen van VWS engineers om de Europese verordening voor het DCC te vertalen naar een ICT oplossing. Zonder de inzet Open Source was dit niet mogelijk geweest en ook in het vervolg maakt IenW dankbaar gebruik van Open Source referentiesoftware, deze keer ontwikkeld door T Systems in opdracht van de EU. IenW stuurt al jarenlang op het toepassen van Open Source (onder andere op basis van de Open Source strategie van 2011) en, via de IenW Enterprise architectuur, op de verplichte en aanbevolen Open standaarden zoals gepubliceerd door Forum Standaardisatie. We merken op dat de samenstelling van de lijst en de introductie van de Beslisboom op de website van Forum Standaardisatie hun nut hebben: de standaarden voelen minder als corvee, en maken oplossingen daadwerkelijk beter in de praktijk. Binnen IenW helpt daarbij ook de Praktische Toepassing Verplichte Eisen aan Digitale Voorzieningen, en de toepassing van het door IenW zelf ontwikkelde Open Source platform Standaard Platform, dat inmiddels door Logius wordt geëxploiteerd. Door dit soort initiatieven te gebruiken bij inkoop en aanbesteding werkt IenW actief mee aan de invulling van het rijksbeleid. *(Bron: 6. Bedrijfsvoeringsparagraaf, onder paragraaf 2)*
SZW	[Geen]
VWS	Gebruik open standaarden en open source software Binnen het concern VWS wordt indien mogelijk gestreefd naar het gebruik van open standaarden. In een aantal gevallen, bijvoorbeeld bedrijfsvoering met gevoelige informatie, of vanwege een andere technische oplossing, is het gebruik van open standaarden niet altijd mogelijk. Dit geldt ook voor functionele inkoop van software binnen het ministerie van VWS. Indien het proces (functioneel, cq. non-functioneel) een dergelijke IV ondersteuning toelaat, hebben open source oplossingen de voorkeur en worden als wens in het programma van eisen opgenomen. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf onder 2)*

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

Ministerie	Uitvoering 'leg uit'
AZ	Gebruik open standaarden en open source software Er zijn geen bijzonderheden te melden. *(Bron: B Beleidsverslag onder 5: bedrijfsvoeringsparagraaf, meerdere plaatsen.)*
J&V	[Geen]
LNV	[Geen]
OCW	Gebruik open standaarden en open source software De Instructie Rijksdienst schrijft voor dat bij de aanschaf en ontwikkeling van ICT-diensten of ICT-producten in beginsel gebruik moet worden gemaakt van open standaarden van de lijst van het Forum Standaardisatie (www.forumstandaardisatie.nl). Valide afwijkingsgronden zijn opgenomen in de Instructie Rijksdienst. Indien er sprake is van een afwijking van de Instructie Rijksdienst, dan wordt dit gemotiveerd aangegeven. Bij het Ministerie van OCW is bij de meting eind 2021 geen sprake geweest van afwijking van de Instructie Rijksdienst. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf onder 2)*

Als aanvulling op de departementale insteek waarvoor in het bovenstaande is gekozen, volgt – bij wijze van afsluiting – in onderstaand kader de passage uit de Jaarrapportage Bedrijfsvoering Rijk 2021 over het gebruik van open standaarden. Naar aanleiding van recente aanpassingen in de Rijksbegrotingsvoorschriften is deze tekst gewijzigd.

Update Enterprise Architectuur Rijk en bevordering gebruik (open) standaarden

Als Rijksoverheid willen we goed inspelen op nieuwe technische ontwikkelingen. Dit doen we door afspraken te maken over wat we samendoen, waar we goed op elkaar aansluiten en waarvan we met en van elkaar kunnen leren. Hiervoor maken we ook afspraken over verplichte standaarden (pas-toe-of-leg-uit), en delen we goede praktijkvoorbeelden. Samenwerken waar dat moet én waar dat voordeel biedt. Daarbij gebruiken we de Enterprise Architectuur Rijk (EAR), die de huidige en gewenste inrichting van de informatie-voorziening van de Rijksoverheid beschrijft. In het vierde kwartaal van 2021 startte CIO Rijk een onderzoek naar de rol en positie van de EAR binnen de Rijksinformatievoorziening. Het onderzoek Jaarrapportage Bedrijfsvoering Rijk 2021 moet een gedragen visie op de EAR opleveren met, voor, en door betrokkenen, die met de EAR te maken hebben. De EAR wordt op basis van de aanbevelingen uit dit onderzoek herzien. Het gebruik van open standaarden wordt al langere tijd gestimuleerd en dat is voortgezet in 2021. Deze standaarden dragen eraan bij dat informatie beter beveiligd, makkelijker uit te wisselen en voor iedereen toegankelijker wordt. In 2021 vervolgden we eerder aangekondigde acties om de pas-toe-of-leg-uit standaarden met bestaande kaders te koppelen. Denk daarbij aan de verslagleggingskaders (zoals de Rijksbegroting), inkopen en informatiebeveiliging (Baseline Informatiebeveiliging Overheid). Een voorbeeld van het toepassen van open standaarden is de Europese Aanbesteding voor Vernieuwing Rijksportaal. Hier zijn deze standaarden in het Programma van Eisen opgenomen en door de leverancier toegepast bij de realisatie daarvan. De verschillende rijksonderdelen adopteren zelf de standaarden. Om die adoptie te stimuleren, delen we goede praktijkvoorbeelden waarin ook het maatschappelijk effect van het gebruik van open standaarden duidelijk wordt. Het Forum Standaardisatie voert jaarlijks een overheidsbrede meting uit naar het toepassen van de open standaarden die op de pas-toe-of-leg-uit lijst staan en publiceert de uitkomst daarvan op zijn website. Daarbij is ook een overzicht met analyse naar grote organisaties opgenomen (zie Monitor Open

Standaarden | Forum Standaardisatie). In aanbestedingen vragen rijksorganisaties steeds vaker om de relevante open standaarden. Uit de Monitor 2021 komt naar voren dat bij een aantal aanbestedingen van het Rijk de relevante standaarden goed zijn uitgevraagd. Bij de meeste aanbestedingen is echter om een deel van de relevante standaarden gevraagd. De uitleg in de jaarverslagen (waarom er niet om sommige standaarden is gevraagd) ontbreekt echter structureel. Daarnaast laat de monitor zien dat het gebruik van standaarden in de door het Rijk beheerde voorzieningen ver gevorderd is (rond de 84 procent). Eind 2021 liep ook de streefbeeldafspraak af om volledig aan Internet Protocol versie 6 (IPv6) te voldoen. Hierin boekten het Rijk en de uitvoeringsorganisaties voortgang. Van websites 79 procent en e-mail 40 procent (in maart) naar respectievelijk 80 procent en 46 procent (in september). Niettemin is het streefbeeld nog niet gehaald en de tijd hiervoor dringt.

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 2020 in de Monitor 2021 valt op dat dit jaar bij evenveel departementen een verwijzing naar het beleid rond de toepassing van open standaarden is verschenen.

3.5.2. Reacties op en discussie over de beoordelingen

Sinds enkele jaren informeren wij aanbesteders over de beoordeling van hun aanbesteding en in het verlengde daarvan worden zij uitgenodigd om op die beoordeling te reageren. Een citaat uit de betreffende mail: *"Graag horen wij van u hoe het komt dat niet alle open standaarden zijn gevraagd in deze aanbesteding. Als dit een reden is van bijzonder gewicht, zoals bedoeld in artikel 3 lid 2 van de Instructie rijksdienst inzake aanschaf ICT-diensten en ICT-producten, dan kan dit immers leiden tot een andere beoordeling."* Dit blijkt steeds meer in een behoefte te voorzien. Bovendien draagt het bij aan meer begrip over en weer; zowel bij de beoordelaars als bij degenen van wie een aanbesteding is beoordeeld. Soms leidt dit proces van hoor en wederhoor nog tot een aanpassing van de beoordeling; zowel ten aanzien de relevantie van een specifieke standaard als ten aanzien van de kwestie of een stadaard al dan niet is uitgevraagd. Eerder in deze rapportage is bovendien gebleken dat hoor en wederhoor ertoe kan leiden dat een aanbesteding om goede redenen buiten de monitor-rapportage gehouden dient te worden.

Om een inkijkje te geven in de discussie die ontstaat tijdens dit proces van hoor en wederhoor volgt hieronder als afsluiting van dit hoofdstuk een korte bloemlezing.

Aanbestedende partij (waterschap): "De aanbesteding betrof een gesloten netwerk. Het gebruik van het publieke internet was hierbij niet toegestaan, derhalve zijn in rood afgedrukte standaarden (d.w.z.: niet uitgevraagd) niet relevant".

Beoordelaar: "U heeft een terecht punt dat de door ons aangevoerde standaarden niet relevant zijn in het geval van WAN diensten. Echter in de bestektekst lezen we (o.a.) dat de aanbesteding tevens betrekking heeft op: 'Het leveren van Support in de vorm van een Webportaal voor het beheer en management van de netwerkdiensten'. Dit is de reden om de genoemde standaarden relevant te achten. Dit is slechts een onderdeel van de aanbesteding. Echter, wanneer een leverancier bouwt wat u vraagt, zal er naast de WAN diensten ook een SaaS-dienst/website in de lucht gebracht worden die dient te beschikken over de nodige (informatie)beveiliging, email functionaliteit en de open standaarden die hier bij horen."

Aanbestedende partij: "Nu begrijp ik jullie reactie beter, maar vallen de meeste of wellicht alle voorgestelde standaarden niet onder de BIO paraplu?"

Beoordelaar: "De BIO en soortgelijke documenten worden inderdaad vaak aan aanbestedingen toegevoegd. Soms wordt ook de lijst met open standaarden van BFS integraal opgenomen. De reden dat dit niet afdoende is in het kader van deze beoordeling is omdat daarmee de verantwoordelijkheid voor het selecteren en implementeren van de relevante open standaarden naar de leverancier wordt verplaatst. Dit gecombineerd met het gegeven dat het juridisch gezien de verantwoordelijkheid van de aanbesteder is om aan het open standaarden beleid te voldoen, maakt dat het opnemen van algemene documenten/richtlijnen onvoldoende is. Aan de hand van de specifieke functionaliteit van de aan te besteden dienst dienen de relevante open standaarden expliciet te worden geëist."

Aanbestedende partij (ZBO): "Bedankt voor je bericht. Ik heb de vraag intern uitgezet en kom binnenkort met een reactie." En later: "Hieronder een korte verklaring waarom niet alle open standaarden zijn gevraagd in de aanbesteding voor (…):

- *Een aantal van de genoemde standaarden hebben betrekking op de email server. In de gevraagde oplossing wordt de email server van (…) gebruikt, waarvoor deze open standaarden wel van toepassing zijn.*
- *Daarnaast worden een aantal standaarden genoemd die gelden voor API's binnen de Nederlandse overheid. Deze kun je niet opleggen aan een wereldwijd algemeen toepasbare pakket.*
- *Tenslotte is ODF van toepassing als er bewerkelijke documenten worden uitgewisseld, en de gevraagde oplossing wisselt juist onbewerkelijke documenten (PDF) uit."*

Beoordelaar: "Met betrekking tot de email standaarden heeft u een terecht punt. Waar een mailserver uiteindelijk geplaatst wordt is voor ons niet altijd goed vast te stellen aan de hand van de bestekteksten. Dit zullen we aanpassen in de eindbeoordeling. Met betrekking tot de API standaarden is het inderdaad begrijpelijk dat er beperkte/geen invloed is op externe koppelvlakken. Echter zoals we de bestekteksten lezen zal de aan te besteden dienst tevens een eigen API endpoint bevatten waar externe partijen/diensten mee kunnen verbinden. Hier heeft de leverancier wel invloed op. Op dit vlak zijn de API standaarden dan wel noodzakelijk om van de leverancier te eisen. Ook ODF zullen we aanpassen in de eindbeoordeling."

Aanbestedende partij (gemeente): "Ik heb de betrokken personen bij deze aanbesteding (voor zover nog aanwezig) bevraagd en gewezen op onderstaande. Wij nemen de opmerkingen mee in onze evaluaties en interen processen. Korte reactie gehad vanuit de werkgroep:

- *ISO: We hebben een DigiD-proof systeem uitgevraagd. De BIO (afgeleid van de ISO 27xxx) is daar een impliciet onderdeel van. De ICO is gebruikt in de aanbesteding. ISO27002 wordt als eis genoemd in een van de bijlagen;*
- *DANE: Hoeft m.i. niet uitgevraagd te worden, omdat de dienst onder het internetdomein van de gemeente draait en niet onder het internetdomein van de leverancier/derden;*
- *STARTTLS: Is m.i. omschreven als eis in de SAAS applicatiecriteria (eis 16), maar wordt niet bij naam genoemd. Het expliciet noemen is inderdaad beter.*

Wij danken u voor de feedback.".

Beoordelaar: "Met betrekking tot ISO 27001/27002 heeft u een terecht punt. Dit zullen we aanpassen in de eindbeoordeling. Met betrekking tot STARTTLS en DANE is doorslaggevend of er email functionaliteit in de dienst zit. Uit de bestekteksten hebben we afgeleid dat dit het geval is. Voor de implementatie van deze standaarden is niet relevant of het domein bij de gemeente draait, maar hoe de uitgaande mailserver van het eindproduct geconfigureerd wordt. In de praktijk kan het inderdaad betekenen dat een dienst volledig binnen de online infrastructuur van de gemeente gaat draaien, maar dat doet niet af aan de noodzakelijkheid van het eisen van deze standaarden."

Aanbestedende partij (gemeente): "Dank u voor uw terugkoppeling. Ik heb geschakeld met de verantwoordelijke vakafdeling. Uiteraard zijn wij als (…) blij met uw oordeel (bijna perfect….), waarbij de credits liggen bij de collega's van de vakafdeling en alle overig inhoudelijk betrokkenen (extern adviseur, key-users/ ervaringsexperts). Volgens u zijn de relevante standaarden voor onze aanbesteding (…): ISO 27001, ISO 27002, HTTPS en HSTS, TLS, SPF, DKIM, DMARC, STARTTLS & DANE, DNSSEC, IPv4 en IPv6, StUF, Digitoegankelijk, PDF, ODF en SAML. U vraagt waarom open standaarden ODF en SAML niet zijn uitgevraagd, hierbij onze reactie.

<u>Standaarden</u>
ISO 27001, ISO 27002, HTTPS en HSTS, TLS, SPF, DKIM, DMARC, STARTTLS & DANE, DNSSEC, IPv4 en IPv6, StUF, Digitoegankelijk, PDF:
Algemene reactie: een aantal hiervan is eigenlijk te voor de hand liggend maar niet specifiek uitgevraagd. Wat betreft StuF is deze uitgevraagd in relatie tot nieuw API standaarden, zoals 'haalcentraal'. PDF en document creatie zijn documentsoorten die worden aangeboden aan / doorgestuurd door het zaaksysteem maar de creatie ligt elders. Wat betreft de ISO-certificering wordt nu voldaan door de leverancier die de oplossing beschikbaar gaat stellen.

<u>Standaarden die volgens u niet uitgevraagd zijn</u>
ODF: Niet uitgevraagd omdat voor het zaaksysteem het type document dat wordt ontvangen of verstuurd hier niet wordt bepaald.
SAML: Binnen de structuur die wij nu nog hanteren (ADFS) is dit niet snel voldoende te implementeren. Kanttekening hierbij is dat wij wel via de Nota van Inlichtingen 1 (zie vraag en antwoord 91 en 139, bijgevoegd) het gebruik van SAML toestaan. Dus niet geëist, maar uiteindelijk wel toegestaan. Mogelijk dat uw oordeel daardoor nog positiever uitvalt.

<u>Reden van bijzonder gewicht</u>
Gezien de bovenstaande toelichtingen heeft dit volgens ons niet geleid tot een reden van bijzonder gewicht in de aanbesteding, waardoor een andere beoordeling/ uitkomst mogelijk is. De aanbesteding is naar onze mening correct gegund."

Beoordelaar: "Met betrekking tot ODF gaat het aan de kant van de beoordelaars om een inschatting aan de hand van de omschrijving van de dienst. Indien u aangeeft dat dit geen onderdeel uitmaakt van het eindproduct, dan zullen we dit aanpassen in de eindbeoordeling. Met betrekking tot SAML en single-sign-on is het wel van belang dat aan te besteden diensten van gesloten/commerciële systemen migreren naar open systemen. Het kan zijn dat implementatie in de praktijk vanwege bredere infrastructuur keuzes niet mogelijk blijkt, maar het is wel van belang dat bestekteksten dit eisen. Verder is de kwaliteit van deze aanbesteding bovengemiddeld hoog en is ons duidelijk geworden dat er binnen de organisatie diepe kennis aanwezig is op het gebied van open standaarden."

Aanbestedende dienst (gemeente): "Bedankt voor je mail. In de aanbesteding wordt de GIBIT van toepassing verklaard. In bijlage 5a verwijzen we naar de website https://www.forumstandaardisatie.nl/open-standaarden. Hierin worden volgens mij alle in het rood genoemde standaarden vermeld. Ontbreekt er dan nog iets? Dan ga ik namelijk verder onderzoeken of daar een geldige reden voor is."

Beoordelaar: "Ik begrijp uw vraag goed. In veel aanbestedingen wordt verwezen naar de lijst open standaarden. De verwachting is dat de leveranciers vervolgens zich deze lijst eigen maken en vervolgens alle standaarden gaan toepassen. De praktijk laat echter zien dat dit niet het geval is. Zonder expliciete eisen kunnen gebrekkige/onveilige producten opgeleverd worden. Vervolgens worden vingers gewezen naar wie duidelijker had moeten aangeven of iets echt belangrijk is of niet. Daar komt bij dat de uiteindelijke verantwoordelijkheid voor het toepassen van open standaarden (praktisch en juridisch) ligt bij de aanbesteder en niet de leverancier. Het klopt inderdaad dat ISO 27001 en 27002 onderdeel zijn van de GIBIT. Dit zullen we aanpassen in de eindbeoordeling.
Afrondend lijkt het me goed om aan te geven dat het soms lastig blijft om tot een absoluut sluitende beoordeling te komen aangezien in het vroege stadium van de ontwikkeling/levering van de dienst voor partijen nog vaak onduidelijkheden bestaan. Over sommige technische aspecten wordt pas in een latere fase beslist. Bovenal is het de bedoeling van de monitor en deze contactmomenten om het gebruik van open standaarden aan te moedigen en bespreekbaar te maken. De hoop is dat dit over de lange termijn leidt tot effectievere ICT diensten."

Aanbestedende dienst (ministerie): "Dank voor uw bericht. Ik denk dat (…) zich niet hoeft te schamen voor de (voorlopige) uitkomst. Ten aanzien van de onvolkomenheid (het niet toepassen van de STIX TAXII standaard) heb ik een paar vragen:

- *STIX TAXII moet worden toegepast indien er sprake is van structurele uitwisseling van cyberdreigingsinformatie tussen Opdrachtgever en Opdrachtnemer. Hoe komt men tot de conclusie dat daarvan sprake zou zijn bij deze opdracht? Ik kan daar niets over terugvinden in het programma van eisen.*
- *In eis 21 hebben wij de eis verwoord dat het geleverde netwerk en dienstverlening voldoet bij aan de "verplichte standaarden uit de lijst open standaarden van Bureau Forum Standaardisatie". De tekst is voorzien van een URL naar de pagina waar deze standaarden (inclusief STIX TAXII) is vermeld. Volstaat deze eis niet in het geval dat er toch op enige schaal cyberdreigingsinformatie wordt uitgewisseld?*

Ik hoop dat u mij het antwoord op deze vragen kunt toesturen, ik zal daarna met alle plezier bij (…) informeren waarom deze standaard niet expliciet in het PvE is vermeld."

Beoordelaar: '"Met betrekking tot punt 1: veel aanbestedingen betreffen tegenwoordig Software-as-a-Service (SaaS). Hierbij zijn infrastructurele zaken minder van belang aangezien hosting en connectiviteit wordt uitbesteed. De onderhavige aanbesteding wijkt af van SaaS aangezien hier vooral infrastructuur wordt gevraagd. Dit betekent dat de dienst tevens betrekking heeft op zaken die normaliter aan de hoster worden overgelaten, zoals hoe om te gaan met digitale dreigingen gericht tegen de onderhavige infrastructuur en de uitwisseling van informatie daaromtrent. Met betrekking tot punt 2: een algemene verwijzing naar de lijst met open standaarden is onvoldoende specifiek aangezien de verantwoordelijkheid hiermee wordt verplaatst naar de leverancier. De intentie is vooral dat binnen de aanbestedende organisatie kennis en bewustwording ontstaat omtrent de open standaarden."

Aanbestedende dienst (ZBO): Voor onderstaande heb ik intern navraag gedaan bij de betrokken projectleider. Hij gaf mij het volgende antwoord:
Wat wij hebben aanbesteed is de beschikbaarheid van een WCSM-omgeving als dienst (SaaS-cloud) waarin managed hosting integraal onderdeel uitmaakt van de dienstverlening. Wij meenden daarom dus geen detailspecificaties te hoeven geven over standaarden voor de security van managed hosting. Door de eisen NEN ISO 9001, ISO27001 e.v., ITIL-conform en Digitoegankelijkheid meenden wij de hoogst haalbare kwaliteitsnormen te hanteren aan platform en leverancier. De standaarden in het rood zijn in die zin een conditio sine qua non. Graag ontvangen we een advies of wij bij de volgende aanbesteding van SaaS-cloud dienstverlening met inbegrip van managed hosting, alsnog deze de facto standaarden expliciet moeten meenemen.

Beoordelaar: "Ik begrijp de reactie omtrent het wel/niet aanleveren van productspecificaties. Het probleem in de praktijk is echter dat een leverancier die een dergelijke opdracht zonder specificaties gegund krijgt, een product kan afleveren dat gebrekkig/onveilig is zonder dat deze hier op basis van de bestekteksten op aangesproken kan worden. Ervaring leert dat extra werk/functionaliteit/ maatregelen/beveiliging die niet expliciet geëist worden, een veel kleinere kans hebben om geïmplementeerd te worden. Daarnaast is het tegenwoordig van belang dat ook binnen de aanbestedende organisaties bewustwording ontstaat omtrent het belang van open standaarden en in dit specifieke geval, informatiebeveiliging."

4. Toepassing van open standaarden via voorzieningen

4.1. Over dit deelonderzoek

4.1.1. Waarom overheidsbrede voorzieningen relevant zijn

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

Tot 2020 onderzochten wij een grote, gevarieerde verzameling van 35 voorzieningen elk jaar opnieuw. Inmiddels voldoen veel voorzieningen aan een redelijk groot deel van alle voor hen relevante voorzieningen. Het blijft belangrijk om de toepassing van open standaarden bij deze voorzieningen te blijven volgen, maar dat hoeft niet meer per sé jaarlijks. Een lagere frequentie biedt ook meer ruimte voor de implementatie van de standaarden, inclusief nieuwe standaarden op de lijst. En het beperkt de administratieve lasten voor de beheerders.

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

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

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

4.1.2. Welke voorzieningen zijn onderzocht?

Dit jaar zijn de 17 voorzieningen onderzocht die direct raken aan de communicatie en gegevensuitwisseling met burgers en bedrijven. Het gaat om de volgende voorzieningen:

- DigiD [Logius]
- DigiD Machtigen [Logius]
- Afsprakenstelsel ETD [Logius]
- PKI Overheid [Logius]
- MijnOverheid [Logius]
- Berichtenbox bedrijven [RVO]

- Overheid.nl [KOOP]
- Ondernemersplein [KVK]
- Samenwerkende Catalogi [Logius]
- Rijksoverheid.nl / web-domein [DPC / MinAZ]
- Rijksoverheid.nl / email-domein [SSC-ICT]
- website RDW.nl (voertuigen) [RDW]
- website WOZ-waardeloket.nl [Kadaster]
- website Handelsregister KvK (NHR) [KVK]
- website PDOK (open geo-data) [Kadaster]
- TenderNed [PIANOo / DICTU]
- Digi-Inkoop [Logius]

De 19 voorzieningen die vorig jaar zijn onderzocht (relevant voor de gegevensuitwisseling en communicatie tussen overheden en onderliggende infrastructuur) zijn: BSN Beheervoorziening en GBA-V, Doc-Direct, Rijksportaal, BAG, BRK, BGT, WOZ, BRT, BRI, BRO, BRV, NHR, Digilevering, Digimelding, Stelselcatalogus, DigiPoort, Diginetwerk en Digitale Werkomgeving Rijk.

4.1.3. Werkwijze

Voor dit onderzoek is gebruik gemaakt van de 'pas toe of leg uit'-lijst van 1 april 2022. Met elke beheerder is gekeken welke standaarden van deze lijst voor de voorziening relevant zijn. Daarbij is telkens uitgegaan van de eindgebruiker. Dat is degene die in de keten baat zou moeten hebben bij het gebruik van open standaarden. Dit is expliciet zo gekozen, omdat het open standaardenbeleid vooral gericht is op het stimuleren van interoperabiliteit. In eerdere onderzoeken is gebleken dat beheerders van voorzieningen soms terminologie gebruiken als '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. In deze gevallen is er 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 de voorzieningen daarvan gebruik maken. Het vertrekpunt daarbij is telkens het overzicht van het vorige meetmoment, in dit geval dus 2020. Waar mogelijk zijn de standaarden vooraf door de onderzoekers zelf getoetst. Daarbij maken we onder andere gebruik van de testen die beschikbaar zijn via internet.nl en RIPEstat. In paragraaf 4.1.5 wordt uitleg gegeven over het toetsen van de standaarden. Daarnaast kijken we of de geplande activiteiten om aan standaarden te voldoen inmiddels uitgevoerd zijn. Voor nieuwe standaarden op de lijst maken we in samenspraak met de beheerders een inschatting of ze relevant zijn voor de voorziening.

Vervolgens sturen we het voorbereide overzicht met relevante standaarden per voorziening toe aan de beheerder. We vragen hen onze inschatting te valideren en een toelichting toe te voegen. Op basis van hun reactie wordt de verzamelde informatie aangescherpt. Het resultaat daarvan wordt voorgelegd aan de opdrachtgever en wordt vervolgens in een definitieve versie toegestuurd aan de beheerders. Na hun akkoord wordt de informatie opgenomen in deze 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 (telefonisch) besproken. In de gevallen waar de verschillen ook

na de gesprekken bleven bestaan, is dit duidelijk opgenomen in de rapportage. Vanuit enkele beheerders is gedurende het beantwoordingsproces de correspondentie gestopt, ondanks herhaalde pogingen tot contact. Aan deze beheerders hebben wij schriftelijk aangegeven op welke manier de antwoorden in de rapportage zijn opgenomen.

4.1.4. Aandachtspunten voor de lezer

Voorzieningen en standaarden geordend op basis van functionaliteit

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

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

Status

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

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

Met ‘conform’ wordt in dit onderzoek bedoeld dat de standaard door de eindgebruiker te gebruiken is.

Relevantie standaard

Voor de relevantiebepalingen zijn per standaard de beschrijvingen van het functioneel en organisatorisch toepassingsgebied gehanteerd (zoals vermeld op de pas toe of leg uit-lijst van het Forum Standaardisatie). Standaarden die niet relevant zijn voor een voorziening zijn niet in de tabel opgenomen. Voor de standaarden die ten opzichte van de vorige meting in 2020 nieuw zijn op de lijst is samen met de beheerders een inschatting gemaakt in hoeverre ze relevant voor de voorziening zijn.

4.1.5. Wijze van toetsen standaard

Toetsen en het bevragen van beheerders

Het toetsen wanneer een voorziening aan een standaard voldoet is lastig. Het vereist een heldere afbakening van de voorziening en heldere voorwaarden wanneer voldaan wordt aan een standaard. Deels hanteren we beschikbare (openbare) toetsen zoals internet.nl en RIPEstat. om de compliancy vast te stellen. We hebben geen toegang tot interne systemen of documenten. Dat gaat de scope van dit onderzoek te buiten. 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 gerelateerde voorzieningen

(bijvoorbeeld indien er gebruik gemaakt wordt van hetzelfde platform). Op die manier ontstaat er een beeld van de mate waarin de voorziening voldoet aan de standaarden.

Waar de antwoorden van de beheerder en PBLQ van elkaar afwijken, gaan we hierover met de beheerder in gesprek en mocht het verschil van mening blijven bestaan wordt daar melding van gemaakt in deze rapportage. In de toelichtingskolom geven de beheerders zo goed mogelijk aan of ze aan de standaard voldoen en of waarom niet.

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

Gebruik van internet.nl

Voor een groot aantal standaarden maken we gebruik 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 voor web- en emaildomeinen. Het gaat om de volgende standaarden:

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

Gebruik van RIPEstat

De standaard RPKI wordt getoetst met RIPEstat. Aan de hand van een IP-adres wordt getest in hoeverre de RPKI-standaard is doorgevoerd.

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

Webrichtlijnen en Digitoegankelijk

Op 24 mei 2018 is het Tijdelijk besluit digitale toegankelijkheid overheid gepubliceerd in het Staatsblad. Het besluit, dat de Europese toegankelijkheidsrichtlijn (2016/2102) omzet in bindende nationale regelgeving, is per 1 juli 2018 in werking getreden. Het doel is om de toegankelijkheid van websites en mobiele applicaties (apps) van overheidsinstanties te waarborgen. Het besluit maakt deel uit van een breder pakket aan maatregelen met als doel een inclusieve benadering van digitale overheidsdienstverlening. Uitgangspunt daarbij is dat mensen met en zonder beperking op gelijke basis moeten kunnen deelnemen aan de maatschappij. Als websites goed in elkaar zitten kunnen ze door iedereen worden gebruikt, ook door bezoekers met een beperking.

Concreet moeten overheden vanaf 23 september 2020 voldoen aan het besluit. Vanaf deze datum moeten overheidsinstanties de toegankelijkheidsnorm toepassen op al hun websites.

Als een website nog niet volledig toegankelijk is, moet de organisatie op basis van een gestructureerde aanpak binnen een redelijk haalbare termijn voldoen aan alle toegankelijkheidseisen. In een toegankelijkheidsverklaring, die is ondertekend door een bestuurder of een verantwoordelijk functionaris, wordt verklaard hoe ver de overheidsinstantie is gevorderd met de toegankelijkheid van de website.

Voor dit onderzoek is per voorziening gekeken of er een toegankelijkheidsverklaring in het openbare register is gepubliceerd. De toegankelijkheidsverklaring kent een nalevingsstatus. Deze geeft aan hoe ver een overheidsinstantie is gevorderd met het toegankelijk maken van een website en lopen uiteen van:

- Score A: Voldoet volledig
- Score B: Voldoet gedeeltelijk
- Score C: Eerste maatregelen genomen
- Score D: Voldoet niet
- Score E: Geen toegankelijkheidsverklaring gepubliceerd

In de tabel is per voorziening aangegeven welke score de toegankelijkheidsverklaring heeft, indien deze is opgenomen in het register. In Tabel 9 is die score, voor de vergelijkbaarheid met andere standaarden, als volgt vertaald: A = Voldoet, B = Deels, C = Gepland, rest = Niet.

ISO 27001/2 en de BIO

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

4.2. Overzicht: open standaarden in overheidsbrede voorzieningen

In Tabel 9a en 9b zijn de bevindingen over de overheidsbrede voorzieningen in één overzicht samengebracht. In de rapportage van PBLQ, opgenomen in Bijlage B4, wordt de mate waarin elke voorziening aan de relevante standaarden voldoet gedetailleerd besproken.

4.2.1. Per voorziening beschouwd

Dit jaar onderzoeken wij zoals gezegd 17 voorzieningen die vooral van belang zijn voor de gegevensuitwisseling en communicatie met burgers en bedrijven. Wij richten ons in deze paragraaf vooral op die 17 voorzieningen. Volgend jaar onderzoeken we opnieuw de 19 voorzieningen, die relevant zijn voor de gegevensuitwisseling en communicatie tussen overheden en de onderliggende infrastructuur. De cijfers (van vorig jaar) over deze 19 voorzieningen zijn – voor een completer beeld – wèl opgenomen in Tabel 9b verderop.

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

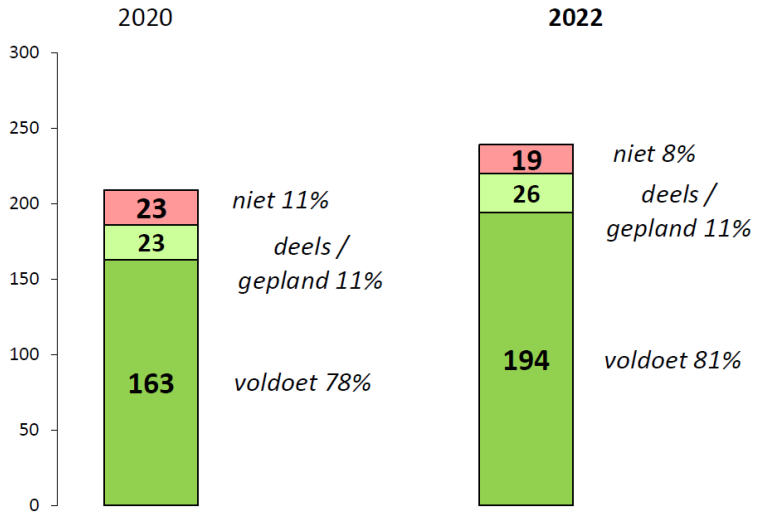
- de websites van Handelsregister (22 standaarden) en van RDW (20 standaarden),
- voor MijnOverheid (18 standaarden) en Overheid.nl (17 standaarden),
- en voor de website PDOK (geodata) en TenderNed (beide 16 standaarden.

Voor de 17 dit jaar onderzochte voorzieningen samen was in totaal 239 keer een open standaard relevant, dat is gemiddeld per voorziening 14,1 open standaarden.

In de meeste gevallen voldoen deze voorzieningen aan de relevante open standaarden. Vergeleken met twee jaar geleden is het percentage 'voldoet' nog iets gestegen van 78% naar 81%. Het aantal gevallen waarin de voorziening deels aan de standaard voldoet of daarvoor concrete plannen was dit jaar 11%, net als twee jaar geleden. Samen met het percentage dat 'voldoet' is dat voor dit jaar dus 92%.

Deze positieve ontwikkeling geldt niet alleen voor de percentages. Kijken we naar de absolute aantallen, dan is het beeld zeker zo positief. Er zijn dit jaar in totaal meer gevallen waarin een standaard voor een voorziening relevant is: in 2019 ging het om 209 gevallen, dit jaar om 239 gevallen.

Figuur 8: Dit jaar onderzocht: 17 voorzieningen
Relevant voor communicatie en gegevensuitwisseling met burgers en bedrijven



Het aantal keer 'voldoet' is gestegen van 163 naar 194 keer. Het aantal keer 'voldoet niet' is iets afgenomen van 23 tot 19. En het aantal keer 'deels/gepland' nam toe van 23 tot 26 keer.

Gezien de aard van deze 17 voorzieningen (communicatie en gegevensuitwisseling met burgers en bedrijven) is het niet verrassend dat het in bijna driekwart van de gevallen om standaarden uit het domein Internet & beveiliging gaat (174 keer). Daarnaast gaat het in 14% van de gevallen om standaarden uit het domein Document & webcontent (34 keer) en in 6% van de gevallen om het domein REST API's (14 keer). De 11 standaarden uit de domeinen Water & bodem, Bouw, Onderwijs & loopbaan en Overige waren voor geen enkele van de onderzochte 17 voorzieningen relevant.

Verschillende voorzieningen onderscheiden zich dit jaar in positieve zin:
- Het emaildomein van Rijksoverheid.nl voldoet aan alle 9 relevante standaarden.
- Zes voorzieningen voldoen 'bijna' aan alle standaarden, doordat zij aan een groot deel voldoen en aan de resterende standaarden deels voldoen, of dat gepland hebben. Dit geldt voor DigiD, DigiD Machtigen, PKI Overheid, Stelsel ETD, MijnOverheid en voor het webdomein van Rijksoverheid.nl.

In Tabel 9a (hierna) is een gedetailleerd overzicht opgenomen van de 17 voorzieningen die van belang zijn voor communicatie en gegevensuitwisseling met burgers en bedrijven, de daarvoor relevante open standaarden en de mate waarin de voorziening daaraan voldoet. Naar verwachting zullen deze voorzieningen in 2024 opnieuw worden onderzocht.

Ter aanvulling zijn daarna in Tabel 9b de 'oude' gegevens (uit het onderzoek van vorig jaar) opgenomen voor de 19 voorzieningen, die vooral gericht zijn op de communicatie en de gegevensuitwisseling tussen overheden onderling of de onderliggende infrastructuur. In 2023 zullen deze voorzieningen naar verwachting weer worden onderzocht.

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

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

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

Tabel 9a: Toepassing open standaarden in 17 voorzieningen die dit jaar onderzocht zijn

Relevant voor communicatie en gegevensuitwisseling met burgers en bedrijven

		I&A				D&I									G&R		D&V		
	V = voldoet *D = voldoet deels* *G = gepland* *N = voldoet niet* *(leeg = n.v.t.)*	DigiD	DigiD Machtigen	PKI Overheid	Stelsel ETD	MijnOverheid	Berichtenbox bedrijven	Overheid.nl	Ondernemersplein	Samenwerkende Catalogi	Rijksoverheid.nl - webdomein	Rijksoverheid.nl - emaildomein	*website* RDW.nl	*website* WOZ Waardeloket	*website* Handelsregister KvK	*website* PDOK (geodata)	TenderNed	Digi-Inkoop	*aantal keer relevant Tabel A:*
	aantal relevante OSn:	*13*	*13*	*11*	*14*	*18*	*13*	*17*	*12*	*9*	*11*	*9*	*20*	*11*	*22*	*16*	*16*	*14*	*23*
	DKIM	V			V	V	V	V				V	V		V	V	V	V	*11*
	DMARC	V	V	V	V	V	V	V	V	V		V	V	D	V	V	V	V	*16*
	DNSSEC	V	V	V	V	V	V	V	V		V	V	D	V	V	V	V	V	*16*
	HTTPS & HSTS	V	V	V	V	V	V	V	N	G	V		V	V	V	N	V	V	*16*
	IPv4 & IPv6	V	V	D	V	V	N	V	V	V	V	V	V	V	V	V	V	V	*17*
	NEN-ISO\IEC 27001	V	V	V	V	V		V	V		V	V	V	V	V	V	V	V	*15*
	NEN-ISO\IEC 27002	V	V	V	V	V		V	V		V	V	V	V	V	V	V	V	*15*
	NL GOV							V					V		N				*3*
	RPKI	V	V	V	V	V	V	N	V	V	V		V	V	N	V	V	N	*16*
	SAML	V	V		V	V	V						V		V		V		*8*
	SPF	V	V	V	V	V	V		V	G		V	V	V	V	V	V	V	*15*
	STARTTLS & DANE	V			V	G		V				V	N		N	V	V		*9*
	STIX en TAXII																		*0*
	TLS	V	V	V	V	V	V	V	V	G	V	V	V	N	V	V	V	V	*17*
	WPA2 Enterprise																		*0*
	AdES Baseline Profiles												G		V				*2*
	Digitoegankelijk	D	D	D	D	V	D	D	G	G	D		D	V	G	G	D	G	*16*
	ODF 1.2										V								*1*
	OWMS																		*0*
	PDF (NEN)		V	V	V	V	V	V			D		V	V	V		V	V	*12*
	SKOS							V					V		G				*3*
	OpenAPI Specification					V				N			V		D	V	N		*6*
	REST-API Design Rules					V		N	V	N			N		V	N	N		*8*
	NLCIUS												N		N			V	*3*
	SETU																	V	*1*
	WDO Datamodel																		*0*
	XBRL																		*0*
	Digikoppeling		D			V	V								V				*4*
	Geo-standaarden															V			*1*
	StUF					V	V								V	V			*4*
	Aquo-standaarden																		*0*
	GWSW																		*0*
	SIKB 0101																		*0*
	SIKB 0102																		*0*
	COINS																		*0*
	IFC																		*0*
	NLCS																		*0*
	VISI																		*0*
	BWB							V	V		V								*3*
	ECLI																		*0*
	JCDR							V											*1*
	e-Portfolio																		*0*
	NL_LOM																		*0*
	EML_NL																		*0*

Tabel 9b: Toepassing open standaarden in 19 andere voorzieningen (onderzocht in 2020)

(Deze standaarden worden in 2022 weer onderzocht.)

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

4.2.2. *Per standaard beschouwd*

Van alle 44 open standaarden op de 'pas toe of leg uit'-lijst zijn er 27 relevant voor één of meer van de dit jaar onderzochte voorzieningen. Er zijn 12 open standaarden die voor meer dan 9 van de 17 voorzieningen relevant zijn:

- IPv6+IPv4 en TLS (beide relevant voor alle 17 dit jaar onderzochte voorzieningen),
- DMARC, DNSSEC, HTTPS & HSTS, RPKI en DigiToegankelijk (alle vijf relevant voor 16 van de 17 voorzieningen),
- NEN-ISO\IEC 27001, NEN-ISO\IEC 27002 en SPF (15), PDF (12) en DKIM (11).

De mate waarin voorzieningen aan de standaard (als die relevant is) voldoen is hoog: voor 18 van de 27 standaarden die relevant zijn geldt dat tenminste 80% van de voorzieningen aan die standaard voldoet. Het gaat om de volgende 18 open standaarden:

- voor 10 van deze 14 standaarden geldt dat alle voorzieningen waarvoor deze standaard relevant is er aan voldoen; 4 van die standaarden zijn voor veel voorzieningen relevant: DKIM, NEN-ISO\IEC 27001, NEN-ISO\IEC 27002 en SAML; de andere 6 standaarden zijn voor een beperkter aantal voorzieningen relevant, maar die voldoen wel allemaal aan die standaard: ODF, SETU, Geo-standaarden, StUF, BWB en JCDR;
- de 8 open standaarden waaraan tussen 80% en 99% van de voorzieningen voldoet zijn: DMARC en DNSSEC (94%), SPF (93%), PDF (92%), IPv6+IPv4 en TLS (88%), HTTPS & HSTS en RPKI (81%).

Van deze 18 standaarden vallen er 11 in het domein ‘Internet & beveiliging’, de andere 7 zijn verspreid over de domeinen ‘Document & (web)content’ (2), ‘E-facturatie & administratie’ (1), de ‘Stelselstandaarden’ (2) en ‘Juridische verwijzingen’ (2).

Enkele standaarden scoren juist relatief laag: van de voorzieningen waarvoor deze relevant zijn voldoet slechts 13% (volledig) aan Digitoegankelijk, 33% aan NLCIUS en 38% aan REST-API Design Rules.

Tabel 10: Open standaarden relevant / voldoet, twee sets voorzieningen

	onderzocht in 2022: **17 voorzieningen: gegevensuitwisseling en communicatie burgers/bedrijven**			*vorig jaar onderzocht:* *19 voorzieningen: gegevensuitwisseling overheden en infrastructuur eronder*		
	Relevant in % van 17	**Voldoet** in % relevant	**V + D + G** in % relevant	Relevant in % van 19	Voldoet in % relevant	V + D + G in % relevant
Internet & beveiliging:						
DKIM	**65%**	**100%**	**100%**	68%	92%	92%
DMARC	**94%**	**94%**	**100%**	79%	87%	93%
DNSSEC	**94%**	**94%**	**100%**	84%	69%	94%
HTTPS & HSTS	**94%**	**81%**	**88%**	89%	41%	94%
IPv4 & IPv6	**100%**	**88%**	**94%**	95%	44%	78%
NEN-ISO\IEC 27001	**88%**	**100%**	**100%**	79%	100%	100%
NEN-ISO\IEC 27002	**88%**	**100%**	**100%**	79%	100%	100%
NL GOV	**18%**	**67%**	**67%**	53%	0%	0%
RPKI	**94%**	**81%**	**81%**	95%	72%	78%
SAML	**47%**	**100%**	**100%**	58%	55%	100%
SPF	**88%**	**93%**	**100%**	74%	93%	93%
STARTTLS & DANE	**53%**	**67%**	**78%**	58%	36%	55%
STIX en TAXII	**0%**			5%	100%	100%
TLS	**100%**	**88%**	**94%**	79%	67%	100%
WPA2 Enterprise	**0%**			0%		
Document & (web)content:						
AdES Baseline Profiles	**12%**	**50%**	**100%**	11%	100%	100%
Digitoegankelijk	**94%**	**13%**	**100%**	68%	0%	100%
ODF 1.2	**6%**	**100%**	**100%**	16%	67%	67%
OWMS	**0%**			37%	29%	29%
PDF (NEN)	**71%**	**92%**	**100%**	63%	58%	100%
SKOS	**18%**	**67%**	**100%**	47%	22%	89%
REST API's:						
OpenAPI Specification	**35%**	**50%**	**67%**	42%	88%	100%
REST-API Design Rules	**47%**	**38%**	**38%**	58%	18%	73%
E-facturatie & administratie:						
NLCIUS	**18%**	**33%**	**33%**	32%	0%	0%
SETU	**6%**	**100%**	**100%**	5%	100%	100%
WDO Datamodel	**0%**			0%		
XBRL	**0%**			5%	100%	100%
Stelselstandaarden:						
Digikoppeling	**24%**	**75%**	**100%**	84%	38%	94%
Geo-standaarden	**6%**	**100%**	**100%**	32%	100%	100%
StUF	**24%**	**100%**	**100%**	42%	75%	75%
Water & Bodem:						
Aquo-standaarden	**0%**			5%	100%	100%
GWSW	**0%**			0%		
SIKB 0101	**0%**			0%		
SIKB 0102	**0%**			0%		
Bouw:						
COINS	**0%**			0%		
IFC	**0%**			0%		
NLCS	**0%**			0%		
VISI	**0%**			0%		
Juridische verwijzingen:						
BWB	**18%**	**100%**	**100%**	11%	50%	100%
ECLI	**0%**			0%		
JCDR	**6%**	**100%**	**100%**	0%		
Onderwijs & loopbaan:						
e-Portfolio	**0%**			0%		
NL_LOM	**0%**			0%		
Overig:						
EML_NL	**0%**			0%		

5. Gegevens over het gebruik van open standaarden

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

Het 'pas toe of leg uit'-regime is gericht op de aanschaf van ICT, en dus op het toepassen van open standaarden bij toevoegingen aan en bij vernieuwingen van het ICT-systeem. Gegevens over het feitelijk gebruik geven een beeld voor het gehele ICT-systeem. Bovendien gaat het bij het 'pas toe of leg uit'-regime om het vragen om open standaarden, en daarbij 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 om (voor alle open standaarden) vast te stellen in welke mate die feitelijk gebruikt worden. Net als bij eerdere versies van de monitor beperkt dit het aantal standaarden waarover gegevens beschikbaar zijn.

Het opvragen van gegevens bij de verschillende beheerorganisaties is dit jaar wederom uitgevoerd door de accountmanagers van BFS. Vervolgens zijn de bevindingen vastgelegd in een kort verslag voor elk van de standaarden. Bundeling hiervan heeft geleid tot de notitie 'Inventarisatie gebruiksgegevens 2022 door BFS' (zie Bijlage B4).

Daarnaast doet BFS elk halfjaar onderzoek naar internetveiligheids-standaarden, een deel van de gebruiksgegevens is afkomstig uit de 'Meting Informatieveiligheidstandaarden overheid voorjaar 2022' dd. 26 augustus 2022 (zie Bijlage B5).

5.1. Gebruiksgegevens 2021: inventarisatie door accountmanagers BFS

In de notitie 'Inventarisatie gebruiksgegevens 2022 door FS' (zie Bijlage B4) 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 11 zijn de uitkomsten van deze inventarisatie samengevat.

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

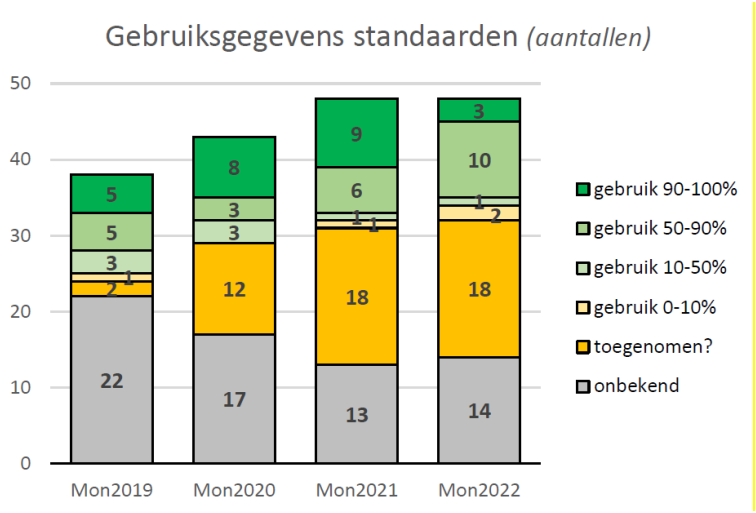
Tabel 11: Gebruiksgegevens 2022, per standaard

	Beeld BFS		Resultaten IV-meting
	ontwikkeling t.o.v. 2021	*gebruiksgegevens*	
Internet & beveiliging:			
DKIM	vergelijking niet mogelijk	82 %	82 %
DMARC policy	vergelijking niet mogelijk	72%	72 %
DNSSEC web	vergelijking niet mogelijk	89 %	89 %
en DNSSEC email	vergelijking niet mogelijk	57 %	57 %
HTTPS	vergelijking niet mogelijk	92 %	92 %
en HSTS	vergelijking niet mogelijk	57 %	57 %
IPv6 en IPv4 web	vergelijking niet mogelijk	70 %	70 %
en IPv6 en IPv4 email	vergelijking niet mogelijk	50 %	50 %
NEN-ISO\IEC 27001:2005nl	onduidelijk	[geen cijfers]	
NEN-ISO\IEC 27002:2007nl	onduidelijk	[geen cijfers]	
NL GOV Assurance	onduidelijk	[geen cijfers]	
RPKI	onduidelijk	beperkte cijfers	
SAML	onduidelijk	[geen cijfers]	
SPF policy	vergelijking niet mogelijk	87 %	87 %
STARTTLS	vergelijking niet mogelijk	81 %	81 %
en DANE	vergelijking niet mogelijk	46 %	46 %
STIX & TAXII	toegenomen	beperkte cijfers	
TLS	vergelijking niet mogelijk	75 %	75 %
WPA2 Enterprise	licht toegenomen	van 563 naar 587	
Document & (web)content:			
Ades Baseline Profiles	onduidelijk	[geen cijfers]	
Digitoegankelijk	licht toegenomen	beperkte cijfers	
ODF	beperkt gebruik	3 %	
OWMS	onduidelijk	[geen cijfers]	
PDF	stabiel	diverse indicatoren	
SKOS	stabiel	globale cijfers	
REST API's:			
OpenAPI Specification	onduidelijk	[geen cijfers]	
REST_API Design Rules	onduidelijk	[geen cijfers]	
E-facturatie & administratie:			
NLCIUS	toegenomen	globale cijfers	
SETU	licht toegenomen	globale cijfers	
WDO Datamodel	toegenomen	[geen cijfers]	
XBRL	stabiel	diverse indicatoren	
Stelselstandaarden:			
Digikoppeling	stabiel	91 %	
Geo−standaarden	toegenomen	diverse indicatoren	
StUF	toegenomen	diverse indicatoren	
Water & Bodem:			
Aquo Standaard	stabiel	diverse indicatoren	
GWSW	toegenomen	diverse indicatoren	
SIKB 0101	stabiel	[geen cijfers]	
SIKB 0102	toegenomen	[geen cijfers]	
Bouw:			
COINS	onduidelijk	[geen cijfers]	
IFC	beperkt gebruik	6% (nulmeting 2021)	
NLCS	licht toegenomen	[cijfers nog onduidelijk]	
Visi	licht toegenomen	diverse indicatoren	
Juridische verwijzingen:			
BWB	vergelijking niet mogelijk	[nauwelijks cijfers]	
ECLI	vergelijking niet mogelijk	[nauwelijks cijfers]	
JCDR	vergelijking niet mogelijk	[nauwelijks cijfers]	
Onderwijs & loopbaan:			
E−portfolio	onduidelijk	[nauwelijks cijfers]	
NL LOM	licht toegenomen	diverse indicatoren	
Overig:			
EML_NL	stabiel	[overal toegepast]	

Over de meeste standaarden uit het domein Internet & beveiliging zijn cijfers beschikbaar (dankzij de IV-meting). Veel van deze standaarden worden inmiddels door veel overheden gebruikt (meestal 80 à 90%, dus nog niet voor de door het OBDO nagestreefde 100%). Uitzonderingen zijn DANE (46%), IPv6& IPv4 web (50%), DNSSEC email en HSTS (beide 57%).

Doordat de opzet van de IV-meting is veranderd, is een vergelijking met voorgaande jaren niet goed mogelijk. Desondanks hebben wij de gebruiksgegevens van alle standaarden in Figuur 12 naast elkaar gezet. Doordat de IV-standaarden op een andere manier worden gemeten is het aantal standaarden met een hoog gebruik (90-100%) afgenomen en met een gebruik tussen 50% en 90% toegenomen. Daarnaast is voor 18 standaarden waarover geen harde gegevens beschikbaar zijn wel de indruk dat het gebruik toeneemt.

Figuur 12: Gebruiksgegevens over open standaarden (aantallen)



5.2. Gebruiksgegevens 2022: resultaten IV-meting

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

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

Uit de 'Meting Informatieveiligheidstandaarden overheid voorjaar 2022' (zie Bijlage B5, de uitkomsten zijn opgenomen in de rechterkolom van Tabel 11) blijkt dat het streefbeeld voor eind 2019 op het moment van de meting – twee jaar later – nog niet was gerealiseerd. Wel is de toepassing van een aantal standaarden gegroeid. Hierbij moet worden aangetekend dat de standaarden met ingang van dit jaar op een andere manier worden gemeten, met als gevolg lagere percentages. Zo worden HTTPS (92%), DNSSEC web (89%) en SPF Policy (87%) veel toegepast – maar nog niet voor 100%. Op enige afstand daarachter volgen DKIM (82%), DANE (81%), TLS (75%), DMARC Policy (72%) en IPv6& IPv4 email (70%).

BIJLAGEN

B1. Instructie Rijksdienst (inclusief toelichting)

B2. Overzicht van de beoordeelde aanbestedingen uit 2021

B3. Rapportage Open standaarden en voorzieningen (PBLQ)

B4. Inventarisatie gebruiksgegevens 2022 door BFS

B5. Rapportage IV-meting voorjaar 2022 (BFS)

B1. Instructie Rijksdienst (inclusief toelichting)

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

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

De Staatssecretaris van Economische Zaken,

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

Besluit:

Artikel 1

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

Artikel 2

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

Artikel 3

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

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

Den Haag, 8 november 2008

De Staatssecretaris van Economische Zaken,
F. Heemskerk.

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

Artikel 1 (definities)

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

Artikel 2 (adressaten)

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

Artikel 3 (pas toe of leg uit)

1. Bij de aanschaf van een ICT-dienst of ICT-product voor een toepassingsgebied dat voorkomt op de lijst die op de website www.forumstandaardisatie.nl is gepubliceerd, wordt gekozen voor een ICT-dienst of een ICT-product dat gebruikt maakt van een bij het desbetreffende toepassingsgebied vermelde open standaard.

2. Van het eerste lid kan worden afgeweken indien een dergelijke dienst of product naar verwachting in onvoldoende mate wordt aangeboden, onvoldoende veilig of zeker functioneert, of om andere redenen van bijzonder gewicht.

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

Artikel 4 (naleving)

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

Artikel 5 (inwerkingtreding wijzigingen lijst)

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

TOELICHTING

Algemeen

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

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

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

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

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

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

Artikelsgewijs

Artikel 1

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

Artikel 3

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

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

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

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

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

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

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

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

De Staatssecretaris van Economische Zaken,
F. Heemskerk.

B2. Overzicht van de beoordeelde aanbestedingen uit 2021

De 32 aanbestedingen van Rijk en uitvoeringsorganisaties en de 35 van mede-overheden die dit jaar zijn beoordeeld zijn in Tabel B2.1 en Tabel B2.2 opgesomd, met een korte omschrijving van het onderwerp van de aanbesteding, de open standaarden die de beoordelaars relevant achten en de uiteindelijke beoordeling. Hiervoor is de volgende indeling gehanteerd (conform Hoofdstuk 3):

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

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

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

Tabel B2.1 Overzicht van beoordeelde aanbestedingen Rijk en uitvoeringsorganisaties

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
Sociale Verzekeringsbank	Het doel van de aanbesteding is om een Overeenkomst te sluiten met één Dienstverlener voor de levering van WAN- en internetconnectiviteit en aanverwante dienstverlening. De WAN- en internetverbindingen moeten veilig, betrouwbaar en schaalbaar zijn en goede prestaties bieden. Het betreft het leveren en onderhouden van een beveiligd en privaat WAN netwerk.	ISO 27001 ISO 27002 HTTPS & HSTS TLS IPv4 & IPv6 DNSSEC		perfect	100%
Kamer van Koophandel	Het mogelijk maken om te 'vergelijken op NAW'. Klanten die KVK een overzicht bedrijven, stichtingen en/of rechtspersonen aanleveren, zonder nadere identificerende gegevens (o.a.	ISO 27001		perfect	100%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
	KVk-nr, vestigingsnummer, subdossiernummer) wordt bij de opdrachtnemer gematcht en vergeleken.	ISO 27002			
Tweede Kamer der Staten Generaal	Doel is om een overeenkomst met één contractpartij af te sluiten voor het applicatie-beheer van meerdere applicaties. Hosting van de applicaties doet de Tweede Kamer zelf.	ISO 27001 ISO 27002		perfect	100%
Ministerie van SoZaWe	De doelstelling van de aanbesteding is het contracteren van een betrouwbare, ervaren en kundige leverancier van softwarepakketten. Het contract met een leverancier moet leiden tot een geïmplementeerde en adequaat onderhouden applicatie die alle subsidie uitvoeringsvarianten ondersteunt en wordt geintegreert in het dan bestaande ICT-landschap. De onderdelen van de applicaties zijn het klantportaal, zaakmanagement, relatiemanagement en documentmanagement.	ISO 27001 ISO 27002 HTTPS & HSTS TLS IPv4 & IPv6 DNSSEC SPF DKIM DMARC STARTTLS & DANE PDF SAML ODF Digitoegankelijk BWB	Digikoppeling	op de goede weg; op weg naar perfect	94%
Ministerie van VWS	Hosting van (initieel) vier OTAP omgevingen voor corona gerelateerde applicaties.	ISO 27001 ISO 27002	STIX TAXII	op de goede weg; op weg naar perfect	80%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
		IPv4 & IPv6 SAML			
Kadaster	Het betreft een aanbesteding waarin ze een toekomst vaste ESM Oplossing uitvragen ter vervanging van de huidige Enterprise Service Management oplossing. Opdrachtnemer dient zorg te dragen voor stabiliteit en continuïteit van de gevraagde opdracht.	ISO 27001 ISO 27002 HTTPS & HSTS TLS DNSSEC SPF DKIM DMARC STARTTLS & DANE SAML	IPv4 & IPv6 Digitoegankelijk NL GOV OpenAPI spec. REST-API DR	op de goede weg: op weg naar perfect	67%
RWS	Het leveren van een Platvorm as a service (PAAS) oplossing t.b.v. het verstrekken van video-beelden van 26 specifieke locaties langs rijkswegen in Nederland, met als doel de weggebruiker en medewerkers van het Verkeerscentrum Nederland te voorzien van live videobeelden op een aantal specifieke wegvakken in Nederland.	ISO 27001 ISO 27002 HTTPS & HSTS TLS	DNSSEC IPv4 & IPv6	op de goede weg: op weg naar perfect	67%
RWS	Het leveren van service en support aan wifi-systemen op minimaal 5 tot 11 schepen van de Rijksrederij. Bij een eventuele uitbreiding ontstaat ook behoefte aan levering en installatie van wifi apparatuur op de nieuw bij het netwerk aan te sluiten schepen.	ISO 27001 ISO 27002	WPA2-Enterprise	op de goede weg: op weg naar perfect	67%
UWV	Het versturen van berichten naar mobiele telefoons. Aanbesteder beoogt derhalve met deze	ISO 27001	SPF	op de goede weg: middenmoot	64%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
	opdracht om op een efficiënte en kosteneffectieve wijze te communiceren met de doel-groepen waarop de dienst-verlening van UWV zich richt	ISO 27002 HTTPS & HSTS TLS IPv4 & IPv6 DNSSEC SAML	DKIM DMARC STARTTLS & DANE		
Sociale Verzekeringsbank	Een oplossing die ervoor zorgt dat de data uit de bronsystemen op snelle en geautomatiseerde wijze verwerkt worden in duidelijke, volledige, inhoudelijk correcte correspondentie over de gevalsbehandeling en die vervolgens via verschillende kanalen naar de ontvanger kan worden verstuurd. De SVB vraagt een oplossing uit die bestaat uit standaardsoftware in de vorm van Software-as-a-Service (SaaS). Betreft ook routering van berichten richting Berichtenbox en MijnOverheid.	ISO 27001 ISO 27002 HTTPS & HSTS TLS PDF SAML Digitoegankelijk Digikoppeling	IPv4 & IPv6 DNSSEC OpenAPI spec. REST-API DR NL GOV	op de goede weg: middenmoot	62%
Ministerie van Defensie	Deze aanbesteding bestaat uit 2 percelen: 1) Replacement of the Coast Guard RCS, connecting to the (existing) transmit-receive stations and making way for expansion of the transceiver pool and sites; 2) Conversion of the E1 lines to E1-over-IP. Deze beoordeling betreft perceel 2/B, waarvoor o.a. eisen in bijv. H6 niet van toepassing zijn. De huidige RCS installatie is verouderd. De huidige E1 lijnen worden 1 april 2022 uitgefaseerd. Voor die tijd	ISO 27001	IPv4 & IPv6	op de goede weg: middenmoot	60%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
	moeten ze omgezet zijn in E1-over-IP lijnen.	ISO 27002 PDF	ODF		
RWS	Capaciteitsonderzoek rijkswegen 2021 t/m 2024: opstellen en opleveren van verkeersgegevens met betrekking tot vooral bij Rijkswaterstaat in beheer zijnde wegen, ten behoeve van het optimaliseren van het wegontwerp, het bijdragen aan dynamisch verkeersmanagement en aan het voorzien in data voor verkeersmodellen, de planning van wegwerkzaamheden, alsmede in zijn algemeenheid het bijdragen aan een robuust hoofdwegennet.	ODF PDF Digitoegankelijk	ISO 27001 ISO 27002	op de goede weg: middenmoot	60%
Stichting Samenwerking Beroepsonderwijs Bedrijfsleven	Het leveren van: - het gebruiksrecht (licenties) voor een integrale, standaard bedrijfsvoering applicatie (SBB vervangt niet het CRM systeem voor het primaire proces); - de hosting van de applicatie en het (via Internet en browser) beschikbaar stellen aan gebruikers; - beheer en onderhoud; - de ondersteuning bij het gebruik en beheer door SBB van de applicatie (helpdesk); - de salarisverwerking en uitbetaling van salarissen en vergoedingen; - meedenken over het meerjarenperspectief en het bieden van een natuurlijke adviesfunctie richting SBB.	ISO 27001 ISO 27002 HTTPS & HSTS TLS SAML PDF Digikoppeling NLCIUS	ODF DNSSEC IPv4 & IPv6 SPF DKIM DMARC STARTTLS & DANE	op de goede weg: middenmoot	59%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
		Digitoegankelijk XBRL			
KvK	Met het oog op de veiligheid van haar werknemers wil KVK, naast het voldoen aan haar wettelijke verplichtingen, haar BHV organisatie verder professionaliseren. Belangrijk is hierbij aandacht voor continuïteit en uniformiteit, zodat BHV-ers van verschillende locaties elkaar eenvoudig kunnen vervangen. Het betreft ook leveren en beheren van een app.	DNSSEC HTTPS & HSTS TLS ISO 27001 ISO 27002 Digitoegankelijk SAML	IPv4 & IPv6 SPF DKIM DMARC STARTTLS & DANE NL LOM	op de goede weg: middenmoot	54%
Ministerie EZK / RVO	Het betreft het digitaliseren van de post die RVO ontvangt. Post komt in postzakken op de RVO locatie binnen. Na een beperkte sortering worden de te digitaliseren poststukken ongeopend in postzakken (per dag, per ontvangstwijze) aan de opdrachtnemer ter beschikking gesteld. De opdrachtnemer draagt zorg voor het digitaliseren van deze poststukken. Metadatering maakt onderdeel uit van de opdracht. Opdrachtnemer moet ook de Classificatiemodule leveren. Dit is de digitale online tool waarin medewerkers de gescande stukken kunnen benaderen.	ISO 27001 ISO 27002 HTTPS & HSTS TLS DNSSEC PDF SAML	SPF DKIM DMARC STARTTLS & DANE IPv4 & IPv6 ODF	op de goede weg: middenmoot	54%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
UWV	Deze aanbesteding betreft het vervangen van de huidige brievenboeksystemen door één gemeenschappelijke voorziening voor E-Publicatie voor de gehele organisatie die het mogelijk maakt om formele gepersonaliseerde communicatie-uitingen aan de klant (kanaalonafhankelijk) te creëren, op te maken en samen te voegen. Brievenboeksystemen zijn geautomatiseerde systemen waarmee brieven worden gemaakt en naar klanten worden gestuurd. De opdracht omvat het leveren van de Voorziening E-Publicatie, implementatie van de software, en beheer en onderhoud van de software.	ISO 27001 ISO 27002 HTTPS & HSTS TLS PDF Digitoegankelijk NL GOV	IPv4 & IPv6 DNSSEC SPF DKIM DMARC STARTTLS & DANE SAML	op de goede weg: middenmoot	50%
Ministerie van BuZa	The Shared Service Organization 3W of the ministry of Foreign Affairs has the intention to find a contractor who can provide payroll management services either independently or through subcontractors or consortium members for the embassies and consulates in Eastern-Europe. The Contracting authority expects one web-based platform for its access to information.	ISO 27001 ISO 27002 HTTPS & HSTS TLS PDF DNSSEC	IPv4 & IPv6 SPF DKIM DMARC STARTTLS & DANE ODF	op de goede weg: middenmoot	50%
Belastingdienst	Deze aanbesteding heeft als doel een overeenkomst af te sluiten met één contractpartner voor het middels een SaaS-dienst beschikbaar stellen van	ISO 27001	IPv4 & IPv6	op de goede weg: middenmoot	50%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
	een Online security awareness game (OSAG Dienst). De prestatie omvat naast het beschikbaar stellen van de OSAG Dienst ook de levering van additionele diensten.	ISO 27002 HTTPS & HSTS TLS PDF SAML	DNSSEC SPF DKIM DMARC STARTTLS & DANE		
Ministerie VWS	Het klantcontactcentrum (KCC) is het centrale klantenloket van het CIBG. Hier worden de klanten (burgers, professionals en organisaties) geïnformeerd. De klantvragen komen via diverse kanalen binnen en worden ook via diverse kanalen beantwoord (zoals telefoon, mail, balie, webcare, brief). De uitdaging is om een geïntegreerde oplossing (een Customer Care platform) te realiseren voor het KCC, waarin een verbetering van het klantcomfort centraal staat.	ISO 27001 ISO 27002 HTTPS & HSTS TLS PDF Digitoegankelijk DNSSEC	IPv4 & IPv6 SPF DKIM DMARC STARTTLS & DANE SAML ODF	op de goede weg: middenmoot	50%
RDW	Het betreft een aanbesteding van een SaaS oplossing op het gebied van Identity & Access management. De RDW wenst middels een generiek IAM oplossing + bijbehorende dienstverlening, een optimale situatie te realiseren ten aanzien van gebruik en beheer van digitale identiteiten voor RDW om zodoende een veilig en verantwoord gebruik van digitale RDW diensten te kunnen realiseren.	ISO 27001 ISO 27002 HTTPS & HSTS	IPv4 & IPv6 SPF DKIM	op de goede weg: middenmoot	50%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
		TLS SAML DNSSEC	DMARC STARTTLS & DANE NL GOV		
LVNL	LVNL is op zoek naar een centraal, gebruiksvriendelijk en toekomstbestendig systeem dat de betrokken medewerkers bij het brevetteringsproces ondersteunt in het monitoren, plannen en registreren van de vakbekwaamheidsprogramma's . Het betreft een SaaS oplossing.	ISO 27001 ISO 27002 HTTPS & HSTS TLS DNSSEC	IPv4 & IPv6 SPF DMARC DKIM STARTTLS & DANE E-portfolio NL SAML	op de goede weg: middenmoot	42%
Raad voor Rechtsbijstand	Het leveren, implementeren en beheren van een standaard piketapplicatie (roosteren, plannen en melden) voor het verlenen van rechtsbijstand door de Raad voor Rechtsbijstand. Per kalenderdag sturen ketenpartners (Politie, KMAR, DT&V, IND, AVIM, Burgemeesters, OM en Rechtbanken) gemiddeld 350 piketmeldingen die terecht moeten komen bij de juiste advocaat.	ISO 27001 ISO 27002 HTTPS & HSTS TLS Digitoegankelijk	DNSSEC IPv4 & IPv6 SPF DKIM DMARC STARTTLS & DANE SAML	op de goede weg: middenmoot	42%
NPO	Het betreft de inkoop van software en licenties voor een muziek-schedulingsysteem. Dit zijn specialistische applicaties waarmee de muziekredacties van de NPO-radiozenders voor elk programma automatisch een speellijst laten samenstellen die tijdens dat programma wordt	ISO 27001	IPv4 & IPv6	op de goede weg: nog een heel eind te gaan	27%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
	uitgezonden. Verder behoren implementatiewerkzaamheden en supportwerkzaamheden van de software binnen de scope van de aanbesteding.	ISO 27002 PDF	SPF DKIM DMARC STARTTLS & DANE DNSSEC HTTPS & HSTS TLS		
Stichting Samenwerking Beroepsonderwijs Bedrijfsleven	De levering van vaste telefonie diensten, telefonie- en omnichannel callcenterfunctionaliteit en de integratie van de omnichannel callcenter applicatie met Microsoft Dynamics365 van en voor aanbestedende dienst.	ISO 27001 ISO 27002 IPv4 & IPv6	HTTPS & HSTS TLS DNSSEC SPF DKIM DMARC STARTTLS & DANE ODF	op de goede weg: nog een heel eind te gaan	27%
Instituut Fysieke Veiligheid	Het IFV beschikt op dit moment over een eigen website: www.IFV.nl, die is ontwikkeld in SharePoint 2013. Dat platform wordt na april 2022 niet meer wordt ondersteund. Het IFV wil zijn website vernieuwen en heeft daarbij in lijn met de keuze van zijn opdrachtgevers en klanten (brandweer en veiligheidsregio's in Nederland) gekozen voor het open source WCMS-platform Wordpress.	ISO 27001 ISO 27002 Digitoegankelijk	HTTPS & HSTS TLS IPv4 & IPv6 DNSSEC SPF DKIM DMARC	op de goede weg: nog een heel eind te gaan	27%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
			STARTTLS & DANE		
Ministerie van BZK	De levering van eerstelijns contactcenterdiensten voor Logius. Hiertoe behoort o.a. het inrichten van de, voor de dienstverlening relevante, eigen systemen, en het koppelen met de relevante Logius systemen.	ISO 27001 ISO 27002 PDF	IPv4 & IPv6 ODF DNSSEC HTTPS & HSTS TLS SPF DKIM DMARC STARTTLS & DANE	op de goede weg: nog een heel eind te gaan	25%
Ministerie van Financiën	Denmark, Luxembourg, the Netherlands and Sweden (the Eurovignette Treaty Member States) are levying a user charge for the use of motorways by heavy goods vehicles (> or = 12 tons), the so called 'Eurovignette'. With this Tender, the Member States want to tender a common system for the Eurovignette charges. This common system is based on several booking channels: web based on-line bookings, interface bookings (bookings via fleet and fuel card issuers and two Member States) and terminal bookings.	ISO 27001 ISO 27002 Digitoegankelijk	IPv4 & IPv6 DNSSEC SPF DKIM DMARC STARTTLS & DANE HTTPS & HSTS TLS XBRL WDO Datamodel	op de goede weg: nog een heel eind te gaan	23%
Ministerie van I&W	Deze aanbesteding betreft het beheer, onderhoud en	ISO 27001	HTTPS & HSTS	op de goede weg: nog een	18%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
	doorontwikkeling van KNMI.nl en de Extranetten (omgeving met dashboards voor zakelijke afnemers) die het KNMI aanbiedt. Het betreft beheer, onderhoud en doorontwikkeling op basis van de huidige techniek. Ruby on Rails in combinatie met Active Admin CMS voor KNMI.nl, en React.js (frontend) en PHP (backend) voor Extranetten. Hosting wordt door de opdrachtnemer uitgevoerd op het door de KNMI ingerichte AWS Platform.	ISO 27002	TLS IPv4 & IPv6 DNSSEC SPF DKIM DMARC STARTTLS & DANE Digitoegankelijk	heel eind te gaan	
Prorail	Levering en bediening van een Traffic Generator and Application Simulator ETCS voor GSM-R voor het uitvoeren van testen. Inclusief beheer, onderhoud en opleiding van de applicatie.		HTTPS & HSTS TLS IPv4 & IPv6 DNSSEC	slecht	(n.v.t.)
Ministerie van I&W	Nationale Databank Wegverkeersgegevens zoekt een opdrachtnemer die een aantal van haar missie-kritische applicaties en verbindingen richting deze applicaties 24/7 gaat monitoren en daarop wanneer benodigd actie onderneemt richting afgesproken partijen.		ISO 27001 ISO 27002 HTTPS & HSTS TLS SPF DKIM DMARC	slecht	(n.v.t.)

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
			STARTTLS & DANE		
Politie	De opdracht behelst de levering van software en aanvullende dienstverlening voor analyse en classificatie van aan kinderporno (KP) gerelateerd beeldmateriaal.		ISO 27001 ISO 27002	slecht	(n.v.t.)
NPO	A player that allows streaming audio and video content from the public broadcasters to be displayed on npo touchpoints. Such as NPO Start, Sites & apps, BVN, broadcasting sites etc. The Player must enable the widest possible formats of audio and video. The Player will be functionally the same for all platforms.		HTTPS & HSTS TLS IPv4 & IPv6 Digitoegankelijk OpenAPI Spec. REST-API DR	slecht	(n.v.t.)

Tabel B2.2 Overzicht van beoordeelde aanbestedingen Mede-overheden

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
Gemeente Gorinchem	De levering, inrichting en beheren van een nieuw e-HRM systeem (SaaS-oplossing). Daarnaast wenst de gemeente de volledige ondersteuning bij de implementatie en de koppelingen met omringende applicaties. Vervolgens is de opdrachtnemer verantwoordelijk voor het verzorgen van scholing, support en advies.	DNSSEC ISO 27001 ISO 27002 HTTPS & HSTS TLS SAML PDF DKIM DMARC SPF STARTTLS & DANE IPv4 & IPv6		perfect	100%
Gemeente Etten-Leur	Het leveren van: (1) Data- en servicediensten waaronder (a) een Container Management Systeem, (b) een Servicepunt Afval voor de inwoners, (c) een Afval informatiewebsite met Inwoner Portaal afvalregistraties, (d) een Afval informatie App en (2) Technische servicediensten, namelijk het ter onderhoud/ vervanging/reparatie innemen, afvoeren, aanvullend leveren en uitzetten minicontainers van diverse inhoudsmaten, incl. chips (voor Restafval, GFT-afval en OPK-afval) en identificatiesticker.	HTTPS & HSTS TLS DNSSEC SPF DKIM DMARC STARTTLS & DANE IPv4 & IPv6 StUF ISO 27001 ISO 27002 Digitoegankelijk		perfect	100%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
		PDF			
Gemeente Heerde	Een standaard (off-the-shelf) Zaaksysteem en aanverwante applicatiefuncties met aanvullend een aantal specifieke koppelingen en diensten.	ISO 27001 ISO 27002 HTTPS & HSTS TLS SPF DKIM DMARC STARTTLS & DANE DNSSEC IPv4 & IPv6 StUF SAML Digitoegankelijk Digikoppeling		perfect	100%
Gemeente Heerhugowaard	Er is behoefte aan een applicatie Gegevensdistributie & Servicebus die de volgende kerntaken dient te ondersteunen: (1) een uitschrijving van de scope is te vinden in het programma van eisen en wensen, (2) een strippenkaart voor 5 dagen per jaar ondersteuning op functioneel gebied; (3) implementatie diensten rond de fusie Heerhugowaard-Langedijk en (4) onderhoudsovereenkomst en beheer voor de duur van de overeenkomst..	ISO 27001 ISO 27002 HTTPS & HSTS TLS SPF DKIM DMARC STARTTLS & DANE DNSSEC IPv4 & IPv6 StUF SAML Digitoegankelijk		perfect	100%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
		Digikoppeling			
Provincie Flevoland	De vervanging van het financiële systeem inclusief koppelingen middels een software as a service (SAAS) oplossing.	ISO 27001 ISO 27002 HTTPS & HSTS TLS SPF DKIM DMARC STARTTLS & DANE DNSSEC IPv4 & IPv6 ODF PDF Digitoegankelijk SAML NLCIUS XBRL Ades baseline prof.	Digikoppeling	op de goede weg: op weg naar perfect	94%
SED Organisatie	Binnenkort wordt het zaak-systeem van de SED organisatie en de gemeenten Drechterland, Enkhuizen en Stede Broec niet meer ondersteund. Het zaak-systeem wordt ook gebruikt bij het Recreatieschap Westfriesland en Afvalbeheer Westfriesland, waaraan de SED organisatie op een aantal vlakken ondersteuning verleend. In deze overgangsperiode tussen traditioneel zaakgericht werken en werken volgens Common Ground zoekt de SED organisatie een partner om de levering van en aanvullende dienstverlening rond het zaaksysteem voort te zetten.	ISO 27001 ISO 27002 HTTPS & HSTS TLS SPF DKIM DMARC STARTTLS & DANE	SAML	op de goede weg: op weg naar perfect	93%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
		DNSSEC IPv4 & IPv6 StUF Digitoegankelijk PDF			
Gemeente Waddinxveen	De gemeente wil de digitale dienstverlening en het digitaal werken zo optimaal mogelijk kunnen ondersteunen met een zaak- en archiefsysteem.	ISO 27001 ISO 27002 HTTPS & HSTS TLS SPF DKIM DMARC STARTTLS & DANE DNSSEC IPv4 & IPv6 StUF SAML Digitoegankelijk Digikoppeling	PDF	op de goede weg: op weg naar perfect	93%
Gemeente Dordrecht	Het leveren, implementeren en onderhouden van een subsidiebeheersysteem.	ISO 27001 ISO 27002 HTTPS & HSTS TLS IPv4 & IPv6 SPF DKIM DMARC STARTTLS & DANE PDF DNSSEC SAML StUF STIX en TAXII	ODF	op de goede weg: op weg naar perfect	93%
Servicecentrum MER	Het werkend opleveren en vervolgens ter beschikking stellen, inclusief onderhouden en ondersteunen, van een ICT-oplossing voor een HR-systeem met een inrichting voor drie	ISO 27001	SAML	op de goede weg: op weg naar perfect	87%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
	gemeenten en 1 serviceorganisatie, te weten Maasgouw, Echt-Susteren, Roerdalen en Servicecentrum MER, inclusief het uitvoeren van de salarisverwerking.	ISO 27002 HTTPS & HSTS TLS SPF DKIM DMARC STARTTLS & DANE DNSSEC IPv4 & IPv6 StUF PDF ODF	Digitoegankelijk		
Waterschap Brabantse Delta	De implementatie en het beheer ten aanzien van Plan- en Regelsoftware Digitaal Stelsel Omgevingswet.	ISO 27001 ISO 27002 HTTPS & HSTS TLS SPF DKIM DMARC STARTTLS & DANE DNSSEC SAML STIX en TAXII Digikoppeling	IPv4 & IPv6 BWB	op de goede weg: op weg naar perfect	86%
Gemeente Breda	De opdracht omvat het leveren, installeren en in stand houden van een systeem ten behoeve van camerahandhaving voor gemeente Breda ('all-in prijs').	DNSSEC ISO 27001 ISO 27002 HTTPS & HSTS TLS IPv4 & IPv6 SPF DKIM DMARC	SAML PDF	op de goede weg: op weg naar perfect	85%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
		STARTTLS & DANE Digikoppeling			
Gemeente Groningen	In deze aanbesteding wordt gevraagd om het leveren en plaatsen van repro-apparatuur inclusief alle bijbehorende software. Daarbij verder: onderhoud van de repro-apparatuur, het leveren en implementeren van ondersteunende software, het up-to-date houden van de software, opleiden en trainen van de gebruikers en het leveren van verbruiksmaterialen exclusief papier.	HTTPS & HSTS TLS ISO 27001 ISO 27002 PDF	IPv4 & IPv6	op de goede weg: op weg naar perfect	83%
Gemeente 's Hertogenbosch	Een nieuw financieel systeem dat de medewerkers, zowel de financiële medewerkers als de niet financiële medewerkers, moet ondersteunen in de rechtmatige, juist en volledige uitvoering van de werkzaamheden.	HTTPS & HSTS TLS SPF DKIM DMARC STARTTLS & DANE DNSSEC IPv4 & IPv6 PDF SAML	ISO 27001 ISO 27002 XBRL ODF	op de goede weg: op weg naar perfect	71%
Gemeente Nissewaard	De levering en de bijhorende dienstverlening van een digitale applicatie ten aanzien van parkeervergunningen en de bezoekersregeling.	ISO 27001 ISO 27002 PDF HTTPS & HSTS TLS IPv4 & IPv6	SAML SPF DKIM DMARC STARTTLS & DANE	op de goede weg: midden-moot	64%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
		DNSSEC Digitoegankelijk StUF			
Provincie Gelderland	De Opdracht bevat de volgende drie hoofdonderdelen: 1. Het opstellen en laten valideren van plankaarten voor reguliere publieke laadinfrastructuur (personenauto's, deelauto's, taxi's, bestelbusjes) voor 3 jaar vooruit tot en met 2025 voor 77 gemeenten in NAL-regio Oost. 2. Het (op)leveren en beheren van een technische oplossing voor het visueel maken van de plankaarten en die ter beschikking stellen aan de NAL-regio Oost en diens 77 inliggende gemeenten. 3. Het integreren van de technische oplossing met andere externe systemen, waaronder die met een aanvraag- en monitoringsportal, lokale GIS systemen en systemen van de netbeheerders.	Digitoegankelijk	ISO 27001	op de goede weg: middenmoot	63%
		DNSSEC HTTPS & HSTS TLS SPF DKIM DMARC STARTTLS & DANE IPv4 & IPv6 PDF	ISO 27002 ODF Geo standaarden OpenAPI spec. REST-API DR		
Gemeente Roosendaal	De levering, implementatie en beheer van een financieel systeem volgens het SaaS-principe met bijbehorende dienstverlenging.	ISO 27001	HTTPS & HSTS	op de goede weg: middenmoot	58%
		ISO 27002 DNSSEC SPF DKIM DMARC STARTTLS & DANE	TLS IPv4 & IPv6 PDF XBRL		

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
Gemeente Eindhoven	Vervanging van het uitgaand subsidiesysteem, bestaande uit: (1) het ondersteunen van het subsidieverstrekkingsproces middels een passende applicatie, (2) de mogelijkheden voor het koppelen van deze applicatie met bestaande applicatie van de gemeente Eindhoven (hoe past het in het applicatielandschap?) en (3) de wijze waarop implementatie van de betreffende applicatie plaatsvindt (denk aan applicatie inrichting, training/opleiding, datamigratie)	ISO 27001 ISO 27002 HTTPS & HSTS TLS DNSSEC Digikoppeling SAML StUF	IPv4 & IPv6 SPF DKIM DMARC STARTTLS & DANE Digitoegankelijk PDF OpenAPI spec. REST-API DR	op de goede weg: middenmoot	47%
Gemeente Zaanstad	Het volledig bedrijfsklaar installeren, opleveren, afleveren en onderhouden van een systeem of systemen voor mobiele scanapparatuur en -software, opgebouwd op een door de gemeente Zaanstad te leveren elektrische auto, waarmee door middel van het scanvoertuig de controle van het betaald parkeren gebied wordt uitgevoerd.	HTTPS & HSTS TLS ISO 27001 ISO 27002 SAML Digitoegankelijk	DNSSEC IPv4 & IPv6 PDF SPF DKIM DMARC STARTTLS & DANE	op de goede weg: middenmoot	46%
Gemeente Den Haag	Burgers moeten al hun zaken met de overheid vooral digitaal kunnen afhandelen. Veel informatie ontstaat daarom digitaal en moet digitaal worden opgeslagen en beheerd. Het werken met 'digitaal geboren' informatie vereist een andere werkwijze en andere kennis dan	ISO 27001	IPv4 & IPv6	op de goede weg: middenmoot	46%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
	bij papieren archieven. Om digitale collecties in de toekomst duurzaam en betrouwbaar te beheren en beschikbaar te stellen werkt de gemeente aan een nieuwe bewaaromgeving: het e-depot.	ISO 27002 HTTPS & HSTS TLS OpenAPI spec. REST-API DR	DNSSEC SPF DKIM DMARC STARTTLS & DANE PDF		
Bizob	De levering, inrichting en het onderhoud van back-up en restore voorzieningen ten behoeve van de ICT-systemen van de GGD.	ISO 27001 ISO 27002	HTTPS & HSTS TLS IPv4 & IPv6	op de goede weg: middenmoot	40%
Gemeente Geldrop-Mierlo	Het werkend opleveren en vervolgens ter beschikking stellen van een burgerzakenapplicatie, inclusief onderhoud en ondersteuning.	Digikoppeling ISO 27001 ISO 27002 SAML StUF IPv4 & IPv6	DNSSEC HTTPS & HSTS TLS SPF DKIM DMARC STARTTLS & DANE PDF Digitoegankelijk	op de goede weg: middenmoot	40%
BAR-organisatie	De levering van alle benodigde hard- en software en de ondersteunende diensten voor het mogelijk maken van een Raadsinformatiesysteem.	HTTPS & HSTS TLS PDF SAML	ISO 27001 ISO 27002 DNSSEC SPF DKIM DMARC STARTTLS & DANE IPv4 & IPv6 ODF	op de goede weg: nog een heel eind te gaan	31%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
Waterschap Vallei en Veluwe	Het leveren en netwerkdiensten, onder te verdelen in: 1. IP-VPN netwerkdiensten; 2. APN netwerkdiensten voor IoT diensten. Verder het leveren van Support in de vorm van een Webportaal voor het beheer en management van de netwerkdiensten en transitiemanagement voor een naadloze en tijdige transitie van het huidige netwerk naar het nieuwe netwerk.	ISO 27001 ISO 27002 PDF	HTTPS & HSTS TLS SPF DKIM DMARC DNSSEC IPv4 & IPv6 STARTTLS & DANE	op de goede weg: nog een heel eind te gaan	27%
Provincie Gelderland	Het leveren, implementeren en beheren van een Nieuw Personeels- en Salarissysteem.	ISO 27001 ISO 27002 Digitoegankelijk	DNSSEC HTTPS & HSTS TLS SPF DKIM DMARC STARTTLS & DANE IPv4 & IPv6 PDF	op de goede weg: nog een heel eind te gaan	25%
Noord-Hollands Archief	De opdracht betreft ICT-dienstverlening en bestaat uit de volgende onderdelen: werkplekbeheer, servicedesk, beveiligingsdiensten, technisch beheer en beheer van de WAN-verbindingen.	ISO 27001 ISO 27002 SAML	IPv4 & IPv6 DNSSEC HTTPS & HSTS TLS SPF DKIM DMARC STARTTLS & DANE	op de goede weg: nog een heel eind te gaan	25%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
			PDF		
Gemeente Den Haag	Tijdens de raads- en commissievergaderingen worden er opnames gemaakt en kunnen de vergaderingen live worden bekeken. De opdracht omvat de verzorging van live streaming en VODcasts van de raadzaal en commissie-/perskamer inclusief hosting en website.	ISO 27001 ISO 27002 Digitoegankelijk	IPv4 & IPv6 DNSSEC HTTPS & HSTS TLS SPF DKIM DMARC STARTTLS & DANE PDF	op de goede weg: nog een heel eind te gaan	25%
Bizob	Het implementeren en inrichten en vervolgens ter beschikking stellen van een burgerzaken-applicatie gekoppeld met een applicatie datadistributie, inclusief onderhoud en ondersteuning comform GIBIT 2020.	ISO 27001 ISO 27002 StUF	HTTPS & HSTS TLS SAML IPv4 & IPv6 SPF DKIM DMARC STARTTLS & DANE PDF DNSSEC Digitoegankelijk Digikoppeling	op de goede weg: nog een heel eind te gaan	20%
Veiligheidsregio Gooi en Vechtstreek	Contracteren van een Leverancier die het (tweedelijns)-beheer van de ICT-infrastructuur uitvoert voor Veiligheidsregio Gooi en Vechtstreek inclusief het (tweedelijns)-beheer van de samenwerkingsomgeving van VRGV en Veiligheidsregio Flevoland.	ISO 27001	IPv4 & IPv6	op de goede weg: nog een heel eind te gaan	20%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
		ISO 27002	DNSSEC HTTPS & HSTS TLS SPF DKIM DMARC STARTTLS & DANE		
Gemeente Roosendaal	De gemeente wil van het HUIS van Roosendaal een gebouw maken, waar je op een kwalitatief goede manier kunt vergaderen, werken en elkaar kunt ontmoeten. Door de huidige COVID-situatie heeft e.e.a. in een versnelling gebracht. Het elkaar ontmoeten, vergaderingen, met elkaar kunnen brainstormen of kennis uitwisselen zal niet meer altijd fysiek op dezelfde plek plaatsvinden. Een hybride vorm van werken is daarmee een manier van werken geworden. Hierbij kan een deel van de mensen fysiek aanwezig zijn op kantoor en een deel online vanuit huis of elders. Daar waar het gaat om een hybride vorm van (samen) kunnen werken is een gedegen keuze van de juiste audio- en beeld technieken, als onderdeel van de AV-installaties, een zeer belangrijk aspect.	ISO 27001	HTTPS & HSTS	op de goede weg: nog een heel eind te gaan	20%
		ISO 27002	TLS SPF DKIM DMARC STARTTLS & DANE DNSSEC IPv4 & IPv6		
Veiligheidsregio Hollands Midden	Een geschikt, betrouwbaar, gebruiksvriendelijk, modern en SaaS gebaseerd systeem voor Repressieve Operationele Informatie Voorziening dat bestaat uit: (1) software die functionaliteiten biedt op het vlak van actuele (maatwerk) route-navigatie en incident- / object-informatie voor circa 150	ISO 27001	DNSSEC	op de goede weg: nog een heel eind te gaan	17%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
	voertuigen en circa 250 losse persoonsgebonden devices van VRHM. VRHM medewerkers benaderen deze software via tablets en smartphones; (2) een bijbehorende beheeromgeving waarin VRHM route navigatie up to date kan houden en het functioneel beheer kan uitvoeren; (3) waarbij er koppelingen zijn met diverse andere VRHM systemen zoals het meldkamersysteem en Geo-magazijn; (4) de inrichting van het nieuwe systeem te verzorgen met name op het gebied van de (maatwerk) route informatie, inclusief koppelingen, gebruikers-rechten en instructie van VRHM medewerkers, en (5) dit systeem te onderhouden, door te ontwikkelen en up tot date te houden.	ISO 27002	SPF DKIM DMARC STARTTLS & DANE IPv4 & IPv6 HTTPS & HSTS TLS Geo standaarden SAML		
Gemeente Den Haag	Een scanoplossing parkeerhandhaving bestaande uit de volgende onderdelen: - implementatie en door-ontwikkeling van een scandienst binnen de Haagse parkeerketen; - beschikbaar stellen van scan-middelen (bestaande uit de scanoplossing en de drager (voertuig)) aan de Handhavingsorganisatie; - integraal beheren van de koppelingen binnen de separate onderdelen van de aangeboden scandienst en het in stand houden van de koppelvlakken met systemen van derden binnen de Haagse parkeerketen; - verzorgen van het communicatiesysteem middels onder andere een IT platform,	PDF	IPv4 & IPv6	op de goede weg: nog een heel eind te gaan	14%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
	waar alle scandata worden verzameld, opgeslagen en verwerkt zodat de data geanalyseerd kunnen worden ten behoeve van een meer efficiënte handhaving in Den Haag (inclusief het beheer en onderhoud hiervan).	Digikoppeling	DNSSEC HTTPS & HSTS TLS ISO 27001 ISO 27002 SPF DKIM DMARC STARTTLS & DANE SAML Geo standaarden		
Waterschap Noorderzijlvest	Telecommunicatiediensten in 2 percelen. Perceel 1: Mobiele telecommunicatiediensten, bestaande uit (a) persoons-gebonden mobiele spraak- en datacommunicatie en (b) object-gebonden mobiele datacommunicatie. Perceel 2: Vaste data-communicatie verbindingen, bestaande uit (a) unmanaged dataverbindingen met de (huidige) bandbreedte zoals opgegeven in het prijzenblad bandbreedte op locatie (best effort), en (b) centrale managed internetverbinding (IAS) op de hoofdlocatie van NZV, inclusief apparatuur en herstelservice. ontwikkelen, implementeren, beheren, onderhouden en doorontwikkelen van een data-distributiesysteem. De nieuwe datadistributie-applicatie gaat ingezet worden om de datadistributie en het beheer van gemeenten Zaltbommel en Maasdriel te faciliteren.	IPv4 & IPv6	HTTPS & HSTS TLS ISO 27001 ISO 27002 SPF	op de goede weg: nog een heel eind te gaan ***NB: het Waterschap heeft bij deze beoordeling een aantal kanttekeningen geplaatst. Deze kwamen helaas te laat binnen om nog te verwerken.***	10%

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel	
			DKIM DMARC STARTTLS & DANE DNSSEC		
Provincie Groningen	Het technisch beheer van snn.nl en sterknoordnederland.nl wordt verzorgd door een externe leverancier. Deze samenwerking is 4 jaar geleden gestart. De provincie staat nu op het punt om via een aanbesteding opnieuw een externe partner te kiezen voor het beheer en de doorontwikkeling van de websites snn.nl en sterknoordnederland.nl, inclusief doorlopend onderhoud.	Digitoegankelijk	ISO 27001 ISO 27002 Digikoppeling HTTPS & HSTS TLS IPv4 & IPv6 SPF DKIM DMARC STARTTLS & DANE DNSSEC	op de goede weg: nog een heel eind te gaan	8%
Gemeente Westerkwartier	Onder E-HRM as a service verstaat de gemeente software die als een online dienst wordt aangeboden.		HTTPS & HSTS TLS ISO 27001 ISO 27002 StUF SPF DKIM DMARC PDF DNSSEC IPv4 & IPv6 SAML STARTTLS & DANE	slecht	(n.v.t)
N.V. HVC	Telefonie: mobiel, vast, service-nummers en connectiviteit.		IPv4 & IPv6 ISO 27001	slecht	(n.v.t)

aanbesteder	onderwerp van aanbesteding	relevante standaarden: gevraagd	relevante standaarden: NIET gevraagd	oordeel
			ISO 27002	

B3. Rapportage Open standaarden en voorzieningen (PBLQ)

Auteurs: Jinne Samsom, Piet Hein Minnecré en Sandra Taal, PBLQ, 25-10-2022

1. Inleiding

1.1. Aanleiding

De Monitor Open Standaarden brengt jaarlijks in kaart of het 'pas toe of leg uit'-principe voor open standaarden 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 het gebruik van open standaarden bij verschillende overheidsvoorzieningen.

1.2. Opdrachtformulering

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

De voorzieningen zijn opgedeeld in een set voorzieningen (1) die direct raakt aan de communicatie en gegevensuitwisseling met burgers en bedrijven en een set voorzieningen (2) die hoofzakelijk is gericht op de communicatie en gegevensuitwisseling tussen overheden dan wel op de onderliggende infrastructuur.

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

Dit jaar zijn de voorzieningen onderzocht die direct raken aan de communicatie en gegevensuitwisseling met burgers en bedrijven. Dit betekent dat de resultaten van dit jaar worden vergeleken met de bevindingen van het voorzieningenonderzoek van de monitor uit 2020.

1.3. Werkwijze

Voor dit onderzoek is gebruik gemaakt van de 'pas toe of leg uit'-lijst van 1 april 2022. Onder bijlage A is de volledige lijst opgenomen en is aangegeven welke veranderingen er hebben plaatsgevonden. De lijst met beheerders per voorziening is opgenomen onder bijlage B. Met elke beheerder is gekeken welke standaarden van deze lijst voor de voorziening relevant zijn. Daarbij is telkens uitgegaan van de eindgebruiker. Dat is degene die in de keten baat zou moeten hebben bij het gebruik van open standaarden. Dit is expliciet zo gekozen, omdat het beleid ten aanzien van standaardisatie vooral gericht is op het stimuleren van interoperabiliteit. In eerdere onderzoeken is gebleken dat beheerders van voorzieningen soms terminologie gebruiken als '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. In deze gevallen is er 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 de voorzieningen daarvan gebruik maken. Het vertrekpunt daarbij is telkens het overzicht van het vorige meetmoment, in dit geval dus 2020. Waar mogelijk zijn de standaarden vooraf door de onderzoekers zelf getoetst. Daarbij maken we onder meer gebruik van de testen die beschikbaar zijn via internet.nl en RIPEstat. Onder paragraaf 1.4.4 wordt meer uitleg gegeven over het (zelf) toetsen van de standaarden. Daarnaast kijken we of de geplande activiteiten om aan standaarden te voldoen inmiddels uitgevoerd zijn. Voor nieuwe standaarden op de lijst maken we in samenspraak met de beheerders een inschatting of ze relevant zijn voor de voorziening.

Vervolgens sturen we het voorbereide overzicht met relevante standaarden per voorziening toe aan de beheerder. We vragen hen onze inschatting te valideren en een toelichting toe te voegen. Op basis van hun reactie wordt de verzamelde informatie aangescherpt. Het resultaat daarvan wordt voorgelegd aan de opdrachtgever en wordt vervolgens in een definitieve versie toegestuurd aan de beheerders. Na hun akkoord wordt de informatie opgenomen in deze 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 (telefonisch) besproken. In de gevallen waar de verschillen ook na de gesprekken bleven bestaan, is dit duidelijk opgenomen in de rapportage. Vanuit enkele beheerders is gedurende het beantwoordingsproces de correspondentie gestopt, ondanks herhaalde pogingen tot contact. Aan deze beheerders hebben wij schriftelijk aangegeven op welke manier de antwoorden in de rapportage zijn gekomen.

1.4. Aandachtspunten voor de lezer

1.4.1. Voorzieningen en standaarden geordend op basis van functionaliteit

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

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

1.4.2. Status

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

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

Met ‘conform’ wordt in dit onderzoek bedoeld dat de standaard door de eindgebruiker te gebruiken is.

1.4.3. Relevantie standaard

Voor de relevantiebepalingen zijn per standaard de beschrijvingen van het functioneel en organisatorisch toepassingsgebied gehanteerd (zoals vermeld op de pas toe of leg uit-lijst van het Forum Standaardisatie). Standaarden die niet relevant zijn voor een voorziening zijn niet in de tabel opgenomen. Voor de standaarden die ten opzichte van de vorige meting in 2020 nieuw zijn op de lijst is samen met de beheerders een inschatting gemaakt in hoeverre ze relevant voor de voorziening zijn.

1.4.4. Wijze van toetsen standaard

Toetsen en het bevragen van beheerders

Het toetsen wanneer een voorziening aan een standaard voldoet is lastig. Het vereist een heldere afbakening van de voorziening en heldere voorwaarden wanneer voldaan wordt aan een standaard. Deels hanteren we beschikbare (openbare) toetsen zoals internet.nl en RIPEstat. om de compliancy vast te stellen. We hebben geen toegang tot interne systemen of documenten. Dat gaat de scope van dit onderzoek te buiten. 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 gerelateerde voorzieningen (bijvoorbeeld indien er gebruik gemaakt wordt van hetzelfde platform). Op die manier ontstaat er een beeld van de mate waarin de voorziening voldoet aan de standaarden.

Waar de antwoorden van de beheerder en PBLQ van elkaar afwijken, gaan we hierover met de beheerder in gesprek en mocht het verschil van mening blijven bestaan wordt daar melding van gemaakt in deze rapportage. In de toelichtingskolom geven de beheerders zo goed mogelijk aan of ze aan de standaard voldoen en of waarom niet.

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

Gebruik van internet.nl

Voor een groot aantal standaarden maken we gebruik 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 voor web- en emaildomeinen. Het gaat om de volgende standaarden:

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

Gebruik van RIPEstat

De standaard RPKI wordt getoetst met RIPEstat. Aan de hand van een IP-adres wordt getest in hoeverre de RPKI-standaard is doorgevoerd.

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

Webrichtlijnen en Digitoegankelijk

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

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

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

Voor dit onderzoek is per voorziening gekeken of er een toegankelijkheidsverklaring in het openbare register is gepubliceerd. De toegankelijkheidsverklaring kent een nalevingsstatus. Deze geeft aan hoe ver een overheidsinstantie is gevorderd met het toegankelijk maken van een website en lopen uiteen van:

- Score A: Voldoet volledig
- Score B: Voldoet gedeeltelijk
- Score C: Eerste maatregelen genomen
- Score D: Voldoet niet
- Score E: Geen toegankelijkheidsverklaring gepubliceerd

ISO 27001/2 en de BIO

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

2. Identificeren en authentiseren

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.

De DigiD applicatie (aanvragen, inloggen etc.) draait op het domein digid.nl. Dit domein kent ook een e-mail-functionaliteit. De website van DigiD draait op het subdomein www.digid.nl. Alle genoemde domeinen maken deel uit van de scope van het onderzoek.

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-zone) 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 DigiD de HSTS-policy met een geldigheidsduur van 1 jaar (zie: https://internet.nl/site/digid.nl/).
IPv4 en IPv6 (Internetnummers)	Ja	Het domein DigiD.nl is via IPv4 en IPv6 toegankelijk. Ook het mailverkeer verloopt via IPv4 en 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 verantwoordt zich over deze norm aan het kerndepartement (BZK).
RPKI	Ja	De Logius voorziening DigiD is aangesloten op IP-reeksen die ontsloten worden via leveranciers uit het raamcontract ON2013. Deze IP-reeksen voldoen aan RPKI.

SAML (Inloggegevens)	Ja	DigiD biedt afnemers een SAML-koppelvlak aan om authenticaties uit te kunnen voeren. Wanneer de afnemer "single sign on" wil gebruiken is dit alleen mogelijk via het SAML-koppelvlak. De SAML- koppelvlakspecificaties van DigiD zijn gepubliceerd op de website van Logius (zie: https://logius.nl/diensten/digid/documentatie/koppelvlakspecificatie-digid-saml-authenticatie)
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is relevant voor DigiD bij het verzenden van mails vanuit DigiD , en DigiD voldoet ook aan deze standaard (zie: https://internet.nl/mail/digid.nl/).
STARTTL enDANE (Beveiligd, versleuteld mailverkeer)	Ja	De mailservers van DigiD passen STARTTLS en DANE toe (zie: https://internet.nl/mail/digid.nl/). Vanwege ondersteuning van oudere e-mailservers is een risicoafweging gemaakt om de TLS-versies 1.0 en 1.1 inclusief bepaalde ciphersuites te blijven aanbieden, zolang dit niet direct onveilig is voor de mailservers van DigiD.
TLS (Beveiligde, versleutelde verbindingen)	Ja	DigiD ondersteunt voor de websitedomeinen alleen TLS v1.2. In 2022 wordt ondersteuning voor TLS v1.3 toegevoegd.
Document en (web/app)content		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Deel (Status B)	DigiD heeft onderzoek gedaan naar de toegankelijkheid van de websites en mobiele apps. Er wordt nog niet voldaan aan alle toegankelijkheidseisen uit de norm (Status B) maar er zijn verbetermaatregelen benoemd en er is een planning hiervoor gemaakt. DigiD is daarom in control over de toegankelijkheid van de websites en mobiele apps. (zie de diverse verklaringen van DigiD op https://www.toegankelijkheidsverklaring.nl/register?w=digid)

Ten opzichte van 2020 voldoet de voorziening aan de nieuwe standaard RPKI. Op het gebied van de nieuwe standaard Digitoegankelijk voldoet de voorziening gedeeltelijk (status B).

Concluderend moeten voor DigiD nog de volgende standaarden (volledig) worden geïmplementeerd: Digitoegankelijk.

2.2. DigiD Machtigen

Beheerorganisatie: Logius
Werking en inhoud van DigiD
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	Er is een DMARC record geconfigureerd als een van de anti-phishing maatregelen (zie: https://internet.nl/mail/machtigen.digid.nl/). Verder wordt er geen email verstuurd onder domeinnaam machtigen.digid.nl en is DMARC niet veel aan de orde.

		E-mails verzonden door de voorziening Machtigen worden verstuurd onder het @digid.nl domein, het DMARC record en ander email gerelateerde standaarden worden door DigiD voorzien, en waarvan Machtigen in kennis wordt gesteld.
DNSSEC (Beveiligde domeinnamen)	Ja	Het domein https://machtigen.digid.nl voldoet aan DNSSEC (zie: https://internet.nl/site/machtigen.digid.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	DigiD Machtigen maakt gebruik van HTTPS voor de communicatie tussen clients (zoals browsers) en servers. De DigiD Machtigen website heeft ook een HSTS-policy (zie: https://internet.nl/site/machtigen.digid.nl/). Tot nader orde wordt nog gebruik gemaakt van PKIOverheid certificaten van publieke CA2020
IPv4 en IPV6 (Internetnummers)	Ja	De website van DigiD Machtigen is via IPv4 en IPv6 toegankelijk en ondersteund (zie: https://internet.nl/site/machtigen.digid.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Overheid (BIO) van toepassing die is gebaseerd op NEN-ISO27001/2. Logius verantwoord zich over de BIO aan het kerndepartement (BZK).
RPKI	Ja	De Logius voorziening DigiD Machtigen is aangesloten op IP-reeksen die ontsloten worden via leveranciers uit het raamcontract ON2013. Deze IP-reeksen voldoen aan RPKI.
SAML v2.0 (Inloggegevens)	Ja	Het authenticatiekoppelvlak met eHerkenning voldoet aan de SAML standaard. Het authenticatiekoppelvlak met DigiD maakt gebruik van SAML. Naast authenticatie gebruikt DigiD Machtigen de SAML standaard ook om een getekend machtigingsbewijs af te geven, namelijk als een SAML assertion.
SPF (Preventie van mailspoofing/ phishing)	Ja	DigiD Machtigen verstuurt geen email aan gebruikers, vanaf het @machtigen.digid.nl domein. Er is wel een SPF record aangemaakt voor het domein: 'machtigen.digid.nl' die aangeeft dat er vanaf dit domein geen email wordt verstuurd. E-mails verzonden door Machtigen worden verstuurd onder het @digid.nl domein. De bijbehorende SPF record en andere email gerelateerde standaarden vallen onder de verantwoordelijkheid van DigiD. De voorziening Machtigen ontvangt van DigiD, middels een collegiaal informatiebeveiligingsoverleg, updates over het SPF record en andere email gerelateerde standaarden.
TLS (Beveiligde, versleutelde verbindingen)	Ja	TLS is geïmplementeerd. DigiD Machtigen ondersteunt TLS v1.2. Hieraan is een beperkte set aan cipher-suites toegekend, welke voldoen aan norm 'voldoende' en 'goed' in de NCSC "ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0" TLS 1.0 en 1.1 worden niet meer ondersteund op machtigen.digid.nl.
Document en (web/app)content		

Digitoegankelijk (EN 301 549 met WCAG 2.1)	Deels (Status B)	DigiD Machtigen heeft onderzoek gedaan naar de toegankelijkheid van de website. Er wordt nog niet voldaan aan alle toegankelijkheidseisen uit de norm (Status B), er zijn verbetermaatregelen benoemd. DigiD Machtigen is daarom in control over de toegankelijkheid van de website (zie de diverse verklaringen van DigiD op https://www.toegankelijkheidsverklaring.nl/register?w=digid). Vanaf 21 juni voldoet DigiD Machtigen volledig aan de WCAG.
PDF/A en PDF 1.7 (Document-publicatie/ archivering)	Ja	De voorziening voldoet aan deze standaard.
Stelselstandaarden		
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Deels	Recent ontwikkelde koppelvlakken en/of nieuwe versies van bestaande koppelvlakken zijn Digikoppeling compliant (bijvoorbeeld BOP). Er zijn echter nog koppelvlakken waarvan geen Digikoppeling compliant versie is gemaakt en/of koppelvlakken waar nog diensten en afnemers op aangesloten zitten (bijvoorbeeld PBS, een koppelvlak waarover een aangesloten dienstaanbieder kan controleren of iemand daadwerkelijk gemachtigd is om te handelen namens een vertegenwoordigde). Deze koppelvlakken bestaan uit de tijd dat de Digikoppeling standaard in ontwikkeling was en voldoen deels aan de uiteindelijk ontstane Digikoppeling standaard. Vanwege nieuwe ontwikkeling van koppelvlakken, is besloten niet meer te investeren in dit huidige koppelvlak.

Ten opzichte van 2020 voldoet DigiD Machtigen aan TLS en aan de nieuwe standaard RPKI. De status 'deels' van de Digikoppeling standaard is ongewijzigd. Op het gebied van de nieuwe standaard Digitoegankelijk voldoet de voorziening gedeeltelijk (status B).

Concluderend moeten voor DigiD Machtigen nog de volgende standaarden (volledig) worden geïmplementeerd: Digitoegankelijk. De voorziening voldoet deels aan Digikoppeling 2.0, maar heeft weloverwogen besloten om niet verder te investeren in het huidige koppelvlak.

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 zeven toegetreden vertrouwensdienstverleners (TSP's) die PKIoverheidscertificaten verstrekken. Dit zijn: KPN, 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	Het email-domein PKIoverheid.nl voldoet aan DMARC (zie: https://internet.nl/mail/pkioverheid.nl/).

DNSSEC (Beveiligde domeinnamen)	Ja	Het PKIoverheid-deel van de website van Logius en de website van PKIoverheid maken gebruik van DNSSEC (zie: https://internet.nl/domain/crl.pkioverheid.nl/ en https://internet.nl/domain/www.logius.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	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. De redirects www.pkioverheid.nl en pkioverheid.nl zijn inmiddels (tijdelijk) uitgezet/verwijderd.
IPv4 en IPV6 (Internetnummers)	Deels	IPv6 is geïmplementeerd voor de informatiepagina's van PKIoverheid op de Logius website (zie: https://internet.nl/domain/www.logius.nl/) en voor het ontvangend maildomein. De PKIoverheid specifieke applicatiepagina's zijn op dit moment nog niet geschikt voor IPv6 (zie: https://internet.nl/domain/crl.pkioverheid.nl/). Inmiddels is Logius met de leverancier van pkioverheid.nl bezig met een impactanalyse voor de benodigde werkzaamheden voor IPv6. Een exacte planning/realisatiedatum is nog niet af te geven omdat de voorziene oplossingsrichting nog niet volledig is uitgewerkt.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Primair is het Webtrust normenkader van toepassing op PKIoverheid. Dit kader kent strengere eisen dan deze ISO-standaarden vereisen. Implementatie van de BIO is daarnaast uitgevoerd op basis van best effort.
RPKI	Ja	Zowel voor het deel op de Logius website als op pkioverheid.nl zelf is RPKI ingeregeld.
SPF (Preventie van mailspoofing/phishing)	Ja	Records zijn geconfigureerd om alle mail namens pkioverheid.nl te rejecten (geen geldige bron opgenomen in het SPF record). Er wordt geen mail verstuurd vanuit pkioverheid.nl of een van haar subdomeinen.
TLS	Ja	Zowel het PKIoverheid deel van de website van Logius als de website van PKIoverheid zelf maken 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		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Deels (Status B)	Zie de toegankelijkheidsverklaring op https://www.toegankelijkheidsverklaring.nl/register/3344
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 2020 voldoet de voorziening aan HTTPS en HSTS, SPF en aan de nieuwe standaard RPKI. De status van IPv4 en IPv6 is van nee naar deels gegaan. Op het gebied van de nieuwe standaard Digitoegankelijk voldoet de voorziening gedeeltelijk (status B).

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

2.4. Afsprakenstelsel elektronische toegangsdiensten

Beheerorganisatie: Logius
Werking en inhoud van het Afsprakenstelsel elektronische toegangsdiensten
eHerkenning is een veilig en betrouwbaar inlogmiddel waarmee men bij ruim 500 verschillende dienstverleners, zoals UWV, gemeenten, Belastingdienst en verzekeraars kan inloggen.

Het Afsprakenstelsel Elektronische Toegangsdiensten is een set van technische, functionele, juridische en organisatorische afspraken op basis waarvan het netwerk van eHerkenning wordt geleverd in een publiek-private samenwerking.

Sinds 2016 is het Afsprakenstelsel Elektronische Toegangsdiensten in het onderzoek opgenomen in plaats van eHerkenning. Het afsprakenstelsel bevat de voor dit onderzoek relevante eisen voor eHerkenning en is in beheer bij de 'Beheerorganisatie eHerkenning', die is ondergebracht bij Logius. Meer informatie is te vinden op de website https://eherkenning.nl/nl/wat-is-eherkenning.

Standaard	Status	Toelichting beheerder
Internet en beveiliging		
DKIM (Preventie van mailspoofing/phishing)	Ja	Bij verstuurde e-mail wordt DKIM toegepast, bij ontvangst gebeurt dit door de centrale e-mailvoorziening, die Logius als dienst afneemt van het Shared Service Centrum van het Rijk (SSC-ICT).
DMARC (Anti-phishing)	Ja	Deze standaard is geïmplementeerd, zie https://internet.nl/mail/eherkenning.nl.
DNSSEC (Beveiligde domeinnamen)	Ja	Deze standaard is geïmplementeerd, zie https://internet.nl/site/eherkenning.nl .
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	HTTPS en HSTS wordt toegepast op alle websites en webapplicaties onder beheer van de beheerorganisatie en deelnemers in het stelsel.
IPv4 en Ipv6 (Internetnummers)	Ja	Deze standaard is geïmplementeerd, zie https://internet.nl/site/eherkenning.nl.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	In het afsprakenstelsel wordt certificering tegen ISO27001 geëist voor de deelnemers. De beheerorganisatie eHerkenning is als stelselbeheerder ook gecertificeerd volgens ISO27001. Daarvoor is ook een in control statement beschikbaar.
RPKI	Ja	RPKI is geïmplementeerd via de hosting partij van de website eherkenning.nl ICTU.
SAML (Inloggegevens)	Ja	SAML is een verplichte eis vanuit het stelsel.
SPF	Ja	SPF wordt toegepast bij de voorziening (mail en webserver).

(Preventie van mailspoofing/phishing)		
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	STARTTLS is geïmplementeerd voor eherkenning.nl. DANE voor SMTP is voor de maildomeinen geïmplementeerd bij de centrale e-mailvoorziening, die Logius als dienst afneemt van het Shared Service Centrum van het Rijk (SSC-ICT).
TLS (Beveiligde, versleutelde verbindingen)	Ja	Mailservers, webdomein en het netwerk eHerkenning ondersteunen alleen veilige TLS-versies (>= TLS 1.2)
Document en (web/app)content		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Deels (Status B)	De nieuwe website eherkenning.nl is een verbetering mbt toegankelijkheid omdat bij het ontwerp van de nieuwe website eerdere bevindingen zijn meegenomen.
PDF 1.7, PDF/A-1 of PDF/A-2 (Documentpublicatie/ archivering)	Ja	Primair wordt de stelseldocumentatie via HTML op eherkenning.nl gepubliceerd. Stelseldocumentatie wordt met behulp van officesoftware gepubliceerd in PDF/A-formaat. Overige documenten worden met een aparte tool in PDF/A formaat geconverteerd, omdat het gehanteerde DMS dit niet ondersteunt.

Ten opzichte van 2020 voldoet de voorziening inmiddels aan DMARC, IPv4 en IPv6 en TLS. De voorziening voldoet ook aan de nieuwe standaard RPKI. Op het gebied van de nieuwe standaard Digitoegankelijk voldoet de voorziening gedeeltelijk (status B).

Concluderend moeten voor het Afsprakenstelsel elektronische toegangsdiensten nog de volgende standaarden (volledig) worden geïmplementeerd: Digitoegankelijk.

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 diensten en informatie en is daarom met DigiD beveiligd. 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	Ja	MijnOverheid voldoet aan DKIM (zie: https://internet.nl/mail/mijnoverheid.nl/ en https://internet.nl/mail/mijn.overheid.nl/).

(Preventie van mailspoofing/ phishing)		
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.
IPv4 en IPV6 (Internetnummers)	Ja	De standaard wordt toegepast, maar is niet te testen via internet.nl omdat MijnOverheid de internet.nl scanner in de anti-DDOS protection blokkeert. MijnOverheid gaat in gesprek met internet.nl
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Op de Rijksoverheid is de BIO van toepassing die is gebaseerd op NEN-ISO27001. Logius heeft zich over toepassing van deze norm verantwoord door het afgeven van In Control Verklaringen (ICV'en) aan de eigenaar (BZK/DGOBR). De ICV's zijn nog up-to-date.
RPKI	Ja	De Logius Voorzieningen zijn aangesloten op IP-reeksen die ontsloten worden via leveranciers uit het raamcontract ON2013. Deze leveranciers voldoen aan RPKI. Specifiek voor de IP-reeksen die gekoppeld worden aan het nieuwe platform van Logius, moet RPKI nog ingericht worden. Dat gebeurt nog voor de voorzieningen worden overgezet.
SAML (Inloggegevens)	Ja	Authenticatie loopt via SAML.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Gepland	Bij het vervangen van mail certificaat is vergeten om TLSA record te updaten. Dit wordt zo snel mogelijk opgelost.
TLS (Beveiligde, versleutelde verbindingen)	Ja	In de dienstverlening aan burgers maakt MijnOverheid gebruik van een TLS 1.2-verbinding (zie: https://internet.nl/site/mijn.overheid.nl). De koppelingen met afnemers (overheidsorganisaties) lopen ook via TLS op basis van PKIoverheid-certificaten. MijnOverheid gebruikt TLS 1.2 en veilige cipher suites. Een aantal oude ciphers wordt nog ondersteund omdat er anders problemen ontstaan bij afnemers, burgers e.d. TLS 1.3 moet nog geïmplementeerd worden. Oudere versies worden niet meer geaccepteerd.
Document en (web/app)content		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Ja (Status A)	MijnOverheid.nl voldoet aan de wettelijke eisen rondom Digitoegankelijk met het behalen van de A-status op het gebied van WCAG 2.1.

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. Voor de PDF bijlagen die door afnemers naar de berichtenbox worden gestuurd wordt een validatie uitgevoerd of ze voldoen aan de standaarden. De afnemer krijgt in het leverancierssportaal de terugkoppeling of een bijlage voldoet of niet. Daarmee wordt de afnemer door Logius geïnformeerd over het wel of niet voldoen aan de standaard. Logius is zelf niet verantwoordelijk voor het voldoen aan de standaard. Onze verantwoordelijkheid is om de afnemers te informeren of ze voldoen aan de standaard.
REST-API Design Rules	Ja	MijnOverheid kent drie REST API´s: 1. API t.b.v. de Berichtenbox app; 2. DvMG (Delen van MijnGegevens) API t.b.v. het ad-hoc, met directe instemming van de burger, delen van inkomensgegevens met woonruimteverdelers; Profielservice API t.b.v. delen van bereikbaarheidsgegevens met GNS t.b.v. KOOP bekendmakingen attenderen.
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 2020 is de status van STARTTLS en DANE van ja naar gepland gegaan. De voorziening voldoet aan de nieuwe standaarden REST-API Design Rules en RPKI. Op het gebied van de nieuwe standaard Digitoegankelijk voldoet de voorziening volledig (status A).

Concluderend moeten voor MijnOverheid nog de volgende standaarden (volledig) worden geïmplementeerd: STARTTLS en DANE.

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. De mogelijkheden hiervoor worden nu bekeken.

Standaard	Status	Toelichting beheerder
Internet en beveiliging		
DKIM (Preventie van mailspoofing/phishing)	Ja	@antwoordvoorbedrijven.nl en @berichtenbox.antwoordvoorbedrijven.nl voldoen hieraan. Dit kan gecontroleerd worden op https://internet.nl/mail/antwoordvoorbedrijven.nl en https://internet.nl/mail/berichtenbox.antwoordvoorbedrijven.nl N.B. De notificaties de we sturen hebben als afzender noreply-berichtenbox@antwoordvoorbedrijven.nl
DMARC (Anti-phishing)	Ja	@antwoordvoorbedrijven.nl en @berichtenbox.antwoordvoorbedrijven.nl voldoen hieraan. Dit kan gecontroleerd worden op https://internet.nl/mail/antwoordvoorbedrijven.nl en https://internet.nl/mail/berichtenbox.antwoordvoorbedrijven.nl N.B. De notificaties de we sturen hebben als afzender noreply-berichtenbox@antwoordvoorbedrijven.nl
DNSSEC (Beveiligde domeinnamen)	Ja	Volgens internet.nl voldoet het domein berichtenbox.antwoordvoorbedrijven.nl (zie: https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	De Berichtenbox voor bedrijven voldoet volledig aan HTTPS en HSTS.
IPv4 en IPv6 (Internetnummers)	Nee	De Berichtenbox voor bedrijven voldoet op 4 van de 5 punten aan IPv6. Enkel de IPv6-bereikbaarheid van nameservers ontbreekt.
RPKI	Ja	De publieke IP-adressen van berichtenbox zijn voorzien van een geldig certificaat. Bij verbindingen naar publieke IP-adressen wordt de geldigheid van handtekeningen gecontroleerd.
SAML (Inloggegevens)	Ja	eHerkenning is SAML-based en wordt toegepast voor het inloggen op de Berichtenbox.
SPF (Preventie van mailspoofing/phishing)	Ja	@antwoordvoorbedrijven.nl en @berichtenbox.antwoordvoorbedrijven.nl voldoen hieraan. Dit kan gecontroleerd worden op https://internet.nl/mail/antwoordvoorbedrijven.nl en https://internet.nl/mail/berichtenbox.antwoordvoorbedrijven.nl N.B. De notificaties de we sturen hebben als afzender noreply-berichtenbox@antwoordvoorbedrijven.nl
TLS (Beveiligde, versleutelde verbindingen)	Ja	De Berichtenbox ondersteunt veilige TLS-versies.
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.
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Deels (Status B)	Voldoet gedeeltelijk. Verbeteringen nog te doen op het vlak van responsiveness.
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 2020 voldoet de voorziening aan HTTPS en HSTS en TLS. De status van IPv4 en IPv6 gaat van gepland naar nee. De voorziening voldoet aan de nieuwe standaard RPKI. Op het gebied van de nieuwe standaard Digitoegankelijk voldoet de voorziening gedeeltelijk (status B).

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

3.3. Overheid.nl

Beheerorganisatie: Kennis- en Exploitatiecentrum Officiële Overheidspublicaties (KOOP)
Werking en inhoud van Overheid.nl
De website Overheid.nl biedt centrale internettoegang voor informatie en diensten van de Nederlandse overheid. Overheid.nl is bestemd voor burgers, bedrijven en ondernemers en andere overheden. Overheid.nl bevat naast informatie en diensten ook de contactgegevens van Nederlandse overheidsorganisaties. Ook het domein wetten.overheid.nl valt onder deze voorziening.

Standaard	Status	Toelichting beheerder
Internet en beveiliging		
DKIM (Preventie van mailspoofing/phishing)	Ja	DKIM is geïmplementeerd (zie: https://internet.nl/mail/overheid.nl/).
DMARC (Anti-phishing)	Ja	DMARC is volledig doorgevoerd.
DNSSEC (Beveiligde domeinnamen)	Ja	Overheid.nl voldoet aan DNSSEC (zie: https://internet.nl/site/www.overheid.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	Overheid.nl voldoet aan HTTPS en HSTS (zie: https://internet.nl/site/overheid.nl/).
IPv4 en IPV6 (Internetnummers)	Ja	Er wordt voldaan aan IPv4 en IPv6 (zie: https://internet.nl/domain/www.overheid.nl/).

NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Vanaf 2015 staat overheid.nl niet meer op de risicokaart van BZK en hoeft hiervoor geen ICV (In Control Verklaring) meer te worden afgegeven. Voor OEB, de applicatie die centraal staat in het publiceren van overheidsinformatie en richtinggevend is voor alle KOOP-dienstverlening, wordt wel jaarlijks een ICV afgegeven; deze is gebaseerd op de BIO die weer is gebaseerd op NEN-ISO/IEC 27001/27002. Alle dienstverlening van KOOP is ondergebracht bij een hostingpartij die jaarlijks een ISAE3402 Type II verklaring laat opstellen; deze verklaring baseert zich mede op de certificering met NEN-ISO/IEC 27001/27002.
NL GOV Assurance profile for OAuth 2.0	Ja	Digikoppeling REST profiel houdt de standaarden OpenAPI Specification (OAS), OAuth 2.0 en PKI aan.
RPKI	Nee	Bij KOOP valt deze momenteel in de categorie 'leg uit'. KOOP zit midden in de migratie naar het Standaard Platform van Logius.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	Overheid.nl voldoet hieraan (zie: https://internet.nl/mail/overheid.nl/).
TLS (Beveiligde, versleutelde verbindingen)	Ja	De mail vanuit overheid.nl is 100% compliant.
Document en (web/app)content		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Deels (Status B)	Alle onderdelen van Overheid.nl hebben minimaal Status B. De portaal Overheid.nl zal op 1 juli 2022 A-status hebben. Een belemmering bij sub-portalen van Overheid.nl is dat er veel content van derden die wettelijk verplicht gepubliceerd moet worden, die door de aanleverende partijen niet toegankelijk is gemaakt. Dat belemmert de volledige A-status.
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.
REST-API Design Rules	Nee	Op Overheid.nl wordt gebruik gemaakt van de internationale SRU standaard. Deze standaard voor bibliothecaire recordmanagement biedt eenvoudig toegang tot alle informatie op Overheid.nl en sluit aan bij de XML-structuren van de content zelf. Ook kan er integraal gezocht worden door de collecties. Het vervangen van SRU door een REST-API is een kostbare en tijdrovende klus waar momenteel geen middelen voor beschikbaar gesteld zijn. Voor nieuwe collecties zoals PLOOI wordt wel direct gewerkt met REST-API's.
SKOS (Thesauri en begrippen-woordenboeken)	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 2020 voldoet de voorziening aan TLS en de nieuwe standaard NL GOV Assurance profile for OAuth 2.0. De voorziening voldoet (nog) niet volledig aan de nieuwe standaarden REST-API Design Rules en RPKI. Op het gebied van de nieuwe standaard Digitoegankelijk voldoet de voorziening gedeeltelijk (status B).

Concluderend moeten voor Overheid.nl nog de volgende standaarden (volledig) worden geïmplementeerd: REST-API Design Rules, RPKI en Digitoegankelijk.

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. Ondernemersplein.kvk.nl is de vervanger van ondernemersplein.nl, die sinds 2019 slechts doorverwijst.

Standaard	Status	Toelichting beheerder
Internet en beveiliging		
DMARC (Anti-phishing)	Ja	Ondernemersplein als onderdeel van kvk.nl voldoet aan DMARC.
DNSSEC (Beveiligde domeinnamen)	Ja	Ondernemersplein voldoet aan DNSSEC voor de website. E-mails worden verstuurd vanuit het kvk.nl domein.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Nee	Aan deze standaard wordt voldaan voor het domein kvk.nl. HSTS is aanwezig op ondernemersplein.kvk.nl, huidige instellingen worden binnenkort herzien.
IPv4 en IPv6 (Internetnummers)	Ja	IPv6 is aanwezig en conform overheid streefbeleid.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Ondernemersplein is onderdeel van de website van de Kamer van Koophandel. KVK is ISO 27001 gecertificeerd vanaf 2016. KVK is in 2019 opnieuw succesvol gecertificeerd.
RPKI	Ja	BGP wordt voor KvK door de internetleverancier ingeregeld.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd voor zowel kvk.nl, als ondernemersplein.kvk.nl.
TLS	Ja	De websites ondernemersplein.kvk.nl en www.kvk.nl zijn beveiligd met minimaal TLS 1.2.

(Beveiligde, versleutelde verbindingen)		
Document en (web/app)content		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Deels (Status C)	Ondernemersplein is WCAG 2.1 AA gecertificeerd https://www.accessibility.nl/inspecties/inspectie/site-1118.
REST-API Design Rules	Ja	Voor Ondernemersplein API´s zijn de REST-API Design Rules voor zover mogelijk toegepast.
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 2020 voldoet de voorziening aan IPv4 en IPv6 en de nieuwe standaarden REST-API Design Rules en RPKI. De voorziening voldoet (nog) niet volledig aan HTTPS en HSTS. Op het gebied van de nieuwe standaard Digitoegankelijk zijn de eerste stappen gezet (status C).

Concluderend moeten voor het Ondernemersplein nog de volgende standaarden (volledig) worden geïmplementeerd: HTTPS en HSTS en Digitoegankelijk.

3.5. Samenwerkende catalogi

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

De validator wordt in 2022 ondergebracht bij een andere dienstverlener, inclusief het voldoen aan de van toepassing zijnde open standaarden. Tot die tijd is de service uit de lucht en kunnen gebruikers XML-bestanden mailen aan Logius waarna ze handmatig worden getest.

Standaard	Status	Toelichting beheerder
Internet en beveiliging		
DMARC (Anti-phishing)	Ja	De SC API (zoekdienst.overheid.nl) voldoet aan deze standaard.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Gepland	De SC API (zoekdienst.overheid.nl) voldoet niet volledig. De verwachting is dat de voorziening in 2022 gaat voldoen.
IPv4 en IPv6 (Adressering van ICT-systemen binnen een netwerk)	Ja	Zowel de informatieve pagina's op logius.nl als de SC API (zoekdienst.overheid.nl) voldoen aan IPv4 en IPv6.

RPKI	Ja	De RPKI standaard wordt toegepast
SPF (Preventie van mailspoofing/phishing)	Gepland	Domein voor de SC API (zoekdienst.overheid.nl) is niet SPF compliant. De verwachting is dat het voldoen in 2022 gaat plaatsvinden.
TLS (Beveiligde, versleutelde verbindingen)	Gepland	De SC API (zoekdienst.overheid.nl) voldoet niet aan deze standaard. De verwachting is dat het voldoen in 2022 gaat plaatsvinden.
Document en (web/app)content		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Deels (Status C)	De pagina's op Logius.nl zijn Digitoegankelijk. Voor de SC validator komt er nieuwe verklaring op het moment dat de voorziening is gemigreerd naar de DICTU. Dat zal eerst een status C zijn totdat er onderzoek is uitgevoerd.
Open API Specification (Beschrijven van REST API's)	Nee	De leverancier van de SC API (KOOP) geeft in Q1 2023 een indicatieve planning af m.b.t. het voldoen aan de standaard
REST-API Design Rules	Nee	De leverancier van de SC API (KOOP) geeft in Q1 2023 een indicatieve planning af m.b.t. het voldoen aan de standaard

Ten opzichte van 2020 voldoet de voorziening aan de nieuwe standaard RPKI, maar niet meer aan SPF en Open API Specification. Er zijn planningen afgegeven voor HTTPS en HSTS, SPF en TLS. De voorziening voldoet verder niet aan de nieuwe standaard REST-API Design Rules. Op het gebied van de nieuwe standaard Digitoegankelijk zijn de eerste stappen gezet (status C).

Concluderend moeten voor de Samenwerkende Catalogi nog de volgende standaarden (volledig) worden geïmplementeerd: HTTPS en HSTS, REST-API Design Rules, SPF, TLS, Digitoegankelijk en Open API Specification.

3.6. RDW.nl

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

De beheerder heeft ervoor gekozen om de toelichting (gedeeltelijk) leeg te laten als de voorziening aan een standaard voldoet. Er zijn toelichtingen opgenomen als er extra uitleg wordt gegeven.

Standaard	Status	Toelichting
Internet en beveiliging		
DKIM (Preventie van mailspoofing/phishing)	Ja	

DMARC (Anti-phishing)	Ja	
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. Inmiddels is Microsoft bezig om hier invulling aan te geven: Microsoft 365 Roadmap.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	
IPv4 en IPv6 (Internetnummers)	Ja	
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	
NL GOV Assurance profile for OAuth 2.0	Ja	OAuth2.0 wordt ondersteund door RDW. Voornamelijk voor de interne bedrijfsvoering, maar er is één externe koppeling waarop OAuth2.0 wordt toegepast.
RPKI	Ja	
SAML (Inloggegevens)	Ja	
SPF (Preventie van mailspoofing/phishing)	Ja	
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Nee	RDW gebruikt momenteel de Symantec Mail Gateway (SMG). In GUI van de SMG wordt alleen nog maar TLS 1.2 of hoger geaccepteerd en is dit dusdanig ingesteld (1.0 en 1.1 worden dus actief geblokkeerd). Voor DANE zijn we afhankelijk van de roadmap van Microsoft. Zie ook DNSSEC.
TLS (Beveiligde, versleutelde verbindingen)	Ja	
Document en (web/app)content		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Deels (Status B)	Er is een zelfverklaring aanwezig, zie https://www.toegankelijkheidsverklaring.nl/register/1979 In juli 2021 is een nulmeting uitgevoerd, gevolgd door een volledige toegankelijkheidstest op rdw.nl begin 2022. Oplossingen voor de mogelijk gemelde issues (op gebied van ontwerp, bouw en content) worden z.s.m. daarna doorgevoerd, waarbij in het 3e kwartaal 2022 een hertest toegankelijkheid wordt uitgevoerd op rdw.nl. De testen worden door een onafhankelijke partij uitgevoerd. Dit heeft tot doel om via deze aanpak niveau A te bereiken.

Open API Specification (Beschrijven van REST API's)	Ja	
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/archivering)	Ja	
REST-API Design Rules	Nee	De bestaande REST-API's zijn niet tegen de REST-API Design Rules aangehouden.
SKOS (Thesauri en begrippen-woordenboeken)	Ja	
E-facturatie en administratie		
NLCIUS (Elektronisch factureren)	Nee	RDW meldt op de website hoe klanten e-facturen aan RDW kunnen versturen. Het is bij de beheerder niet duidelijk of daarin NLCIUS wordt gebruikt.
Ades Baseline Profiles	Gepland	De RDW voldoet op dit moment niet aan deze standaard. De RDW heeft een aanbesteding lopen waarmee voor ondertekening kan worden voldaan aan de Ades Baseline Profiles standaard. Naar verwachting vindt de implementatie Q4 2022 plaats.

Ten opzichte van 2020 voldoet de voorziening aan DMARC, HTTPS en HSTS, IPv4 en IPv6, TLS en de nieuwe standaarden NL GOV Assurance profile for OAuth 2.0 en RPKI. De status van DNSSEC en NLCIUS zijn ongewijzigd en blijven nee. De status van STARTTLS en DANE gaat van gepland naar nee. De voorziening voldoet daarnaast (nog) niet volledig aan de nieuwe standaard REST-API Design Rules. Voor Ades Baseline Profiles is een planning afgegeven. Op het gebied van de nieuwe standaard Digitoegankelijk voldoet de voorziening gedeeltelijk (status B).

Concluderend moeten voor RDW nog de volgende standaarden (volledig) worden geïmplementeerd: DNSSEC, REST-API Design Rules, STARTTLS en DANE, Digitoegankelijk, NLCIUS en Ades Baseline Profiles.

3.7. Rijksoverheid.nl

Voor deze voorziening worden het webdomein en maildomein door twee verschillende organisaties beheerd. In de rapportage worden om deze reden de resultaten van het webdomein van het maildomein gescheiden weergegeven.

Beheerorganisaties:

- **Webdomein: Dienst Publiek en Communicatie (DPC), Ministerie van Algemene Zaken**
- **Maildomein: SSC ICT**

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-mailadres @rijksoverheid.nl wordt gebruikt door mensen van het ministerie van BZK en samenwerkingsverbanden tussen verschillende ministeries.

Van het webdomein is DPC eigenaar en beheerder. DPC is tevens de beheerder van het hoofddomein voor de DNS.

Het e-maildomein @rijksoverheid.nl wordt technisch beheer door SSC-ICT. Door een gebrek aan afspraken is er echter geen beheereigenaar van het domein. SSC-ICT gaat dit bespreken op CIO-niveau met de ministeries van AZ en BZK. SSC-ICT wordt alleen door AZ aangestuurd op mailzaken waar er een relatie is met DNS en de mail/web-domeinen.

3.7.1. Resultaten webdomein:

Standaard	Status	Toelichting beheerder
Internet en beveiliging		
DNSSEC (Beveiligde domeinnamen)	Ja	Rijksoverheid.nl is ondertekend met DNSSEC (zie: https://internet.nl/site/www.rijksoverheid.nl/). DPC biedt DNSSEC ook aan aan al haar klanten die domeinen via haar registrar-functie afnemen.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening voldoet aan deze standaard (zie: https://internet.nl/site/www.rijksoverheid.nl/).
IPv4 en IPV6 (Internetnummers)	Ja	De website rijksoverheid.nl ondersteunt zowel IPv6 als IPv4 (zie: https://internet.nl/site/www.rijksoverheid.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De leveranciers hebben een NEN 27001/2 implementatie waarin de beveiliging van rijksoverheid.nl meegaat. DPC zelf valt onder de VIR/BIO-implementatie van het moederdepartement AZ.
RPKI (Beveiligen van de routing infrastructuur)	Ja	Wij publiceren bij onze hoster RPKI informatie voor al onze domeinen.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Het webdomein van rijksoverheid.nl voldoet aan TLS (zie: https://internet.nl/site/www.rijksoverheid.nl/).
Document en (web/app)content		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Deels (Status B)	Voldoen aan Toegankelijkheid is al jaren dagelijks onderdeel van ons werk: 'toegankelijkheid by design'. Dit geldt voor de redactionele teams en voor de functioneel/technische teams. Gezien de omvang van Rijksoverheid.nl zijn er altijd kleine, meestal redactionele elementen die niet voldoen. Die worden als verbetering opgepakt en ingepland. Redactioneel blijven vooral PDF documenten een probleem. PDF bestanden worden op alle ministeries op vele plekken gemaakt, met allerlei software, buiten de invloedsfeer van DPC. Deze PDF's zijn vaak niet toegankelijk.
ODF 1.2 (Documentbewerkingen)	Ja	Het Platform Rijksoverheid Online en dus ook Rijksoverheid.nl accepteert alleen het gebruik van de volgende formaten: odt, ods, odp, pdf, rtf, zip, epub, csv, xml, sha2
PDF 1.7 / PDF A/1 en PDF A/2 (Documentpublicatie/ archivering)	Deels	De centrale redactie van Rijksoverheid.nl stuurt waar mogelijk op het aanbieden van de juiste typen PDF's. De centrale redactie heeft echter beperkt zicht op soort en type PDF's die door decentrale redacteuren van de ministeries zelfstandig

		op rijksoverheid.nl worden geplaatst. Hierdoor worden er ook typen PDF gebruikt die buiten deze standaard vallen, bijvoorbeeld versie PDF 1.4 en 1.5.
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 2020 voldoet het webdomein van Rijksoverheid.nl aan RPKI. De status van PDF 1.7 / PDF A/1 en PDF A/2 is ongewijzigd en blijft deels. Op het gebied van de nieuwe standaard Digitoegankelijk voldoet de voorziening gedeeltelijk (status B).

Concluderend moeten voor het webdomein van Rijksoverheid.nl nog de volgende standaarden (volledig) worden geïmplementeerd: Digitoegankelijk en PDF 1.7 / PDF A/1 en PDF A/2.

3.7.2. Resultaten maildomein

Standaard	Status	Toelichting beheerder
Internet en beveiliging		
DKIM (Preventie van mailspoofing/ phishing)	Ja	DKIM is geïmplementeerd (zie: https://internet.nl/mail/rijksoverheid.nl/).
DMARC (Anti-phishing)	Ja	DMARC policy staat op reject, de meest strikte policy (zie: https://internet.nl/mail/rijksoverheid.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	Rijksoverheid.nl is ondertekend met DNSSEC (zie: https://internet.nl/mail/www.rijksoverheid.nl/). DPC biedt DNSSEC ook aan al haar klanten die domeinen via haar registrar-functie afnemen (zie: https://internet.nl/mail/rijksoverheid.nl/).
IPv4 en IPV6 (Internetnummers)	Ja	IPv6 is voor de mailservers geïmplementeerd (zie: https://internet.nl/mail/rijksoverheid.nl). Het technisch beheer van een aantal maildomeinen wordt uitgevoerd door SSC-ICT. De internet facing kant van de DMZ levert IPV6 sinds 2021
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De leveranciers hebben een NEN 27001/2 implementatie waarin de beveiliging van rijksoverheid.nl meegaat. DPC zelf valt onder de VIR/BIO-implementatie van het moederdepartement AZ. SSC-ICT zelf valt onder de VIR/BIO-implementatie van het moederdepartement MINBZK. SSC-ICT werkt via deze standaard en wordt hier ook op geaudit. De laatste audits hebben plaatsgevonden in 2019, 2020 en 2021.
SPF (Preventie van mailspoofing/phishing)	Ja	Het e-maildomein @rijksoverheid.nl is integraal van SPF voorzien (zie: https://internet.nl/mail/rijksoverheid.nl/). Deze wordt door SSC-ICT beheerd in samenwerking met AZ. Technisch gezien is SSC-ICT het aanspreekpunt.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	Verzendende mailservers die STARTTLS ondersteunen, kunnen met ontvangende mailserver(s) een beveiligde verbinding opzetten. Rijksoverheid.nl voldoet aan DANE (zie: https://internet.nl/mail/rijksoverheid.nl/). Deze wordt door SSC-ICT

		beheerd in samenwerking met AZ. Technisch gezien is SSC-ICT het aanspreekpunt.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De nieuwe versies en oude worden ondersteund. Best practice is de oude TLS versies aan laten staan op de mailservers i.v.m. interoperabiliteit.

Ten opzichte van 2020 voldoet de voorziening aan IPv4 en IPv6.

Concluderend kan worden gesteld dat het maildomein van Rijksoverheid.nl aan alle van toepassing zijnde standaarden voldoet.

3.8. WOZ Waardeloket

Beheerorganisatie: Kadaster
Werking en inhoud van WOZ-waardeloket
Het WOZ-waardeloket biedt de mogelijkheid de WOZ-waarde van woningen te raadplegen. Het WOZ-waardeloket is bedoeld voor het individueel raadplegen van afzonderlijke woningen. De getoonde WOZ-waarden zijn formeel door de desbetreffende gemeente vastgestelde WOZ-waarden. De gemeente is dan ook verantwoordelijk voor deze WOZ-waarde. Sommige getoonde objectkenmerken, zoals bouwjaar en gebruiksoppervlakte, zijn afkomstig uit de Basisregistratie Adressen en Gebouwen. Ook voor deze gegevens is de gemeente verantwoordelijk. De getoonde grondoppervlakte is afkomstig uit de Basisregistratie Kadaster.

Standaard	Status	Toelichting beheerder
Internet en beveiliging		
DMARC (Anti-phishing)	Deels	Centraal geregeld: deze standaard is geïmplementeerd en actief voor ons e-maildomein @kadaster.nl (zie: https://internet.nl/mail/kadaster.nl/). Er is geen mailserver voor het domein wozwaardeloket.nl en er is hiervoor geen DMARC policy quarantine of reject actief (zie: https://internet.nl/mail/wozwaardeloket.nl). De DMARC policy is daardoor niet voldoende strikt waardoor er niet aan de standaard wordt voldaan.
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC wordt ondersteund (zie: https://internet.nl/site/www.wozwaardeloket.nl).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	HTTPS en HSTS zijn geïmplementeerd (zie: https://internet.nl/site/www.wozwaardeloket.nl).
IPv4 en IPv6 (Internetnummers)	Ja	Exact dezelfde website is zowel over IPv4 als IPv6 bereikbaar (zie: https://internet.nl/site/www.wozwaardeloket.nl).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Het Kadaster is gecertificeerd voor NEN-ISO/IEC 27001 en hanteert 27002. Het Handboek Beveiliging Kadaster is volledig op de BIR gebaseerd. In het jaarverslag is een in control statement opgenomen.

RPKI	Ja	Controle toont aan dat juiste prefixen worden geaccepteerd en ongeldige prefixen worden afgewezen).
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd (zie: https://internet.nl/mail/wozwaardeloket.nl).
TLS (Beveiligde, versleutelde verbindingen)	Nee	Het Kadaster eist minimaal TLS 1.2. De inbraakdetectiesystemen (IDS) en inbraakpreventiesystemen (IPS) van het Kadaster hebben geen ondersteuning voor Secure Renegotiation. Het probleem raakt alle Kadaster endpoints. Tegenwoordig wordt het meeste verkeer op de IPS/IDS ontsleuteld om zicht te krijgen op aanvallen (threats). Wanneer de IDS/IPS een threat detecteert wordt de verbinding gereset. Daardoor houdt het Kadaster veel problemen buiten de deur. Het nadeel is dat pentesten door deze aanpak constateren dat het Kadaster Secure Renegotiation niet ondersteunt. Er wordt door onze IT-leverancier gezocht naar een oplossing voor dit probleem.
Document en (web/app)content		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Ja (Status A, voorlopig)	Het WOZ-waardeloket voldoet aan de eisen voor Digitoegankelijkheid. De website is net vernieuwd. Een zelfrapportage hiervoor komt later online.
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/ archivering)	Ja	Het WOZ-waardeloket biedt de mogelijkheid een schermafdruk van de gegevens in PDF 1.7-formaat te downloaden.

Ten opzichte van 2020 voldoet de voorziening aan de nieuwe standaard RPKI en PDF 1.7, A/1 en PDF A/2. De status van DMARC is van nee naar deels gegaan. De voorziening voldoet niet langer aan TLS. Op het gebied van de nieuwe standaard Digitoegankelijk voldoet de voorziening volledig (status A), maar hier is (voorlopig) nog geen zelfrapportage van aanwezig in het register met toegankelijkheidsverklaringen.

Concluderend moeten voor het WOZ-waardeloket nog de volgende standaarden (volledig) worden geïmplementeerd: DMARC en TLS.

4. Gegevens en registreren

4.1. NHR (Handelsregister)

Beheerorganisatie: Kamer van Koophandel
Werking en inhoud NHR
Het Handelsregister is de basisregistratie waarin alle rechtspersonen en ondernemingen in Nederland zijn opgenomen. Aansluiten op de Basisregistratie Handelsregister gaat om het tot stand brengen van een elektronische verbinding tussen het Handelsregister en de afnemer. Actuele gegevens uit het Handelsregister kunnen worden overgebracht via de informatieproducten van het Handelsregister. Bij de toetsing van NHR is dit jaar naar de website kvk.nl en de onderliggende systemen en koppelingen gekeken.

Standaard	Status	Toelichting beheerder
Internet en beveiliging		
DKIM (Preventie van mailspoofing/phishing)	Ja	Het domein kvk.nl voldoet aan DKIM (zie: https://internet.nl/mail/kvk.nl/).
DMARC (Anti-phishing)	Ja	NHR voldoet op mailservers aan DMARC (zie: https://internet.nl/mail/kvk.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	Dit is inmiddels geregeld voor alle kvk.nl domeinen.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening gebruikt zowel HTTPS als HSTS. Alleen voor kvk.nl werkt HSTS niet, dit is in 2019 hersteld. Was nog niet gebeurd omdat kvk.nl alleen redirect naar www.kvk.nl en deze werkt wel onder HSTS. Er was en is dus geen security risico.
IPv4 en IPv6 (Internetnummers)	Ja	Dit is geregeld voor alle kvk.nl domeinen. De website is beschikbaar op zowel IPv4 als IPv6 (± 20% van de bezoekers).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De KvK is sinds 2016 ISO 27001 gecertificeerd en hanteert ISO27002.
NL GOV Assurance profile for OAuth 2.0	Onbekend	*Geen antwoord van de beheerder*
RPKI	Nee	KvK moet de eerste stappen naar het toepassen van RPKI nog maken.
SAML (Inloggegevens)	Ja	eHerkenning is SAML-based en wordt toegepast voor het aanleveren van jaarrekeningen en informatieverstrekking. In de notarisapplicatie kan de notaris van achter zijn computer rechtstreeks opgave doen. Ook hier wordt gebruik gemaakt van SAML als authenticatieprocedure. Omdat gebruik wordt gemaakt van een generiek identificatie- en authenticatiesysteem voor alle diensten van KvK kan SAML voor elke dienst ingezet worden voor authenticatie.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd voor NHR.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Nee	Deels afgedekt, maar er zijn nog openstaande acties, waardoor niet al het smtp verkeer over de actuele versie van TLS gaat.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De mailserver kvk-nl.mail.protection.outlook.com ondersteunt nog TLS 1.1. Dit is een externe mailserver. De leverancier (Microsoft) dient de TLS versies uit te faseren. De KVK zal dit opnemen met de leverancier. Op deze mailserver wordt ook TLS 1.2 ondersteunt. KVK is actief bezig om alle TLS implementaties op versie 1.3 te krijgen, daarbij is ook de Wet Digitale Overheid een belangrijke aanleiding. Dat verloopt voorspoedig. Een uitzondering geldt voor een stuk legacy-programmatuur (AS/400 software) waar TLS 1.0 nog wordt

		gebruikt. Hiervoor zal een exceptie met risicoanalyse worden opgesteld ter nadere bespreking. In afwachting van de uitfasering van deze legacy willen wij zo min mogelijk aanpassingen daarin doen. Het uitfaseren van deze legacy heeft nogal wat vertraging bij ons opgelopen, waardoor dit in 2022 nog niet is afgerond.
Document en (web/app)content		
Ades Baseline Profiles (Digitaal ondertekenen van documenten)	Ja	De NHR voldoet aan de Ades Baseline Profiles standaard.
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Deels (Status C)	De toegankelijkheid van onze corporate website, incl. genomen en nog te nemen maatregelen worden daar gepubliceerd. Zie https://www.kvk.nl/toegankelijkheid/. Inzake pdf-documenten, voldoen de door KvK aangemaakte, verstrekte pdf's aan de vereiste versie. Een openstaande actie is de mobiele website via de HR app. Er is pas recent besloten hier mee door te gaan (eerder was besloten hier mee te gaan stoppen) zodat de acties om te voldoen aan Digitoegankelijkheidseisen nog moeten worden genomen.
Open API Specification (Beschrijven van REST API's)	Deels	Nieuwe of gewijzigde API's van KVK voldoen hieraan. De oudere, bestaande nog niet, dit werk staat nu voor Q4 van 2022 gepland.
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.
REST-API Design Rules	Ja	KvK hanteert de design rules.
SKOS (Thesauri en begrippen-woordenboeken)	Gepland	De realisatie van onze gegevenscatalogus m.b.t. SKOS heeft vertraging opgelopen door andere prioriteiten inzake de gegevenscatalogus m.b.t. actualiteit en volledigheid. Dit project (SKOS variant) is naar 2023 geschoven.
Stelselstandaarden		
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Ongeveer 10% van het verkeer van het NHR gaat naar medeoverheden. Die uitwisselingen vinden allemaal plaats via Digikoppeling en StUF.
StUF (Uitwisseling administratieve overheidsgegevens)	Ja	Ongeveer 10% van het verkeer van het NHR gaat naar medeoverheden. Die uitwisselingen vinden allemaal plaats via Digikoppeling en StUF.
E-facturatie en administratie		
NLCIUS (Elektronisch factureren)	Nee	Dit is helaas nog niet gebeurd vanwege andere prioriteiten en resource-problemen bij ons team hiervoor.

Ten opzichte van 2020 voldoet de voorziening aan DNSSEC en IPv4 en IPv6. De status van STARTTLS en DANE is van gepland naar nee gegaan. De status van Open API Specification, SKOS en NLCIUS zijn ongewijzigd. De status van de nieuwe standaard NL GOV Assurance profile for OAuth 2.0 is

onbekend. De voorziening voldoet aan de nieuwe standaard REST-API Design Rules, maar nog niet aan de nieuwe standaard RPKI. Op het gebied van de nieuwe standaard Digitoegankelijk zijn de eerste maatregelen genomen (status C).

Concluderend, moeten voor NHR nog de volgende standaarden (volledig) worden geïmplementeerd: STARTTLS en DANE, RPKI, Digitoegankelijk, Open API Specification, SKOS, NLCIUS, en mogelijk NL GOV Assurance profile for OAuth 2.0.

4.2. PDOK

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

Standaard	Status	Toelichting
Internet en beveiliging		
DKIM (Preventie van mailspoofing/phishing)	Ja	Het Kadaster voldoet aan DKIM.
DMARC (Anti-phishing)	Ja	Deze standaard is geïmplementeerd.
DNSSEC (Beveiligde domeinnamen)	Ja	De website www.pdok.nl ondersteunt DNSSEC (zie: https://internet.nl/domain/www.pdok.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Nee	HSTS-policy wordt gebruikt, de webservers ondersteunen HSTS. Uit de test op internet.nl komen nog enkele issue's naar voren die bekend zijn. We zijn in overleg met de leverancier om verbeteringen door te voeren rondom HTTPS en HSTS.
IPv4 en IPv6 (Internetnummers)	Ja	Zowel IPv4 als IPv6 worden ondersteund door het Kadaster (zie: https://internet.nl/domain/www.pdok.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Het Kadaster is gecertificeerd voor NEN-ISO/IEC 27001 en hanteert 27002. Het Handboek Beveiliging Kadaster is volledig op de BIR gebaseerd en is deels door standaarden op basis van de BIO vervangen. In het jaarverslag is een in control statement opgenomen.
RPKI	Ja	RPKI wordt toegepast
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd (zie: https://internet.nl/mail/pdok.nl/).
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	STARTTLS en DANE zijn geïmplementeerd (zie: https://internet.nl/mail/pdok.nl/).

TLS (Beveiligde, versleutelde verbindingen)	Ja	Deze standaard wordt volledig door het Kadaster ondersteund (zie: https://internet.nl/domain/www.pdok.nl/). PDOK volgt de richtlijnen van het NCSC voor TLS. Hieruit blijkt dat mogelijke problemen met cipher-volgorde wat betreft vertrouwelijkheid geen risico vormen, omdat de data openbaar is volgens de BIV classificatie.
Document en (web/app)content		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Deels (Status C)	Er is een toegankelijkheidsverklaring voor PDOK, zie https://www.pdok.nl/toegankelijkheid. We voldoen nog niet voor 100% aan de WCAG richtlijnen.
Open API Specification (Beschrijven van REST API's)	Ja	Deze standaard is geïmplementeerd en wordt toegepast.
REST-API Design Rules	Nee	PDOK voldoet niet aan deze standaard. Het doel van PDOK is om te voldoen aan de OGC API standaarden
Stelselstandaarden		
Geo-standaarden	Ja	PDOK maakt gebruik van OGC en INSPIRE standaarden voor haar webservices. Webservices kennen verschillende formaten qua uitlevering. Downloads worden via formaten GeoPackages en GML aangeleverd en uitgeserveerd.
StUF	Ja	Voor het uitserveren van de BGT.

Ten opzichte van 2020 is de status van HTTPS HSTS van gepland naar nee gegaan. De voorziening voldoet aan de nieuwe standaard RPKI. De voorziening voldoet (nog) niet aan de nieuwe standaard REST-API Design Rules. Op het gebied van de nieuwe standaard Digitoegankelijk zijn de eerste maatregelen genomen (status C).

Concluderend moeten voor PDOK nog de volgende standaarden (volledig) worden geïmplementeerd: HTTPS en HSTS, Digitoegankelijk en de REST-API Design Rules.

5. Dienstverlening en verbinden

5.1. TenderNed

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

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

Standaard	Status	Toelichting beheerder
Internet en beveiliging		
DKIM (Preventie van mailspoofing/phishing)	Ja	E-mails verzonden vanuit TenderNed zijn beveiligd met DKIM (zie: https://internet.nl/mail/tenderned.nl/).

DMARC (Anti-phishing)	Ja	Dienstverlener DICTU heeft DMARC aangezet.
DNSSEC (Beveiligde domeinnamen)	Ja	Het domein is gesigned met DNSSEC (zie: https://internet.nl/site/www.tenderned.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	Configuratie aanpassing is doorgevoerd om ook HSTS volledig te ondersteunen.
IPv4 en IPV6 (Internetnummers)	Ja	Configuratie aanpassing is doorgevoerd op ook IPV6 volledig te ondersteunen.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	TenderNed is ISO27001/2 gecertificeerd. Dit wordt jaarlijks geaudit.
RPKI	Ja	De dienstverlener van TenderNed geeft aan te voldoen aan RPKI.
SAML (Inloggegevens)	Ja	Per 1 juli 2014 is het mogelijk voor gebruikers om, naast de huidige registreer- en inlogmogelijkheden, gebruik te maken van inloggen via eHerkenning.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is inmiddels aangezet door de technisch dienstverlener DICTU (zie: https://internet.nl/mail/tenderned.nl/).
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	STARTTLS en DANE worden ondersteund.
TLS (Beveiligde, versleutelde verbindingen)	Ja	TenderNed past TLS 1.2 toe (zie: https://internet.nl/site/www.tenderned.nl/). Voor een aantal koppelingen wordt nog TLS 1.0 gebruikt voor compatibiliteit.
Document en (web/app)content		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Deels (Status B)	We hebben op dit moment de B status. We zijn in onderzoek om de A status behalen.
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. We zijn aan het onderzoeken om onze Swagger specificaties om te zetten naar OAS 3.0 specificaties.
REST-API Design Rules	Nee	Voldoet TenderNed nog niet volledig aan. We zijn in onderzoek hoe wij aan alle regels kunnen voldoen.
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 2020 voldoet de voorziening aan HTTPS en HSTS, IPv4 en IPv6 en aan de nieuwe standaard RPKI. De status van Open API Specification is ongewijzigd en blijft nee. Op het gebied van de nieuwe standaard Digitoegankelijk voldoet de voorziening gedeeltelijk (status B).

Concluderend moeten voor TenderNed nog de volgende standaarden (volledig) worden geïmplementeerd: Digitoegankeljik, Open API Specification en REST-API Design Rules.

5.2. DigiInkoop

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

DigiInkoop wordt volledig uitgefaseerd in juli 2023. Vervanging van het leverancierssportaal DigiInkoop zal vanaf eind juli 2022 zijn gerealiseerd. Hierbij wordt rekening gehouden met de implementatie van de van toepassing zijnde open standaarden.

Standaard	Status	Toelichting beheerder
Internet en beveiliging		
DKIM (Preventie van mailspoofing/phishing)	Ja	DKIM is volledig geïmplementeerd. (zie: https://internet.nl/mail/digiinkoop.nl/).
DMARC (Anti-phishing)	Ja	DMARC is volledig geïmplementeerd met voldoende strikte policy.
DNSSEC (Beveiligde domeinnamen)	Ja	DigiInkoop voldoet aan DNSSEC (zie: https://internet.nl/mail/digiinkoop.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening voldoet aan HTTPS en HSTS.
IPv4 en IPV6 (Internet-nummers)	Ja	IPv4 en IPv6 zijn geïmplementeerd.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	DigiInkoop voldoet aan de BIO. Er is een in control statement afgegeven. Leverancier Ordina voldoet aan ISO 27001.
RPKI	Nee	Logius als houder van de IP-adressen voldoet aan deze standaard. Echter als leverancier DigiInkoop maakt Ordina gebruik van diensten van Oracle. Oracle voldoet niet aan deze standaard. In Q3 zullen werkzaamheden worden verricht om te voldoen aan de standaard RPKI
SPF (Preventie van mailspoofing/phishing)	Ja	DigiInkoop voldoet aan deze standaard (zie: https://internet.nl/mail/digiinkoop.nl/).

TLS (Beveiligde, versleutelde verbindingen)	Ja	DigiInkoop is TLS 1.2 compliant (zie: https://internet.nl/mail/digiinkoop.nl/). mta.dc.ordina.nl is uitgefaseerd.
Document en (web/app)content		
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Deels (Status C)	DigiInkoop voldoet niet aan de vereiste toegankelijkheid standaard. Echter DigiInkoop wordt volledig uitgefaseerd in juli 2023. Vervanging van het leverancierssportaal DigiInkoop zal vanaf eind juli 2022 zijn gerealiseerd. Het nieuwe leverancierssportaal voldoet aan de vereiste standaard.
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. Zie: https://www.logius.nl/diensten/digiinkoop/hoe-werkt-het/ubl-ohnl en https://www.logius.nl/ondersteuning/gegevensuitwisseling/setu-hr-xml-ohnl).
E-facturatie en administratie		
NLCIUS (Elektronisch factureren)	Ja	Per 19 april 2019 is de NLCIUS verplicht voor overheden, volgens Europese richtlijn 2014/55/EU. De SMEF 2.0 standaard wordt opgevolgd door de NLCIUS. Implementatie is conform planning in Q2 2019 gerealiseerd.
SETU (Informatie flexibele arbeidskrachten)	Ja	DigiInkoop ondersteunt de uitwisseling van SETU-hr-XML berichten. Uitfaseren van oude versie doet SETU bijna niet, dus 'standaarden-technisch' zijn alle versienummers actueel (ook oudere). Op Digipoort en in EPV staat: - SETU 1.2 voor HumanResource en StaffingOrder en - SETU 1.3 voor Invoice en TimeCard. - SETU 2.2 voor Invoice = de NLCIUS variant (de SETU factuur via Digipoort moet gekenmerkt worden als NLCIUS).

Ten opzichte van 2020 voldoet de voorziening aan DMARC en IPv4 en IPv6. De voorziening voldoet niet aan de nieuwe standaard RPKI. Op het gebied van de nieuwe standaard Digitoegankelijk zijn de eerste maatregelen genomen (status C). De beheerder geeft aan de digitoegankelijkheid wordt meegenomen bij de invoering van het nieuwe portaal.

Concluderend moeten voor DigiInkoop nog de volgende standaarden (volledig) worden geïmplementeerd: RPKI en Digitoegankelijk.

Bijlage A: Pas toe of leg uit-lijst per 1 april 2022

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

De dit jaar onderzochte voorzieningen zijn hiervoor voor het laatst onderzocht in 2020. Sinds dit meetmoment zijn de volgende standaarden nieuw op de lijst gekomen:

- Digitoegankelijk (EN 301 549 met WCAG 2.1)
- NL GOV Assurance Profile for OAuth 2.0
- REST-API Design Rules
- RPKI

Ten opzichte van 2020 staan de volgende standaarden niet langer op de lijst:

- CMIS
- OWMS (OWMS was ten tijde van uitvoering van het onderzoek *onder behandeling* en wordt waarschijnlijk vervangen door een nieuwe standaard)

Bijlage B: Contactpersonen of beheerders per voorziening

Naam voorziening	Contactpersoon
DigiInkoop	Jeroen Dooremolen
DigiD	Evert Jan van der Marck
DigiD Machtigen	Ruben Tromp
Stelsel elektronische toegangsdiensten	Sander Boer
MijnOverheid	Moussa Sabili
PKIoverheid	Jochem van den Berge
Rijksoverheid.nl (webdomein)	Gerrit Berkouwer
Rijksoverheid.nl (maildomein)	Cees Vaes
Samenwerkende Catalogi	Kristian Mul
Berichtenbox voor bedrijven	Alec Oosterink
NHR	Rob Spoelstra
Ondernemersplein	Gaico Aertssen
Overheid.nl	Erna Wisselaar
PDOK	Finn Tiebout
RDW.nl	Gert Stel
Tenderned	Rudi van Eijk
WOZ-waardeloket	Rijk van Haaften

ICTU

Rapport

B4. Inventarisatie gebruiksgegevens 2022 door BFS

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

Net als vorig jaar is dit deelonderzoek dit jaar uitgevoerd door de accountmanagers van het Bureau Forum Standaardisatie (BFS). Helaas is het niet altijd even eenvoudig om (voor alle open standaarden) vast te stellen in welke mate die feitelijk door overheden gebruikt worden. De accountmanagers van BFS hebben hiervoor contact opgenomen met beheerders van standaarden en sommige specifiek voor de standaard relevante voorzieningen. Voor een aantal standaarden uit het domein Internet en beveiliging zijn de gebruiksgegevens afkomstig uit het halfjaarlijkse onderzoek naar internet-veiligheids-standaarden (zie Meting informatieveiligheidstandaarden overheid voorjaar 2022, augustus 2022, opgenomen in Bijlage B6). De peildatum van deze meest recente IV-meting is -in afwijking van eerdere peildata (maart en september)- mei 2022.

Over het gebruik van de volgende zes standaarden is dit jaar geen (actuele) informatie beschikbaar: NL GOV, Ades Baseline Profiles, OpenAPI Specification, REST-API Design Rules, COINS en SAML.

B4.1. Domein Internet en beveiliging

Voor een aantal standaarden binnen dit domein is zoals gezegd gebruik gemaakt van de opbrengst van de meting IV-standaarden door Forum Standaardisatie. Het betreft de volgende standaarden: DKIM, DMARC, SPF, DNSSEC, HTTPS & HSTS, TLS, IPv6 en IPv4 en STARTTLS & DANE.

In de meest recente meting (mei 2022) zijn 2.584 domeinnamen getoetst. Vorig jaar (Monitor 2021) was nog sprake van een onderscheid tussen een groep 559 primaire (veelgebruikte) internetdomeinen waarop in de IV-meting de focus lag en een bredere selectie van circa 2.200 overheidsdomeinnamen. Een soortgelijke exercitie is in de Monitor 2020 voor het eerst geïntroduceerd. In die twee monitor-rapportages zijn de uitkomsten van de beide metingen (primair en bredere meting) met elkaar vergeleken. De rode draad bij die vergelijking: een behoorlijk verschil waarbij de uitkomst van de bredere meting over de volle breedte lagere scores laat zien dan die van de meting op de primaire domeinen.

Een dergelijk onderscheid is er dit jaar niet meer; nu is alleen een meting beschikbaar van wat voorheen de bredere groep werd genoemd. Gezien het bovenstaande is het niet verantwoord om een goede vergelijking te maken tussen de meting van dit jaar en die van de voorafgaande jaren, waarbij een analyse op de kerndomeinen centraal stond. Ook een vergelijking met de eerdere bredere metingen van de afgelopen twee jaren is niet goed te maken. Daarvoor verschilt de samenstelling van de bredere groep teveel. Daarom is ervoor gekozen een herstart te maken met de presentatie van de open standaarden die in de IV-

meting zijn onderzocht. Dat betekent dat de uitkomst dit keer niet in een tijdsperspectief kan worden geplaatst.

DKIM, DMARC en SPF

Waarom belangrijk ?

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

- DKIM: dit is een techniek waarmee e-mailberichten kunnen worden gewaarmerkt. Een domeinnaamhouder kan in het DNS-record van de domeinnaam aangeven met welke sleutel e-mail namens de betreffende domeinnaam ondertekend moet worden (op de 'pas toe of leg uit' lijst sinds juni 2012 - we vermelden telkens de oorspronkelijke plaatsing op de 'pas toe of leg uit'-lijst);
- DMARC: maakt het mogelijk om beleid in te stellen over de manier waarop een e-mailprovider om moet gaan met e-mail waarvan niet kan worden vastgesteld dat deze afkomstig is van het vermelde afzenderdomein. Hierdoor kunnen organisaties voorkomen dat anderen e-mails versturen namens het e-maildomein van de organisatie (op de 'pas toe of leg uit'-lijst sinds mei 2015);
- SPF: dit is een techniek waarmee een domeinhouder de IP-adressen van verzendende mailservers kan publiceren in de DNS. Een ontvangende mailserver kan deze IP-adressen gebruiken om te controleren of een e-mail daadwerkelijk afkomstig is van een verzendende mailserver van de betreffende domeinhouder (op de 'pas toe of leg uit'-lijst sinds mei 2015).

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaarden kijken we naar de ondersteuning van DMARC, DKIM en SPF op 2.584 domeinen van de overheid. Zie hiervoor de IV-meting van voorjaar 2022 (Bijlage B.).

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 validatie van de DMARC-, DKIM- en SPF-kenmerken door ontvangende mailservers van een overheidsorganisatie niet worden gemeten.

	voorjaar 2022
DMARC policy	72 %
DKIM	82 %
SPF Policy	87 %

Het gebruik van anti-phishing standaarden ligt bij de hier gepresenteerde standaarden grofweg rond de 80%, met DMARC als relatieve achterblijver (72%). Dat betekent dat voor 28% van de internetdomeinen nog een strikt DMARC-beleid operationeel moet worden om phishingmails uit naam van overheidsorganisaties te voorkomen. In een volgende monitor-rapportage kunnen deze cijfers in perspectief worden geplaatst.

Een uitsplitsing van deze cijfers naar type overheid laat een volgend beeld zien.

	Centrale overheid (n=1.787)	Provincies (n=22)	Water-schappen (n=30)	Gemeenten (n=359)	Gemeen-schappelijke regelingen (n=378)
DMARC policy	74 %	68 %	87 %	86 %	48 %
DKIM	78 %	82 %	97 %	99 %	82 %
SPF Policy	86 %	77 %	93 %	95 %	84 %

In dit overzicht vallen met name de relatief hoge scores op bij de drie laatstgenoemde overheidscategorieën: de waterschappen, de gemeenten en de gemeenschappelijke regelingen.

DNSSEC

Waarom belangrijk ?

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

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaard kijken we wederom naar het gebruik van DNSSEC-handtekeningen op 2.558 webdomeinen respectievelijk 1.493 email-server-domeinen van de overheid. Zie hiervoor de IV-meting van voorjaar 2022 (Bijlage B.).

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

DNSSEC	voorjaar 2022
op web-domein	89 %
op mailserver-domein	57 %

Bij webdomeinen is sprake van een hoge score (89%), voor mailserverdomeinen ligt dit beduidend lager (57%). In de IV-meting wordt over dit laatste opgemerkt dat leveranciersondersteuning door met name clouddienstverleners de grootste implementatiedrempel is voor DNSSEC (ook voor DANE). Uit diezelfde IV-meting: "Het is belangrijk dat overheden die nog niet voldoen hun leverancier blijven vragen om ondersteuning van deze standaarden."

In een volgende monitor-rapportage kunnen deze cijfers in perspectief worden geplaatst.

Een uitsplitsing van deze cijfers naar type overheid laat een volgend beeld zien.

	Centrale overheid (n=1.769 resp. 730)	Provincies (n=22 resp. 18)	Water-schappen (n=30 voor beide)	Gemeenten (n=359 resp. 354)	Gemeen-schappelijke regelingen (n=378 resp. 361)
DNSSEC web	89 %	95 %	100 %	99 %	80 %
DNSSEC mail	66 %	28 %	40 %	57 %	39 %

Op webdomeinen scoren de verschillende categorieën overheid hoog tot zeer hoog, waarbij de gemeenschappelijke regelingen iets achterblijven (met altijd nog 80%). Bij maildomeinen scoort de centrale overheid met 66% het hoogst, en gemeenten zitten op het overall gemiddelde van 57%. De andere drie categorieën scoren duidelijk onder-gemiddeld. De eerdere opmerking hierboven met betrekking cloud-dienstverleners voor email-verkeer is hierbij een factor van belang ter verklaring van de lage scores.

HTTPS & HSTS en TLS

Waarom belangrijk ?

HTTPS & HSTS en ook TLS zorgen samen voor beveiligde verbindingen met websites, met als doel de veilige uitwisseling van gegevens tussen een webserver en client (vaak een webbrowser). Dit maakt het voor cybercriminelen moeilijker om verkeer om te leiden naar valse websites en om de inhoud van webverkeer te onderscheppen.
HTTPS zorgt voor het gebruik van HTTP over een met TLS beveiligde verbinding. Dit betekent dat het webverkeer door middel een certificaat wordt versleuteld.
HSTS zorgt ervoor dat een webbrowser, na het eerste contact over HTTPS, bij vervolgbezoek de website altijd direct over HTTPS opvraagt.
Deze standaarden staan op de ‘pas toe of leg uit’-lijst sinds mei 2017.

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

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaarden kijken we naar het gebruik op 2.558 webdomeinen van de overheid. Zie ook de IV-meting van voorjaar 2022 (Bijlage B.).

	voorjaar 2022
HTTPS doorv.	92 %
HSTS	75 %
TLS cf. NCSC	75 %

Op basis van deze cijfers blijkt dat bij drie van de vier in het onderzoek betrokken webdomeinen de TLS- en HSTS-configuraties op orde zijn. Voor HTTPS ligt deze score hoger (meer dan negen van de tien). In volgende monitor-rapportages kunnen deze cijfers in perspectief worden geplaatst.

Een uitsplitsing van deze cijfers naar type overheid laat een volgend beeld zien.

	Centrale overheid (n=1.769)	Provincies (n=22)	Water-schappen (n=30)	Gemeenten (n=359)	Gemeen-schappelijke regelingen (n=378)
HTTPS doorv.	91 %	82 %	100 %	99 %	92 %
HSTS	75 %	91 %	93 %	97 %	52 %
TLS cf. NCSC	72 %	95 %	97 %	94 %	66 %

De centrale overheid – met verreweg de grootste groep webdomeinen – laat een score zien die vrijwel overeenkomt met het overall beeld[1]. Verder valt op dat zowel gemeenten als waterschappen hele hoge scores laten zien, duidelijk meer dan de andere overheids-categorieën. De gemeenschappelijke regelingen blijven achter. Als duiding daarvan wordt in de IV-meting verondersteld dat " … de streefbeeldafspraken niet doorgesijpeld [zijn] naar deze instanties, hoewel zij in veel gevallen gefinancierd worden vanuit de andere overheden."

IPv6 & IPv4

Waarom belangrijk ?

De standaard bepaalt dat ieder ICT-systeem binnen het netwerk een uniek nummer (IP-adres) heeft. Hierdoor kunnen ICT-systemen elkaar herkennen en onderling data uitwisselen. IPv6 heeft een veel grotere hoeveelheid beschikbare IP-adressen ten opzichte van de voorganger IPv4. Dit maakt verdere groei en innovatie van het internet mogelijk. IPv6 is niet backwards compatible. Dit wil zeggen dat een IPv4-systeem niet een IPv6-systeem kan bereiken, of andersom. Om die reden moet een organisatie bij de aanschaf van een ICT-product/-dienst beide versies uitvragen. De standaard staat op de 'pas toe of leg uit' lijst sinds november 2010.

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaard kijken we naar de bereikbaarheid van overheids-websites via de internetstandaard IPv6 voor 2.558 webdomeinen respectievelijk 2.584 voor e-mailverkeer van de overheid.

IPv6	voorjaar 2022
webverkeer	70 %
e-mailverkeer	50 %

[1] De IV-monitor biedt aanvullend inzicht van deze categorie, uitgesplitst naar ministerie.

De adoptie van IPv6 voor e-mailverkeer ligt in deze meting op de helft (50%). De score voor webverkeer is beter, met 70% adoptiegraad. In volgende monitor-rapportages kunnen deze cijfers in perspectief worden geplaatst.

Een uitsplitsing van deze cijfers naar type overheid wijst het volgende uit.

	Centrale overheid (n=1.769 resp. 1.787)	Provincies (n=22 voor beide)	Water-schappen (n=30 voor beide)	Gemeenten (n=359 voor beide)	Gemeen-schappellijke regelingen (n=378 resp. 386)
webverkeer	68 %	82 %	97 %	94 %	49 %
emailverkeer	52 %	72 %	43 %	64 %	33 %

De centrale overheid scoort dicht bij het over-all gemiddelde voor beide variabelen. En terwijl provincies en gemeenten duidelijk bovengemiddeld scoren, blijft de categorie 'gemeenschappelijke regelingen' op beide variabelen duidelijk achter.

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

Waarom belangrijk ?

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

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

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

De Nederlandse overheid heeft haar eigen kaders voor informatiebeveiliging die zijn afgeleid van de 27001- en 27002-normen. Tot 2019 hadden alle bestuurslagen een eigen baseline, de BIR (Rijk), BIG (gemeenten), IBI (provincies) en BIWA (waterschappen). Deze baselines zijn (met uitzondering van de BIR2017) voor een groot deel nog gebaseerd op de ISO-normering uit 2005 en lopen achter op de actuele ISO-normen. De BIO is gebaseerd op de actuele, internationale standaard voor informatiebeveiliging (NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002) en heeft risicomanagement als uitgangspunt. Alle overheidslagen hebben zichzelf verplicht de BIO toe te passen. Forum Standaardisatie heeft medio 2018 reeds geadviseerd om actief op adoptie van de BIO in te zetten, en de voortgang te monitoren. In reactie

daarop heeft de werkgroep BIO aangegeven dat iedere overheidslaag zelf zal monitoren wat de voortgang is van de implementatie van de BIO. Vanaf 1 januari 2019 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines voor Rijk, Gemeenten, Waterschappen en Provincies.

Feitelijk gebruik

Voor de Monitor 2022 zijn door de verschillende overheidslagen geen kwantitatieve gegevens over het gebruik van hun beveiligingsbaselines aangeleverd. Verantwoording over de beveiliging vindt in beginsel plaats aan de eigen controlerende organen.

Rijksoverheid

CIO Rijk meldt dat de opvolger van de BIR2017, de BIO 1.04, op 11-2-2020 is gepubliceerd in de staatcourant en geldt voor alle overheidslagen. In 2020 hebben de departementen in de jaarlijkse CISO-gesprekken gemeld dat BIO 1.04 is of wordt geïmplementeerd. Een aantal departementen heeft ervoor gekozen om de BIO 1.04 in eigen departement specifieke baselines op te nemen. De departementen hebben aangegeven dat de initiële implementatie van de BIO 1.04 risicogericht is afgerond en dat via de PDCA-cyclus de implementatie actueel wordt gehouden. De BIO wordt momenteel geëvalueerd en de Rijksoverheid doet mee aan de evaluatie. Toepassing van de BIO is inmiddels dus onderdeel van de PDCA-cyclus.

Provincies

Alle provincies zijn bezig met het implementeren van de BIO en doen dat in combinatie met de ambitie om ISO 27001 certificeerbaar te worden voor 1 of meerdere processen.

In 2021 was één provincie ISO 27001 en BIO gecertificeerd (vorig jaar ook één provincie). Dit is gerealiseerd door de BIO als extra normenkader aan de 27001-certificering toe te voegen. Diverse andere provincies waren in 2021 ook bezig met een ISO 27001-certificeertraject en nemen daar de BIO ook expliciet in mee (vorig jaar twee provincies).

Daarnaast zullen alle provincies op basis van risicoanalyses het juiste BBN niveau bepalen en daar de juiste maatregelen voor implementeren.

In de 2e helft 2021 hebben alle provincies een audit ondergaan, door dezelfde auditor. Op basis van deze auditresultaten hebben de provincies hun aanpak voor de komende periode bepaald om de certificeerbaarheid te realiseren.

Waterschappen

Terugblikkend is de BIO bestuurlijk vastgesteld in de Ledenvergadering van 12 oktober 2018 van de Unie van Waterschappen. De BIO is daarmee vanaf 1 januari 2020 van toepassing.

Waterschappen zijn bezig met de volwaardige implementatie van de BIO; zij gebruiken alle de BIO als normenkader voor informatiebeveiliging. Deze is aangevuld met de IEC62443, specifiek voor procesautomatisering

Naast de individuele verbeteracties wordt in gezamenlijkheid gewerkt aan het verhogen van de digitale weersrand van zowel de sector, als ook die van ketenpartners. In onderlinge samenwerking wordt onder meer gewerkt aan de ontwikkeling van een sectormethodiek van risicoanalyses, een CyberSecurity Implementatie Richtlijn (CSIR) en een ketenanalyse methodiek. Voortgang van de individuele en sectorale voortgang is dit jaar door een onafhankelijke partij beoordeeld. De resultaten van deze audit zijn zowel op individueel, als ook op sectoraal niveau, door de auditor voorzien van aanbevelingen. Waterschappen werken zowel sectoraal als individueel aan het verhogen van de digitale weerbaarheid. In 2024 zal opnieuw een sector brede audit uitgevoerd worden.

Gemeenten

Implementatie van de BIO is een doorlopend proces van plannen, uitvoeren, controleren en bijstellen. Gemeenten leggen jaarlijks verantwoording af aan de eigen gemeenteraad over de implementatie van de BIO middels ENSIA (de Eenduidige Normatiek Single Information Audit). Daarmee hanteert 100% van de gemeenten de BIO als normenkader.

Het geheel van overheidslagen overziend wordt de vraag in welke mate een en ander inmiddels conform BIO is ingericht weinig concreet beantwoord. De passages die betrekking hebben op de verschillende overheidslagen beperken zich voornamelijk tot een procedurele insteek, waaruit blijkt dat men ermee bezig is. Een vergelijking met de stand van zaken vorig jaar is dan ook niet goed te maken.

Relevante ontwikkeling

De BIO wordt op dit moment geëvalueerd door overheidspartijen en zal in navolging van de vernieuwde ISO normering van V1.04 naar V2.0 gaan.

NL GOV Assurance

Net als vorig jaar is ook dit jaar geen informatie beschikbaar over de drie API-standaarden. Mogelijk komt daar de komende jaren verandering in getuige het volgende bericht.

Forum Standaardisatie heeft sinds enkele jaren verplichte API standaarden op de 'Pas toe of leg uit'-lijst. Deze standaarden dragen bij aan betere informatievoorziening voor goede dienstenverlening aan bedrijven en burgers. Gezien het belang van API's voor de digitale overheid is het noodzakelijk om het gebruik van verplichte API-standaarden te meten en hierover te rapporteren in de Monitor open standaarden. Er is behoefte deze meting te faciliteren middels een testtool aangevuld met dynamische meetrapportages. Eind 2021 heeft Bureau Forum Standaardisatie (BFS) hiervoor een opdracht uitgezet om de testtool in te bouwen in developer.overheid.nl, een centrale plek voor alle API's van de overheid. Voor het verder aanjagen van adoptie zal BFS deze testtool gebruiken om meer inzicht te krijgen in het voldoen aan de verplichte API standaarden en implementatiegraad. De testtool en meetrapportage wordt ook beschikbaar gesteld aan de partij die de Monitor open standaarden oplevert. Bovendien komt er een publiek toegankelijk dashboard met dynamische meetrapportages. De verwachting is dat eind 2022 de opdracht tot afronding komt en begin 2023 de testtool als ook de meetmogelijkheden volledig operationeel zijn.

RPKI

Waarom belangrijk ?

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

Feitelijk gebruik

Vorig jaar zijn vragen voorgelegd aan 14 deelnemers aan Overheidsbrede Verdiepingssessies Connectiviteit, georganiseerd door Logius. Daarop hebben toen elf organisaties gereageerd. Dit jaar zijn 16 organisaties aangeschreven. Van niet meer dan 7 organisaties is een (soms gedeeltelijke) reactie ontvangen: de Belastingdienst, de politie, de VNG, SSC ICT, Logius en de ministeries van Defensie en Justitie en veiligheid. Dit leidt ertoe dat – met een toch al smalle basis van respondenten – een vergelijking met vorig jaar niet gemaakt kan worden.

De vraagstelling is dit jaar grotendeels hetzelfde als vorig jaar. De eerste drie vragen zijn identiek en luiden aldus:

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

Hieraan is dit jaar nog een vierde vraag toegevoegd, alleen aan de orde als de eerste en/of de derde vraag met 'nee' is beantwoord. In dat geval wordt gevraagd naar een eventuele planning: op welke termijn de organisatie van plan is dit (volledig) te gaan doen.

De eerste vraag wordt door vier van de zeven respondenten bevestigend beantwoord (vorig jaar: zeven van de elf).

De tweede vraag wordt door één enkele organisatie met "ja" beantwoord (vorig jaar twee), door één organisatie met deels (net als vorig jaar). Let wel: deze vraag is voor drie van de zeven organisaties niet van toepassing omdat bij hen geen sprake is van IP-adressen van leveranciers.

Bij de laatste van de drie vragen reageren twee organisaties bevestigend, met daarbij de kanttekening dat de internetprovider dat voor hen doet.

Bij de vierde vraag – naar de planning – geven twee organisaties een concrete termijn aan waarbinnen men een en ander wil realiseren. Bij de andere organisaties is een dergelijke planning er (nog) niet of is niet geantwoord op de vraag.

Zoals eerder al opgemerkt kan over de ontwikkeling van het gebruik van RPKI **geen uitspraak** worden gedaan op basis van het verzamelde materiaal.

Relevante ontwikkeling

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

SAML

Over deze standaard is helaas geen informatie beschikbaar. In de achterliggende jaren was dat wel telkens mogelijk.

STARTTLS & DANE

Waarom belangrijk ?

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

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

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

Feitelijk gebruik

Als indicator voor het feitelijk gebruik van deze open standaarden kijken we naar de ondersteuning van STARTTLS en DANE op 1.493 e-mailservers van de overheid. Zie hiervoor de IV-meting van voorjaar 2022 (Bijlage B.). Voor wat betreft STARTTLS is getest of bij de mailservers STARTTLS is geconfigureerd zoals door het NCSC is aanbevolen. De test op DANE bestaat eruit dat wordt nagegaan of de nameservers van de mailservers één of meer TLSA-records voor DANE bevatten.

	voorjaar 2022
STARTTLS cf. NCSC	81 %
DANE	46 %

Bij vier op de vijf e-mailservers (81%) is de STARTTLS-configuratie conform de richtlijnen van NCSC geconfigureerd; bij één op de vijf moet dat nog gebeuren. DANE scoort met minder dan 50% laag in vergelijking met de andere standaarden die in de IV-meting zijn meegenomen. In volgende monitor-rapportages kunnen deze cijfers in perspectief worden geplaatst.

Een uitsplitsing van deze cijfers naar type overheid levert het volgende beeld op.

	Centrale overheid (n=730)	Provincies (n=18)	Water-schappen (n=30)	Gemeenten (n=354)	Gemeen-schappelijke regelingen (n=361)
STARTTLS cf. NCSC	80 %	81 %	79 %	86 %	80 %
DANE	55 %	19 %	24 %	53 %	25 %

De verschillende categorieën overheden ontlopen elkaar weinig waar het gaat om de toepassing van STARTTLS. Bij DANE ligt dat anders. Terwijl de centrale overheid en de gemeenten met een percentage boven de 50% relatief goed scoren, blijven de andere drie categorieën duidelijk achter.

STIX & TAXII

Waarom belangrijk ?

STIX en TAXII zijn standaarden voor partijen die samenwerken op het gebied van cybersecurity. Door standaarden te gebruiken wordt het mogelijk om sneller en gemakkelijker informatie te delen over cyberdreigingen om zodoende de juiste maatregelen te kunnen nemen om computersystemen te beschermen. Daarbij is STIX een gegevensopslagformaat dat gebruikt wordt voor het beschrijven van kwetsbaarheden en incidenten. TAXII is een protocol voor de uitwisseling van deze gegevens. Het gebruik van deze standaarden is een belangrijke stimulans voor de versterking van de weerbaarheid tegen cyberdreigingen. De standaarden STIX en TAXII staan op de 'pas toe of leg uit' lijst sinds november 2017.

Feitelijk gebruik

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

Om zicht te geven op het feitelijke gebruik moeten we kijken naar de organisaties die cybersecurity-informatie verwerken met onderscheid tussen de coördinerende instanties en de daarbij aangesloten organisaties.

Nationaal niveau

Het Nationaal Cyber Security Center (NCSC) heeft als taak om Nederland weerbaar te maken tegen cyberdreigingen. Op dit moment werkt het NCSC vooral voor de Rijkoverheid en vitale sectoren van de industrie maar die doelgroepen worden de komende tijd uitgebreid naar andere sectoren. Het NCSC maakt voor zijn dienstverlening onder meer gebruik van het Nationaal Detectie Netwerk (NDN) dat zich richt op het onderling delen van dreigings- en incidentinformatie. Bij deze informatieuitwisseling wordt onder meer de TAXII

standaard gebruikt en bij de analyse van cybersecurity-gegevens wordt de STIX standaard gebruikt.

Veel Rijksoverheidsorganisaties maken voor hun informatievoorziening en hun informatiebeveiliging gebruik van shared service organisaties (zoals SSC-ICT, DICTU, DUO, JIO, en SSC Campus). Deze shared service organisaties hebben SOC-afdelingen (Security Operations Center) waar de monitoring, detectie en afhandeling van informatiebeveiligingsincidenten is belegd. Het zijn vooral deze SOC's die gebruikers zijn van de cybersecurity tools waar de STIX en TAXII standaarden op van toepassing zijn. Momenteel is de Rijksoverheid druk doende om alle organisaties aan te sluiten op een SOC.

Het NCSC sluit de organisaties aan op het NDN en dat is dan ook een goede maatstaf voor het actieve gebruik van STIX en TAXII binnen de Rijksoverheid. De grotere organisaties als de Politie en de Belastingdienst hebben een eigen SOC maar de meeste organisaties binnen de Rijksoverheid sluiten aan via het SOC van hun shared service organisatie.

Binnen de Rijksoverheid zijn 158 van de 205 organisaties aangesloten bij het NDN waarvan 101 organisaties zijn aangesloten via de sensor van een shared service organisatie. Dat geeft een dekkingsgraad geeft van 77%.

In absolute getallen is het aantal aangesloten partijen in vergelijking met vorig jaar toegenomen van 155 naar 158. Dit is een indicator van de trend dat binnen de Rijksoverheid het gebruik van systemen voor de bescherming tegen cyberdreigingen langzaam maar zeker toeneemt. In de monitor van vorig jaar (2021) is een hogere dekkingsgraad gerapporteerd (82%). De lagere dekkingsgraad dit jaar houdt verband met het feit dat het feitelijk gebruik minder hard is opgelopen dan de omvang van de doelgroep waarop men zich richt (van 190 naar 205).

Gemeentelijk niveau

De Informatiebeveiligingsdienst (IBD) van VNG Realisatie faciliteert de verspreiding van threat intelligence voor verschillende gemeenten als onderdeel van de collectieve aanbesteding GGI-Veilig. Het grootste deel van de gemeenten heeft niet de kennis en capaciteit om eigenstandig het proces van threat intelligence uit te voeren. Een van de onderdelen waar het om gaat is SIEM/SOC-dienstverlening die door KPN geleverd wordt.

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

Het nieuwe Cyber Threath Intelligence platform (CTI platform) dat onderdeel is van de SIEM/SOC-dienst is in het derde kwartaal van 2021 in gebruik genomen. Hierbij is ook de NDN-feed ten behoeve van gemeenten gekoppeld. Voor gemeenten die aangesloten zijn op GGI Veilig zijn deze standaarden STIX/TAXII geborgd. Dit gaat nu inmiddels om 16 organisaties

die samen 45 gemeenten vertegenwoordigen. In situaties waarbij gemeenten een beheerde dienst afnemen bij een leverancier is geen zicht op de exact gebruikte uitwisselingsstandaarden. Het is echter de verwachting dat ook leveranciers deze uitwisselingsstandaarden gebruiken.

Ter vergelijking: in de vorige monitor was sprake van 5 organisaties die samen 10-12 gemeenten vertegenwoordigen. In die periode liepen er gesprekken met tientallen andere gemeenten om ook aan te sluiten. In de tussenliggende periode is dat derhalve geeffectueerd; er is sprake van een toename van het gebruik.

Relevante ontwikkeling

Vanuit NCSC wordt aangegeven dat de cijfers van het NDN slechts een indicatie geven van het feitelijke gebruik van de standaarden. Verder heeft men bij het NCSC op dit moment nog geen zicht op de andere overheidsorganisaties buiten het Rijk. Er leeft wel een idee om het gebruik van de standaarden in de toekomst op een andere manier te monitoren, en dat is via het SOC-stelsel Rijk dat momenteel in oprichting is.

Verder de volgende kanttekening: de meeste cybersecurity softwareproducten geven aan STIX en TAXII te ondersteunen maar dat is slechts ten dele waar. TIP systemen (Threat Intelligence Platform) gebruiken voor hun interne gegevensverwerking doorgaans een eigen opslagformaat. De ondersteuning van STIX bestaat dan uit de mogelijkheid om gegevens via een conversiemodule in STIX formaat te kunnen importeren en exporteren. Bij de aanschaf van software moet derhalve worden opgelet dat de standaard zodanig wordt toegepast dat de gegevens zo veel mogelijk verliesloos kunnen worden uitgewisseld met systemen van andere leveranciers. TAXII ondersteuning is vooral van belang voor SOC's om te kunnen aansluiten op relevante feeds van cyberdreigingen en –incidenten. Tegen de achtergrond van het bovenstaande kan worden gesteld dat de marktondersteuning nog gebreken kent, die kunnen leiden tot problemen rond interoperabiliteit.

Laatste opmerking vanuit NCSC betreft het feit dat in de achterliggende periode nieuwe versies van beide standaarden beschikbaar zijn gekomen. Ten opzichte van de oude versie 1.2.1 is een meer uitgebreide versie 2.0 vastgesteld die in de praktijk echter lastig bruikbaar is gebleken. Inmiddels zijn de kinderziektes verholpen en is een nieuwe versie 2.1 vastgesteld, die volgens NCSC veel beter bruikbaar is. Dat impliceert dat moet worden bezien of deze versie 2.1 op de pas-toe-of-leg-uit lijst kan komen te staan. Deze kwestie speelde ten tijde van het verschijnen van de vorige monitor ook al. In de praktijk wordt nog veel gebruik gemaakt van de oude versies.

Vanuit de hoek van VNG Realisatie wordt hier nog aan toegevoegd dat de IBD het Malware Information Sharing Platform (MISP) in gebruik heeft genomen. Hierop zullen naar verwachting het komende jaar meer gemeentelijke leveranciers aangesloten worden, met een positief effect op de adoptie van STIX/TAXII.

WPA2 Enterprise

Waarom belangrijk ?

WPA2 Enterprise maakt het mogelijk dat gebruikers automatisch en veilig toegang krijgen tot aangesloten WiFi-netwerken. Ook als deze WiFi-netwerken zich buiten de eigen organisatie bevinden. De authenticatie vindt plaats op basis van bestaande identiteitsgegevens van de gebruiker. Hierdoor hoeven gebruikers niet opnieuw in te loggen. Met het gebruik van WPA2 Enterprise is ook de integriteit van de netwerkverbinding geborgd. Bij WPA2 Enterprise spelen drie partijen een rol: de 'gebruiker', de 'Identity Provider (IdP)' en de 'Service Provider (SP)'. Zodra een gebruiker contact maakt met het betreffende WiFi-punt toetst de SP (beheerder van het WiFi-punt) op basis van de inloggegevens bij de IdP (de thuisorganisatie van de gebruiker) de identiteit van de gebruiker. Na positieve verificatie van de identiteit van de gebruiker, wordt toegang verleend tot het WiFi-netwerk zonder dat aanvullende inlog noodzakelijk is. Diensten zoals Govroam (een overheidsbreed wifi-netwerk), Rijk2Air (specifiek ingericht voor Rijksambtenaren) en Eduroam (doelgroep: onderwijs- en onderzoek-instellingen) maken gebruik van WPA2 Enterprise. De standaard staat op de 'pas toe of leg uit' lijst sinds 2 februari 2016.

Feitelijk gebruik

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

	2016 (sept.)	**2017** (sept.)	**2018** (sept.)	**2019** (sept.)	**2020** (juni)	**2021** (aug/sept)	**2022** (juni)
Govroam	49	132	244	307	332	337	351
Eduroam	157 (mei)	199	215	222	231	250	254
samen	206	331	459	529	563	587	605

Uit bovenstaand overzicht blijkt dat het gebruik van WPA2 Enterprise vergeleken met vorig jaar **licht toegenomen** is met ruim 3%.

Het aantal gekoppelde instellingen aan Eduroam is hoog en zit tegen het maximum aan; de groeipotentie voor de komende periode is daarmee beperkt geworden. Het aantal gekoppelde organisaties aan Govroam stijgt gestaag. Hier ligt ook nog voldoende potentie om het aantal deelnemers te laten stijgen. Bij de huidige (ruim 350) gebruikers zijn meer dan 900 locaties aangesloten waar per dag in totaal gemiddeld zo'n 200.000 authenticaties plaatsvinden.

Relevante ontwikkeling

Vanuit de stichting Govroam zijn vier ontwikkelingen gemeld:

- getgovroam is succesvol gelanceerd met reeds enkele tientallen organisaties die er gebruik van maken. Getgovroam maakt het eenvoudig om via een app een govroam-

profiel te genereren op basis van EAP-TLS, na inlog via SAML met de credentials van de thuisorganisatie, en is gebaseerd op geteduroam;
- op verzoek beperkt govguest (dienst voor tijdelijke veilige wifi-toegang voor bezoekers zonder govroam-account) sinds half 2022 de toegang voor gasten tot uitsluitend de wifi-netwerken van de organisatie waar zij te gast zijn, om zo het bezwaar weg te nemen dat gasten bij andere organisaties online kunnen komen;
- stichting govroam is bezig alle nieuwe diensten te ontsluiten met Single Sign On door centrale koppelingen op basis van wederom een Open Source bouwsteen van SURF, namelijk OpenConext;
- een opvallende ontwikkeling is dat stichting govroam steeds vaker het belang van veilige doch transparante internettoegang tracht te benadrukken, nu die geregeld door organisaties zover beperkt wordt dat roamende ambtenaren aldaar hun werk niet meer kunnen doen (omdat bijvoorbeeld VPN naar de thuisorganisatie niet meer werkt, of door 'conflicterende' videoconferencingapplicaties).

B4.2. Domein Document en (web/app)content

Ades Baseline Profiles

Over deze standaard is helaas geen informatie beschikbaar.

Digitoegankelijk

Waarom belangrijk ?

Digitoegankelijk is de Nederlandse naam voor de Europese norm 301 549 die voorziet in toegankelijkheidsrichtlijnen voor overheidswebsites en de documenten die daarop gepubliceerd zijn. EN 301 549 verwijst naar de technische standaard WCAG 2.1 van W3C die specificeert hoe content op websites, in webapplicaties en in documenten toegankelijk kunnen worden gemaakt. Daarnaast beschrijft EN 301 549 instructies voor het inkopen van toegankelijke producten en diensten. Door toepassing van Digitoegankelijk worden websites, webapplicaties en documenten voor iedereen toegankelijk, ook voor ouderen en mensen met functiebeperkingen. Bij dit laatste kan het gaan om een permanente (bijvoorbeeld dyslexie, kleurenblind, slechthorend, slechtziend, motorisch beperkt), een tijdelijke (bijvoorbeeld een gebroken pols) of een situationele functiebeperking (bijvoorbeeld in de zon, in de trein of met een baby op de arm). Zo krijgt iedereen altijd dezelfde toegang tot overheidsinformatie. Vanaf 23 september 2020 is toepassing van deze standaard wettelijk verplicht. De standaard staat op de 'pas toe of leg uit' lijst sinds oktober 2016.

Feitelijk gebruik

Stichting Accessibility, inmiddels onderdeel van Bartiméus, doet sinds 2004 regelmatig overheidsbreed onderzoek naar de toegankelijkheid van websites. In 2019 heeft men een vernieuwde onderzoeksaanpak in gang gezet om zicht te krijgen op de toegankelijkheid van websites en mobiele applicaties van Nederlandse overheidsorganisaties. In november 2019 is

de nulmeting verschenen van dit onderzoek op basis van de vernieuwde aanpak, twee jaar later is een tweede meting verschenen[2].

De meting kent net als de nulmeting een gelaagde onderzoeksopzet, met een oplopende mate van diepgang van het onderzoek. Daaruit komen (onder meer) de volgende inzichten naar voren (tussen haakjes de cijfers uit de nulmeting):

- Globaal beeld: met behulp van testsoftware zijn de homepages van 3.072 Nederlandse overheidswebsites[3] (in 2019: 1.814) automatisch onderzocht op toegankelijkheid. Van het totale aantal van 50 succescriteria kan 10-25% automatisch worden gemeten (in 2019: 5 tot 15%). De (semi-)automatische tool vond bij 28% van de onderzochte websites geen afwijkingen (in 2019: 23%). Die websites zouden dus potentieel goed toegankelijk zijn. Om te bepalen of dat echt zo is, is echter nog handmatig onderzoek nodig van de succescriteria die niet door de tool worden getoetst.
- Een aanvullende automatische toetsing van 435 websites (uit de groep van 3.072). Bij dit vereenvoudigd onderzoek werden door de testsoftware meer pagina's onderzocht. Daarbij daalde het percentage websites zonder fouten naar 6%. Een score uit de nulmeting ontbreekt op dit punt.
- Voor het diepgaand onderzoek zijn in overleg met maatschappelijke organisaties, 32 websites gekozen en handmatig onderzocht (in 2019: 60 websites). Geen van de onderzochte websites bleek volledig foutloos (in 2019 evenmin). Het gemiddeld aantal van de 50 criteria waaraan nog niet wordt voldaan bedraagt 14,2 succescriteria per website (in 2019: 12,4). Dat aantal van 14,2 is deels te verklaren doordat er verhoudingsgewijs veel websites met nalevingsstatus B, C, D en E in de steekproef zitten en maar 1 website met nalevingsstatus A. Als alleen wordt gerekend met de websites uit het register van toegankelijkheidsverklaringen (nalevingsstatus A t/m D), is het gemiddelde aantal fouten 10,85. Een deel van deze fouten (12%) wordt mede veroorzaakt door pdf-documenten. Exclusief deze documenten is het aantal fouten dus iets lager.
- Er zijn 8 mobiele applicaties getoetst op alle 50 succescriteria. Slechts 1 van de 8 onderzochte mobiele applicaties voldeed volledig aan de standaard. De overige applicaties hebben tussen de 3 en 19 succescriteria fout. Een vergelijking met de meting uit 2019 is lastig te maken. Toen zijn 23 mobiele applicaties getoetst maar op niet meer dan 11 succescriteria. De uitkomst toen was dat geen van de mobiele applicaties aan alle 11 getoetste succescriteria voldeed.

De belangrijkste conclusie uit de meting 2021 is dat het overgrote deel van de websites en de mobiele applicaties van de onderzochte Nederlandse overheidsinstanties op dit moment niet volledig voldoen aan alle toegankelijkheidseisen. Dit betekent overigens niet automatisch dat een overheidsinstantie niet voldoet aan de vereisten van het Tijdelijk besluit

[2] Monitor toegankelijkheid 2021. Websites en mobiele applicaties van Nederlandse overheidsinstellingen, November 2021, Stichting Accessibility. Opdrachtgever hierbij is Logius.

[3] Deze totaallijst van websites de adressen bestaat uit het register van toegankelijkheidsverklaringen aangevuld met websites uit het onderzoek uit 2019.

digitale toegankelijkheid overheidswebsites. Ook als website(s) en apps niet voldoen aan de norm kan een overheidsinstantie voldoen aan het besluit, zolang die organisatie maar aantoonbaar werkt aan verbetering van de toegankelijkheid door het toepassen van de standaard.

Daar waar het mogelijk is om een vergelijking te maken met de meting uit 2019, lijkt wel sprake te zijn van enige verbetering, het gebruik lijkt **licht toegenomen**. Dit is overigens niet meer dan een indicatie. De aantallen websites en apps die zijn onderzocht, zijn te klein om op basis daarvan statistisch significante uitspraken te kunnen doen.

Relevante ontwikkeling

Om de ontwikkelingen met betrekking tot digitoegankelijkheid te blijven volgen, zal deze monitor naar verloop van tijd weer worden herhaald.

ODF en PDF

Waarom belangrijk ?

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

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

Feitelijk gebruik

De meting is gedaan op basis van een steekproef bij overheidsorganisaties die vallen binnen het organisatorisch werkingsgebied van de pas-toe-of-leg-uit lijst. De steekproef bestaat uit een totaal van 97 organisaties uit verschillende delen van de overheid:

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

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

De meting is dit jaar door dezelfde organisatie en op dezelfde manier uitgevoerd als in 2021. Voor het tellen van documenten op websites gebruiken wij net als in 2021 Google search (https://www.google.com). Door de aard van commerciële zoekmachines moet wel rekening worden gehouden met een zekere meetfout. Zoekmachines vinden niet noodzakelijk alle documenten op een website. Anderzijds kunnen de zoekresultaten door het caching beleid van de zoekmachine referenties bevatten naar documenten die al niet meer geldig zijn. Dit is een nadeel van de huidige meetmethode maar vooralsnog is er nog geen werkbaar alternatief voor[4].

Uit de meting die hieronder wordt gepresenteerd kunnen slechts trends worden opgemaakt, gebaseerd op een steekproef (tussen haakjes de gegevens uit respectievelijk 2021 en 2020).

	Top 30 overheid	**G30 gemeenten**	**Provincies**	**Water-schappen**
Aantal gevonden PDF	396.552 (312540, 325008)	220.320 (183370, 168005)	135.457 (150451, 116886)	19.126 (19711, 22951)
Aantal gevonden ODF	876 (952, 17)	5 (15, 4)	127 (181, 8)	0 (3, 1)
Aantal gevonden MS Office	16.060 (14523, 39)	10.241 (17928, 30)	9.150 (10886, 25)	278 (348, 6)
Percentage PDF van alle gevonden documenten	95,90% (95.28%, 99,99%)	95,56% (91.09%, 99,98%)	93,59% (93,15% 99,97%)	98,57% (98.25%, 99,97%)
Percentage ODF van de gevonden bewerkbare documenten	5% (6%, 30%)	<1% (<1%, 12%)	1% (2%, 24%)	0% (1%, 14%)
Percentage ISO PDF	33% (35%, 47%)	55% (45%, 43%)	31% (33%, 33%)	52% (67%, 29%)
Percentage digitaal toegankelijke PDF	0% (23%, 23%)	7% (7%, 17%)	0% (17%, 25%)	0% (0%, 0%)

De belangrijkste observaties naar aanleiding van dit overzicht:

- Meer documenten dan in 2021 op websites van overheden. Op websites van de rijksoverheid groeit het aantal documenten het hardst. Bij de 30 grootste gemeenten

[4] De inzet van een eigen '*crawler*' bleek in voorgaande jaren nog grotere problemen met zich mee te brengen. Een *crawler* moet zorgvuldig afgesteld worden, kost veel rekentijd en kan een website zwaar belasten. Afhankelijk van de afstelling ziet een *crawler* vaak belangrijke aantallen documenten op een website over het hoofd. Dit bleek geen passende oplossing in voorgaande jaren.

groeide het aantal documenten eveneens. Bij provincies en waterschappen nam het aantal documenten juist iets af.

- PDF blijft veruit het meest gebruikte format voor de publicatie van documenten. Over alle gemeten websites heeft 95% van de documenten een PDF format. Dat is vergelijkbaar met de 94% van vorig jaar. Bij de 30 grootste gemeenten nam het percentage PDF bestanden het duidelijkst toe, van 91,09% naar 95,56%. Bij provincies, waterschappen en op de 30 grootste websites van de overheid groeide het aandeel PDF bestanden marginaal.
- Op de 97 onderzochte websites vonden wij in totaal 771.455 PDF bestanden. Dat is een gemiddelde van 7.953 PDF bestanden per website. Dit is 17% meer dan in 2021. Net als vorige jaren vinden we onder de websites grote verschillen in aantallen PDFs die erop gepubliceerd staan. Sommige websites, zoals die van de gemeenten Tilburg en Haarlemmermeer, hebben hooguit enkele tientallen PDF documenten. Andere websites zoals die van de Politie of Autoriteit Financiële Markten hebben er tienduizenden.
- Van de steekproef van 97 PDF bestanden (1 per onderzochte organisatie) voldeed 46% aan de ISO standaard PDF 1.7 of PDF/A op de 'pas toe of leg uit'-lijst. Dat is gelijk aan het percentage uit 2021. De gemeenten en waterschappen doen het gemiddeld beter dan de rijksoverheid en provincies. We vonden een viertal documenten (5% van de totale steekproef) die als PDF gepubliceerd waren, maar geen geldige PDF bestanden bleken.
- Van de steekproef van 97 PDF bestanden van na 2019 is slechts 2% digitaal toegankelijk. Dat is aanzienlijk minder dan de 12% die we maten in 2021. Dit jaar vonden wij slechts in de steekproef van de gemeenten een tweetal digitaal toegankelijke PDF bestanden. In de steekproef van de rijksoverheid, provincies en waterschappen vonden wij geen enkel digitaal toegankelijk PDF bestand. Wel moeten wij hierbij aantekenen dat de steekproef de uitkomst bepaalt. De steekproef heeft ieder jaar dezelfde omvang van 97 bestanden maar bestaat ieder jaar uit andere willekeurig gekozen documenten. Het kan dus zijn dat je per toeval minder digitaal toegankelijke documenten treft.
- Ongeveer 9% websites van de organisatie publiceert geen of vrijwel geen informatie meer in PDF. Dit aantal is ongeveer gelijk als in 2021. Het vermijden van PDF bestanden heeft vaak een positief effect voor de digitale toegankelijkheid van de website. De Rijksoverheid is hierin een voorloper: 27% van de 30 grootste websites van de Rijksoverheid hebben (vrijwel) geen PDFs meer. Een aantal organisaties hanteert een HTML-first beleid, wat de digitale toegankelijkheid ten goede komt. Voorbeelden hiervan zijn het CBS, het Kadaster, Geonovum, de gemeente Haarlemmermeer en de websites werkenvoornederland.nl, werkenbijdefensie.nl, crisis.nl (NCTV) en consuwijzer.nl (ACM).
- In sommige gevallen houdt een organisatie zich wel aan de voorgeschreven sjablonen voor publicatie, maar zijn de sjablonen niet digitaal toegankelijk. Dat geldt bijvoorbeeld voor Rijkswaterstaat, dat zich voor publicaties in PDF netjes aan de Rijkshuisstijl houdt. Het gebruik van Rijkshuisstijl sjablonen in Word leidt na PDF export echter niet tot digitaal toegankelijke PDF bestanden. Een ander voorbeeld is de website rijksbegroting.nl waar voornamelijk Kamerstukken op te vinden zijn die in het officiële format van de Eerste en Tweede Kamer zijn opgemaakt. Deze PDF bestanden zijn ook niet digitaal toegankelijk.
- ODF vormt slechts 2,74% van de bewerkbare documenten op alle onderzochte websites. Dat is iets meer dan in 2021.

Op basis van de meetresultaten en observaties kan een aantal trends worden onderscheiden in het gebruik van open documentstandaarden:

- Het aantal documenten op websites van de overheid blijft groeien. De verwachting is dat de Wet open overheid deze trend verder zal versterken.
- Ongeveer de helft (46%) van de PDF bestanden uit de steekproef op overheidswebsites voldoet aan de standaarden PDF 1.7 en PDF/A op de 'pas toe of leg uit' lijst. Dat is gelijk aan het percentage van vorig jaar. Er is dus **geen stijgende of dalende trend** waarneembaar.
- Digitale toegankelijkheid van PDF bestanden op overheidswebsites blijft een knelpunt. Slechts 2% van de recente (jonger dan 2019) PDF bestanden uit de steekproef bleek digitaal toegankelijk. Ten opzichte van eerdere jaren is hier **geen verbetering** te zien. Wel zien wij dat steeds meer organisaties kiezen voor HTML-first publicatiebeleid, waarbij geen er nieuwe PDF bestanden meer op de website komen. Dit komt de digitale toegankelijkheid van de websites meestal ten goede.
- Ook dit jaar moeten we concluderen dat ODF **veel te weinig wordt toegepast** waar dat verplicht is. Dit is een voortzetting van de trend van eerdere jaren.

Relevante ontwikkeling

ODF wordt beheerd door OASIS. Deze internationale organisatie heeft geen specifieke ambities om het gebruik van ODF bij de Nederlandse overheid te stimuleren. In Nederland wordt het gebruik van ODF gestimuleerd door de OpenDoc Society (http://www.opendocsociety.org/) en NLnet (https://nlnet.nl/project/odfautotests/). Zo hebben deze organisaties het ODF Plugfest enkele malen (in 2011 en 2015) in Nederland georganiseerd en stellen ze open source toolondersteuning beschikbaar voor ODF. De laatste jaren zijn deze organisaties echter niet actief geweest met het stimuleren van het gebruik van ODF.

PDF/A en PDF 1.7 worden beheerd door ISO. Deze internationale organisatie heeft geen specifieke ambities om het gebruik van PDF bij de Nederlandse overheid te stimuleren. Dit geldt ook voor de NEN die de ISO specificaties beschikbaar stelt. De PDF Association stimuleert het gebruik van PDF/A en PDF 1.7 en heeft een Benelux Chapter met een contact in Nederland (https://www.pdfa.org/local-contacts/?highlight=benelux%20chapter). De PDF Association en in het bijzonder de Benelux Chapter worden gedragen door leveranciers van producten gerelateerd aan PDF. De stimulering en ondersteuning van PDF/A en PDF 1.7 vanuit de PDF Association is daarom nauw verweven met het commerciële aanbod.

Het Nationaal Archief stimuleert het gebruik van PDF/A voor duurzame toegankelijke toepassingen. Bij het Nationaal Archief kunnen overheidsorganisaties terecht voor advies en ondersteuning bij het gebruik van PDF/A.

OWMS

Voor deze standaard loopt een toetsingsprocedure om OWMS niet meer te verplichten of aan te bevelen aan de overheid. Een kleine 2 jaar geleden heeft het Forum Standaardisatie

groen licht gegeven voor het starten van een verwijderingsprocedure van de 'pas toe of leg uit' lijst. Om die reden is er dit jaar geen navraag meer gedaan naar gebruiksgegevens.

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

SKOS

Waarom belangrijk ?

Het publiceren van gegevensbestanden in de vorm van begrippenlijsten, digitale woordenboeken en taxonomieën door overheidsorganisaties gebeurt vaak in de vorm van documenten die niet bruikbaar zijn voor computerprogramma's. SKOS zorgt ervoor dat deze kennisrepresentaties via het internet aan elkaar kunnen worden gekoppeld en maakt het mogelijk dat gegevensbestanden makkelijker als open data kunnen worden hergebruikt. Dit vindt plaats via linked data principes. Het toepassen van de standaard draagt bij aan het eenduidig vastleggen van betekenis van begrippen en maakt de (familie)relaties tussen de verschillende definities van begrippen beter inzichtelijk. Met SKOS zijn data uit verschillende systemen zodoende beter te vergelijken en te interpreteren. Daarnaast zijn er ook standaarden op 'pas toe of leg uit'-lijst die op hun beurt weer gebruik maken van SKOS en aanpalende linked data standaarden, zoals GWSW voor stedelijk waterbeheer of Aquo-standaard voor watermanagement. De standaard staat op de 'pas toe of leg uit'-lijst sinds 18 mei 2015.

Feitelijk gebruik

Er is (nog) geen objectieve meetmethode voorhanden om het gebruik van SKOS inzichtelijk te maken. In principe kan het gebruik van SKOS vrijwel automatisch worden gemeten op aggregatoren van begrippenlijsten, zoals het internationale Linked Open Vocabularies (LOV) of het leveranciersgebonden thesaurusplatform BegrippenXL. Er is weinig zicht in hoeverre overheidsorganisaties dergelijke aggregatoren inzetten voor publiceren van begrippenlijsten (op LOV lijkt vooralsnog alleen de linked open data van het Kadaster en van het Centraal Bureau voor de Statistiek te zijn aangemeld). In de markt zijn leveranciers actief die platforms bieden voor het verzamelen van linked data sets. TriplyDB heeft op het moment van deze meting één dataset van een overheidsorganisatie. Het al eerder genoemde thesaurusplatform BegrippenXL biedt een overzicht van 43 begrippenlijsten van bijna alleen overheden. Het thesaurusplatform is volledig gebaseerd op de SKOS (en direct daaraan gerelateerde, andere linked data standaarden). Verschillende overheidsdomeinen hebben eigen initiatieven zoals het Termennetwerk van het Netwerk Digitaal Erfgoed dat een hulpmiddel is om bestaande definities voor het beschrijven van erfgoedobjecten uit diverse (inter)nationale begrippenlijsten eenvoudig te kunnen vinden. Op het Dataregister van de Nederlandse Overheid is op moment van deze meting één dataset aangemeld die gebruik maakt van SKOS.

Net als in voorgaande jaren lijkt een enquête de beste manier om gebruiksgegevens van SKOS boven water te krijgen. De enquête is in juni 2022 uitgezet bij 50 overheden en semi-overheden. Deze groep bestaat voornamelijk uit gebruikers van de LOD Nederland groep op LinkedIn en is vrijwel gelijk aan de steekproef die is gebruikt bij de meting van 2019, 2020 en 2021. Daarnaast is er op twee platforms en op een LinkedIn-groep een oproep geplaatst voor deze enquête en heeft Bureau Forum Standaardisatie dezelfde oproep via website en via Twitter en LinkedIn gepubliceerd. De inhoud van de enquête is dezelfde als in 2021, zodat de antwoorden te vergelijken zijn. Ook in 2022 is gebruik gemaakt van EUSurvey, de open enquête applicatie van de Europese Commissie.

In totaal is de enquête 73 keer ingevuld waaruit 51 unieke organisaties zijn af te leiden. Van de 51 unieke organisaties geeft 57% (29 organisaties) aan een begrippenlijst, woordenboek of taxonomie op het internet te publiceren. Dit is een stijging ten opzichte van 2021 (aandeel begrippenlijsten: 50%). Dit zijn in principe organisaties die in aanmerking komen voor de verplichting van SKOS. Als wordt ingezoomd op deze 29 organisaties die kwalificeren voor een verplichting van SKOS, dan zien we het volgende:

- 21 daarvan gebruiken SKOS (72% van 29). Dat is min of meer stabiel in vergelijking tot meerjarig gebruik (2019: 74%; 2020: 56%; 2021: 77%). Het lagere percentage van 2020 (56%) kan worden beschouwd als een eenmalige uitschieter naar beneden (vanwege lage respons was de steekproef dat jaar te weinig representatief).
- Over deze 21 gebruikers van SKOS nog het volgende:
  - 7 organisaties maken alleen gebruik van SKOS
  - 13 organisaties geven aan zowel SKOS als Web Ontology Language (OWL) te gebruiken. OWL is een andere open standaard op de lijst aanbevolen standaarden van het Forum Standaardisatie, met een soortgelijk functioneel toepassingsgebied als SKOS. SKOS en OWL zijn ook goed in combinatie te gebruiken.
- 3 van de 21 organisaties gebruiken SKOS niet maar deze organisaties gebruiken wel OWL.
- 12 van de 21 organisaties (57%) gebruiken naast SKOS ook de open standaard Shapes Constraint Language (SHACL). Dit is een aanbevelenswaardige combinatie omdat SHACL de kwaliteit van datasets borgt. SHACL staat (net als OWL) op de lijst aanbevolen standaarden van het Forum Standaardisatie.

De basis om een uitspraak te doen over de ontwikkeling van het gebruik van SKOS is smal. Met inachtneming van die constatering is het mogelijk te zeggen dat er sprake is van een **stabilisering van het gebruik** van SKOS t.o.v. voorgaande jaren. Een belangrijke bijbehorende conclusie is ook: daar waar deze open standaarden (SKOS maar als alternatief ook OWL) gebruikt moeten worden, gebeurt dat ook. De groeipotentie voor het gebruik van SKOS zit hem er vooral in dat meer overheidsorganisaties hun data (meer) als linked data gaan publiceren.

Enkele aanvullende observaties:

- Waar de overheid linked data toepast en publiceert, gebeurt dit vrijwel altijd met open standaarden. De resultaten bevestigen het beeld dat SKOS meestal gebruikt wordt waar het ‘pas toe of leg uit’-beleid dat verplicht. De resultaten zijn in lijn met de resultaten van eerdere jaren en laten een stabilisering zien.

- We zien dit jaar in de respons dat vooral uitvoeringsorganisaties SKOS en linked data toepassen. Uit de respons van decentrale overheden zoals gemeentes, provincies en provinciale instellingen komt een beeld naar voren dat zij geen begrippenlijst, woordenboek of taxonomie op internet publiceren.
- De enquête is in 2022 uitgezet via oproepen op twee platforms, via de website van Forum Standaardisatie en social media, extra ten opzichte van de steekproef van voorgaande jaren (2019, 2020 en 2021). Dit heeft geleid tot een hogere respons. Deze hogere respons heeft de uitkomsten van het percentuele gebruik van SKOS uit de steekproef van voorgaande jaren bevestigd.
- Het feit dat een organisatie SKOS gebruikt, zegt minder over de kwaliteit van de datasets. De kwaliteit van de kennisrepresentatie met SKOS is minstens even belangrijk als de inzet van de standaard op zich, maar is veel moeilijker objectief te beoordelen zonder gedetailleerde kennis van het domein.
- Bijna twee derde van organisaties die SKOS gebruiken, gebruikt ook de OWL-standaard. De toepassingsgebieden van SKOS en OWL overlappen deels, waarbij OWL de 'zwaardere' standaard is die bij formelere kennissystemen wordt ingezet. Dit suggereert dat ook SKOS meestal wordt toegepast in grotere, serieuze linked data projecten. Vanwege de overlap zou het interessant zijn om te onderzoeken hoe deze organisaties SKOS en OWL combineren. De deze keer uitgezette enquête lijkt de 'alles of niets' trend van vorige jaren te bevestigen: óf een organisatie doet helemaal niet aan linked data, óf een organisatie pakt het meteen serieus aan met gebruik van bijbehorende open standaarden.

Relevante ontwikkeling

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

Het publiceren van linked data, en van (SKOS) kennissystemen in het bijzonder, vereist specialistische kennis over semantiek en standaarden. Desondanks wordt er in verschillende overheidsdomeinen volop gewerkt aan linked data, zowel sectoroverstijgend als depatementoverstijgend. De trend lijkt te zijn dat overheden meer linked data in productie in gebruik heeft of voornemens is linked data te gaan gebruiken. Kadaster, de erfgoedsector en de onderwijssector zetten al een aantal jaar achtereen grote stappen. In 2022 heeft Ministerie van Financiën de miljoenennota en de achterliggende processen via linked data ontsloten. Deze inzet van Ministerie van Financiën is een stap voorwaarts in adoptie van linked data; de stap wordt gezien als een voorbeeldfunctie, en kan op navolging rekenen.

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

Forum Standaardisatie en het Platform Linked Data Nederland overleggen over de meerwaarde om linked data standaarden te combinen in één groep op de lijst open standaarden. Dit naar analogie van de stelselstandaarden Geo-standaarden, Digikoppeling en StUF die op de 'pas toe of leg uit'-lijst staan en die ook uit verschillende deelstandaarden bestaan. De linked data community geeft het signaal af dat 'pas toe of leg uit'-verplichting van SKOS bijdraagt aan de adoptie van SKOS (en van aanpalende linked data standaarden). Dit signaal gaat mee in de vraag of de gecombineerde linked data standaarden dan als groep op de 'pas toe of leg uit'-lijst of de lijst aanbevolen standaarden moet komen. Een vervolg hierop is in 2023 te verwachten.

B4.3. Domein REST API's

OpenAPI Specification

Geen informatie beschikbaar. Zie de toelichting bij NL GOV Assurance.

REST_API Design Rules

Geen informatie beschikbaar. Zie de toelichting bij NL GOV Assurance.

B4.4. Domein E-facturatie en administratie

NLCIUS

Waarom belangrijk ?

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

Feitelijk gebruik

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

maatschappelijke belang. De belangrijkste gebruikersgroepen zijn aangesloten bij het STPE: softwareleveranciers van financiële pakketten, PEPPOL service providers, leveranciers van telecommunicatie en IT, en overheden het Rijk, provincies en gemeenten). Deze gebruikersgroepen leveren ook hun bijdrage aan het Nationaal Multi-belanghebbenden Forum e_Procurement (NMBF).

Het STPE maakt gebruik van data van de Nederlands Peppolautoriteit (NPa), Logius en leverancier Ionite B.V. (e-facturatie specialist) voor een observatie van de ontwikkeling van het gebruik van NLCIUS. Deze observaties betreffen de NLCIUS-adoptie op het PEPPOL-netwerk. Dat laat buiten beschouwing de graad van adoptie via andere kanalen, zoals bilaterale koppelingen of email. We nemen echter aan dat het grootste deel van NLCIUS-facturen over het PEPPOL netwerk verzonden worden, en dus dat NLCIUS-adoptie op dat netwerk indicatief is voor de totale NLCIUS-adoptie.

Uit de gegevens van NPa is het volgende op te maken:
- het aantal verstuurde e-facturen in het NLCIUS-formaat via het Peppol-netwerk is met 38% gestegen t.o.v. 2020;
- het aantal ontvangen e-facturen in het NLCIUS-formaat via het Peppol-netwerk is met 6% gestegen t.o.v. 2020. De reden dat de aantallen verstuurde en ontvangen facturen uit elkaar lopen is dat er serviceproviders tussen zitten die vaak facturen omzetten in andere formaten t.b.v. de ontvanger.

Uit de gegevens van Ionite blijkt het volgende:
- het aantal endpoints in Nederland is naar 17.945 in de Peppol Directory gestegen. Dit is een stijging van 34% t.o.v. 2020;
- het aantal endpoints dat documenttype SI-UBL 2.0 invoice ondersteunt, groeide naar 17.206. Een stijging van 37% t.o.v. 2020;
- het aantal endpoints dat documenttype SI-UBL 2.0 creditnote ondersteunt, groeide naar 13.390. Een stijging van 118% t.o.v. 2020.

Tot slot blijkt uit gegevens van Logius het volgende:
- in 2021 is ongeveer 65% van de verwerkte facturenstroom (ongeveer 2 miljoen per jaar) in het NLCIUS-formaat;
- T.o.v. 2020 is een lichte stijging van 14% in het aantal ontvangen facturen te zien via het Rijksoverheid Peppol Accesspoint.

Mede op basis van bovenstaande gegevens schat het STPE in dat het gebruik van NLCIUS is **toegenomen**. Deze data laten immers niet alleen een groei zien in het aantal NLCIUS endpoints maar ook in het totaal volume van e-facturen, wat het beste verklaard wordt door stijgend gebruik van NLCIUS. Dit beeld wordt bevestigd door de gesprekken die vanuit STPE zijn gevoerd met een aantal stuurgroepleden. Uit die gesprekken is naar voren gekomen dat de adoptie nog steeds langzaam verloopt maar dat er wel sprake is van een (lichte) stijging.

Relevante ontwikkeling

STPE en de NPa zijn onlangs, in april 2021,begonnen met het intensiveren van de samenwerking, met als doelen: efficiënter werken, meer duidelijkheid naar de achterban, en

het vormen van gezamenlijk toekomstbeeld. Als onderdeel hiervan zijn TNO en NPa in mei 2021 bijeengekomen om inhoudelijke kwesties die de werkgroepen aangaan gezamenlijk op te pakken. Het eerste gezamenlijke doel dat is geïdentificeerd, is om gebruikers van de oude SI-UBL 1.2 standaard over te laten stappen op NLCIUS of PEPPOL BIS v3. Dit alles speelt tegen een achtergrond waarbij allerlei gesprekken gaande zijn over de factuurstandaarden en hun toekomst. Ook over NLCIUS.

Daarnaast blijft het STPE actief rondom de ontwikkelingen van het Europese amendement en het elektronische 'bonnetje' (e-Receipt). Er zijn belangrijke stappen gezet om de Nederlandse wensen opgenomen te krijgen in dit amendement. Het STPE heeft een waardevolle bijdrage gelevers aan de verdere ontwikkeling van een Europese e-Receipt standaard.

SETU

Waarom belangrijk ?

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

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

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

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

Feitelijk gebruik

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

De SETU beschikt niet over gebruikscijfers, aangezien het berichtenverkeer niet via een centraal platform geregeld wordt. De enige concrete informatie over gebruikscijfers die de SETU heeft is een gebruikerspeiling uit 2020, waarin ook is nagegaan in welke volumes haar achterban berichtuitwisseling doet op basis van de SETU-standaarden. Op jaarbasis kwam dat toen per SETU-bericht per organisatie uit op het volgende (dit beeld is ook al opgenomen in de vorige monitor):

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

Deze cijfers betreffen overigens ook organisaties die buiten de publieke sector vallen. Uit de cijfers blijkt dat er grote verschillen bestaan tussen de implementatie van de diverse berichten in de standaard. Zo worden de factuur (Invoice) en urenbrief (Timecard) op veel grotere schaal geadopteerd dan de overige berichten, die aan het begin van het proces toegepast dienen te worden.

Van de kant van de beheerorganisatie wordt de inschatting gemaakt dat het gebruik van de standaard **licht toegenomen** is. Dit wordt gebaseerd op de groei van de uitzendbranche in 2021 en specifiek ook het totaal aantal uren, respectievelijk 18% en 20% ten opzichte van 2020 (Bron: Jaarcijfers uitzendbranche 2021). Veel van de SETU-standaarden zijn direct of indirect gekoppeld aan het aantal uren, bijvoorbeeld de Timecard, waarop de uren worden geregistreerd. Vandaar dat de inschatting is gemaakt dat een groei in de branche tot een groei in gebruik van de standaard heeft geleid.

Relevante ontwikkeling

Na een positieve consultatie zijn onderstaande versies voor de SETU-standaarden doorgevoerd:

- SETU Standard for Ordering and Selection v1.4
- SETU Standard for Assignment v1.4
- SETU Standard for Reporting Time and Expenses v1.4
- SETU Standard for Invoicing v2.2
- SETU Standard for Vacancies v1.1 (nieuw)

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

Daarnaast is de SETU in 2021 gestart met het formuleren van haar nieuwe strategie. Hieraan zal in 2022 vervolg worden gegeven. De SETU wil haar koers aanpassen aan ontwikkelingen sinds de oprichting van SETU in 2007, zoals de veranderende rol van uitzendorganisaties, de complexiteit van de back-offices, (toekomstige) wijzigingen in wet- en regelgeving en digitaliseringstrends.

Verbreding van haar scope is één van de thema's in de nieuwe SETU strategie. Uit de werkgroep Trends & Ontwikkelingen, die in 2021 is gestart om relevante ontwikkelingen op het gebied van digitalisering en data-uitwisseling in de sector vroegtijdig te signaleren, is bijvoorbeeld de behoefte aan standaardisatie van planningsgegevens naar voren gekomen.

In 2022 wordt de uitwerking van gestandaardiseerde koppelvlakken op het gebied van planning opgepakt.

Community management is en blijft een belangrijk onderwerp voor de SETU. In 2021 is gestart met het organiseren van webinars, niet alleen voor huidige leden van de SETU, maar voor alle geïnteresseerden. Hiermee is de SETU in contact gekomen met een bredere achterban en dit heeft geleid tot nieuwe leden.

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

WDO Datamodel

Waarom belangrijk ?

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

Het doel van het gebruik van de standaard is een vlot en efficiënt verloop van de aankomst, het vertrek, de doorvoer en de vrijgave van goederen, vervoersmiddelen en personen in de internationale handel. In veel landen wordt de douaneaangifte nog steeds (gedeeltelijk) op papier ingediend. Daarnaast moeten veel gerelateerde documenten, bijvoorbeeld certificaten van oorsprong of landbouwcertificaten, op papier bij andere overheidspartijen worden ingediend. In veel andere landen wordt al elektronisch gecommuniceerd, maar worden lokale standaarden gebruikt. Het betreft hier vaak nog verschillende standaarden omdat overheidsorganisaties vaak een eigen standaard voorschrijven, ook binnen de Europese Unie. Door het gebruik van het WDO Datamodel kunnen de diverse overheids-organisaties dezelfde taal spreken en eenvoudig informatie uitwisselen. Voor de administratie van import en export bevat het WDO Datamodel zogenaamde 'informatiepakketten' voor gegevensuitwisseling. Een informatiepakket beschrijft de semantiek van de uitgewisselde informatie: gegevens- en procesmodellen en hiervan afgeleide berichtspecificaties (MIG: Message Implementation Guidelines).

De standaard staat op de 'pas toe of leg uit' lijst sinds 15 april 2014.

Feitelijk gebruik

Met als focus de overheidssector is het WDO Datamodel is niet alleen van nut voor de Douane maar ook voor andere overheidsinstellingen die betrokken zijn bij grensoverschrijdend verkeer zoals Rijkswaterstaat, de Havenautoriteiten, de Koninklijke Marechaussee en de Nederlandse Voedsel en Warenautoriteit. Voor de Douane betreft het gebruik van de standaard de goederenstromen, maar daarnaast biedt het WDO Datamodel

zoals eerder al opgemerkt ook informatie over personen (voor bijvoorbeeld de Marechaussee) en informatie over vervoermiddelen (voor bijvoorbeeld Rijkswaterstaat).

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

- Single Window: dit betreft 22 binnenkomende en 15 uitgaande berichttypes, alle gebaseerd op het WDO Datamodel. Gebruikers: Douane, Rijkswaterstaat en overige grensbewaking;
- Douane aangifte (DMS): dit betreft 2 binnenkomende en 1 uitgaand berichttypen, deels gebaseerd op EU CDM (en dus ook op WDO Datamodel omdat het een subset van het WDO Datamodel is), met de Douane als gebruiker;
- Douane eCommerce (DECO): dit betreft 2 binnenkomende en 1 uitgaand berichttypen, ook deels gebaseerd op EU CDM, met de Douane als gebruiker;
- Control bericht (gebruikt voor ontvangstbevestigingen en het melden van (syntax)fouten) en Meta Data (gebruikt als enveloppe voor alle aangiftestromen), beide gebaseerd op het WDO Datamodel;
- De MIG voor ICS2-PNI 1.0 is opgeleverd en in gebruik genomen; dit betreft 1 binnenkomend en 1 uitgaand berichttype, gebaseerd op het WDO Datamodel 3.8.1.

Net als in voorgaande jaren ontbreken harde gegevens over het feitelijk gebruik. Een goede vergelijking met het gebruik vorig jaar gebaseerd op cijfers is daarom niet te maken. Dat neemt niet weg dat de Douane melding maakt van een **toename van het gebruik**. Er is namelijk sprake van een forse stijging van e-commerce. Consumenten bestellen steeds meer online; door corona zelfs nog meer. Ook bestellen ze steeds vaker direct bij buitenlandse webshops in plaats van bij Nederlandse winkels. Het gevolg: containers liggen nu vol met tienduizenden pakketjes voor evenzoveel particulieren. Eerder zaten er in een container vaak maar 1 of een paar grote orders. Het aantal aangiftes dat de Douane moet verwerken, is daardoor explosief gestegen: van 30 miljoen in 2018 naar honderden miljoenen in 2021. Deze groei betekent flink wat extra werk voor de Douane (bron: Jaaroverzicht douane 2021).

Relevante ontwikkeling

De volgende bericht-/aangiftestromen staan op de rol om in gebruik genomen te worden:

- Voor het Single Window wordt in het derde kwartaal van 2022 MIG release)1K01 uitgebracht met 6 nieuwe berichten, gebaseerd op EU systemen AES en ICS2 (alleen voor Douane);
- Douane Vervoersaangifte (DVA): dit betreft Transit en zal op termijn de Nederlandse toepassing van NCTS gaan vervangen. Het betreft 2 binnenkomende en 1 uitgaand berichttypen, ook deels gebaseerd op EU CDM (alleen voor Douane).

Aanvullend hierop nog twee andere ontwikkelingen die relevant zijn:

- WDO niveau. Er wordt door het WDO DMPT (Data Model Projects Team) momenteel gewerkt aan een nieuwe majorversie van het WDO datamodel, naar verwachting zal deze versie (4.0.0) in het eerste of tweede kwartaal van 2023 worden gepubliceerd. Voor gebruik in Nederland van deze nieuwe majorversie is nog geen planning bekend. Er is

overigens ook geen verplichting door de WDO opgelegd om op enig moment over te gaan op de nieuwe versie.
- Nationaal niveau. In Nederland is de douane bezig met de ontwikkeling van het zogenaamde NL CDM. Dit datamodel zal worden gebaseerd op WDO datamodel versie 3.11.0 (de laatste subversie van versie 3) en de basis worden voor alle nu op WDO datamodel en/of EU CDM gebaseerde MIG's. Het is de bedoeling dat de invoering van dit NL CDM geruisloos en dus ook zonder consequenties voor de diverse MIG's gaat plaatsvinden.

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

XBRL

Waarom belangrijk ?

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

Feitelijk gebruik

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

	Realisatie 2019	**Realisatie 2020**	**Realisatie 2021**	**Realisatie 2022 t/m april**
Belastingdienst				
Aangifte IB + VPB	16.558.025	15.568.706	15.846.758	6.209.729
Loonheffingen (incl. UZGB)	8.650.532	8.869.092	8.978.265	3.176.642
Erfbelasting + Schenkbelasting	4.073	16.115	31.496	15.824
Aangifte OB + Intercomm. prestaties	5.429.106	5.890.273	6.379.104	3.029.126
Toeslagen	1.325.719	1.279.414	1.355.471	541.922

KvK – Reporting Services (SBR)				
Jaarrekeningen	1.020.450	886.373	889.466	222.255
DUO – Reporting Services (SBR)				
Jaarrekeningen	1.953	1.942	1.963	56
SBR Wonen - Reporting Services (SBR)				
DPI (prognose informatie)	1.112	1.194	898	151
DVI (verantwoordingsinformatie)	1.363	1.370	1.745	9
SBR Wonen Jaarrekening	1.364	1.242	1.226	6

Een vergelijking van de cijfers over de (volledige) jaren 2019, 2020 en 2021 lijkt erop te duiden dat de adoptie van SBR en daarmee XBRL binnen Nederland per saldo **stabiliseert**; waar op het ene onderdeel sprake is van een lichte stijging is elders sprake van een lichte daling.

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

Relevante ontwikkeling

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

Ook internationaal wordt de standaard breed gebruikt door financiële toezichthouders zoals de Europese Centrale Bank maar ook nationale partijen zoals de SEC (USA) en de ESMA (EU).

Een recente trend is de toename van duurzaamheidsrapportages. In juni 2022 sloten Europarlementariërs en EU-regeringen een voorlopig akkoord over nieuwe rapportageregels voor grote bedrijven. De Corporate Sustainability Reporting Directive (CSRD) zal bedrijven meer verantwoordelijk maken door hen te verplichten hun impact op mens en planeet bekend te maken. Dat is bedoeld om een einde te maken aan greenwashing en de basis te leggen voor standaarden voor duurzaamheidsrapportages op mondiaal niveau. Deze rapportages zullen in XBRL formaat moeten worden opgesteld.

B4.5. Domein Stelselstandaarden

Digikoppeling

Waarom belangrijk ?

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

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

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

Feitelijk gebruik

Logius (Stelselvoorzieningen) heeft op verschillende peilmomenten (maart 2013, augustus 2013, augustus 2014, augustus 2015, zomer 2016 tot en met 2022) lijsten aangeleverd waarop (onderdelen van) overheden en uitvoeringsorganisaties stonden die op Digikoppeling zeggen te zijn aangesloten. Daaruit is het onderstaande overzicht af te leiden.

Het overzicht wijst uit dat gedurende een reeks van jaren sprake is van een gestage groei van het gebruik van Digikoppeling, die over de afgelopen twee jaar **lijkt te stabiliseren**. Dit is niet per definitie slecht nieuws. In de categorieën gemeenten, provincies en waterschappen is de dekking sinds 2019 volledig te noemen. Voor de categorie Rijk en uitvoeringsorganisaties geldt dat niet voor alle onderdelen Digikoppeling relevant is, zoals bijvoorbeeld voor Gemeenschappelijke regelingen en Adviescolleges.

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 % [5]		57 %	23 %	14 %	40 %
Zomer 2015	64 %		63 %	42 %	24 %	58 %

[5] 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.

Zomer 2016	40 %		75 %	67 %	46 %	64 %
Zomer 2017	67 %		92 %	67 %	50 %	76 %
Zomer 2018	X [6]		98 %	75 %	59 %	95 % [7]
Zomer 2019		60 %	100 %	100 %	100 %	90 % [2]
Zomer 2020		65 %	100 %	100 %	100 %	91%
Zomer 2021		65 % [8]	100 %	100 %	100 %	91 %
Zomer 2022		65 %	100 %	100 %	100 %	91 %

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

Relevante ontwikkeling

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

- in april 2022 heeft het OBDO De toevoeging van een RESTful API-profiel aan Digikoppeling goedgekeurd en naar aanleiding hiervan is een nieuwe versie van de Digikoppeling standaard uitgebracht. Dankzij dit nieuwe profiel is het nu ook mogelijk om binnen het toepassingsgebied van Digikoppeling API's toe te passen conform de Restful API Design Rules (eveneens een 'pas toe of leg uit' -standaard);
- de Digikoppeling architectuur is hierbij ook aangepast. Enerzijds om het nieuwe RESTful API-profiel op te kunnen nemen in de Digikoppeling standaard. Anderzijds om de harde koppeling tussen het type bevraging en de specifieke Digikoppeling koppelvlakken los te laten. In de nieuwe architectuur worden verschillende transactiepatronen beschreven en wordt weergegeven hoe dit met de verschillende koppelvlakken kan worden ingevuld.

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

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

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

Geo-Standaarden

Waarom belangrijk ?

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

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

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

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

Feitelijk gebruik

In de laatste twee monitors stond al vermeld dat PDOK elk jaar aanzienlijke groeicijfers laat zien. De meest actuele beschikbare gegevens bevestigen dat beeld ook nu weer (bron: PDOK factsheet 2021). Voor verschillende variabelen ziet de ontwikkeling er als volgt uit:

- aan de afnamekant is er een groei van 30,9 miljard hits op PDOK over 2020 naar 36,4 miljard hits over 2021, een groei van 18%;
- aan de aanbodzijde is het aantal datasets gegroeid van 218 (2020) naar 239 in 2021, een groei van 10%;

- het aantal services is gestegen van 562 in 2020 naar 747 in 2021, ook een toename (+33%);
- het aantal hits op het Nationaal Georegister (NGR) is vrijwel stabiel gebleven: 20,8 miljoen in 2020 tegen 21,2 miljoen in 2021 (+2%).

Het geheel overziend is wederom sprake van **toename van het gebruik**, zij het niet meer de forse groei op onderdelen waarover in de vorige monitor werd gerapporteerd. Wat opvalt is de groeiversnelling dit jaar bij het aantal services. Die groei komt mede doordat er nu weer standaardmethodes zijn om data aan te bieden. Verder valt op dat sprake is van een stabilisatie bij het gebruik van het NGR, na een opvallende daling van het gebruik vorig jaar.

Relevante ontwikkeling

In 2022 verwachten we de nieuwe versie van de NEN3610 aan te kunnen melden (is in laatste stappen van proces bij NEN). Verder is de kans groot dat we in 2022 de procedure starten om de profielen voor WMS en WFS te vervangen door de OGC API standaarden, al dan niet in combinatie met de geo-extensie op de NL API strategie. Daarover werd in de vorige monitor ook al gesproken.

StUF

Waarom belangrijk ?

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

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

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

StUF berichten wordt voornamelijk door applicaties gegenereerd, verstuurd, ontvangen en verwerkt. Berichten gaan dus heen en weer 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 op BAG, Kadaster, BRP en vele andere registraties worden via StUF berichten uitgewisseld. Dit gaat dus over vele miljoenen berichten per jaar.

Uit de cijfers blijkt dat gemeenten, ketenpartners en hun leveranciers StUF breed gebruiken. Er is veel pakketsoftware op de markt of dit komt binnenkort op de markt. De adoptie voor StUF BG **neemt nog steeds toe** in oplossingen, al neemt het aantal leveranciers hiervan juist af. Voor StUF ZKN neemt deze af. De reden hiervoor is dat er nieuwe ontwikkelingen zijn voor een nieuwe API-standaard. Onderstaande tabel geeft een beeld van de adoptie van de twee StUF onderdelen (StUF-BG en StUF-ZKN) door de ICT-markt.

	Totaal		**StUF-BG**		**StUF-ZKN**	
Aantal leveranciers	276	(258)	67	(80)	55	(69)
Aantal softwareproducten (incl. versies)	3632	(3413)	1420	(1291)	501	(715)
wv. beschikbaar/in gebruik	1590	(1551)	460	(416)	187	(262)
wv. gepland/in ontwikkeling	109	(112)	60	(52)	16	(28)

Peildatum april 2022 (tussen haakjes de cijfers van de vorige monitor)
(bron VNG-Realisatie: www.softwarecatalogus.nl)

Uit het overzicht valt af te lezen dat het aantal leveranciers is gestegen (overall een stijging van 7%). Dit komt onder andere doordat het gebruik van de softwarecatalogus niet meer van een convenant afhankelijk is. Dit heeft voor een overall toename van pakketten gezorgd; het aantal softwarepakketten stijgt met 6,4%. Als aanvulling op de cijfers uit de tabel: het gebruik van de softwarecatalogus door gemeenten is gelijk aan het gebruik bij de vorige meting in 2021.

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

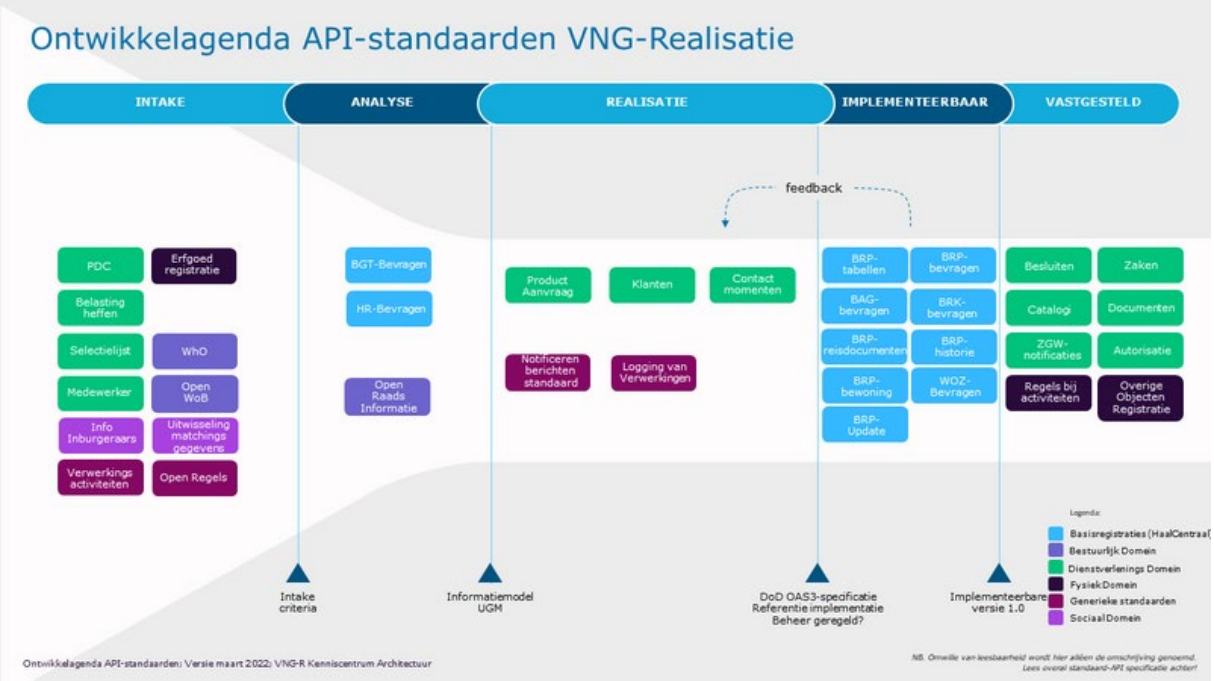
Er zijn geen grote wijzigingen doorgevoerd in StUF koppelvlakken. Trendmatig zien we over de gehele breedte deze periode een stijging van het aantal tests door leveranciers. Voor deze twee specifieke StUF koppelingen zien we een lichte daling. Dit valt samen met de ontwikkeling richting het gebruik van API's voor het zaakgericht werken (zie hieronder bij relevante ontwikkeling).

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

Relevante ontwikkeling

VNG Realisatie zet in het kader van Common Ground in op het gebruik van REST API standaarden. In verband daarmee worden er REST API standaarden ontwikkeld als alternatief voor de StUF standaarden. Ook wordt gestuurd op het vervangen van de StUF standaarden in het gemeentelijke IT landschap. Met name bij Zaakgericht Werken worden daar resultaten geboekt. Een ander initiatief in dat kader zijn de Haal Centraal API's waarmee gegevens direct bij een aantal basis registraties opgevraagd kunnen worden. Op de lange termijn zal dit in ieder geval leiden tot een afname van het gebruik van de StUF standaard en zo mogelijk zelfs tot het verdwijnen van de StUF standaarden.

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



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

B4.6. Domein Water en bodem

Aquo-standaard

Waarom belangrijk ?

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

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

Feitelijk gebruik

Het gebruik van de Aquo-standaard binnen het waterbeheer is groot. Zo hebben de waterbeheerders (waterschappen, de provincies en Rijkswaterstaat) jaarlijks de verplichting om aan bij het ministerie van Infrastructuur & Waterstaat te rapporteren over de waterkwaliteit en waterveiligheid. Hiervoor zijn verschillende informatiestromen ingericht die het Informatiehuis Water organiseert en faciliteert. Door daarbij gebruik te maken van de Aquo-standaard is sprake van uniforme en efficiënte gegevensuitwisseling. De volgende informatie over het gebruik van de Aquo-standaard is afkomstig uit het jaarverslag 2021 van het Informatiehuis Water (april 2022):

- Aquo Wiki unieke bezoekers 250-400 per week
- Aquo-Domeintabellen Service (raadplegen): ca. 5.000.000 keer
- IM Metingen (uitwisselen): ca. 10.000.000 keer
- Aquo-kit webservice: meer dan 480.000 keer
- Binnen Z-info: ca. 1.000.000 keer
- In de Centrale Distributielaag van het Waterschapshuis ca. 40.000 keer

Voor de onderdelen die in de vorige monitor ook al vermeld zijn, geldt dat het gebruik in 2021 ongeveer hetzelfde is als in 2020 – het is **stabiel**.

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

- Instroom op de Aquo-standaard:
  - aantal ingediende wijzigingsvoorstellen: 184 (vorig jaar: 132)
  - aantal gemelde incidenten: 135 (vorig jaar: 117).

  Beide stijgingen zijn mogelijk een gevolg van het online werken waardoor de gebruikers ons makkelijker kunnen vinden. Bovendien bieden we sinds 2020 online introducties op de Aquo-standaard aan.
- aantal waterbeheerders dat een wijzigingsvoorstel indient / een incident meldt:
  - betrokken instanties bij wijzigingsvoorstellen: 33 (vorig jaar: 27)

- betrokken instanties bij melden incident: 47 (vorig jaar: 44)

Relevante ontwikkeling

In 2021 is de nieuwe Aquo-omgeving: Aquo Wiki, in gebruik genomen. Deze nieuwe geïntegreerde omgeving wordt al veelvuldig gebruikt getuige het aantal unieke bezoekers van 250 tot 400 per week (zie bovenstaand cijfer-overzicht).

GWSW

Waarom belangrijk ?

Riolering is een essentiële maatschappelijke voorziening en het beheer ervan een sleuteltaak voor gemeenten. Het doelmatig managen van (afval)watersystemen vereist een gemeenschappelijke taal. Ook maatschappelijke opgaven zoals klimaatadaptatie, energietransitie en de bouwopgave vereisen een (digitale) integrale aanpak, waarbij gezamenlijke definities van gegevens een voorwaarde zijn. Het Gegevenswoordenboek Stedelijk Water (GWSW), een speciale datastructuur die systemen en processen op het gebied van stedelijk waterbeheer beschrijft, voorziet hierin. De GWSW-ontologie specificeert het uniform vastleggen, uitwisselen, presenteren en (her)gebruiken van data van objecten (kenmerken, conditie, metingen) en processen.

De GWSW-standaard staat op de 'pas toe of leg uit' lijst sinds 23 maart 2020.

Feitelijk gebruik

Eind 2021 hebben 160 gemeenten rioleringsdatasets op het landelijke dataplatform met rioleringsdatasets geplaatst. Een jaar daarvoor, eind 2020, waren dat nog 120 gemeenten. De **gestage groei** (net als vorig jaar) is toe te schrijven aan het volgende:

- in 2021 zijn meer beheerapplicaties het GWSW gaan ondersteunen waardoor gemeenten in staat zijn het GWSW zelf toe te passen;
- steeds meer gemeenten willen hun rioleringsdata open publiceren via Publieke Dienstverlening Op de Kaart (PDOK)[9];
- andere (software-)toepassingen gaan GWSW-conforme rioleringsdata benutten waardoor gemeenten gemotiveerd raken het GWSW zelf ook te gaan toepassen;
- toenemende regionale samenwerking is voor gemeenten en waterschappen een prikkel om het GWSW te gebruiken als basis voor hun beheer en daarbij benodigde data(uitwisseling).

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

- alle bestekken voor rioolreiniging en –inspectie schrijven het RibX uitwisselformaat voor;

[9] PDOK is een platform voor het ontsluiten van geodatasets van Nederlandse overheden.

- en uit de jaarlijkse GWSW applicatietoets blijkt dat de meerderheid van de rioleringsbeheerpakketten, alle inspectiesoftware en alle modelleringssoftware de voorgeschreven GWSW-formaten kunnen uitwisselen.

Relevante ontwikkeling

Het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) heeft op 12 mei 2021 op voorspraak van Forum Standaardisatie een aantal mutaties op de officiële lijsten met open standaarden bekrachtigd. GWSW versie 1.4 is daarmee op de 'Pas toe of leg uit'-lijst vervangen door versie 1.5.1 en eind 2021 is dat vervangen door versie 1.5.2. Overheden zijn verplicht bij alle relevante software-aanbestedingen de GWSW-standaard inclusief gespecificeerde uitwisselformaten OroX, HydX en RibX te eisen. Met name de module GWSW-HYD ten behoeve van hydraulische modellering en de ontsluiting rioleringsdata naar PDOK leiden tot meer gebruiksmogelijkheden voor gemeenten, waterschappen en adviesbureaus.

Voor gemeenten is het nog niet vanzelfsprekend dat de vigerende GWSW-standaard en uitwisselformaten als eis gelden voor hun integraal softwarepakket voor beheer van (objecten in) de openbare ruimte. Hoewel het draagvlak bij functioneel beheerders afgelopen twee jaar wel sterk gegroeid is, is dat bij inkoopafdelingen, management en bestuur nog niet bekend en vanzelfsprekend. Omdat implementatie van het GWSW op termijn wel zal leiden tot aanpassingen in werkprocessen, benodigde competenties en inrichting van ICT-systemen, is ook daar wel draagvlak nodig. De PTOLU-status zal daaraan bijdragen. De zeer positieve verhouding van de kosten (voor ontwikkeling en implementatie van de GWSW-standaard) tot de baten (in de vorm van betere inzichten, betere investeringen, betere beheermaatregelen en betere afstemming) zal dat versterken.

SIKB0101 en SIKB0102

Waarom belangrijk ?

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

SIKB0102 voorziet in de optimalisering van de digitale uitwisseling van archeologische gegevens tussen opgravende instanties, vondstendepots en/of archeologische registers. Een opgravende instantie, overheidsorganisatie of een bedrijf dat archeologisch onderzoek en/of vondsten doet heeft namelijk een wettelijke plicht om binnen twee jaar na afronding van de opgraving de verzamelde informatie beschikbaar te stellen aan daartoe ingestelde depots binnen de overheid: op landelijk niveau, provinciaal, en op gemeentelijk niveau. SIKB0102 staat op de 'pas toe of leg uit' lijst sinds februari 2016.

Feitelijk gebruik

Voor beide standaarden geldt dat informatie over de milieu-hygiënische kwaliteit van de bodem (SIKB0101) respectievelijk over archeologische vondsten in de bodem (SIKB0102) in de regel niet door overheden zelf wordt gegenereerd. Marktpartijen zoals onderzoeksbureaus en opgravende bedrijven voeren het onderzoek uit. Daarna leveren deze marktpartijen de verzamelde informatie aan bij overheden, waarna de overheden deze informatie weer onderling delen. De keten van bodeminformatie bestaat in deze context dus zowel uit private partijen als uit overheidsorganisaties. De beide standaarden worden zowel gebruikt voor de uitwisseling binnen het private domein, de uitwisseling van het private domein met het publieke domein als voor de uitwisseling van overheidsorganisaties onderling. SIKB0101 en SIKB0102 zijn breed geïmplementeerde standaarden binnen de domeinen Bodem en Archeologie.

Specifiek met betrekking tot SIKB0101 is de praktijk dat alle gemeenten, omgevingsdiensten en provincies werken met software die gebruik maakt van de datastandaard SIKB0101. Dit blijkt uit de overeenkomsten die SIKB heeft met de leveranciers van software die SIKB0101 gebruiken. Deze leveranciers zijn lid van de Technische Werkgroep die de wijzigingsverzoeken behandelt voor SIKB0101. Softwareleveranciers als ook de eindgebruikers van data zijn in het Centraal College van Deskundigen (CCvD) Datastandaarden vertegenwoordigd, waar besluitvorming plaatsvindt over de doorontwikkeling van de standaard. Daarnaast wordt voor Fase II van de Basisregistratie Ondergrond (BRO) SIKB0101 expliciet genoemd als uitwisselstandaard voor de data over de milieukwaliteit van de bodem.

Op jaarbasis worden miljoenen data uitgewisseld via SIKB0101 tussen applicaties die deze standaarden hebben geïmplementeerd. In de vorige monitor was nog sprake van toename van het gebruik van SIKB0101, vooral toe te schrijven aan een breder gebruik van de standaard. Dit jaar wordt vanuit de beheerorganisatie aangeven dat het **gebruik van SIKB0101 stabiel** is. Gezien het feit dat alle gemeenten, omgevingsdiensten en provincies werken met software die gebruik maakt van de datastandaard SIKB0101, is de groeipotentie voor wat betreft het aantal gebruikers uit de overheidssector niet groot meer bij SIKB0101.

Via SIKB0102 is sprake van uitwisseling van tienduizenden data; dit betreft een veel kleinere markt dan die van SIKB0101. Voor deze standaard SIKB0102 is sprake van **toename van het gebruik** gedurende het afgelopen jaar. Bij SIKB0102 is vooral sprake van toename in de keten bij opgravende bedrijven waar digitale uitwisseling steeds meer gemeengoed wordt. De beheerorganisatie achter de standaarden, SIKB, ziet dit aan de toename van het aantal softwareleveranciers en -ontwikkelaars die een deelnameovereenkomst hebben met SIKB voor het gebruik van SIKB0102 (en ondersteuning). Ook wordt een toenemend gebruik van de validatietool waargenomen. Dit geldt zowel voor marktpartijen (opgravende bedrijven) als depots. De volgende partijen gebruiken de datastandaard SIKB0102 in hun software en stellen het gebruik ervan verplicht:

- landelijk registratiesysteem ARCHIS van de Rijksdienst voor het Culturele Erfgoed (RCE);
- Data Archiving and Networking Services (DANS). Het E-depot voor de duurzame opslag van digitale data;

- BIJ12, beheerder van het provinciaal depot beheer system (Archeodepot). Archeodepot wordt inmiddels door 11 van de 12 provincies gebruikt.

De aanlevering aan het provinciale informatiesysteem Archeodepot loopt inmiddels 100% via SIKB0102. Nagenoeg alle provincies maken gebruik van dit systeem waarvan het beheer is ondergebracht bij GBO-BIJ12. Vanuit Archeodepot worden gegevens volledig geautomatiseerd doorgezet naar het landelijke E-depot van DANS. Aansluiting van Archis op deze landelijke voorziening is in ontwikkeling. In 2021 zijn de eerste stappen gezet om ook gemeenten met een eigen depot (in totaal 26 gemeenten) aan te laten sluiten op Archeodepot.

Relevante ontwikkeling

De drinkwatersector (publiek/privaat) is in 2019 gestart met de implementatie van SIKB0101. In nauw overleg met Geonovum is gesproken over harmonisatie van de standaarden van de Basisregistratie Ondergrond (BRO) met SIKB0101. Op dit moment worden voorbereidingen getroffen voor het uitbreiden van de Basisregistratie Ondergrond met data over de milieuhygiënische kwaliteit van de bodem (BRO fase II). Voor deze fase van de BRO geldt SIKB0101 als uitgangspunt voor de uitwisseling met de landelijke voorziening BRO. Eerder is overigens al opgemerkt dat de groeipotentie voor wat betreft het aantal gebruikers uit de overheidssector van SIKB0101 niet groot meer is.

Voor de komende jaren zal Archeodepot open worden gesteld voor meer gemeentelijke depots waarmee de standaard SIKB0102 ook binnen de gemeenten een steeds belangrijkere rol gaat spelen. Dit proces van openstelling is gaande (zie hierboven). Met name bij gemeenten valt dan ook nog winst te behalen voor wat betreft het gebruik, maar ook bij provincies die recent zijn gestart met digitale uitwisseling.

B4.7. Domein Bouw

COINS

Over deze standaard is dit jaar helaas geen informatie ontvangen.

IFC

Waarom belangrijk ?

IFC is een gestandaardiseerde, digitale beschrijving van assets in de bouw- en infrasector en wordt ontwikkeld door de internationale organisatie buildingSMART. In Nederland wordt de standaard ondersteund door de lokale buildingSMART organisatie. Het is een open, internationale standaard (ISO 16739-1:2018) en bevordert uitwisseling van leveranciers-neutrale en bruikbare informatie tussen hardware-apparaten, softwareplatforms, en interfaces voor veel verschillende use cases. IFC is een standaard voor zowel semantische afspraken als voor dataformats en richt zich specifiek op BIM-informatie over bouwwerken.

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

Feitelijk gebruik

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

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

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

Er wordt eens in de twee jaar gemeten. Bovenstaande sores zijn derhalve dezelfde als vorig jaar. Bij een volgende meting (2023) zal moeten blijken hoe een en ander zich ontwikkelt. Vooralsnog is sprake van lage scores op kennis en gebruik van deze standaard bij de genoemde deelsector, het **gebruik is beperkt**. Dit beeld sluit aan bij de opbrengst van het in augustus 2021 verschenen Evaluatierapport Bouwstandaarden, uitgevoerd in opdracht van Bureau Forum Standaardisatie. Enkele conclusies uit die evaluatie luiden als volgt:

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

Relevante ontwikkeling

In 2019 en 2020 is aangetoond in een door TNO samen met het ministerie van BZK ontwikkelde Proof of Concept dat geautomatiseerde checks op wet- en regelgeving op basis van IFC mogelijk is.

Inmiddels is de gemeente Rotterdam gestart met een pilot voor automatische vergunning-controleservice waarbij IFC als uitwisselformaat is gekozen en gekoppeld wordt aan gebouwgegevens. Met behulp van de ifc OWL-ontologie kan men IFC-gegevens beschikbaar stellen zodat gebouwgegevens eenvoudig kunnen worden gekoppeld aan

materiaalgegevens, GIS-gegevens, gegevens van productfabrikanten, sensorgegevens, classificatieschema's, sociale gegevens, enzovoort. Het resultaat is een web van gekoppelde gebouwdata dat grote kansen biedt voor databeheer en -uitwisseling in de bouwsector en daarbuiten. Deze ontwikkeling bevindt zich weliswaar nog in de ontwikkelfase, maar kan in de toekomst een grote impact kan hebben in het kader van de Wet Kwaliteitsborging.

Naast deze ontwikkeling wordt IFC4.3 momenteel verder ontwikkeld als uitbreiding voor de beschrijving van infrastructuurwerken binnen de domeinen Spoorwegen, Wegen, Havens en Waterwegen, met inbegrip van de elementen die in die domeinen gemeenschappelijk zijn. Naar verwachting wordt ook deze standaard op niet al te lange termijn door ISO erkend als standaard.

NLCS

Waarom belangrijk ?

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

Feitelijk gebruik

Het feitelijk gebruik door overheidsorganisaties ziet er als volgt uit.

Type overheid	Aantal gebruikers CAD Software met NLCS in 2020	Aantal gebruikers CAD Software met NLCS in 2021
Gemeenten	138	138
Waterschappen	15	8
Provincies	10	11
Rijksoverheid	5	5
Netbeheerders	5	5
Kennisinstellingen	6	6
Totaal	179	173

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

Over de groeipotentie van het gebruik van NLCS het volgende. Zeker in de gemeentelijke markt beschikken niet alle organisaties over een civieltechnische afdeling en/of medewerkers met vakinhoudelijke kennis. Deze gemeenten laten zich voor de ontwerp-werkzaamheden conform NLCS volledig ontzorgen door marktpartijen (opdrachtnemers).

Deze gemeenten voldoen dus indirect wel aan de 'pas toe of leg uit' norm, maar zullen niet beschikken over eigen software oplossingen. Verder is het gebruik van de standaard bij beheerders van ondergrondse infrastructuur nog een stuk lager dan zou kunnen. Diverse organisaties gebruiken nog eigen laagindelingen. Dat is wel aan het veranderen en zal nog een stuk sneller gaan wanneer NLCS geschikt wordt gemaakt voor deze sector.

Relevante ontwikkeling

Op 17 juni 2022 is NLCS 5.0 gelanceerd, de langverwachte opvolger van NLCS 4.2. In deze versie is een mapping tussen NLCS met zowel BGT als GWSW opgenomen. Door opname van deze mappings in de database van de NLCS zijn de mappings echt in de NLCS verankerd, waarmee het importeren van BGT/GWSW datasets vanuit verschillende softwarepakketten nu een uniform resultaat opleveren.

Vanuit de markt is er al langer vraag naar uitbreiding van de NLCS voor zowel stedelijk spoor als netbeheer. Binnen de NLCS waren deze groepen slechts beperkt ingericht. Na een inventarisatie binnen de stedelijk spoor en netbeheerbedrijven, staat 2022 in het teken van het uitwerken van de betreffende hoofdgroepen binnen de NLCS. Er zijn afspraken gemaakt met leveranciers om naast de NLCS 5.0 te kunnen werken met testversies van de diverse uitbreidingen. Deze worden als "losse test modules" toegevoegd aan de NLCS-database. Hiermee wordt in een iteratief proces gekomen tot een verdere ontwikkeling van de standaard wat uiteindelijk definitief opgenomen wordt in een toekomstige versie van de NLCS. Zo is deze toekomstige versie geschikt bevonden door de stedelijk spoorbedrijven en netbeheerders waarna de uitbreiding breed uitgedragen kan worden naar alle gebruikers. Met deze uitbreiding is de verwachting dat we meer stedelijk spoorbedrijven en netbeheerders als gebruikers van de NLCS kunnen toevoegen.

Met NLCS 5.0 is een eerste basis gelegd voor de verdere uitbreiding van de NLCS en de aansluiting op informatiemodellen zoals IMBOR, IMKL, GWSW. De vraag naar een koppeling tussen CAD en GIS wordt vanuit de markt steeds luider. Er wordt gewerkt aan een werkbaar principe waarbij het mogelijk wordt om met de CAD-applicatie de objecten te definiëren vanuit het datamodel (OTL) inclusief de kenmerken (attributen) en deze vervolgens middels een geschikte tooling als NLCS-objecten te tekenen. Het doel is om aanvullende kenmerken als data aan de NLCS-objecten te koppelen, zodat hier vervolgens een dataset uit gegenereerd kan worden voor onder andere Assetmanagement. Op het moment dat er een werkbaar principe is kan dit voor de verschillende werkpakketten/ontwikkelingen binnen de NLCS worden ingezet. Deze werkpakketten zijn cruciaal in de opmaat van de NLCS naar een BIM 'Level 2' standaard.

Wij gaan ook voor het werkpakket NLCS – RAW bestekken op dit principe verder investeren. Al 15 jaar doet de markt pogingen om CAD- en RAW-programma's met elkaar te verbinden. Eerder bleek dit niet opportuun, onder andere door het ontbreken van een standaard voor CAD-tekeningen en een sterk verzuilde bedrijfscultuur. Inmiddels zijn de benodigde standaarden beschikbaar en groeit het besef dat je met digitalisering deze werkzaamheden efficiënter uit kunt voeren. Zaak is de verzuiling in de branche te doorbreken, door

standaarden in samenhang te zetten. Met als uiteindelijk doel integrale digitale samenwerking tussen tekenaars, bestekschrijvers, calculators en beheerders.

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

Ook voor het werkpakket Nationaal dataportaal wegverkeer wordt de link tussen CAD en GIS gezocht. Vanuit de brede informatiebehoefte voor mobiliteit werkt het Ministerie van IenW aan het oprichten van een netwerkregistratie voor wegen zodat publieke en private gebruikers kunnen beschikken over digitale informatie over de verkeerskundige inrichting van het wegennetwerk.

Naast de werkpakketten met betrekking tot CAD en GIS is ook het werkpakket Inmetingen (landmeetkundig) verwerken op basis van NLCS direct in de keten relevant. Steeds meer opdrachtgevers eisen dat de ingewonnen meetgegevens direct ingezet kunnen worden in het project. Leveranciers van apparatuur voor data-inwinning sluiten steeds meer aan op de (inter)nationale ontwikkelingen met betrekking tot data-standaarden. Dit is echter nog niet goed geland binnen gebouwde omgeving waar de NLCS een steeds belangrijke en prominente rol speelt. Het doel is om afspraken te maken en te verankeren in de NLCS zodat ingewonnen data direct, conform NLCS, toegepast kunnen worden in de levenscyclus van assets/objecten in de gebouwde omgeving.

VISI

Waarom belangrijk ?

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

Feitelijk gebruik

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

- overheidsorganisaties: 135 (129, 118), als volgt uitgesplitst:
  - Rijk 8
  - Provincies 12
  - Waterschappen 15

  - Gemeenten 96
  - Energiesector 4
- individuele gebruikers bij overheden 9.263 (12.839, 11.480)
- overheidsprojecten 8.021 (7.774, 5.747)

(Peildatum: zomer 2022. Tussen haakjes de gegevens uit de monitor van de afgelopen twee jaren.)

De beheerorganisatie geeft aan dat sprake is van een **lichte toename van het gebruik**. Op twee van de drie variabelen in bovenstaand overzichtje is sprake van een beperkte stijging. Het aantal individuele gebruikers laat weliswaar een duidelijk lagere score zien maar daar moet bij worden aangetekend dat met ingang van dit jaar alleen unieke gebruikers worden geteld (voorheen: gebruikers gekoppeld aan projecten). Bredere toepassing van VISI kan als volgt worden geduid:

- Organisaties kiezen steeds vaker voor het toepassen van VISI, voorafgaand aan de uitvoeringsfase, denk aan ontwerp- en voorbereidingsfase. Dat doet met name het aantal projecten toenemen;
- Projecten schrijven steeds vaker voor dat VISI actief / online moet blijven, ook tijdens de garantie- en onderhoudstermijn;
- Organisaties besluiten steeds vaker om projecten langer actief te houden als online archief, ten behoeven van de toegankelijkheid en traceerbaarheid van de online communicatie en informatie.

Relevante ontwikkeling

Binnen de twee sectoren Bouw & Utiliteit en de installatiebranche is de toepassing van VISI nog erg beperkt. Langzaam komen er steeds meer toepassingen voor nieuwbouw en renovatie van woningbouw. Ook deze trend zal zich vermoedelijk komende jaren gaan doorzetten.

Ook in de energiesector wordt VISI steeds vaker toegepast. Door de grote druk vanwege de energietransitie op de energiesector om projecten versneld uit te voeren zien we in het tweede deel van 2021 al een forse stijging van het aantal projecten bij de verschillende gebruikers in de energiesector. Een trend die zich in 2022 zeker gaat doorzetten.

Op internationaal vlak is van belang dat de Europese Commissie (EC) het 'Rolling plan voor ICT Standard récession 2022' heeft gepubliceerd. Hierin stelt de organisatie welke ICT standaarden moeten bijdragen aan de doelen van de EU. De Commissie heeft daarin ISO 29481-2 (VISI) als een belangrijke ISO bouwstandaarden bestempeld. Dat mag als belangrijke (inter)nationale mijlpaal gezien worden. Er is een nieuwe ISO norm uitgebracht, ISO 29481-3 Building Information Models - Information Delivery Manual – Part3. Data schema en code. Vanuit de Nederlandse VISI beheerorganisatie is actief een bijdrage geleverd om VISI (ISO 29481-2) hierin verwerkt te krijgen. Dit heeft er toe geleid dat de ISO 29481-3 ook transactie- en bericht-structuren bevat.

B4.8. Domein Juridische identificatie en verwijzing

BWB, ECLI en JCDR

BWB

Waarom belangrijk ?

BWB staat voor Basis Wetten Bestand. Het is de Juriconnect-standaard voor identificatie van en verwijzing naar wet- en regelgeving, staat op de 'pas toe of leg uit'-lijst sinds 2 februari 2016. Deze standaard zorgt voor vindbare en betrouwbare data als het gaat om wet- en regelgeving wordt ook wel "logische links naar wetgeving" genoemd. De standaard is een URI, een Uniform Resource Identifier, een unieke computer-leesbare identificatiecode voor een ding, een stuk informatie of data. In dit geval dus voor wet- en regelgeving.

Feitelijk gebruik

BWB 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. Verder wordt BWB toegepast in LiDO, waarover hieronder meer.

Relevante ontwikkeling

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

JCDR

Waarom belangrijk ?

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. Deze standaard zorgt -net als BWB- voor vindbare en betrouwbare data als het gaat om decentrale regelgeving. De standaard is ook een URI , een Uniform Resource Identifier.

Feitelijk gebruik

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

Relevante ontwikkeling

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

ECLI

Waarom belangrijk ?

ECLI is de Europese standaard voor de identificatie van rechterlijke uitspraken en verwijzing daarnaar. ECLI staat op de 'pas toe of leg uit'- lijst sinds 28 november 2013.

Feitelijk gebruik

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

Relevante ontwikkeling

Een nieuwe versie van de standaard is in oktober 2019 gepubliceerd in het Publicatieblad van de Europese Unie. Deze nieuwe versie bevat vooral uitbreidingen; de functionaliteit van de oorspronkelijke standaard blijft ongewijzigd. De nieuwe versie wordt niet nog gebruikt. De Europese Commissie is nu bezig met de implementatie. De vertraging is mede te wijten aan de coronacrisis.

Indicatie feitelijk gebruik van de drie standaarden (BWB, JCDR en ECLI) samen

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

Het gebruik van LiDO wordt sinds de Monitor Open standaarden 2018 aangemerkt als een graadmeter voor het gebruik van de standaarden BWB, JCDR en ECLI samen. Het gebruik lag vorig jaar op ongeveer 540.000 bezoeken en 1.400.000 page-views per maand (peilmoment: 1 januari 2021). Er was toen sprake van een behoorlijke stijging. Dit jaar liggen de cijfers behoorlijk lager periode juni 2021 – mei 2022):

- 2.352.160 bezoekers >> bijna 200.000 per maand
- 4.597.363 page-views >> bijna 400.000 per maand

Een vergelijking van deze cijfers met voorgaande jaren is evenwel niet te maken. Ongeveer een jaar geleden is de meetmethode namelijk aangepast (van log-based naar pixel-based). Daarom kan geen uitspraak worden gedaan over de ontwikkeling van het gebruik.

B4.9. Domein Onderwijs en loopbaan

E-Portfolio NL NEN 2035

Waarom belangrijk ?

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

Feitelijk gebruik

Volgens de gegevens van NEN is de standaard in 2021 4 keer aangeschaft en 5 keer ingezien via NEN Connect (het licentiesysteem van NEN). De score van vorig jaar was 4 keer aangeschaft respectievelijk 12 keer ingezien. Geen van de hier bedoelde gebruikers van de standaard is werkzaam bij een publieke organisatie.

Het aantal gebruikers in 2021 was 16, waarbij het onduidelijk was of hier vertegenwoordigers van overheden bij zaten. Het totale gebruik is afgenomen.

Relevante ontwikkeling

De herziene versie van de internationale standaard ISO/IEC 20013 uit 2020 heeft dezelfde scope als NEN 2035. Beide standaarden bevatten geen tegenstrijdigheden. Over het algemeen heeft het gebruik van een internationale standaard de voorkeur boven een nationale en de ervaring leert dat, wanneer een internationale standaard gepubliceerd is deze gewoonlijk het gebruik van de nationale standaard minimaliseert omdat partijen voor de internationale standaard kiezen. In het geval van de e-portfolio standaarden is dat echter niet het geval: ISO/IEC 20013 is, ondanks gerichte promotie door NEN, niet aangeschaft of ingezien bij NEN.

Ondanks dat de standaard weinig wordt gebruikt, zijn de partijen die de standaard gebruiken hierover zeer tevreden. De partijen met wie gesproken is, geven aan dat NEN 2035 voldoende handvatten biedt en goed bruikbaar is voor hun doelstellingen. Zij zijn tevreden over de toepasbaarheid van NEN 2035 en geven aan geen noodzaak te zien om een andere (internationale) standaard te gaan gebruiken. Uit de gesprekken blijkt dat partijen NEN 2035 bruikbaarder achten dan het internationale alternatief. Voorgesteld wordt NEN 2035 op de lijst te laten staan en in 2022 breder onder de aandacht te brengen bij overheids- en onderwijsorganisaties. NEN zal hiertoe artikelen publiceren in haar eigen nieuwsbrieven en op de eigen website en daarnaast de samenwerking zoeken met organisatie die publicaties voor de onderwijssector bieden.

NL LOM

Waarom belangrijk ?

Door het metadateren van onderwijsmateriaal is zowel het eigen materiaal als het materiaal van anderen (beter) terug te vinden en op verschillende plekken beschikbaar. Dit bevordert de herbruikbaarheid van onderwijsmateriaal. In NL LOM staat beschreven welke metadata toegekend moeten worden aan educatieve content om de vindbaarheid en vergelijkbaarheid van leermateriaal te vergroten. Metadata beschrijven in dit geval de kenmerken van leerobjecten. Te denken valt aan auteursgegevens, titel, uitgever, taal, en dergelijke. NL LOM is een Nederlands toepassingsprofiel van de internationale standaard IEEE-LOM. Deze standaard staat op de pas-toe-of-leg-uit-lijst sinds 29 mei 2011.

Feitelijk gebruik

NL-LOM wordt gebruikt door verschillende organisaties in de onderwijs- en publieke sector. Om een beeld te krijgen van het gebruik van Nl-LOM kan het volgende onderscheid dienen:

- gebruiksgegevens van NL-LOM binnen de Edurep aansluitingen;
- gebruiksgegevens van NL-LOM buiten de Edurep aansluitingen.

Er zijn op Edurep momenteel 37 collecties aangesloten[10] waarvan het grootste deel met een NL-LOM-aansluiting. Een aantal partijen levert een ander formaat aan (DC/DIDL-MODS). Deze groep van 37 collecties is als volgt samengesteld:

- 10 komen van Kennisnet zelf;
- 15 komen van het Hoger Onderwijs: hogescholen en universiteiten;
- 5 zijn afkomstige uit de sector natuur- en milieu-educatie (NME);
- de overige zijn onafhankelijke partijen (voorbeelden: Webkwestie of de Anne Frank Stichting) en andere publiek gefinancierde partijen zoals KlasCement, SchoolTV of het Nationaal Archief.

Het afgelopen jaar is een aantal nieuwe collecties aangesloten. In die zin zou dat een indicatie kunnen zijn van een **lichte toename** van het gebruik van NL-LOM *binnen de Edurep aansluitingen*.

Voor het overige (buiten Edurep) zijn geen gegevens beschikbaar. Het doen van uitspraken over een ontwikkeling van het gebruik is daar dan ook verder niet mogelijk.

Relevante ontwikkeling

Vanuit het project Erfgoed (erop gericht om de erfgoed-sector beter vindbaar te maken in het onderwijs) is Edurep dit jaar geschikt gemaakt om educatieve evenementen te kunnen

[10] Zie https://demonstrator-s.edurep.nl/nllom. Bron van dit overzicht is Kennisnet. Van Bureau Edustandaard en van SURF is geen reactie ontvangen.

verwerken. Hierbij gaat het over het delen van een 'leermiddel', zoals bijvoorbeeld een rondleiding op een specifieke plaats en een bepaalde tijd.

In dit traject is aan het licht gekomen dat NL-LOM niet toereikend is om dit soort gegevens te verwerken, en is besloten om dergelijke gegevens in een andere standaard te verwerken: Schema.org. En aangezien Schema.org een standaard is waarmee ook andere soorten gegevens kunnen worden uitgedrukt (bijvoorbeeld ook educatieve applicaties), is besloten om de NL-LOM data ook uit te drukken in Schema.org (LearningResource - Schema.org Type).

Wat Schema.org ook interessant maakt is de mogelijkheid voor een partij om dit mee te leveren als metadata van webcontent, waarmee een en ander beter vindbaar wordt in zoekmachines. De verwachting is dat het voor een betrokken partij een veel interessantere propositie is om in te investeren dan in een specifieke standaard alleen voor een aansluiting Edurep. Vanuit Edurep-perspectief kan dan ook worden gesteld dat Schema.org een alternatief voor NL-LOM biedt dat de potentie heeft om beter te renderen.

Bureau Edustandaard geeft aan dat de standaard weliswaar in het onderwijsveld goed geadopteerd is, maar dat daarmee het werkingsgebied ook wel is verzadigd. SURF heeft de ambitie uitgesproken het werkingsgebied uit te willen breiden naar onder andere de cultuursector, bijvoorbeeld bij het Rijksmuseum Daarnaast is de ambitie uitgesproken door SURF om overheidsbreed de adoptie te verhogen. De standaard is voor het onderwijs dusdanig geïntegreerd en nuttig, dat handhaving op de 'Pas toe of leg uit'-lijst niet per se nodig is. Wanneer men daadwerkelijk andere sectoren deze standaard wil gaan laten gebruiken, is handhaving op de 'Pas toe of leg uit'-lijst wel nuttig en zelfs noodzakelijk.

Wanneer de activiteiten eind 2022 door SURF en Bureau Edustandaard nog niet hebben geleid tot het resultaat dat meer organisaties(buiten de onderwijssector) de standaard hebben geadopteerd, is de optie om de standaard te verwijderen opnieuw te overwegen.

B4.10. Domein Overig

EML_NL

Waarom belangrijk ?

EML_NL is het Nederlands toepassingsprofiel op de Election Markup Language standaard. De standaard definieert de gegevens en de uitwisseling van digitale gegevens bij verkiezingen (die vallen onder de Nederlandse Kieswet). Daarbij gaat het om de uitwisseling van gegevens over kandidaten en over uitslagen om zo de verkiezingsuitslag en zetelverdeling vast te kunnen stellen. EML_NL draagt ertoe bij dat het verkiezingsproces transparant plaatsvindt en met minder kans op overname- en optelfouten. De standaard staat op de 'pas toe of leg uit'-lijst sinds 28 november 2013.

Feitelijk gebruik

De EML_NL standaard is opgenomen in de Ondersteunende Software Verkiezingen OSV2020. Het gebruik van de OSV2020 is daarmee een indicator voor het gebruik van de EML_NL standaard. OSV2020 wordt beschikbaar gesteld bij verkiezingen die onder de Kieswet vallen.

Alle bij het verkiezingsproces betrokken overheden maken gebruik van OSV2020 programmatuur bij verkiezingen en passen zo de EML_NL toe. Zo is – sinds de vorige versie van deze monitor – de OSV2020 en daarmee de EML_NL standaard toegepast bij de Gemeenteraadsverkiezingen van 16 maart 2022. De Kiesraad heeft de verkiezingsgegevens van deze als EML_NL dataset ontsloten op data.overheid.nl en de gegevens in de EML_NL bestanden gebruikt voor het opnemen van de verkiezingsuitslag in de Databank verkiezingsuitslagen.

Het gegeven dat inmiddels alle overheden in geval van verkiezingen gebruik maken van de OSV2020 programmatuur maakt dat met deze standaard in de huidige vorm een **stabiel** 100% doelbereik wordt gerealiseerd.

Relevante ontwikkeling

In de vorige monitor is al opgemerkt dat het dossier ten aanzien van verkiezings-programmatuur onderwerp van gesprek was tussen de Kiesraad, het ministerie van BZK en de VNG. Toen werd gesteld dat het – afhankelijk van de uitkomst van dat overleg – zou kunnen zijn dat kaders en eisen ten aanzien de OSV2020 worden herzien met mogelijk ook gevolgen voor de manier waarop het gebruik van EML_NL wordt voorgeschreven. Inmiddels is een concept wetsvoorstel Wet programmatuur verkiezingsuitslag in internet consulatie geweest. Verschillende partijen hebben hierop gereageerd/geadviseerd waaronder de VNG/NVVB en de Kiesraad. Het ministerie van BZK heeft het wetsvoorstel (op dit moment) nog niet ingediend bij de Tweede Kamer.

Geplaatst tegen deze achtergrond blijft de EML_NL standaard voorlopig nog op de ‘pas toe of leg uit’-lijst staan.

Forum Standaardisatie
Standaard Samenwerken

Meting Informatieveiligheidstandaarden overheid voorjaar 2022

Inclusief IPv6

Datum document: 26 augustus 2022

Status document: Definitief t.b.v. SO OBDO *(inclusief enkele correcties BFS, versie 8-11-2022)*

Inhoudsopgave

Leeswijzer

Dit rapport is piramidaal gestructureerd en begint in hoofdstuk 1 met de conclusies, adviezen, en het totaalbeeld.

Hoofdstukken 2 en 3 gaan in op het algehele beeld rond de adoptie van respectievelijk websitebeveiligingsstandaarden en e-mailbeveiligingsstandaarden.

Hoofdstuk 4 gaat in op de adoptie van IPv6 voor websites en e-mail.

Hoofdstuk 5 en 6 gaan dieper in op de adoptiegraad per standaard van respectievelijk de verschillende overheidscategorieën en ministeries.

Hoofdstuk 7 beschrijft de achtergrond van de meting, waaronder de beleidsmatige afspraken, desbetreffende standaarden en de methodiek.

De bijlagen geven detailinzicht per internetdomein, gecategoriseerd naar overheidscategorie of ministerie.

1. Samenvatting

Overheidsbreed zijn afspraken gemaakt om moderne internetstandaarden voor websites en e-mail versneld te adopteren. Forum Standaardisatie meet op verzoek van het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) halfjaarlijks de

implementatievoortgang van deze afspraken. De afgesproken uiterlijke implementatiedata zijn voor alle standaarden al verstreken, waardoor verwacht mag worden dat alle webapplicaties en e-mailsystemen deze standaarden correct toepassen. In dit document wordt gerapporteerd over de stand van zaken per mei 2022.

Overheden die internetdomeinen niet veilig configureren nemen onnodige risico's. Het gaat daarbij om een verhoogde kans op phishing uit naam van overheidsorganisaties, en een verhoogde kans op manipulatie en afluisteren van web- en e-mailverkeer. Een prominent voorbeeld van de gevolgen van onveilige configuratie van standaarden is een incident van e-mailphishing namens *@overheid.nl* in 2018, toen van 200 burgers DigiD-inloggegevens zijn buitgemaakt.

De meting laat zien dat bij 53% van de internetdomeinen alle verplichte websitestandaarden correct zijn toegepast. Het gaat om belangrijke beveiligingsstandaarden voor vertrouwelijk webverkeer, en IPv6 voor duurzame bereikbaarheid van online diensten.

Bij 44% van de internetdomeinen zijn alle verplichte e-mailstandaarden correct toegepast. Hier gaat het om belangrijke beveiligingsstandaarden om e-mailvervalsing uit naam van de overheid te voorkomen en het e-mailverkeer vertrouwelijk te houden, en ook IPv6 voor duurzame bereikbaarheid van online diensten.

Met de meting zijn in totaal 2584 overheidsdomeinen gecontroleerd. Dat is een uitbreiding ten opzichte van voorgaande metingen, in de voorgaande meting zijn 559 overheidsdomeinen gecontroleerd. De 2584 overheidsdomeinen zijn slechts een deelwaarneming van alle overheidsdomeinen, het totaalportfolio heeft vele duizenden meer domeinen. De overheid heeft als geheel geen zicht op het totaalportfolio. Dit rapport toont met diverse doorsnedes inzicht in de stand van zaken per overheidscategorie en per ministerie. De mate van adoptie kan gezien worden als een indicator voor de effectiviteit van sturing op kwaliteit van de informatievoorziening.

1.1. Adviezen

Zeven jaar na het maken van de eerste streefbeeldafspraak, en ruim twee jaar na het maken van de laatste, is geen van de streefbeelden voor de overheid als geheel gehaald. Het ontbreekt aan effectieve sturingsmechanismen om overheidsbrede afspraken eenduidig te laten landen en nageleefd te krijgen binnen individuele overheidsorganisaties. Zodra de Wet Digitale Overheid van kracht wordt kunnen standaarden wettelijk worden verplicht, zoals reeds is voorgenomen met HTTPS en HSTS. Ook hier speelt de vraag hoe deze verdergaande verplichtingen de operationele werkvloer bereiken, en hoe vervolgens gestuurd wordt op naleving van de verplichtingen.

Advies 1: onderzoek welke sturingsmechanismen kunnen worden ingezet om overheidsbrede architectuurafspraken en kwaliteitseisen (beleid) – bijvoorbeeld in de vorm van gemeenschappelijke standaarden en streefbeeldafspraken – effectief te laten landen in de uitvoering bij de individuele overheidsorganisaties (implementatie).

Positieve uitschieters binnen overheidscategorieën en tussen ministeries zijn vaak te verklaren vanuit proactieve sturing (regie) op de toepassing van standaarden, bijvoorbeeld vanuit een CIO- of CISO-office (voorbeelden: CIO BZK en CISO VWS). Proactieve sturing op de omvang en kwaliteitsaspecten van het internetdomeinportfolio is noodzakelijk om risico's voor zowel organisaties als burgers te kunnen beheersen. Als handreiking heeft Forum Standaardisatie vijf basisprincipes voor regie op internetdomeinen op een rij gezet. Voor de Rijksoverheid heeft het Rijksprogramma voor Duurzaam Digitale Informatiehuishouding (RDDI), in samenwerking met Forum Standaardisatie, in 2021 de Handreiking Beheer Internetdomeinen Rijksoverheid gepubliceerd.

Het komt regelmatig voor dat websites of e-maildiensten decentraal ingekocht worden, terwijl er centrale (overheids)dienstverlening bestaat waarmee dezelfde diensten efficiënter geleverd kunnen worden. Met regie op internetdomeinen kan er beter op gestuurd worden dat centrale dienstverlening ook wordt benut.

Advies 2: organiseer regie op internetdomeinen binnen ministeries en individuele overheidsorganisaties. Jaag dit initieel project- of programmamatig aan, en borg dit vervolgens in de lijnorganisatie.

Centralisering van dienstverlening heeft veelal een positief effect op de toepassing van standaarden. Wanneer een gemeenschappelijke dienstverlener een standaard consequent toepast heeft dit een hefboomeffect. Dit is zichtbaar bij diverse dienstverleningsconcepten; bijvoorbeeld de centrale registrarrol die de Dienst Publiek en Communicatie (AZ/DPC) vervult voor de Rijksoverheid, maar ook bij gemeenschappelijke dienstverleners voor web en e-maildiensten, zoals SSC-ICT, DICTU en diverse regionale dienstverleners.

Advies 3: verken of het centrale dienstverleningsconcept rond DNS-beheer van de Rijksoverheid ook kan worden ingezet bij decentrale overheden.

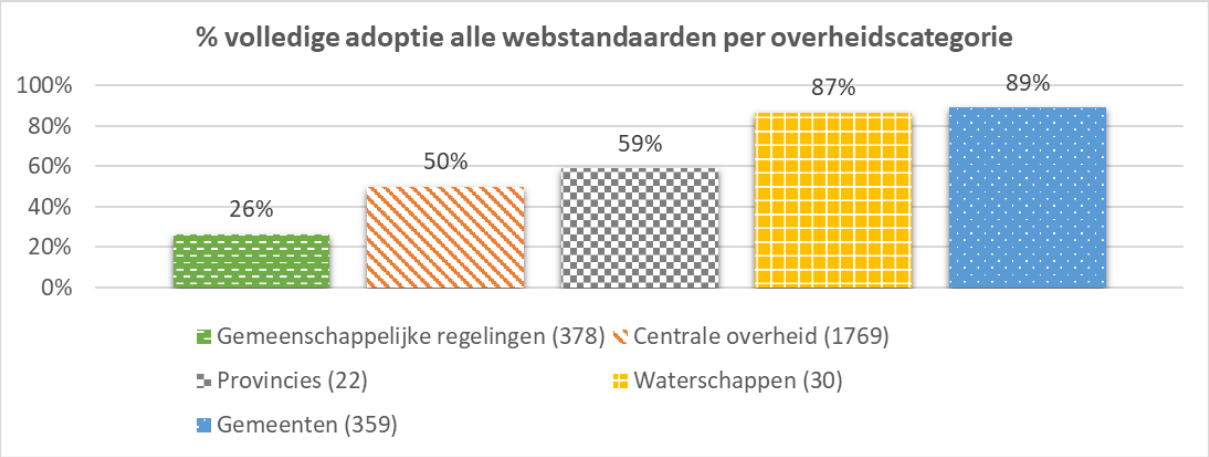
Overheden besteden hun e-mailvoorzieningen steeds vaker uit aan clouddienstverleners. Een aantal van dit soort dienstverleners ondersteunen niet alle verplichte standaarden. Conform het open standaardenbeleid zou formeel moeten worden gekozen voor dienstverlening die de standaarden wel ondersteunt. Indien hiervan is afgeweken is het belangrijk dat overheden hun dienstverleners alsnog blijven vragen om ondersteuning van verplichte standaarden. Diverse dienstverleners geven in informele gesprekken aan dat een gebrek aan klantvraag een reden is om niet te investeren in ondersteuning van de voor overheid verplichte standaarden.

Advies 4: zorg ervoor dat naleving van IT-kwaliteitseisen – waaronder ondersteuning van verplichte open standaarden – onderdeel zijn van het leveranciersmanagement van individuele overheidsorganisaties. Vraag leveranciers periodiek naar de planning voor ondersteuning van standaarden. Overweeg om over te stappen als een leverancier onvoldoende meebeweegt.

1.2. Websitestandaarden

1.2.1. Totaalbeeld websites per overheidscategorie (incl. IPv6)

Onderstaande cijfers laten zien in welke mate de verschillende overheidscategorieën *alle* afgesproken websitestandaarden voor veilig en modern webverkeer toepassen (inclusief IPv6). Gemeenten en waterschappen lopen gemiddeld gezien ver voor op de andere categorieën. De gemeenschappelijke regelingen lopen ver achter. Waarschijnlijk zijn de streefbeeldafspraken niet doorgesijpeld naar deze instanties, hoewel zij in veel gevallen gefinancierd worden vanuit de andere overheden.



Hoofdstuk 2 gaat in meer detail in op de specifieke websitebeveiligingsstandaarden, hoofdstuk 4 gaat in op IPv6.

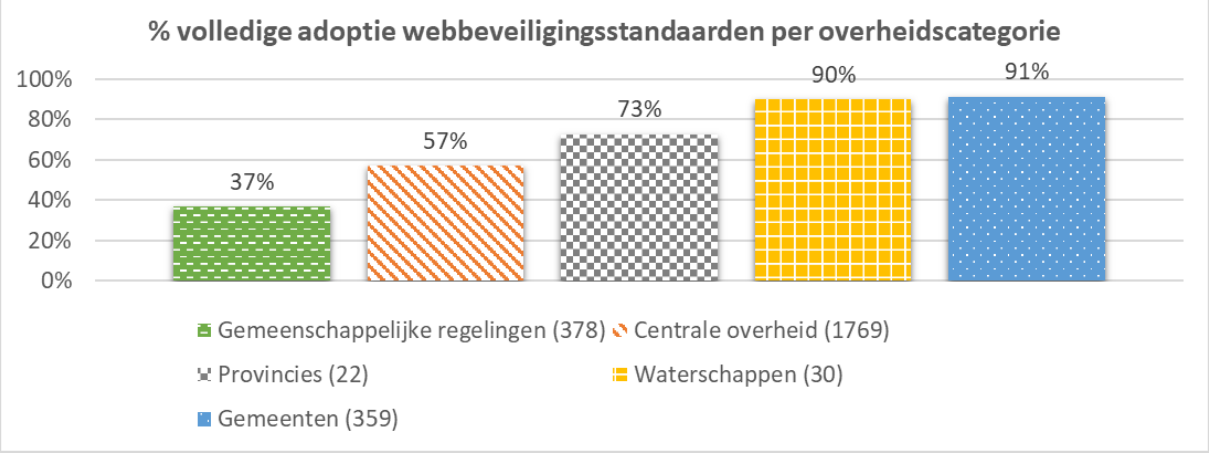
1.2.2. Websitebeveiligingsstandaarden (excl. IPv6)

Door toepassing van websitebeveiligingsstandaarden wordt de verbinding met overheidswebsites beter beveiligd, zodat criminelen niet zomaar uitgewisselde gegevens kunnen onderscheppen of manipuleren.

Deze paragraaf laat het totaalbeeld per overheidscategorie en het totaalbeeld per ministerie zien (zonder IPv6).

1.2.2.1. Adoptie per overheidscategorie

De achterblijvers zijn met name te vinden bij de centrale overheid en de gemeenschappelijke regelingen. De centrale overheid is getalsmatig oververtegenwoordigd

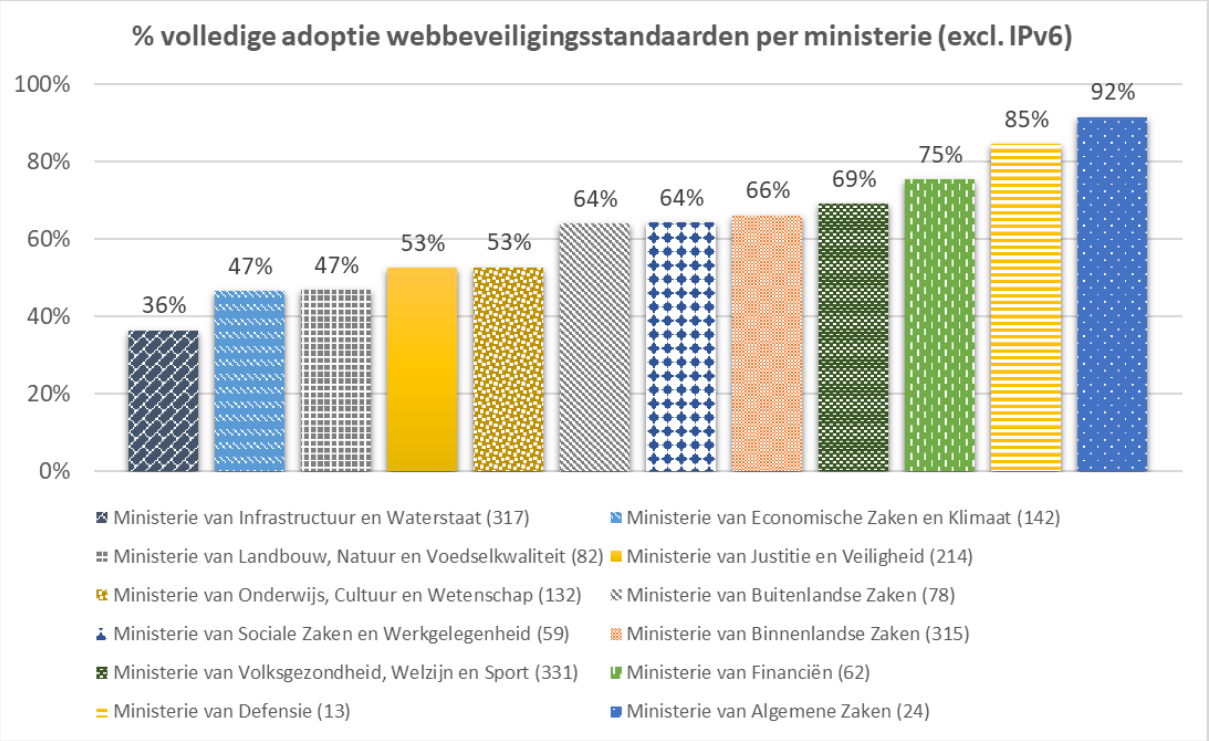


Centrale overheid	57%	1769
Provincies	73%	22
Waterschappen	90%	30
Gemeenten	91%	359
Gemeenschappelijke regelingen	37%	378

Voor meer details per overheidscategorie zie hoofdstuk 5.

1.2.2.2. Adoptie per ministerie

Wanneer wordt gekeken naar de verschillende ministeries – inclusief de instanties die onder hun beleidsverantwoordelijkheid vallen – dan vallen de ministeries van Infrastructuur en Waterstaat (36%), Landbouw, Natuur en Voedselkwaliteit en Economische Zaken en Klimaat (beide 47%), en Justitie en Veiligheid en Onderwijs, Cultuur en Wetenschap (beide 53%) in negatieve zin op.



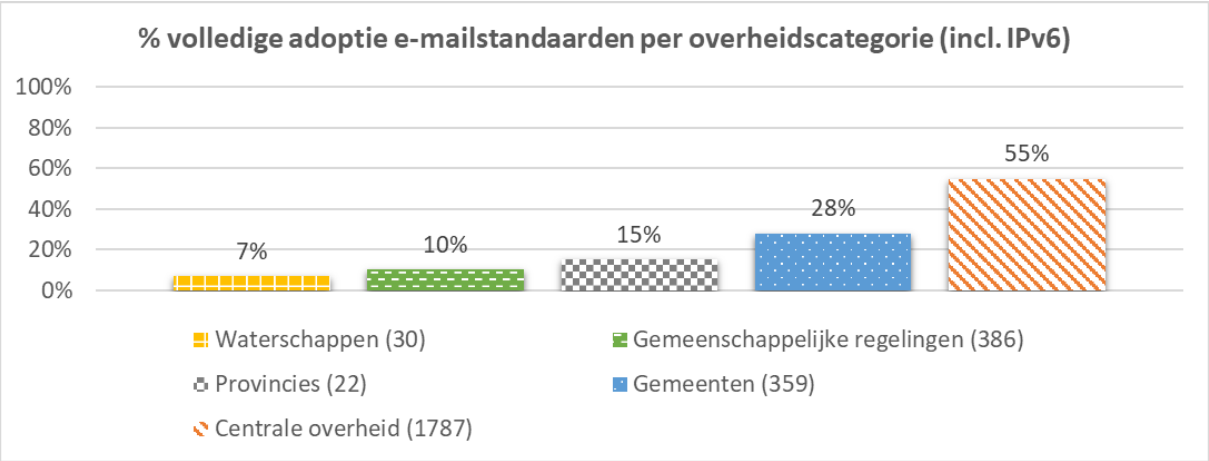
Voor meer details per ministerie zie hoofdstuk 6.

1.3. E-mailstandaarden

1.3.1. Totaalbeeld e-mail per overheidscategorie (incl. IPv6)

Onderstaande cijfers laten zien in welke mate de verschillende overheidscategorieën *alle* afgesproken websitestandaarden voor veilig en modern e-mailverkeer (inclusief IPv6)

toepassen. De centrale overheid loopt voorop in de toepassing van deze standaarden. Dat komt met name door een hoge mate van gebruik van gemeenschappelijke dienstverleners die de standaarden correct toepassen. Lokale overheden lopen achter, enerzijds komt dit door een hogere mate van gebruik van clouddiensten die niet alle standaarden ondersteunen. Anderzijds zal bij gemeenschappelijke regelingen het gebrek aan bewustzijn een rol spelen.



Hoofdstuk 3 gaat in meer detail in op de specifieke e-mailbeveiligingsstandaarden, hoofdstuk 4 gaat in op IPv6.

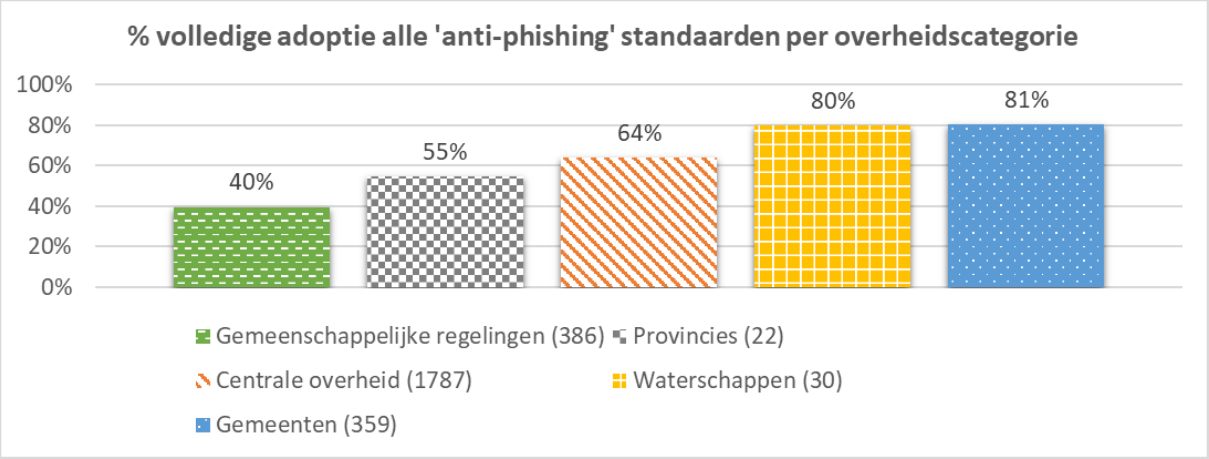
1.3.2. E-mailstandaarden voor bestrijding van phishing (excl. IPv6)

Door toepassing van e-mailstandaarden voor het bestrijden van phishing wordt e-mailverkeer met de overheid beter beveiligd, zodat criminelen niet zomaar overheidsdomeinen kunnen misbruiken als afzenddomein voor bijvoorbeeld phishing-aanvallen.

Deze paragraaf laat het totaalbeeld per overheidscategorie en het totaalbeeld per ministerie zien (zonder IPv6).

1.3.2.1. Adoptie per overheidscategorie

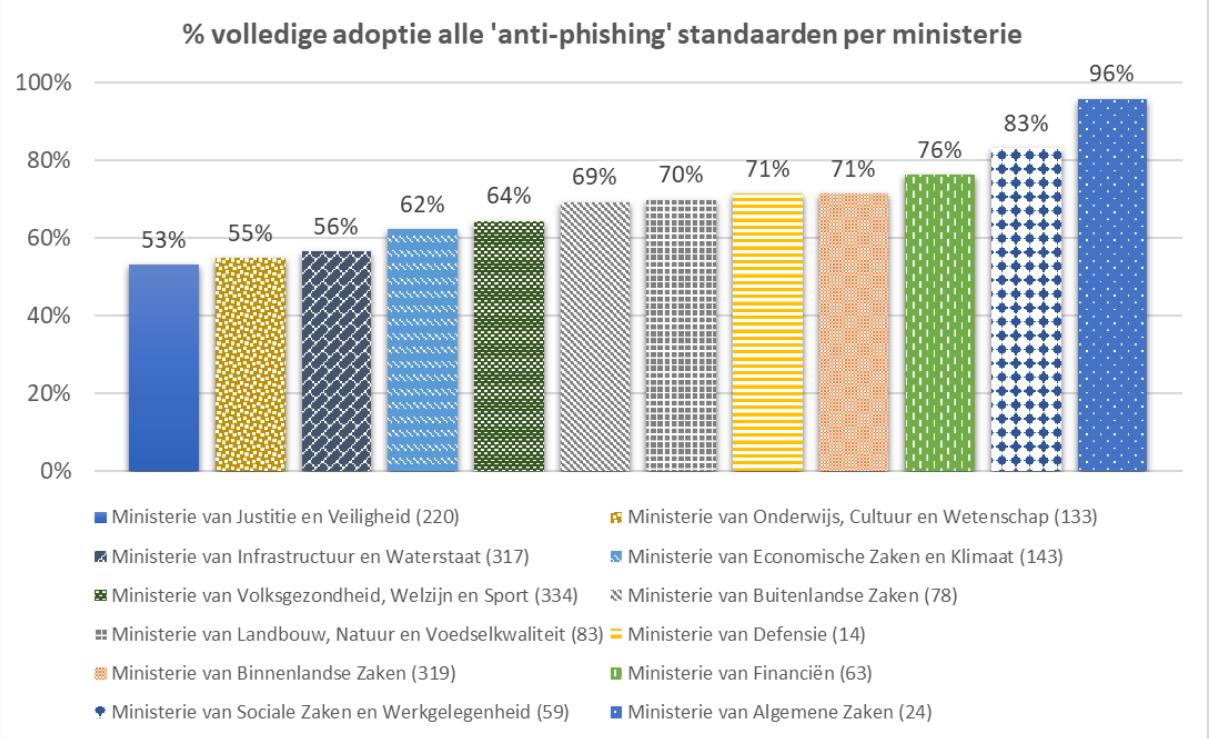
De waterschappen en gemeenten zijn positieve uitschieters in deze categorie. Wel gaat het bij deze categorieën voornamelijk om primaire domeinnamen. Er is geen inzicht in secundaire domeinnamen die in gebruik zijn, die waarschijnlijk gezamenlijk in de duizenden lopen. De gemeenschappelijke regelingen, waar lokale overheden vaak in participeren, scoren slecht met 40% goed geconfigureerde e-maildomeinen.



Voor meer details per overheidscategorie zie hoofdstuk 5.

1.3.2.2. Adoptie per ministerie

Wanneer wordt gekeken naar de verschillende ministeries – inclusief de instanties die onder hun beleidsverantwoordelijkheid vallen – dan vallen de ministeries van Algemene Zaken (96%) en Sociale Zaken en Werkgelegenheid (83%) positief op. Bijna alle ministeries met een portfolio kleiner dan 100 internetdomeinen scoren rond de 70% en hoger. Positieve opvaller met een portfolio groter dan 100 internetdomeinen is het ministerie van Binnenlandse Zaken met 71% volledige adoptie van anti-phishing standaarden voor haar portfolio van 319 gecontroleerde internetdomeinen. De ministeries van Justitie en Veiligheid (53%), Onderwijs, Cultuur en Wetenschap (55%), en Infrastructuur en Waterstaat (56%), hebben nog veel werk te verzetten om e-mailvervalsing namens haar domeinnamen te voorkomen.



Voor meer details per ministerie zie hoofdstuk 6.

1.3.3. E-mailstandaarden voor vertrouwelijk e-mailverkeer (excl. IPv6)

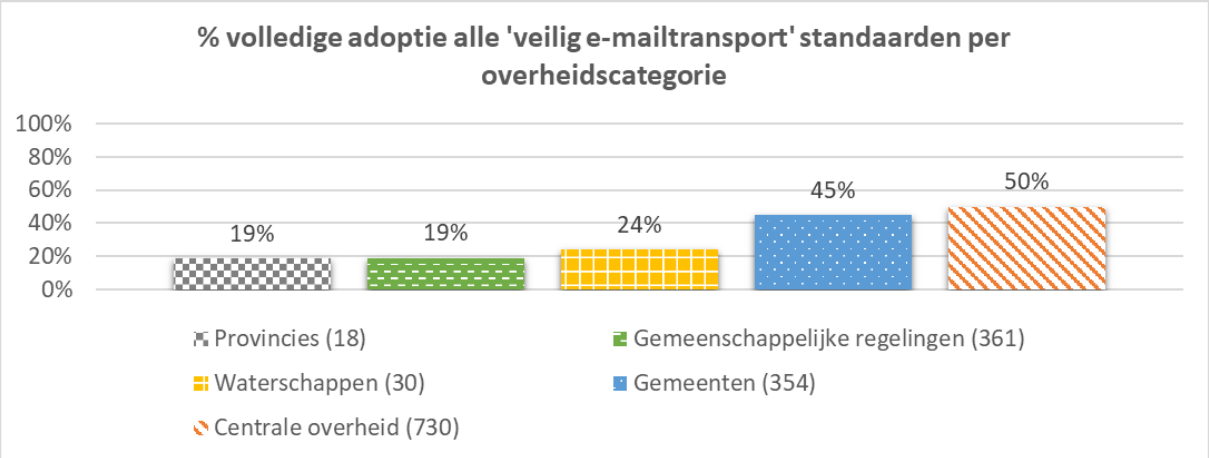
Door toepassing van e-mailstandaarden voor vertrouwelijk e-mailverkeer wordt e-mailverkeer met de overheid beter beveiligd, zodat criminelen niet zomaar e-mails kunnen onderscheppen of manipuleren.

Omdat we alleen kunnen testen of de e-mailontvangst van de betreffende overheden voldoende veilig e-mailverkeer mogelijk maakt, hebben we internetdomeinen zonder een ontvangende mailserver niet meegenomen in de statistieken. Hierdoor is het aantal gecontroleerde domeinen minder dan bij de standaarden voor bestrijding van phishing.

Deze paragraaf laat het totaalbeeld per overheidscategorie en het totaalbeeld per ministerie zien (zonder IPv6).

1.3.3.1. Adoptie per overheidscategorie

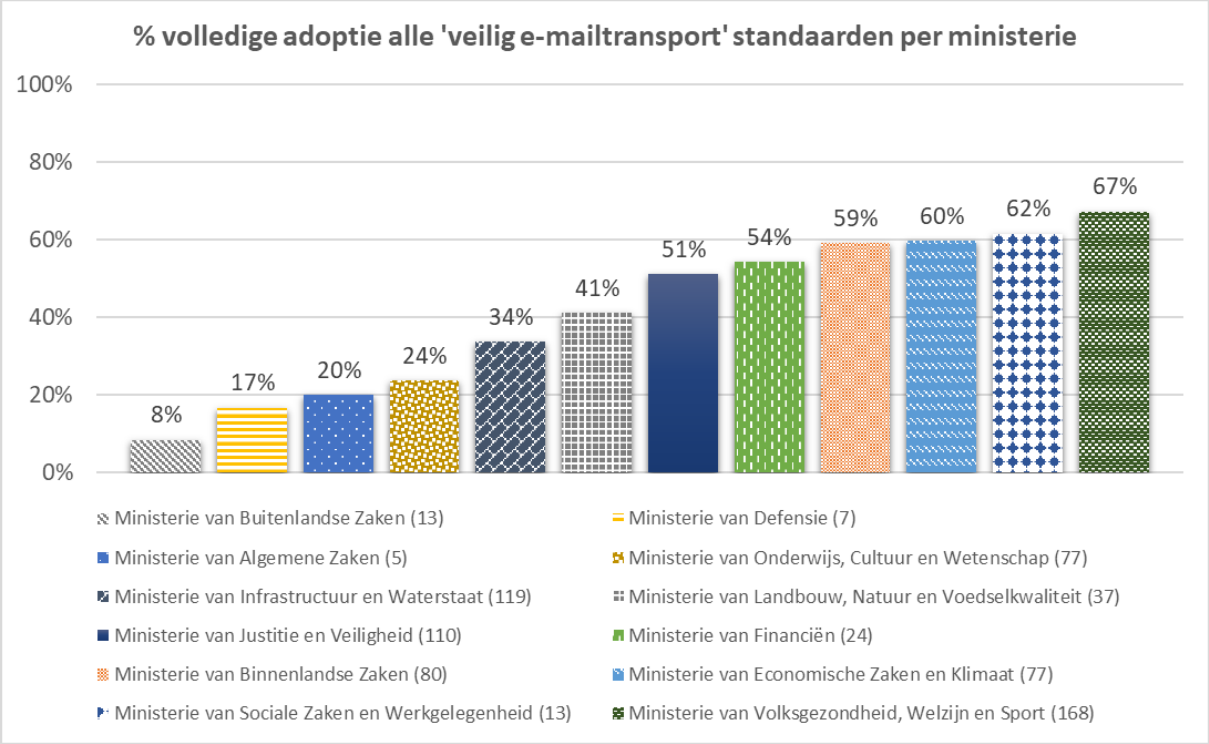
De centrale overheid en gemeenten scoren over het algemeen het beste op deze standaarden. Het gebruik van gemeenschappelijke e-maildienstverleners geeft daarbij een hefboomeffect. Lokale overheden maken veel meer gebruik van clouddiensten voor e-mailverkeer, die de standaarden DNSSEC en DANE over het algemeen niet ondersteunen. Dit is met name zichtbaar in de adoptiegraad bij provincies, gemeenschappelijke regelingen en waterschappen.



Voor meer details per overheidscategorie zie hoofdstuk 5.

1.3.3.2. Adoptie per ministerie

Wanneer wordt gekeken naar de verschillende ministeries – inclusief de instanties die onder hun beleidsverantwoordelijkheid vallen – dan valt op dat ministeries die actief sturen op toepassing van standaarden beter scoren, zoals de ministeries van Volksgezondheid, Welzijn en Sport, Sociale Zaken en Werkgelegenheid en Binnenlandse Zaken en Koninkrijksrelaties. Ook het ministerie van Economische Zaken en Klimaat scoort relatief hoger, omdat de meeste e-mail door de huisleverancier wordt verzorgd. Het ministerie van Buitenlandse Zaken is een negatieve opvaller met slechts 8% volledige adoptie van standaarden voor veilig e-mailtransport.



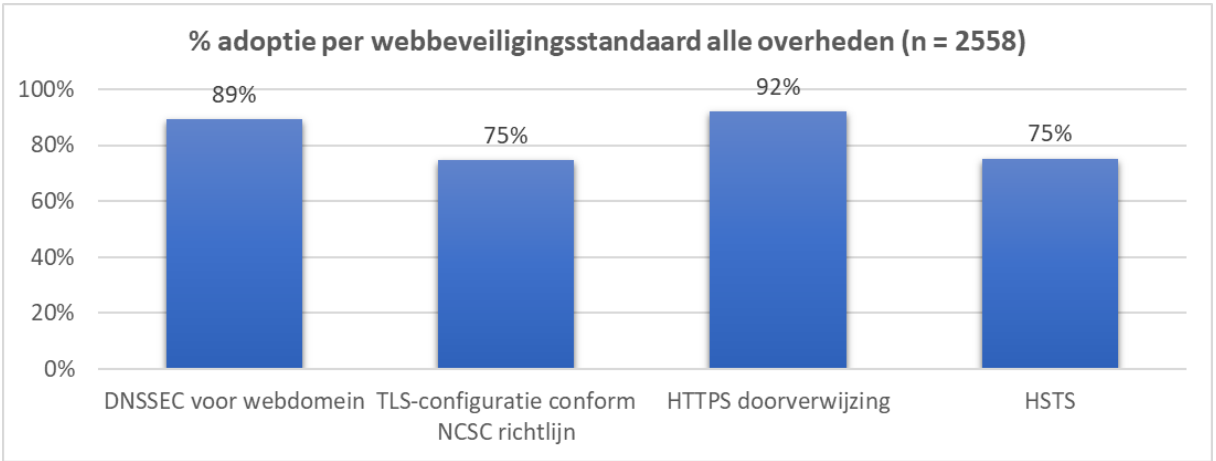
Voor meer details per ministerie zie hoofdstuk 6.

2. Adoptie per websitebeveiligingsstandaard

Dit hoofdstuk toont de algehele adoptiegraad per websitebeveiligingsstandaard.

Hoofdstukken 5 en 6 gaan in meer detail in op de adoptiegraad van specifieke standaarden per respectievelijk overheidscategorie en ministerie.

Onderstaande statistieken tonen onder meer aan dat bij een kwart van de internetdomeinen de TLS- en HSTS-configuraties niet op orde zijn. Overheden moeten HTTPS en HSTS toepassen conform de ICT-beveiligingsrichtlijnen voor webapplicaties, en configureren hun TLS-verbindingen conform de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) van het NCSC.

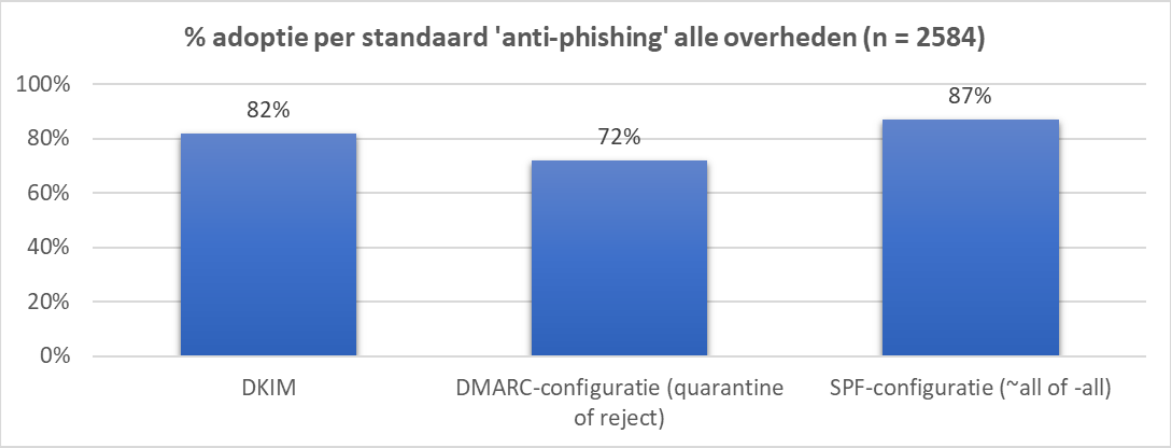


3. Adoptie per e-mailbeveiligingsstandaard

Dit hoofdstuk toont de algehele adoptiegraad per e-mailbeveiligingsstandaard. Hoofdstukken 5 en 6 gaan in meer detail in op de adoptiegraad van specifieke standaarden per respectievelijk overheidscategorie en ministerie.

3.1. E-mailstandaarden voor bestrijding van phishing

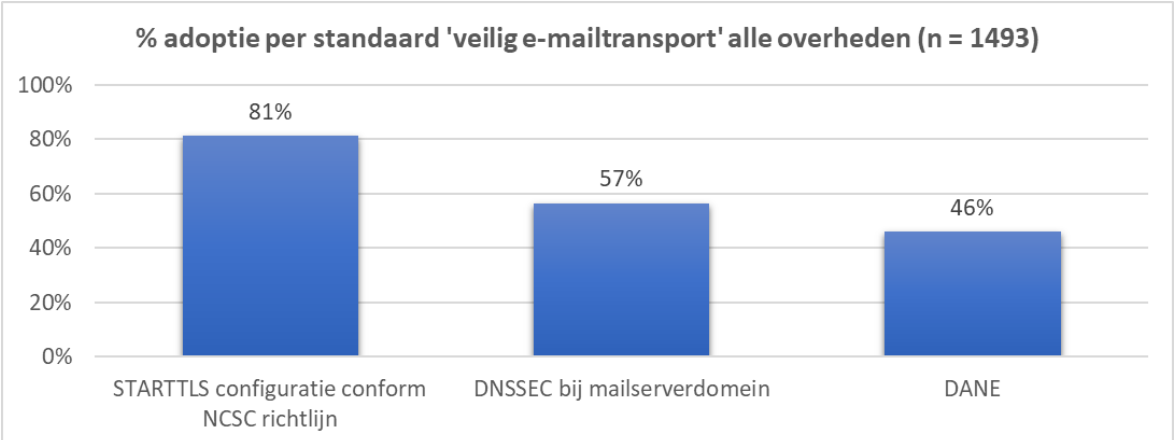
Om phishingmails uit naam van overheidsorganisaties (inclusief bewindspersonen) te voorkomen, moet voor 28% van de internetdomeinen nog een strikt DMARC-beleid worden ingesteld. Het streefbeeld was om dit eind 2019 voor elkaar te hebben.



3.2. E-mailstandaarden voor vertrouwelijk e-mailverkeer

Bij één op de vijf e-mailservers is de STARTTLS-configuratie niet toekomstvast geconfigureerd. Overheden dienen hun TLS-verbindingen te configureren op basis van de ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) van het NCSC.

DANE is de minst toegepaste standaard uit de meting met een adoptiegraad van 46%. DNSSEC bij mailserverdomein en DANE zorgen in samenhang voor geauthenticeerde versleuteling van e-mailtransport tussen de verzendende en ontvangende mailserver. Dit voorkomt dat een actieve aanvaller zomaar mailverkeer kan afluisteren.



De grootste implementatiedrempel voor DNSSEC en DANE is leveranciersondersteuning door met name clouddienstverleners. Het is belangrijk dat overheden die nog niet voldoen hun leverancier blijven vragen om ondersteuning van deze standaarden.

4. Adoptie IPv6 voor websites en e-mail

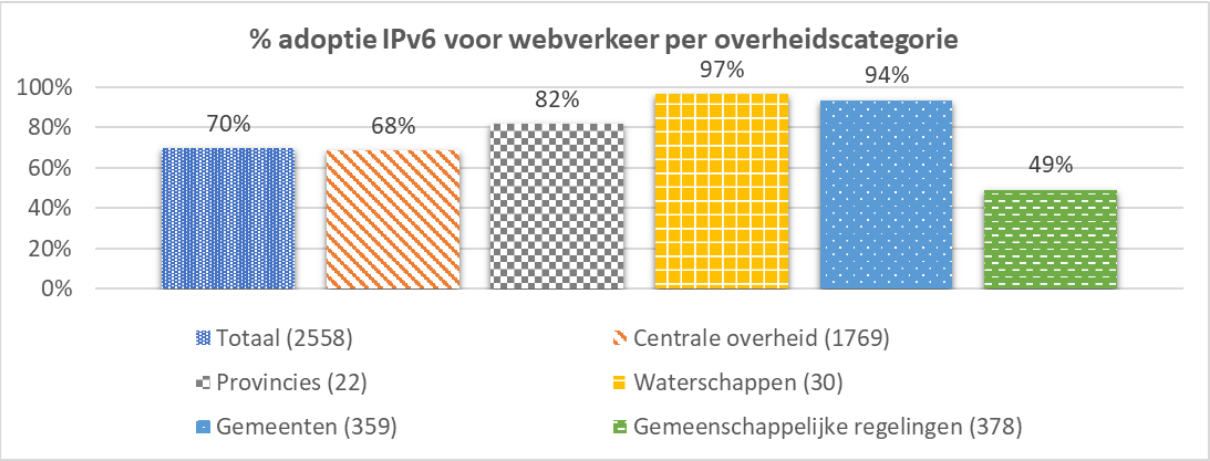
IPv6 is de open internetstandaard die iedere internetgebruiker nodig heeft om ook in de toekomst onbelemmerd gebruik te kunnen maken van internet. Er zijn verschillende goede redenen om voor IPv6 te kiezen, juist ook als overheid: groei en innovatie van internet, directere en snellere dienstverlening, en tegengaan van fraude.

De overheid heeft ook een voorbeeldfunctie om moderne internetstandaarden zoals IPv6 te gebruiken. Deze standaarden zorgen er namelijk voor dat het internet nu en in de toekomst voor iedereen wereldwijd veiliger en toegankelijker wordt waardoor ook nieuwe innovatie kan plaatsvinden. Brede ondersteuning van IPv6 binnen Nederland is ook belangrijk voor onze mondiale concurrentiepositie.

4.1. IPv6 voor webverkeer per overheidscategorie

De gemeenschappelijke regelingen scoren ver onder de maat bij het gebruik van IPv6 voor webverkeer. De overheidsbrede afspraken hebben onvoldoende doorwerking gehad naar deze instanties, ondanks dat zij meestal gefinancierd worden vanuit de andere overheden.

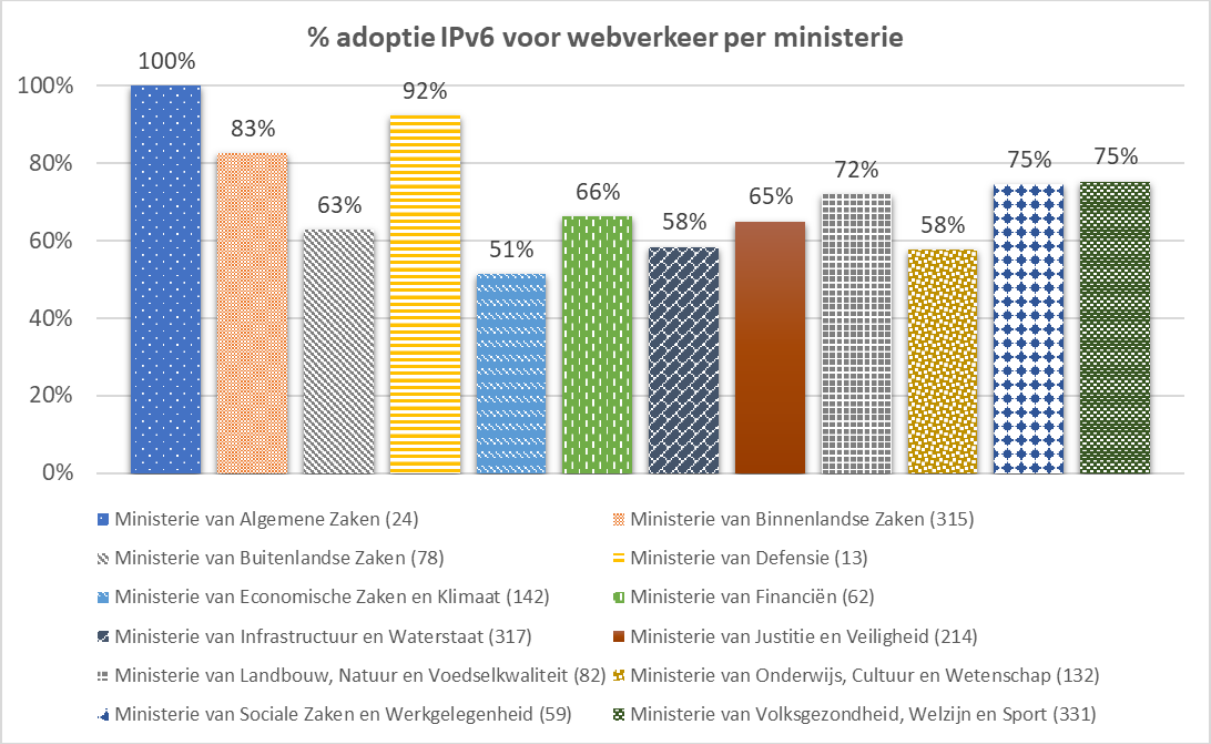
De centrale overheid scoort relatief lager dan de andere lokale overheden. Dat komt doordat er onevenredig veel secundaire webdomeinen in deze categorie zijn meegenomen. Deze secundaire webdomeinen zijn vaak gehost bij externe dienstverleners die niet goed aangestuurd zijn op het toepassen van IPv6 voor websites en webapplicaties.



4.2. IPv6 voor webverkeer per ministerie

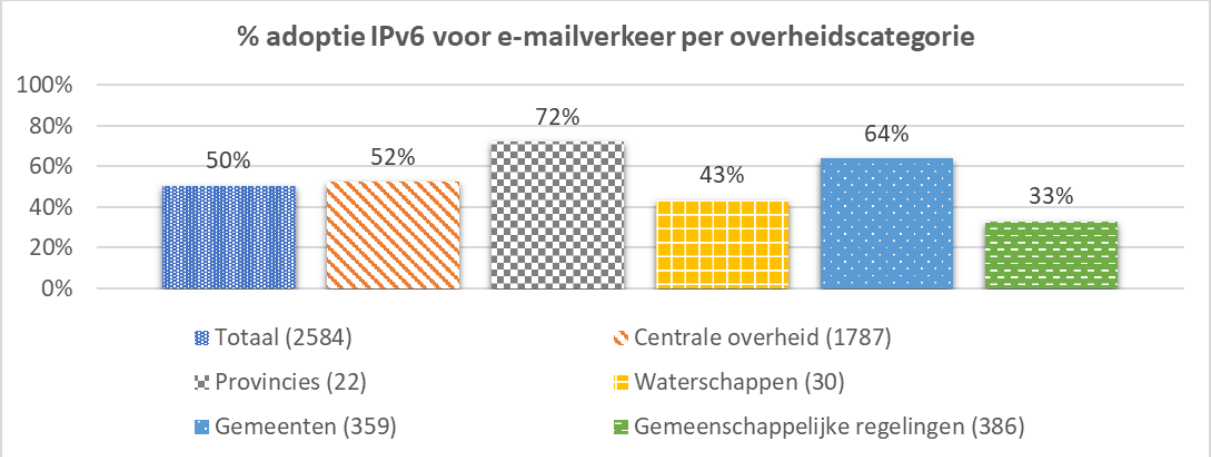
Positieve uitschieters – met een klein webportfolio – zijn de ministeries van Algemene Zaken (100%) en Defensie (92%). Negatieve opvaller is het ministerie van Economische Zaken (51%),

terwijl dit beleidsmatig de aanjager is van IPv6 richting het bedrijfsleven. Dit ministerie heeft nog een uitdaging om de voorbeeldfunctie waar te maken.



4.3. IPv6 voor e-mailverkeer per overheidscategorie

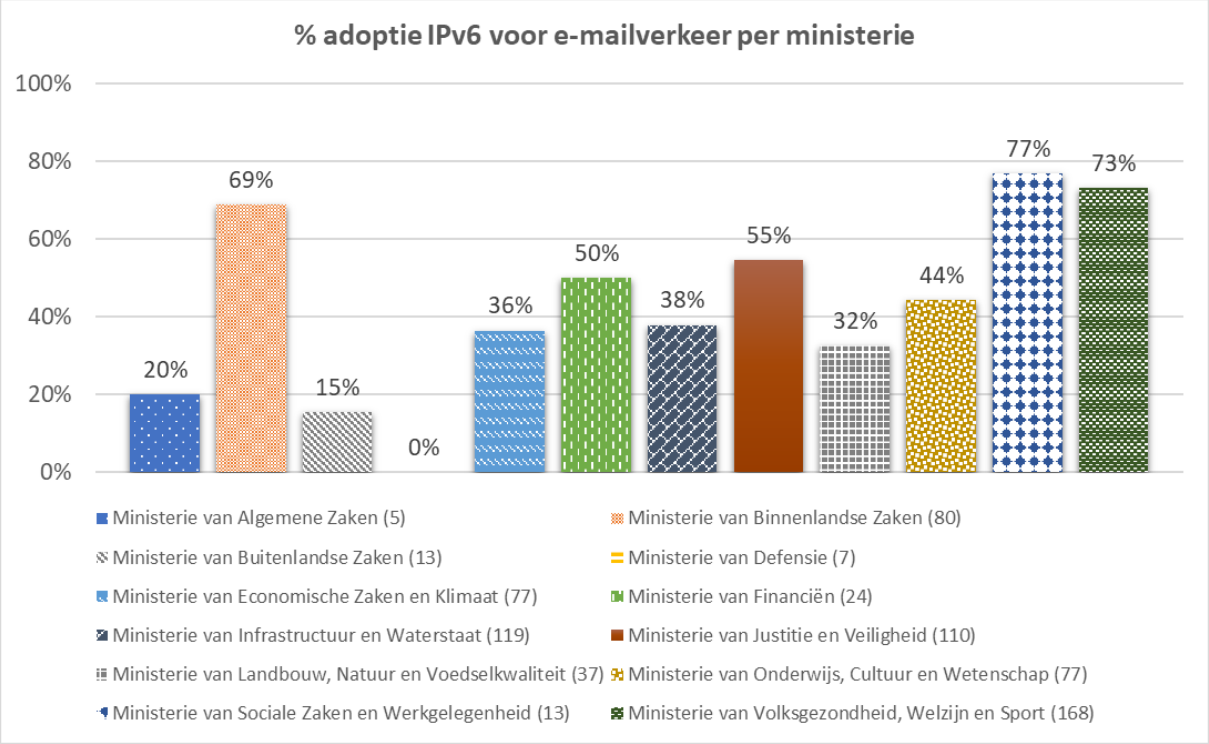
Ook bij het gebruik van IPv6 voor e-mailverkeer scoren de gemeenschappelijke regelingen ver onder de maat met een adoptiegraad van slechts 33%. Ook de waterschappen komen daar niet ver boven met 43%. Vermoedelijk zit er voor de centrale overheid (52%) nog rek in het adoptiepercentage door ongebruikte mailservers uit de domeinconfiguratie te verwijderen.



4.4. IPv6 voor e-mailverkeer per ministerie

Wanneer wordt gekeken naar de verschillende ministeries – inclusief de instanties die onder hun beleidsverantwoordelijkheid vallen – dan valt in eerste instantie het ministerie van Defensie op, die helemaal geen IPv6 e-mailverkeer mogelijk maakt. Ook de ministeries van Buitenlandse Zaken (15%) en Algemene Zaken (20%) hebben ondanks een klein portfolio aan ontvangen e-maildomeinen een erg lage adoptiegraad.

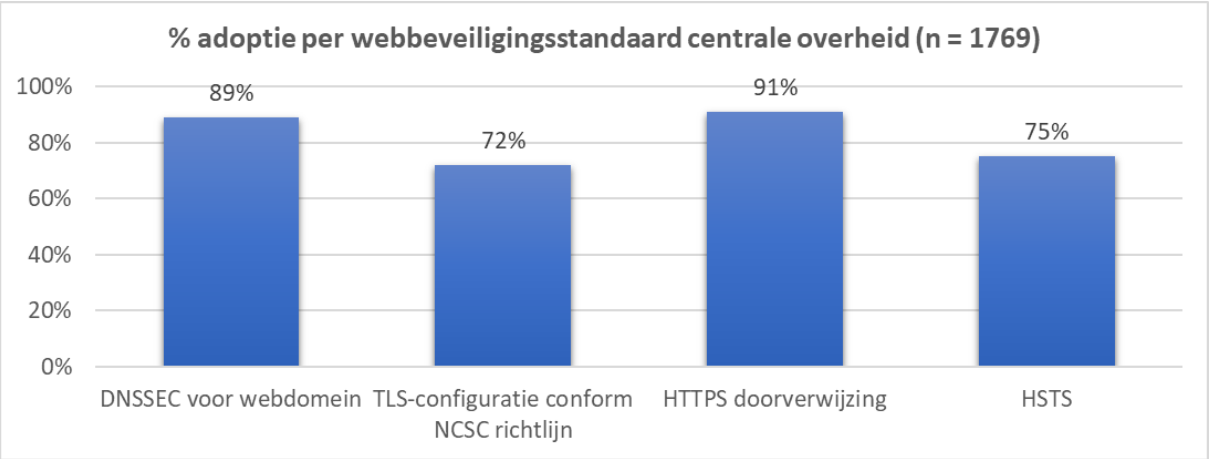
Positieve opvallers zijn de ministeries met een proactieve (projectmatige) sturing op toepassing van standaarden. Het gaat daarbij om de ministeries van Sociale Zaken en Werkgelegenheid (77%), Volksgezondheid, Welzijn en Sport (73%), en Binnenlandse Zaken en Koninkrijksrelaties (69%).

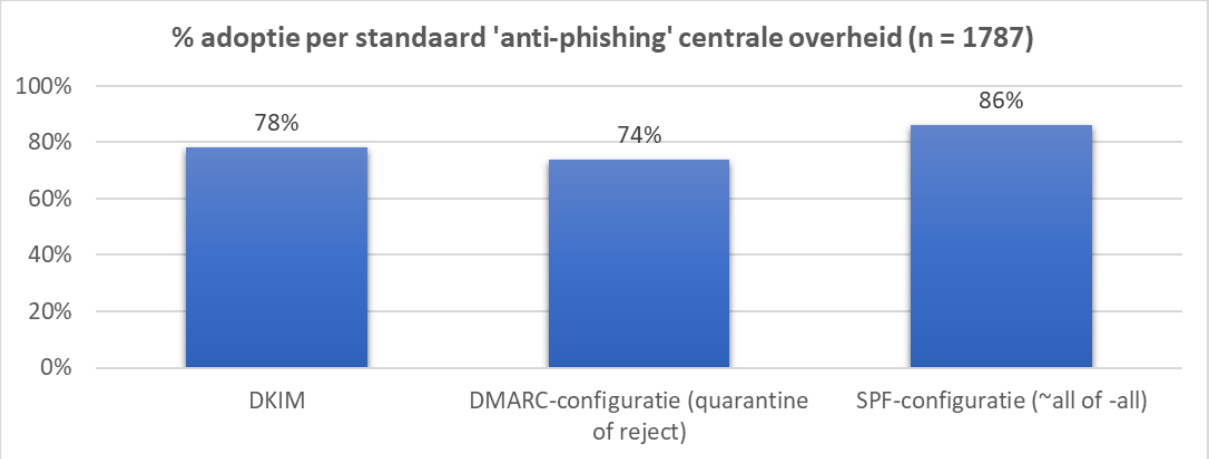


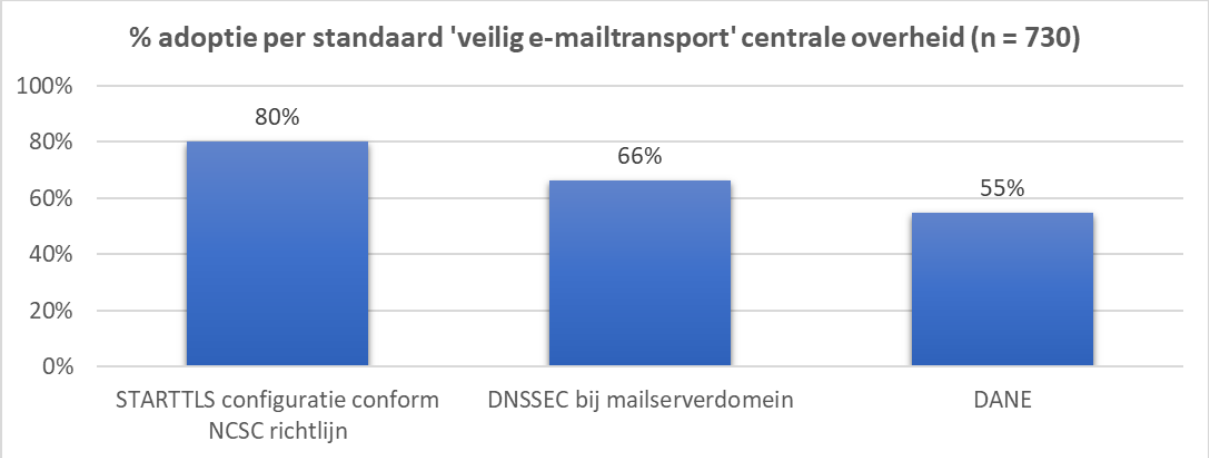
5. Adoptie per overheidscategorie

De volgende paragrafen tonen de adoptiestatistieken per beveiligingsstandaard per overheidscategorie.

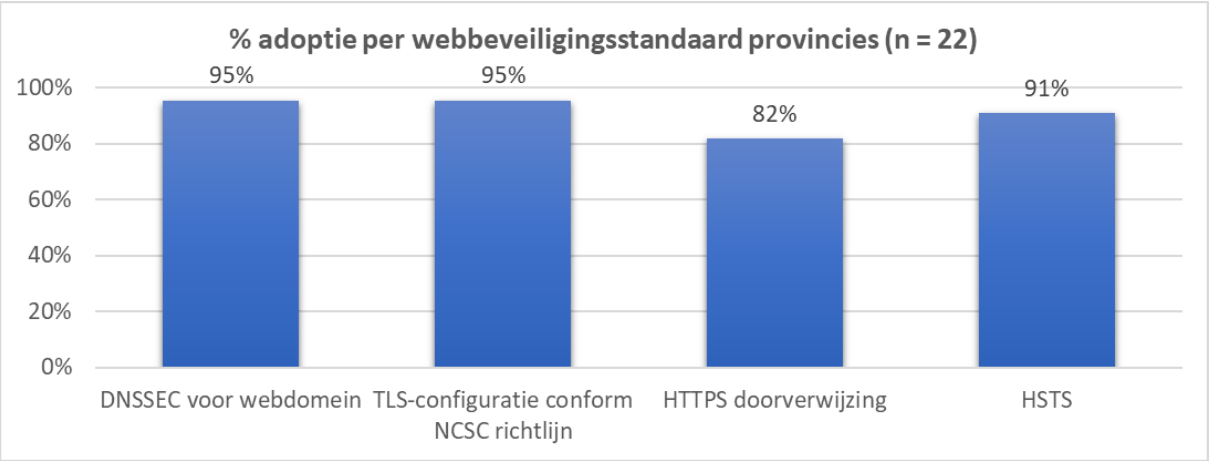
5.1. Centrale overheid

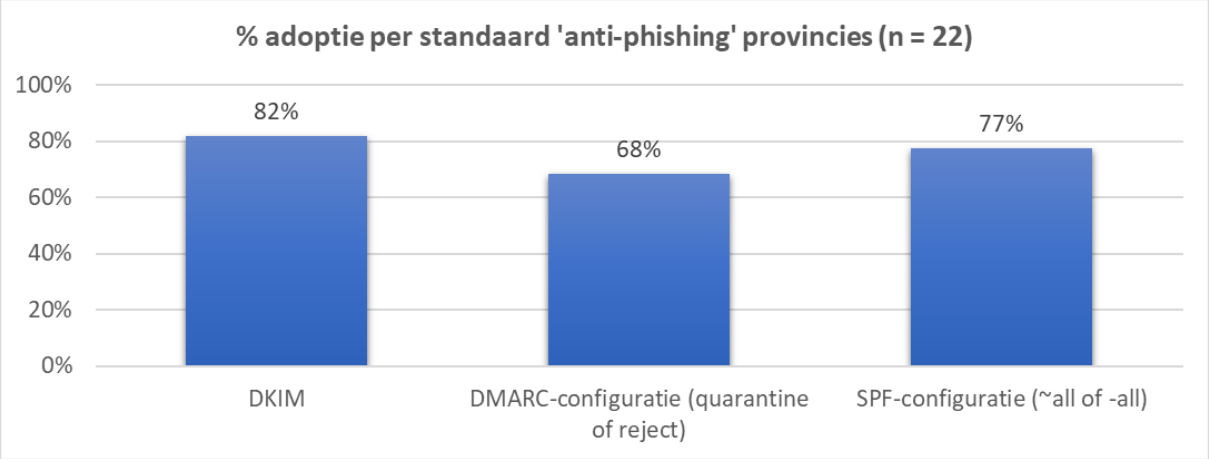


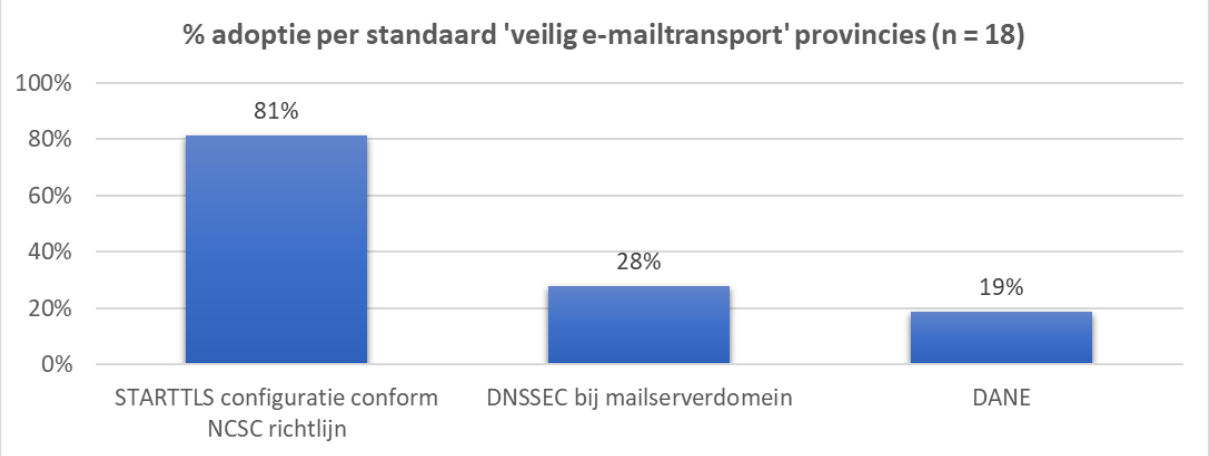




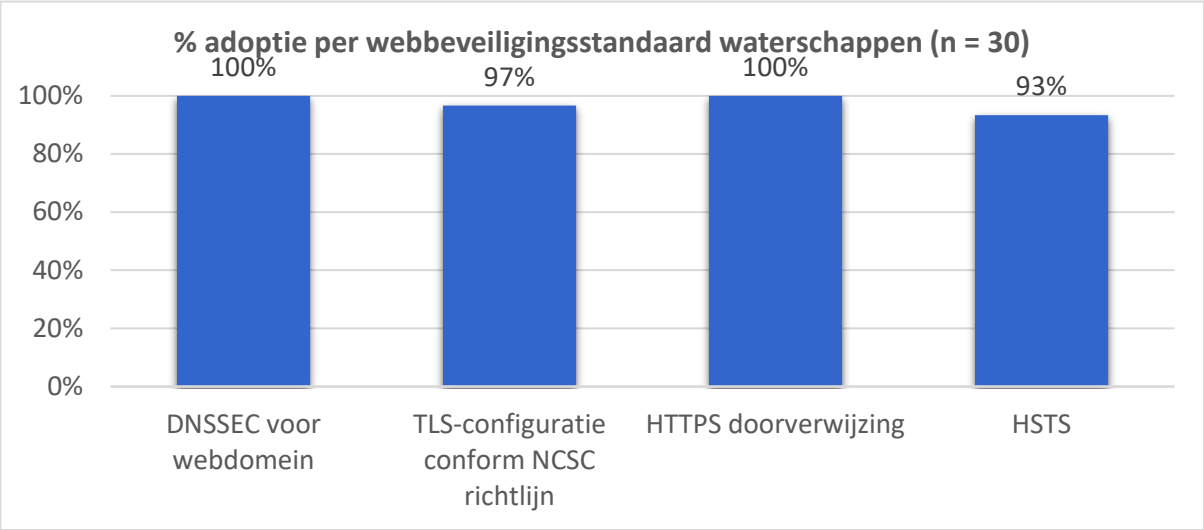
5.2. Provincies

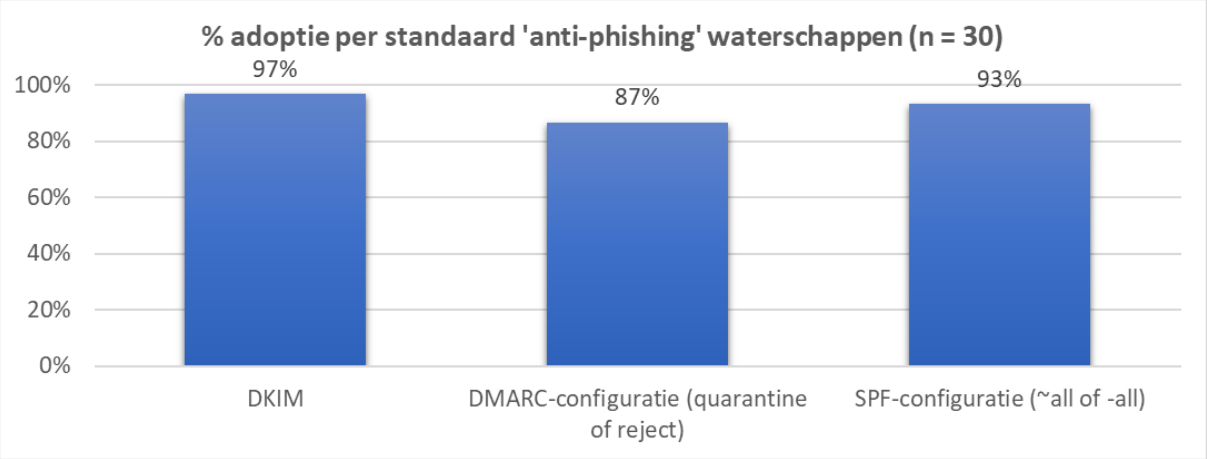


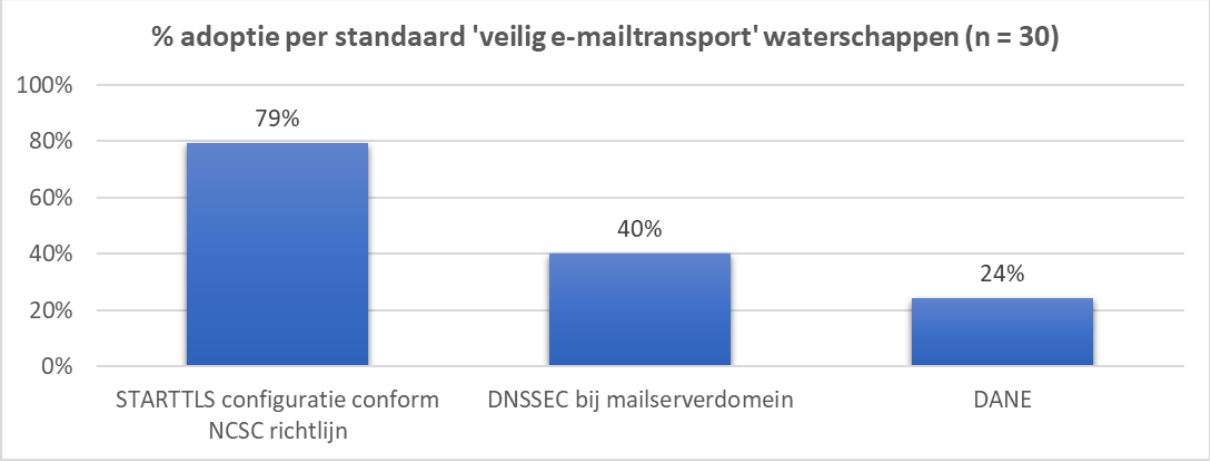




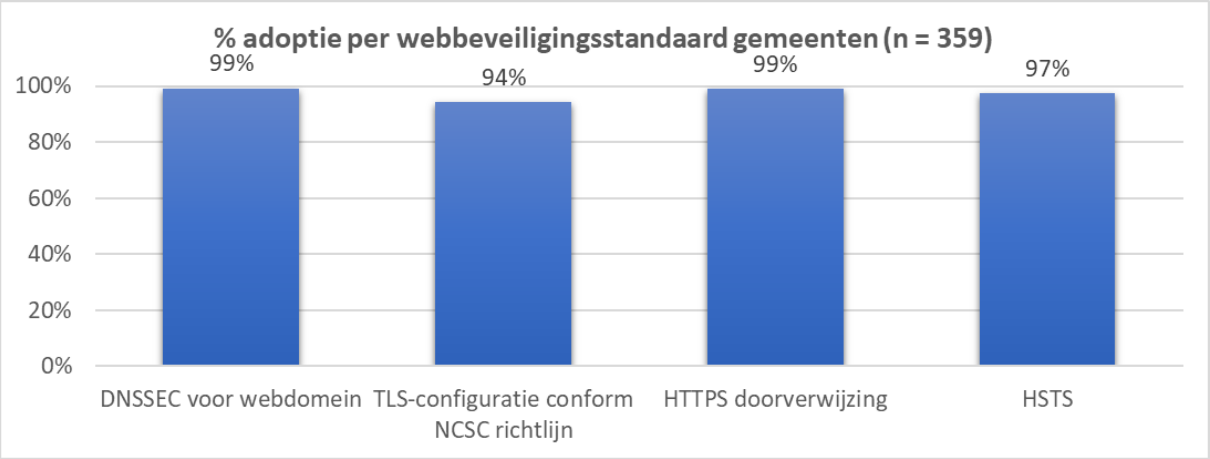
5.3. Waterschappen

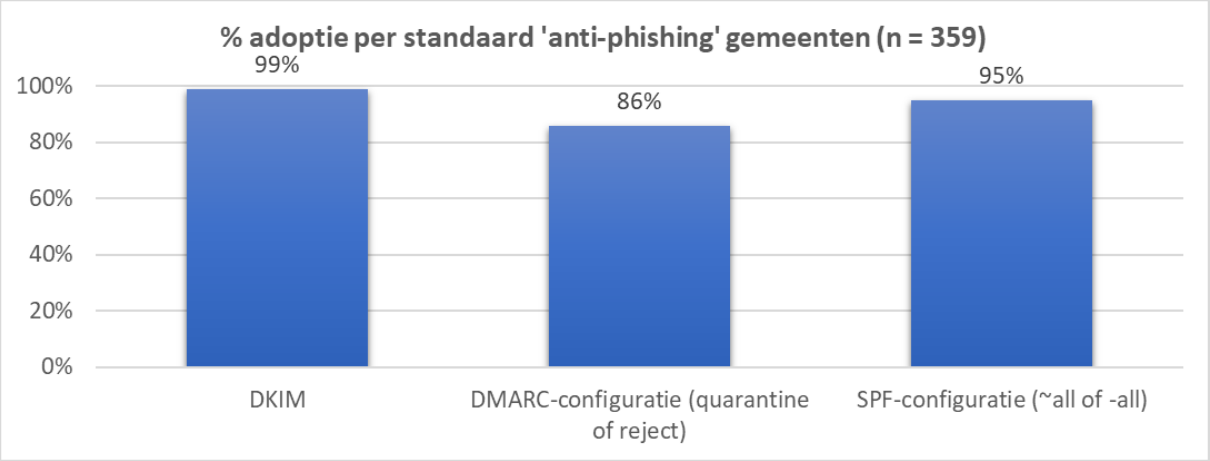


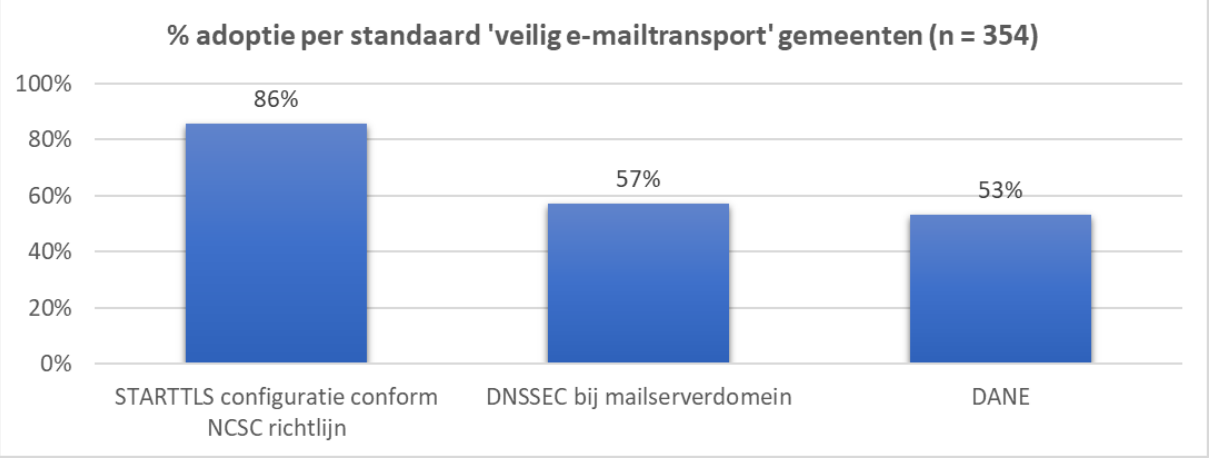




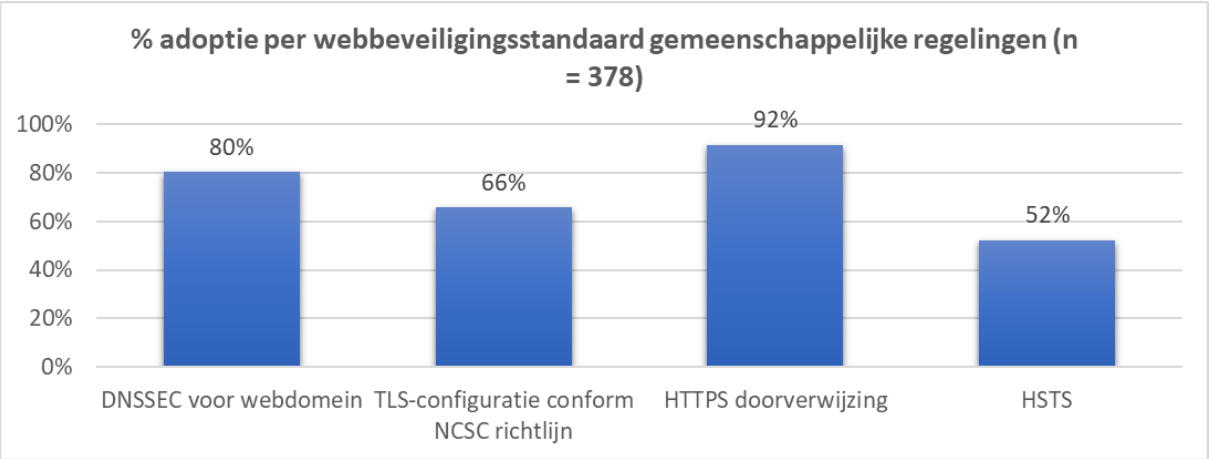
5.4. Gemeenten

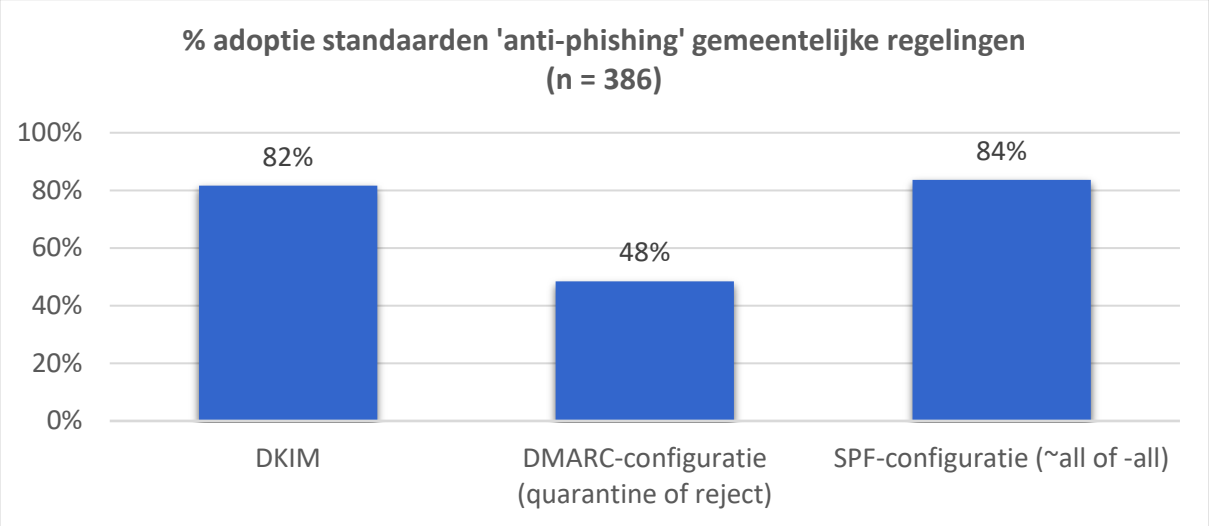


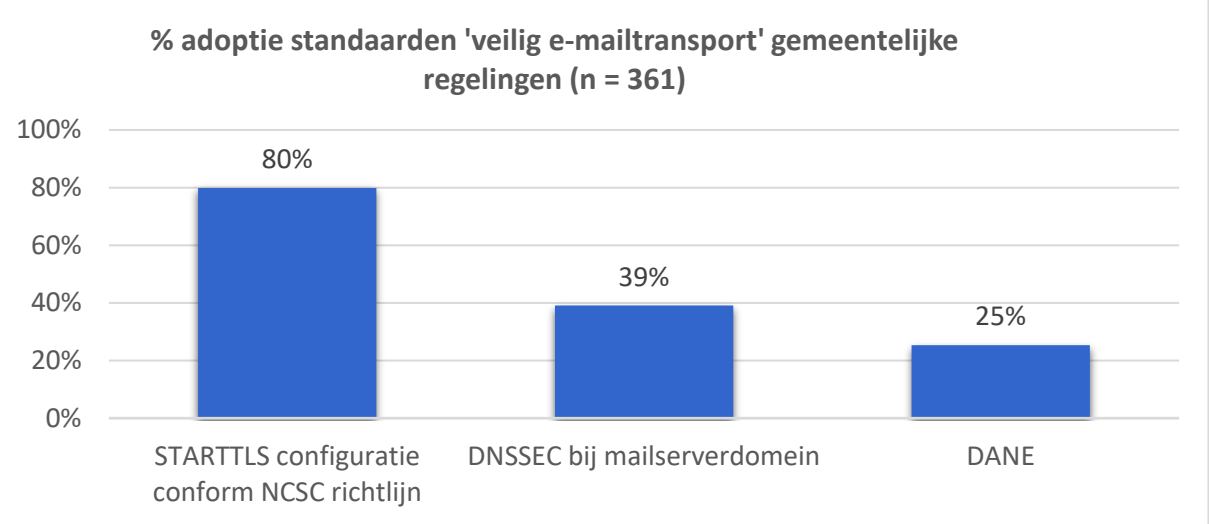




5.5. Gemeenschappelijke regelingen



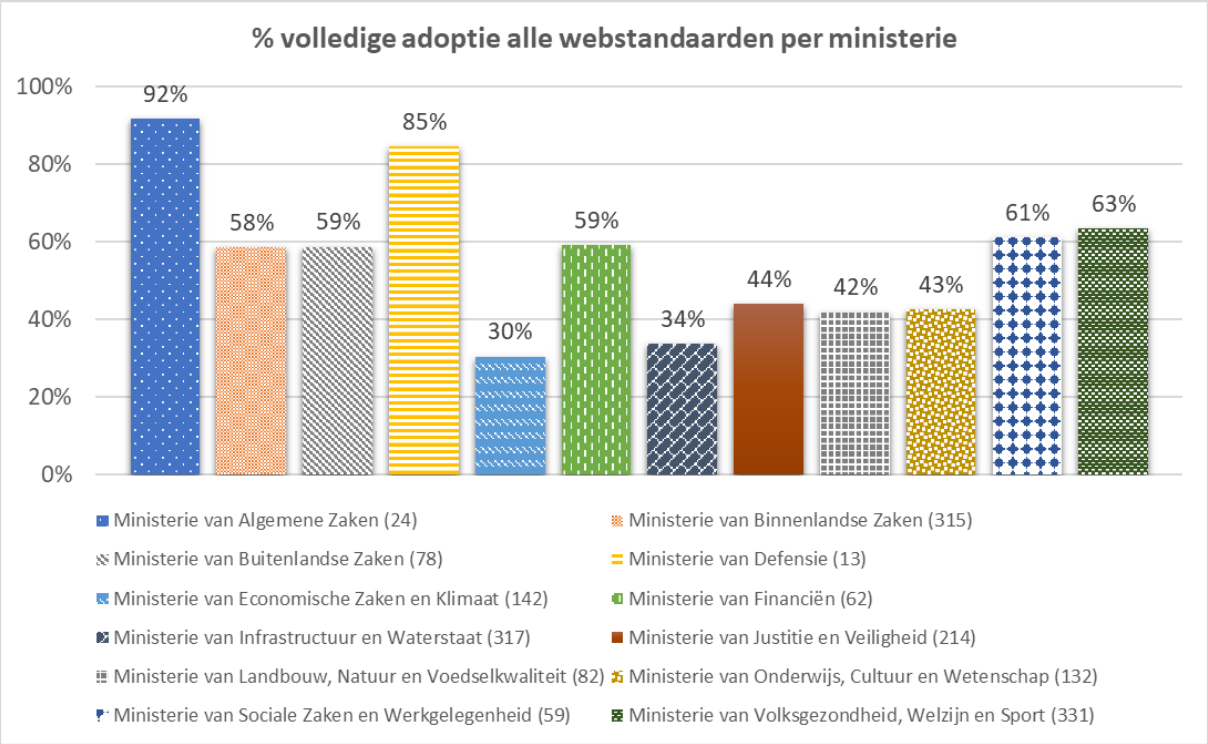




6. Adoptie per ministerie

6.1. Totaalbeeld websitestandaarden (incl. IPv6)

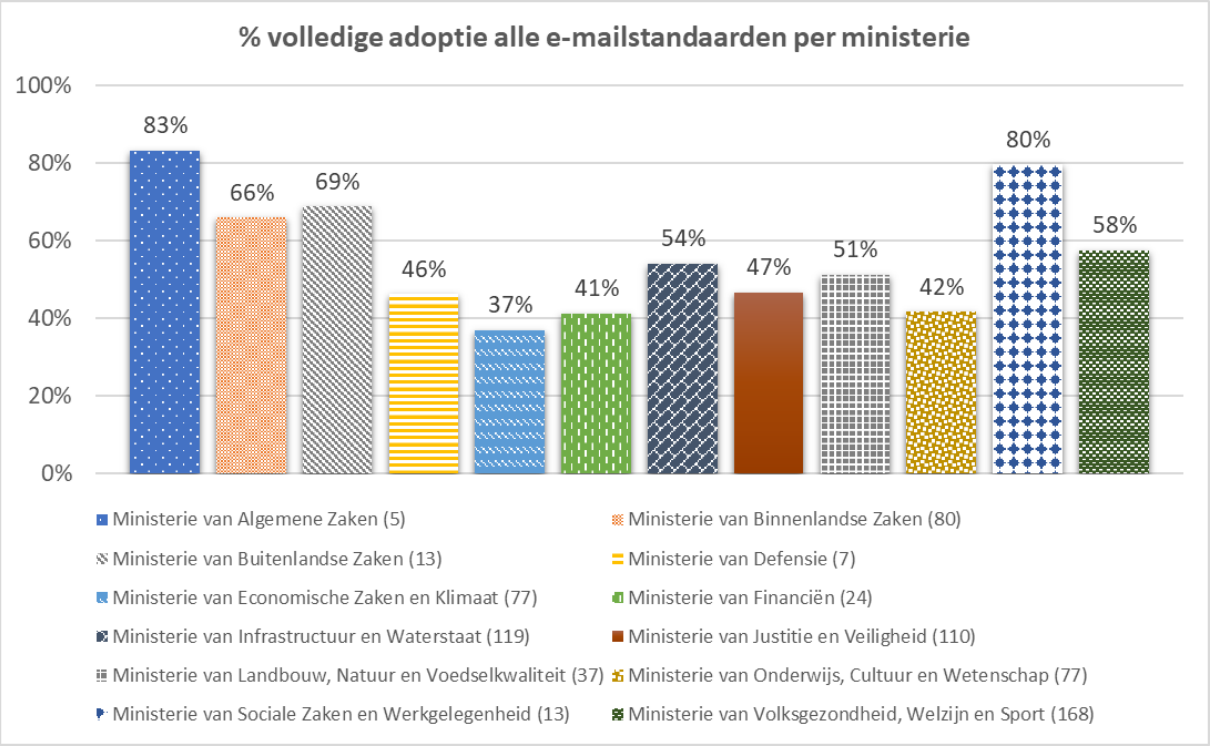
Onderstaande cijfers laten zien in welke mate de verschillende ministeries – inclusief de instanties die onder hun beleidsverantwoordelijkheid vallen – *alle* afgesproken websitestandaarden voor veilig en modern webverkeer toepassen (inclusief IPv6).



Over het algemeen hebben ministeries met een klein webportfolio, zoals de ministeries van Algemene Zaken en Defensie, een hoge mate van adoptie. Ook ministeries als Buitenlandse Zaken en Financiën, met een relatief beperkt portfolio, scoren hoger dan gemiddeld. De ministeries van Binnenlandse Zaken en Volksgezondheid hebben een relatief hoge adoptiegraad afgezet tegen de hoge omvang van hun portfolio. Dit komt omdat zij in de voorgaande jaren actief (projectmatig) hebben gestuurd op toepassing van standaarden.

6.2. Totaalbeeld e-mailstandaarden (incl. IPv6)

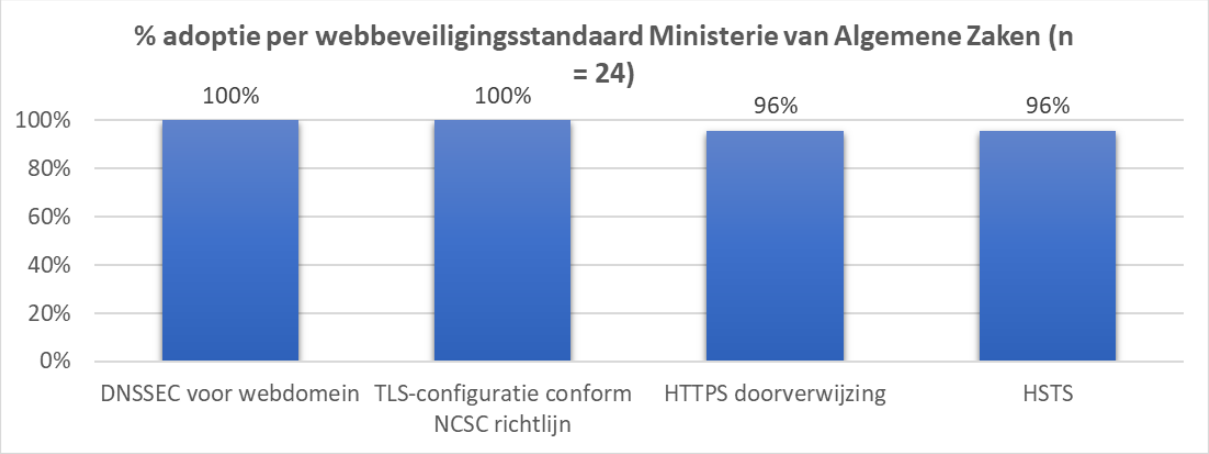
Onderstaande cijfers laten zien in welke mate de verschillende ministeries – inclusief de instanties die onder hun beleidsverantwoordelijkheid vallen – *alle* afgesproken e-mailstandaarden voor veilig en modern e-mailverkeer toepassen (inclusief IPv6).

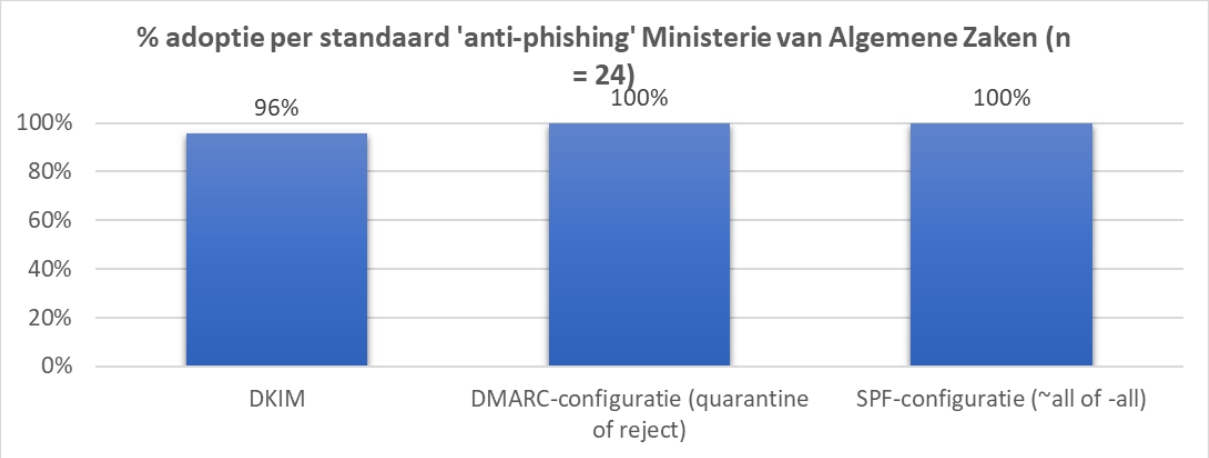


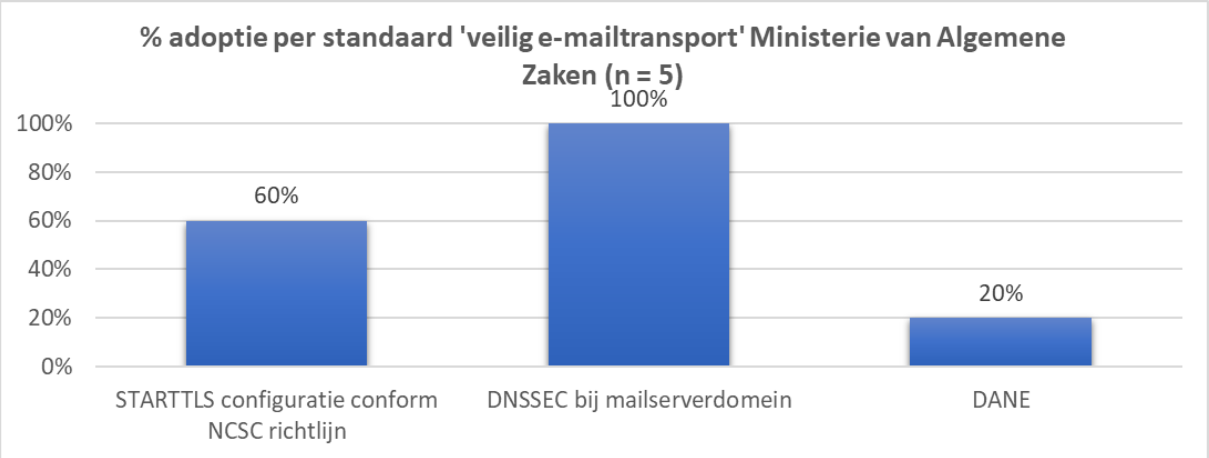
Vergelijkbaar met de adoptie van websitestandaarden, zien we dat ministeries met een beperkt portfolio, of actieve sturing op toepassing van standaarden, over het algemeen een hogere adoptiegraad bereiken.

De volgende paragrafen tonen de adoptiestatistieken per beveiligingsstandaard per ministerie.

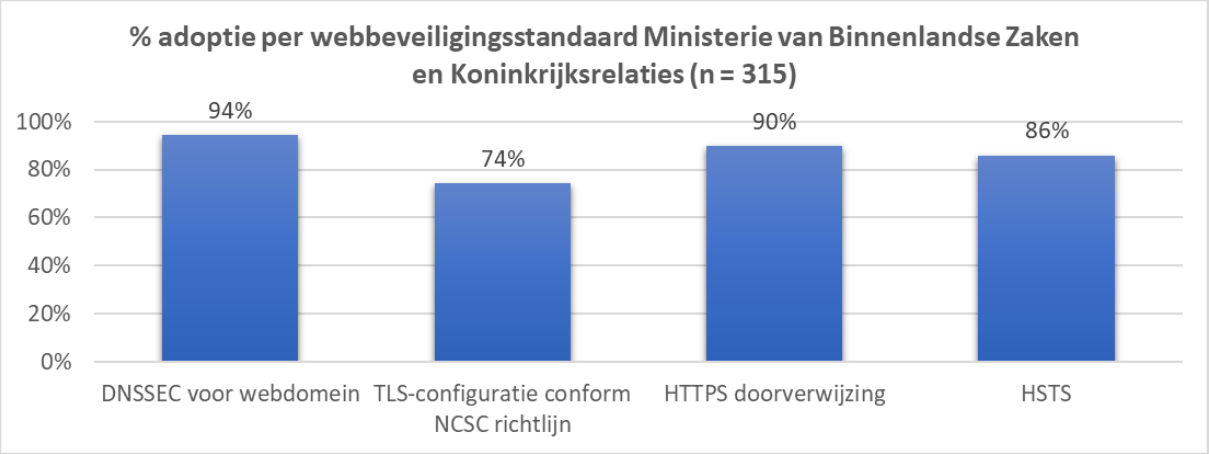
6.3. Ministerie van Algemene Zaken

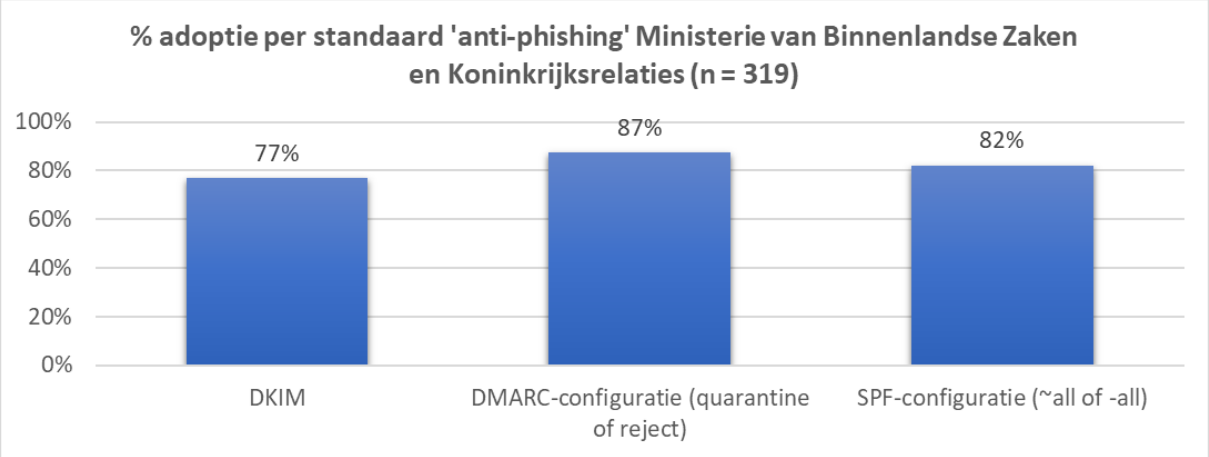


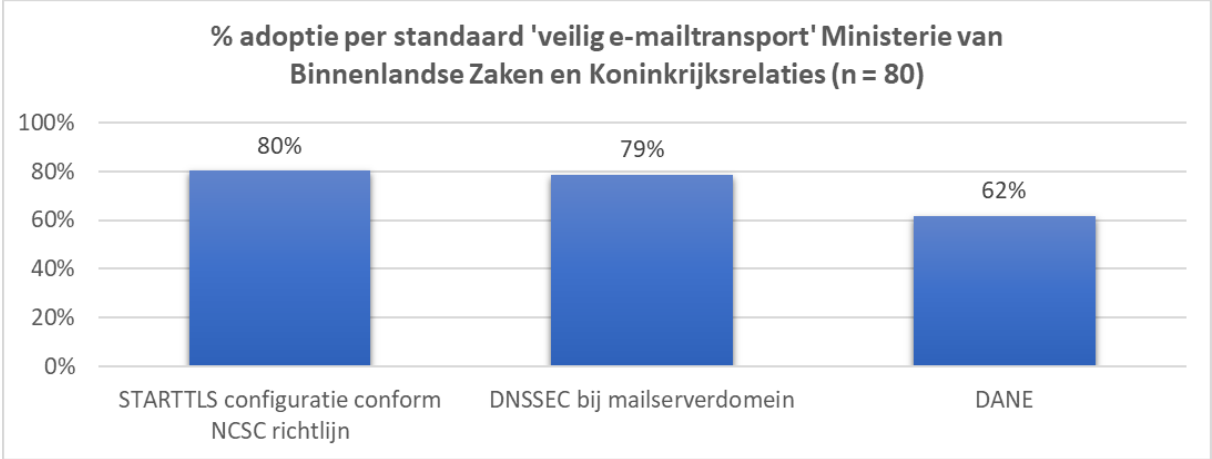




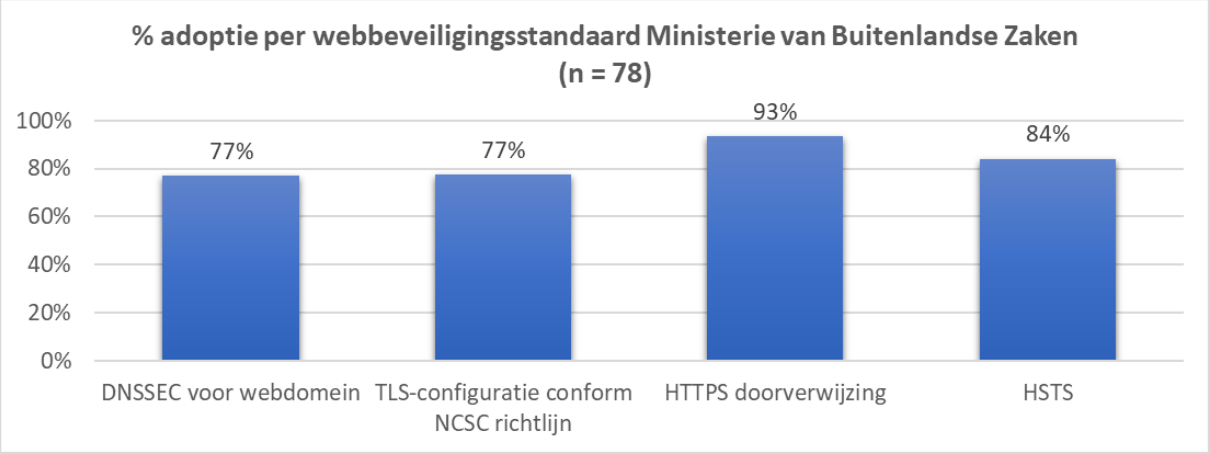
6.4. Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

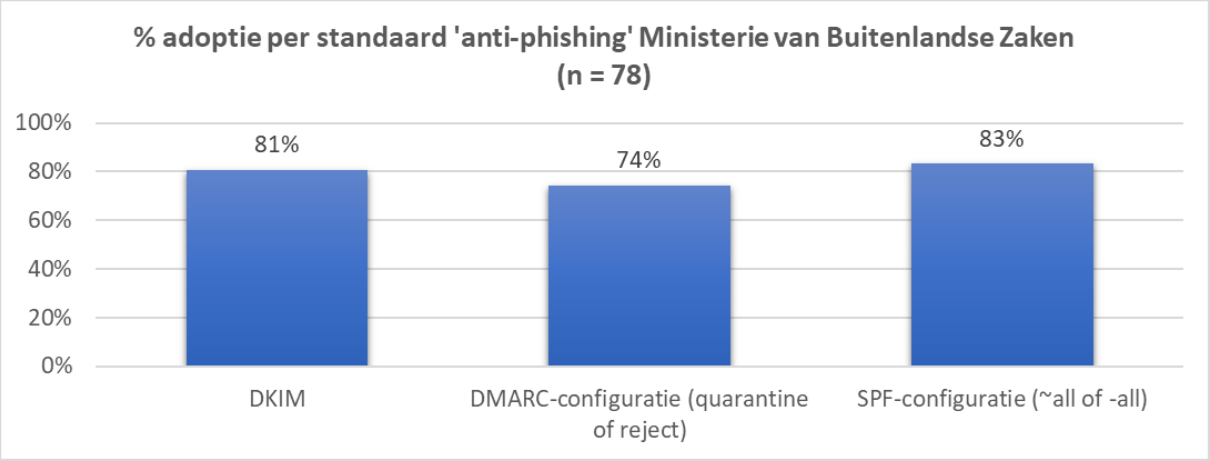


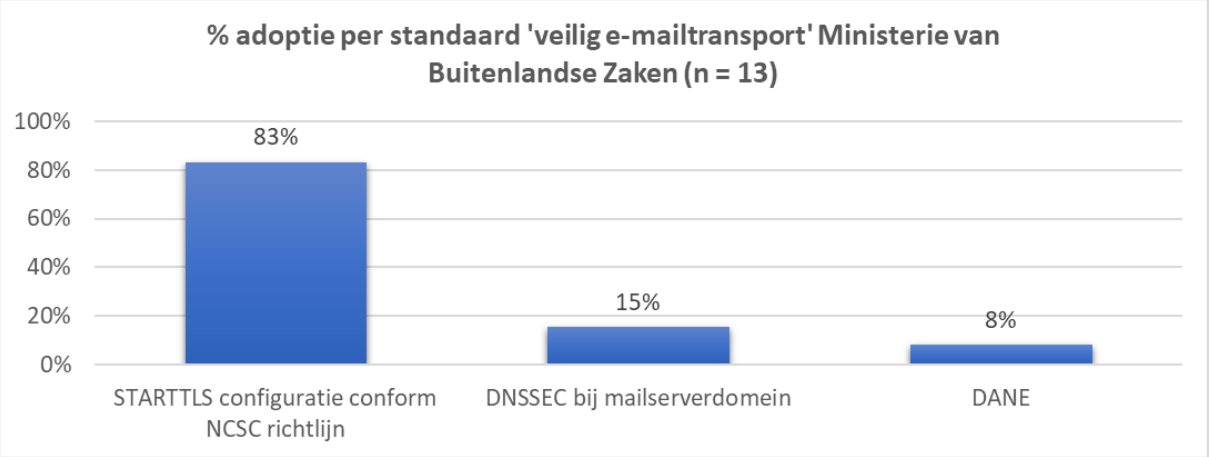




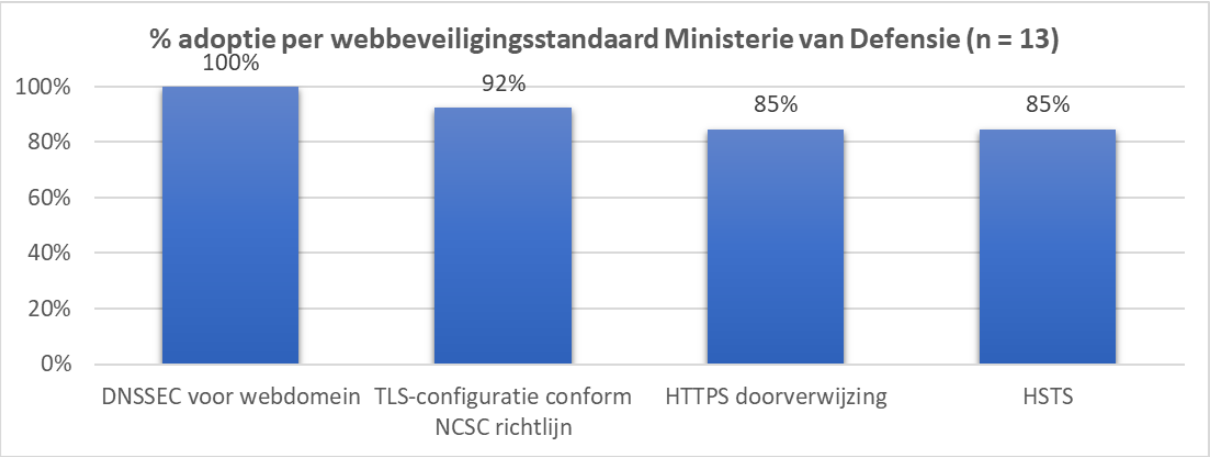
6.5. Ministerie van Buitenlandse Zaken

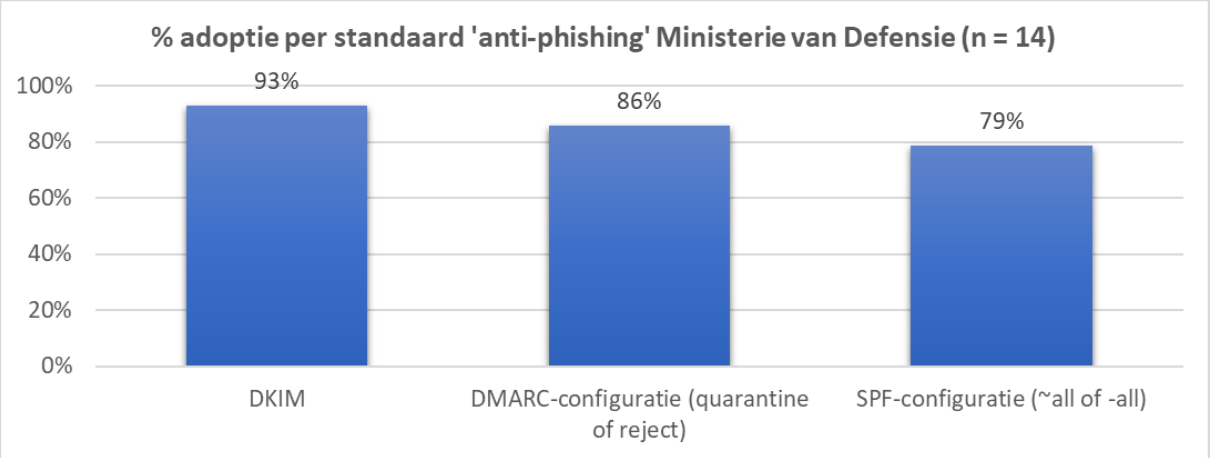


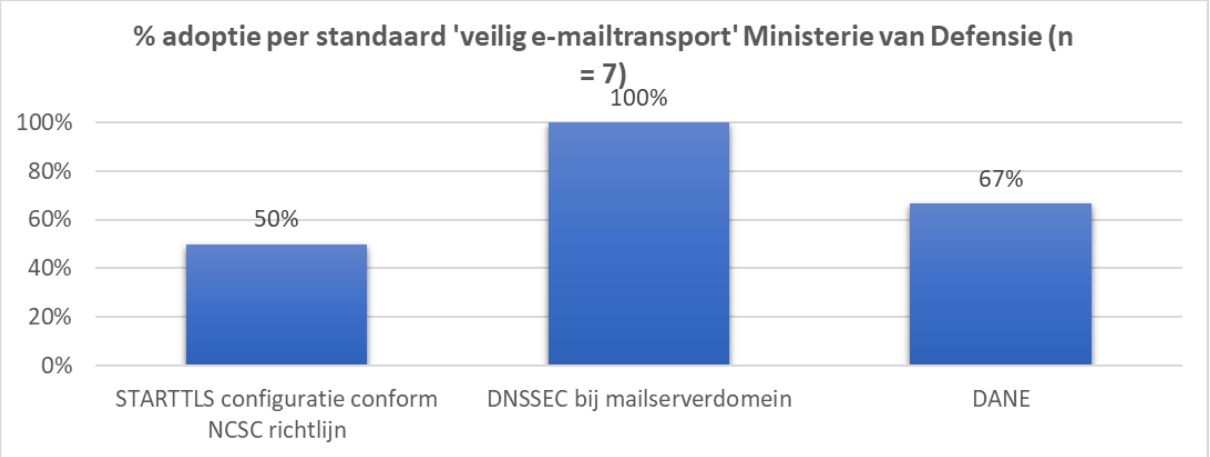




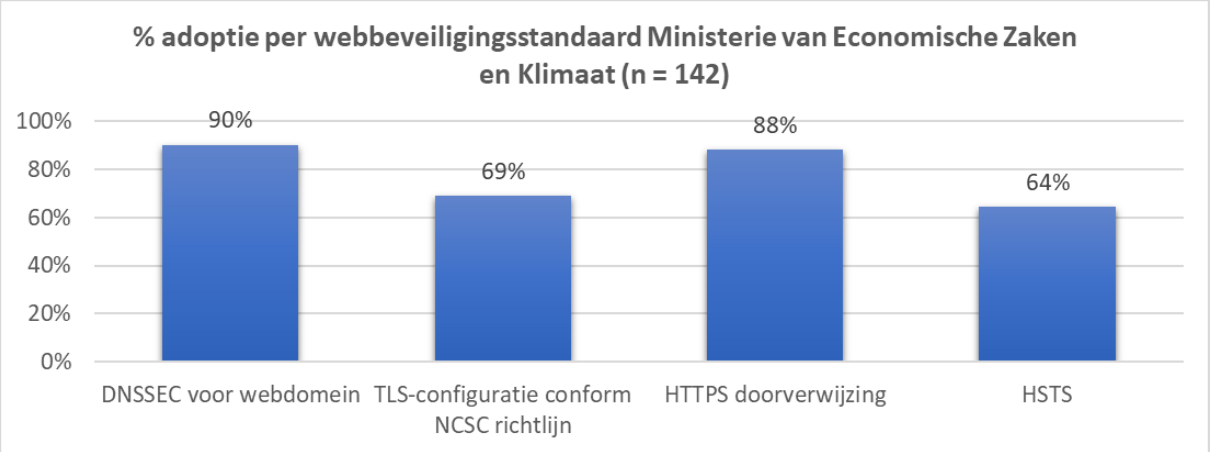
6.6. Ministerie van Defensie

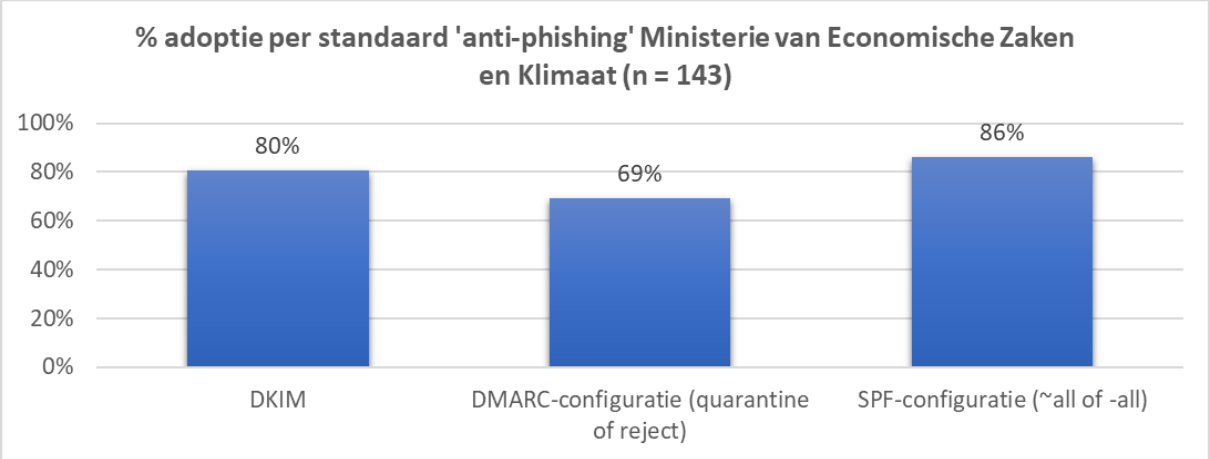


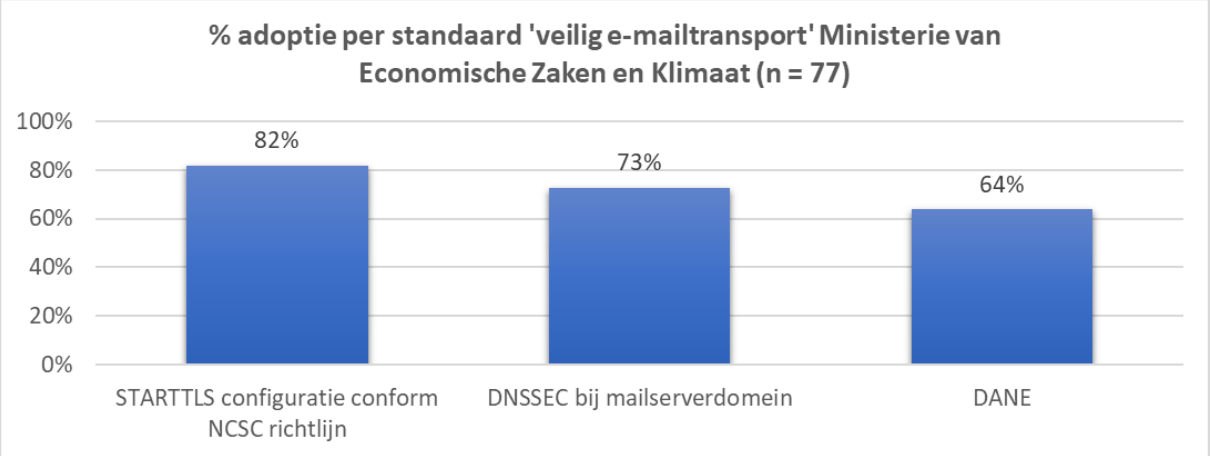




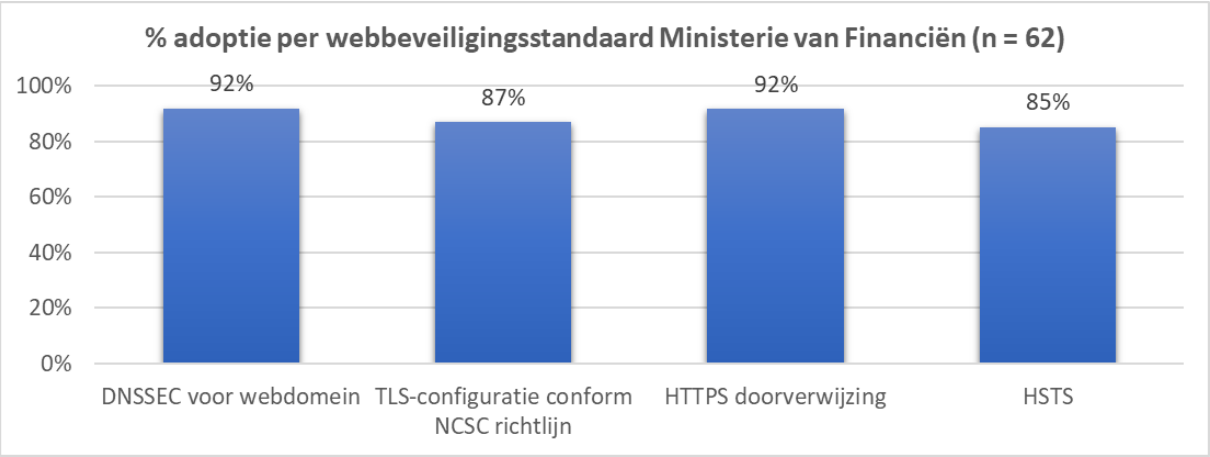
6.7. Ministerie van Economische Zaken en Klimaat

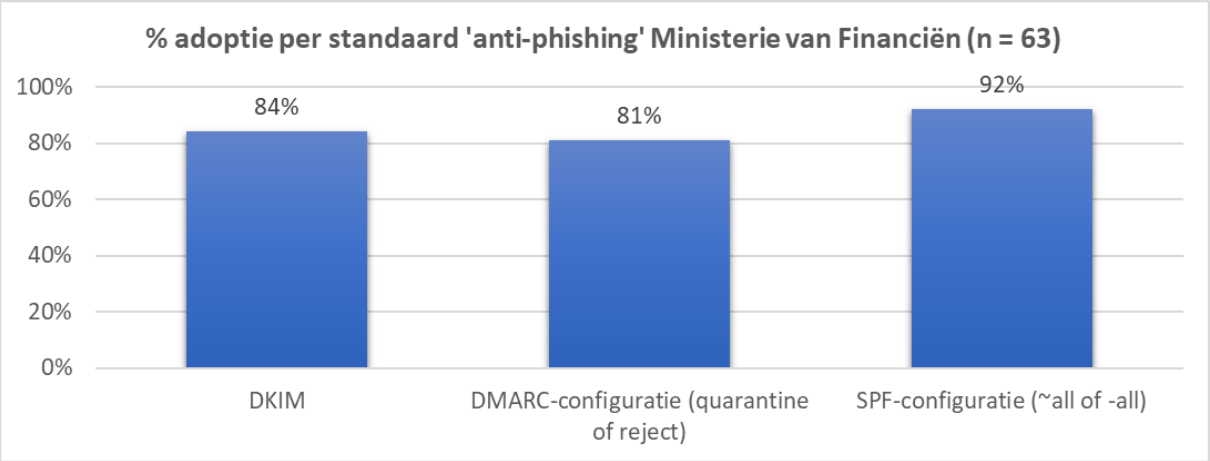


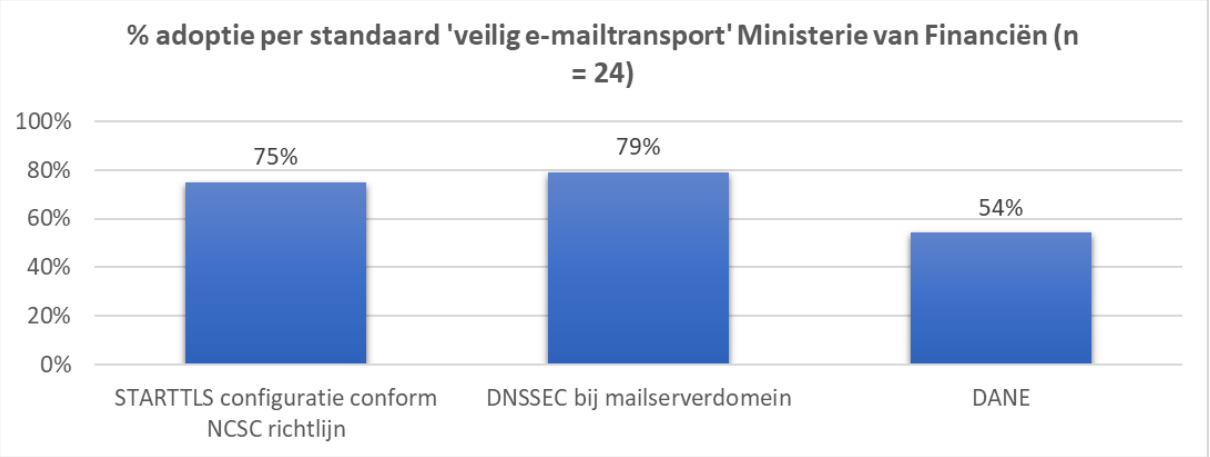




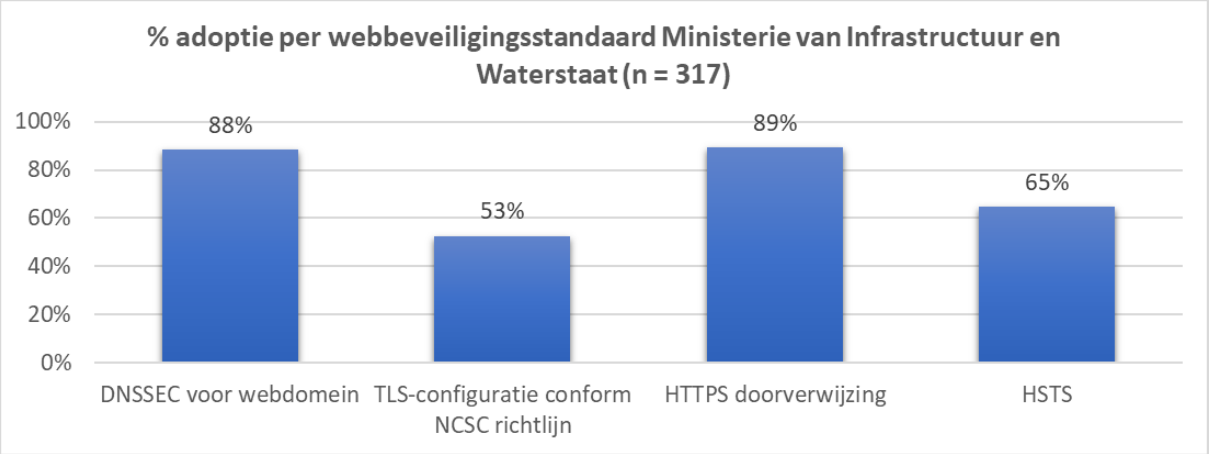
6.8. Ministerie van Financiën

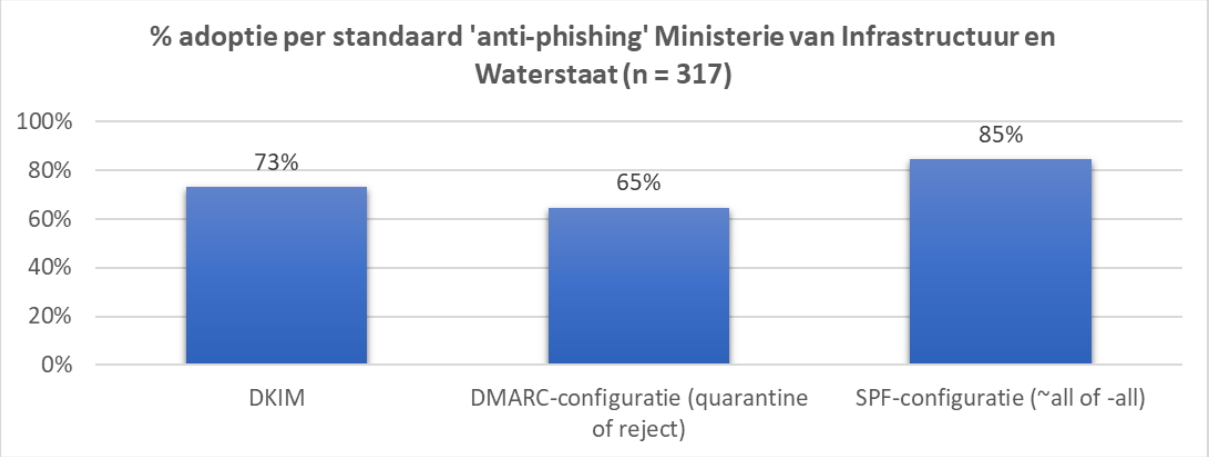


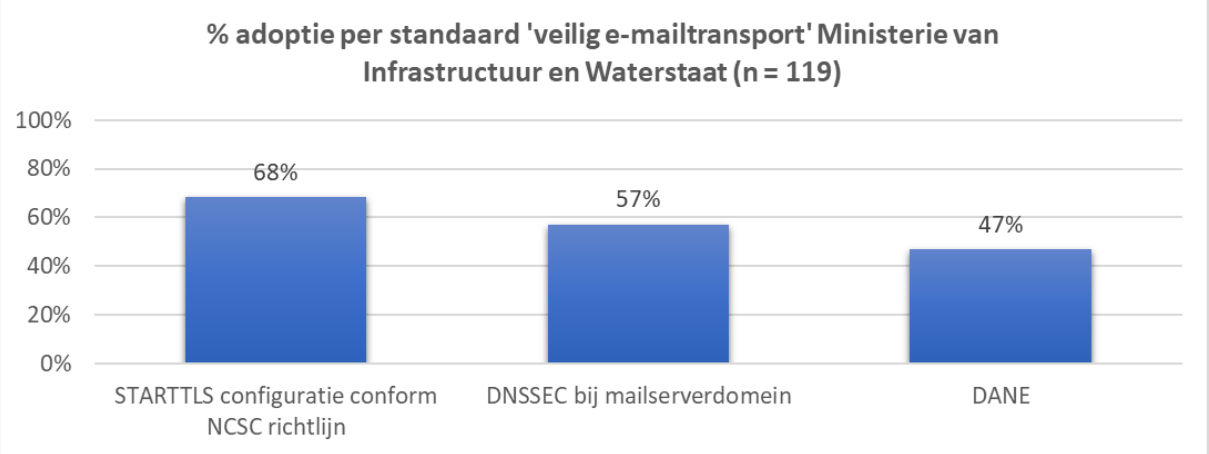




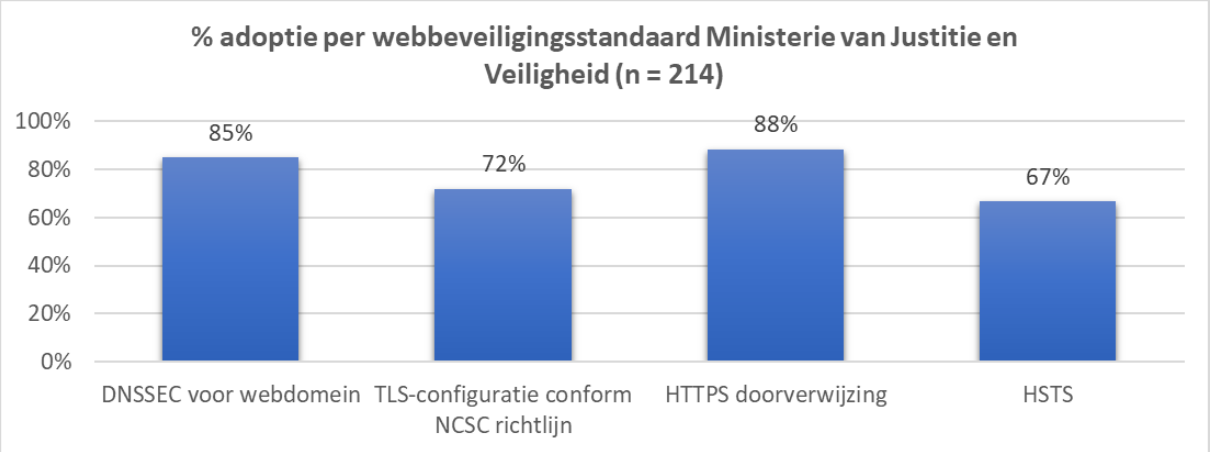
6.9. Ministerie van Infrastructuur en Waterstaat

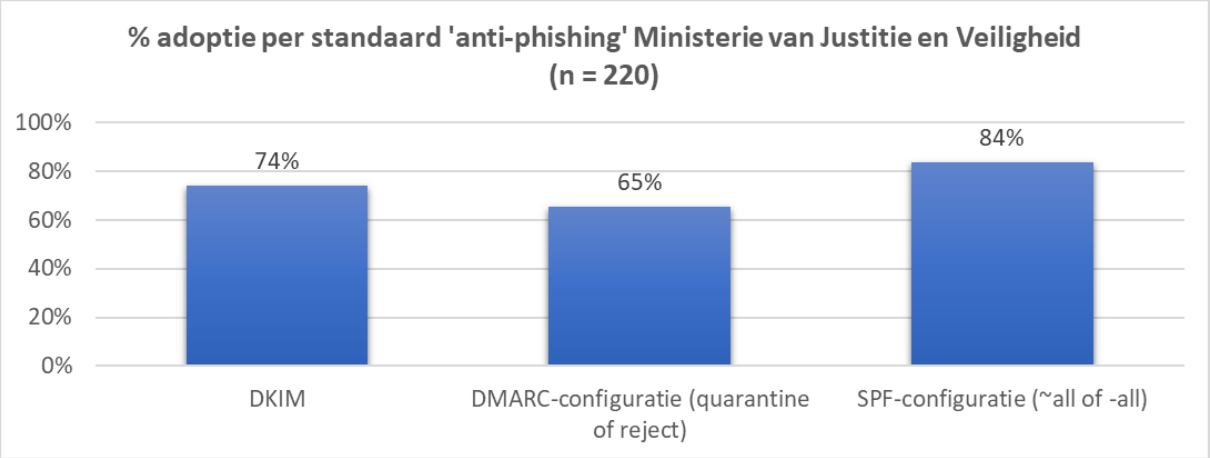


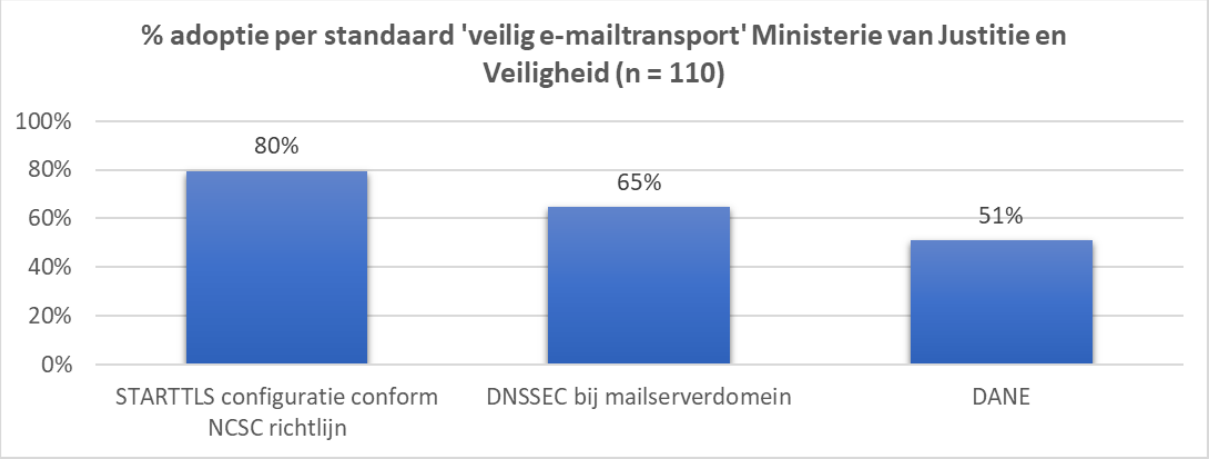




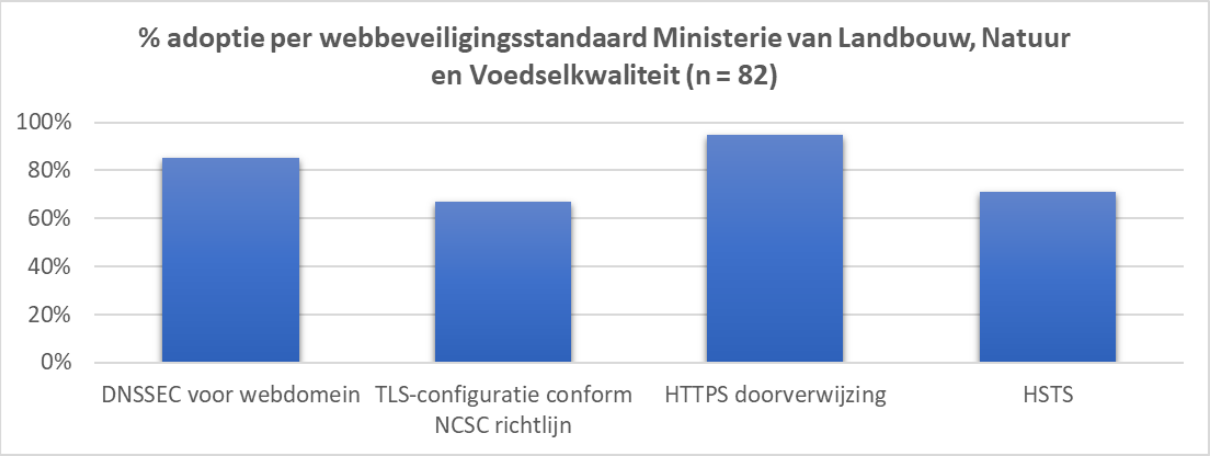
6.10. Ministerie van Justitie en Veiligheid

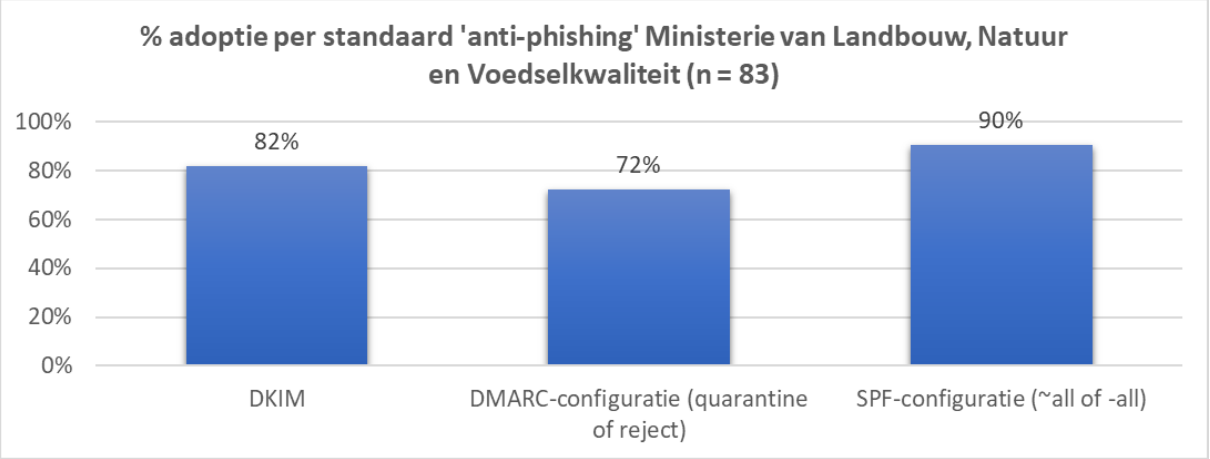


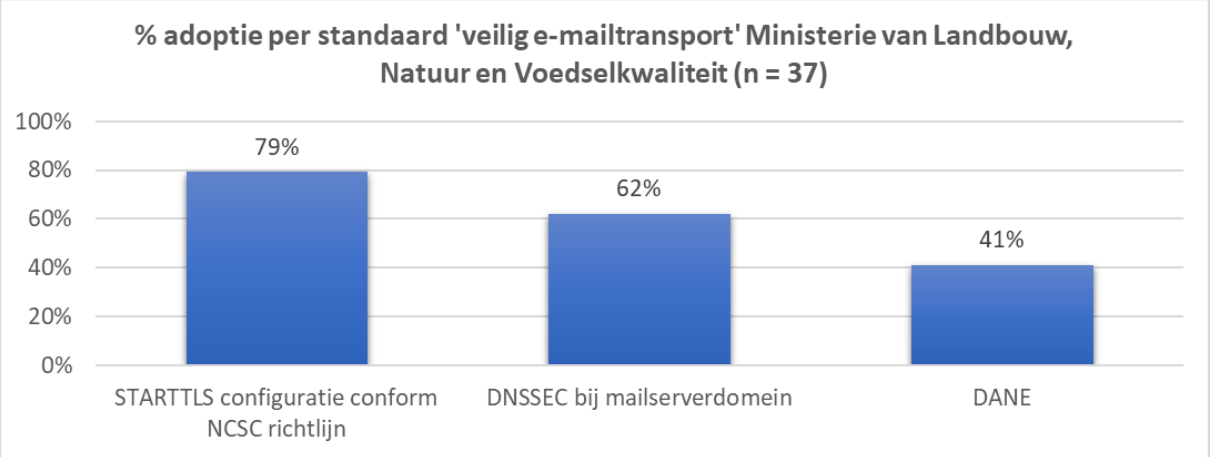




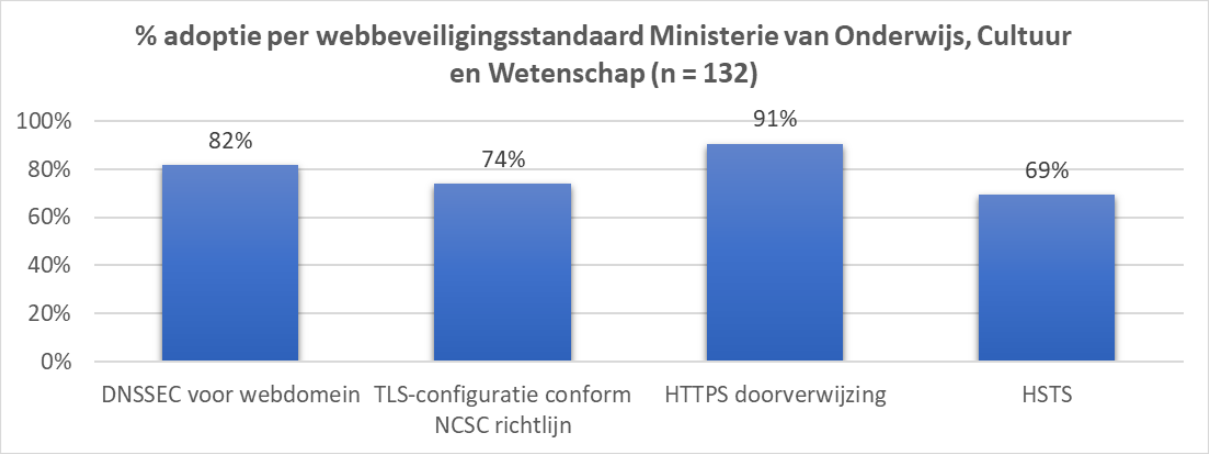
6.11. Ministerie van Landbouw, Natuur en Voedselkwaliteit

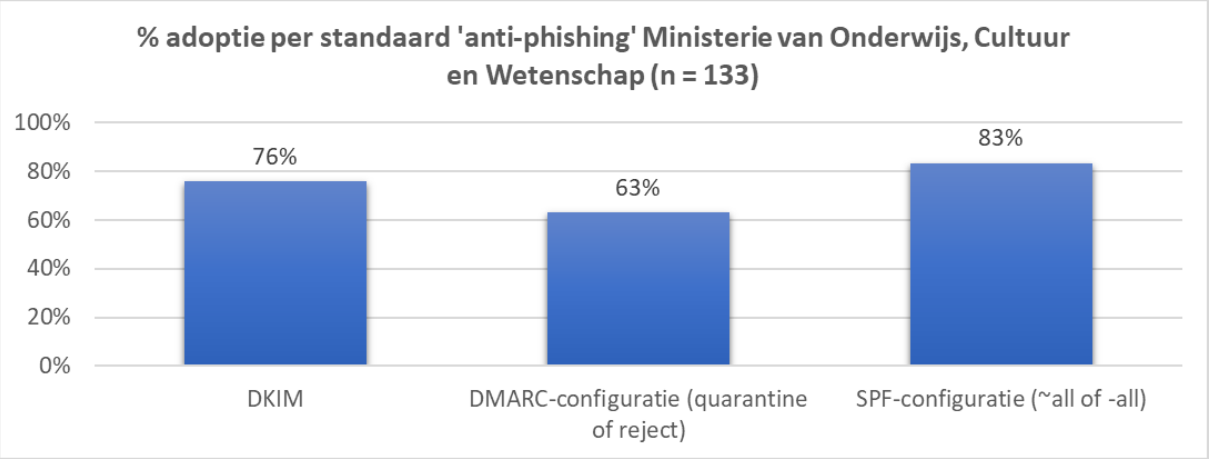


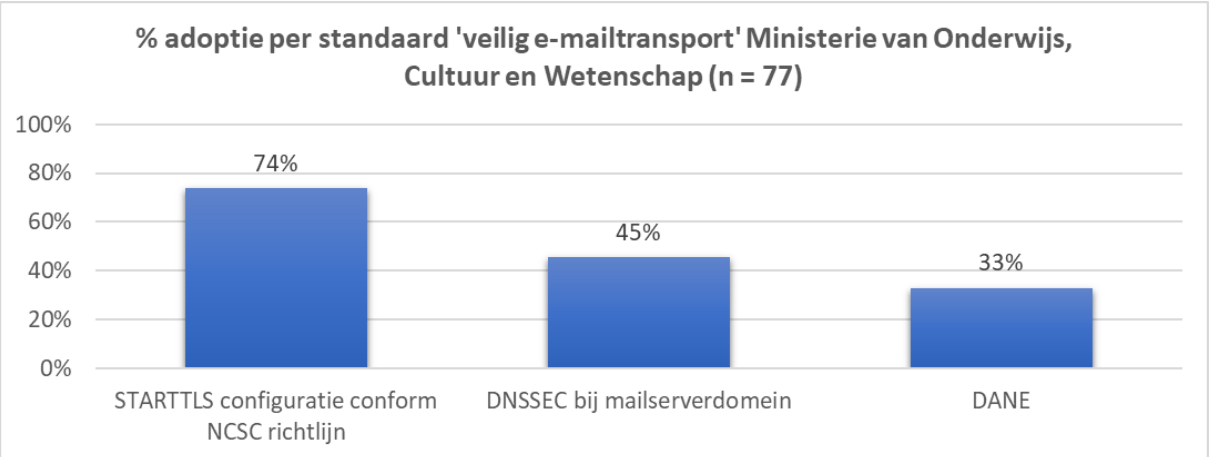




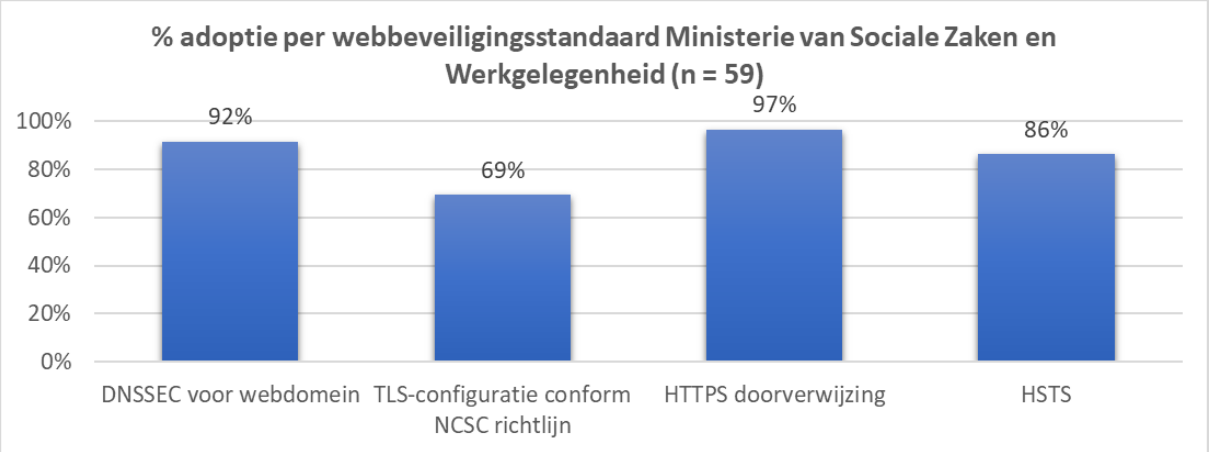
6.12. Ministerie van Onderwijs, Cultuur en Wetenschap

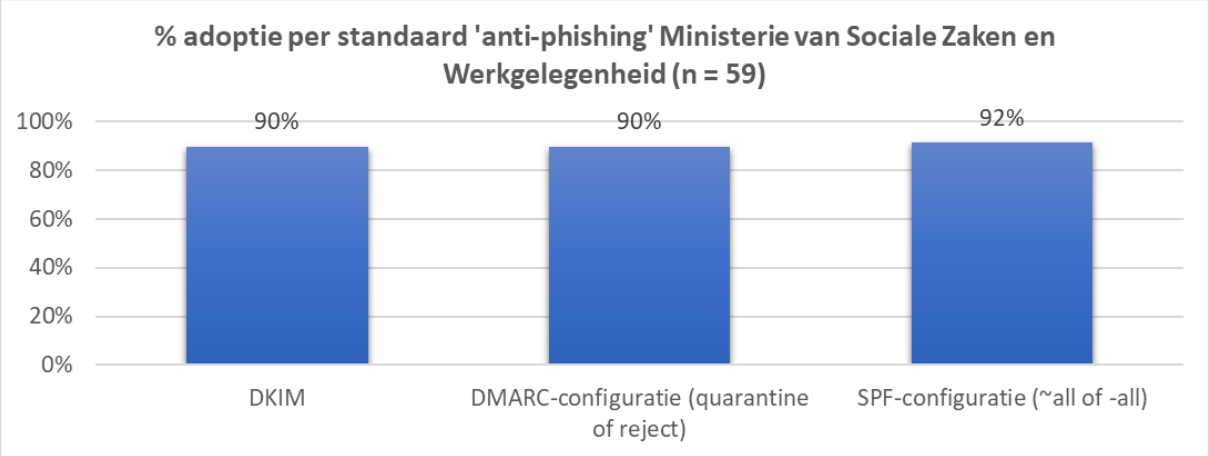


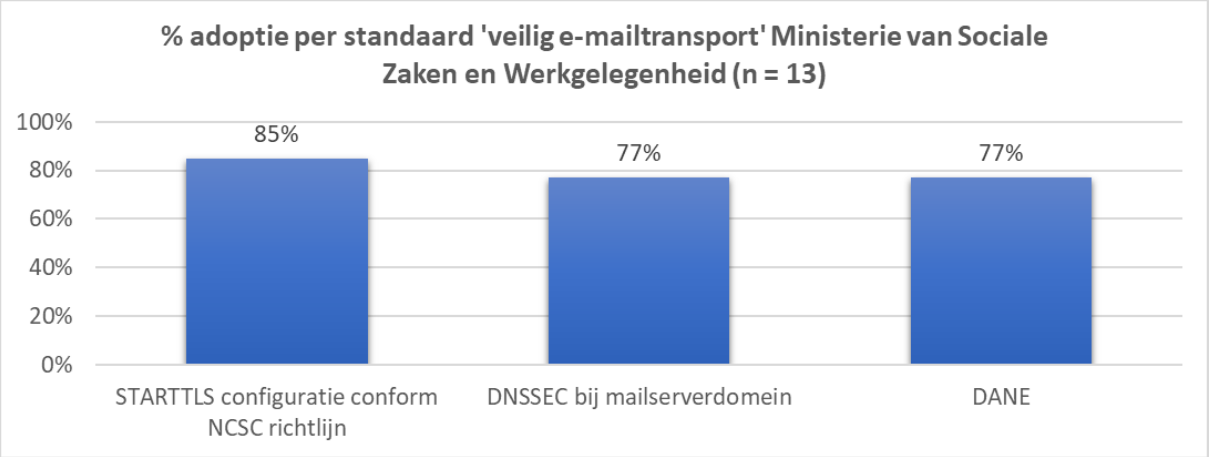




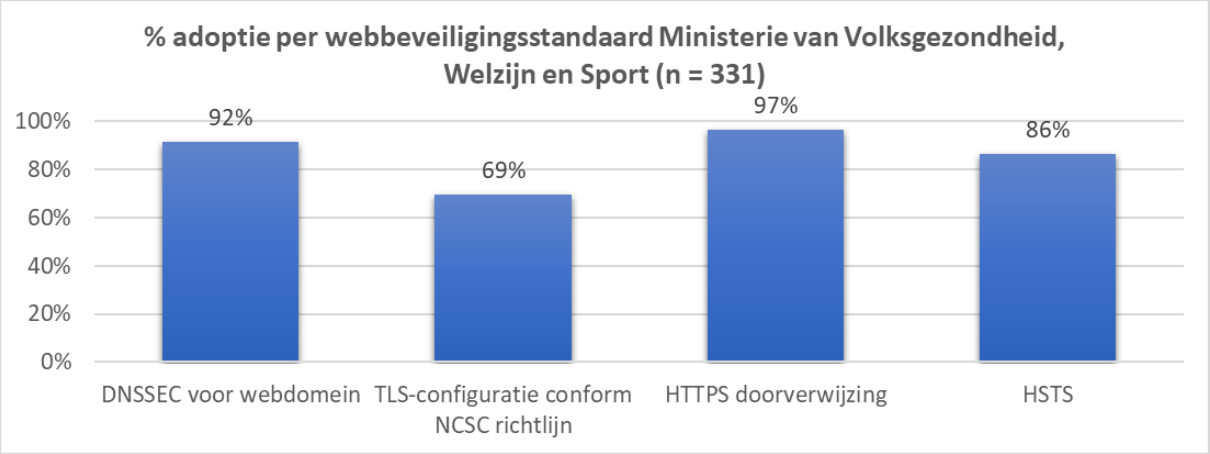
6.13. Ministerie van Sociale Zaken en Werkgelegenheid

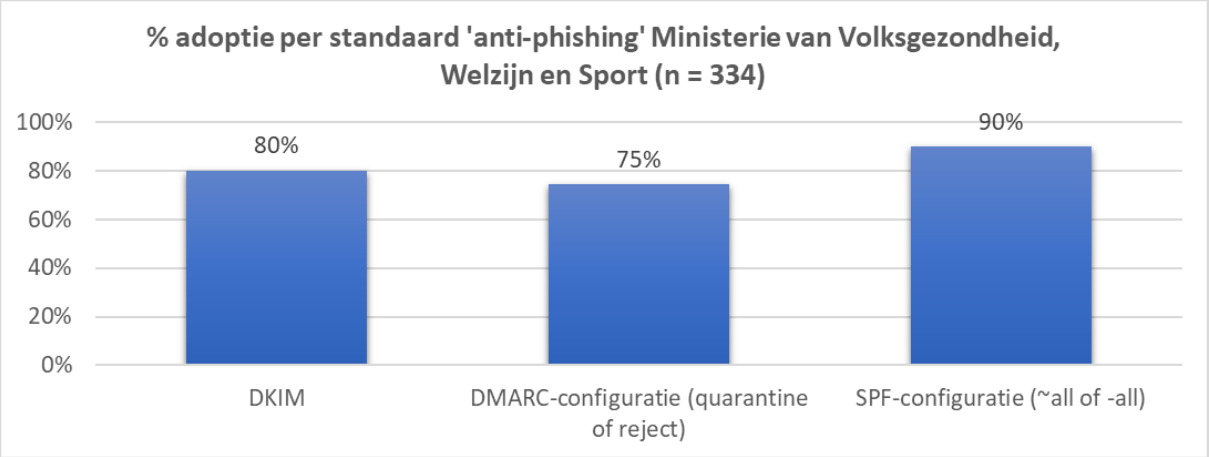


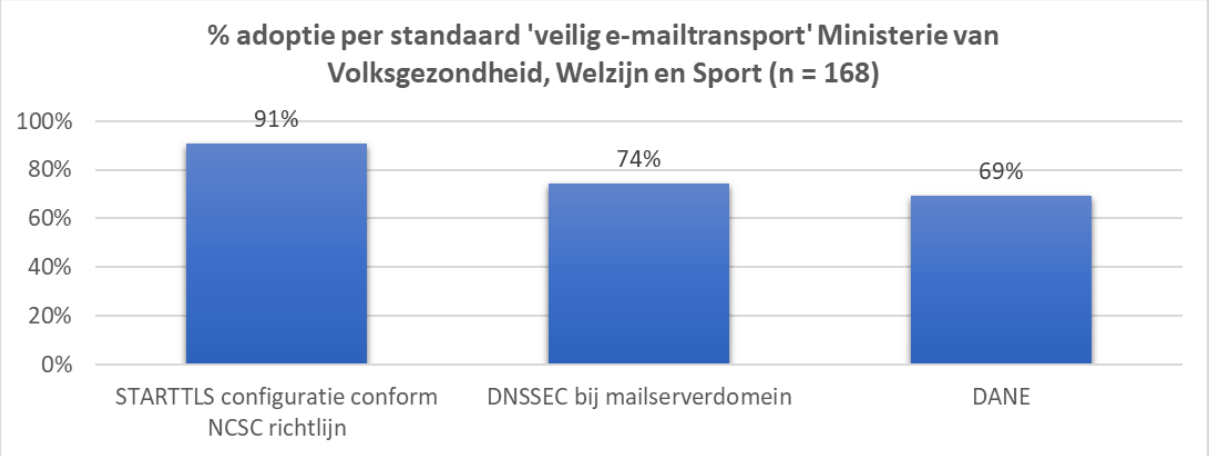




6.14. Ministerie van Volksgezondheid, Welzijn en Sport







7. Achtergrond

Sinds 2015 biedt het Platform Internetstandaarden de mogelijkheid om via de website Internet.nl domeinen te toetsen op het gebruik van verschillende moderne internetstandaarden, waaronder een aantal informatieveiligheidstandaarden en IPv6, 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 bepaalde standaarden versneld te willen adopteren. Dit betekent concreet dat voor deze standaarden niet langer 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.

Na de eerste interbestuurlijke afspraak zijn er door het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) drie aanvullende streefbeeldafspraken met verschillende uiterlijke implementatiedeadlines gemaakt. Van websites en e-mail van de overheid wordt vereist dat deze na het verlopen van de deadlines aan de standaarden en juiste configuratie voldoet.

Onderdeel van de afspraken is dat Forum Standaardisatie de voortgang van de adoptie meet en inzichtelijk maakt. De halfjaarlijkse Meting Informatieveiligheidstandaarden is ook onderdeel van de jaarlijkse Monitor Open Standaarden.

7.1. Om welke standaarden gaat het

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

UITERLIJKE IMPLEMENTATIE-DATUM	STANDAARDEN
EIND 2017	HTTPS en TLS: beveiligde verbindingen van website 'met gevoelige gegevens' DNSSEC: integriteit domeinnaam-gegevens SPF: echtheidswaarmerk ter preventie mailspoofing DKIM: echtheidswaarmerk ter preventie mailspoofing DMARC: beleid en rapportage ter preventie mailspoofing
EIND 2018	HTTPS, TLS en HSTS conform de TLS-richtlijnen van NCSC: beveiligde verbindingen van alle websites
EIND 2019	STARTTLS en DANE: encryptie van mailverkeer SPF en DMARC: het instellen van strikt beleid voor deze emailstandaarden
EIND 2021	IPv6 (naast IPv4): moderne internetadressering van overheidswebsites en e-maildomeinen van e overheid

7.2. Om welke internetdomeinen gaat het

In totaal zijn in deze meting 2584 internetdomeinen van overheidsorganisaties getoetst, bestaande uit:

- Alle internetdomeinen uit het Websiteregister Rijksoverheid;
- Alle internetdomeinen uit het Register van Overheidsorganisaties op organisaties.overheid.nl;
- Internetdomeinen uit voorgaande metingen.

De lijst betreft een selectie van alle overheidsdomeinnamen. De lijst is niet volledig en kan dat ook niet zijn omdat de overheid momenteel geen overzicht heeft over alle domeinnamen. De gemeten internetdomeinen zijn bij lange na niet alle domeinen waar het OBDO direct en indirect voor verantwoordelijk is. Zo heeft het ministerie van AZ zicht op meer dan 9.000 internetdomeinen van de Rijksoverheid waarvan het overzicht niet openbaar is gepubliceerd. Een 100%-score op de gemeten domeinen garandeert geenszins dat hiermee *alle* overheidsdomeinen beschermd zijn tegen bijvoorbeeld phishing.

7.3. Hoe wordt gemeten

De meting geeft de stand van zaken weer van mei 2022. De meting laat zien of op een domeinnaam de standaarden worden toegepast. De resultaten zijn voorgelegd aan een aantal koepelorganisaties en stakeholders en begin juli geactualiseerd indien nodig.

De meting wordt uitgevoerd middels een bulktoets via de API van Internet.nl. Voor de web-standaarden wordt het hoofddomein getoetst met de toevoeging www. (dus: www.forumstandaardisatie.nl), omdat het gebruikelijk is dat de website daarop bereikbaar is. Voor de maildomeinen wordt getoetst zonder enig voorvoegsel omdat dat doorgaans gebruikt wordt als e-maildomein (dus @forumstandaardisatie.nl).

Op Internet.nl is eenvoudig te testen of een website of e-mail een aantal moderne internetstandaarden ondersteunen, ook de standaarden waarover streefbeeldafspraken zijn gemaakt zijn onderdeel van de test. De score die een domeinnaam op Internet.nl kan halen (namelijk max. 100%) heeft een directe relatie met het resultaat uit deze meting, aangezien deze meting alle standaarden bevat die de Internet.nl score kunnen beïnvloeden.

De website Internet.nl is een initiatief van het Platform Internetstandaarden. In het platform participeren verschillende partners uit de internetgemeenschap (zoals Internet Society, RIPE NCC, SIDN en SURFnet) en Nederlandse overheid (Forum Standaardisatie, het Ministerie van Economische Zaken en Klimaat, en NCSC). Het uitgangspunt is dat Internet.nl de adviezen van Forum Standaardisatie en NCSC met betrekking tot de Internetstandaarden volgt.

De meting geeft geen inzicht in het risiconiveau van een bepaald domein. Zo is het aannemelijk dat de aantrekkelijkheid van misbruik hoger is bij domeinen van grote uitvoerders (zoals *phishing* met aanmaningen) dan bij domeinen van kleine gemeenten.

7.4. 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;
- validatie van de DMARC-, DKIM- en SPF-kenmerken door ontvangende mailservers van een overheidsorganisatie;
- validatie van DANE-kenmerken door verzendende mailservers van een overheidsorganisatie.

7.5. 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.

7.5.1. Webstandaarden

Wij meten het gebruik van de beveiligingsstandaarden en IPv6 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).

STANDAARD	BESCHRIJVING
DNSSEC	Domain Name System (DNS) is het registratiesysteem van namen en bijbehorende internetnummers en andere domeinnaaminformatie. Het is vergelijkbaar met een telefoonboek. Dit systeem kan worden bevraagd om namen naar nummers te vertalen en omgekeerd. Er is getest of de domeinnaam ondertekend is met DNSSEC, zodat de integriteit van de DNS-informatie is beschermd. De streefbeeldafspraak was om hier vóór 2018 aan te voldoen.
TLS CF. NCSC	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. TLS behoort bovendien zodanig geconfigureerd te zijn dat deze voldoet aan de aanbevelingen van het Nationaal Cyber Security Center (NCSC). Zodat de vertrouwelijkheid, de authenticiteit en integriteit van een bezoek aan een website is gegarandeerd. De streefbeeldafspraak was om hier voor 2019 aan te voldoen.

HTTPS REDIRECT	Er wordt getest of een webserver bezoekers automatisch doorverwijst van HTTP naar HTTPS op dezelfde domeinnaam óf dat deze ondersteuning biedt voor alleen HTTPS en niet voor HTTP. Op Internet.nl heet deze subtest 'HTTPS Redirect'. De streefbeeldafspraak was om hier voor 2019 aan te voldoen.
HSTS	HSTS zorgt ervoor dat een browser eist dat een website altijd HTTPS blijft gebruiken na het eerste contact over HTTPS. Dit helpt voorkomen dat een derde -bijvoorbeeld een kwaadaardige WiFi hotspot- een browser kan omleiden naar een valse website. Door HTTPS samen met HSTS te gebruiken wordt het gebruik van beveiligde verbindingen zoveel mogelijk afgedwongen. De streefbeeldafspraak was om hier vóór 2019 aan te voldoen.
IPV6 WEB	Internet Protocol versie 6 (IPv6) maakt communicatie van data tussen ICT-systemen op het Internet mogelijk. Er wordt getest of alle nameservers (minimaal twee) en tenminste één webserver een IPv6-adres hebben en bereikbaar zijn. Er wordt ook getest of de IPv6 website gelijk lijkt aan de IPv4 website. De streefbeeldafspraak was om hier vóór 2022 aan te voldoen.

7.5.2. E-mailstandaarden

Wij meten het gebruik van anti-phishing standaarden 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 respectievelijk de policies –all en p=reject).

STANDAARD	BESCHRIJVING
DMARC POLICY	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. Zolang er geen beleid is ingesteld weet de ontvanger nog niet wat te doen met verdachte e-mail. De configuratie moet op orde zijn. (Opm: Actieve policies zijn ~all en –all voor SPF, en p=quarantine en p=reject voor DMARC) Er wordt gecontroleerd of de syntax van de DMARC-record correct is en of deze een voldoende strikte policy bevat. De streefbeeldafspraak was om hier voor 2020 aan te voldoen.
DKIM	Met DKIM kunnen e-mailberichten worden gewaarmerkt. De ontvanger van een e-mail kan op die manier controleren of een e-mailbericht écht van de afzender afkomstig is en of het bericht onderweg ongewijzigd is gebleven.

	Getest wordt of de domeinnaam DKIM ondersteunt. Voor non-mail domeinen waar dit goed is ingesteld heeft DKIM verder geen toegevoegde waarde. In de meting wordt dit weergegeven middels de score "NVT" (niet van toepassing) voor DKIM. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
SPF POLICY	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 syntax van de SPF-record geldig is en of deze een voldoende strikte policy bevat om misbruik van het domein door phishers en spammers tegen te gaan. De streefbeeldafspraak was om hier voor 2020 aan te voldoen.
STARTTLS CF. NCSC	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. Net zoals bij HTTPS kan er bij STARTTLS gebruik worden gemaakt van verschillende versies van het TLS en verschillende versleutelingsstandaarden (ciphers). Aangezien niet alle versies en combinaties als voldoende veilig worden beschouwd, is het belangrijk om hierin de juiste keuze te maken en ook regelmatig te controleren of de gebruikte instellingen nog veilig zijn. Getest wordt of STARTTLS is geconfigureerd zoals door het NCSC is aanbevolen. De streefbeeldafspraak was om hier vóór 2020 aan te voldoen.
DANE	DANE, dat voortbouwt op DNSSEC, zorgt er in combinatie met STARTTLS voor dat een verzendende e-mailserver de authenticiteit van een ontvangende e-mailserver kan controleren en het kan het gebruik van TLS bovendien afdwingen. Getest wordt of de nameservers van de mailservers één of meer TLSA-records voor DANE bevatten. De streefbeeldafspraak was om hier voor 2020 aan te voldoen.
DNSSEC MX	DNSSEC is een randvoorwaarde voor het instellen van DANE. Daarom wordt getest of de domeinnamen van de mailservers (MX) ondertekend zijn met DNSSEC. Dit in het kader van de streefbeeldafspraak om voor 2020 STARTTLS en DANE te ondersteunen.
IPV6 E-MAIL	Internet Protocol versie 6 (IPv6) maakt communicatie van data tussen ICT-systemen op het Internet mogelijk. Er wordt getest of alle nameservers (minimaal twee) van het e-maildomein en alle mailservers (MX) een IPv6-adres hebben en bereikbaar zijn. De streefbeeldafspraak was om hier vóór 2022 aan te voldoen.