Rapport

Monitor Open standaarden: rapportage 2018

Onderzoek naar het gebruik van open standaarden van de 'pas toe of leg uit'-lijst van het Forum Standaardisatie door overheidsorganisaties:
bij aanbestedingen (juli 2017 - juni 2018),
in overheidsbrede voorzieningen (zomer 2018)
en per standaard (zomer 2018)

Van Jaap Korpel & Joost Vreuls

Versie Versie 1.2

Datum 31-1-2019

Inhoudsopgave

1. Managementsamenvatting 3

2. Inleiding en beleidscontext 9

2.1. Waarom open standaarden? 9
2.2. Het open standaardenbeleid in jaartallen 9
2.3. Juridisch kader 11
2.4. Monitor Open standaarden 12
2.5. Bronnen van de gepresenteerde gegevens 12

3. Open standaarden bij aanbestedingen ('pas toe' en 'leg uit') 14

3.1. Onderzoek van feitelijke aanbestedingen 14
3.2. 'Pas toe' bij feitelijke aanbestedingen in 2017/2018 17
3.3. 'Pas toe' per open standaard 23
3.4. 'Leg uit' bij feitelijke aanbestedingen 26
3.5. Welke open standaarden waren relevant bij feitelijke aanbestedingen 29

4. Toepassing open standaarden via voorzieningen 32

4.1. Inleiding 32
4.2. Overzicht: open standaarden in overheidsbrede voorzieningen 34

5. Open standaarden: gebruiksgegevens 39

5.1. Gebruiksgegevens 2018: inventarisatie door accountmanagers BFS 39
5.2. Gebruiksgegevens 2018: resultaten IV-meting 41
5.3. Gebruiksgegevens 2018: indicatieve gegevens ODF en PDF o.b.v. 'crawler' 41

Bijlagen

A. Functioneel toepassingsgebied en organisatorisch werkingsgebied per standaard
B. FAQ Monitor Open standaarden
C. Aanbestedingen: schema 'Pas toe of leg uit' in het kort
D. Overzicht van de beoordeelde aanbestedingen 2017/2018
E. Notitie *'Meer over gebruik van de standaarden van de 'pas toe of leg uit'-lijst'* (BFS)
F. Gegevens over het gebruik van PDF op basis van 'crawler' (BFS)
G. Rapportage *'IV-meting september 2018'*, Bureau Forum Standaardisatie

Separaat:
H. Rapport *'Monitor Open Standaarden Voorzieningen 2018'* (Versie 1.1, 13-11-2018), PBLQ

1. Managementsamenvatting

De kernvraag van de jaarlijkse Monitor Open standaarden is of, en zo ja in welke mate, overheden de verplichte open standaarden (pas toe of leg uit) van het Forum Standaardisatie daadwerkelijk gebruiken wanneer ze van toepassing zijn, zoals onder meer wordt voorgeschreven in de Instructie rijksdienst voor de aanschaf van ICT-diensten en ICT-producten.

In grote lijnen is dit jaar het antwoord op die vraag:

- Het gebruik van de verplichte open standaarden neemt van jaar op jaar geleidelijk toe. Maar het einddoel dat alle overheden de relevante open standaarden toepassen is ook in 2018 nog niet bereikt.
- Bij 85% van de 52 onderzochte aanbestedingen werd om één of meer van de relevante open standaarden gevraagd, maar vaak niet om alle relevante open standaarden. Slechts bij 15% van de aanbestedingen werd om alle of tenminste om alle cruciale relevante open standaarden gevraagd. Dat is bovendien minder dan vorig jaar.
- De 35 onderzochte overheidsbrede voorzieningen voldoen in belangrijke mate aan de relevante open standaarden: van de 464 gevallen waarin een open standaard relevant was wordt in 70% van de gevallen daaraan voldaan en in 18% van de gevallen wordt deels voldaan of er zijn concrete plannen om er binnenkort aan te voldoen.

Waarom open standaarden? Achtergrond open standaardenbeleid en juridisch kader (H2)

Het open standaardenbeleid is gericht op het vergroten van de interoperabiliteit en van de leveranciers-onafhankelijkheid voor de publieke sector, waardoor een kwalitatief hoogwaardige, kostenefficiënte en veilige informatie-uitwisseling mogelijk wordt gemaakt. Voor de Nederlandse overheid zijn open standaarden de norm: voor de gehele (semi-) publieke sector geldt sinds 2009 een 'pas toe of leg uit'-regime.

Open standaarden voor 'pas toe of leg uit'

Er zijn veel open standaarden en een groot deel daarvan wordt ook in de publieke sector breed toegepast[1]. Voor een aantal open standaarden is een extra stimulans wenselijk, maar is een wettelijke verplichting nog een brug te ver. Het gaat daarbij om open standaarden die sterk bijdragen aan het vergroten van de interoperabiliteit en de leveranciers-onafhankelijkheid voor de publieke sector en waarvoor breed draagvlak bestaat, maar die op dit moment nog niet breed geadopteerd zijn. Deze worden, na een zorgvuldige en open toetsingsprocedure, door het Forum Standaardisatie op de lijst voor 'pas toe of leg uit' geplaatst. Op deze open standaarden (zomer 2018 waren dit er 44) is het 'pas toe of leg uit'-regime van toepassing.

Meer informatie over deze standaarden en hun toepassingsgebied is te vinden in Bijlage A. Meer informatie over de beleidscontext en het juridisch kader staat in hoofdstuk 2 en Bijlage B.

[1] Naast de 'pas toe of leg uit'-lijst beheert het Forum Standaardisatie ook een lijst met *aanbevolen* open standaarden. Op deze lijst staan standaarden die al gangbaar zijn of die pril zijn en veelbelovend. Dit onderzoek beperkt zich tot de standaarden op de 'pas toe of leg uit'-lijst.

Monitor Open standaarden 2018 (H2)

In opdracht van het Bureau Forum Standaardisatie voert ICTU jaarlijks de Monitor Open standaarden uit. Voor u ligt de rapportage die betrekking heeft op de periode juli 2017 t/m juni 2018 ('pas toe of leg uit' bij feitelijke aanbestedingen), respectievelijk de situatie in de zomer van 2018 (open standaarden in overheidsbrede voorzieningen en gebruiksgegevens van open standaarden). De Monitor is gebaseerd op gegevens uit drie bronnen, die samen een goed beeld vormen van de voortgang van het open standaardenbeleid:

- onderzoek van 'pas toe of leg uit' bij feitelijke aanbestedingen in 2017/2018;
- onderzoek naar de toepassing van open standaarden bij overheidsbrede voorzieningen;
- onderzoek naar gebruiksgegevens van open standaarden, voorzover beschikbaar.

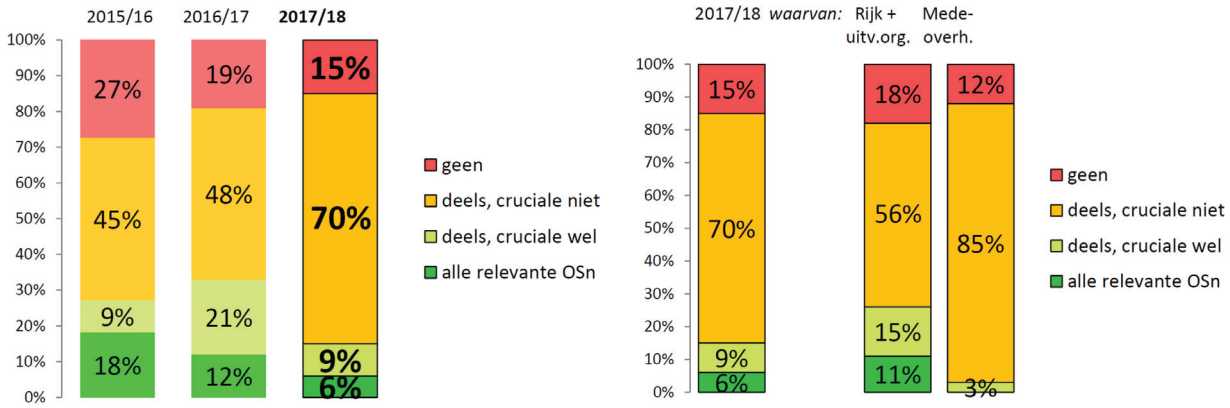
In het navolgende worden de voornaamste bevindingen per deelonderzoek samengevat. De positieve bevindingen hebben een groen blokje (+), de minder positieve een oranje (-).

Open standaarden bij aanbestedingen (H3)

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

'Pas toe' bij feitelijke aanbestedingen

Voor de monitor is, net als vorig jaar, een groot aantal aanbestedingen onderzocht. Dit keer zijn 34 aanbestedingen van de rijksoverheid en uitvoeringsorganisaties en 33 aanbestedingen van mede-overheden onderzocht, in totaal 67 aanbestedingen (uit het 3e en 4e kwartaal van 2017 en 1e en 2e kwartaal van 2018). De resultaten worden beschreven in hoofdstuk 3.



Het percentage aanbestedingen waarbij *niet* om een open standaard is gevraagd daalde verder van 19% vorig jaar naar 15% dit jaar. In 6% van de onderzochte aanbestedingen is gevraagd om alle relevante open standaarden, en in 9% van de aanbestedingen is tenminste om de cruciale standaard(en) gevraagd. Samen is dat 15%, en dat is minder dan vorig jaar (33%) en ook minder dan het jaar dáárvoor. Het percentage aanbestedingen waarbij om één of meer cruciale standaarden niet is gevraagd – de middencategorie – is flink gestegen: van 48% vorig jaar tot 70% dit jaar.

Rijk en uitvoeringsorganisaties deden het in 2017/2018 beter dan de mede-overheden: bij 11% van de aanbestedingen werd om alle relevante standaarden gevraagd (mede-overheden: 0%) en daarnaast bij nog 15% om tenminste alle cruciale standaarden (mede-overheden: 3%). Bij 18% van de Rijks-aanbestedingen werd om geen enkele standaard gevraagd, de mede-overheden deden dàt beter: 12%.

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

+	Bij 4 aanbestedingen (6%) is om alle relevante standaarden gevraagd. Hierbij gaat het alleen om aanbestedingen Rijk en uitvoeringsorganisaties: van het Ministerie van BZK, het Zorginstituut Nederland (twee keer) en de RDW.
-	Het aandeel aanbestedingen waarbij om alle relevante standaarden is gevraagd, is ten opzichte van vorig jaar verder afgenomen van 12% naar 6%.
+	Naast de 4 aanbestedingen (6%) waarbij om alle relevante standaarden is gevraagd, werd bij 53 aanbestedingen (79%) om een deel van de relevante open standaarden gevraagd. Dat is meer dan vorig jaar (69%).
+	Van de 53 aanbestedingen waarbij om *een deel van* de standaarden is gevraagd, werd bij 6 aanbestedingen (9% van alle aanbestedingen) wel om alle cruciale open standaarden gevraagd (maar om één of meer niet-cruciale standaarden niet).
+	De keerzijde hiervan is, dat bij 15% van alle aanbestedingen om geen enkele van de relevante open standaarden werd gevraagd. Dat is overigens een iets betere score dan vorig jaar (19%).
+	Sommige standaarden (vooral NEN-ISO/IEC 27001 en 27002, HTTPS & HSTS, TLS en PDF zijn beduidend vaker relevant bij een aanbesteding dan de andere standaarden.
+	Om enkele standaarden wordt, als ze relevant zijn voor een aanbesteding, in de meeste gevallen ook daadwerkelijk gevraagd: NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002,HTTPS & HSTS, SAML, PDF, StUF, Digitoegankelijk).
-	Twee standaarden werden relatief weinig gevraagd: IPv4 & IPv6 en ODF zijn frequent als relevant aangemerkt, maar in slechts 16% respectievelijk 14% van die gevallen werd om de standaard gevraagd.

Een aantal aanbestedingen onderscheidde zich in positieve zin, drie goede voorbeelden zijn:

- Ministerie van BZK (onafhankelijke ICT-dienstverlener voor het Huis voor Klokkenluiders). Alle 12 (!) open standaarden die relevant worden geacht, zijn ook uitgevraagd: DNSSEC, IPv4/IPv6, ISO 27001/27002, SAML, HTTPS & HSTS, WPA2 Enterprise, SPF, DKIM, DMARC en (minder cruciaal) ODF en PDF. In de aanbestedingsstukken wordt op veel plaatsen verwezen naar het gebruik van open standaarden en men verwijst naar de 'Pas toe of leg uit'-lijst van het Forum Standaardisatie. Aanbieders worden nadrukkelijk aangespoord om het gebruik van niet algemeen geaccepteerde standaarden te vermijden.
- Zorginstituut Nederland (leveren, onderhouden en doorontwikkelen e-HRM oplossing). In de aanbesteding is naar alle (in totaal 11 !) relevante open standaarden gevraagd: Digitoegankelijk, HTTPS & HSTS, TLS, ISO 27001/27002, ODF, PDF, en minder cruciaal: SAML, SPF, DKIM en DMARC.
- Gemeente Molenwaard (burgerzakensysteem voor de nieuwe gemeente Molenlanden). Relevante standaarden: Digikoppeling, Digitoegankelijk, DNSSEC, HTTPS & HSTS, TLS, ISO 27001 / 27002, StUF, PDF en SAML. De experts die de aanbesteding hebben beoordeeld merken het volgende op. "Alle standaarden zijn gevraagd, behalve Digitoegankelijk en DNSSEC. Zonde, want het is verder een goed voorbeeld van hoe het wel moet! Er wordt goed aandacht besteed aan het gebruik van open standaarden. Men verwijst expliciet naar open standaardenbeleid en 'pas toe of leg uit' lijst van het Forum Standaardisatie. Ook moet de geleverde software binnen twaalf maanden geconformeerd zijn aan nieuwe releases van de open standaarden van het Forum Standaardisatie."

'Leg uit' in jaarverslagen

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

Of er sprake is geweest van 'Leg uit' is na te gaan voor een deel van de dit jaar onderzochte aanbestedingen: alleen voor de aanbestedingen in het 3e en 4e kwartaal van 2017 (over 2018 zal door overheden pas verantwoording afgelegd worden in het jaarverslag dat in het voorjaar van 2019 verschijnt). Voor 28 van de aanbestedingen in het 3e en 4e kwartaal van 2017 was 'Leg uit' zonder twijfel vereist, omdat hierbij niet gevraagd werd om één of meer cruciale open standaarden of om geen enkele relevante standaard gevraagd is.

-	Van expliciete 'Leg uit' voor met name genoemde aanbestedingen was in de jaarverslagen van de betreffende overheidsorganisaties (waaronder 3 ministeries) geen sprake: nergens wordt een concrete afwijking van de 'pas toe of leg uit'-lijst genoemd.
-	In het jaarverslag over 2017 hebben 4 van de 11 ministeries een alinea over 'pas toe of leg uit' opgenomen (vorig jaar eveneens 4).
+	Het ministerie van BZK heeft een alinea over 'pas toe of leg uit' opgenomen, en verwijst bovendien naar het overzicht dat Logius jaarlijks publiceert met afwijkingen van de lijst voor 'pas toe of leg uit' in haar ICT-producten en -diensten en bedrijfsvoering.

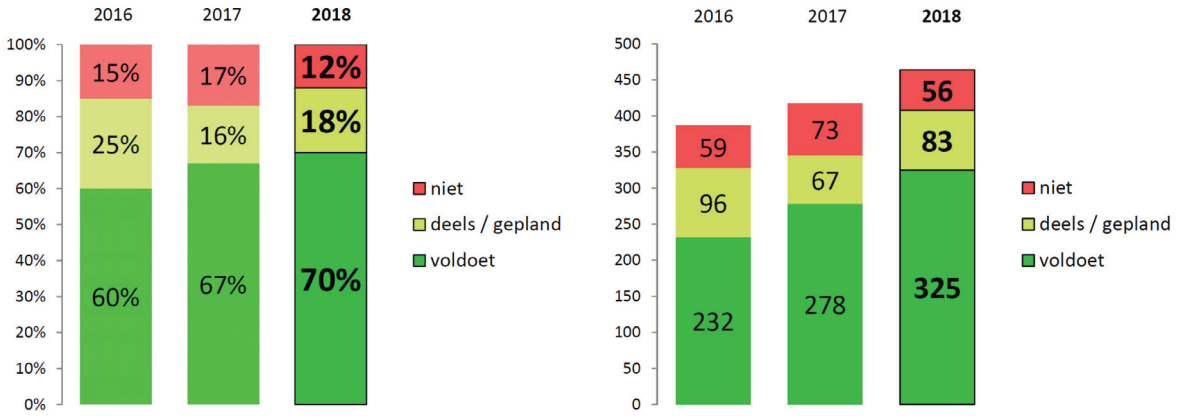
Toepassing van open standaarden via overheidsbrede voorzieningen (H4)

Voor een deel van hun informatiesystemen maken overheden gebruik van overheidsbrede voorzieningen zoals GDI-voorzieningen, shared services et cetera. Als daarin relevante open standaarden zijn toegepast, dan leidt dat tot breed gebruik van die open standaarden. Passen de ontwikkelaars en de beheerders van deze voorzieningen alle relevante open standaarden toe?

Daarom is ook dit jaar onderzocht in hoeverre de belangrijkste voorzieningen (35 in totaal) voldoen aan de relevante open standaarden. Er zijn 26 voorzieningen onderzocht die samen de GDI (Generieke Digitale Infrastructuur) vormen[2]. Daarnaast zijn dit jaar opnieuw 9 andere voorzieningen onderzocht die vorig jaar ook onderzocht zijn[3].

Een belangrijk deel van alle voorzieningen blijkt te voldoen aan de relevante open standaarden, en de mate waarin voorzieningen voldoen aan relevante open standaarden neemt bovendien toe. Van alle 464 gevallen waarbij een open standaard voor een voorziening relevant was, voldoet in 70% de voorziening daar aan (vorig jaar 67%). Het aantal gevallen waarin de voorziening deels aan de standaard voldoet of daarvoor concrete plannen heeft is iets toegenomen: van 16% vorig jaar naar 18% dit jaar. Samen is dat 88%.

[2] Niet onderzocht zijn: het eID-stelsel (nog in ontwikkeling), BLAU en BRO (nog niet gerealiseerd) en NORA, en daarnaast de Standaardenlijst en de Standaarden incl. die van de Pas toe of leg uit-lijst.
[3] ODC Noord, Digi-Inkoop, Doc-Direct, DWR, P-Direct, Rijksoverheid.nl, Rijkspas, Rijksportaal en TenderNed.



In absolute aantallen (zie rechter figuur hierboven) is te zien dat het aantal gevallen waarin aan open standaarden wordt voldaan is gestegen van 278 in 2016 tot 325 dit jaar.

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

+	Voor veel voorzieningen is een flink aantal open standaarden relevant: gemiddeld ruim 13 standaarden per voorziening. Van de 44 standaarden op de lijst voor 'pas toe of leg uit' zijn er 30 relevant voor één of meer overheidsbrede voorzieningen.
+	Voor 15 van deze 30 open standaarden geldt dat 80% of meer van de voorzieningen aan die standaard – indien relevant – voldoet. Daarvan vallen 7 standaarden in het domein 'Internet & beveiliging' en 3 in het domein 'Document & webcontent'.
-	Zeven standaarden scoren relatief laag: van de voorzieningen waarvoor deze relevant zijn voldoet er geen enkele aan CMIS en NLCIUS, en voldoet 25% aan STARTTLS & DANE, 40% aan SKOS, 42% aan IPv4&IPv6, 46% aan Digitoegankelijk en 47% aan Digikoppeling.
+	In de meeste gevallen voldoen de onderzochte voorzieningen aan de meeste ervoor relevante standaarden: aan 70% wordt voldaan, aan 18% voldoet de voorziening deels of dit is gepland en in 12% van de gevallen wordt op dit moment (nog) niet voldaan aan een relevante open standaard. NB: Uitgangspunt van het open standaardenbeleid is, dat aanpassing plaatsvindt op het moment dat een voorziening ontwikkeld, vernieuwd of vervangen wordt.
+	Op dit moment voldoen 10 van de 35 voorzieningen geheel of gedeeltelijk aan alle (gemiddeld ruim 13) relevante open standaarden en/of hebben concrete plannen om daaraan op korte termijn te voldoen. Negen van deze tien zijn GDI-voorzieningen.
+	Veel voorzieningen hebben ten opzichte van de vorige meting vooruitgang geboekt, met als meest positieve voorbeelden DigiLevering en DigiMelding, en daarnaast ook BAG, BRK, WOZ en BGT, MijnOverheid, DigiD en Ondernemersplein.

Verschillende voorzieningen onderscheiden zich dit jaar in positieve zin:

- BRI (inkomen) voldoet aan alle 6 relevante standaarden;
- DigiD voldoet aan alle 11 van de 12 relevante standaarden en voor de resterende standaard is dat gepland;
- PKI Overheid voldoet aan 10 van de 11 relevante standaarden en voor de resterende standaard is dat gepland.

Deze voorzieningen onderscheidden zich ook vorig jaar positief (naast enkele anderen).

Gebruiksgegevens van een aantal open standaarden (H5)

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

Dergelijke gebruiksgegevens zijn niet in alle gevallen eenvoudig te verzamelen. Dit jaar is dat voor het eerst gedaan door de accountmanagers van het Bureau Forum Standaardisatie, in de zomer van 2018, met de volgende uitkomsten:

+	Het beeld van BFS is voor 17 standaarden positief: NEN-ISO\IEC 27001 en 27002, SAML, STIX & TAXII, WPA2 Enterprise, NLCIUS, SETU, XBRL, Geo−standaarden, StUF, Aquo Standaard, SIKB 0101, SIKB0102, BWB, ECLI, JCDR en EMN_NL.
-	Voor acht standaarden is het beeld volgens BFS gemengd: IPv6/IPv4, CMIS, OWMS, SKOS, WDO Datamodel en Visi. Voor negen standaarden ontbreekt het BFS aan informatie: AdEs Baseline Profiles, Digitoegankelijk, ODF 1.2, PDF\A-1, PDF\A-2, PDF1.7, Digikoppeling, IFC, E−portfolio, NL LOM en STOSAG.

Halfjaarlijkse meting Internetveiligheidsstandaarden (Bijlage H)

In 2015 is het Forum Standaardisatie gestart met een halfjaarlijkse evaluatie van een groot aantal overheidsdomeinen op het voldoen aan internet- en veiligheidsstandaarden. Het Nationaal Beraad heeft eind 2015 de ambitie uitgesproken deze standaarden versneld te willen adopteren. In het OBDO hebben de overheden in april afgesproken dat volledige adoptie voor de volgende standaarden stapsgewijs gerealiseerd moet worden:

- uiterlijk eind 2017: DNSSEC, HTTPS, TLS (web) en DKIM, DMARC, SPF (mail);
- uiterlijk eind 2018: HSTS, HTTPS, TLS: veilige configuratie conform NCSC (web);
- uiterlijk eind 2019: voor DMARC, SPF instellen van strikte policies, STARTTLS&DANE (mail).

De halfjaarlijkse IV-meting betreft vijf webstandaarden (DNSSEC, HTTPS, TLS, TLS_NCSC, HSTS) en negen mailstandaarden (DANE, DKIM, DMARC, DMARC_policy, DNSSEC_MX, SPF, SPF_policy, STARTTLS, STARTTLS_NCSC). Voor een set van 563 domeinen is in september 2018 met behulp van Internet.nl getoetst of zij voldoen aan deze standaarden.

+	Van de vijf webstandaarden wordt TLS het meest toegepast (96%). De toepassing van de andere standaarden is duidelijk gegroeid: DNSSEC tot 90%, HTTPS tot 89%, TLS_NCSC tot 87 % en HSTS tot 79%.
+	De afspraken voor eind 2017 zijn voor TLS dus inmiddels bijna en voor DNSSEC en HTTPS nog niet helemaal gerealiseerd.
+	Van de negen mailstandaarden worden STARTTLS (94%) en SPF (93%) het meest toegepast, gevolgd door SPF_policy (85%), DKIM (84%) en DMARC (73%).
-	De afspraken voor eind 2017 zijn voor SPF dus inmiddels bijna gerealiseerd, terwijl voor DKIM en vooral DMARC nog een flink stuk te gaan is.
+	De andere vier mailstandaarden worden op dit moment nog minder vaak gebruikt: DNSSEC_MX (69%), STARTTLS_NCSC (55%), DMARC_policy (28%) en DANE (22%). Voor volledige adoptie van deze standaarden zijn de deadlines echter nog niet verstreken.

2. Inleiding en beleidscontext

2.1. Waarom open standaarden?

Sinds 2009 moet een aantal standaarden overheidsbreed verplicht toegepast worden: de open standaarden van de 'pas toe of leg uit'-lijst. Deze lijst wordt beheerd door het Forum Standaardisatie. Het gebruik van deze standaarden is essentieel

- om het digitale verkeer binnen en tussen overheden en tussen overheden en burgers en bedrijven soepel te laten doorstromen (interoperabiliteit),
- om grip te krijgen op de kosten voor ICT (door leveranciersafhankelijkheid te beperken)
- en om te zorgen voor veiligheid en betrouwbaarheid in het digitale verkeer: onder andere om cybercriminaliteit tegen te gaan en persoonsgegevens te beschermen.

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

2.2. Het open standaardenbeleid in jaartallen

2008

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

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

Leg uit:
Overheden mogen alleen afwijken (d.w.z. 'niet toepassen') ingeval van redenen van bijzonder gewicht[4]. Overheden zijn verplicht om afwijkingen gemotiveerd vast te leggen in de administratie en zijn verplicht om zich over de mate van naleving te verantwoorden in het jaarverslag.

Zie Bijlage C voor een stroomschema.

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

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

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

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

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

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

2018
In maart komt het nieuwe Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) voor het eerst bijeen. Het OBDO heeft de bestuurlijke afspraken van het Nationaal Beraad overgenomen cq. verlengd. Het OBDO heeft op 18 april 2018 besloten dat ook mede-overheden bij aanschaf van ICT moeten kiezen voor de relevante open standaarden van de pas-toe-of-leg-uit-lijst.

Daarnaast zijn in het OBDO specifieke afspraken gemaakt voor de adoptie van een aantal internet-veiligheidsstandaarden.
Streefbeeld eind 2017:
- TLS wordt toegepast bij alle overheidswebsites waarbij burgers en/of bedrijven gegevens moeten invoeren, of waarbij gegevens vooringevuld zijn;
- DNSSEC wordt gebruikt voor elke domeinnaam waarmee een overheidsorganisatie met burgers en/of bedrijven communiceert;
- de 'e-mail'-standaarden DMARC, SPF en DKIM worden toegepast voor alle overheids-domeinnamen of deze nu wel of niet gebruik maken van mail.

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

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

2.3. Juridisch kader

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

Ministeries en uitvoeringsorganisaties: Rijksinstructie en Rijksbegrotingsvoorschriften
Voor de rijksoverheid (zowel ministeries als uitvoeringsorganisaties) is sinds november 2008 de Rijksinstructie[5] van kracht:

> *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.*

Deze verplichting geldt voor de aanbesteding, inkoop of ontwikkeling van ICT-producten en -diensten ter waarde van € 50.000 en meer. Niet alleen voor nieuwe producten of diensten, maar ook als het gaat om aanpassing van bestaande producten of diensten. In Bijlage C is een schema opgenomen waarin het 'pas toe of leg uit'-principe in het kort wordt toegelicht.

Een open standaard van de lijst is altijd relevant als het betreffende ICT-product of -dienst valt binnen het functionele toepassingsgebied van die open standaard, als de organisatie bovendien valt binnen het organisatorische werkingsgebied van de betreffende standaard.[6] Er kunnen redenen zijn om de open standaard toch niet toe te passen. De aanbesteder kan echter niet zelf besluiten dat een open standaard 'in dit geval niet relevant is': of een standaard relevant is, hangt uitsluitend af van functioneel toepassingsgebied en organisatorisch werkingsgebied. Wanneer besloten wordt om niet te vragen om één of meer open standaarden die wèl van toepassing zijn, dan moet dit worden vastgelegd in de administratie en moet hierover bovendien verantwoording afgelegd worden in het jaarverslag. Afwijkingen zijn overigens alleen mogelijk bij redenen van bijzonder gewicht (zie daarover ook de toelichting van de Instructie rijksdienst).

Daarnaast is sinds een aantal jaren in de RijksBegrotingsVoorschriften[7] een bepaling opgenomen m.b.t. de bedrijfsvoeringparagraaf:

> *In het onderdeel financieel en materieel beheer wordt vermeld als is afgeweken (het 'comply of explain'-beginsel) van artikel 3, eerste lid van de Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten). De Tweede Kamer wil dat de overheid meer gebruik maakt van open standaarden en open source software. De Instructie rijksdienst schrijft voor dat bij de aanschaf en ontwikkeling van ICT-diensten of ICT-producten in beginsel gebruik moet worden gemaakt van open standaarden van de lijst van het College Standaardisatie. Valide afwijkingsgronden zijn opgenomen in de Instructie Rijksdienst. Als er sprake is van afwijking van de Instructie Rijksdienst dan wordt dit gemotiveerd aangegeven.*

---

[5] *Besluit van de staatssecretaris van Economische Zaken van 8 november 2008 tot vaststelling van de Instructie rijksdienst inzake aanschaf ICT-diensten en ICT-producten* (artikel 3, lid 1).
[6] Het functionele toepassingsgebied en het organisatorische werkingsgebied van elke standaard zijn vermeld in de lijst voor 'pas toe of leg uit'. Zie ook Bijlage A van dit rapport.
[7] De Rijksbegrotingsvoorschriften zijn opgesteld door het Ministerie van Financiën en bevatten de voorschriften voor de verantwoording over de begroting, uitvoering van de begroting en de begroting.

Mede-overheden: iNUP-Resultaatafspraak 20 en Richtlijnen commissie BBV

In de iNUP-bestuursakkoorden was als Resultaatafspraak 20 opgenomen, voorzover het open standaarden betreft:

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

Deze resultaatafspraak was van toepassing op gemeenten, provincies en waterschappen. Daarnaast is - voor gemeenten en provincies - in de Richtlijnen van de commissie BBV (Besluit begroting en verantwoording provincies en gemeenten) de aanbeveling opgenomen:

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

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

2.4. Monitor Open standaarden

Het Forum Standaardisatie heeft ICTU gevraagd om jaarlijks, gebruikmakend van verschillende bronnen, een integrale beleidsgerichte rapportage te verzorgen. Die moet inzicht geven in het gebruik van de verplichte standaarden op de lijst voor 'pas toe of leg uit' en zo in de vorderingen van he open standaardenbeleid in het algemeen.

De Monitor Open standaarden brengt voor de ministeries, uitvoeringsorganisaties van de Manifest-groep, gemeenten, provincies en waterschappen in kaart in hoeverre de open standaarden van de lijst door overheidsorganisaties worden toegepast.

2.5. Bronnen van de gepresenteerde gegevens

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

- onderzoek van feitelijke aanbestedingen in 2017/2018,
- onderzoek toepassing open standaarden bij overheidsbrede voorzieningen,
- onderzoek overige gebruiksgegevens van een aantal open standaarden.

Onderzoek feitelijke aanbestedingen in 2017/2018

Dit jaar zijn aanbestedingen onderzocht van de rijksoverheid (en uitvoerings-organisaties) en van mede-overheden uit de periode juli 2017-juni 2018. 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'). Het onderzoek toetst (op basis van openbaar beschikbare documenten) in hoeverre de aanbestedingen voldoen aan het 'pas toe of leg uit'-beginsel, zoals dat (voor het Rijk) is vastgelegd in de Instructie Rijksdienst en de RijksBegrotingsVoorschriften.

Onderzoek open standaarden bij overheidsbrede voorzieningen en shared services

Dit jaar is een onderzoek uitgevoerd naar de mate waarin 35 voorzieningen voldoen aan de open standaarden die daarvoor relevant zijn: 26 voorzieningen van de GDI (Generieke

Digitale Infrastructuur) en 9 andere voorzieningen die in de voorgaande jaren ook onderzocht zijn. Hiervoor zijn de betreffende beheerorganisaties benaderd.

Onderzoek overige gebruiksgegevens van een aantal open standaarden

Om na te gaan in welke mate open standaarden daadwerkelijk worden toegepast zijn overige gebruiksgegevens verzameld voor een aantal open standaarden. Dit jaar is dat voor het eerst gedaan door de accountmanagers van het Bureau Forum Standaardisatie.

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

Het centrale beleidsinstrument van het open standaardenbeleid is het 'pas toe of leg uit'-principe: overheden moeten bij ICT-aanbestedingen de relevante open standaarden van de lijst toepassen, of verantwoording afleggen in hun jaarverslag als zij deze standaarden niet toepassen, ondanks dat zij relevant zijn.

In het kader van de Monitor Open standaarden 2018 is nu voor het zevende achtereenvolgende jaar onderzoek gedaan naar de toepassing van open standaarden bij aanbestedingen door overheden. Per aanbesteding is vastgesteld welke open standaarden van de lijst daarop van toepassing waren en in hoeverre daar daadwerkelijk om is gevraagd ('pas toe'). Vervolgens is nagegaan in hoeverre overheden in hun jaarverslag verantwoording hebben afgelegd, wanneer bij aanbestedingen van de lijst werd afgeweken ('leg uit').

De aanpak van dit deelonderzoek wordt beschreven in paragraaf 3.1. De resultaten komen aan bod in paragrafen 3.2 (‘pas toe’ bij aanbestedingen), 3.3 (mate van ‘pas toe’ per open standaard), 3.4 (‘leg uit’ in jaarverslagen) en 3.5 (mate waarin open standaarden relevant waren bij de onderzochte aanbestedingen).

3.1. Onderzoek van feitelijke aanbestedingen

Dit jaar is, net als in de voorgaande jaren, onderzoek gedaan naar de aanbestedingen door het Rijk (met inbegrip van de uitvoeringsorganisaties, agentschappen en ZBO's) en de decentrale overheden (voor de periode Q3 en Q4 2017 en Q1 en Q2 2018). Dit jaar is de rol van eerste en tweede expert dezelfde als vorig jaar: de beoordeling van aanbestedingen is uitgevoerd door Linda Oosterheert MSc en Robin de Veer (TNO), mr. dr. Mathieu Paapst en mr. Arend-Jan Wiersma (ICTRecht) leverden de second opinion op de Rijks-aanbestedingen.

Onderzocht zijn aanbestedingen die op TenderNed.nl zijn gepubliceerd. Het betreft daardoor voornamelijk Europese aanbestedingen (drempelwaarden voor Europese aanbestedingen[8]: voor de rijksoverheid > € 135.000 (vanaf 1-1-2018: € 144.000) en voor decentrale overheden > € 209.000 (vanaf 1-1-2018: € 221.000). Aanbestedingen onder deze grenzen (maar groter dan € 50.000) worden weinig op TenderNed.nl gepubliceerd en vallen om die reden grotendeels buiten het onderzoek. Verder zijn detacheringen (waaronder maatwerk-opdrachten) in principe niet onderzocht, omdat ‘pas toe of leg uit’ daarbij hoogstens op bijzondere wijze kan plaatsvinden (bijvoorbeeld door bepaalde competenties te eisen). Daarnaast is moeilijk te beoordelen of daarbij ICT-producten/-diensten gerealiseerd worden waarop open standaarden van toepassing zijn en in hoeverre die daarbij geëist worden. Een kanttekening hierbij: in de onderzoekspraktijk bleek deze grens niet altijd even duidelijk te trekken. Voor een goede beoordeling moeten de aanbestedingsdocumenten bestudeerd kunnen worden, die moeten dus (nog) voor de beoordelaars beschikbaar zijn.

In principe worden elk jaar *alle* gevonden relevante aanbestedingen van Rijksoverheid en uitvoeringsorganisaties beoordeeld. Dit jaar ligt het aantal beoordeelde aanbestedingen van

[8] Deze drempelwaarden worden telkens voor een periode van twee jaar door de Europese Commissie vastgesteld. Met ingang van 1 januari 2018 zijn nieuwe drempelwaarden van kracht.

de Rijksoverheid (34) op het gebruikelijke niveau. Dat neemt niet weg dat ook dit jaar een aantal aanvankelijk geselecteerde aanbestedingen bij nader inzien door de experts als 'niet beoordeelbaar' gekwalificeerd moest worden. Daarbij gaat het bijvoorbeeld om:

- een aanbesteding gericht op het herzien van een modelinstrument. Op het eerste oog lijkt het om een ICT-aanbesteding te gaan maar dat blijkt bij nader inzien niet het geval. Open standaarden kunnen hierop niet van toepassing worden verklaard;
- een aanbesteding waarbij wordt gevraagd om een projectvoorstel, om vervolgens uit de ingediende projectvoorstellen de beste te selecteren en daarop verder te borduren; er ligt derhalve geen projectvoorstel aan de basis van de aanbesteding maar daar wordt juist om gevraagd zodat een koppeling met open standaarden (nog niet) mogelijk is;
- een aanbesteding betreft beheer en onderhoud van informatievoorziening c.q. industriële automatisering maar in feite betreft het geen ICT-aanbesteding;
- net als in eerdere jaren blijkt ook dit jaar in een enkel geval weer sprake van een raamovereenkomst die onvoldoende gedetailleerd uitgewerkt is om een oordeel te kunnen geven over de relevantie van open standaarden.

Voor de mede-overheden wordt elk jaar een *steekproef* getrokken uit de gevonden aanbestedingen. Dit jaar zijn 33 aanbestedingen van mede-overheden beoordeeld, dat is beduidend meer dan in voorgaande jaren. Voor deze verdubbeling is bewust gekozen om beter zicht te krijgen op de aanbestedingen door mede-overheden.

De beoordeling heeft plaatsgevonden in twee tranches: aanbestedingen uit de periode juli tot en met december 2017 en uit de periode januari tot en met juni 2018. Uiteindelijk zijn in totaal 67 aanbestedingen beoordeeld: 34 van het Rijk (departementen en uitvoerings-organisaties, agentschappen, ZBO's) en een steekproef van 33 aanbestedingen van mede-overheden. De 67 beoordeelde aanbestedingen vormen een goede afspiegeling van de overheids-ICT-aanbestedingen, voor zover die binnen de beschreven zoek-kaders vallen.

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

- veel overheidsorganisaties werken met (ICT-)mantelovereenkomsten, die voor langere periode van kracht zijn en/of met enkele jaren verlengd worden; aanbestedingen binnen de mantelovereenkomst worden direct bij de mantelpartijen uitgezet en zijn dus niet via TenderNed.nl te achterhalen;
- de vervangingscyclus van veel bedrijfs-software is 5 tot 8 jaar, wat betekent dat dergelijke applicaties maar eens in de zoveel jaar (opnieuw) worden aanbesteed; met name bij kleinere overheidsorganisaties kan dit betekenen dat men slechts zeer incidenteel van doen heeft met het beleid rond open standaarden;
- de huidige lijst voor 'pas toe of leg uit' bevat onder andere diverse semantische open standaarden, waaronder een aantal met een zeer specifiek toepassingsgebied; dergelijke standaarden blijken in de praktijk vaker relevant voor maatwerk-oplossingen dan voor standaardsoftware-pakketten; zoals gezegd valt juist een deel van de maatwerk-opdrachten buiten het onderzoek (detacheringen, mantel-overeenkomsten);
- uit de praktijk van de beoordeling door de experts van de aanbestedingen blijkt dat een aantal standaarden uitsluitend in combinatie al dan niet relevant worden geacht, ook al staan deze standaarden los op de lijst; voorbeelden van dergelijke combinaties zijn DKIM-DMARC-SPF (e-mail standaarden) en ISO-27001 en ISO-27002.

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

- vervanging van een website: ontwerpen, ontwikkelen, hosten en doorontwikkelen van de website en bijbehorende advisering hierover (ministerie / Rijk);
- levering, onderhoud en doorontwikkeling van een volledige e-HRM oplossing, inclusief de verwerking van salarissen en ter beschikking stellen van tweedelijns helpdesk (ZBO / Rijk);
- aanschaf van licenties voor een cloudapplicatie voor implementatie, hosten, support, verdere ontwikkeling, onderhoud en beheer van het zaaksysteem met de volgende functionaliteiten: zaak-, relatiebeheer-, archief- en portal-functionaliteit (ZBO / Rijk);
- het Huis voor Klokkenluiders zoekt een onafhankelijke ICT-dienstverlener om de kleine organisatie op ICT-gebied te ontzorgen en een digitale werkomgeving bij onder te brengen; de werkzaamheden van Het Huis voor Klokkenluiders zijn zeer vertrouwelijk en vragen om een beveiligde digitale werkomgeving (ministerie / Rijk);
- met behulp van de aanwezige software een nieuw Examen Management Systeem bouwen, inrichten en onderhouden; migratie van (persoons)gegevens van het oude naar het nieuwe systeem vallen binnen de scope (ZBO / Rijk);
- het implementeren en onderhouden van een geautomatiseerde ondersteuning van alle activiteiten in het kader van ketensamenwerking, schuldhulpverlening en de bankfunctie van de Gemeentelijke Kredietbank (gemeente);
- hosting en dataopslag voor rioleringen en gemalen; hieruit komen diverse rapportages over waterbeheer, rioleringen en gemalen, met deze inspecties en meldingen stuurt de gemeente op de onderhoudsstrategie en worden analyses gemaakt (gemeente);
- om te voldoen aan de wettelijke eis voldoen om medische gegevens van kinderen digitaal vast te leggen in het Digitaal Dossier Jeugdgezondheidszorg (DD JGZ) zoekt men een partij die alles voor een operationele (SaaS) applicatie verzorgt (veiligheidsregio);
- het beschikbaar stellen van een website waarop kiesgerechtigden zich ten behoeve van de waterschapsverkiezingen kunnen oriënteren op een politieke partij (waterschap);
- het leveren van hardware voor eindgebruikers (waaronder tablets, laptops, desktops, mobiele telefoons en accessoires) en servers voor de centrale infrastructuur (provincie).

Toetsingskader

Het onderzoek is gebaseerd op de gepubliceerde, openbare informatie over de aanbestedingen. Dit sluit aan bij de transparantie die ten grondslag ligt aan het open standaardenbeleid. Bovendien is dat de informatie waarop de aanbieders zich (in elk geval in eerste instantie) hebben moeten baseren. Dat impliceert dat informatie uit bijvoorbeeld een Nota van Inlichtingen ook niet mee mag wegen bij het opmaken van de beoordeling. In tegenstelling tot eerdere jaren is de kwestie van informatie uit de Nota van Inlichtingen overigens dit jaar en vorig jaar in het geheel niet aan de orde geweest bij de beoordelingen.

Daarnaast is onderzocht op welke wijze de verantwoording ('leg uit') over 2017 heeft plaatsgevonden[9].

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

[9] Zie paragraaf 3.4.

Er is voor een aanbesteding sprake van een 'relevante open standaard', als het betreffende ICT-product of -dienst valt binnen het functionele toepassingsgebied van die standaard, en als de aanbestedende organisatie bovendien valt binnen het organisatorische werkingsgebied van de standaard. Voor één aanbesteding kunnen uiteraard meerdere open standaarden relevant zijn.
Of een standaard van toepassing is, hangt dus uitsluitend af van het functioneel toepassingsgebied en het organisatorisch werkingsgebied. Wanneer de aanbestedende organisatie besluit om niet te vragen om één of meer open standaarden die wèl van toepassing zijn, dan moet dit worden vastgelegd in de administratie en moet hierover bovendien verantwoording afgelegd worden in het jaarverslag. Afwijkingen zijn overigens alleen mogelijk bij redenen van bijzonder gewicht.

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

3.2. 'Pas toe' bij feitelijke aanbestedingen in 2017/2018

In totaal had in de beoordeelde 67 aanbestedingen om 555 open standaarden gevraagd moeten worden, feitelijk werd er echter 240 keer om een open standaard gevraagd - dat is dus 43% daarvan (zie de groene rijen middenin tabel 1). Dit is vergelijkbaar met het percentage van de afgelopen jaren (2014/2015: 43% en 2015/2016: 44%, 2016/2017 45%). In 2012 en 2013 lag dit percentage overigens beduidend lager, op respectievelijk 30% en 25%.

Bij 4 van de 67 aanbestedingen (6%; vorig jaar 12%, de grijze kolommen in tabel 1) werd om alle relevante open standaarden gevraagd, dat is 'pas toe' in strikte zin: 1 aanbesteding door een ministerie en 3 aanbestedingen door een ZBO. Daarnaast werd bij 53 aanbestedingen (79%; vorig jaar 69%) gevraagd om een deel van de voor die aanbesteding relevante standaarden. Bij de resterende 10 aanbestedingen (15%; vorig jaar 19%) - waarbij één of meer open standaarden relevant waren - werd om geen enkele open standaard gevraagd.

Deze driedeling is in twee opzichten verder genuanceerd. Enerzijds door onderscheid te maken tussen de voor een bepaalde aanbesteding *cruciale* open standaarden en de andere relevante open standaarden. Anderzijds kan bij de aanbesteding op meer algemene wijze aandacht besteed zijn aan open standaarden. Dit leidt tot zeven categorieën voor de mate waarin aanbestedingen voldoen aan het open standaardenbeleid:

- er is om alle relevante open standaarden gevraagd (6%),
- er is om een deel van de relevante open standaarden gevraagd, onderverdeeld in:
    - er is om alle cruciale open standaarden gevraagd maar om één of meer andere open standaarden niet (9%),
    - er is om open standaarden gevraagd, maar om minimaal één cruciale niet (70%),
- er zijn geen relevante open standaarden gevraagd, onder te verdelen in:
    - er wordt alleen verwezen naar architectuur-kaders (3%),
    - er wordt in algemene zin aandacht besteed aan open standaardenbeleid (0%),
    - er is geen aandacht voor open standaardenbeleid (12%),
    - de aanbesteding is strijdig met het open standaardenbeleid (0%).

Tabel 1: 'Pas toe' en 'leg uit' bij feitelijke aanbestedingen 2017/2018

(Bron: onderzoek feitelijke aanbestedingen juli 2017 t/m juni 2018, uitgevoerd zomer 2018)

	Ministeries + Uitvoerings-organisaties		Gemeenten + Provincies + Waterschappen		**Totaal 2017 / 2018**		Totaal 2016 / 2017	
	totaal	in %	totaal	in %	**totaal**	in %	totaal	in %
aanbestedingen waarbij OS relevant	*34*	*100 %*	*33*	*100 %*	**67**	*100 %*	*52*	*100 %*
alle relevante OSn gevraagd	**4**	**11 %**	**0**	**0 %**	**4**	**6 %**	**6**	**12 %**
deel van relevante OSn gevraagd	**24**	**71 %**	**29**	**88 %**	**53**	**79 %**	**36**	**69 %**
* cruciale OSn gevraagd	5	(15 %)	1	(3 %)	**6**	(9 %)	11	(21 %)
* OSn gevraagd, maar cruciale niet	19	(56 %)	28	(85 %)	**47**	(70 %)	25	(48 %)
geen relevante OSn gevraagd	**6**	**18 %**	**4**	**12 %**	**10**	**15 %**	**10**	**19 %**
* alleen architectuur-kaders	1	(3 %)	1	(3 %)	**2**	(3 %)	0	(0 %)
* algemene aandacht aan OSn-beleid	0	(0 %)	0	(0 %)	**0**	(0 %)	0	(0 %)
* geen aandacht voor OSn-beleid	5	(15 %)	3	(9 %)	**8**	(12 %)	8	(15 %)
* strijdig met OSn-beleid	0	(0 %)	0	(0 %)	**0**	(0 %)	2	(4 %)
totaal aantal relevante OSn	278	100 %	277	100 %	**555**	100 %	317	100 %
* aantal cruciale relevante OSn	213	77 %	198	71 %	**411**	74 %	198	62 %
totaal aantal gevraagde relevante OSn	138	50 %	102	37 %	**240**	43 %	142	45 %
* niet alle OSn gevraagd => Leg Uit vereist	30	(83 %)	33	(100 %)	**63**	(94 %)	46	(88 %)
cruciale OSn wel gevraagd	5		1		**6**		11	
Leg Uit in jaarverslag beslist vereist	25		32		**57**		35	
- idem, maar beperkt tot Q3+Q4 2017 [10]	*13*	*(100 %)*	*15*	*(100 %)*	**23**	*(100 %)*	*20*	*(100 %)*
- concrete verantwoording in jaarverslag	*0*	*(0 %)*	*0*	*(0 %)*	**0**	*(0 %)*	*0*	*(0 %)*
- beperkte verantwoording in jaarverslag	*2*	*(15 %)*	*0*	*(0 %)*	**2**	*(9 %)*	*3*	*(15 %)*
- geen Leg Uit in jaarverslag	*11*	*(85 %)*	*15*	*(100 %)*	**21**	*(91 %)*	*17*	*(85 %)*
Totaal	34	100 %	33	100 %	**67**	100 %	52	100 %

NB: groen gemarkeerde deel betreft aantallen standaarden, rest van tabel aantallen aanbestedingen

Ook dit jaar blijken er verschillen te zijn tussen Rijk en uitvoeringsorganisaties enerzijds en de mede-overheden (gemeenten, provincies, waterschappen) anderzijds. Het zijn dit jaar echter andere verschillen dan vorig jaar. Vorig jaar waren de scores van de mede-overheden beduidend minder goed dan die van het Rijk, dit jaar is dàt verschil minder groot.

Bij 11% van de aanbestedingen door Rijk en uitvoeringsorganisaties werd om alle relevante standaarden gevraagd (vorig jaar nog 17%). Bij de decentrale overheden is bij geen enkele onderzochte aanbesteding om alle relevante standaarden gevraagd (vorig jaar evenmin, het jaar daarvoor nog bij 17%). Bij 71% van de Rijks-aanbestedingen – min of meer

[10] Controle op de toepassing van 'leg uit' heeft alleen kunnen plaatsvinden over de aanbestedingen uit 2017, waarover verantwoording had moeten worden afgelegd in het Jaarverslag 2017.

vergelijkbaar met vorig jaar – is om een deel van de relevante open standaarden gevraagd, tegen 88% voor de decentrale overheden. Met name de midden-categorie 'relevante standaarden gevraagd maar minimaal één cruciale niet' is bij de mede-overheden sterk gestegen en erg groot geworden: dit jaar 85% van de aanbestedingen (vorig jaar: 47%).

Bij 18% van de Rijks-aanbestedingen werd om geen enkele relevante standaard gevraagd, tegen 12% voor de decentrale overheden. Het percentage aanbestedingen waarbij om geen enkele open standaard werd gevraagd is voor het Rijk opgelopen van 11% vorig jaar naar 18% dit jaar, voor de decentrale overheden is juist flink teruggelopen van 36% naar 12%.

Uit het horizontaal met groen gemarkeerde blok in de tabel valt op dat driekwart van de relevante standaarden (74%) door de beoordelaars als cruciaal worden aangemerkt. Dat is het geval als de betreffende standaard van belang is voor de *kern* van de applicatie. Vorig jaar was dit aandeel lager, toen was 62% van de relevante standaarden cruciaal. Met een score van 74% komen we weer in de buurt van de score van twee jaar terug (79%). Met betrekking tot dit verschil het volgende:

- het aantal standaarden dat per aanbesteding *relevant* wordt geacht, ligt dit jaar duidelijk hoger dan vorig jaar (gemiddeld ruim 8 standaarden per aanbesteding, vergeleken met gemiddeld 6 standaarden per aanbesteding in de voorafgaande jaren) en deze stijging manifesteert zich zowel bij het Rijk als bij de mede-overheden;
- ook de stijging van het aandeel *cruciale standaarden* daarbinnen manifesteert zich zowel bij het Rijk – van 66% naar 77% – als bij de mede-overheden (van 55% naar 71%).

Tot slot is opvallend aan tabel 1 dat ook het aandeel bevraagde standaarden voor het Rijk en mede-overheden weer wat meer naar elkaar toe beweegt. Twee jaar geleden scoorden Rijk en mede-overheden nog gelijk (44%), maar vorig jaar was de score van het Rijk bijna twee maal zo hoog als van de mede-overheden (54% tegenover 28%). Dit jaar is het verschil kleiner: 50% voor Rijk en 37% voor mede-overheden. Ook hier nemen dus de grote onderlinge verschillen van vorig jaar weer af.

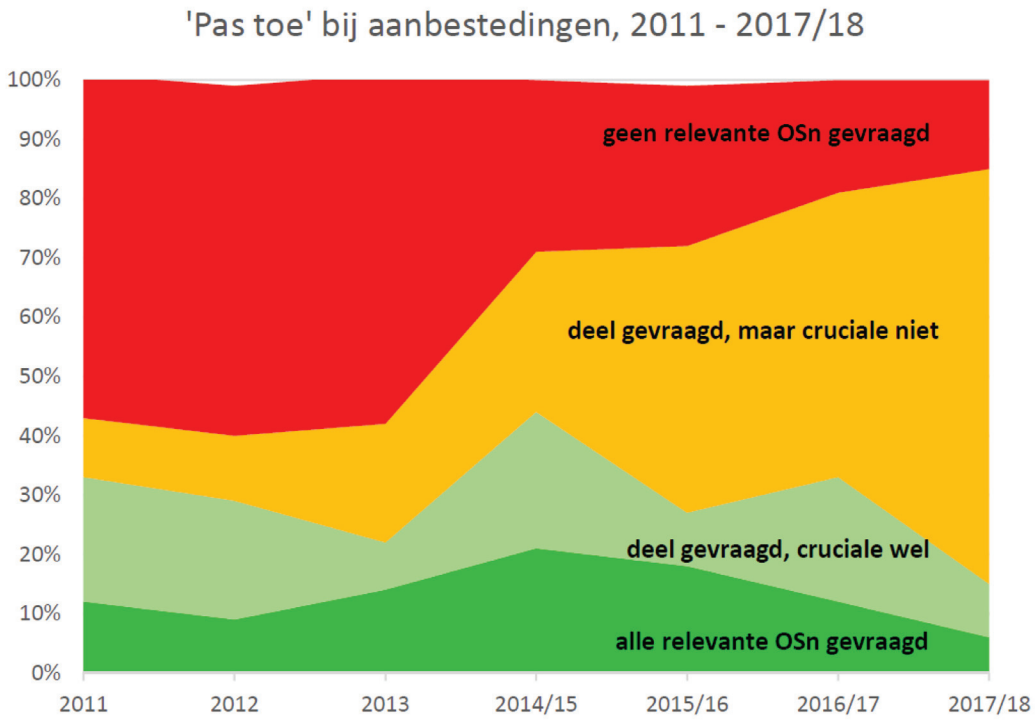
Op basis van tabel 1 en de cijfers van de voorgaande jaren is de ontwikkeling als volgt:

- Het aantal aanbestedingen waarbij om alle relevante standaarden is gevraagd is afgenomen, van 12% vorig jaar naar nu 6%. Dit is het derde jaar op rij dat in deze categorie sprake is van een afname (drie jaar geleden lag dit percentage nog op 21%). De daling dit jaar is toe te schrijven aan het feit dat bij Rijk sprake is van een terugloop van 17% naar 11%; de score voor mede-overheden lag al op 0% en daarin is dit jaar geen verandering gekomen.
- Voor het aantal aanbestedingen waarbij om geen enkele standaard is gevraagd is sprake van een duidelijke verbetering: een daling 19% naar 15%, nadat vorig jaar ook al sprake was van een daling, toen van 27% naar 19%. Deze verbetering dit jaar wordt volledig gerealiseerd bij de mede-overheden waar sprake is van een daling van 35% naar 12% dit jaar. Bij Rijk is juist sprake van een wat minder goede score: 18% dit jaar tegen 11% vorig jaar.
- Omdat bovenstaande twee categorieën teruglopen laat de middencategorie – een deel van de relevante standaarden gevraagd – een oplopend percentage zien, overigens net als vorig jaar: een stijging van 69% naar 79% (vorig jaar: van 55% naar 69%). De verschuiving *binnen* deze middencategorie is niet echt gunstig:

- wel gevraagd om alle cruciale open standaarden maar om één of meer andere niet: teruggelopen van 21% vorig jaar naar 9% nu en daarmee terug op het oude niveau van 2 jaar terug, waarbij moet worden opgemerkt dat de schommelingen in deze categorie een grillig beeld vertonen (drie jaar geleden immers 23%);
- gevraagd om open standaarden, maar om minimaal één cruciale niet: van 48% vorig jaar naar maar liefst 70% dit jaar.

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

Figuur 2: 'Pas toe' bij feitelijke aanbestedingen 2011 - 2017/2018

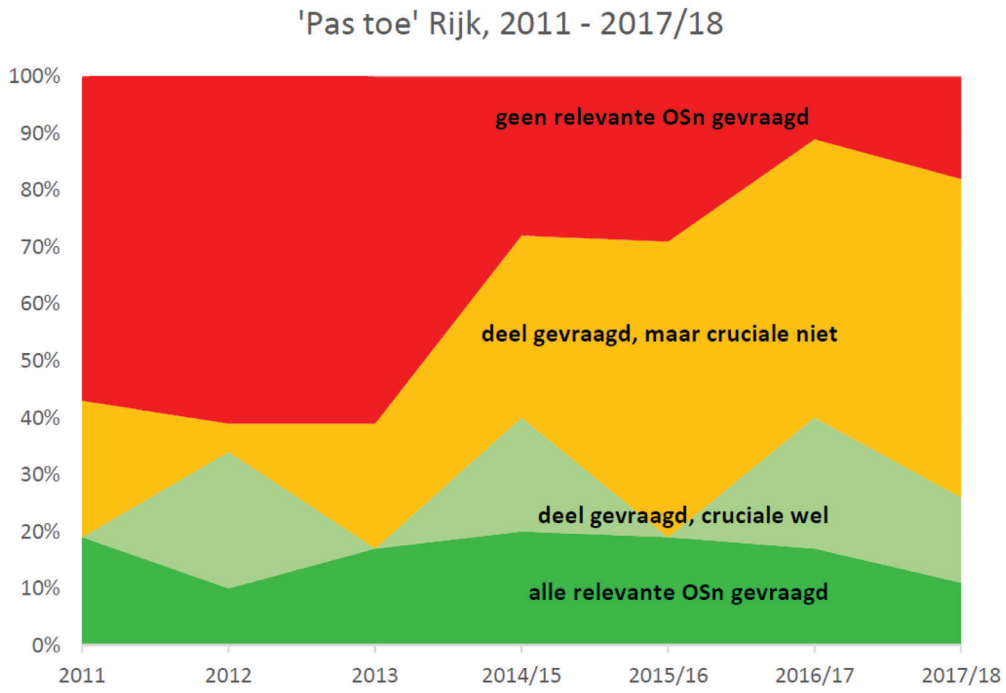


Het goede nieuws uit deze figuur is dat het aantal aanbestedingen waarvoor geen enkele standaard is gevraagd (rood) is gedaald in vergelijking met vorig jaar. Het aandeel daalde van 19% vorig jaar naar 15% dit jaar. Daarmee zet de verbetering verder door, na met name een forse verbetering in de monitor 2014/2015. In de periode daarvóór (2011-2013) was het percentage altijd net onder de 60%.

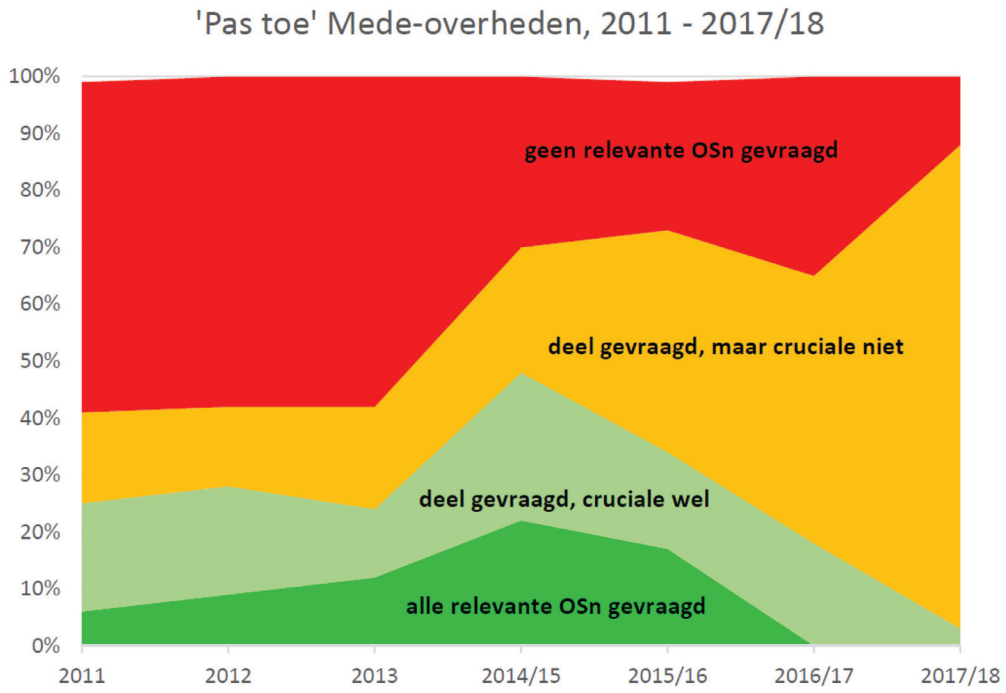
Minder gunstig is de ontwikkeling aan de andere kant van het spectrum. Zowel het aandeel donkergroen als lichtgroen loopt terug. Het percentage 'alle standaarden gevraagd' (donkergroen) loopt net als in vorige jaren enigszins terug, nu van 12% naar 6%. Maar ook het aandeel lichtgroen ('alle als cruciaal aangemerkte standaarden gevraagd maar een of meer andere standaarden niet') loopt terug, van 21% naar 9%. Voor het lichtgroene en het donkergroene deel samen – alle cruciale open standaarden zijn gevraagd – gaat de score dit jaar (15%) de verkeerde kant op, dat is nog niet eerder zo laag geweest. Dit is mogelijk te verklaren doordat (a) er per aanbesteding meer standaarden relevant zijn (gemiddeld 8 in plaats van 6) èn (b) een groter deel daarvan als cruciaal is aangemerkt (74% in plaats van 62%). Daardoor is het dit jaar moeilijker om één van de 'groene' scores te behalen.

Deze ontwikkeling kan ook worden uitgesplitst naar Rijk en uitvoeringsorganisaties, respectievelijk mede-overheden. Daaruit blijk dat de ontwikkeling binnen die beide categorieën door de jaren heen een verschillend beeld laat zien – zie figuur 3a en 3b.

Figuur 3a: 'Pas toe' bij aanbestedingen Rijk 2011 - 2017/2018



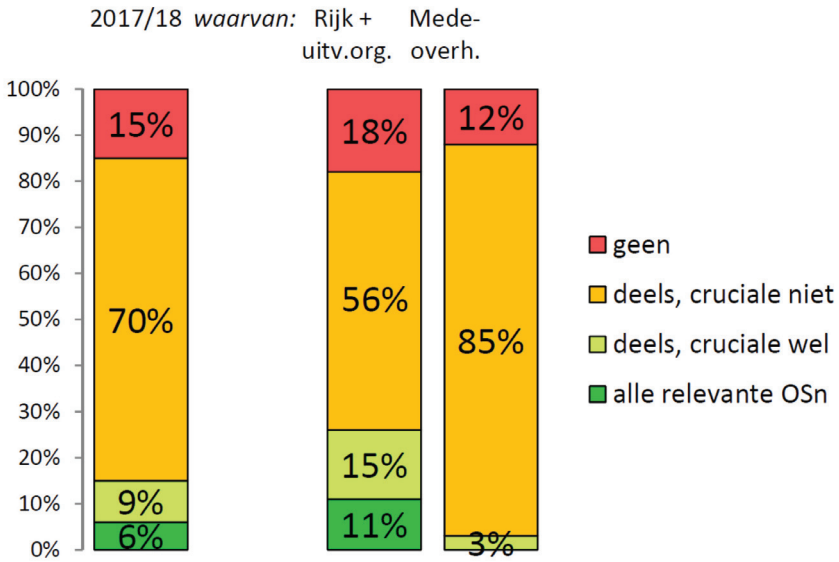
Figuur 3b: 'Pas toe' bij aanbestedingen Mede-overheden 2011 - 2017/2018



Dit jaar is (bewust) het aantal aanbestedingen door mede-overheden verdubbeld. Uit een nadere analyse blijkt dit slechts een beperkte invloed te hebben op de totaal-cijfers.

In figuur 4 (rechts) is duidelijk te zien dat de verschillen tussen enerzijds Rijk en uitvoerings-organisaties en anderzijds mede-overheden groot zijn: bij 56% van de Rijks-aanbestedingen werd om een deel van de relevante standaarden gevraagd maar om tenminste één cruciale niet (mede-overheden: 85%), bij 11% werd om alle relevante standaarden gevraagd (mede-overheden: 0%) en bij 15% om alle cruciale standaarden (mede-overheden: 3%).

Figuur 4: 'Pas toe' bij aanbestedingen: uitsplitsing Rijk vs. mede-overheden 2017/2018



Enkele goede voorbeelden

Net als in de vorige monitors brengen we ook nu weer enkele goede voorbeelden van aanbestedingen die in lijn zijn met het open standaardenbeleid voor het voetlicht. Het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties is net als vorig jaar terug te vinden in dit rijtje, met een A-score (alle relevante standaarden uitgevraagd) bij een aanbesteding met een complex beeld van relevante standaarden. Om dezelfde reden staat ook Zorginstituut Nederland (ZIN) erbij. En als derde krijgt scoorde ook de gemeente Molenwaard uitstekend volgens de onderzoekers.

Ministerie van BZK: Het Huis voor Klokkenluiders zocht een onafhankelijke ICT-dienstverlener om deze kleine organisatie op ICT-gebied te ontzorgen en een digitale werkomgeving bij onder te brengen. De werkzaamheden van Het Huis zijn zeer vertrouwelijk. De aanbesteding omvat het leveren van een beveiligde digitale werkomgeving, ICT-infrastructuurdiensten/hosting, hardware met software voor werkplekken (incl. onderhoud en beheer), en koppelingen met het SaaS-systeem en Citrix-werkomgeving.
Alle 12 (!) open standaarden die relevant worden geacht, zijn ook uitgevraagd: DNSSEC, IPv4/6, ISO 27001/27002, SAML, HTTPS & HSTS, WPA2 Enterprise, SPF, DKIM, DMARC en – minder cruciaal – ODF en PDF. In de aanbestedingsstukken wordt op veel plaatsen verwezen naar het gebruik van open standaarden en men verwijst naar de 'Pas toe of leg uit'-lijst van het Forum Standaardisatie. Ook worden de aanbieders nadrukkelijk aangespoord om het gebruik van niet algemeen geaccepteerde standaarden te vermijden.

Zorginstituut Nederland: het leveren, onderhouden en doorontwikkelen van een volledige e-HRM oplossing, die geïmplementeerd moet worden bij Zorginstituut Nederland. Daarnaast betreft het de verwerking van salarissen en het ter beschikking stellen van een tweedelijns helpdesk. De processen die het systeem moet begeleiden zijn performance management, uitstroom, verzuim- & verlofregistratie, personeelsregistratie, doorstroom en overkoepelende processen.
In de aanbesteding is naar alle (in totaal 11 !) relevante open standaarden gevraagd: Digitoegankelijk, HTTPS & HSTS, TLS, ISO 27001/27002, ODF, PDF, en minder cruciaal: SAML, SPF, DKIM en DMARC. (Van ZIN is overigens nog één andere aanbesteding ten behoeve van deze monitor beoordeeld. Ook daar was sprake van een A-score, zij het dat in dat geval alleen de ISO-standaarden relevant waren.)

Gemeente Molenwaard: de gemeenten Giessenlanden en Molenwaard vormen samen de nieuwe gemeente Molenlanden. Voor deze nieuwe gemeente is men op zoek naar een partij voor het leveren, inrichten, implementeren, koppelen, operationaliseren, in stand houden en doorontwikkelen van één nieuw burgerzakensysteem. Tevens dienen de huidige twee basisregistraties samengevoegd te worden tot één nieuwe Basisregistratie personen voor de gemeente Molenlanden.
De volgende standaarden worden relevant geacht: Digikoppeling, Digitoegankelijk, DNSSEC, HTTPS & HSTS, TLS, ISO 27001 / 27002, StUF, PDF en SAML. De experts die de aanbesteding hebben beoordeeld merken het volgende op. "*Alle standaarden zijn gevraagd, behalve Digitoegankelijk en DNSSEC. Zonde, want het is verder een goed voorbeeld van hoe het wel moet! Er wordt goed aandacht besteed aan het gebruik van open standaarden. Men verwijst expliciet naar het open standaardenbeleid en de 'pas toe of leg uit' lijst van het Forum Standaardisatie. Ook moet de geleverde software binnen twaalf maanden geconformeerd zijn aan nieuwe releases van de open standaarden van het Forum Standaardisatie.*"

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. Van alle relevant geachte standaarden (bij 67 aanbestedingen was dit jaar 555 keer een open standaard relevant) is in 240 gevallen (43%) 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 ligt dit jaar gemiddeld beduidend hoger dan vorig jaar (8,3 dit jaar tegen 6,1 standaarden per aanbesteding vorig jaar[11]);
- het percentage uitgevraagd ligt met 43% iets lager dan vorig jaar (2017: 45%)[12];
- de combinatie van bovenstaande twee punten betekent enerzijds dat er dit jaar per aanbesteding meer standaarden zijn uitgevraagd dan vorig jaar (3,6 versus 2,7);
- maar er zijn ook meer relevant geachte standaarden NIET uitgevraagd: het gemiddelde aantal niet-gevraagde standaarden ligt per aanbesteding dit jaar op 4,7 (vorig jaar: 3,4).

[11] Het aantal standaarden op de lijst voor 'pas toe of leg uit' is min of meer vergelijkbaar met vorig jaar. Let wel: de standaarden die in november 2017 en in mei 2018 op de lijst zijn geplaatst, zijn nog niet in de beoordeling meegenomen.
[12] In 2016 was dit 44% en in 2015 43%; dat was toen een flinke verbetering ten opzichte van het jaar daarvoor (25%).

Tabel 5: 'Pas toe' bij feitelijke aanbestedingen in 2017 / 2018, per standaard

(Bron: onderzoek feitelijke aanbestedingen juli 2017 t/m juni 2018, uitgevoerd zomer 2018)

4 x ≥ 75 % 14 x 25-75 % 9 x < 25 %	Ministeries + Uitvoerings-Organisaties		Gemeenten + Provincies + Waterschappen		**Totaal 2017/2018**		*Totaal 2016/2017*
aantal aanbestedingen: n =	*34*		*33*		*67*		*52*
	relevant	comply: gevraagd in % van relevant	relevant	comply: gevraagd in % van relevant	relevant	comply: gevraagd in % van relevant	comply: gevraagd in % van relevant
Internet & beveiliging:							
DKIM	16	44 %	7	14 %	23	35 %	0 %
DMARC	16	44 %	7	14 %	23	35 %	
DNSSEC	10	30 %	8	12 %	18	22 %	21%
HTTPS & HSTS	29	66 %	31	29 %	60	47 %	
IPv6 en IPv4	12	17 %	13	15 %	25	16 %	42 %
NEN-ISO\IEC 27001:2005nl	33	67 %	33	70 %	66	68 %	63 %
NEN-ISO\IEC 27002:2007nl	33	48 %	33	58 %	66	53 %	62 %
SAML	11	64 %	14	43 %	25	52 %	40 %
SPF	16	44 %	7	14 %	23	35 %	0 %
STARTTLS en DANE	1	0 %	0		1	0 %	0 %
TLS	29	66 %	31	19 %	60	42 %	57 %
WPA2 Enterprise	2	50 %	1	0 %	3	33 %	0 %
Document & (web)content:							
Ades	1	100 %			1	100 %	
CMIS	2	0 %	3	33 %	5	20 %	20 %
Digitoegankelijk *)	16	44 %	9	56 %	25	48 %	58 %
ODF 1.2	15	20 %	14	7 %	29	14 %	12 %
OWMS	1	0 %			1	0 %	100 %
PDF **)	21	67 %	20	50 %	41	59 %	50 %
SKOS							
E-facturatie & administratie:							
Sem. Model e-Factureren	1	0 %	2	50 %	3	33 %	33 %
SETU	1	100 %			1	100 %	
WDO Datamodel							
XBRL v2.1	4	25 %	4	0 %	8	13 %	33 %
Stelselstandaarden:							
Digikoppeling	3	33 %	17	24 %	20	25 %	33 %
Geo−standaarden	1	0 %	1	0 %	2	0 %	0 %
StUF	1	0 %	15	80 %	16	75 %	50 %
Water & Bodem:							
Aquo Standaard			2	50 %	2	50 %	0 %
SIKB 0101			1	100 %	1	100 %	
SIKB 0102							
Bouw:							
IFC							
Visi							
Juridische verwijzingen:							
BWB							100 %
ECLI							
JCDR							
Onderwijs & loopbaan:							
E−portfolio	3	0 %	4	0 %	7	0 %	0 %
NL LOM							0 %
Overig:							
EMN_NL							
STOSAG							0 %
Totaal	**278**	**50 %**	**277**	**37 %**	**555**	**43 %**	**45 %**

**) Voorheen: Webrichtlijnen. Net als voorgaande jaren alleen beoordeeld voor externe webapplicaties.*
***) Bij de beoordelingen is geen onderscheid gemaakt tussen de verschillende PDF-varianten.*

Dit is ook terug te zien in de scores voor 'Pas toe' per afzonderlijke standaard (zie tabel 6). Het aantal standaarden waarop beter wordt uitgevraagd dan vorig jaar houdt ongeveer gelijke tred met het aantal standaarden waar juist het omgekeerde het geval is: een minder goede uitvraag (procentueel gezien) dan vorig jaar:

- zeven standaarden werden vaker dan gemiddeld gevraagd: ISO 27001/02, HTTPS & HSTS, SAML, PDF, StUF en Digitoegankelijk (voorheen: Webrichtlijnen). TLS valt hier net buiten met een uitvraag-percentage van 42% (gemiddeld 43%).
- Ades, SETU en SIKB01 scoren in de tabel weliswaar een uitvraag-percentage van 100% maar voor deze standaarden geldt dat die slechts één maal als relevant zijn aangemerkt.
- Met name de mate waarin gevraagd werd om DKIM, SPF en DMARC is sterk verbeterd, zowel bij het Rijk als bij de mede-overheden, met een score van 35% tegen 0% vorig jaar.
- Andere standaarden die een duidelijke stijging van de uitvraag laten zien, zijn StUF, SAML en PDF. Ter vergelijking: vorig jaar stonden DKIM en StUF nog vermeld bij de dalers;
- vijf standaarden laten een tegenovergesteld beeld zien met een relatief flinke daling: hiervan is met name sprake bij IPv4/6 (na juist een inhaalslag de goede kant op vorig jaar) en in wat mindere mate bij TLS, Digitoegankelijk, de ISO-27002 en Digikoppeling.

3.4. 'Leg uit' bij feitelijke aanbestedingen

Voor twee sets van beoordeelde aanbestedingen is nagegaan in hoeverre 'leg uit' plaatsgevonden heeft in jaarverslagen over 2017: de aanbestedingen uit Q3 en Q4 2017 die in deze Monitor 2018 zijn beoordeeld èn de set aanbestedingen uit Q1 en Q2 2017 die vorig jaar zijn beoordeeld (in het kader van de Monitor 2017).

Bij vier aanbestedingen die in het kader van deze monitor 2018 zijn beoordeeld, is om alle relevante standaarden gevraagd. Bij de andere 63 aanbestedingen had dus in het jaarverslag verantwoording afgelegd moeten worden ('Leg uit') voor het niet toepassen van de betreffende relevante standaard(en). Bij zes daarvan is wèl om de (voor die aanbesteding) cruciale relevante open standaarden gevraagd, en is alleen niet gevraagd om enkele minder cruciale open standaarden.

Voor de resterende 57 aanbestedingen (door 46 verschillende overheidsorganisaties) is 'Leg uit' zonder twijfel vereist, omdat hierbij niet gevraagd werd om één of meer van de relevante cruciale open standaarden (47 aanbestedingen) of zelfs om geen enkele relevante standaard gevraagd is (10 aanbestedingen).

Van deze 57 aanbestedingen is het voor 28 aanbestedingen (door 24 overheidsorganisaties, waarvan dit jaar niet meer dan 3 ministeries[13]) op dit moment mogelijk om in het Jaarverslag 2017 te controleren of 'leg-uit' is toegepast; deze 28 aanbestedingen dateren uit Q3 – Q4 2017. Voor de resterende 29 aanbestedingen kan dat pas na het verschijnen van de jaarverslagen over 2018. Van 'Leg uit' was in de jaarverslagen van deze 24 overheids-organisaties echter geen sprake, in geen van de jaarverslagen wordt een concrete aanbesteding genoemd uit het voorliggende onderzoek waarbij van de lijst voor 'pas toe of leg uit' werd afgeweken.

[13] Te weten de ministeries van BZK, Defensie en Financiën (lees: Belastingdienst).

Bij de decentrale overheden waarvan aanbestedingen zijn onderzocht is in de jaarverslagen geen enkele verwijzing naar het standaardenbeleid teruggevonden[14]. Bij de departementen ligt dat genuanceerder. Er is naar de jaarverslagen van alle 11 ministeries en Wonen en Rijksdienst (W&R) gekeken, hoewel strikt genomen alleen de volgende departementen onderwerp van onderzoek zijn: Financiën (lees: Belastingdienst), Binnenlandse Zaken en Defensie. Van deze drie departementen zijn namelijk aanbestedingen beoordeeld uit Q3+Q4 2017, met een beoordeling die noodzaakt tot 'leg uit'. In onderstaand schema zijn deze drie ministeries aangegeven met oranje.

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

- vier ministeries (vorig jaar ook vier) hebben een vorm van verantwoording opgenomen in het jaarverslag 2017;
- daaronder het ministerie van BZK; dit departement heeft niet alleen een alinea over 'pas toe of leg uit' opgenomen, maar meldt bovendien dat zij (conform de Instructie Rijksdienst) een lijst bijhoudt van afwijkingen van de lijst; daarnaast verwijst BZK naar het overzicht dat Logius jaarlijks publiceert met afwijkingen van de lijst voor 'pas toe of leg uit';
- in het jaarverslag van Wonen en Rijksdienst wordt voor de rijksbrede bedrijfsvoerings-onderwerpen (daaronder: open standaarden) verwezen naar het Ministerie van BZK;
- zeven ministeries vermelden niets over open standaarden.

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

Ministerie[15]	**Uitvoering 'leg uit'**
AZ	Het Ministerie van Algemene Zaken heeft geen grote ICT-projecten van meer dan € 5 miljoen uitgevoerd in 2017. Gebruik open standaarden en open source software. Er zijn geen bijzonderheden te melden. *(Bron: B Beleidsverslag onder 3: bedrijfsvoeringsparagraaf, onder 2).* (Vergelijkbare teksten voor Kabinet van de Koning en de Commissie van Toezicht betreffende de Inlichtingen- en Veiligheidsdiensten).
BZK	Het Ministerie van BZK heeft in 2017 gehandeld conform artikel 3, eerste lid van de «Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten». Er zijn in de regel geen nieuwe ICT-diensten of -producten aangeschaft waarbij is afgeweken van de open standaarden op de «pas toe of leg uit»-lijst van het Nationaal Beraad Digitale Overheid. Behoudens noodzakelijke uitbreiding van het aantal gebruikerslicenties voor de bestaande systemen zijn er geen afwijkingen. Logius past relevante open standaarden toe in haar overheidsbrede ICT-producten, zoals Digipoort, MijnOverheid, e-Herkenning en DigiD. Jaarlijks publiceert Logius in zijn online jaaroverzicht een overzicht van de toepassing van open standaarden binnen de Logius-producten met eventuele afwijkingen en toelichting. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf, onder 2)*
BUZA	[Geen]
DEF	[Geen]
EZ	[Geen]
FIN	[Geen. NB: vorig jaar nog wel]

[14] Ook in de gehanteerde (lokale / regionale) beleidskaders met betrekking tot inkoop en aanbesteding is geen verwijzing gevonden naar het hier bedoelde onderliggende beleid.
[15] Bij de benaming van de ministeries worden de in 2017 geldende namen gehanteerd.

IM	Bestuurskern Er wordt gestuurd met de Enterprise Architectuur en de Open Source Software (OSS) strategie actief op de inzet van OSS en op het voldoen aan Open Standaarden. Het Standaard Platform is een goed praktijkvoor-beeld. Het Standaard Platform is volledig gebaseerd op Open Source Software en voldoet aan de Open en Rijksbrede standaarden, zoals opgenomen in de Lijst Open Standaard van het Forum Standaardisatie. Open standaarden ICT-diensten RWS RWS stuurt op de door het Forum standaardisatie vastgestelde open standaarden door toepassing daarvan in Project Start Architecturen (PSA). Deze worden gevolgd voor zover dat mogelijk is bij elke nieuwe ICT-toepassing. Het is traceerbaar welke open standaarden gevolgd worden door middel van de RWS standaardenlijst, waarin ook de standaarden van het Forum Standaardisatie zijn opgenomen. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf, onder 2)*
V&J	[Geen]
OCW	[Geen]
SZW	In 2017 zijn geen afwijkingen gebleken aan de eis van voldoen aan de open standaarden. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf onder 2)*
VWS	[Geen]
WR	*[Niet anders dan de volgende verwijzing:]* Voor de rijksbrede bedrijfsvoeringsonderwerpen wordt u verwezen naar de bedrijfsvoerings-paragraaf van het jaarverslag van begrotingshoofdstuk VII BZK.

'Leg uit' voor aanbestedingen uit Q1+Q2 2017 (vorig jaar beoordeeld)

In de vorig jaar verschenen Monitor 2017 zijn onder andere aanbestedingen beoordeeld uit Q1+Q2 2017. Voor 15 van deze aanbestedingen was 'leg uit' aan de orde maar dat kon op dat moment nog niet onderzocht worden. Dat onderzoek heeft nu plaatsgevonden, omdat de Jaarverslagen 2017 nu wèl beschikbaar zijn.

Deze 15 aanbestedingen (door 14 overheidsorganisaties, waarvan 4 ministeries[16]) zijn vrijwel gelijk verdeeld over 'Rijk' en 'mede-overheden'. Van 'Leg uit' in strikte zin was in de jaarverslagen van deze 14 overheidsorganisaties evenmin sprake. In geen van de jaarverslagen wordt een concrete aanbesteding genoemd waarbij volgens het onderzoek van vorig jaar van de lijst voor 'pas toe of leg uit' werd afgeweken.

Evenals vorig jaar 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 2016 in de monitor 2017 valt op dat bij één departement de verwijzing naar het beleid rond de toepassing van open standaarden is komen te vervallen (het ministerie van Financiën). Vorig jaar was dit het geval met het ministerie van I&M maar daar is deze keer wel weer een verwijzing naar toepassing van open standaarden teruggevonden

De bevindingen met betrekking tot het 'Leg uit' principe in 2017 zijn min of meer gelijk aan de voorgaande jaren (2011 tot en met 2016), met de nuancering zoals hierboven beschreven.

[16] Te weten de ministeries van BZK, Defensie, Financiën (lees: Belastingdienst) en Veiligheid & Justitie.

3.5. Welke open standaarden waren relevant bij feitelijke aanbestedingen

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

Van de 39 standaarden[17] op de lijst voor 'pas toe of leg uit' waren 28 standaarden[18] minimaal bij één aanbesteding relevant (in 2016: 25 van de 38), de andere 11 waren dus voor geen van de 67 onderzochte aanbestedingen relevant. Daarvan waren verreweg de meeste (8) ook vorig jaar voor geen enkele onderzochte aanbesteding relevant: ECLI, JCDR, EMN_NL, WDO Datamodel, SIKB0102, IFC, VISI en SKOS.

Een vijftal standaarden steekt er met kop en schouders bovenuit als het gaat om de mate waarin zij relevant worden geacht: ISO 27001/02 zijn bijna altijd relevant (99%), TLS (90%), HTTPS & HSTS (89%) en PDF (61%). Van deze standaarden stonden er vier ook vorig jaar bovenaan (HTTPS & HSTS werd vorig jaar nog niet meegenomen).

Daarna volgt een groep van vier standaarden die bij 25 of meer aanbestedingen als relevant zijn aangemerkt: SAML, IPv4/IPv6, Digitoegankelijk (voorheen: webrichtlijnen) en ODF. In vergelijking met vorig jaar is er een standaard uit dit rijtje weggevallen (DNSSEC, terwijl dat vorig jaar juist een nieuwkomer was) en is ODF er aan toegevoegd (vorig jaar maakte deze standaard nog deel uit van de kopgroep). Kort achter dit viertal volgt een zestal standaarden tussen de 15 en 25 keer als relevant is aangemerkt: DKIM, DMARC, SPF, DNSSEC, Digikoppeling en StUF.

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 ook 7):

- Geo- en Aquo-standaarden beide twee keer, en
- STARTTLS & DANE, Ades, OWMS, SETU en SIKB0101 één keer.

Eerder in dit hoofdstuk is al opgemerkt dat het aantal relevant geachte standaarden per aanbesteding duidelijk hoger ligt dan vorig jaar. Dit valt ook terug te lezen in tabel 6: de meeste standaarden scoren een hoger percentage ‘relevant’ dan vorig jaar. Uitschieters daarbij zijn DKIM, SPF, Digitoegankelijk, PDF, Digikoppeling, en – in iets mindere mate – TLS, SAML en StUF. Echte uitschieters de andere kant op – veel minder vaak ‘relevant’ dan vorig jaar – zijn er niet: ODF komt nog het meest in de buurt met een daling van 50% vorig jaar naar 43% nu (vorige jaar was ODF ook de meest in het oog springende daler op dit punt).

[17] Op de lijst staan in augustus 2018 2017 44 standaarden, maar COINS, NLCIUS, NLCS, OpenAPI en STIX-TAXII zijn niet meegenomen in de beoordeling omdat deze pas sinds kort op de lijst staan. In de tussenliggende periode is er ook een standaard van de lijst verdwenen: OSI-PMH.
[18] NB: bij het beoordelen van de aanbestedingen is geen onderscheid gemaakt tussen PDF 1.7, PDF/A1 en PDF/A2 terwijl deze wel als drie afzonderlijke standaarden op de lijst staan.

Tabel 6: Open standaarden relevant / gevraagd bij feitelijke aanbestedingen in 2017/2018

(Bron: onderzoek feitelijke aanbestedingen juli 2017 t/m juni 2018, uitgevoerd zomer 2018)

	Ministeries + Uitvoerings-organisaties		Gemeenten + Provincies + Waterschappen		**Totaal 2017/2018**	
aantal aanbestedingen: n =	*34*		*33*		**67**	
	relevant in % van aanbest.n	gevraagd in % van aanbest.n	Relevant in % van aanbest.n	gevraagd in % van aanbest.n	**relevant in % van aanbest.n**	**gevraagd in % van aanbest.n**
Internet & beveiliging:						
DKIM	47 %	21 %	21 %	3 %	**34 %**	**12 %**
DMARC	47 %	21 %	21 %	3 %	**34 %**	**12 %**
DNSSEC	29 %	9 %	24 %	3 %	**27 %**	**6 %**
HTTPS & HSTS	85 %	56 %	94 %	27 %	**89 %**	**42 %**
IPv6 en IPv4	35 %	6 %	39 %	6 %	**37 %**	**6 %**
NEN-ISO\IEC 27001:2005nl	97 %	65 %	100 %	70 %	**99 %**	**67 %**
NEN-ISO\IEC 27002:2007nl	97 %	47 %	100 %	56 %	**99 %**	**52 %**
SAML	32 %	21 %	42 %	18 %	**37 %**	**19 %**
SPF	47 %	21 %	21 %	3 %	**34 %**	**12 %**
STARTTLS en DANE	3 %	0 %			**1 %**	**0 %**
TLS	85 %	56 %	94 %	18 %	**90 %**	**38 %**
WPA2 Enterprise	6 %	3 %	3 %	0 %	**4 %**	**1 %**
Document & (web)content:						
Ades	3 %	3 %			**1 %**	**1 %**
CMIS	6 %	0 %	9 %	3 %	**7 %**	**1 %**
Digitoegankelijk *)	47 %	21 %	27 %	15 %	**37 %**	**18 %**
ODF 1.2	44 %	9 %	42 %	3 %	**43 %**	**6 %**
OWMS	3 %	0 %			**1 %**	**0 %**
PDF **)	62 %	41 %	61 %	30 %	**61 %**	**36 %**
SKOS						
E-facturatie & administratie:						
Sem. Model e-factureren	3 %	0 %	6 %	30 %	**4 %**	**1 %**
SETU	3 %	3 %			**1 %**	**1 %**
WDO Datamodel						
XBRL v2.1	12 %	3 %	12 %	0 %	**12 %**	**1 %**
Stelselstandaarden:						
Digikoppeling	9 %	3 %	52 %	12 %	**30 %**	**7 %**
Geo−standaarden	3 %	0 %	3 %	0 %	**3 %**	**0 %**
StUF	3 %	0 %	45 %	36 %	**24 %**	**18 %**
Water & Bodem:						
Aquo Standaard			6 %	3 %	**3 %**	**1 %**
SIKB 0101			3 %	3 %	**1 %**	**1 %**
SIKB 0102						
Bouw:						
IFC						
Visi						
Juridische verwijzingen:						
BWB						
ECLI						
JCDR						
Onderwijs & loopbaan:						
E−portfolio	9 %	0 %	12 %	0 %	**10 %**	**0 %**
NL LOM						
Overig:						
EMN_NL						
STOSAG						
Totaal	**278**	**50 %**	**277**	**37 %**	**555**	**45 %**

**) Voorheen: Webrichtlijnen. Net als voorgaande jaren alleen beoordeeld voor externe webapplicaties.*
***) Bij de beoordelingen is geen onderscheid gemaakt tussen de verschillende PDF-varianten.*

In vergelijking met de vorige monitor is een drietal standaarden deze keer bij geen enkele aanbesteding relevant gebleken en vorig jaar wel. Dit betreft BWB, NL-LOM en STOSAG, maar daar moet wel bij worden aangetekend dat de relevantie van deze standaarden vorig jaar ook al niet groot was.

Andersom: geen enkele standaarden was dit jaar wel relevant en vorig jaar niet (afgezien van de standaarden die vorig jaar vanwege recente plaatsing op de lijst niet waren meegenomen).

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 ongeveer even vaak om de relevante standaarden gevraagd als vorig jaar: 43% dit jaar tegen 45% vorig jaar. In tabel 6 is voor de afzonderlijke standaarden berekend hoe vaak daarom is gevraagd wanneer de standaard relevant was (in % van het aantal aanbestedingen). De hoogste scores zijn in de betreffende kolom terug te vinden bij: NEN-ISO\IEC 27001/27002 (67% respectievelijk 52%), HTTPS & HSTS (42%) TLS (38%) en PDF (36%). Vorig jaar stonden dezelfde standaarden op dit punt bovenaan (behalve HTTPS & HSTS want die is vorig jaar nog niet in het onderzoek meegenomen).

Na dit rijtje koplopers volgt nog een zestal standaarden met een score van boven de 10%: SAML (19%), StUF (18%), Digitoegankelijk (voorheen: Webrichtlijnen) met 18%, en DKIM, DMARC en SPF met alle drie 12% . Om de andere standaarden is slechts bij enkele aanbestedingen gevraagd of - ten onrechte - zelfs in het geheel niet. Dit laatste is het geval bij STARTTLS en DANE, OWMS, de Geo-standaarden en E-portfolio. Deze 0%-scores doen zich meestal voor bij standaarden die slechts incidenteel (1 of 2 keer) als relevant zijn aangemerkt. Uitzondering hierop is E-portfolio: deze standaard is 7 keer aangemerkt als relevant maar in geen enkel geval uitgevraagd.

4. Toepassing open standaarden via voorzieningen

4.1. Inleiding

De afzonderlijke overheids-organisaties zijn primair zelf verantwoordelijk voor het toepassen van open standaarden. Voor een deel van hun informatiesystemen maken overheden echter gebruik van overheidsbrede voorzieningen (GDI-voorzieningen, shared services etc.). Sommige daarvan worden overheidsbreed toegepast, andere vooral door de Rijksoverheid of juist door mede-overheden. Als daarin de relevante open standaarden zijn toegepast, dan leidt ook dat tot een breder gebruik van open standaarden.

Daarom is ook dit jaar onderzocht in hoeverre de belangrijkste overheidsbrede voorzieningen (35 in totaal) voldoen aan de relevante open standaarden[19]. Hiervoor zijn 26 voorzieningen onderzocht die samen de GDI (Generieke Digitale Infrastructuur) vormen[20]. Anderzijds zijn ook de 9 andere voorzieningen die vorige jaren zijn onderzocht nogmaals onderzocht.

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

Het gaat om de volgende 26 + 9 voorzieningen:

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

Werkwijze

Voor dit onderzoek is gebruik gemaakt van de 'pas toe of leg uit'-lijst van mei 2018. Per voorziening is gekeken of de standaarden op deze lijst relevant zijn. Daarbij is telkens uitgegaan van de eindgebruiker. Dat is diegene die in de keten baat zou moet hebben bij het gebruik van open standaarden. Dit is expliciet zo gekozen, omdat het beleid gericht is op het stimuleren van interoperabiliteit. In eerdere onderzoeken is gebleken dat beheerders van

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

voorzieningen soms terminologie gebruiken zoals 'voorbereid' zijn op een standaard, het 'deels geïmplementeerd' hebben of 'standaard XYZ-ready' zijn. Hiermee bedoelen zij dat ze zelf voldoen aan de standaard of bezig zijn de standaard te implementeren, maar dat de andere partijen in hun keten nog geen gebruik kunnen maken van de standaard. Er is bijgevolg dan ook geen sprake van interoperabiliteit.

Op basis van publiek beschikbare informatie en kennis van experts en van de onderzoekers is een eerste inschatting gemaakt of de voorziening de relevante standaard ook daadwerkelijk ondersteunt. Hiervan is een overzicht gemaakt dat is toegestuurd aan vertegenwoordigers van de voorzieningen. Op basis van hun reactie is de verzamelde informatie aangescherpt. Het resultaat is voorgelegd aan de opdrachtgever en vervolgens in een definitieve versie toegestuurd aan de vertegenwoordigers van de voorzieningen en opgenomen in de rapportage[21]. Daar waar er verschillen van mening zijn over het al dan niet voldoen aan de voorzieningen zijn deze verschillen nader met elkaar besproken. In de gevallen waar de verschillen ook na de gesprekken bleven bestaan, is dit opgenomen in de rapportage.

Aandachtspunten voor de lezer

Status

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

- Ja: De voorziening is conform[22] de standaard,
- Nee: De voorziening is niet conform de standaard,
- Deels: Onderdelen van de voorziening zijn conform, maar niet alle onderdelen[23],
- Gepland: Er zijn concrete plannen (gekoppeld aan een datum) om de voorziening op korte termijn conform te maken aan de standaard.

Relevant of niet relevant

Voor de relevantiebepalingen zijn per standaard de beschrijvingen van het functioneel toepassingsgebied en van het organisatorisch toepassingsgebied, zoals vermeld op de pas-toe-of-leg-uit lijst van het Forum Standaardisatie, gehanteerd[24]. Standaarden die niet relevant zijn voor een voorziening, zijn niet in de tabel opgenomen. In een beperkt aantal gevallen is onder de tabel nog een toevoeging opgenomen over standaarden die in de eerste inschatting wel relevant leken, maar dat bij nadere inspectie (nog) niet zijn. Ook in gevallen waar verwarring zou kunnen ontstaan over de relevantie is een nadere toelichting onder de tabel opgenomen. Daarnaast is voor de standaarden die dit jaar nieuw zijn op de lijst, opgenomen of ze relevant zijn. Deze inschatting is samen met de beheerders van de voorzieningen gemaakt.

---

[21] Zie Bijlage G.

[22] Met 'conform' wordt in dit onderzoek bedoeld dat de standaard door de eindgebruiker te gebruiken is.

[23] Het betekent dus niet dat een voorziening gedeeltelijk aan een standaard voldoet, maar dat een onderdeel van de voorziening helemaal aan de standaard voldoet. Voor alleen dit onderdeel is dan in feite de status "Ja" van toepassing, maar niet voor de overige onderdelen. Idealiter zouden op termijn alle onderdelen van een voorziening aan de relevante standaard moeten voldoen.

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

Webrichtlijnen en Digitoegankelijk

Op 24 mei is het *Tijdelijk besluit digitale toegankelijkheid overheid* gepubliceerd in het Staatsblad. Het besluit, dat de Europese toegankelijkheidsrichtlijn (2016/2102) omzet in bindende nationale regelgeving, treedt per 1 juli 2018 in werking. Het doel is om de toegankelijkheid van websites en mobiele applicaties (apps) van overheidsinstanties te waarborgen. Het besluit maakt deel uit van een breder pakket aan maatregelen dat een inclusieve benadering van digitale overheidsdienstverlening moet realiseren. Uitgangspunt daarbij is dat mensen met en zonder beperking op gelijke basis moeten kunnen deelnemen aan de maatschappij. Als websites goed in elkaar zitten kunnen ze door iedereen worden gebruikt, ook door bezoekers met een beperking.
Het besluit verplicht overheidsinstanties om te zorgen dat hun websites en/of mobiele applicaties toegankelijk zijn conform de geldende standaard EN 301 549, en daarover een actuele toegankelijkheidsverklaring af te geven. Er geldt een gefaseerde toepassing. Nieuwe websites gepubliceerd vanaf 23 september 2018 moeten uiterlijk op 23 september 2019 voldoen. Bestaande website gepubliceerd vóór 23 september 2018 moeten een jaar later voldoen. Mobiele applicaties moeten uiterlijk 23 juni 2021 voldoen.

In deze monitor zijn we, gelet op de invoeringsdatum van 1 juli 2018 en de gefaseerde invoeringssystematiek, nog uitgegaan van de systematiek voor Webrichtlijnen. Concreet: is er een toets uitgevoerd en is er een onderbouwing in de vorm van een toetsingsrapport, een beschrijving van de toets, of een verwijzing naar een certificaat van een inspectie-instelling zoals Accessibility of Waarmerk drempelvrij.nl.

De BIR en ISO 27001/27002

Binnen de rijksoverheid dient elke organisatie een eigen implementatie van de BIR te hebben. De BIR is gebaseerd op ISO 27001. Indien een organisatie voldoet aan de BIR, dan voldoen zij binnen de context van dit rapport ook aan de verplichting om de ISO 27001/2 standaard te gebruiken. Waar er een aparte certificering op het gebied van ISO 27001 is toegekend, geven wij dit apart aan.

TLS

In de toelichting bij deze standaard op de lijst staat de volgende tekst:

> *"TLS 1.2 wordt door experts beschouwd als de meest veilige versie. Deze versie is daarom de norm. Deze is niet echter 'backwards compatible'. Ten behoeve van de interoperabiliteit dienen daarom ook de versies 1.1 en 1.0 toegepast te worden, met name als wederpartijen (nog) niet klaar zijn voor versie 1.2."*

In dit onderzoek krijgen daarom voorzieningen die versie 1.2 (nog) niet ondersteunen de score 'Nee'.

4.2. Overzicht: open standaarden in overheidsbrede voorzieningen

In Tabel 8a + 8b zijn de bevindingen over de 35 onderzochte overheidsbrede voorzieningen in één overzicht samengebracht. In de rapportage van PBLQ, opgenomen in Bijlage G, wordt het beeld van de mate waarin elke voorziening aan de relevante open standaarden voldoet gedetailleerd besproken. Het gaat om de 26 onderzochte GDI-voorzieningen, plus de 9 andere onderzochte voorzieningen.

Per standaard beschouwd

Van alle 44 open standaarden op de 'pas toe of leg uit'-lijst zijn er 30 relevant voor één of meer overheidsbrede voorzieningen. Er zijn 14 open standaarden die voor meer dan 20 voorzieningen relevant zijn: IPv6/IPv4 en DMARC (beide relevant voor 31 voorzieningen), TLS en HTTPS+HSTS (beide relevant voor 28), DNSSEC, NEN-ISO\IEC 27001 en NEN-ISO\IEC 27002 (relevant voor 27), DKIM (relevant voor 25), SPF (23), Digitoegankelijk, PDF/A-1, PDF/A-2 en PDF 1.7 (22) en STARTTLS+DANE (20).

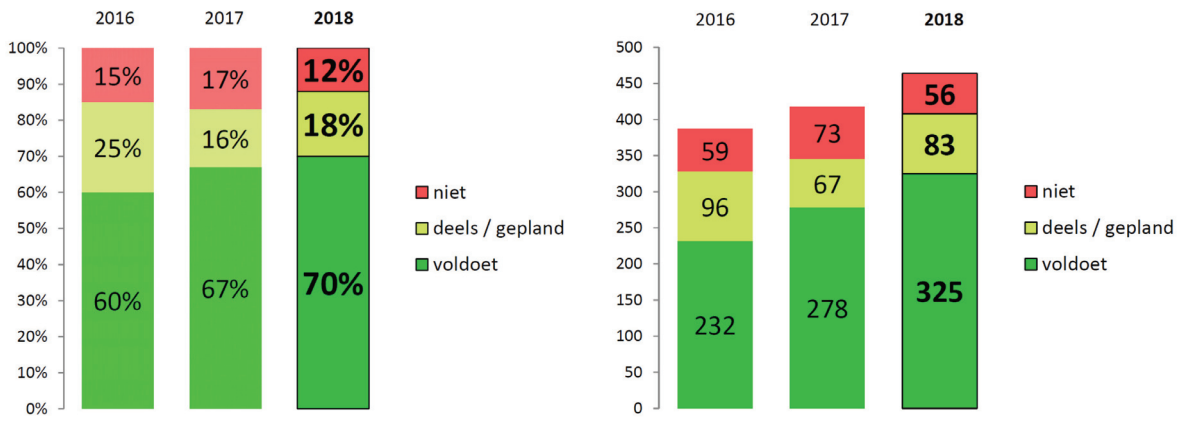
De mate waarin voorzieningen aan de standaard (als die relevant is) voldoen is hoog: voor 15 van de 30 open standaarden geldt dat tenminste 80% van de voorzieningen aan die standaard voldoet. Het gaat om de volgende 15 open standaarden: TLS (26 van de 28 voorzieningen voldoet daaraan), NEN-ISO\IEC 27001 en 27002 (26 van de 27 voorzieningen), DNSSEC (23 van de 27), SPF (20 van de 23), PDF/A-1, PDF/A-2 en PDF 1.7 (19 van de 22), SAML (12 van de 15), Geo-standaarden (alle 5 de voorzieningen), BWB (alle 5), WPA2 Enterprise (alle 3), SETU en XBRL & Dimensions (alle 2) en tenslotte JCDR (relevant voor één voorziening en die voldoet er aan). Daarvan vallen 7 standaarden in het domein 'Internet & beveiliging' en 3 in het domein 'Document & webcontent'.

Zeven standaarden scoren relatief laag: van de voorzieningen waarvoor deze relevant zijn voldoet er geen enkele aan CMIS en NLCIUS, en voldoet 25% van de voorzieningen aan STARTTLS & DANE, 40% van de voorzieningen aan SKOS, 42% aan IPv4&IPv6, 46% aan Digitoegankelijk en 47% aan Digikoppeling.

Per voorziening beschouwd

Voor een deel van de voorzieningen zijn relatief veel open standaarden relevant, zoals voor de NHR (Basisregistratie Handelsregister: 22 standaarden), de basisregistraties BAG, BRK, WOZ, BGT en BRV (20 standaarden), Digitale Werkomgeving Rijk, MijnOverheid, Rijksoverheid.nl en P-Direct (18), Overheid.nl, Doc-Direct en ODC Noord (17) en TenderNed (16). Voor andere voorzieningen, zoals Diginetwerk (5), Samenwerkende Catalogi (4) en e-Factureren (1) zijn slechts enkele open standaarden relevant.

Figuur 7: Toepassing open standaarden in 35 voorzieningen: in % en absolute aantallen



Gemiddeld zijn voor een voorziening ruim 13 open standaarden relevant. Vorig jaar waren dat er nog 12 per voorziening (toen stonden er iets minder standaarden op de lijst) en het jaar daarvoor bijna 11 per voorziening.

In de meeste gevallen voldoen deze voorzieningen ook aan de relevante open standaarden (zie Figuur 7): in 464 gevallen (combinaties van voorziening en relevante standaard) is een standaard van de lijst relevant, in 325 gevallen (70%, vorig jaar 67%) voldoet de voorziening daar aan en in 83 gevallen (18%, vorig jaar was dat 16%) voldoet de voorziening daar deels aan of is dat gepland. In 56 gevallen (12%, vorig jaar 17%) voldoet de voorziening op dit moment nog niet aan een relevante open standaard.

In absolute aantallen (zie rechts in Figuur 7) is het aantal gevallen waarin aan open standaarden wordt voldaan gestegen van 232 in 2016 tot 325 dit jaar.

Bekijken we de voorzieningen apart, dan blijkt dat slechts één voorziening voldoet aan alle relevante standaarden: BasisRegistratie Inkomen (6 standaarden). Daarnaast zijn er negen voorzieningen die aan alle standaarden ofwel voldoen, danwel deels voldoen danwel concrete plannen hebben om daar op korte termijn aan te gaan voldoen (vorig jaar waren dat er 6). Voor 10 van de 35 onderzochte voorzieningen geldt dus, dat zij aan alle standaarden voldoen, deels voldoen of gepland hebben daar op korte termijn aan te gaan voldoen. Negen van deze tien voorzieningen maken deel uit van de Generieke Digitale Infrastructuur.

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

Vergeleken bij twee jaar geleden hebben vooral Digilevering en Digimelding zich sterk verbeterd: twee jaar geleden voldeden zij aan 20% (1 van de 5 relevante standaarden), dit jaar aan 63% (5 van 8). Ook een duidelijke verbetering is er bij: Ondernemersplein (van 42% naar 79% voldoet), BAG, BRK, WOZ en BGT (van 40% naar 75%), MijnOverheid (van 53% naar 94%) en ODC Noord (van 29% naar 47%).

Tabel 8a: Toepassing open standaarden in 35 voorzieningen

		Identificeren & authenticeren						Dienstverlening & informatieverstrekken								
	V = voldoet *D = voldoet deels* *G = gepland* *N = voldoet niet* *(leeg = n.v.t.)*	DigiD	DigiD Machtigen	PKI Overheid	BSN Beheervz + GBA-V (x2)	Stelsel ETD	Rijkspas	MijnOverheid	Berichtenbox bedrijven	Overheid.nl	Ondernemersplein	Samenwerkende Catalogi	Rijksportaal	ODC Noord	Doc-Direct	Rijksoverheid.nl
	aantal relevante OSn:	*12*	*14*	*11*	*14*	*15*	*11*	*18*	*14*	*17*	*14*	*4*	*7*	*17*	*17*	*18*
Internet & beveiliging	DKIM	V				V	G	V	N	V	V			V	V	V
	DMARC	V	V	V		G	N	V	N	V	V	G	V	N	V	V
	DNSSEC	V	V	V		V	G	V	V	V	V			V		V
	HTTPS & HSTS	V	V	V	V	V		V	V	G	V			V	D	V
	IPv4 & IPv6	V	V	G	N	V	N	N	N	V	V		N	D	V	V
	NEN-ISO\IEC 27001	V	V	V	V	V	V	V		V	V			V	V	V
	NEN-ISO\IEC 27002	V	V	V	V	V	V	V		V	V			V	V	V
	SAML	V	D			V	V	V	V				G	G	V	V
	SPF	V	V			V	V	V	N		V				V	V
	STARTTLS & DANE	G				N	N	V		V	N			G		G
	STIX en TAXII															
	TLS	V	V	V	V	V	V	V	V	G	V			V	N	V
	WPA2 Enterprise													V		
Document & (web)content	AdES Baseline Profiles														N	
	CMIS										N				N	
	Digitoegankelijk	V	G			V		V	N	G	V	D		G		V
	ODF 1.2												V	V	N	V
	OpenAPI Specification							V				N				
	OWMS			V						V	N	V		G		V
	PDF 1.7		V	V		V		V	V	V			V	D	V	N
	PDF/A-1		V	V		V		V	V	V			V	D	V	N
	PDF/A-2		V	V		V		V	V	V			V	D	V	N
	SKOS									V					N	
E-facturatie	NLCIUS															
	SETU															
	WDO Datamodel															
	XBRL															
Stelselsta	Digikoppeling		D		N		V	V	V						N	
	Geo-standaarden															
	StUF				N			V	V							
Water &	Aquo-standaarden															
	SIKB 0101															
	SIKB 0102															
Bouw	COINS															
	IFC															
	NLCS															
	VISI															
Juridische	BWB									V	V					V
	ECLI															
	JCDR									V						
Onder	e-Portfolio															
	NL_LOM															
Overig	EML_NL															
	STOSAG															

Tabel 8b: Toepassing open standaarden in 35 voorzieningen

		Gegevens & registreren									Dienstverlening & verbinden						
	V = voldoet *D = voldoet deels* *G = gepland* *N = voldoet niet* *(leeg = n.v.t.)*	NHR (Nieuw HandelsReg.)	BAG, BRK, WOZ en BGT (x4)	BRT (topografie)	BRV (voertuigen)	BRI (inkomen)	Digilevering	Digimelding	Stelselcatalogus	P-Direct	e-Factureren	SBR (Standard Bus. Rep.)	DigiPoort	Diginetwerk	TenderNed	Dig. Werkomgeving Rijk	Digi-Inkoop
	aantal relevante OSn:	*22*	*80*	*10*	*20*	*6*	*8*	*8*	*10*	*18*	*1*	*13*	*12*	*5*	*16*	*18*	*14*
Internet & beveiliging	DKIM	V	V		V	V	V	V		V		G	V		N	D	G
	DMARC	V	V	V	V		G	G	V	V		G	G	V	N	D	G
	DNSSEC	V	V		V		V	V	V	N		V	G	V	V	D	V
	HTTPS & HSTS	D	G	G	G		N	N	N	G			V		V	G	V
	IPv4 & IPv6	D	V		N		G	N	V	N		V	G	G	N	G	N
	NEN-ISO\IEC 27001	V	V	V	V	V				D			V	V	V	V	V
	NEN-ISO\IEC 27002	V	V	V	V	V				D			V	V	V	V	V
	SAML	V			V					V					V	V	
	SPF	V	V		V		V	V		V		V	G		V	V	G
	STARTTLS & DANE	G	G	G	V		V	V				G			N	G	
	STIX en TAXII																
	TLS	V	V	V	V	V				V		V	V		V	V	V
	WPA2 Enterprise					V										V	
Document & (web)content	AdES Baseline Profiles	V								N		V					
	CMIS	D			N												
	Digitoegankelijk	D	V	N	D				V	G		G			N	D	
	ODF 1.2									N						V	
	OpenAPI Specification	G	V		V										N		
	OWMS			N	V												
	PDF 1.7	V	V		V				V	D		V			V	V	V
	PDF/A-1	V	V		V				V	D		V			V	V	V
	PDF/A-2	V	V		V				V	D		V			V	V	V
	SKOS	N	D	V	V				V								
E-facturatie	NLCIUS	N	N								G						G
	SETU												V				V
	WDO Datamodel																
	XBRL											V	V				
Stelselsta	Digikoppeling	V	D		D	V	V	V		V			V			D	
	Geo-standaarden		V	V													
	StUF	V	V														
Water &	Aquo-standaarden																
	SIKB 0101																
	SIKB 0102																
Bouw	COINS																
	IFC																
	NLCS																
	VISI																
Juridische	BWB								V	V							
	ECLI																
	JCDR																
Onder	e-Portfolio																
	NL_LOM																
Overig	EML_NL																
	STOSAG																

5. Open standaarden: gebruiksgegevens

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 *aanbestedingen,* en daarmee op het toepassen van open standaarden bij afzonderlijke toevoegingen aan en vernieuwing van het ICT-systeem van overheden. Gegevens over het feitelijk gebruik geven een beeld voor het gehele ICT-systeem. Bovendien gaat het bij het 'pas toe of leg uit'-regime om het vragen om open standaarden, en wordt niet gemeten in hoeverre het gevraagde ook (volledig) is geleverd. Tenslotte kunnen overheden open standaarden ook toepassen, mogelijk zelfs zonder zich daarvan bewust te zijn, doordat zij voorzieningen of producten gebruiken waarin deze open standaarden toegepast zijn. Voor een completer beeld is het feitelijk gebruik dus een interessante indicator. Helaas is het lang niet altijd even eenvoudig gebleken om (voor alle open standaarden) vast te stellen in welke mate die feitelijk gebruikt worden.

Dit deel-onderzoek is dit jaar voor het eerst uitgevoerd door de accountmanagers van BFS. Dit heeft geleid tot de notitie *'Meer over gebruik van de standaarden van de 'pas toe of leg uit'-lijst'* (zie bijlage E). Daarnaast doet BFS elk halfjaar onderzoek naar internet-veiligheids-standaarden, voor de *'Rapportage 'IV-meting september 2018'* (zie bijlage H). Aanvullende gegevens zijn door BFS aangeleverd in het overzicht *'Gegevens over het gebruik van PDF op basis van crawler'* (zie bijlage F).

5.1. Gebruiksgegevens 2018: inventarisatie door accountmanagers BFS

In de notitie *'Meer over gebruik van de standaarden van de 'pas toe of leg uit'-lijst'* wordt het beeld op basis van de verzameld informatie samengevat in drie indicaties:

- Rood: Er is een negatief beeld over het gebruik van de standaard
- Oranje: Er is een gemengd beeld over het gebruik
- Groen: Er is een positief beeld over het gebruik of de ontwikkeling ervan

In Tabel 9 zijn deze indicaties weergegeven voor de standaarden die niet in de IV-meting zijn opgenomen. Het beeld van BFS is voor 17 standaarden positief: NEN-ISO\IEC 27001 en 27002, SAML, STIX & TAXII, WPA2 Enterprise, NLCIUS, SETU, XBRL, Geo−standaarden, StUF, Aquo Standaard, SIKB 0101, SIKB0102, BWB, ECLI, JCDR en EMN_NL.

Voor acht standaarden is het beeld volgens BFS gemengd: IPv6/IPv4, CMIS, OWMS, SKOS, WDO Datamodel en Visi. En voor negen standaarden ontbreekt informatie of is het beeld negatief: AdEs Baseline Profiles, Digitoegankelijk, ODF 1.2, PDF\A-1, PDF\A-2, PDF1.7, Digikoppeling, IFC, E−portfolio, NL LOM en STOSAG.

Tabel 9: Gebruiksgegevens 2018, per standaard

(Bron: onderzoek door BFS naar gebruiksgegevens zomer 2018, zie Bijlagen E, F en H)

	Beeld BFS	**Resultaten IV-meting**			**'Crawler'**
	(accountmanagers)	afspraak OBDO: 100% eind 2017	eind 2018 (NCSC)	eind 2019 (policy)	
Internet & beveiliging:					
DKIM		84%			
DMARC		73%		policy: 28%	
DNSSEC		90%			
HTTPS en HSTS		HTTPS 89% HSTS 79%	NCSC: 87%		
IPv6 en IPv4	GEMENGD				
NEN-ISO\IEC 27001:2005nl	POSITIEF				
NEN-ISO\IEC 27002:2007nl	POSITIEF				
SAML	POSITIEF				
SPF		93%		policy: 85%	
STARTTLS en DANE		STARTTLS 94% DANE 22%	NCSC: 55%		
STIX & TAXII	POSITIEF				
TLS		96%	NCSC: 87%		
WPA2 Enterprise	POSITIEF				
Document & (web)content:					
AdEs Baseline Profiles	NEGATIEF				
CMIS	GEMENGD				
Digitoegankelijk *)	NEGATIEF				
ODF 1.2	NEGATIEF				zelden
OWMS	GEMENGD				
PDF**)	NEGATIEF				meestal
SKOS	GEMENGD				
E-facturatie & administratie:					
NLCIUS	POSITIEF				
SETU	POSITIEF				
WDO Datamodel	GEMENGD				
XBRL v2.1	POSITIEF				
Stelselstandaarden:					
Digikoppeling	GEMENGD				
Geo−standaarden	POSITIEF				
StUF	POSITIEF				
Water & Bodem:					
Aquo Standaard	POSITIEF				
SIKB 0101	POSITIEF				
SIKB0102	POSITIEF				
Bouw:					
IFC	NEGATIEF				
Visi	GEMENGD				
Juridische verwijzingen:					
BWB	POSITIEF				
ECLI	POSITIEF				
JCDR	POSITIEF				
Onderwijs & loopbaan:					
E−portfolio	NEGATIEF				
NL LOM	GEMENGD				
Overig:					
EMN_NL	POSITIEF				
STOSAG	NEGATIEF				

5.2. Gebruiksgegevens 2018: resultaten IV-meting

In het OBDO hebben de overheden afgesproken dat volledige adoptie voor de volgende standaarden stapsgewijs gerealiseerd moet worden:

- uiterlijk eind 2017: DNSSEC, HTTPS, TLS (web) en DKIM, DMARC, SPF (mail);
- uiterlijk eind 2018: HSTS, HTTPS, TLS: veilige configuratie conform NCSC (web);
- uiterlijk eind 2019: voor DMARC, SPF instellen van strikte policies, STARTTLS&DANE (mail).

Uit de '*Rapportage 'IV-meting september 2018'* (zie bijlage H) blijkt dat het streefbeeld voor eind 2017 nog niet helemaal is gerealiseerd. In tabel 9 zijn deze uitkomsten opgenomen.

Van de vijf webstandaarden wordt TLS het meest toegepast (96%). De toepassing van de andere standaarden is duidelijk gegroeid: DNSSEC tot 90%, HTTPS tot 89%, TLS_NCSC tot 87 % en HSTS tot 79%. De afspraken voor eind 2017 zijn voor TLS dus inmiddels bijna en voor DNSSEC en HTTPS nog niet helemaal gerealiseerd.

Van de negen mailstandaarden worden STARTTLS (94%) en SPF (93%) het meest toegepast, gevolgd door SPF_policy (85%), DKIM (84%) en DMARC (73%). De afspraken voor eind 2017 zijn voor SPF dus inmiddels bijna gerealiseerd, terwijl voor DKIM en vooral DMARC nog een flink stuk te gaan is.

De andere vier mailstandaarden worden op dit moment nog minder vaak gebruikt: DNSSEC_MX (69%), STARTTLS_NCSC (55%), DMARC_policy (28%) en DANE (22%). Voor volledige adoptie van deze standaarden zijn de deadlines echter nog niet verstreken.

5.3. Gebruiksgegevens 2018: indicatieve gegevens ODF en PDF o.b.v. 'crawler'

Bureau Forum Standaardisatie ontwikkelt een 'crawler' die websites afzoekt naar documenten en daarvan het documentformaat vaststelt. Op dit moment is daarvan een bèta-versie beschikbaar. Omdat de crawler nog experimenteel is, kunnen hier nog geen definitieve conclusies aan worden verbonden.

De indicatieve gegevens zijn opgenomen in Bijlage F. Deze zijn niet vergelijkbaar met de gegevens uit de voorgaande monitors, en dus zijn uitspraken over de ontwikkeling in het gebruik niet mogelijk. Een indicatie over het *niveau in 2018* van het gebruik is hieruit wèl af te leiden: de crawler is op de geselecteerde acht websites nauwelijks ODF-documenten tegen gekomen. Op beperkte schaal zijn er ook MS Office-documenten aangetroffen. De meeste documenten hebben een PDF-format, maar onduiudelijk is nog *welk* PDF-format dat dan is.

In de Monitor 2019 zal worden bekeken of de gevonden documenten voldoen aan de eisen van duurzame toegankelijkheid (PDF/A) en digitale toegankelijkheid (digitoegankelijk.nl).

Bijlagen

A. Functioneel toepassingsgebied en organisatorisch werkingsgebied per standaard

B. FAQ Monitor Open standaarden

C. Aanbestedingen: schema 'Pas toe of leg uit' in het kort

D. Overzicht van de beoordeelde aanbestedingen 2017/2018

E. Notitie 'Meer over gebruik van de standaarden van de 'pas toe of leg uit'-lijst' (BFS)

F. Gegevens over het gebruik van PDF op basis van 'crawler' (BFS)

G. Rapportage 'IV-meting september 2018', Bureau Forum Standaardisatie

Separaat:

H. Rapport 'Monitor Open Standaarden Voorzieningen 2018' (Versie 1.1, 13-11-2018), PBLQ

Bijlage A. Functioneel toepassingsgebied en organisatorisch werkingsgebied per standaard

Standaard versienummer *(op lijst sinds)*	**Functioneel toepassingsgebied**	**Organisatorisch werkingsgebied**
Internet & beveiliging		
DKIM RFC 6376 *(15 juni 2012)*	DKIM moet worden toegepast op alle overheidsdomeinnamen waarvandaan wordt gemaild én op alle mailservers waarmee de overheid e-mail verstuurt en ontvangt. Op 24 mei 2018 is de omschrijving van het functioneel toepassingsgebied door het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) opnieuw bekrachtigd.	Overheden en instellingen uit de publieke sector.
DMARC RFC 7489 *(18 mei 2015)*	DMARC moet worden toegepast op alle overheidsdomeinnamen, ook op domeinen waarvan niet wordt gemaild, én op alle mailservers waarmee de overheid e-mail ontvangt. Op 24 mei 2018 is de omschrijving van het functioneel toepassingsgebied door het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) opnieuw bekrachtigd.	Overheden en instellingen uit de publieke sector
DNSSEC RFC 4033, RFC 4034, RFC 4035 *(15 juni 2012)*	DNSSEC moet worden toegepast op alle overheidsdomeinnamen én op DNS-resolvers die clients van overheidsorganisaties direct of indirect van DNS-antwoorden voorzien. Op 24 mei 2018 is de omschrijving van het functioneel toepassingsgebied door het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) opnieuw bekrachtigd.	Overheden en instellingen uit de (semi-) publieke sector.
HTTPS en HSTS RFC 2818, RFC 6797 *(9 mei 2017)*	HTTPS en HSTS moeten worden toegepast op de communicatie tussen clients (zoals webbrowsers) en servers voor alle websites en webservices. Op 24 mei 2018 is de omschrijving van het functioneel toepassingsgebied door het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) opnieuw bekrachtigd.	Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.
IPv6 en IPv4 v4 en v6 *(25 november 2010)*	IPv6 en IPv4 moeten in combinatie ('dual stack') worden toegepast op communicatie tussen toepassingen in (een) netwerk(en). Op 24 mei 2018 is de omschrijving van het functioneel toepassingsgebied door het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) opnieuw bekrachtigd.	Overheden en instellingen uit de (semi) publieke sector.
NEN-ISO\IEC 27001 2013 *(18 mei 2015)*	NEN-ISO/IEC 27001 moet worden toegepast op het formuleren van eisen voor het vaststellen, implementeren, bijhouden en continu verbeteren van een managementsysteem voor informatie-beveiliging en het vaststellen van het toepassingsgebied (de scope) van dit managementsysteem. Op 24 mei 2018 is de omschrijving van het functioneel toepassingsgebied door het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) opnieuw bekrachtigd.	Overheden en instellingen uit de publieke sector.
NEN-ISO\IEC 27002 2013 *(18 mei 2015)*	NEN-ISO/IEC 27002 moet worden toegepast op het formuleren van beheersmaatregelen inzake informatiebeveiliging, hierbij rekening houdend met de omgeving(en) waarin de informatiebeveiligings-risico's gelden. Op 24 mei 2018 is de omschrijving van het functioneel toepassingsgebied door het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) opnieuw bekrachtigd.	Overheden en instellingen uit de publieke sector.
SAML 2.0 *(20 mei 2009)*	SAML moet worden toegepast op de uitwisseling van authenticatie- en autorisatiegegevens om gebruikers na eenmalig inloggen toegang te geven tot meerdere diensten.	Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.
SPF RFC 7208 *(18 mei 2015)*	SPF moet worden toegepast op alle overheidsdomeinnamen, ook op domeinen waarvan niet wordt gemaild, én op alle mailservers waarmee de overheid e-mail ontvangt. Op 24 mei 2018 is de omschrijving van het functioneel toepassingsgebied door het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) opnieuw bekrachtigd.	Overheden en instellingen uit de publieke sector.
STARTTLS en DANE RFC 3207, RFC 7672 *(19 september 2016)*	STARTTLS en DANE moeten in combinatie worden toegepast op ontvangende e-mailservers.	Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-)publieke sector.
STIX en TAXII resp. v1.2.1 en v1.1.1 *(21 november 2017)*	STIX 1.2.1 en TAXII 1.1.1 moeten worden toegepast op de gestructureerde uitwisseling van informatie over digitale dreigingen tegen informatiesystemen.	Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.

Standaard versienummer *(op lijst sinds)*	**Functioneel toepassingsgebied**	**Organisatorisch werkingsgebied**
TLS 1.2, 1.1 en 1.0 *(16 september 2014)*	TLS moet worden toegepast op de uitwisseling van gegevens tussen clients en servers, inclusief machine-to-machine communicatie.	Overheden (Rijk, provincies, gemeenten, en waterschappen) en instellingen uit de publieke sector.
WPA2 Enterprise versie 2 [802.11] *(2 februari 2016)*	WPA2 Enterprise moet worden toegepast op het tot stand brengen van toegang tot WiFi-netwerken, met uitzondering van openbare netwerken voor gastgebruik. Op 24 mei 2018 is de omschrijving van het functioneel toepassingsgebied door het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) opnieuw bekrachtigd.	Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.
Document en (web)Content		
Ades Baseline Profiles Xades 2.1, Pades 2.1, Cades 2.2 en Asic 2.2 *(9 mei 2017)*	De AdES Baseline Profiles moeten worden toegepast op: 1. de ondertekening van XML-, CMS-, PDF- en ZIP-bestanden met geavanceerde en/of gekwalificeerde elektronische handtekeningen, zegels of tijdstempels; 2. de verificatie van deze handtekeningen, zegels en tijdstempels. Op 24 mei 2018 is de omschrijving van het functioneel toepassingsgebied door het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) opnieuw bekrachtigd.	Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.
CMIS 1.0 *(9 december 2014)*	CMIS moet worden toegepast op het ontsluiten van ongestructureerde gegevens in content repositories van content management systemen (CMS'en) en van document management systemen (DMS'en), met als doel deze gegevens uit te wisselen met andere CMS'en en DMS'en. Op 24 mei 2018 is de omschrijving van het functioneel toepassingsgebied door het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) opnieuw bekrachtigd.	Overheden (Rijk, provincies, gemeenten en waterschappen) en overige instellingen uit de publieke sector.
Digitoegankelijk 1.1.2 *(19 oktober 2016)*	Digitoegankelijk (EN 301 549 met WCAG 2.0) moet worden toegepast op het aanbieden van webgebaseerde informatie-, interactie-, transactie- en participatiediensten.	Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.
ODF 1.2 *(15 juni 2012)*	Voor de uitwisseling van reviseerbare documenten.	Overheden en instellingen uit de publieke sector.
OWMS 4.0 *(15 november 2011)*	OWMS moet worden toegepast op het aanbieden van metadata over publieke informatieobjecten op internet. Op 24 mei 2018 is de omschrijving van het functioneel toepassingsgebied door het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) opnieuw bekrachtigd.	Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.
PDF (NEN-ISO) 32000-1 (PDF 1.7) 19005-1 (PDF/A-1) 19005-2 (PDF/A-2) *(18 november 2009)*	PDF moet worden toegepast op de uitwisseling en publicatie van niet- of beperkt reviseerbare documenten. *[Welke van deze standaarden gebruikt moet worden hangt af van de toepassing, zie de toelichting op website BFS]*	Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.
SKOS SKOS W3C Recommandation 18 august 2009 *(18 mei 2015)*	SKOS moet worden toegepast op de publicatie van niet geformaliseerde systemen voor kennisrepresentatie op het internet, met als doel: 1. kennis over de betekenissen en samenhang van de onderliggende begrippen te ordenen en toegankelijk te maken; 2. hergebruik mogelijk te maken. De expertgroep maakt geen kanttekeningen bij het functioneel toepassingsgebied van SKOS. Op 24 mei 2018 is de omschrijving van het functioneel toepassingsgebied door het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) opnieuw bekrachtigd.	Overheden en instellingen uit de publieke sector.

Standaard versienummer *(op lijst sinds)*	**Functioneel toepassingsgebied**	**Organisatorisch werkingsgebied**
Stelselstandaarden		
Digikoppeling 2.0 *(24 mei 2018)*	Digikoppeling moet worden toegepast op alle digitale gegevensuitwisseling met behulp van gestructureerde berichten die plaatsvindt met voorzieningen die onderdeel zijn van de GDI, waaronder de basisregistraties, of die sector-overstijgend is. Geautomatiseerde gegevensuitwisseling tussen informatiesystemen op basis van NEN3610 is uitgesloten van het functioneel toepassingsgebied. Op 24 mei 2018 is de omschrijving van het functioneel toepassingsgebied door het Overheidsbrede Beleidsoverleg Digitale Overheid (OBDO) opnieuw bekrachtigd.	Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-)publieke sector.
Geo−standaarden *(9 december 2014)*	Uitwisseling van geografische informatie tussen organisaties, waarbij de ruimtelijke dimensie van significant belang is.	Overheden, semi-overheden en instellingen uit de publieke sector.
StUF meest recente *(12 november 2008)*	* Uitwisseling en bevraging van basisgegevens die behoren tot een aantal wettelijk vastgestelde basisregistraties, zoals Personen (GBA), Adressen (BRA), Gebouwen (BGA), Kadaster (BRK), Nieuw Handelsregister (NHR) en Waarde Onroerende Zaken (WOZ); * uitwisseling en bevraging van zaakgegevens die behoren tot de producten- en dienstenportfolio van gemeenten; * uitwisseling van domein- of sectorspecifieke gegevens waarin ook basis- en/of zaakgegevens voorkomen en waarvoor geen andere (inter)nationale (XML-gebaseerde) berichtenstandaard is vastgesteld.	Gemeenten en ketens waarbinnen gemeenten participeren.
E-facturatie en administratie		
NLCIUS 1.0 *(25 mei 2018)*	NLCIUS moet worden toegepast op de verzending van elektronische facturen door organisaties die deelnemen aan het economisch verkeer in Nederland (waaronder overheden) welke zijn bestemd voor Nederlandse overheden en instellingen uit de (semi-)publieke sector en de ontvangst hiervan door deze overheden en instellingen.	Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit publieke sector.
SETU resp. 1.2, 1.2, 1.3, 1.3 *(20 mei 2009)*	De elektronische berichtenuitwisseling rondom de bemiddeling/inhuur van flexibele arbeidskrachten	Overheden en instellingen uit de (semi-)publieke sector
WDO Datamodel 3.3 *(15 april 2014)*	Gegevensuitwisseling tussen het bedrijfsleven en de bij grens-overschrijding betrokken overheden om de formaliteiten te vervullen voor de opslag, aankomst, import, doorvoer, export, vertrek en vrijgave van goederen, vervoermiddelen en personen.	Overheden (Rijk, provincies, gemeenten en waterschappen), semi-overheden en instellingen binnen de publieke sector.
XBRL v2.1 en Dimensions v1 *(17 april 2010)*	XBRL v2.1 moet worden toegepast bij de digitale uitwisseling van documenten en berichten dat te kenmerken is als verantwoordingsverkeer en waarin financiële informatie een belangrijke component is.	Overheden en instellingen uit de (semi) publieke sector.
Onderwijs & loopbaan		
E−portfolio NEN 2035:2014 nl *(18 mei 2010)*	Het uitwisselen van informatie over de ontwikkelingsvoortgang van een individu, die het individu als levenslang lerende zelf beheert, tussen organisaties in de leerketen waar het individu leert en werkt.	Overheden en instellingen uit de publieke sector.
NL LOM 1.0 *(29 mei 2011)*	Metadatering van content die ontsloten wordt ten behoeve van educatieve doeleinden.	Alle organisaties die content ontwikkelen, beschikbaar stellen, arrangeren en gebruiken voor educatieve doeleinden alsook leveranciers van applicaties ter ondersteuning van dit proces.
Bouw		
IFC 2x3 TC1 *(15 november 2011)*	Uitwisseling in het kader van bouwwerkinformatiemodellen	Overheden, semi-overheden en instellingen binnen de publieke sector.
Visi 1.4 *(9 december 2014)*	Formele communicatie tussen partijen in de bouwsector, zowel grond- weg en waterbouw, de burger & utiliteitsbouw als de installatiebranche.	Overheden, semi-overheden en instellingen binnen de publieke sector.

Standaard versienummer *(op lijst sinds)*	**Functioneel toepassingsgebied**	**Organisatorisch werkingsgebied**
Water & bodem		
Aquo Standaard Aquo 2018-06 *(17 mei 2016)*	Uitwisselen van uniforme gegevens over water tussen partijen die betrokken zijn bij het waterbeheer voor de kwaliteitsverbetering van het waterbeheer.	Overheden (Rijk, provincies en gemeenten) en instellingen uit de (semi-)publieke sector.
SIKB 0101 13.5 *(9 december 2014)*	Uitwisselen van onderzoeksgegevens over de milieuhygiënische kwaliteit van de bodem en de specifieke gegevens die direct voortkomen uit (of vooruitlopen op) de besluiten die het bevoegd gezag naar aanleiding daarvan heeft genomen	Overheden (Rijk, provincies, gemeenten en waterschappen), semi-overheden en instellingen uit de publieke sector.
SIKB 0102 3.3.0 *(2 februari 2016)*	Voor de digitale uitwisseling van archeologische informatie tussen opgravende instanties, vondstendepots en/of archeologische registers.	Nederlandse overheden (Rijk, provincies en gemeenten) en instellingen uit de (semi-)publieke sector.
Juridische verwijzingen		
BWB 1.3.1 *(2 februari 2016)*	Elektronische verwijzing naar (delen van) geconsolideerde wetten en regelingen met het doel om deze met anderen te delen.	Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.
ECLI 1.0 *(28 november 2013)*	Identificatie van rechterlijke uitspraken, onder meer ter citatie.	Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.
JCDR 1.0 *(28 november 2013)*	Identificatie van geconsolideerde decentrale regelgeving en een gestandaardiseerde manier om hiernaar elektronisch te verwijzen met het doel om deze met anderen te delen.	Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.
Overige open standaarden		
EMN_NL 1.0 *(28 november 2013)*	De definitie en uitwisseling van kandidaatgegevens en uitslaggegevens bij verkiezingen welke onder de Nederlandse Kieswet vallen	Overheden (Rijk, provincies, gemeenten en waterschappen), semi-overheden en andere instellingen uit de publieke sector.
STOSAG 1.0 *(15 november 2011)*	STOSAG moet worden toegepast op digitaal container- en pasmanagement voor afval en grondstoffen.	Gemeenten en gemeentelijke afvalinzamelaars.

Bijlage B. FAQ Monitor Open standaarden

In deze bijlage vindt u een aantal veelgestelde vragen (en het antwoord daarop) over de monitor en over het open standaardenbeleid.

Vragen over de monitor

Q Hoe wordt voor de monitor bepaald of een standaard relevant is voor een aanbesteding?

A *Hiervoor is het functionele toepassingsgebied en het organisatorische werkingsgebied bepalend. Voor de monitor wordt dit bepaald op basis van de openbare documenten van de aanbesteding. Om deze beoordeling te objectiveren wordt tenminste de helft van alle beoordeelde aanbestedingen ook door een tweede expert beoordeeld (second opinion), waarna de eventuele verschillen in de beoordeling besproken worden.*

Q Wat als de aanbestedingsinformatie niet (meer) compleet is?

A *Als de stukken niet meer beschikbaar waren (op TenderNed) is geprobeerd om de stukken via de contactpersoon te achterhalen. Als dat niet gelukt is, dan is de aanbesteding niet beoordeeld.*

Q Onze inkoop-contactpersoon is niet (meer) beschikbaar, krijgen we nu een onvoldoende?

A *Nee. Als de stukken nog op TenderNed beschikbaar zijn is de aanbesteding net als alle andere aanbestedingen op basis van die stukken beoordeeld. Als de stukken niet meer beschikbaar waren en het is niet gelukt om de stukken via de contactpersoon te achterhalen, dan is de aanbesteding niet beoordeeld.*

Q Zijn niet-openbare aanbestedingen ook beoordeeld voor de monitor?

A *Nee. Omdat de stukken van niet-openbare aanbestedingen in veel gevallen niet openbaar beschikbaar zijn, hebben wij dergelijke aanbestedingen niet beoordeeld. NB: Het 'pas toe of leg uit'-regime is overigens wèl van toepassing op niet-openbare aanbestedingen.*

Q Wordt de Nota van inlichtingen meegenomen bij de beoordeling van de aanbesteding?

A *Nee. Het onderzoek is gebaseerd op de (openbare) informatie waarop aanbieders zich in eerste instantie hebben moeten baseren. In de monitor is wel inzichtelijk gemaakt in welke gevallen in de Nota van inlichtingen alsnog de standaarden aan bod kwamen.*

Q Twee jaar geleden liet de monitor een forse verbetering zien (bij meer aanbestedingen is gevraagd om alle of tenminste om alle cruciale open standaarden die relevant zijn). Is er niet gewoon anders (minder streng) gemeten?

A *Nee, dat is niet het geval, om drie redenen:*

- *vorig jaar is bij de aanbestedingen om twee keer zoveel open standaarden gevraagd (en daarop heeft de beoordelaar geen invloed);*
- *de nieuwe hoofdbeoordelaar heeft iets meer open standaarden relevant geacht (en dus niet: minder); dat is niet onlogisch aangezien er nieuwe standaarden bijgekomen zijn;*
- *weliswaar is van hoofdbeoordelaar gewisseld, maar voor de second opinion is (bewust) dezelfde expert gevraagd; en (na enige discussie) waren de hoofdbeoordelaar en de expert het eens over de besproken aanbestedingen (evenals vorige jaren).*

Q Vallen alleen 'harde IT-projecten' binnen scope van de monitor?

A *Nee. Alle aanbestedingen met een duidelijke IT-component vallen binnen de scope van de monitor. Voorbeeld: in een aanbesteding van een communicatieproject, waarbij onder andere een website wordt gemaakt, is 'pas toe of leg uit' van toepassing op de bouw van de website.*

Q Kunnen we niet gewoon in algemene zin verwijzen naar de lijst voor 'pas toe of leg uit'?

A *Nee. Het effectief toepassen van een open standaard vereist, dat bij de aanbesteding expliciet gevraagd wordt om deze standaard. Anders krijgt de aanbieder de verantwoordelijkheid voor het correct toepassen ervan. In de praktijk levert dat niet het beoogde resultaat, omdat de aanbiedingen alleen te beoordelen zijn op het correct toepassen van de lijst als (a) de aanbesteder zelf weet welke open standaarden van toepassing zijn, en (b) de aanbesteder hierom ook expliciet gevraagd heeft.*

Q Kunnen we niet gewoon verwijzen naar de gangbare architectuurkaders van de overheid?

A *Nee, dat is nuttig maar niet voldoende. Het effectief toepassen van een open standaard vereist, dat bij de aanbesteding expliciet gevraagd wordt om deze standaard. Anders krijgt de aanbieder de verantwoordelijkheid voor het correct toepassen ervan. In de praktijk levert dat niet het beoogde resultaat, omdat de aanbiedingen alleen te beoordelen zijn op het correct toepassen van de lijst als (a) de aanbesteder zelf weet welke open standaarden van toepassing zijn, en (b) de aanbesteder hierom ook expliciet gevraagd heeft.*

Vragen over het open standaardenbeleid

1. De 'pas toe of leg uit' lijst lijkt willekeurig. Waarom deze standaarden en geen andere?

   Het Forum Standaardisatie richt zich op standaarden voor gegevensuitwisseling. Standaarden voor andere toepassingen dan gegevensuitwisseling, bijvoorbeeld proces-standaarden zoals PRINCE of ITIL, staan niet op de lijst. Een standaard kan op de lijst geplaatst worden als een belanghebbende organisatie deze aanmeldt. Als u vindt dat er een standaard mist, dan kan u die bij het Forum Standaardisatie aanmelden voor de lijst.

2. Waarom staan er geen wettelijk verplichte standaarden op de 'pas toe of leg uit' lijst?

   Wettelijke verplichting gaat boven het 'pas toe of leg uit' beleid. Daarom staan wettelijk verplichte standaarden niet op de 'pas toe of leg uit' lijst.

3. Is de reikwijdte van de 'pas toe of leg uit' lijst beperkt tot de rijksoverheid?

   Nee. Alle (semi-) overheidsorganisaties hebben de verplichting om de open standaarden op de 'pas toe of leg uit' lijst toe te passen. Het Nationaal Beraad Digitale Overheid stelt dat de 'pas toe of leg uit' verplichting overheidsbreed geldt. Dus ook voor provincies, gemeenten, waterschappen en ZBO's die allen in het Nationaal Beraad gerepresenteerd zijn.

4. Wanneer is een standaard 'open'?

   Het Forum Standaardisatie hanteert vier kenmerken waaraan een standaard moet voldoen om als 'open standaard' aangemerkt te worden. De benodigde documentatie moet laagdrempelig beschikbaar zijn. Er mogen geen hindernissen zijn op het terrein van intellectueel eigendomsrecht. Belanghebbenden moeten voldoende inspraakmogelijkheden hebben tijdens de (door)ontwikkeling van de standaard. En de onafhankelijkheid en duurzaamheid van de standaardisatieorganisatie moet verzekerd zijn.

5. Op welk moment moet mijn organisatie voldoen aan een standaard?

   Bij elke aanbesteding moet u voor die aanbesteding relevante standaarden uitvragen die op de 'pas toe of leg uit' lijst staan. Dit geldt voor de aanschaf van software, hardware en ICT-diensten, maar ook voor inhuur en (door)ontwikkeling. Het geldt voor nieuwe producten of diensten, maar ook voor voortzetting van reeds eerder verleende diensten en voor aanvulling op of wijziging van bestaande producten of diensten.

6. Moet mijn organisatie voldoen aan alle standaarden op de 'pas toe of leg uit' lijst?

   Nee. Elke overheidsorganisatie moet bij ICT-aanbestedingen vragen om de voor die aanbesteding relevante open standaarden van de 'pas toe of leg uit' lijst. Van een relevante open standaard is sprake, als het betreffende ICT-product of -dienst valt binnen het functionele toepassingsgebied van die standaard, en als de aanbestedende organisatie bovendien valt binnen het organisatorische werkingsgebied van de standaard. De 'pas toe of leg uit' lijst vermeldt het functionele toepassingsgebied en het organisatorische werkingsgebied van elke standaard. Voor een aanbesteding kunnen meerdere open standaarden relevant zijn.

7. Wie controleert of wij standaarden van de 'pas toe of leg uit' lijst uitvragen?

Het Forum Standaardisatie publiceert ieder jaar een Monitor die het uitvragen van open standaarden bij de overheid meet en evalueert.

8. Mijn organisatie heeft voorkeur voor een standaard die niet op de lijst staat, mogen wij deze dan uitvragen?

Nee, het is verplicht om de open standaard op de 'pas toe of leg uit' lijst die van toepassing zijn, uit te vragen. Wel kan u het Forum Standaardisatie verzoeken om een standaard toe te voegen of te verwijderen van de 'pas toe of leg uit' lijst, of om het toepassingsgebied van een standaard aan te passen. Hier heeft het Forum Standaardisatie een procedure voor, die onder andere een openbare consultatie omvat.

9. Mijn organisatie doet functionele aanbestedingen. Kunnen wij dan wel naar specifieke standaarden vragen?

Ja, functioneel aanbesteden sluit het uitvragen van open standaarden niet uit. Ook als een leverancier moet voldoen aan open standaarden, heeft deze nog alle vrijheid van implementatie. Vergelijk het met het aanbesteden van de bouw van een brug of pont. Indien u functioneel aanbesteedt vraagt u naar een "constructie waarmee voertuigen van de ene oever naar de andere komen" maar u kunt daarbij wel degelijk aangeven dat het geleverde product aan beide oevers moet aansluiten op de rijweg (de standaard).

10. Verplicht het 'pas toe of leg uit' beleid alleen het uitvragen of ook het daadwerkelijk gebruik van de relevante standaarden?

De rijksinstructie inzake de aanschaf van ICT-producten en diensten zegt: "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."

11. Moeten wij ook open standaarden uitvragen voor systemen die intern zijn aan onze organisatie? (Moet onze netwerkprinter bijvoorbeeld IPv6 ondersteunen?)

Open standaarden hebben als doel de gegevensuitwisseling tussen overheidsorganisaties te ondersteunen. Indien uw organisatie een ICT-systeem of dienst aanbesteedt, evalueer dan zorgvuldig of dit gegevensuitwisseling over de organisatiegrens met zich mee brengt. Met 'shared services' is dit vaak het geval. De netwerkprinter uit het voorbeeld lijkt op het eerste gezicht een organisatie intern systeem. Maar als het de printer een scan kan sturen naar een e-mailadres buiten de organisatie, dan kan IPv6 toch een relevante standaard zijn.

12. De instructie rijksdienst bij aanschaf van ICT-diensten of ICT-producten lijkt van toepassing te zijn op onze aanbesteding. Hoe kunnen wij bepalen welke open standaarden wij moeten uitvragen?

Gebruik de beslisboom op de website van het Forum Standaardisatie om de relevante open standaarden voor een aanbesteding te identificeren. Vervolgens kan u de bestekteksten gebruiken die het Forum Standaardisatie beschikbaar stelt.

13. Hoe vragen wij bij onze aanbesteding relevante open standaarden uit?

Het Forum Standaardisatie heeft bestekteksten opgesteld voor veel voorkomende ICT-aanbestedingen waarin open standaarden moeten worden uitgevraagd. U kan deze gebruiken in uw aanbesteding.

14. Ik ben het ermee oneens dat een bepaalde standaard verplicht is. Wat kan ik doen?

Als u denkt dat een standaard ten onrechte verplicht is, dan kan u bij het Forum Standaardisatie een verzoek indienen om de standaard van de pas-toe-of-leg-uit lijst te

verwijderen. Het Forum Standaardisatie heeft een procedure voor het verwijderen van een standaard van de lijst. De procedure omvat onder andere een openbare consultatie zodat ook andere geïnteresseerden zich over het voorstel tot verwijdering kunnen uitspreken.

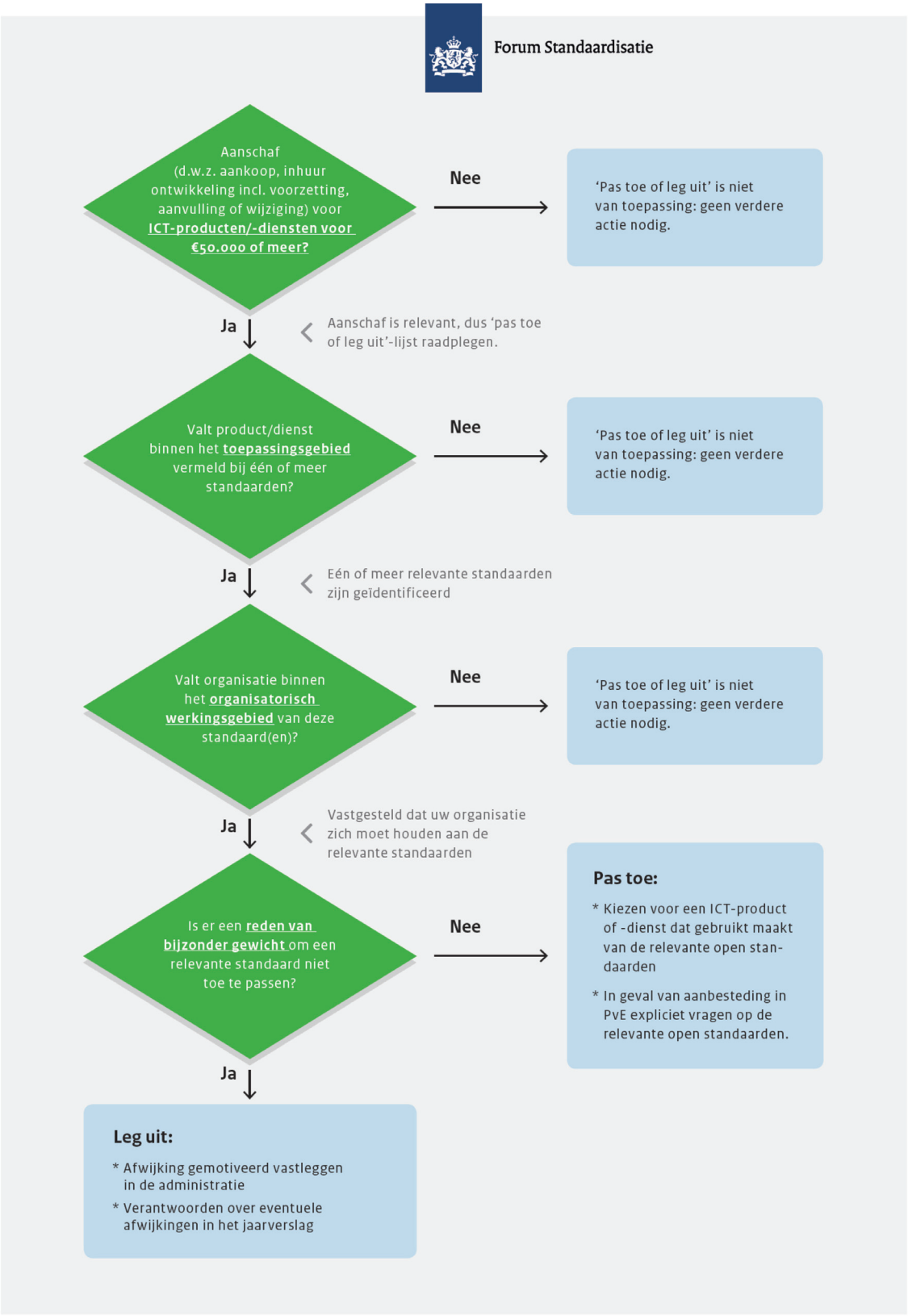
15. Ik ben het niet eens met het toepassingsgebied van een standaard. Wat kan ik doen?
    Als u denkt dat het toepassingsgebied van een standaard niet juist gedocumenteerd is, dan kan u bij het Forum Standaardisatie een verzoek tot wijziging indienen. Het Forum Standaardisatie heeft een procedure voor het wijzigen van het toepassingsgebied van een standaard. De procedure omvat onder andere een openbare consultatie zodat ook andere geïnteresseerden zich over het wijzigingsvoorstel kunnen uitspreken.

16. Ik wil een standaard aanmelden die niet op de lijst staat. Hoe doe ik dat?
    U kunt nieuwe standaarden aanmelden voor de pas-toe-of-leg-uit lijst. Het Forum Standaardisatie heeft een procedure voor het toevoegen van een standaard aan de lijst. De procedure omvat onder andere een openbare consultatie zodat ook andere geïnteresseerden zich over het voorstel kunnen uitspreken.

17. Waar kan ik hulp krijgen bij het uitvragen en toepassen van een standaard?
    Het Bureau Forum Standaardisatie kan u helpen bij het uitvragen en toepassen van een standaard. Het Bureau Forum Standaardisatie ondersteunt u zelf of brengt u in contact met experts die u verder kunnen helpen.

18. Ontwikkelt het Forum Standaardisatie standaarden?
    Nee, dat doen de beheerorganisaties. Vind de namen van de beheerorganisaties bij de standaarden op de lijst. Het Forum Standaardisatie beheert de lijst met open standaarden, die vooral bekend is geworden als de 'pas toe of leg uit' lijst, maar deze lijst bevat ook aanbevolen standaarden. Pas als een open standaard voldoende ontwikkeld is en tot op zekere hoogte geadopteerd, komt deze in aanmerking voor plaatsing op de lijst met open standaarden.

Bijlage C. Aanbestedingen: schema 'Pas toe of leg uit' in het kort



Bijlage D. Overzicht van de beoordeelde aanbestedingen 2017/2018

De 34 aanbestedingen van Rijk en uitvoeringsorganisaties en de 33 van mede-overheden die dit jaar zijn beoordeeld zijn in Tabel D1 en Tabel D2 opgesomd, met een korte omschrijving van het onderwerp van de aanbesteding, met de open standaarden die de beoordelaars relevant achten (uitgesplitst in cruciale en niet-cruciale) en met de uiteindelijke beoordeling. Hiervoor is de volgende indeling gehanteerd (conform Hoofdstuk 3):

A om alle relevante open standaarden is expliciet gevraagd
B om een deel van de relevante open standaarden is gevraagd, waaronder alle cruciale
C om een deel van de relevante open standaarden is gevraagd, maar om minimaal één cruciale niet
D er wordt alleen verwezen naar architectuurkaders (geen concrete open standaarden gevraagd)
E er wordt alleen in algemene zin verwezen naar open standaarden(beleid)
F er is in het geheel geen aandacht voor open standaarden
G er wordt expliciet gevraagd om zaken die strijdig zijn met open standaardenbeleid

Relevante standaarden waar in de aanbesteding om is gevraagd zijn groen gemarkeerd, relevante standaarden waarom niet is gevraagd zijn niet gemarkeerd.

Tabel D1: Overzicht van beoordeelde aanbestedingen Rijk en uitvoeringsorganisaties

aanbesteder	inhoud aanbesteding	standaarden[25] cruciaal	standaarden niet-cruciaal	oordeel
Zorginstituut Nederland	Het ontwerpen, bouwen en opleveren van de Decentrale Validatiemodule onder de afdeling iStandaarden	ISO 27001/27002		A
Min. BZK	ICT-Infrastructuurdiensten en ICT-werkplekken voor Het Huis voor Klokkenluiders	DNSSEC IPv4/6 ISO 27001/27002 SAML HTTPS en HSTS WPA2 Enterprise SPF DKIM DMARC	ODF PDF	A
Zorginstituut Nederland	Het leveren, onderhouden en doorontwikkelen van een volledige e-HRM oplossing, die geïmplementeerd moet worden. Daarnaast betreft het de verwerking van salarissen en het ter beschikking stellen van een tweedelijns helpdesk	Digitoegankelijk HTTPS en HSTS TLS ISO 27001/27002 ODF PDF	SAML, SPF DKIM DMARC	A
RDW	Het leveren van een end point protection oplossing en het implementeren, installeren en configureren hiervan plus het leveren van support	ISO 27001/27002		A
LVNL	Uitbesteden van het beheer en de ontwikkeling van het Qlik Sense landschap	ISO 27001/27002	IPv4/6 TLS	B

[25] Alle standaarden die worden genoemd, zijn volgens de beoordelaars relevant. Een deel daarvan was volgens de beoordelaars voor de betreffende aanbesteding cruciaal. Standaarden waarom in de aanbesteding is gevraagd zijn groen gemarkeerd, standaarden waarom *niet* is gevraagd geel.

aanbesteder	inhoud aanbesteding	standaarden[25] cruciaal	standaarden niet-cruciaal	oordeel
NWO	Een applicatie van een personeelsinformatie- en salarissysteem, hoofdzakelijk bestaande uit standaardsoftware	ISO 27001/27002 HTTPS en HSTS TLS	XBRL ODF PDF SAML DNSSEC	B
Stichting RPO	Ontzorgen op het gebied van Content Delivery Network (CDN)-dienstverlening. Een CDN is een netwerk van proxyservers die geografisch verspreid zijn over het internet in verschillende datacenters	ISO 27001/27002 HTTPS en HSTS TLS IPv4/IPv6	PDF ODF	B
Belasting-dienst	De toekomstige levering van Nieuwe Functionaliteiten Kanalen en Interactievoorzieningen voor het Contact Center inclusief support alsmede het leveren van support voor de huidige Installed Base. Het gaat ook om het afnemen van licenties	ISO27001/27002	HTTPS en HSTS TLS Digitoegankelijk DKIM SPF DMARC	B
NPO	Het leveren van development en design voor de ontwikkeling van 9 nieuwe apps voor NPO Radio algemeen en de diverse radiomerken van de NPO, inclusief beheer, ondersteuning en onderhoud	HTTPS en HSTS TLS Digitoegankelijk	SAML	B
Belasting-dienst	Een Rijksbrede HR werving & selectie oplossing ter ondersteuning van in-, door- en uitstroom van medewerkers van het Rijk en Defensie	ISO 27001/27002 Digitoegankelijk ODF PDF HTTPS en HSTS TLS SETU	SAML E-portfolio IPv4/IPv6 CMIS DNSSEC DMARC SPF DKIM	C
Belasting-dienst	Een ERD-volgsysteem, inclusief onderhoud, beheer, implementatie, consultancy en de benodigde training	ISO 27001/27002 HTTPS en HSTS TLS ODF PDF Digikoppeling		C
Min. Def	Een KVM (Keyboard, Video, Mouse) oplossing om 12 bestaande (gescheiden) informatiesystemen op de beeldschermen van 27 meldtafels te kunnen weergeven in de Operations Room	ISO 27001/27002 HTTPS en HSTS TLS IPv4/IPv6		C
KvK	Een SaaS applicatie voor registratie, afhandeling en rapporteren van ICT-en facilitaire-processen, en afhandeling van HRM-vragen	ISO 27001/27002 TLS ODF PDF HTTPS en HSTS Digitoegankelijk	SAML DMARC SPF DKIM	C

aanbesteder	inhoud aanbesteding	standaarden[25] cruciaal	standaarden niet-cruciaal	oordeel
NWO	Een nieuwe applicatie ter vervanging van het ProjectNet-ZonMwDelfi pakket. ZonMw financiert gezondheidsonderzoek. Het doel van de nieuwe applicatie is om het subsidieproces te faciliteren en te ondersteunen.	ISO 27001/27002 HTTPS en HSTS TLS ODF PDF XBRL Digitoegankelijk CMIS SAML	DMARC SPF DKIM	C
Min. BZK	Een nieuwe overeenkomst voor het Planningsteem voor de Interdepartementale Post- en Koeriersdienst, onderdeel van de Uitvoeringsorganisatie Bedrijfsvoering Rijk	ISO 27001/27002 HTTPS en HSTS TLS DNSSEC IPv4/IPv6 Digitoegankelijk STARTTLS / DANE SPF DKIM DMARC	ODF PDF SMeF	C
LVNL	Een Network based Intrusion Detection Systeem, welke helpt bij de monitoring van de datastromen binnen het LAN van de Luchtverkeersleiding Nederland	ISO 27001/27002 IPv4/IPv6	HTTPS en HSTS TLS DNSSEC	C
KvK	Het verkrijgen van software voor het digitaal ondertekenen van documenten	ISO 27001/27002 HTTPS en HSTS TLS PDF Ades		C
KB	De vervanging van twee bestaande apps voor de Koninklijke Bibliotheek, namelijk een eBook app (deBibliotheek) en een audiobook app (LuisterBieb)	ISO 27001/27002 HTTPS en HSTS TLS PDF Digitoegankelijk		C
KvK	Een efficiënte betalingsafhandeling bij de KvK voor de internetkassa en pinbetalingen integreren in één overeenkomst	ISO 27001/27002 HTTPS en HSTS TLS WPA2 Enterprise IPv4/IPv6	PDF	C
Min. SZW	Een zaakgericht werken systeem die de processen van de afdeling CAV kan ondersteunen, om hun taken op het gebied van Cao-aanmelding, AVV en Pensioenen uit te kunnen voeren	ISO 27001/27002 Digitoegankelijk OWMS StUF HTTPS en HSTS TLS	PDF DKIM SPF DMARC	C
NPO	Een ervaren onderzoeksbureau dat in samenwerking met NPO en de omroepen de prestaties van de online diensten van de Nederlandse Publieke Omroep door middel van Online Analytics in kaart kan brengen	ISO 27001/27002 HTTPS en HSTS TLS	PDF	C
Min. BZK	Het opleveren van een nieuwe website voor de Raad van State	ISO 27001/27002 Digitoegankelijk HTTPS en HSTS TLS DNSSEC IPv4/IPv6		C

aanbesteder	inhoud aanbesteding	standaarden[25] cruciaal	standaarden niet-cruciaal	oordeel
Min. BZK	Het leveren van een integrale SaaS oplossing voor de HRM en F&C processen en waarbij de salaris administratie/-verwerking als dienstverlening wordt aangeboden	ISO 27001/27002 TLS HTTPS en HSTS DNSSEC XBRL E-portfolio ODF PDF SAML	SPF DKIM DMARC	C
SVB	Het ontwerp, de bouw, het beheer én integrale exploitatie (hosting) van een werkend digitaal Meldloket WagwEU, inclusief de naadloze aansluiting op de noodzakelijke Identificatie- en Authenticatie Management (IAM) dienstverlening	ISO 27001/27002 HTTPS en HSTS TLS Digitoegankelijk Digikoppeling SAML IPv4/IPv6 DNSSEC	SPF DKIM DMARC PDF	C
RWS	Een arbeidsmarktpositiemeter, welke een zo reëel mogelijke inschatting geeft van de positie van een rijksambtenaar op de huidige en toekomstige arbeidsmarkt	ISO 27001/27002 HTTPS en HSTS TLS E-portfolio Digitoegankelijk	PDF SPF DKIM DMARC	C
Min. Buza	Een vervangend informatiesysteem (Vergoedingen Declaraties Buitenland systeem (VDBS)) voor het Vergoedingen Incidenteel en Permanent Systeem (VIPS) dat daarmee helpt de werkprocessen van 3W voor uitgezonden medewerkers te verbeteren	ISO 27001/27002 HTTPS en HSTS TLS SPF DKIM DMARC XBRL ODF PDF	SAML	C
Min. Buza	Het realiseren en implementeren van één platform voor internationale vacatures om hiermee vacatures bekend te stellen en kandidaten te informeren	ISO 27001/27002 HTTPS en HSTS TLS Digitoegankelijk SPF DKIM DMARC DNSSEC IPv4/IPv6	PDF	C

aanbesteder	inhoud aanbesteding	standaarden[25] cruciaal	standaarden niet-cruciaal	oordeel
Comm. Media	De aanschaf van licenties voor een cloudapplicatie voor, de implementatie van en het hosten, support, verder ontwikkelen, onderhoud en beheer van het zaaksysteem	ISO 27001/27002 HTTPS en HSTS TLS Digikoppeling ODF PDF SAML SPF DKIM DMARC IPv4/IPv6 DNSSEC Digitoegankelijk		C
LVNL	Een middleware-oplossing genaamd MuleSoft te beheren en door ontwikkelen, met inbegrip van advies voor het daadwerkelijk leggen van koppelingen en maken van interfaces	ISO 27001/27002		D
Min. BZK	Het beheer, onderhoud en (door)ontwikkeling op het softwarepakket GEF'97 uit te voeren (voorziet in de uitvoering van de financiële-verhoudingswet 1997)	ISO 27001/27002		F
IUC-Noord	Het realiseren van een data entry vanaf de digitale afbeeldingen van een archief, het koppelen van digitale afbeeldingen van een archief aan een bestaande index, en het toepassen van optical character recognition op afbeeldingen van (deels) getypte archieven	ISO 27001/27002 ODF		F
IFV	Met behulp van de aanwezige software een nieuw Examen Management Systeem gaat bouwen, inrichten en onderhouden. Migratie van (persoons)gegevens van het oude naar het nieuwe systeem vallen binnen de scope	ISO 27001/27002 HTTPS en HSTS TLS Digitoegankelijk ODF PDF	DMARC SPF DKIM	F
Min. IW	Afsluiten van een overeenkomst met één opdrachtnemer die ten behoeve van overheden logistieke data vergaart, verzamelt in een database en deze data gestructureerd beschikbaar maakt	ISO 27001/27002 HTTPS en HSTS TLS Digitoegankelijk SPF DKIM DMARC	Geo-standaarden	F
IUC-Noord	Dienstverleningsovereenkomst voor software packaging, oftewel het aanpassen of converteren van de installer van een bestaande applicatie	ISO 27001/27002 HTTPS en HSTS TLS		F

Tabel D2: Overzicht van beoordeelde aanbestedingen mede-overheden

aanbesteder	inhoud aanbesteding	standaarden[26] cruciaal	standaarden niet-cruciaal	oordeel
Omgevings-dienst West-Holland	Een aanbesteding voor de verlening van ICT support inclusief werkplekbeheer.	ISO 27001/27002	HTTPS en HSTS TLS IPv4/IPv6 ODF PDF WPA2 Enterprise XBRL	B
Gemeente Nijmegen	Het implementeren en onderhouden van een geautomatiseerde ondersteuning van alle activiteiten in het kader van ketensamenwerking, schuldhulpverlening en de bankfunctie van de Gemeentelijke Kredietbank.	Digikoppeling Digitoegankelijk HTTPS en HSTS TLS ISO 27001/27002 StUF	PDF	C
Gemeente Vlaardingen	Aanschaf van nieuwe storage apparatuur, welke geïntegreerd dient te worden in de bestaande ICT-infrastructuur.	HTTPS en HSTS TLS IPv4/IPv6 ISO 27001/27002		C
Gemeente Hilversum	Een klantvolgsysteem ten behoeve van Sociaal Plein.	Digikoppeling Digitoegankelijk E-Portfolio HTTPS en HSTS TLS ISO 27001/27002 ODF PDF StUF	SAML SPF DKIM DMARC	C
Gemeente Den Haag	De (door)ontwikkeling, het beheer en de kwaliteitszorg van OutSystems.	HTTPS en HSTS TLS ISO 27001/27002 StUF	SAML	C
Gemeente Apeldoorn	Het ontwerpen en implementeren van een firewall en het leveren van support op de firewallopstelling	HTTPS en HSTS TLS IPv4/IPv6 ISO 27001/27002		C
Regionaal Inkoop-bureau IJmond	Een toekomstbestendige oplossing die verbindingen/koppelingen legt tussen gemeentelijke applicaties, gemeentelijke en landelijke basis- en kernregistraties en ketenpartners.	Digikoppeling HTTPS en HSTS TLS IPv4/IPv6 ISO 27001/27002 StUF	ODF	C
Bestuurs-dienst Ommen-Hardenberg	Levering van de EMM (Enterprise Mobility Management) oplossing, onderhoud, support en aanverwante dienstverlening, en één partij voor het leveren van de gevraagde mobiele smartphones.	HTTPS en HSTS TLS ISO 27001/27002	SAML SPF DKIM DMARC	C

[26] Alle standaarden die worden genoemd, zijn volgens de beoordelaars relevant. Een deel daarvan was volgens de beoordelaars voor de betreffende aanbesteding cruciaal. Standaarden waarom in de aanbesteding is gevraagd zijn groen gemarkeerd, standaarden waarom *niet* is gevraagd geel.

aanbesteder	inhoud aanbesteding	standaarden[26] cruciaal	standaarden niet-cruciaal	oordeel
Veiligheids-regio Kennemer-land	Alles voor een operationele (SaaS) applicatie m.b.t. het Digitaal Dossier Jeugdgezondheidszorg (DD JGZ) verzorgen. Dit betekent het op afstand beschikbaar maken van het elektronische dossier en zorgen voor een volledig operationele functionaliteit ('ready for use'), inclusief het beheer en onderhouden van deze functionaliteiten.	Digikoppeling Digitoegankelijk DNSSEC HTTPS en HSTS TLS IPv4/IPv6 ISO 27001/27002 StUF	PDF SAML	C
GSRK (Kempen-gemeenten)	De levering, het onderhoud, en het beheer van een hoogwaardig beveiligd datacommunicatienetwerk.	HTTPS en HSTS TLS IPv4/IPv6 ISO 27001/27002		C
GRS A2-gemeenten	Levering en onderhoud van een ICT oplossing voor het sociaal domein voor (1) de gehele front-office Wmo, Jeugd en Werk en Inkomen (W en I) en (2) de back-office Wmo en Jeugd.	Digikoppeling Digitoegankelijk DNSSEC HTTPS en HSTS TLS IPv4/IPv6 ISO 27001/27002 StUF	ODF PDF	C
Gemeente Best	Opleveren en vervolgens het ter beschikking stellen, inclusief onderhouden en ondersteunen, van een ICT oplossing voor BAG, WOZ en belastingen.	Digikoppeling ISO 27001/27002 StUF	ODF PDF SAML	C
Gemeente Middelburg	De levering van toegangscontrolesystemen voor ondergrondse containers en een containermanagementsysteem.	HTTPS en HSTS TLS IPv4/IPv6 ISO 27001/27002	ODF PDF	C
GR Werk-organisatie BUCH	Het leveren, implementeren en onderhouden van een financieel systeem, dat een geïntegreerd geheel dient te zijn van onder andere financiële administratie, budgettering, projectadministratie, inkoop en verkoop.	Digikoppeling HTTPS en HSTS TLS ISO 27001/27002 SMeF StUF XBRL	ODF PDF SAML SPF DKIM DMARC	C
Waterschap Noorder-zijlvest	Leveren, implementeren en onderhouden van een onderhoudsbeheersysteem (OBS).	Aquo-standaard HTTPS en HSTS TLS ISO 27001/27002		C
Gemeente Utrecht	De ondersteuning van de gemeente bij het verzamelen, verwerken, controleren en beheren van persoons-, schoolloopbaan- en dossiergegevens van leerlingen in de gemeente, de behandeling van verzuim en het beoordelen van aanvragen en afgeven van beschikkingen voor leerling vervoer.	Digikoppeling E-Portfolio HTTPS en HSTS TLS ISO 27001/27002 StUF	ODF PDF SAML	C

aanbesteder	inhoud aanbesteding	standaarden[26] cruciaal	standaarden niet-cruciaal	oordeel
Bureau Inkoop & Aanbestedingen Zuidoost-Brabant	Opleveren en ter beschikking stellen, inclusief onderhouden en ondersteunen, van één systeem voor bodeminformatie voor heel Noord-Brabant.	Digikoppeling Geo-standaarden HTTPS en HSTS TLS ISO 27001/27002 SIKB0101 StUF	PDF	C
Unie van waterschappen	Een website waarop kiesgerechtigden zich ten behoeve van de waterschapsverkiezingen kunnen oriënteren op een politieke partij.	Digitoegankelijk DNSSEC HTTPS en HSTS TLS IPv4/IPv6 ISO 27001/27002		C
Gemeente Breda	Een standaardapplicatie ter ondersteuning van HRM-processen en salarisverwerking.	Digikoppeling HTTPS en HSTS TLS ISO 27001/27002		C
Provincie Zuid-Holland	Het leveren van hardware voor eindgebruikers (waaronder tablets, laptops, desktops, mobiele telefoons en accessoires) alsmede voor servers voor de centrale infrastructuur.	HTTPS en HSTS TLS IPv4/IPv6 ISO 27001/27002		C
Bureau Inkoop & Aanbestedingen Zuidoost-Brabant	Een ICT-oplossing voor eHRM en salarisproductie.	Digikoppeling HTTPS en HSTS TLS ISO 27001/27002	E-Portfolio ODF PDF SAML SPF DKIM DMARC	C
Gemeente Molenwaard	Het leveren, inrichten, implementeren, koppelen, operationaliseren, in stand houden en doorontwikkelen van één nieuw burgerzakensysteem.	Digikoppeling Digitoegankelijk DNSSEC HTTPS en HSTS TLS ISO 27001/27002 StUF	PDF SAML	C
Bureau Inkoop & Aanbestedingen Zuidoost-Brabant	Opleveren en vervolgens het implementeren, onderhouden en ondersteunen van een ICT oplossing voor belastingen en invordering.	Digikoppeling HTTPS en HSTS TLS ISO 27001/27002 StUF XBRL	PDF ODF SMeF	C
Gemeente Utrecht	Het leveren, implementeren, configureren en onderhouden van een regiesysteem ten behoeve van de Buurtteams Utrecht.	Digitoegankelijk DNSSEC HTTPS en HSTS TLS ISO 27001/27002	PDF SAML	C

aanbesteder	inhoud aanbesteding	standaarden[26] cruciaal	standaarden niet-cruciaal	oordeel
Gemeente Molenwaard	Een werkende oplossing voor het sociaal domein, een backoffice functionaliteit, functionaliteiten voor Jeugd en Participatie en koppelingen met andere applicaties en externe organisaties waarmee informatie wordt uitgewisseld.	Digikoppeling HTTPS en HSTS TLS ISO 27001/27002 StUF	CMIS PDF ODF SAML	C
Provincie Utrecht	Bouwen van een nieuwe Goedopweg website. Doel is om data dat wordt gegenereerd in verschillende projecten samen te brengen in een gecentraliseerd platform en de daar uitvloeiende informatie stromen kanaliseert, centraal verzamelt en beschikbaar stelt.	Digitoegankelijk DNSSEC HTTPS en HSTS TLS IPv4/IPv6 ISO 27001/27002	SPF DKIM DMARC	C
Gemeente Terneuzen	Het opnieuw aanbesteden van een Financiën en HRM oplossing. Er is een verdeling in drie percelen: financieel, E-HRM en tijdregistratie, en roosterplanning.	Digikoppeling Digitoegankelijk DNSSEC HTTPS en HSTS TLS IPv4/IPv6 ISO 27001/27002 StUF XBRL	CMIS PDF SAML SPF DKIM DMARC	C
Gemeente Eindhoven	Een nieuwe applicatie ter vervanging van het bestaande platform voor Centrale Leerlingen Registratie (CLR).	Digikoppeling E-Portfolio HTTPS en HSTS TLS ISO 27001/27002 StUF	CMIS ODF PDF	C
Bureau Inkoop & Aanbestedingen Zuidoost-Brabant	Opleveren, implementeren, hosten, ondersteunen en onderhouden van een ICT oplossing voor E-HRM en salarisverwerking voor de gemeente Asten.	Digikoppeling HTTPS en HSTS TLS ISO 27001/27002	ODF PDF SPF DKIM DMARC	C
Waterschap Hunze & Aa	Een integrale telefonie omgeving als een dienst met vast mobiel integratie, die wordt geleverd vanuit het datacenter van opdrachtnemer.	HTTPS en HSTS TLS ISO 27001/27002	SAML SPF DKIM DMARC	D[27]
Gemeente Utrecht	Hosting en dataopslag voor rioleringen en gemalen. Uit de hosting en opslag komen diverse rapportages over waterbeheer, rioleringen en gemalen. Met deze inspecties en meldingen stuurt de gemeente Utrecht op de onderhoudsstrategie en worden analyses gemaakt.	Aquostandaard DNSSEC HTTPS en HSTS TLS IPv4/IPv6 ISO 27001/27002	PDF	F
Waterschap Brabantse Delta	Het leveren van Microsoft licenties.	ISO 27001/27002	HTTPS en HSTS TLS ODF SAML	F
Enexis Netbeheer	De realisatie van de transitie van het Enexis Core ERP-landschap van SAP R3 naar SAP S/4HANA.	ISO 27001/27002		F

[27] Strik genomen is om ISO 27001/27002 gevraagd, maar zeer indirect: de BIWA is als bijlage opgenomen.

Bijlage E.
Notitie 'Meer over gebruik van de standaarden van de 'pas toe of leg uit'-lijst' (BFS)
Naast het gebruik in aanbestedingen en generieke overheidsvoorzieningen

Inleiding

ICTU onderzoekt in de Monitor Open standaarden in de eerste plaats of aanbesteders aantoonbaar naar de relevante open standaarden van de pas-toe-of-leg-uit lijst hebben gevraagd. Ten tweede is de toepassing van de relevante open standaarden in generieke overheidsvoorzieningen aan bod. Naast deze twee onderzoeken rest de vraag: *wat kan naast deze twee onderdelen nog meer gezegd worden over het gebruik van de standaarden op de 'pas toe of leg uit' -lijst?* .

Dit onderdeel van de Monitor bestaat al vijf jaar maar de aanpak is in 2018 een beetje veranderd. Dit jaar zijn niet de onderzoekers van ICTU maar de accountmanagers van het Bureau Forum Standaardisatie (BFS) nagegaan wat over het gebruik nog meer te zeggen valt. Vaak gebeurde dit door contact op te nemen met beheerders van standaarden en sommige specifiek voor de standaard relevante voorzieningen. Soms anders. De vorm van de rapportage dit jaar is in tabelvorm, waarin de accountmanagers van het Bureau Forum Standaardisatie eveneens kort een indicatie geven van het algemene beeld over het gebruik:

Rood: Er is een negatief beeld over het gebruik van de standaard ☹
Oranje: Er is een gemengd beeld over het gebruik 😐
Groen: Er is een positief beeld over het gebruik of de ontwikkeling ervan ☺

Inhoudelijk is zoveel mogelijk de lijn vastgehouden van het onderzoek zoals dat in voorgaande jaren heeft plaatsgevonden. Helaas is ook dit jaar gebleken dat het moeilijk is om informatie boven water te krijgen. Hoewel er geen standaarden in de tabel staan die rood zijn aangemerkt (negatief beeld over het gebruik) moet BFS over de volgende standaarden tot de conclusie komen dat er te weinig (meer) bekend is:

- **Ades Baselines Profiles** (geavanceerde en gekwalificeerde digitale handtekeningen)
- **Digitoegankelijk** (toegankelijkheid websites)
  NB: Mede afhankelijk van de inrichting (en consequenties) van de wettelijke verplichting van de standaard in Nederland is de verwachting dat de adoptie flink zal toenemen. Hoe dit echter gemeten zal worden is nog niet bekend.
- **ODF 1.2** (bewerkbare documenten)
- **PDF A1, PDF A2 en PDF A3 (**documentpublicatie/ archivering)
  NB: met betrekking tot ODF en PDF ontwikkelt BFS een tool om het gebruik van deze standaarden te meten, de zogenaamde PDF crawler. De eerste testresultaten hiervan gaan hierbij als aparte bijlage. Het streven is om tot een test te komen die net zo goed werkt als internet.nl
- **IFC** (bouwwerkinformatiemodellen)
- **ePortfolio** (werkervaring en competenties).
  NB: De standaard wordt in het najaar van 2018 geëvalueerd. Dit kan resulteren in wijziging van status of aanvullende adoptieadviezen.
- **STOSAG** (Afval verzameling en verwerking) zijn geen gebruiksgegevens bekend.
  NB: De standaard zal naar verwachting in het najaar van 2018 de 'pas toe of leg uit' status verliezen.

Met betrekking tot de meeste informatieveiligheidsstandaarden is het beeld met behulp van internet.nl veel scherper te krijgen. Het gaat om het gebruik van **DNSSEC, IPv4&IPv6, HTTPS & HSTS, DMARC, DKIM, SPF, TLS, STARTTLS & DANE** dat ieder half jaar getest wordt door BFS met behulp hiervan. De meting van medio 2018 gaat als bijlage bij de Monitor (zie Bijlage G).

1. Domein internet en beveiliging

<table>
<tr><th>Open standaard
(op lijst sinds)</th><th>Over de standaard
Data over gebruik en ontwikkeling</th><th>Beeld BFS</th></tr>
<tr><td>IPv4 & IPv6

Nummers voor Internetadressen

(25/11/ 2010)</td><td>IPv4 & IPv6 regelen hoe het unieke nummer er uit moet zien dat ieder systeem heeft binnen een netwerk, het IP-adres. De nummers die gemaakt zijn volgens IPv4 raken op en daarom is het nodig IPv6 te gaan gebruiken.

Met behulp van de webtool op Internet.nl is getest welke overheidswebsites voldoen aan IPv6. Dit zijn de resultaten die aansluiten op de Monitor Open Standaarden 2017. Voor het juiste begrip: in de zomer van 2017 werden 544 domeinnamen onderzocht, in de zomer 2018 waren dit 563.

<table>
<tr><th></th><th>2017</th><th></th><th>2018</th><th></th></tr>
<tr><td>Rijk*</td><td>33 %</td><td>(98)</td><td>45 %</td><td>(127)</td></tr>
<tr><td>Gemeenten</td><td>11 %</td><td>(396)</td><td>25 %</td><td>(388)</td></tr>
<tr><td>Provincies</td><td>25 %</td><td>(16)</td><td>17 %</td><td>(18)</td></tr>
<tr><td>Waterschappen</td><td>9 %</td><td>(34)</td><td>13 %</td><td>(30)</td></tr>
<tr><td>Totaal</td><td>15 %</td><td>(544)</td><td>29 %</td><td>(563)</td></tr>
</table>
*inclusief uitvoeringsorganisaties
Bron: Onderzoek mbv. Internet.nl door BFS

Ontwikkeling: Aanvankelijk was het de ambitie van het kabinet om websites en e-mail van de overheid per 2014 toegankelijk te hebben via IPv6. Zover is het nog lang niet, maar de implementatie van (IPv4&) IPv6 groeit wel gestaag.

Verder meldt Herman Timmermans, projectleider IPv6 en govroam bij VNG Realisatie dat over het gebruik van IPv6 bij gemeenten maandelijks publiekelijk gerapporteerd wordt via de website https://www.waarstaatjegemeente.nl/Jive?var=mdd_ipv6_</td><td></td></tr>
<tr><td>NEN-ISO/ IEC 27001 & 27002

Management systeem / Richtlijnen en principes informatie – beveiliging

(18/5/2015)</td><td>NEN-ISO/ IEC 27001
Deze standaard specificeert de eisen voor het vaststellen, implementeren, uitvoeren, bewaken, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System ten aanzien van algemene bedrijfsrisico's van een organisatie.
NEN-ISO/ IEC 27002
Deze standaard beschrijft best practices voor informatiebeveiliging van een organisatie.

VIR/BIR
Voor de Rijksdienst (departementen en uitvoeringsorganisaties) geldt dat de standaarden ISO/IEC 27001 en 27002 via het VIR (Voorschrift Informatiebeveiliging Rijksdienst) en de BIR (Baseline Informatiebeveiliging Rijksdienst) worden toegepast. In de loop van 2017 is een nieuwe versie van</td><td></td></tr>
</table>

	de BIR2017 vastgesteld. Zowel in 2017 als in 2018 hebben alle 11 departementen een ICV (in control verklaring) afgegeven aan DGOO (Directeur Generaal Overheidsorganisatie). **BIG** Alle Nederlandse gemeenten hanteren de BIG als normenkader voor informatiebeveiliging, deze is gebaseerd op de BIR / ISO27001/2. Eind 2018 wordt de afronding verwacht van de ENSIA vragenlijsten. De uitkomsten hiervan kunnen een indicatie zijn voor het gebruik van de BIG. De uitkomsten hiervan zijn nog niet bekend en zullen waarschijnlijk in de Monitor van 2019 aan bod komen. **IBI** Bij de provincies worden de standaarden ISO/IEC 27001 en 27002 geïmplementeerd via de IBI en hiervoor is een monitoringstool. In 2017 liet deze monitor nog een positieve tendens zien. Een update hierover kwam niet op tijd binnen voor deze notitie. **BIWA** Bij alle waterschappen worden maatregelen van informatieveiligheid doorgevoerd volgens de BIWA. In 2016 hebben alle waterschappen de governance op informatiebeveiliging ingericht, werken zij planmatig (96%) aan de implementatie van de BIWA en wordt het onderwerp actief onder de aandacht gebracht (91%). In de Monitor van 2017 werd aangekondigd dat de waterschappen een BIWA audit zouden krijgen van een extern bureau. Deze audit heeft plaatsgevonden met als resultaat een stand van zaken en verbeterpunten per waterschap. Het doel van de BIWA audit was intern gericht (voor de waterschappen om van te leren) en de resultaten hiervan worden verder niet verder naar buiten toe gecommuniceerd. Wél zijn de resultaten gedeeld in de werkgroep Normatiek. Bron: Navraag bij partijen door BFS in 2018 en Monitor Open Standaarden 2017 p. 118 en verder. Ontwikkeling: Verschillende cijfers laten een beeld zien van gestage groei in het gebruik. NB: De werkgroep Normatiek werkt aan één Overheidsbrede Baseline Informatiebeveiliging (BIO).	
SAML Inloggen (18/5/2009)	SAML specificeert hoe een gebruiker na eenmalig inloggen via zijn browser toegang krijgt tot verschillende diensten van verschillende partijen en zich hier ook eenmalig weer kan afmelden. Met andere woorden: *federatieve (web)browser-based single-sign-on en single-sign-off.* SAML is de standaard geworden voor (nieuwe) aansluitingen waarbij burgers of bedrijven inloggen bij de overheid. Twee belangrijke toepassingen van SAML in Nederland zijn eHerkenning en DigiD, waarmee bedrijven respectievelijk burgers zich kunnen authentiseren in identificeren bij overheden. Het aantal aansluitingen op deze voorzieningen is dan ook in voorgaande jaren als indicator genomen om het gebruik van SAML te meten.	

	Aansluitingen bij eHerkenning en DigiD, gebaseerd op SAML per jaar **2016** **2017** **2018** (vanaf 1 juli) EHerkenning 168 203 359 DigiD 128 290 398 Bron: navraag bij de beheerders van eHerkenning en DigiD bij Logius. Monitor Open Standaarden 2017, p. 122 e.v. Ontwikkeling: het aantal aansluitingen stijgt en daarmee het gebruik van SAML.	
STIX/TAXII Dreigings-informatie (21/11/2017)	STIX en TAXII maken het mogelijk om informatie over een cyberdreiging of cyberaanval op een gestructureerde en automatisch verwerkbare manier te beschrijven en onmiddellijk te communiceren naar belanghebbende organisaties. De standaard wordt gebruikt door het Nationaal Cyber Security Centrum (NCSC),. Het NCSC doet dit in het Nationaal Detectie Netwerk (NDN), een stelsel van samenwerkingsverbanden tussen het NCSC en organisaties uit de Rijksoverheid en andere vitale sectoren. Binnen dit netwerk wordt gestructureerd informatie uitgewisseld over digitale dreigingen. Een NDN-deelnemer is een organisatie die deelneemt aan dit netwerk. Vier van de in totaal tien NDN deelnemers gebruiken STIX/ TAXII. Het NCSC vermeldt hierbij dat het daarbij gaat om relatief grote spelers.	
WPA2 Enterprise Toegang tot WiFi netwerk met netwerkaccount (2/2/2016)	WPA2 Enterprise maakt het mogelijk om automatisch veilig toegang te krijgen tot aangesloten WiFi-netwerken via authenticatie op basis van bestaande identiteitsgegevens. Als indicatie voor het gebruik van deze standaard wordt sinds 2016 begin september het aantal deelnemende organisaties geteld van Govroam en Eduroam. **2016** **2017** **2018** Govroam 49 132 244 Eduroam 157 (mei 2016) 199 215 Bron: https://govroam.nl/over- govroam/deelnemende-organisaties/ https://eduroam.nl/instellingen Ontwikkeling: het gebruik van deze standaard groeit.	

2. Document en (internet)content

Open standaard (op lijst sinds)	Over de standaard Data over gebruik en ontwikkeling	Beeld BFS
SKOS Thesauri en begrippen-woordenboeken	SKOS is de standaard voor het delen en linken van systemen voor kennisrepresentatie. Denk hierbij aan thesauri, taxonomieën, begrippen-woordenboeken, classificatieschema's en systemen voor trefwoordtoekening.	

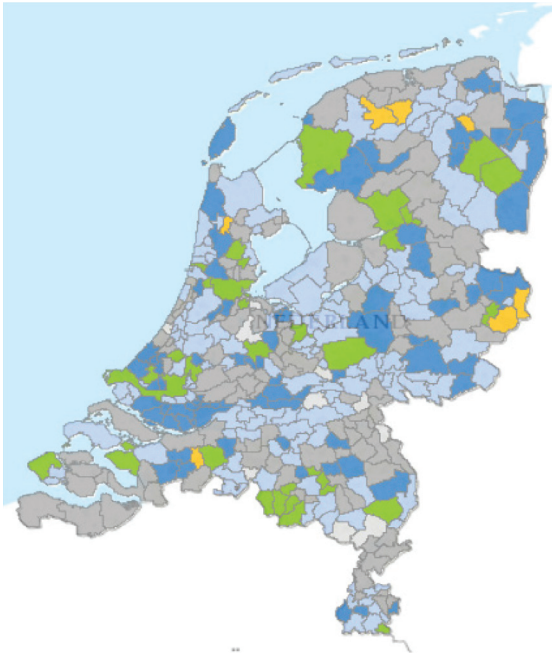
(18/8/2009)	Het Kadaster heeft gebruiksgegevens over eigen datasets waarop zowel SKOS en OAS wordt toegepast. Ook het Nederlands Informatie Instituut voor Oorlogsdocumentatie gebruikt de standaard om datacollecties van verschillende organisaties te koppelen in het Netwerk Oorlogsbronnen.	
CMIS Content uitwisseling tussen CMS-/DMS-Systemen (9/12/2014)	CMIS staat voor Content Management Interoperability Services en regelt hoe content en metadata uitgewisseld kunnen worden al komen deze van verschillende repositories (opslagplaatsen). Er zijn twee grote toepassingen bekend van CMIS: • de website van de Rijksoverheid, meer specifiek tussen het platform van de Ministeries van Algemene Zaken en van Veiligheid en Justitie • de doc- diensten van de 11 ministeries; 8 worden geleverd door SSC-ICT en drie departementen hebben aparte doc-systemen. Bron: Monitor Open standaarden 2017, p. 127 en verder.	
OWMS Metadata overheidsinformatie (15/11/2011)	OWMS is de standaard voor metadatering. KOOP gebruikt OWMS op wetten.overheid.nl.	

Standaarden uit dit domein waar geen gebruiksgegevens over bekend zijn:

- **Ades Baselines Profiles** (geavanceerde en gekwalificeerde digitale handtekeningen)
- **Digitoegankelijk** (toegankelijkheid websites)
  Mede afhankelijk van de inrichting (en consequenties) van de wettelijke verplichting van de standaard in Nederland is de verwachting dat de adoptie flink zal toenemen. Hoe dit echter gemeten zal worden is nog niet bekend.
- **ODF 1.2** (bewerkbare documenten)
- **PDF A1, PDF A2 en PDF A3** (documentpublicatie/ archivering)

3. E-facturatie en administratie

Open standaard (op lijst sinds)	Over de standaard Data over gebruik en ontwikkeling van het gebruik	Beeld BFS
NL CIUS Electronisch factureren (24/5/2018) *(Voorheen **Semantisch Model eFactuur** 15/11/2016)*	NL_CIUS is de standaard voor elektronisch factureren. Het model geeft duidelijkheid aan overheden en bedrijven (gebruikers en ICT-aanbieders) over de elementen en gegevens die op facturen naar overheidsorganisaties gebruikt dienen te worden (specifiek voor de Nederlandse situatie). Rijksoverheden zijn uiterlijk 18 april 2019 wettelijk verplicht elektronische facturen te ontvangen en te verwerken volgens NEN-EN 16931-1 en de bijbehorende syntaxen (UBL (of eventueel CII)). Decentrale overheden hebben daar nog een jaar langer de tijd voor. De beheerorganisatie van NL CIUS (NEN, TNO en simplerinvoicing) heeft geen kwantitatieve indicatoren van diens adoptie in daadwerkelijke e-facturen. Wel bestaat er een beeld over het gebruik van de standaard. Het gebruik van NL CIUS gebeurt in de praktijk indirect via het gebruik van andere e-factuurstandaarden, zoals NEN-EN 16931-1, OHNL of SETU, die voldoen	

	aan SMeF 2.0 en de opvolger NL CIUS. De Factuurstandaard SI-UBL zal in de volgende release een 1 op 1 implementatie van NL CIUS zijn. Het programmabureau e-factureren, opgericht binnen Pianoo voert onderzoek uit naar het gebruik door decentrale overheden op basis van zelfrapportage. Hieruit blijkt: • Bij gemeenten geven 31 aan gereed te zijn. Meer dan 60 gemeenten zijn bezig met implementatie, meer dan 100 met voorbereiding; de overige gemeenten is niet gestart, heeft de implementatie on hold gezet of heeft geen informatie aangeleverd. • Meer dan 5 waterschappen hebben e-facturen geïmplementeerd. De overigen zijn bezig met implementatie of in voorbereiding. Van het waterschap Limburg is de status onbekend en 1 waterschap in Noord-oost Nederland heeft de implementatie on-hold. • Gelderland, Groningen, Overijssel en Zeeland hebben e-factureren geïmplementeerd: 6 zijn bezig met implementatie, 2 zijn in verkennende fase. Bron: https://www.pianoo.nl/nl/themas/elektronisch-factureren https://www.pianoo.nl/nl/themas/e-factureren/praktijk-tools/implementatiemonitor-e-factureren Ontwikkeling: Naar verwachting zal het gebruik van de standaard toenemen door de wettelijke verplichting van elektronisch factureren.  De implementatie van e-factureren bij Gemeenten (juni 2018)	
SETU Informatie flexibele arbeidskrachten	De SETU-standaarden betreffen het elektronisch berichtenverkeer in de branche voor flexibele arbeid. SETU regelt het berichtenverkeer tussen aanbieders en afnemers (inleners) van tijdelijk personeel. De SETU-standaarden worden ontwikkeld en beheerd door de stichting SETU waarin alle grote uitzendorganisaties in Nederland betrokken zijn. SETU beschikt, in lijn met voorgaande jaren, niet over kwantitatieve gegevens over het feitelijke gebruik van de standaarden. De gebruiksgegevens zijn lastig te	

(20/5/2009, nieuwe versies sinds 25/2/2015)	bepalen, aangezien het berichtenverkeer niet via een centraal platform geregeld wordt en er recent ook geen metingen of enquêtes zijn uitgevoerd. TNO onderzocht in 2014 de adoptie van SETU en ontwikkelt de standaard in opdracht van de beheerder. Zij meldden dat alle grote spelers in de markt voor flexibele arbeid zijn aangesloten bij SETU en de SETU-standaarden gebruiken voor hun berichtuitwisseling. Deze spelers vertegenwoordigen 85% van de markt. Uit informele uitvraag bij werkgroepen blijkt dat deze spelers gestaag nieuwe koppelingen ontwikkelen met behulp van de SETU-standaarden. Voor de kleinere spelers in deze markt geldt dat zij afhankelijk zijn van hun softwareleveranciers. In 2018 melde TNO dat er 18 softwareleveranciers bekend (in 2017 waren dit er 16) waren die één of meerdere van de SETU-standaarden ondersteunden. Hierin is dus een licht stijgende lijn te zien ten opzichte van de vorige monitor. Ontwikkeling: SETU is gebaseerd op de Europese norm voor e-Facturatie. In 2018 wordt de 2.1 versie gepubliceerd, volledig in lijn met het Nederlandse gebruiksprofiel van deze Europese norm. (zie hierboven) Gelet op de recent geldende en komende verplichtingen op het gebied van e-facturatie, voorziet TNO een toename in het gebruik.	
XBRL Bedrijfsrapportage (17/4/2010)	eXtensible Business Reporting Language (XBRL) is de internationale open standaard om bedrijfsinformatie te verzamelen, elektronisch uit te wisselen, te analyseren en zo nodig nader te bewerken. Het gebruik van XBRL wordt al een aantal jaren in de Monitor Open Standaarden gemeten door te kijken naar het gebruik van de nationale standaard SBR, Standard Business Reporting die gebruikt wordt in de voorziening Digipoort. In onderstaande tabel het aantal XBRL-berichten van medio 2017 en medio 2018:	

	jan t/m aug 2017 (= 8 maanden)	**jan t/m juli 2018** (= 7 maanden)
<u>Belastingdienst</u>		
• Aangifte inkomstenbelasting en vennootschapsbelasting	10.737.500	10.760.700
• Aangifte omzetbelasting en intracommunautaire prestaties	3.200.819	3.345.401
• Toeslagen	829.332	782.357
• Loonheffingen	825	668
<u>Kamer van Koophandel</u>		
• Deponeren jaarverantwoording	368.638	457.195
<u>CBS</u>		
• Statistiekopgaven	248	-
<u>DUO</u>		
• Jaarverantwoording	2.304	1.791
TOTAAL	**15.139.66**	**15.348.112**

Het totaal aantal berichten van Digipoort is in absolute zin nagenoeg gelijk gebleven, maar de cijfers over 2018 betreffen een kortere periode. Wanneer daarvoor wordt gecorrigeerd (8/7 x 15.348.112 = ruim 17,5 miljoen) is het gebruik van XBRL via deze voorziening duidelijk toegenomen.

WDO Datamodel Douane – informatie *(15/4/2014)*	Voor de administratie van import en export van goederen bevat het WDO Datamodel zogenaamde 'informatiepakketten' voor gegevensuitwisseling. Een informatiepakket beschrijft de semantiek van de uitgewisselde informatie: gegevens- en procesmodellen en hiervan afgeleide berichtspecificaties (Message Implementation Guidelines). Het WDO Datamodel wordt gebruikt door de Douane, Rijkswaterstaat, Zeehavenpolitie/Koninklijke Marechaussee en de Nederlandse Voedsel en Warenautoriteit en Havenautoriteiten. Met betrekking tot het gebruik van deze standaard zijn geen harde gegevens bekend omdat het feitelijke gebruik niet wordt geregistreerd. Ontwikkeling: De Douane verwacht groei in het gebruik van het WDO Datamodel om twee redenen: 1. In Europa is het Europese Customs Data model (EU CDM) geïntroduceerd dat gebaseerd is op het WDO datamodel. Het doel van de Europese Commissie is het harmoniseren en standaardiseren van de informatie uitwisseling tussen de diverse douaneorganisaties binnen de EU. Dit betekent dat, naast de hierboven genoemde douanesystemen, ook het Europese vervoersysteem NCTS op termijn zal worden gebaseerd op het EU CDM/ WDO datamodel. 2. In 2016 is het WDO Datamodel in Europa geïdentificeerd als kwalitatief goede specificatie waarom gevraagd mag worden bij aanbestedingen. Commission Decision 2016/1765. Recent is dit overzicht van 'geïdentificeerde ict specificaties' gepubliceerd. https://ec.europa.eu/growth/industry/policy/ict-standardisation/ict-technical-specifications_en	

4. Stelselstandaarden

Open standaard (op lijst sinds)	Over de standaard Data over gebruik en ontwikkeling in het gebruik	Beeld BFS
Digikoppeling Veilige berichtuitwisseling (17/6/2013)	Zoals een brief in een envelop gaat voor verzending, zo gaat een elektronisch bericht in een digitale verpakking. Digikoppeling bestaat uit koppelvlakstandaarden, die logistieke afspraken bevatten voor veilige berichtenuitwisseling tussen overheden. Digikoppeling onderkent twee hoofdvormen van berichtenverkeer: bevragingen en meldingen.	
Logius heeft op verschillende peilmomenten (maart 2013, augustus 2013, augustus 2014, augustus 2015, zomer 2016, zomer 2017 en zomer 2018) lijsten aangeleverd waarop (onderdelen van) overheden en uitvoeringsorganisaties stonden die op Digikoppeling zeggen te zijn aangesloten. Daaruit is het onderstaande overzicht af te leiden dat laat zien dat gedurende een reeks van jaren sprake is van een gestage groei van het gebruik van Digikoppeling. De ontwikkeling in de tijd bij de categorie 'Rijk' moet met het nodige voorbehoud worden bekeken want deze categorie is gevoelig voor veranderingen in de samenstelling van de populatie. Zo is in 2016 het percentage gedrukt doordat er veel organisaties zijn toegevoegd uit de OOV-sector die niet zijn aangesloten op Digikoppeling.		

Digikoppeling	Rijk + Uitvoerings-Organisaties/ ZBO's + OOV + eOverheid	Gemeenten	Provincies	Waterschappen	**Totaal**
Voorjaar 2013	3 %	31 %	8 %	14 %	22 %
Zomer 2013	4 %	42 %	15 %	14 %	29 %
Zomer 2014	5 %[28]	57 %	23 %	14 %	40 %
Zomer 2015	64 %	63 %	42 %	24 %	58 %
Zomer 2016	40 %	75 %	67 %	46 %	64 %
Zomer 2017	67%	92%	67%	50%	76%
Zomer 2018	X[29]	98%	75%	59%	95%[30]

StUF

Administratieve Overheidsgegevens

(12/11/2008)

De StUF-standaard is een familie van samenhangende gegevens- en berichtenstandaarden. StUF is als open standaard vastgesteld voor de uitwisseling basisgegevens zoals Personen (GBA), Adressen (BRA), Gebouwen (BGA), 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.

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

Adoptiegraad	**Totaal**	**StUF-BG 3.10 en 3.20**	**StUF-ZKN 3.10 en 3.20**
Aantal leveranciers	208 (197)	74 (57)	52 (50)
Aantal softwareproducten (incl. versies)	2760 (2358)	993 (718)	599 (505)
waarvan beschikbaar/in gebruik	1334 (1223)	350 (320)	213 (204)
waarvan gepland/in ontwikkeling	133 (78)	64 (50)	29 (28)

(bron VNG-Realisatie: www.softwarecatalogus.nl - peildatum september 2018; tussen haakjes de cijfers van de vorige monitor)

Geostandaarden

Geografische informatie

De Geostandaarden gaan over het registreren en uitwisselen van informatie met een geografische component. Dat wil zeggen: informatie over objecten die gerelateerd zijn aan een locatie ten opzichte van het aardoppervlak.

[28] 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.

[29] 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%

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

(9/12/2014)	Hierbinnen zijn verschillende domeinen te onderkennen, zoals kadastrale informatie en informatie over waterhuishouding. Om te waarborgen dat de geo-informatiehuishouding van deze domeinen goed op elkaar aansluit, en dat informatie tussen domeinen uitgewisseld kan worden, zijn afspraken nodig over de te gebruiken standaarden. De set Geostandaarden fungeert als ruggengraat van de (voor deze uitwisseling benodigde) Nederlandse geo-informatie infrastructuur. Deze standaarden leggen de betekenis (semantiek) van gegevens vast en beschrijven hoe die gegevens kunnen worden uitgewisseld, ontsloten en doorzoekbaar worden gemaakt. De set bestaat uit: • Basismodel geo-informatie (NEN3610) • ISO 19136:2007 - Geographic information - Geography Markup Language (GML) 3.2.1 • Nederlands metadataprofiel op ISO 19115 voor geografie v2.0.0 • Nederlands metadataprofiel op ISO 19119 voor services v2.0.0 • webserviceprofielen voor Web Feature Service (WFS) en Web Map Service (WMS) Het gebruik -in de zin van het toepassen door aanbieders van data- van de set Geostandaarden in de Nederlandse geo-informatie infrastructuur is wijdverbreid. Zo zijn niet alleen de onderliggende informatiemodellen van de geobasisregistraties (Adressen en Gebouwen - BAG, Grootschalige Topografie -BGT, Topografie -BRT en Kadaster - BRK) en van ruim 68.000 ruimtelijke plannen op NEN3610 gebaseerd, maar ook de onderliggende ecosystemen. Voor bijvoorbeeld zowel de BGT als voor IMRO (ruimtelijke plannen) geldt dat er ruim 400 bronhouders resp. bevoegd gezagen deze gegevens vastleggen conform de op NEN3610 gebaseerde modellen, deze vervolgens uitwisselen o.b.v. GML, ontsluiten o.b.v. WMS en WFS en vindbaar maken met metadata conform de Nederlandse metadataprofielen. Ook de softwareleveranciers in deze domeinen ondersteunen de standaarden voor semantiek en uitwisseling volledig. Het gebruik -in de zin van het afnemen door gebruikers van data- van de set Geostandaarden blijft fors toenemen. Zo genereert het open platform voor geo-informatie van de overheid PDOK (Publieke Dienstverlening op de Kaart) inmiddels meer dan 8 miljard hits per jaar. Een vergelijking van de gebruikscijfers van PDOK over de eerste twee kwartalen van 2018 met die van 2017 biedt een goede indicatie van het gebruik van de verschillende standaarden: het downloaden in GML formaat +67,8%, het afnemen via WFS +82,8% en via WMS +108,9%. Bij het (volledig op de metadataprofielen gebaseerde) Nationaal Georegister zien we elk kwartaal een toename in gebruik van zo'n 15-20%. Een laatste aspect van gebruik is de mate waarin gebruikers betrokken zijn bij ontwikkeling van nieuwe versies van de standaarden. Bij NEN3610 zijn de voorbereidingen gestart voor een nieuwe versie (NEN3610:2019) en de Nederlandse metadataprofielen zijn recent vernieuwd (van 1.3.x naar 2.0.0). In beide gevallen worden de gebruikers betrokken via werkgroepen, in klankbordgroepen en via consultaties. Een mooi voorbeeld van betrokkenheid van gebruikers in consultaties is de consultatie van het op NEN3610 gebaseerde IMGeo 2.2. Hierin zijn ruim 1500 reacties verzameld.	

5. Water en Bodem

Open standaard (op lijst sinds)	Over de standaard Data over gebruik en ontwikkeling in het gebruik	Beeld BFS
Aquo Waterbeheer (17/5/2016)	Aquo is bedoeld voor het vastleggen en gebruiken van gegevens in de watersector. Alle waterschappen en provincies en Rijkswaterstaat leveren hun rapportages middels de Aquo-standaard aan bij het ministerie van Infrastructuur & Waterstaat en bij het European Environment Agency (EEA). Gebruikers van de Aquo zijn ook middels het indienen van wijzigingsverzoeken en het stellen van vragen betrokken bij de ontwikkeling van de standaard. De Aquo-standaard heeft over de periode juni 2018 van 42 verschillende instanties 143 vragen gekregen. Daarnaast zijn er 158 wijzigingsvoorstellen ingediend door 28 verschillende instanties. Het zijn met name de waterschappen en laboratoria die waterkwaliteitsmonsters analyseren die contact opnemen en wijzigingsverzoeken indienen.	
SIKB 0101 Milieu-hygiënische Kwaliteit bodem (9/12/2014)	SIKB 01010 is de standaard voor de uitwisseling van gegevens voor de milieuhygiënische data binnen het bodembeheer. Het gaat daarbij om het vaststellen of voorkomen van schadelijke gevolgen voor de volksgezondheid en het milieu ten gevolge van bodemvervuiling. Alle gemeenten (omgevingsdiensten) en provincies werken met SIKB0101. Dit blijkt uit de contacten die SIKB heeft met de leveranciers van software die SIKB0101 gebruiken. Deze leveranciers zijn lid van het Centraal College van Deskundigen dat de wijzigingsverzoeken behandelt voor SIKB0101. Ook de eindgebruikers zijn in het College vertegenwoordigd. Daarnaast zijn de koepelorganisaties van de gemeenten (VNG), de provincies (IPO) en de waterschappen (UvW) ondertekenaar van het Convenant bodem en ondergrond 2016-2020. Hierin wordt expliciet de standaard genoemd als uitwisselstandaard voor bestaande (digitale) bodeminformatie "zolang dat aantoonbaar meerwaarde heeft en er geen bedrijfseconomische of privacybezwaren bestaan".	
SIKB 0102 Archeologische Bodem-Informatie (2/2/2016)	SIKB 0102 gaat over het uitwisselen van archeologische bodeminformatie. De volgende partijen werken met SIKB0102 en stellen het gebruik ervan verplicht: - Het landelijk registratiesysteem ARCHIS van de Rijksdienst voor het Culturele Erfgoed (RCE) - Opgravers (markt en overheid) 30% van de partijen / 50% qua volume. - De twaalf provinciale depots (Groningen, Drenthe en Friesland werken met één depot) leveren hun informatie met SIKB0102 aan bij DANS. - Data Archiving and Networking Services (DANS) - BIJ12, beheerder van het provinciaal depot beheer system (PDBS) De depots van gemeenten (veelal historische steden) gebruiken hoofdzakelijk eigen systemen.	

6. Bouw

Open standaard (op lijst sinds)	Over de standaard Data over gebruik en ontwikkeling in het gebruik	Beeld BFS
VISI Bouwproces Informatie (9/12/2014)	VISI regelt voor diverse bouwprocessen de formele communicatie tussen partijen. De laatste cijfers die het BIM-loket heeft gegeven over het gebruik van VISI waren voor de Monitor van 2017. Toen is een eerste poging gedaan om het gebruik door overheden in cijfers zichtbaar te maken. Onderstaande gegevens hebben betrekking op de periode 2017 tot en met september: • 90 publieke opdrachtgevers die VISI hebben gebruikt (gemeenten, provincies, waterschappen en landelijke overheid samen); • 169.465 transacties zijn verstuurd door deze opdrachtgevers; • 260.891 verstuurde berichten; • 224.739 verstuurde bijlagen. Toen werd ook ingeschat dat het daadwerkelijke gebruik van VISI waarschijnlijk veel hoger ligt. Voor de Monitor 2018 zijn geen nieuwe cijfers aangeleverd.	

Over **IFC** (bouwwerkinformatiemodellen) is geen gebruiksinformatie bekend.

7. Juridische identificatie en verwijzing

Open standaard (op lijst sinds)	Over de standaard Data over gebruik en ontwikkeling in het gebruik	Beeld BFS
BWB Wet- en regelgeving (2/2/2016)	De standaard van het Basis Wetten Bestand. Regelt met een uniek nummer de identificatie van (onderdelen van) centrale wet- en regelgeving en de verwijzing daarnaar. KOOP (Kennis- en exploitatiecentrum Officiële Overheidspublicaties) gebruikt BWB in het Basiswettenbestand. Het Basis Wettenbestand is zowel beschikbaar via wetten.overheid.nl als via diverse services als open data. Gebruikers van de standaard zijn hergebruikers van de open data van het Basiswettenbestand in het juridisch domein. Hierbij gaat het om overheid (centraal en decentraal), uitgevers van juridische informatie, content integrators, uitvoeringsorganisaties en individuele aanbieders van juridische informatie, universiteiten en hogescholen. Verder is er sinds oktober 2017 een vernieuwde versie van LiDO, linkeddata.overheid.nl. 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. Het aantal bezoekers van LiDO is sinds de lancering in oktober 2017 opgelopen van circa 15.000 bezoekers per maand naar circa 40.000 per	

	maand medio 2018. Het gebruik van LiDO zou - voor het eerst in deze Monitor- kunnen dienen als een cijfermatige indicatie voor het gebruik van de standaarden BWB, JCDR en ECLI.	
JCDR Decentrale regelgeving (28/11/2013)	Juriconnect Decentrale Regelgeving (JCDR) regelt de identificatie van (onderdelen van) *decentrale* regelgeving en de verwijzing daarnaar. De JCDR standaard wordt gebruikt in de Centrale Voorziening voor Decentrale Regelgeving, DROP. Hieraan doen 471 diverse overheidsorganisaties mee. https://www.koopoverheid.nl/voor-overheden/gemeenten-provincies-en-waterschappen/drop/deelnemende-organisaties-drop En zoals hierboven reeds gemeld is er sinds oktober 2017 LiDO, linkeddata.overheid.nl waarin JDCR ook is opgenomen.	
ECLI Rechterlijke uitspraken 28/11/2013)	European Case Law Identifier (ECLI) geeft elke rechterlijke uitspraak binnen Europa een uniek nummer (identifier) waarmee rechterlijke uitspraken geciteerd en gevonden kunnen worden. In Nederland wordt de ECLI toegepast in de publicatie van alle (tucht) rechterlijke uitspraken door alle organisaties van de rechterlijke macht. Alle (tucht)rechterlijke uitspraken zijn met ECLI te vinden op rechtspraak.nl. Gebruikers van ECLI zijn rechters in vonnissen en arresten, rechtsgeleerden en ambtenaren. Ook in de rest van Europa is ECLI de leidende standaard voor het identificeren en citeren van rechterlijke uitspraken. Zoals hierboven ook vermeld bij de standaarden BWB en JCDR: Sinds oktober 2017 is er LiDO, linkeddata.overheid.nl . LiDO maakt onder meer ook gebruik van de ECLI standaard.	

8. Onderwijs en loopbaan

Open standaard (op lijst sinds)	Over de standaard Data over gebruik en ontwikkeling in het gebruik	Beeld BFS
NL_LOM Metadata onderwijscontent (29/5/2011)	NL LOM beschrijft welke metadata toegekend moeten worden aan educatieve content om de vindbaarheid en vergelijkbaarheid van leermateriaal te vergroten. Door het metadateren 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. Edurep is de educatieve zoekmachine voor het onderwijs. Edurep doorzoekt inmiddels 1,5 miljoen leerobjecten en 60 onderwijscollecties. De materialen zijn voorzien van metadata conform de NL LOM standaard. Edurep verwerkt 3 miljoen zoekopdrachten per maand: van lessen en toetsen tot educatief beeldmateriaal. De adoptie van de standaard lijkt buiten de Edurep beperkt. In de vergadering van 13 juni 2018 stemde het Forum Standaardisatie in met de evaluatie van de standaard NL LOM. De evaluatie wordt door een onafhankelijke partij uitgevoerd als onderdeel van regulier onderhoud op de pas-toe-of-leg-uit lijst, en kan resulteren in wijziging van status of aanvullende adoptieadviezen.	

Van **ePortfolio** (werkervaring en competenties) zijn geen gebruiksgegevens bekend. In de vergadering van 13 juni 2018 stemde het Forum Standaardisatie in met de evaluatie van de standaard E-Portfolio, die sinds 2010 op de pas-toe-of-leg-uit lijst staat. De evaluatie wordt door een onafhankelijke partij uitgevoerd als onderdeel van regulier onderhoud op de pas-toe-of-leg-uit lijst, en kan resulteren in wijziging van status of aanvullende adoptieadviezen.

9. Overig

Open standaard (op lijst sinds)	Over de standaard Data over gebruik en ontwikkeling in het gebruik	Beeld BFS
EML_NL Verkiezings-gegevens (28/11/2013)	De EML_NL standaard definieert de gegevens en de uitwisseling van gegevens bij verkiezingen die vallen onder de Nederlandse Kieswet. Het gaat daarbij om de uitwisseling van kandidaatgegevens en uitslaggegevens. EML_NL is opgenomen in Ondersteunende Software Verkiezingen (OSV). De Kiesraad stelt deze software ter beschikking voor gebruik tijdens verkiezingen. De voornaamste gebruikers zijn politieke partijen, gemeenten, hoofdstembureaus en centraal stembureaus. Navraag bij de Kiesraad leert het volgende. In 2017 heeft de Tweede Kamerverkiezing en enkele herindelingsverkiezingen plaatsgevonden. Tweede Kamer verkiezing op 15 maart 2017 OSV-software is beschikbaar gesteld aan: - ongeveer 40 politieke partijen; - 19 hoofdstembureau gemeenten; - 388 gemeenten (uiteindelijk is de software door ongeveer 2/3 van de gemeenten gebruikt); Gemeentelijke herindelingsverkiezingen op 22 november 2017. De OSV-software is beschikbaar gesteld aan: - de 6 nieuw te vormen gemeenten; - ongeveer 60 politieke partijen (lokale afdelingen; onbekend hoeveel er daadwerkelijk gebruik hebben gemaakt van de software). Het gebruik is daarmee niet significant toe of afgenomen vergeleken met de gegevens uit de Monitor uit 2017. Toen waren de gegevens namelijk als volgt: Referendum 6 april 2016 OSV-software is beschikbaar gesteld aan: - 19 hoofdstembureaus gemeenten - 393 gemeenten (alle gemeenten hebben ook daadwerkelijk gebruik gemaakt van de software) Gemeentelijke herindelingsverkiezing op 23 november voor één nieuw te vormen gemeente - de nieuw te vormen gemeente - ongeveer 15 politieke partijen (lokale afdelingen: onbekend hoeveel daadwerkelijk van de software gebruik gemaakt hebben).	

Over **STOSAG** (Afval verzameling en verwerking) zijn geen gebruiksgegevens bekend. De standaard zal naar verwachting in het najaar van 2018 de 'pas toe of leg uit' status verliezen.

Bijlage F. Gegevens over het gebruik van PDF op basis van 'crawler' (BFS)

Bureau Forum Standaardisatie is sinds de zomer van 2017 bezig met de ontwikkeling van een crawler die systematisch websites afzoekt naar documenten. Deze crawler verkeert zomer 2018 nog steeds in bèta. In 2018 is de crawler van BFS ingezet om een vergelijkbare steekproef te presenteren als in de monitor van vorig jaar. De tabellen hieronder geven de resultaten weer waarbij de resultaten uit 2018 worden vergeleken met de resultaten uit voorgaande monitors.

	PDF (ook versies die niet op de pas-toe-of-leg-uit lijst staan)				**ODF**				**Microsoft Office .doc(x)**			
	Zomer 2015	Zomer 2016	Zomer 2017	Zomer 2018	Zomer 2015	Zomer 2016	Zomer 2017	Zomer 2018	Zomer 2015	Zomer 2016	Zomer 2017	Zomer 2018
rijksoverheid.nl	118000	122000	118000	103	209	197	110	0	564	512	566	0
amsterdam.nl	36500	28500	25500	2310	0	0	0	0	3940	3940	4240	10
rotterdam.nl	40900	19600	6010	2605	0	0	0	0	903	587	263	89
utrecht.nl	27000	20200	6390	2590	0	0	0	0	247	142	17	1
drenthe.nl	6310	7580	6310	26	0	0	0	0	248	215	179	0
zuid-holland.nl	2080	15600	11000	4723	0	0	0	0	110	189	201	128
forumstandaardisatie.nl	1430	446	1270	537	22	11	13	4	54	14	14	5
ictu.nl	863	236	56	40	18	4	0	0	46	7	0	0

	PDF+ODF als % van alle bestanden				**Verhouding ODF : MS Office**			
	Zomer 2015	Zomer 2016	Zomer 2017	Zomer 2018	Zomer 2015	Zomer 2016	Zomer 2017	Zomer 2018
rijksoverheid.nl	99,5%	99,6%	99,5%	100,00%	0,37:1	1:1	0,72:1	NVT*
amsterdam.nl	94,2%	87,9%	85,6%	99,57%	0:1	0:1	0:1	0:1
rotterdam.nl	89,7%	97,1%	95,8%	96,70%	0:1	0:1	0:1	0:1
utrecht.nl	96,4%	99,3%	99,7%	99,96%	0:1	0:1	0:1	0:1
drenthe.nl	94,6%	97,2%	97,2%	100,00%	0:1	0:1	0:1	NVT*
zuid-holland.nl	97,4%	98,8%	98,2%	97,36%	0:1	0:1	0:1	0:1
forumstandaardisatie.nl	97,6%	97,0%	98,9%	99,08%	0,4:1	0,69:1	0,93:1	0,8:1
ictu.nl	95,5%	97,2%	100,0%	100,00%	0,50:1	0,55:1	NVT*	NVT*

** noch ODF-bestanden, noch MS Office-bestanden gevonden*

Omdat de crawler nog experimenteel is, kunnen hier nog geen definitieve conclusies aan worden verbonden.

In de Monitor 2019 zal worden bekeken of de gevonden documenten voldoen aan de eisen van duurzame toegankelijkheid (PDF/A) en digitale toegankelijkheid (digitoegankelijk.nl).

Bijlage G.
Rapportage 'IV-meting september 2018', Bureau Forum Standaardisatie

Halfjaarlijkse meting **Informatieveiligheidsstandaarden** Forum Standaardisatie

= September 2018 =

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

Om de voortgang van deze afspraken bij te houden voert het Forum twee keer per jaar een IV-meting uit. De laatste meting dateert van september 2018, waarbij 563 domeinnamen zijn getoetst. Uit de meting van september 2018 blijkt dat het gebruik van de standaarden doorzet.

Samenvatting:

Kijkende naar de eerste streefbeeldafspraak (deadline eind 2017) is de adoptie gestegen naar 87%. Ter vergelijking: begin 2018 was het 80%. Voor de tweede streefbeeldafspraak (deadline eind 2018: op elke overheidssite het slotje (https) geconfigureerd conform NCSC advies) is de adoptie gestegen naar 85%, begin dit jaar was het 78%. Voor de derde streefbeeldafspraak (beveiliging tegen e-mail afluisteren & strenge configuratie e-mail standaarden) is de adoptie momenteel 59%. Hierover zijn geen eerdere gegevens.

Een uitsplitsing van de resultaten naar overheidslaag laat zien dat de adoptie overal groeit. De mate van groei verschilt wel sterk, met name de waterschappen en provincies zijn sterk gegroeid met betrekking tot de webstandaarden. De waterschappen weten zelfs als eerste 100% adoptie te realiseren voor een individuele standaard (TLS). Overigens scoren de gemeenten het beste bij de webstandaarden en voor mail scoort het Rijk het hoogst terwijl het Rijk juist minder scoort bij het web. Bij de waterschappen valt op dat ze goed scoren op de webstandaarden, maar juist bij de mailstandaarden achterblijven.

Om het gebruik verder te bevorderen is het belangrijk om per doelgroep te kijken welke standaarden extra aandacht nodig hebben en of er 'quick wins' zijn. Om voor de webstandaarden 100% te behalen, is het waardevol om organisaties individueel aan te spreken. Zo is via het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) ook opgeroepen om aan te sturen op implementatie bij de achterblijvers, bijvoorbeeld door agendering via de koepels. Daarnaast kan een wettelijke verplichting helpen om de laatste paar procent zo ver te krijgen dat ze de standaarden ondersteunen. Voor de mailstandaarden kunnen echter nog veel grotere stappen gemaakt worden en zal het zonder aanvullende campagnes en/of activiteiten lastig worden om volledige adoptie (voor eind 2019) te realiseren.

Achtergrond

Sinds 2015 biedt het Platform Internetstandaarden[1] de mogelijkheid om via de website Internet.nl domeinen te toetsten op het gebruik van een aantal moderne internetstandaarden, waaronder een aantal informatieveiligheidsstandaarden, die op de 'pas toe of leg uit'-lijst van Forum Standaardisatie

[1] Platform Internet Standaarden is een gezamenlijk initiatief van de Internetgemeenschap en de Nederlandse overheid (Forum Standaardisatie, het Ministerie van Economische Zaken en Klimaat, en NCSC). Zie https://internet.nl/about/

staan. In datzelfde jaar is Forum Standaardisatie gestart om met behulp van Internet.nl een halfjaarlijkse meting van de adoptiegraad van informatieveiligheidsstandaarden voor overheidsdomeinen (web en e-mail) uit te voeren.

Die metingen hebben ertoe geleid dat het Nationaal Beraad in februari 2016 de ambitie uitsprak deze standaarden versneld te willen adopteren[2]. Dit betekent concreet dat voor deze standaarden niet het tempo van 'pas toe of leg uit' wordt gevolgd (d.w.z. wachten op een volgend investeringsmoment en dan de standaarden implementeren) maar dat actief wordt ingezet op implementatie van de standaarden op de kortere termijn[3].

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

Om welke standaarden gaat het

Het Nationaal Beraad en het OBDO hebben bovengenoemde afspraken gemaakt met betrekking tot de volgende standaarden.[4]

REALISATIEDATUM	WELKE STANDAARD GEADOPTEERD
uiterlijk EIND 2017	TLS/HTTPS: beveiligde verbindingen van websites DNSSEC: domeinnaambeveiliging SPF: anti-phishing van email DKIM: anti-phishing van email DMARC: anti-phishing van email
uiterlijk EIND 2018	HTTPS, HSTS en TLS conform de NCSC richtlijn (externe link): beveiligde verbindingen van alle websites
uiterlijk EIND 2019	STARTTLS en DANE: encryptie van mailverkeer SPF en DMARC: het instellen van strikte policies voor deze emailstandaarden.

Om welke domeinnamen gaat het

In totaal zijn in deze meting 563 (vorige keer 530) domeinnamen van overheidsorganisaties getoetst, bestaande uit:

- Domeinen die horen bij de deelnemers van het OBDO;
- De domeinen die horen bij voorzieningen van de basisinfrastructuur (GDI);
- De 30 best bezochte domeinen van Rijksoverheden (en uitvoerders);

2 http://www.binnenlandsbestuur.nl/digitaal/nieuws/nationaal-beraad-wil-sneller-moderne-e.9540822.lynkx
3 Onderdeel van deze afspraak is dat Forum Standaardisatie de voortgang van de adoptie meet en inzichtelijk maakt. De halfjaarlijkse IV-meting is ook onderdeel van de jaarlijkse Monitor Open standaarden beleid.
4 Voor meer informatie ga naar: https://www.forumstandaardisatie.nl/thema/iv-meting-en-afspraken

- De domeinen van de andere overheidsorganisaties die direct of indirect vertegenwoordigd zijn in het OBDO, zoals:
    - Uitvoerders (de Manifestpartijen);
    - Partijen die behorend tot Klein LEF;
    - Gemeenten;
    - Provincies;
    - Waterschappen.

Bij de selectie van de relevante domeinnamen is telkens gekozen voor het hoofdomein waarop de website van de overheidsorganisatie bereikbaar is. Daarnaast is gekozen voor het hoofdomein dat de desbetreffende overheidsorganisatie gebruikt voor e-mail (vaak dezelfde als voor web). Bij uitzondering zijn ook subdomeinen geselecteerd, bijvoorbeeld voor bekende inlogportalen of op verzoek van de beheerder.

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

Het betreft echter nog steeds een selectie van domeinnamen. De lijst is niet volledig en kan dat ook niet zijn omdat de overheid momenteel geen overzicht heeft over alle domeinnamen. De gemeten domeinen zijn bij lange na niet alle domeinen waar het OBDO direct en indirect voor verantwoordelijk is, zo beheert het ministerie van AZ al meer dan 6000 domeinnamen. Een 100% score op deze domeinen garandeert geenszins dat hiermee *alle* overheidsdomeinen beschermd zijn tegen bijvoorbeeld phishing.

Hoe wordt gemeten

De meting geeft de stand van zaken weer op de peildatum 25 september 2018. 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 kun je eenvoudig testen of je website of e-mail een aantal moderne internetstandaarden ondersteunen, ook de standaarden waarover streefbeeldafspraken zijn gemaakt zijn onderdeel van de test. Overigens heeft de score die een domeinnaam op Internet.nl kan halen (namelijk max. 100%) geen relatie met het resultaat uit deze meting aangezien wij toetsen op een subset van de standaarden. De website Internet.nl is een initiatief van het Platform Internetstandaarden. In het platform participeren verschillende partners uit de internetgemeenschap (Internet Society, RIPE NCC, SIDN en SURFnet) en Nederlandse overheid (Forum Standaardisatie, het Ministerie van Economische Zaken en Klimaat, en NCSC). Het uitgangspunt is dat Internet.nl de adviezen van Forum Standaardisatie en NCSC met betrekking tot de Internetstandaarden volgt.

De meting geeft geen inzicht in het risiconiveau van een bepaald domein. Zo is het aannemelijk dat de aantrekkelijkheid van misbruik hoger is bij domeinen van grote uitvoerders (zoals *phishing* met aanmaningen) dan bij domeinen van kleine gemeenten.

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

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.

Web-standaarden

Wij meten het gebruik van de beveiligingsstandaarden voor het web ook op domeinen die alleen gebruikt worden voor mail omdat dit vaak wel domeinnamen zijn die re-directen naar het hoofddomein. Ook hiervoor moet de standaarden juist worden toegepast en burgers weten vaak niet hoe deze domeinen worden gebruikt. Als je re-directs 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 als een zogenaamde 'parking page' wordt getoond. Alleen als een geregistreerd domein geen webpagina bevat dan is HTTPS niet nodig (en niet mogelijk).

DNSSEC	Domain Name System (DNS) is het registratiesysteem van namen en bijbehorende internetnummers en andere domeinnaaminformatie. Het is vergelijkbaar met een telefoonboek. Dit systeem kan worden bevraagd om namen naar nummers te vertalen en omgekeerd. Er is getest of de domeinnaam ondertekend is met DNSSEC, zodat de integriteit van de DNS-informatie is beschermd. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
TLS	Als een bezoeker een onbeveiligde HTTP-verbinding heeft met een website, dan kan een kwaadwillende eenvoudig gegevens onderweg afluisteren of aanpassen, of zelfs het contact volledig overnemen. Getest wordt of TLS is toegevoegd aan HTTP om de verbinding te beveiligen. Op Internet.nl heet deze subtest 'HTTPS available'. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
TLS cf. NCSC	We maken een onderscheid tussen 'TLS' en 'TLS conform NCSC'. In het eerste geval wordt gebruik gemaakt van TLS en in het tweede geval is TLS bovendien zodanig geconfigureerd dat deze voldoet aan de aanbevelingen van het Nationaal Cyber Security Center (NCSC)[5]. Zodat de vertrouwelijkheid, de authenticiteit en integriteit van een bezoek aan een website is gegarandeerd. De streefbeeldafspraak is om hier voor 2019 aan te voldoen.
HTTPS	Er wordt getest of je 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 is 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 is om hier voor 2019 aan te voldoen.

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

Mailstandaarden

Wij meten het gebruik van e-mailbeveiligingsstandaarden ook op domeinen waarvan een organisatie geen e-mail verstuurt. Dit is relevant omdat ook die domeinen worden misbruikt (burgers weten vaak niet dat deze domeinen niet door de organisatie worden gebruikt), en juist domeinen waarvandaan niet gemaild wordt, makkelijk kunnen worden geblokkeerd met behulp van SPF en DMARC (met de policies –all en p=reject). =

DMARC	Met DMARC kan een e-mailprovider kenbaar maken hoe andere (ontvangende) mailservers om dienen te gaan met de resultaten van de SPF- en/of DKIM-controles van ontvangen e-mails. Dit gebeurt door het publiceren van een DMARC beleid in het DNS-record van een domein. In deze test wordt alleen gekeken of DMARC beschikbaar is, niet of er beleid is ingesteld. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
DMARC Policy	Zolang er geen beleid is ingesteld weet de ontvanger nog niet wat te doen met verdachte e-mail. De configuratie moet op orde zijn. (Opm: Actieve policies zijn ~all en –all voor SPF, en p=quarantine en p=reject voor DMARC) Er wordt gecontroleerd of de syntax van de DMARC-record correct is en of deze een voldoende strikte policy bevat. De streefbeeldafspraak is om hier voor 2020 aan te voldoen
DKIM	Met DKIM kunnen e-mailberichten worden gewaarmerkt. De ontvanger van een e-mail kan op die manier controleren of een e-mailbericht écht van de afzender afkomstig is en of het bericht onderweg ongewijzigd is gebleven. Getest wordt of de domeinnaam DKIM ondersteunt. Voor non-mail domeinen waar dit goed is ingesteld heeft DKIM verder geen toegevoegde waarde. In de meting wordt dit weergegeven middels de score "NVT" (niet van toepassing) voor DKIM. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
SPF	SPF heeft als doel spam te verminderen. SPF controleert of een verzendende mailserver die e-mail namens een domein wil versturen, ook daadwerkelijk gerechtigd is om dit te mogen doen. Getest wordt of de domeinnaam een SPF-record heeft. De streefbeeldafspraak was om hier voor 2018 aan te voldoen.
SPF Policy	Aanvullend op bovenstaande test wordt gecontroleerd of de syntax van de SPF-record geldig is en of deze een voldoende strikte policy bevat om misbruik van het domein door phishers en spammers tegen te gaan. De streefbeeldafspraak is om hier voor 2020 aan te voldoen.
STARTTLS	STARTTLS in combinatie met DANE gaan het afluisteren of manipuleren van mailverkeer tegen. STARTTLS maakt het mogelijk om transportverbindingen tussen e-mailservers op basis van certificaten met TLS te beveiligen. Er wordt getest of de ontvangende mailservers (MX) ondersteuning bieden voor STARTTLS. De streefbeeldafspraak is om hier voor 2020 aan te voldoen. Als er geen mailservers aanwezig is voor het domein dan wordt dit weergeven met NVT. Dit geldt ook voor STARTTLS CF. NCSC, DANE en DNSSEC MX.

STARTTLS CF. NCSC[6]	Net zoals bij HTTPS kan er bij STARTTLS gebruik worden gemaakt van verschillende versies van het TLS en verschillende versleutelingsstandaarden (ciphers). Aangezien niet alle versies en combinaties als voldoende veilig worden beschouwd, is het belangrijk om hierin de juiste keuze te maken en ook regelmatig te controleren of de gebruikte instellingen nog veilig zijn. Getest wordt of STARTTLS is geconfigureerd zoals door het NCSC is aanbevolen. De streefbeeldafspraak is om hier voor 2020 aan te voldoen.
DANE	DANE, dat voortbouwt op DNSSEC, zorgt er in combinatie met STARTTLS voor dat een verzendende e-mailserver de authenticiteit van een ontvangende e-mailserver kan controleren en het kan het gebruik van TLS bovendien afdwingen. Getest wordt of de nameservers van de mailservers één of meer TLSA-records voor DANE bevatten. De streefbeeldafspraak is om hier voor 2020 aan te voldoen
DNSSEC MX	DNSSEC is een randvoorwaarde voor het instellen van DANE. Daarom wordt getest of de domeinnamen van de mailservers (MX) ondertekend zijn met DNSSEC. Dit in het kader van de streefbeeldafspraak om voor 2020 STARTTLS en DANE te ondersteunen.

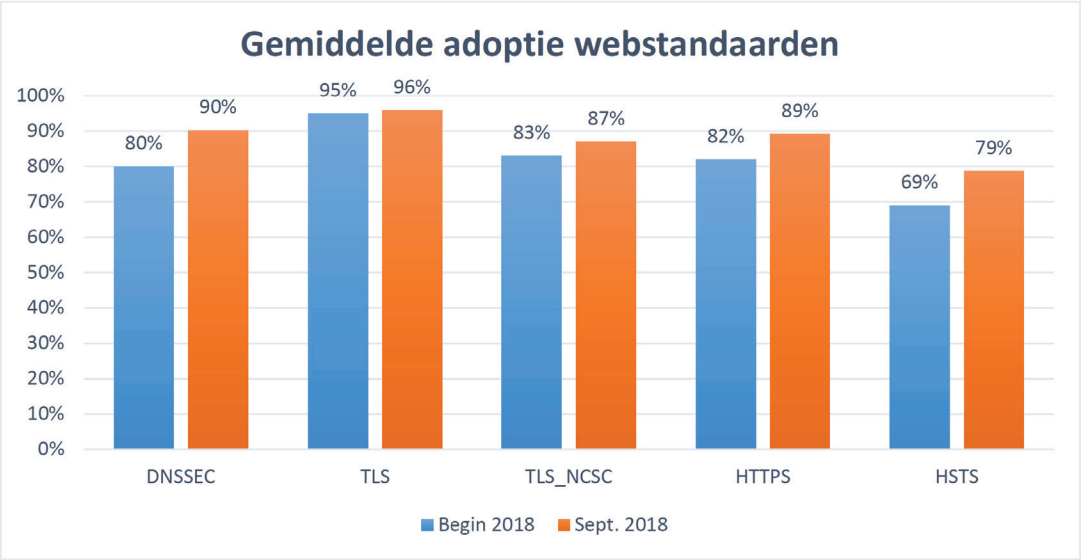
Resultaten meting september 2018

Eind augustus 2018 heeft het Bureau Forum Standaardisatie een eerste meting uitgevoerd, de resultaten zijn voorgelegd aan een aantal koepelorganisaties en stakeholders. Op 25 september 2018 heeft het Bureau Forum Standaardisatie de definitieve IV-meting uitgevoerd. Aangezien de eerste streefbeeldafspraak van het Nationaal Beraad afliep op 31 december 2017, is deze meting anders dan voorgaande metingen. Er zijn nieuwe resultaatafspraken toegevoegd en de te toetsten domeinnamen zijn aangepast. Dit maakt vergelijkbaarheid met de eerdere metingen moeilijker, ook omdat voor sommige standaarden geen eerdere cijfers beschikbaar zijn. Aan de hand van een aantal grafieken wordt de stand van zaken met betrekking tot adoptie toegelicht. De individuele resultaten van de test zijn te vinden op de website van het Forumstandaardisatie.

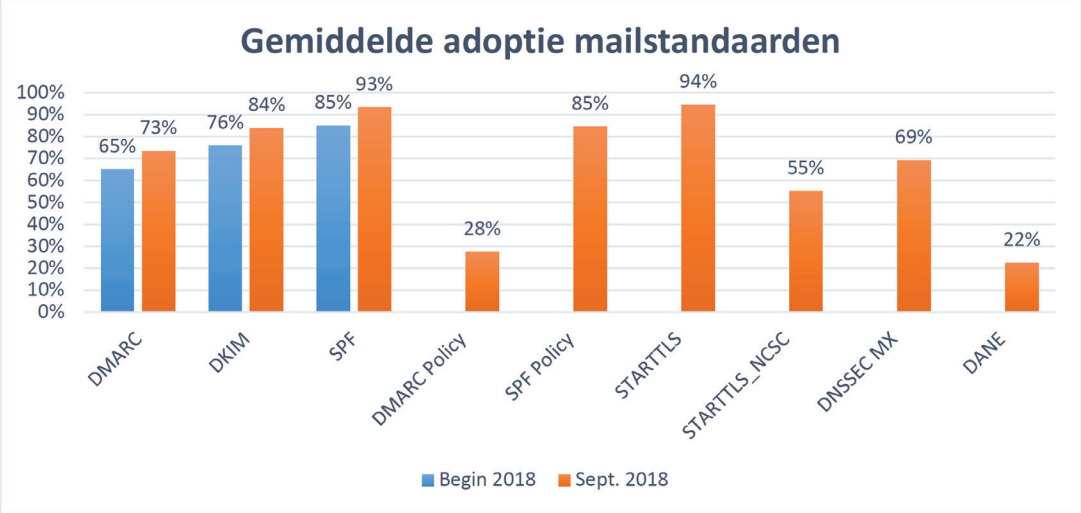
Per standaard

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

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



Voor de standaarden uit de eerdere metingen (DNSSEC, TLS en TLS cf NCSC) zien we dat de groei nog steeds doorzet, met DNSSEC als uitschieter met 10 procentpunten naar 90%. Wel valt op dat de adoptie van TLS niet tot nauwelijks meer stijgt. Hiervoor is een 'één op één' benadering nodig om de 100% te halen. Van de standaarden met als streefdatum uiterlijk 2018 zien we dat HTTPS en TLS cf NCSC een hoge adoptiegraad hebben terwijl HSTS nog wat achterblijft met 79%, maar wel groeit.



Voor de standaarden uit de eerdere metingen (DMARC, DKIM en SPF) zien we dat de groei nog steeds goed doorzet. DMARC blijft, ondanks een stijging van 8 procentpunten, nog wel achter met 73%. Dat deze groei zich doorzet is positief aangezien het risico bestaat dat door het aflopen van de resultaatafspraak de aandacht voor het gebruik van de standaard afneemt.

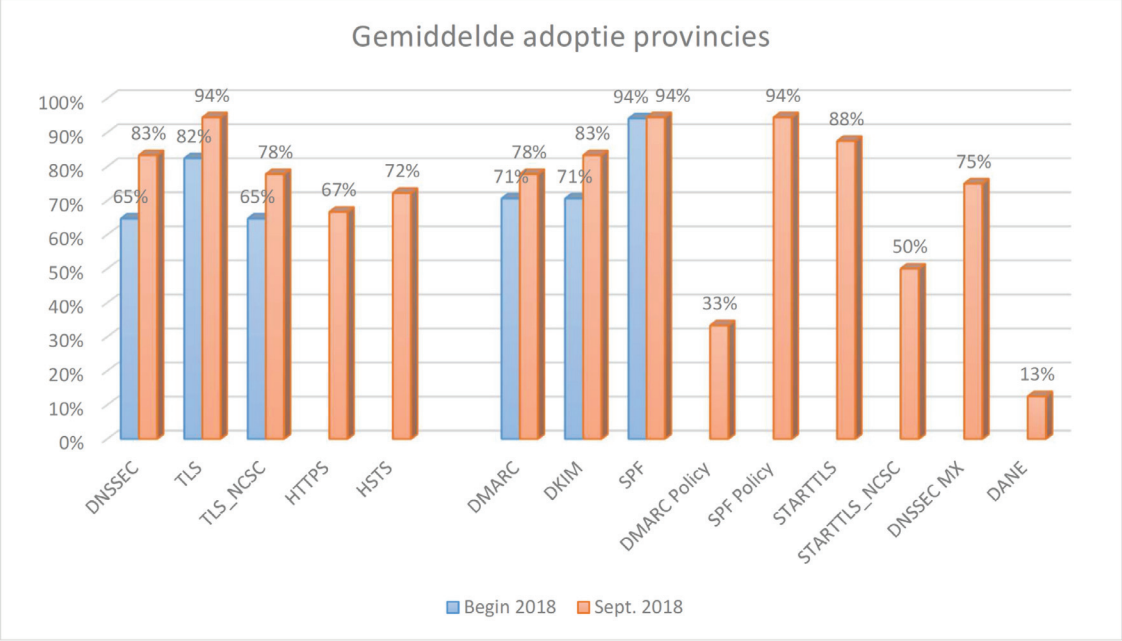
Voor de standaarden met als streefdatum uiterlijk 2019 zien we dat SPF Policy een hoge adoptiegraad heeft met 85% en STARTTLS zelfs al op 94% zit. Terwijl de gewenste configuratie (conform NCSC) nog wel wat achterblijft met 55%. Hier zie je hetzelfde als bij TLS voor web, waar de NCSC configuratie ook achterblijft, maar dat dit in de loop van de tijd wel meer naar elkaar toetrekt. De grote achterblijvers bij mail zijn DANE en DMARC Policy met respectievelijk 22% en 27% adoptie. Voor DANE is een stijging redelijk makkelijk te realiseren omdat DNSSEC MX op de 69% zit. Ook voor DMARC moet het mogelijk zijn omdat veel organisaties al wel DMARC beschikbaar hebben. Verder zien we, in lijn met de eerdere metingen, dat de aandacht voor de web-standaarden significant groter is dan de aandacht voor de mail-standaarden.

Per overheidslaag

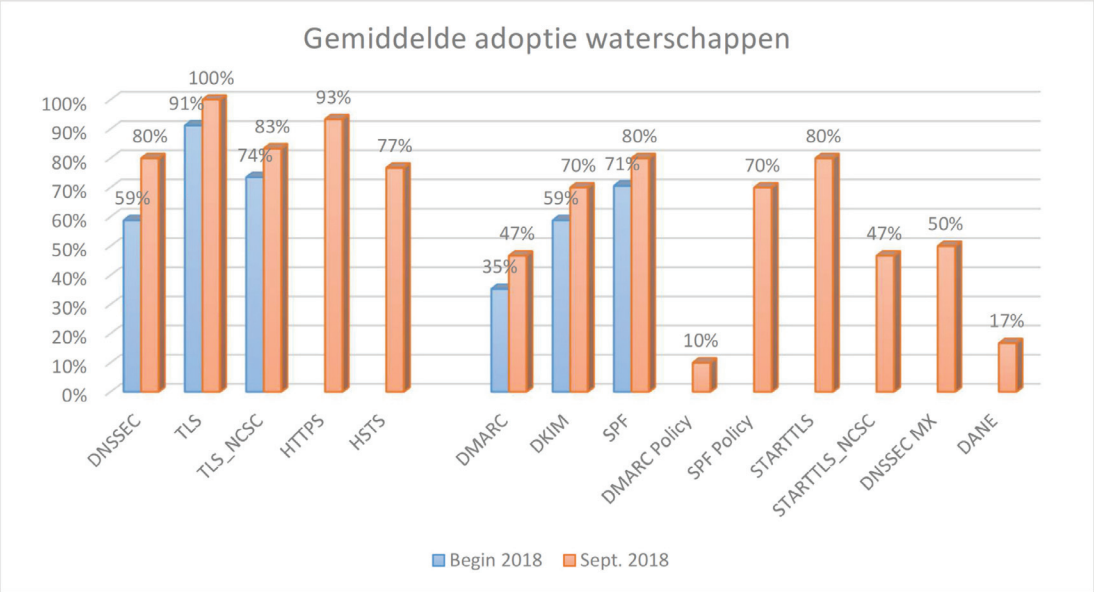
Een uitsplitsing van de resultaten naar overheidslaag laat zien dat in iedere overheidslaag de adoptie groeit. De mate van groei verschilt wel sterk, met name de waterschappen en provincies zijn sterk gegroeid met gemiddeld 12 procentpunt (waterschappen) en 10 procentpunten (provincies). Dit berekend over de standaarden DNSSEC, TLS, TLS cf NCSC, SPF, DKIM en DMARC. De waterschappen weten daarnaast 100% adoptie te realiseren voor TLS.

Wat verder opvalt in relatie tot de nieuwe streefbeeldafspraken is dat de standaard SPF Policy en de aanwezigheid van STARTTLS overal goed scoren. Terwijl voor de standaarden DANE en DMARC Policy het Rijk en de uitvoeringsorganisaties relatief beter scoren dan de provincies, waterschappen en gemeenten.

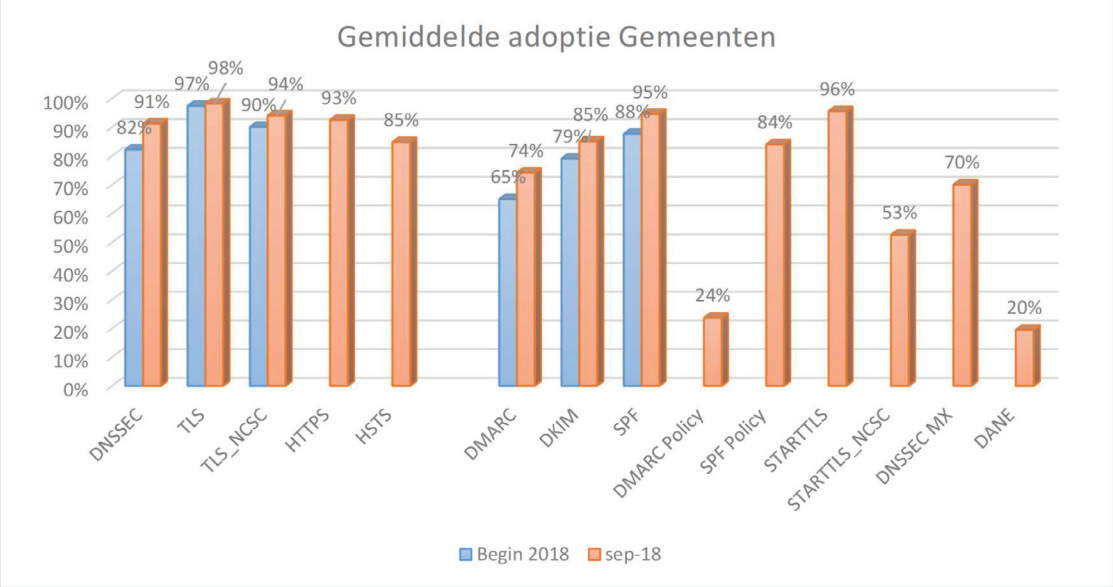
Provincies



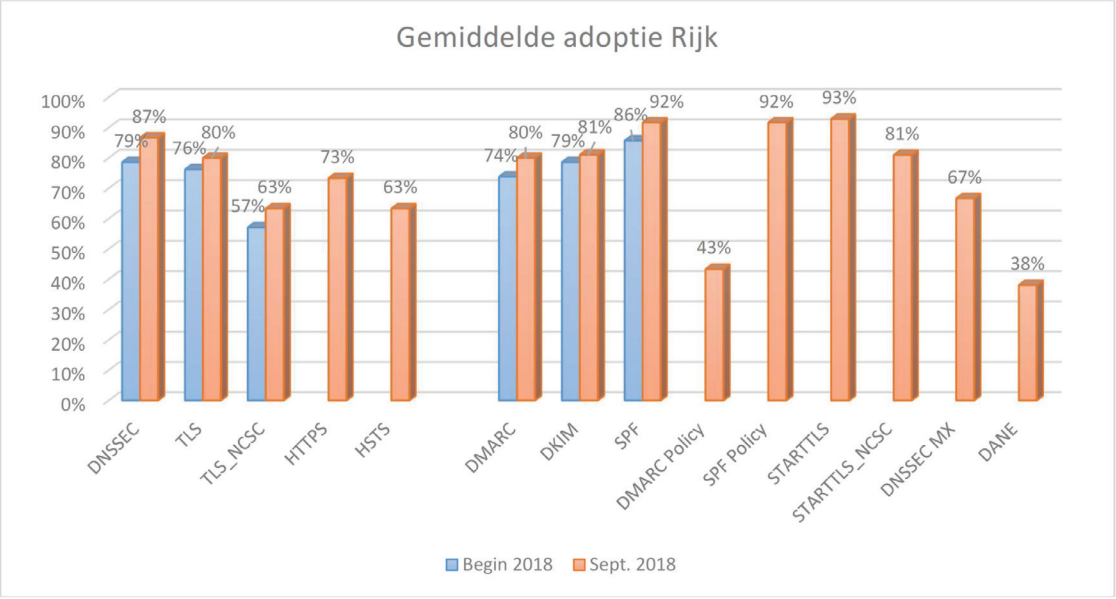
Waterschappen



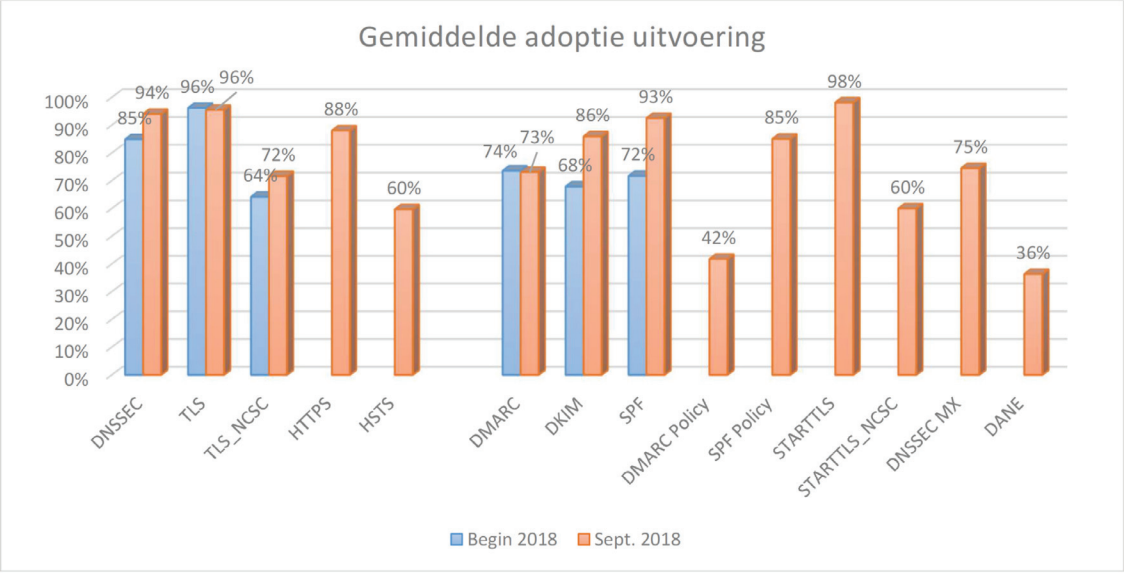
Gemeenten



Het Rijk

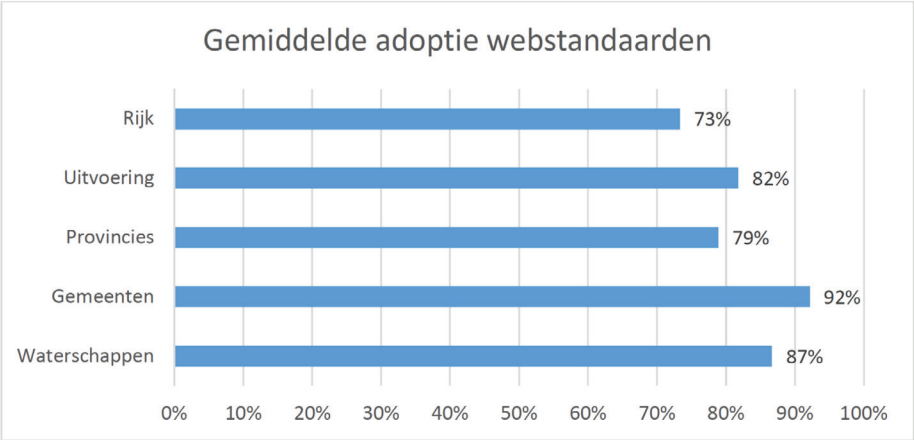


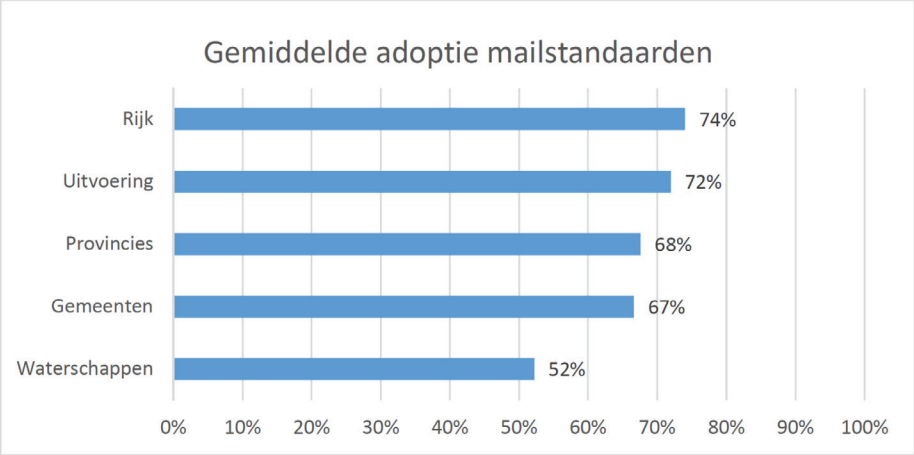
Uitvoering



Als we een vergelijking maken tussen overheidslagen voor de webstandaarden en de mailstandaarden.
Dan valt op dat bij de webstandaarden de gemeenten het best scoren met een gemiddelde adoptie van

92%. Bij de mailstandaarden scoort het Rijk het hoogst met een gemiddelde adoptie van 74% en dat terwijl het Rijk juist minder scoort bij de webstandaarden. Dit laatst komt met name omdat er relatief veel 'redirect' domeinnamen van de afzonderlijke ministeries zijn getoetst in de meting. Ook deze redirects moeten goed worden dichtgezet, dit verdient daarom ook extra aandacht bij aanvullende adoptieacties. Bij de waterschappen valt op dat ze goed scoren op de webstandaarden, maar juist bij de mailstandaarden achterblijven. Voor de waterschappen is het gewenst om extra adoptieacties voor met name de mailstandaarden te organiseren.





Conclusie verklaring van de resultaten
Voor de standaarden uit de eerdere metingen (DNSSEC, TLS en TLS cf NCSC, DKIM, DMARC en SPF) zien we dat de groei doorzet, met DNSSEC als uitschieter met 10 procentpunten naar 90%. Wel valt op dat de adoptie van TLS niet tot nauwelijks meer stijgt. Om 100% te bereiken is dan ook een meer 'één op één' benadering nodig. Van de standaarden met als streefdatum uiterlijk 2018 (HTTPS, HSTS en TLS cf NCSC) zien we dat er al een hoge adoptiegraad is. Volledige adoptie voor 2019 zal echter niet worden gerealiseerd.

Als we kijken naar de nieuwe streefbeeldafspraak dan verloopt de adoptie van de standaarden SPF Policy en STARTTLS erg goed. Voor deze standaarden kan worden verwacht dat ze eind 2019 zo goed als volledig

zijn geadopteerd, wel heeft de correcte implementatie van STARTTLS cf NCSC nog extra aandacht nodig. Tot slot blijft de adoptie van DMARC Policy en DANE erg achter al verschilt dit sterk per overheidslaag.

Zonder aanvullende campagnes, activiteiten en of verplichtingen zal zo goed als volledige adoptie eind 2019 lastig te realiseren zijn voor de mailstandaarden. Dit geldt in minder mate ook voor de mail-standaarden uit de eerste streefbeeldafspraak. Belangrijk is om per doelgroep te kijken welke standaarden extra aandacht nodig hebben en of er 'quick wins' zijn. Om voor de webstandaarden toch 100% te halen, is het misschien mogelijk om organisaties individueel aan te spreken en te helpen. Dit bij voorkeur via de koepelorganisaties. Daarnaast kan een wettelijke verplichting helpen om de laatste paar procent zo ver te krijgen dat ze de standaarden ondersteunen.

PBLQ

Monitor Open Standaarden Voorzieningen 2018

Versie 1.1
30-11-2018

PBLQ
verbinders in de informatiesamenleving

Inhoudsopgave

1. Inleiding 1

1.1 Aanleiding 1
1.2 Opdrachtformulering 1
1.3 Werkwijze 1
1.4 Aandachtspunten voor de lezer 2
1.4.1 Voorzieningen en standaarden geordend op basis van functionaliteit 2
1.4.2 Status 2
1.4.3 Relevantie standaard 2
1.4.4 Wijze van toetsen standaard 3

2. Identificeren en authenticeren 5

2.1 DigiD 5
2.2 DigiD Machtigen 6
2.3 PKIoverheid 8
2.4 Beheervoorziening BSN en GBA-V 10
2.5 Rijkspas 11
2.6 Stelsel elektronische toegangsdiensten 13

3. Dienstverlening en informatieverstrekken 14

3.1 MijnOverheid 14
3.2 Berichtenbox voor bedrijven 17
3.3 Overheid.nl 18
3.4 Ondernemersplein 20
3.5 Samenwerkende catalogi 22
3.6 Rijksportaal 23
3.7 ODC Noord 24
3.8 Doc-Direkt 26
3.9 Rijksoverheid.nl 28

4. Gegevens en registreren 30

4.1 Basisregistraties 30
4.1.1 NHR (Handelsregister) 30
4.1.2 BAG (Basisregistraties Adressen en Gebouwen), BRK (Basisregistratie Kadaster), BGT (Basisregistratie Grootschalige Topografie), WOZ (Basisregistratie Waarde Onroerende Zaken) 32
4.1.3 BRT (Basisregistratie Topografie) 35
4.1.4 BRV (Basisregistratie Voertuigen) 37
4.1.5 BRI (Basisregistratie Inkomen) 39

4.2 Digilevering 40
4.3 Digimelding 41
4.4 Stelselcatalogus 43
4.5 P-Direkt 44

5. Dienstverlening en verbinden 47

5.1 eFactureren 47
5.2 SBR 47
5.3 Digipoort 49
5.4 Diginetwerk 50
5.5 Tenderned 51
5.6 DWR 53
5.7 Digi-Inkoop 55

Bijlage A Geïnterviewde personen 58

1. Inleiding

1.1 Aanleiding

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

1.2 Opdrachtformulering

Doel van deze opdracht is het creëren van een beeld van de toepassing van open standaarden bij de verschillende voorzieningen van de Generieke Digitale Infrastructuur (GDI), plus een aantal voorzieningen die niet bij de GDI behoren.

1.3 Werkwijze

Voor dit onderzoek is gebruik gemaakt van de 'pas toe of leg uit'-lijst van 1 mei 2018. Per voorziening is gekeken of de standaarden op deze lijst relevant zijn. Daarbij is telkens uitgegaan van de eindgebruiker. Dat is diegene die in de keten baat zou moet hebben bij het gebruik van open standaarden. Dit is expliciet zo gekozen, omdat het beleid ten aanzien van standaardisatie vooral gericht is op het stimuleren van interoperabiliteit. In eerdere onderzoeken is gebleken dat beheerders van voorzieningen soms terminologie gebruiken zoals 'voorbereid' zijn op een standaard, het ‘deels geïmplementeerd’ hebben of 'standaard xyz-ready zijn’. Hiermee bedoelen zij dat ze zelf voldoen aan de standaard of bezig zijn de standaard te implementeren, maar dat de andere partijen in hun keten nog geen gebruik kunnen maken van de standaard. Er is bijgevolg dan ook geen sprake van interoperabiliteit op basis van gebruik van de standaard. Wanneer er geen sprake is van interoperabiliteit hebben we dat in deze rapportage aangegeven.

In dit onderzoek wordt per voorziening een overzicht opgesteld van relevante standaarden en de mate waarin daarvan gebruik wordt gemaakt. Het vertrekpunt daarbij is telkens het overzicht van vorig jaar. Waar mogelijk zijn de standaarden opnieuw getoetst. Daarbij maken we onder meer gebruik van de testen die beschikbaar zijn via https://internet.nl. Hiermee kan voor een groot deel van de standaarden getoetst worden of eraan voldaan wordt. Daarnaast kijken we – voor zover mogelijk – of de geplande activiteiten inmiddels uitgevoerd zijn. Voor nieuwe voorzieningen maken we een inschatting welke standaarden relevant zijn. Voor nieuwe standaarden op de lijst maken we een inschatting of ze relevant zijn voor de voorzieningen.

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

1.4 Aandachtspunten voor de lezer

1.4.1 Voorzieningen en standaarden geordend op basis van functionaliteit

In tegenstelling tot vorig jaar zijn de voorzieningen in deze monitor op basis van functionaliteit gegroepeerd conform de indeling die eerder in de Monitor Generieke Digitale Infrastructuur 2018 is gehanteerd. De volgende functionele groepen worden in deze monitor onderscheiden:

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

Omdat niet alle voorzieningen die in dit onderzoek worden getoetst zijn opgenomen in de Monitor Generieke Digitale Infrastructuur 2018 zijn de overige voorzieningen ingedeeld in bovenstaande categorieën in overleg met de opdrachtgever.

Ook de ordening van de standaarden in de tabellen is dit jaar anders dan voorheen. Op verzoek van de opdrachtgever is de volgorde van de flyer[1] met het overzicht van standaarden van het Forum Standaardisatie aangehouden.

1.4.2 Status

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

- Ja: De voorziening is conform[2] de standaard,
- Nee: De voorziening is niet conform de standaard,
- Deels: Onderdelen van de voorziening zijn conform aan, maar niet alle onderdelen[3],
- Gepland: Er zijn concrete plannen (gekoppeld aan een datum) om de voorziening op korte termijn conform te maken aan de standaard.

1.4.3 Relevantie standaard

Voor de relevantiebepalingen zijn per standaard de beschrijvingen van het functioneel toepassingsgebied en van het organisatorisch toepassingsgebied, zoals vermeld op de pas-toe-of-leg-uit lijst van het Forum Standaardisatie gehanteerd.[4] Standaarden die niet relevant zijn voor een voorziening, zijn niet in de tabel opgenomen. In een beperkt aantal gevallen is onder de tabel nog een toevoeging opgenomen over

[1] https://www.forumstandaardisatie.nl/sites/bfs/files/Lijst_verplichte_open_standaarden_juli_2018_1.pdf

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

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

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

standaarden die in de eerste inschatting wel relevant leken, maar dat bij nadere inspectie (nog) niet zijn. Ook in gevallen waar verwarring zou kunnen ontstaan over de relevantie is een nadere toelichting onder de tabel opgenomen. Daarnaast is voor de standaarden die dit jaar nieuw zijn op de lijst, opgenomen of ze relevant zijn. Deze inschatting is samen met de beheerders van de voorzieningen gemaakt.

1.4.4 Wijze van toetsen standaard

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

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

Gebruik van internet.nl
Voor een groot aantal standaarden hebben we gebruik gemaakt van de website internet.nl. De website is een initiatief van het Platform Internetstandaarden[5] en maakt het mogelijk om het gebruik van standaarden te toetsen op basis van een specifiek domein. Het betreft de volgende standaarden:

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

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

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

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

Het besluit maakt deel uit van een breder pakket aan maatregelen dat een inclusieve benadering van digitale overheidsdienstverlening moet realiseren. Uitgangspunt daarbij is dat mensen met en zonder beperking op gelijke basis moeten kunnen deelnemen aan de maatschappij. Als websites goed in elkaar zitten kunnen ze door iedereen worden gebruikt, ook door bezoekers met een beperking.
Het besluit verplicht overheidsinstanties om te zorgen dat hun websites en/of mobiele applicaties toegankelijk zijn conform de geldende standaard EN 301 549, en daarover een actuele toegankelijkheidsverklaring af te geven.
Er geldt een gefaseerde toepassing. Nieuwe websites gepubliceerd vanaf 23 september 2018 moeten uiterlijk op 23 september 2019 voldoen. Bestaande website gepubliceerd vóór 23 september 2018 moeten een jaar later voldoen. Mobiele applicaties moeten uiterlijk 23 juni 2021 voldoen.

In deze monitor zijn we, gelet op de invoeringsdatum van 1 juli 2018 en de gafaseerde invoeringssystematiek zijn we voor dit onderzoek nog uitgegaan van de systematiek voor Webrichtlijnen. Concreet: is er een toets uitgevoerd en is er een onderbouwing in de vorm van een toetsingsrapport, een beschrijving van de toets, of een verwijzing naar een certificaat van een inspectie-instelling zoals Accessibility of Waarmerk drempelvrij.nl.

De BIR en ISO 27001/2
Binnen de rijksoverheid dient elke organisatie een eigen implementatie van de BIR te hebben. De BIR is gebaseerd op ISO 27001. Indien een organisatie voldoet aan de BIR, dan voldoen zij binnen de context van dit rapport ook aan de verplichting om de ISO 27001/2 standaard te gebruiken. Waar er een aparte certificering op het gebied van ISO 27001 is toegekend, geven wij dit apart aan.

TLS
In de toelichting bij deze standaard op de lijst staat de volgende tekst:

> “TLS 1.2 wordt door experts beschouwd als de meest veilige versie. Deze versie is daarom de norm. Deze is echter niet ‘backwards compatible’. Ten behoeve van de interoperabiliteit dienen daarom ook de versies 1.1 en 1.0 toegepast te worden, met name als wederpartijen (nog) niet klaar zijn voor versie 1.2.”

In dit onderzoek krijgen daarom partijen die versie 1.2 (nog) niet ondersteunen de score ‘nee’.

2. Identificeren en authenticeren

2.1 DigiD

Beheerorganisatie: Logius

Werking en inhoud van DigiD (bron: Monitor GDI 2018)
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 al met DigiD geregeld kunnen worden zijn o.a. het doen van belastingaangifte, het regelen van toeslagen, het aanvragen van uitkeringen, het aanvragen van studiefinanciering, het inzien van het landelijk diplomaregister, het aanvragen van een omgevingsvergunning, het registreren van donorschap, het inzien van pensioenoverzichten en zorgverzekeringen en het aanvragen van het rijexamen.

Standaard	Status	Toelichting
		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 release 4.5 van DigiD en inmiddels operationeel. Ook de mailservers voldoen aan de standaard (zie: https://internet.nl/site/digid.nl/ en https://internet.nl/mail/digid.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	DigiD maakt gebruik van HTTPS voor de communicatie tussen clients (zoals browsers) en servers. Verder ondersteunt de DigiD website HSTS-policy met een geldigheidsduur van 1 jaar (zie: https://internet.nl/site/digid.nl/).
IPv4 en IPv6 (Internetnummers)	Ja	De website DigiD.nl is via IPv6 toegankelijk. Inmiddels verlopen ook de mailstromen via IPv6 (zie https://internet.nl/mail/digid.nl/ en https://internet.nl/site/digid.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Rijk (BIR) 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's) aan de eigenaar (BZK/DGOBR).
SAML (Inloggegevens)	Ja	DigiD biedt aan afnemers een SAML-koppelvlak. De meeste afnemers zitten nog op het A-select koppelvlak. SAML-berichtuitwisseling in het eID stelsel (http://www.eid-stelsel.nl) zal anders zijn dan die van DigiD. Om partijen niet tot meerdere migraties te dwingen houdt DigiD het A-select koppelvlak nog in stand.

SPF (Preventie van mailspoofing/phishing)	Ja	SPF is relevant voor DigiD bij alle mails vanuit de DigiD applicatie, en DigiD voldoet ook aan deze standaard (zie https://internet.nl/mail/digid.nl/).
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Gepland	De mailserver van DigiD past STARTTLS toe (zie https://internet.nl/mail/digid.nl/). Planning voor de implementatie van DANE is Q4 2018
TLS (Beveiligde, versleutelde verbindingen)	Ja	DigiD ondersteunt TLS v1.0 en TLS v1.2. TLS 1.1 wordt niet ondersteund, omdat Logius een sterke voorkeur heeft voor TLS 1.2. Om brede comptabiliteit mogelijk te maken wordt TLS 1.0 nog steeds ondersteund.
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Ja	DigiD voldoet aan de WR2-AA richtlijnen van het Waarmerk drempelvrij.nl (zie https://www.digid.nl/toegankelijkheid/). Het certificaat is een jaar geldig. Inspectiedatum is 22 december 2017.

Ten opzichte van 2017 voldoet Digid aan de WR2-AA richtlijnen van het Waarmerk drempelvrij.nl. De STARTTLS/DANE standaard is van de status ‘ja’ naar de status ‘gepland’ gegaan, omdat er een aanstaande implementatie van DANE gepland is voor Q4 2018.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Digid voldoet aan de nieuw opgenomen standaard DMARC. DMARC is voor DigiD geconfigureerd als een van de Anti-phishing maatregelen.

Concluderend, moet voor DigiD de volgende standaard nog (volledig) worden geïmplementeerd: STARTTLS/DANE.

2.2 DigiD Machtigen

Beheerorganisatie: Logius

Werking en inhoud van DigiD Machtigen

DigiD Machtigen stelt burgers in staat anderen namens hen te machtigen. DigiD Machtigen wordt beheerd door Logius. Onderstaande antwoorden zijn grotendeels gebaseerd op de Verantwoording Open Standaarden die jaarlijks door Logius zelf opgesteld wordt.

Standaard	Status	Toelichting
		Internet en beveiliging

DMARC (Anti-phishing)	Ja	Digid Machtigen ontvangt en verstuurd geen email op het domein machtigen.digid.nl. Er is een DMARC record (zie: https://internet.nl/mail/machtigen.digid.nl/)
DNSSEC (Beveiligde domeinnamen)	Ja	Het domein https://machtigen.digid.nl voldoet aan DNSSEC (zie: https://internet.nl/site/machtigen.digid.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	Deze standaarden zijn geïmplementeerd (zie: https://internet.nl/site/machtigen.digid.nl/).
IPv4 en IPV6 (Internetnummers)	Ja	Zowel IPv6 als IPv4 worden ondersteund (zie: https://internet.nl/site/machtigen.digid.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Rijk (BIR) van toepassing die is gebaseerd op NEN-ISO27001. Logius heeft zich over toepassing van de BIR norm verantwoord door het afgeven van In Control Verklaringen (ICV's) aan de eigenaar (BZK/DGOBR).
SAML v2.0 (Inloggegevens)	Deels	Het authenticatie koppelvlak met eHerkenning voldoet aan de SAML standaard. Het authenticatie koppelvlak met DigiD maakt geen gebruik van SAML. Dit koppelvlak is door DigiD Machtigen gerealiseerd toen DigiD nog geen SAML koppelvlak bood. Overgang naar een SAML koppelvlak is voorzien bij aansluiting op het eID stelsel. Naast authenticatie gebruikt DigiD Machtigen de SAML standaard ook om een getekend machtigingsbewijs af te geven, namelijk als een SAML assertion.
SPF (Preventie van mailspoofing/phishing)	Ja	DigiD Machtigen verstuurd geen email aan gebruikers. Er is wel een SPF record aangemaakt voor het domein: machtigen.digid.nl welke aangeeft dat er vanaf dit domein geen email wordt verstuurd.
TLS v1.2, v1.1 en v1.0 (Beveiligde, versleutelde verbindingen)	Ja	TLS is geïmplementeerd. DigiD Machtigen ondersteunt TLS v1.0, TLS v1.1 en TLS v1.2. Voor brede comptabiliteit worden TLS 1.0 en 1.1 nog ondersteund.
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Gepland	Wijzigingen ten behoeve van Digitoegankelijk compliance zijn in Q2 2018 geïmplementeerd. In Q3 wordt dit getoetst door betrokken partijen.

(Toegankelijkheid web content)		
PDF/A en PDF 1.7 (Documentpublicatie/archivering)	Ja	De voorziening voldoet aan deze standaard.
		Overig
Digikoppeling 2.0	Deels	Recent ontwikkelde koppelvlakken en/of nieuwe versies van bestaande koppelvlakken zijn Digikoppeling compliant (bijvoorbeeld DVS 2017). Er zijn echter nog koppelvlakken waarvan geen Digikoppeling compliant versie is gemaakt en/of koppelvlakken waar nog diensten afnemers op aangesloten zitten (bijvoorbeeld PBS). Deze koppelvlakken bestaan uit de tijd dat de Digikoppeling standaard in ontwikkeling was en voldoen deels aan de uiteindelijk ontstane Digikoppeling standaard. Het is de bedoeling dat bestaande dienst afnemers overgaan naar de nieuwe koppelvlakken. Hier wordt niet actief op gestuurd. Door ontwikkelingen rondom eID, eIDAS en Digid Machtigen moeten afnemers in de toekomst gebruik maken van andere koppelvlakken, waardoor gebruik van de niet compliant koppelvlakken zal afnemen.

Ten opzichte van 2017 zijn wijzigingen ten behoeve van Digitoegankelijk in Q2 2018 geïmplementeerd. In Q3 2018 wordt dit getoetst door betrokken partijen. De status is verhoogd van nee naar gepland.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Deze standaard is geïmplementeerd.

Concluderend, moeten voor Digid Machtigen nog de volgende standaarden (volledig) worden geïmplementeerd: Digikoppeling 2.0, Digitoegankelijk (EN 301 549 met WCAG 2.0), SAML v2.0.

2.3 PKIoverheid

Beheerorganisatie: Logius

Werking en inhoud van PKIoverheid (bron: Monitor GDI 2018)
Wat DigiD en eHerkenning zijn voor respectievelijk burgers en bedrijven, is PKIoverheid voor de overheid, PKIoverheid bevat de digitale certificaten die door zogenaamde Trust Service Providers (TSP's) beschikbaar worden gesteld aan overheidsorganisaties, opdat zij veilig met elkaar kunnen communiceren.
Met PKIoverheid wordt de betrouwbaarheid van informatie-uitwisseling via e-mail en websites op basis van Nederlandse (en Europese) wetgeving geborgd. Er zijn zeven TSP's die PKIoverheidscertificaten verstrek- ken. Dit zijn: KPN, ESG, QuoVadis, Digidentity, CIBG, het Ministerie van Infrastructuur en Waterstaat en het Ministerie van Defensie.

Standaard	Status	Toelichting
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	Pkioverheid.nl voldoet aan DMARC.
DNSSEC (Beveiligde domeinnamen)	Ja	Het PKIoverheid-deel van de website van Logius en de website van PKIoverheid maken gebruik van DNSSEC (zie: https://internet.nl/domain/crl.pkioverheid.nl/ en https://internet.nl/domain/www.logius.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	Deze standaard wordt toegepast door de voorziening (zie: https://internet.nl/domain/crl.pkioverheid.nl/ en https://internet.nl/domain/www.logius.nl/).
IPv4 en IPV6 (Internetnummers)	Gepland	IPv6 is geïmplementeerd voor de informatiepagina's van PKIoverheid op de Logius website (zie: https://internet.nl/domain/www.logius.nl/). De PKIoverheid specifieke applicatiepagina's zijn op dit moment nog niet geschikt voor IPv6 (zie: https://internet.nl/domain/crl.pkioverheid.nl/). Dit is gepland voor Q4 2019.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Primair is het Webtrust normenkader van toepassing op PKIoverheid. Dit kader kent strengere eisen dan deze ISO standaarden vereisen. Implementatie van de BIR is daarnaast uitgevoerd op basis van best effort.
TSL 1.2 en 1.1	Ja	Het PKIoverheid deel van de website van Logius maakt gebruik van TLS 1.1 en 1.2 en de website van PKIoverheid zelf maakt gebruik van TLS 1.2 (zie: https://internet.nl/domain/crl.pkioverheid.nl/ en https://internet.nl/domain/www.logius.nl/).
		Document en (web/app)content
OWMS (Metadata overheidsinformatie)	Ja	Het PKIoverheid deel van de website van Logius voldoet aan de standaard, maar niet op de website van PKIoverheid (deze informatie is niet bedoeld voor hergebruik van overheidsinformatie).
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie /archivering)	Ja	Documenten die via de websites beschikbaar worden gesteld worden volgens PDF/A opgesteld.

Ten opzichte van 2017 is er een concrete planning voor de implementatie van IPv6 in Q4 2019.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. PKIoverheid voldoet aan de standaard DMARC.

Concluderend, moet voor PKIoverheid nog de volgende standaarden (volledig) worden geïmplementeerd: IPv4 en IPV6.

2.4 Beheervoorziening BSN en GBA-V

Beheerorganisatie: Rijksdienst voor Identiteitsgegevens (RvIG), Ministerie BZK

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

Standaard	Status	Toelichting
		Internet en beveiliging
HTTPS/HSTS (Beveiligd, Versleuteld Webverkeer)	Ja	Alle aangeboden webservices draaien HTTPS en HSTS.
IPv4 en IPV6 (Bereikbaarheid nieuwe Internetnummers)	Nee	De voorzieningen zijn IPv6-ready in datacentrum, maar er wordt momenteel gebruik gemaakt van IPv4 adressen via Gemnet/Diginetwerk. Het is nog niet bekend wanneer er met het ontsluiten op IPv6 zal worden begonnen. Wel is inmiddels de ontsluiting via DigiNetwerk begonnen.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De Rijksdienst voor Identiteitsgegevens heeft een beveiligingsplan op basis van de BIR. Hier worden externe audits op gedaan. Er is een In Control Verklaring (ICV) aanwezig.
TLS v1.2, v1.1 en v1.0 (Beveiligd Versleuteld emailverkeer)	Ja	De voorziening ondersteunt zowel TLS 1.2, 1.1 als 1.0.
		Stelstelstandaarden
Digikoppeling 2.0 (Veilige berichtuitwisseling)	Nee	Er zijn plannen om voor de BRP (basisregistratie personen) gebruik te gaan maken van Digikoppeling. Gezien het BRP bezinningsproces is de planning onduidelijk. Ontsluiting van BV-BSN middels Digikoppeling zal niet plaatsvinden. Gebruik van beide voorzieningen verloopt via besloten netwerken, meer specifiek en voornamelijk Gemnet/Diginetwerk. Aansluitingen op Diginetwerk zijn inmiddels gerealiseerd en zijn richting gemeenten en afnemers gecommuniceerd.

StUF (Uitwisseling administratieve overheidsgegevens)	Nee	De voorziening spreekt de WSI standaard XML/SOAP met haar gebruikers. Er is geen concrete planning voor de invoering van StUF.

Ten opzichte van 2017 zijn er geen wijzigingen anders dan dat over de aansluitingen met het diginetwerk inmiddels is gecommuniceerd met gemeenten en afnemers.

Van de standaarden die in 2018 nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) zijn er geen relevant voor BSN Beheervoorziening en GBA-V.

Concluderend moet voor de BSN Beheervoorziening en GBA-V nog (volledig) worden geïmplementeerd: Digikoppeling 2.0, IPv4 en IPV6, StUF.

2.5 Rijkspas

Beheerorganisatie: Ministerie van BZK

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

De regie voor de Rijkspas is belegd bij DGOO/CIO Rijk/ICT Voorzieningen en Infrastructuur Rijk, die meer van dergelijke rijksbrede projecten in het portfolio heeft. De uitvoering is belegd bij SSC-ICT m.b.t. hosting van de Rijkspas Verkeershub en het Generiek Centraal Kaartmanagement Systeem (GCMS). De Certificate Authority is ondergebracht onder de bestaande infrastructuur van DICTU. De departementen zijn eigenaar van de Identity management- en toegangscontrolesystemen.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Gepland	Voor Rijkspas worden mails verstuurd vanaf de applicatie voor Interdepartementale Toegang (IdT). In de huidige infrastructuur is dit niet toegepast. De eerdere planning van Q3 2018 voor verhuizing van de Rijkspassystemen naar een nieuw datacenter waar DKIM wel toegepast zal worden is door de leverancier uitgesteld naar Q4 2018.
DMARC (Anti-phishing)	Nee	P-direkt is afhankelijk van SSC-ICT voor implementatie van de standaard. De status hiervan is onbekend.
DNSSEC (Beveiligde domeinnamen)	Gepland	Rijkspas communiceert momenteel nog niet via het publieke internet. De verbinding die daarvoor voorzien is, maakt wel gebruik van DNSSEC. Voor communicatie binnen de Rijksoverheid wordt momenteel gebruik gemaakt van de Haagse

		Ring. Deze ondersteunt nog geen DNSSEC. De planning van 2017 is niet gehaald en is afhankelijk van de verhuizing naar het nieuwe data center. De verhuizing staat gepland voor Q1 2019.
IPv4 en IPV6 (Internetnummers)	Nee	IPv4 wordt toegepast. De Haagse ring, waarover eigenlijk al het verkeer naar de Rijkspas voorzieningen loopt, ondersteunt geen IPv6. Deze dienst wordt door Logius geleverd, en is onderdeel van de 'connectiviteitsdiensten' waarvan I&I gebruik maakt.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De Rijkspas heeft een eigen normen- en beveiligingskader gebaseerd op ISO-9001 en 27001/2. Jaarlijks worden hier ook audits op gedaan, onder andere door de Audit Dienst Rijk.
SAML (Inloggegevens)	Ja	De Interdepartementale Toegang applicatie (IDT) is per 2015 aangesloten op de Single Sign On voorziening via SAML.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd.
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Nee	Rijkspas neemt email dienstverlening af van SSC-ICT, en vanuit deze leverancier is aangegeven de nog niet alle randvoorwaarden in plaats zijn voor deze standaard. Eén van deze randvoorwaarden is DNSSEC, waarvan de implementatie afhankelijk is van de verhuizing naar het nieuwe data center. Na deze implementatie zal SSC-ICT opnieuw de mogelijkheden van STARTTLS en DANE analyseren.
TLS v1.2, v1.1 en v1.0 (Beveiligde, versleutelde verbindingen)	Ja	TLS wordt gebruikt voor het veilig ontsluiten van de website voor IdT.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Rijkspas maakt gebruik van het WUS-gedeelte van de Digikoppeling. De deelnemers kunnen zelf de keuze maken welk protocol ze hanteren, de standaard koppeling Rijkspas of de Digikoppeling.

Ten opzichte van 2017 is de implementatie van DKIM, STARTTLS/DANE, DNSSEC vertraagd vanwege de afhankelijkheid met de verhuizing naar een nieuw datacenter.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. P-direkt is afhankelijk van SSC-ICT voor implementatie van de standaard. De status hiervan is onbekend.

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

2.6 Stelsel elektronische toegangsdiensten

Beheerorganisatie: Logius

Werking en inhoud van het Stelsel Elektronische Toegangsdiensten
Sinds 2016 is het Afsprakenstelsel Elektronische Toegangsdiensten in het onderzoek opgenomen in plaats van eHerkenning. Het afsprakenstelsel bevat de voor dit onderzoek relevante eisen voor zowel Idensys als eHerkenning. Momenteel zijn de wijze waarop deze voorzieningen geclusterd zijn en de eisen die eraan gesteld worden sterk aan verandering onderhevig.

Het Afsprakenstelsel Elektronische Toegangsdiensten is een set van technische, functionele, juridische en organisatorische afspraken op basis waarvan eHerkenning en Idensys worden geleverd. De afspraken hebben als doel om samenwerking en zekerheid in het Netwerk te garanderen. Tegelijkertijd bieden de afspraken ook vrijheid aan de deelnemers om competitieve proposities te leveren aan hun klanten.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	Bij verstuurde email wordt DKIM toegepast, bij ontvangst gebeurd dit door de centrale email voorzieningen van Logius (SSC-ICT).
DMARC (Anti-phishing)	Gepland	Stelsel Elektronische toegangsdiensten voldoet aan DMARC, maar de policy wordt voor Q1 2019 aangescherpt.
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC werd in 2015 in de productieomgeving opgenomen.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	HTTPS en HSTS wordt toegepast op alle websites en webapplicaties onder beheer van de beheerorganisatie.
IPv4 en IPv6 (Internetnummers)	Ja	Beide voorzieningen voldoen aan IPv4 en IPv6.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De BIR is van toepassing op Logius, in het stelsel wordt certificering tegen ISO27001 geëist voor de deelnemers. De beheerorganisatie zelf is als stelselbeheerder ook gecertificeerd volgens ISO 27001. Daarvoor is ook een in controlstatement beschikbaar.
SAML (Inloggegevens)	Ja	SAML is een verplichte eis vanuit het stelsel.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF wordt toegepast bij de voorziening, maar wordt vooralsnog niet vereist als toe te passen techniek voor deelnemers.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Nee	STARTTLS is geïmplementeerd voor eherkenning.nl en idensys.nl. De implementatie van DANE is in zowel 2017 als 2018 nog onderwerp van onderzoek. Hier is nog geen concrete planning voor.

TLS v1.2, v1.1 en v1. (Beveiligde, versleutelde verbindingen)	Ja	Het afsprakenstelsel stelt het gebruik van TLS1.x verplicht.
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Ja	Digitoegankelijk (EN 301 549 met WCAG 2.0) is een eis vanuit het stelsel aan de deelnemers. Bij vermoeden van non-conformiteit kan een toets worden opgestart. De website voor eHerkenning.nl, onder beheer van de beheersorganisatie zelf, voldoet en is getoetst conform WCAG 2.0 (AA): https://www.accessibility.nl/ondersteuning/inspectie/site-1497. Voor Idensys staat dit gepland (mede afhankelijk van besluitvorming).
PDF 1.7, PDF/A-1 of PDF/A-2 (Documentpublicatie/ archivering)	Ja	Primair wordt de stelseldocumentatie via HTML op eherkenning.nl gepubliceerd. Stelseldocumentatie wordt met behulp van office software gepubliceerd in PDF/A-formaat. Overige documenten worden met een aparte tool in PDF/A formaat geconverteerd omdat het gehanteerde DMS dit niet ondersteunt.

Ten opzichte van 2017 zijn IPv4 en IPv6 geïmplementeerd.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Implementatie van DMARC staat gepland voor Q1 2019.

Concluderend, moeten voor het Stelsel Elektronische toegangsdiensten nog de volgende standaarden (volledig) worden geïmplementeerd: DMARC, STARTTLS en DANE.

3. Dienstverlening en informatieverstrekken

3.1 MijnOverheid

Beheerorganisatie: Logius

Werking en inhoud van MijnOverheid (bron: Monitor GDI 2018)
MijnOverheid is een persoonlijk toegangsportaal waarin verschillende diensten van de overheid ontsloten worden. MijnOverheid gaat over persoonlijke, en om die reden met DigiD beveiligde, diensten en informatie. Binnen MijnOverheid heeft de burger toegang tot de Berichtenbox, Lopende Zaken en Persoonlijke Gegevens. De Berichtenbox is de persoonlijke brievenbus waarin burgers post van onder meer de Belastingdienst, RDW, SVB, UWV, gemeenten en pensioenfondsen kunnen ontvangen. Lopende Zaken geeft weer wat de stand is van bijvoorbeeld aanvragen of vergunningen. Inzage Persoonlijke gegevens maakt het mogelijk om te controleren of de eigen gegevens correct zijn

opgeslagen bij de overheid. Logius is verantwoordelijk voor het portaal, de aangesloten partijen zijn verantwoordelijk voor hun eigen dienstverlening die via MijnOverheid benaderd kan worden.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/ phishing)	Ja	MijnOverheid voldoet aan DKIM (zie: https://internet.nl/mail/mijnoverheid.nl/).
DMARC (Anti-phishing)	Ja	Deze standaard wordt toegepast.
DNSSEC (Beveiligde domeinnamen)	Ja	MijnOverheid voldoet aan DNSSEC (zie: https://internet.nl/site/mijnoverheid.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	Deze standaard wordt toegepast (zie: https://internet.nl/mail/mijnoverheid.nl/).
IPv4 en IPV6 (Internetnummers)	Nee	Mijnoverheid gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik. Mijnoverheid ondersteunt op dit moment alleen IPv4. De verwachting is dat implementatie van IPv6 in Q4 2018 kan worden opgepakt maar deze plannen zijn nog niet concreet.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Rijk (BIR) van toepassing die is gebaseerd op NEN-ISO27001. Logius heeft zich over toepassing van deze norm verantwoord door het afgeven van In Control Verklaringen (ICV'en) aan de eigenaar (BZK/DGOBR). De ICV's zijn nog up-to-date.
SAML (Inloggegevens)	Ja	Authenticatie loopt via SAML.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is relevant en geïmplementeerd.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	Deze standaard wordt toegepast.

TLS v1.2, v1.1 en v1.0 (Beveiligde, versleutelde verbindingen)	Ja	In de dienstverlening aan burgers maakt MijnOverheid gebruik van een TLS 1.2-verbinding (Zie: https://internet.nl/site/mijn.overheid.nl). De koppelingen met afnemers (overheidsorganisaties) lopen ook via TLS op basis van PKIoverheid-certificaten.
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Ja	De laatste Webrichtlijnentoets is door Stichting Accessibility uitgevoerd (niet meer door Centric zoals voorheen). De toegankelijkheidsverklaring moet nog geplaatst worden.
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 ondersteunt het genoemde PDF formaat, maar controleert hier niet op. MijnOverheid genereert zelf geen PDF files. In 2016 is een impact-analyse uitgevoerd om te onderzoeken wat het betekent wanneer men PDF-bijlages wel gaat controleren en wat eventuele vervolgacties zijn. Er is toen besloten om niet op formaat te gaan controleren.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisseling en)	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 2017 voldoet MijnOverheid geheel aan Digikoppeling 2.0. De status is verhoogd van deels naar ja. MijnOverheid voldoet aan de Digitoegankelijk (EN 301 549 met WCAG 2.0) standaard. Er is een webrichtlijnen toets uitgevoerd. De status is verhoogd van gepland naar ja. Ten opzichte van 2017 is de relevantie van de OWMS standaard door de beheerder getoetst. De standaard is niet van toepassing bevonden.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) zijn DMARC en Open API Specification relevant. DMARC en Open API Specification zijn geïmplementeerd.

Concluderend, moet MijnOverheid nog de volgende standaard (volledig) implementeren: IPv4 en IPV6.

3.2 Berichtenbox voor bedrijven

Beheerorganisatie: Rijksdienst voor Ondernemend Nederland (RVO).

Inhoud en werking Berichtenbox voor bedrijven (Bron: Monitor GDI 2018)
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.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Nee	DKIM is niet geïmplementeerd (zie: https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/).
DMARC (Anti-phishing)	Nee	De BerichtenBox voor Bedrijven voldoet niet aan DMARC. Deze standaard is mede afhankelijk van SPF en DKIM, welke niet ondersteund worden door de BerichtenBox voor Bedrijven.
DNSSEC (Beveiligde domeinnamen)	Ja	Volgens internet.nl voldoet het domein berichtenbox.antwoordvoorbedrijven.nl (zie: https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	HTTPS en HSTS zijn geïmplementeerd (zie: https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/).
IPv4 en IPv6 (Internetnummers)	Nee	De website van de Berichtenbox ondersteunt IPv4 maar is volgens internet.nl niet toegankelijk via IPv6 (zie https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/). De Berichtenbox is wel IPv6 ready, maar nog niet de hele keten. E-ovb (beheerder van de Berichtenbox) is daarbij ook afhankelijk van leveranciers die hun IPv6 implementatie nog niet op orde hebben. De implementatie moet DICTU-breed gebeuren voordat dit voor de Berichtenbox gedaan zal worden. Een datum voor de implementatie is niet bekend.
SAML (Inloggegevens)	Ja	eHerkenning is SAML-based en wordt toegepast voor het inloggen op de Berichtenbox.
SPF (Preventie van mailspoofing/phishing)	Nee	SPF is niet geïmplementeerd (zie https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/).
TLS v1.2, v1.1 en v1.	Ja	De Berichtenbox maakt gebruik van TLS 1.2 (zie: https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/).

(Beveiligde, versleutelde verbindingen)		
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Nee	Dictu heeft een webrichtlijnen toets gedaan. Een concrete planning voor implementatie van de standaard is nog niet bekend.
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/ archivering)	Ja	Alle berichten kunnen worden gedownload (vanaf de Berichtenbox website) in PDF/A formaat. PDF-documenten worden gegenereerd in PDF A/1.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Overheden kunnen via Digikoppeling geautomatiseerd berichten verzenden en ontvangen. Ondernemers kunnen alleen handmatig (via de website) hun Berichtenbox gegevens opvragen.
STuF (Uitwisseling administratieve overheidsgegevens)	Ja	STuF wordt in combinatie met Digikoppeling gebruikt voor de uitwisseling met alle partijen die via digikoppeling op de berichtenbox zijn aangesloten.

Ten opzichte van 2017 is HSTS nu afgedwongen door de frontend servers. De status van HTTPS/HSTS is verhoogd van nee naar ja. Voor de standaarden die sinds vorig jaar nog geïmplementeerd moeten worden zijn geen data bekend.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Echter voldoet de BerichtenBox voor Bedrijven niet aan DMARC. Deze standaard is mede afhankelijk van SPF en DKIM, welke niet ondersteund worden door de BerichtenBox voor Bedrijven.

Concluderend, moet BerichtenBox voor Bedrijven nog de volgende standaarden (volledig) implementeren: Digitoegankelijk (EN 301 549 met WCAG 2.0), DKIM, DMARC, IPv4 en IPv6, SPF.

3.3 Overheid.nl

Beheerorganisatie: Kennis- en Exploitatiecentrum Officiële Overheidspublicaties (KOOP)

Werking en inhoud van overheid.nl (bron: Monitor GDI 2018)
Overheid.nl biedt centrale internettoegang (website) 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.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	DKIM is geïmplementeerd (zie https://internet.nl/mail/overheid.nl/).
DMARC (Anti-phishing)	Ja	DMARC wordt toegepast op overheid.nl behoudens DMARC policy gepland medio 2018.
DNSSEC (Beveiligde domeinnamen)	Ja	Overheid.nl voldoet sinds Q2 2015 aan DNSSEC (zie: https://internet.nl/site/www.overheid.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Gepland	Het portaal-gedeelte (www.overheid.nl) voldoet aan de standaard (zie https://internet.nl/site/www.overheid.nl/), behoudens HTTP-compressie, gepland medio 2018. Een restant sub-domeinen zal uiterlijk eind 2018 aan deze standaarden voldoen. Alleen wetten.overheid.nl voldoet nog niet. Dit wordt met de laatste toegankelijkheidsupdate in de zomer van 2018 uitgevoerd.
IPv4 en IPV6 (Internetnummers)	Ja	Er wordt voldaan aan IPv4 en IPv6 (zie: https://internet.nl/domain/www.overheid.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Vanaf 2015 staat overheid.nl niet meer op de risicokaart van BZK en hoeft hiervoor geen ICV (In Control Verklaring) meer te worden afgegeven. Voor OEB, de applicatie die centraal staat in het publiceren van overheidsinformatie en richtinggevend is voor alle KOOP-dienstverlening, wordt wel jaarlijks een ICV afgegeven; deze is gebaseerd op de BIR die weer is gebaseerd op NEN-ISO/IEC 27001/27002. Alle dienstverlening van KOOP is ondergebracht bij een hostingpartij die jaarlijks een ISAE3402 Type II verklaring laat opstellen; deze verklaring baseert zich mede op de certificering met NEN-ISO/IEC 27001/27002.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	STARTTLS en DANE zijn geheel geïmplementeerd (zie: https://internet.nl/mail/overheid.nl/).
TLS v1.2, v1.1 en v1.0 (Beveiligde, versleutelde verbindingen)	Gepland	Deze standaard is doorgevoerd, behoudens Client-initiated renegotiation, dit staat gepland voor medio 2018 (zie: https://internet.nl/site/www.overheid.nl/).
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Gepland	Er is een toegankelijkheidsverklaring conform EN 301459. De nieuwe eisen van deze nieuwe richtlijn zijn meegenomen in de vernieuwing van Overheid.nl. Deze is maart 2018 als beta live gegaan. M.b.t. toegankelijkheid is een onafhankelijk onderzoek uitgevoerd. Toegankelijkheidsverklaring zal geplaats worden na afronding beta-fase medio 2018.
OWMS	Ja	Overheid.nl is gemetadateerd conform OWMS.

(Metadata overheidsinformatie)		
PDF 1.7 PDF/A-1 PDF/A-2 (Documentpublicatie/ archivering)	Ja	Alle PDF's van officiële bekendmakingen zijn PDF/A-1a zoals wettelijk bepaald is.
SKOS (Thesauri en begrippenwoordenboeken)	Ja	SKOS is geïmplementeerd voor de waardelijsten van OWMS.
		Juridische identificatie en verwijzing
BWB (Wet- en regelgeving)	Ja	overheid.nl is zelfs de bron van de BWB identificatie. Zie wetten.overheid.nl.
JCDR (Decentrale regelgeving)	Ja	overheid.nl is zelfs de bron van de JCDR identifiers (zie: https://zoek.overheid.nl/lokale_wet_en_regelgeving).

Ten opzichte van 2017 vindt volledige implementatie van HTTPS en HSTS plaats in 2018 i.p.v. 2017. De status blijft vooralsnog gehandhaafd op gepland. Daarnaast zijn ten op zichte van 2017 de standaarden BWB en JCDR opgenomen. Overheid.nl is de bron van de JCDR identifiers en is de bron van de BWB identificatie.

Van de standaarden die in 2018 nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Overheid.nl voldoet aan DMARC.

Concluderend moeten voor overheid.nl nog (volledig) worden geïmplementeerd: Digitoegankelijk (EN 301 549 met WCAG 2.0), HTTPS en HSTS, TLS v1.2, v1.1 en v1.0.

3.4 Ondernemersplein

Beheerorganisatie: Kamer van Koophandel

Werking en inhoud van Ondernemersplein (bron: Monitor GDI 2018)
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.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	DKIM is geïmplementeerd (zie: https://internet.nl/mail/ondernemersplein.nl/).
DMARC (Anti-phishing)	Ja	Ondernemersplein.nl voldoet aan DMARC (zie: https://internet.nl/mail/ondernemersplein.nl/).

DNSSEC (Beveiligde domeinnamen)	Ja	De standaard is geïmplementeerd op de nieuwe DNS omgeving.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	Aan deze standaard wordt voldaan (zie: https://internet.nl/site/www.ondernemersplein.nl/).
IPv4 en IPV6 (Internetnummers)	Ja	De website ondersteunt IPv4 en is toegankelijk via IPv6 (zie: https://internet.nl/site/www.ondernemersplein.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Ondernemersplein is gehost bij de Kamer van Koophandel. Daar liep een ISO 27001 certificeringstraject en Ondernemersplein heeft dit inmiddels toegepast en is door een audit in april 2016 gecertificeerd hierop. Nieuwe toetsing vindt plaats in februari 2019.
SPF (Preventie van mailspoofing/phishing)	Ja	Er wordt aan deze standaard voldaan (zie: https://internet.nl/mail/ondernemersplein.nl/).
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Nee	Aan STARTTLS wordt voldaan, maar aan DANE wordt nog niet voldaan. De KvK geeft aan nog te moeten onderzoeken of hieraan voldaan zal worden. Er is nog geen concreet onderzoekstraject gedefinieerd.
TLS v1.2, v1.1 en v1. (Beveiligde, versleutelde verbindingen)	Ja	Er is een migratie uitgevoerd naar TLS 1.2 en op verzoek van de product owner wordt TLS 1.0 nog ondersteund.
		Document en (web/app)content
CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)	Nee	De tooling (CMS/ESB) ondersteunt de standaard wel, maar deze wordt niet actief gebruikt. Er zijn geen content leveranciers die hun CMS in CMIS vorm aan het Ondernemersplein.nl beschikbaar stellen. Concreet is er dus nog geen toepassing op dit moment en er zijn ook nog geen plannen om dit te doen.
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Ja	Verklaring is beschikbaar. Meer informatie beschikbaar op: https://www.ondernemersplein.nl/toegankelijkheid/. De laatste toets is uitgevoerd in mei 2018.
OWMS (Metadata overheidsinformatie)	Nee	De informatie op de website is gemetadateerd volgens een eigen model die past bij de metadatering van de partners.
		Juridische identificatie en verwijzing
BWB (Wet- en regelgeving)	Ja	Binnen de website, de content van AvB, wordt verwezen naar wetgeving conform de BWB standaard.

Ten opzichte van 2017 voldoet ondernemersplein aan DNSSEC en TLS. De status van DNSSEC is verhoogd van gepland naar ja. De status van TLS is verhoogd van nee naar ja. De SKOS standaard is ten opzichte van 2017 verwijderd. Het ondernemersplein zou nog onderzoeken of de standaard

relevant was, en heeft inmiddels aangegeven geen begrippenlijsten, axonomieën en/of linked data op de website aan te bieden. Daarmee is de standaard niet relevant.

Van de standaarden die in 2018 nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Ondernemersplein voldoet aan DMARC.

Concluderend moeten voor ondernemersplein nog (volledig) geïmplementeerd: CMIS, OWMS, STARTTLS/DANE.

3.5 Samenwerkende catalogi

Beheerorganisatie: Logius

Inhoud en werking van Samenwerkende Catalogi
Samenwerkende Catalogi koppelt de productcatalogi van verschillende overheidsorganisaties. De koppeling van productcatalogi door Samenwerkende Catalogi maakt het 'no wrong door'- principe mogelijk. Dit bekent dat over organisatiegrenzen heen gezocht kan worden naar producten en diensten. Het is de standaard (specificatie) voor het publiceren en uitwisselen van metadata over producten en diensten binnen de overheid, zoals bijvoorbeeld het aanvragen van een vergunning of het aanvragen van een reisdocument. Deze data is voor iedereen doorzoekbaar door middel van de Zoekdienst van KOOP op basis van een API. De eindgebruiker ziet de zoekdienst niet, maar gebruikt de portalen Overheid.nl en Ondernemersplein.nl. Zowel Overheid.nl als het Digitaal Ondernemersplein haalt de productinformatie uit de zoekdienst. Daarnaast kan de eindgebruiker via de desbetreffende overheidswebsites informatie via Samenwerkende Catalogi opvragen.

Standaard	Status	Toelichting
		Internet en beveiliging
DMARC (Anti-phishing)	Gepland	Samenwerkende Catalogi wordt beheerd door Logius waarmee DMARC valt onder het organisatorisch werkingsgebied. De validator is benaderbaar via een subdomein van Logius (scvalidator.logius.nl) waarvoor geldt dat dit een overheidsdomein is waarvandaan niet wordt gemaild. Daarmee valt dit onder het functioneel toepassingsgebied. Het DMARC-compliant maken van de validator staat gepland voor 2018.
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Deels	Publicatie standaard op www.logius.nl zie aldaar voor Digitoegankelijk compliance. Overheid.nl ontsluit decentrale content op basis van Samenwerkende Catalogi, zie voor Digitoegankelijk compliance aldaar; Publicatie op basis van Samenwerkende Catalogi door overheden op eigen website Digitoegankelijk compliance eigen verantwoordelijkheid deelnemers (Rijk/gemeenten/provincies/waterschappen). De validator (scvalidator.logius.nl) is tot op heden niet getest op toegankelijkheid. Deze verplichting zal ingaan op 23 september 2020. Voor die tijd zal de validator zijn getest en eventuele tekortkomingen verholpen.

Open Api Specification (Beschrijven van REST API's)	Nee	Samenwerkende catalogi voldoet niet aan deze standaard. Momenteel wordt de relevantie van deze standaard nader bepaald.
OWMS (Metadata overheidsinformatie)	Ja	Samenwerkende catalogi is volledig gebaseerd op OWMS.

Ten opzichte van 2017 is Digitoegankelijk (EN 301 549 met WCAG 2.0) van 'ja' naar de status 'deels' gegaan. De validator (scvalidator.logius.nl) is tot op heden niet getest op toegankelijkheid. Deze verplichting zal ingaan op 23 september 2020. Voor die tijd zal de validator zijn getest en eventuele tekortkomingen verholpen.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) zijn Open API en DMARC relevant. Samenwerkende Catalogi voldoet nog niet aan deze standaarden. DMARC staat gepland voor 2018 en voor Open API wordt momenteel de relevantie nader bepaald.

Voor Samenwerkende Catalogi moeten dus nog de volgende standaarden (volledig) worden geïmplementeerd: Digitoegankelijk (EN 301 549 met WCAG 2.0), DMARC, Open API.

3.6 Rijksportaal

Beheer organisatie: SSC-ICT

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

Standaard	Status	Toelichting
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	Er wordt in enkele situaties gebruik gemaakt van email. Bijvoorbeeld om te reageren naar een redactie. Hierbij wordt gebruik gemaakt van de generieke email-voorziening van SSC-ICT, die de DMARC standaard ondersteunt.
IPv6 en IPv4 (Internet-nummers)	Nee	Het huidige Rijksportaal (versie 1.6.5) is alleen ingericht voor IPv4. Om performance redenen wordt IPv6 momenteel nog niet toegepast. Als gevolg van de transitie naar het overheidsdatacenter (ODC), het beëindigen van de realisatie van release 1.7 en een lopende verkenning op een nieuwe omgeving is er geen doorontwikkeling t.a.v. nieuwe functionaliteit voor het Rijksportaal.

SAML (Inloggegevens)	Gepland	De implementatie van SAML is in juli 2016 opgeleverd. Het Ministerie van Veiligheid en Justitie is de eerste klant die kan worden aangesloten op de huidige versie 1.6.5 van het Rijksportaal. De acceptatie van SAML is door het Ministerie Justitie en Veiligheid niet volledig afgerond vóór de transitie naar het ODC. Als gevolg hiervan dient deze functionaliteit opnieuw getest te worden. De functionaliteit is overigens wel beschikbaar en wordt nog zonder formele support gebruikt.
		Document en (web/app)content
ODF (Document-bewerkingen)	Ja	ODF wordt ondersteund: ODF-bestanden kunnen geüpload en gedownload worden en de inhoud van ODF-bestanden kan door de zoekmachine worden geïndexeerd. Naast ODF worden op het Rijksportaal ook andere documentformaten gebruikt; het gebruik van ODF wordt niet afgedwongen.
PDF 1.7 PDF/A-1, PDF/A-2 (Documentpublicatie/ archivering)	Ja	PDF wordt ondersteund: PDF-bestanden kunnen geüpload en gedownload worden en de inhoud van PDF-bestanden kan door de zoekmachine worden geïndexeerd. Naast PDF 1.7, PDF/A-1 en PDF/A-2 worden op het Rijksportaal ook andere PDF-versies gebruikt; het gebruik van PDF 1.7, PDF/A-1 en PDF/A-2 wordt niet afgedwongen.

Ten opzichte van 2017 is de status van de SAML standaard op gepland gezet in plaats van ‘ja’, omdat de functionaliteit opnieuw getest wordt en hoewel het beschikbaar is, nog zonder formele support wordt gebruikt.

Van de standaarden die in 2018 nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Rijksportaal voldoet aan deze standaard.

Concluderend moet voor Rijksportaal nog IPv6 en IPv4 en SAML (volledig) worden geïmplementeerd.

3.7 ODC Noord

Beheerorganisatie: Dienst Uitvoering Onderwijs (DUO)

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

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	DKIM is geïmplementeerd voor ODC-Noord.

DMARC (Anti-phishing)	Nee	DNSSEC, SPF, DKIM en delivery over TLS zijn geïmplementeerd. Voor odc-noord.nl en sso-noord.nl zijn er DMARC records.
DNSSEC (Beveiligde domeinnamen)	Ja	ODC-Noord heeft sinds het onderzoek uit 2015 een eigen DNS ingericht, die DNSSEC gebruikt.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De cloud dashboards zijn allemaal uitsluitend via HTTPS benaderbaar een aantal websites draaien op HSTS. De overige websites zijn in de loop van 2017 aangepast. Alle sites zijn voorzien van een SSL-certificaat.
IPv6 en IPv4 (Internetnummers)	Deels	Intern wordt IPv6 gebruikt op een specifiek netwerk. Nog niet alle benodigde producten worden met IPv6 aangeboden. Zodra de markt alles op het juiste niveau kan aanbieden zal dit geïmplementeerd worden en zullen de systemen die vanaf het internet benaderbaar zijn, ook worden ontsloten via IPv6.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	In december 2017 is door ODC-Noord een BIR in Control Verklaring afgegeven, ondersteund door een Assurance verklaring van de ADR. De onderliggende leveranciers voldoen aan de ISO. ODC-Noord voldoet aan de BIR.
SAML (Inloggegevens)	Gepland	ODC-Noord maakt voor het interne systeem geen gebruik van SAML. Bij het ontwikkelen van diensten ten bate van klanten (SaaS) wordt SAML onderzocht en waar mogelijk toegepast. SAML federatie staat op de roadmap voor eind 2018
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Gepland	De implementatie van DANE is voor eind 2018 gepland. STARTTLS is geïmplementeerd.
TLS 1.2, 1.1 en 1.0 (Beveiligde, versleutelde verbindingen)	Ja	Het beleid van ODC-Noord voor internet-gekoppelde systemen is dat TLS (in volgorde) van TLS1.2, TLS1.1 wordt aangeboden. TLS 1.0 wordt niet toegepast tenzij er een explain komt van de site-eigenaar.
WPA2 Enterprise (Toegang tot een WiFi-netwerk met account)	Ja	Deze standaard is toegepast waar ODC-Noord wifi gebruikt.
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Gepland	De websites van ODC-Noord worden op dit moment herbouwd. Digi-toegankelijk is een inrichtingseis. Verwachte oplevering is Q3 2018.
ODF (Document-bewerkingen)	Ja	In de operatie van ODC-Noord wordt over het algemeen gebruik gemaakt van documenten in ODF-formaat. Vanwege opmaak- en interoperabiliteitsproblemen wordt dit voor communicatie met externen beperkt gebruikt.
OWMS (Metadata overheidsinformatie)	Gepland	De websites van ODC-Noord worden op dit moment herbouwd. De vraag of hierbij ook de OWMS worden toegepast staat uit. Implementatie van OWMS staat gepland voor Q4 2018.

PDF 1.7, PDF A/1, PDF A/2 (Document-publicatie/ archivering)	Deels	V.w.b. uitwisseling van (definitieve) documenten met externe partijen wordt gebruik gemaakt van PDF. PDFCreator van Windows wordt als printoptie in de kantoorautomatiseringsomgeving aangeboden. De standaardinstelling is PDF versie 1.4, optioneel is 1.5. Vooralsnog wordt er bij DUO nog voor gekozen om de gratis variant van PDF-creator beschikbaar te stellen. Deze biedt maximaal PDF 1.5. Gebruikers van LibreOffice (dat is het meest gebruikte Office-pakket binnen de operationele omgeving van ODC-Noord) kunnen documenten exporteren naar PDF/A-1. Op dit moment is dat nog geen standaard werkwijze. PDF/A is beschikbaar en wordt gebruikt voor formele documenten

Ten opzichte van 2017 is implementatie van Digitoegankelijk (EN 301 549 met WCAG 2.0) gepland. De status is verhoogd van nee naar gepland. De websites van ODC-Noord worden op dit moment herbouwd. Digi-toegankelijk is een inrichtingseis. Verwachte oplevering is Q3 2018. DKIM is geïmplementeerd. ODC Noord voldoet sinds 2018 aan DKIM, NEN-ISO/IEC 27001/27002 en HTTPS/HSTS. De status van DKIM is verhoogd van gepland naar ja. De status van NEN/ISO/27001/27002 is verhoogd van nee naar ja. De status van HTTPS/HSTS is verhoogd van deels naar ja. Implementatie van SAML en START/TLS staat gepland voor eind 2018.

Van de standaarden die in 2018 nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. ODC Noord voldoet nog niet aan deze standaard.

Concluderend moeten voor ODC Noord nog (volledig) worden geïmplementeerd: Digitoegankelijk (EN 301 549 met WCAG 2.0), DMARC, IPv6 en IPv4, OWMS, PDF 1.7, PDF A/1, PDF A/2, SAML, STARTTLS/DANE.

3.8 Doc-Direkt

Beheerorganisatie: Doc-Direkt

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

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	Volgens SSC-ICT maakt Doc-Direkt gebruik van de mailservers van SSC-ICT, deze zijn onderdeel van het BZK domein, waarvoor DKIM actief is.
DMARC (Anti-phishing)	Ja	Doc-Direkt voldoet aan DMARC.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels	De standaard wordt toegepast. De laatste open realisatie is de website www.handelingenbank.nl. De certificaat aanvraag loopt en realisatie vindt plaats in het 4e kwartaal 2018.
IPv4 en IPv6 (Internetnummers)	Ja	Doc-Direkt voldeed al aan IPv4 en voldoet inmiddels ook aan IPv6.

NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Voor de informatiesystemen waarvan Doc-Direkt eigenaar is, is in 2016 een 'in controle verklaring' opgesteld. Op de punten waar Doc-Direkt afwijkt is een uitleg gegeven (explains) en er is een verbeterplan opgesteld. Verbeteringen worden inmiddels uitgevoerd.
SAML (Inloggegevens)	Ja	Via de werkplek DWR kunnen medewerkers via SSO inloggen op de door Doc-Direkt beheerde DMS applicatie.
SPF (Preventie van mailspoofing/phishing)	Ja	Ook SPF wordt inmiddels toegepast.
TLS v1.2, v1.1 en v1.0 (Beveiligde, versleutelde verbindingen)	Nee	Het is bij Doc-Direkt niet bekend of TLS van toepassing is en daarmee ook niet wanneer dit geïmplementeerd is.
		Document en (web/app)content
Ades Baseline Profiles (Digitaal ondertekenen van documenten)	Nee	Bij Doc-Direct loopt momenteel een onderzoek over de mogelijke toepassing van deze standaard in de toekomst. De uitkomsten daarvan zijn naar verwachting in het eerste kwartaal van 2019 bekend i.p.v. het eerste kwartaal van 2018.
CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)	Nee	De mogelijkheid en noodzakelijkheid van het toepassen van deze standaard werden in 2016 nader onderzocht, maar dit heeft nog niet tot een besluit geleid. Inmiddels zijn er proof of concepts uitgevoerd.
ODF (Documentbewerkingen)	Nee	Voor bewerkbare documenten wordt alleen .doc-formaat gebruikt. Er zijn geen plannen ODF te gebruiken.
PDF 1.7 – PDF A/1 of PDF A/2 (Documentpublicatie/ archivering)	Ja	Doc-Direkt ondersteunt in haar archieven vooral PDF/A. Alles wat gescand wordt gaat naar PDF/A. Daarnaast wordt ook 1.7 veel gebruikt.
SKOS (Thesauri en begrippen-woordenboeken)	Nee	SKOS wordt op dit moment niet toegepast. Er zijn nog geen plannen bekend of en wanneer SKOS geïmplementeerd zal worden.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Nee	Op dit moment wordt door SSC-ICT gewerkt aan operationalisering van Digikoppeling voor het gebruik binnen de dienstverlening van Doc-Direkt.

Ten opzichte van 2017 is er uitloop op het onderzoek dat Doc-Direct uitvoert over de mogelijke toepassing van Ades Baseline Profiles in de toekomst. De uitkomsten daarvan zijn naar verwachting in het eerste kwartaal van 2019 bekend i.p.v. het eerste kwartaal van 2018. Verder wordt door SSC-ICT gewerkt aan operationalisering van Digikoppeling voor het gebruik binnen de dienstverlening van Doc-Direkt. Verder wordt HTTPS/HSTS deels toegepast en is volledige implementatie gepland voor het vierde kwartaal van 2018. De status van HTTPS/HSTS is verhoogd van nee naar deels. Verder voldoet Doc-Direkt inmiddels aan IPv4 en IPv6 en SPF. De status van IPv4 en IPv6 en SPF is verhoogd van nee naar ja.

Van de standaarden die in 2018 nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant.

Concluderend moeten voor Doc-Direkt nog (volledig) worden geïmplementeerd: Ades Baseline Profiles, CMIS, Digikoppeling 2.0, HTTPS/HSTS, ODF, SKOS, TLS v1.2, v1.1 en v1.0.

3.9 Rijksoverheid.nl

Beheerorganisatie: Ministerie van AZ (DPC)

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.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/ phishing)	Ja	DKIM is geïmplementeerd. Dit heeft onder meer betrekking op de nieuwsbrieven die DPC namens de diverse departementale opdrachtgevers verstuurt. Het gaat om de nieuwsbrieven- en persberichten-service voor de Rijksoverheid en het DPC-mailverkeer. Deze zijn met SPF-DKIM-DMARC uitgerust.
DMARC (Anti-phishing)	Ja	DMARC is geïmplementeerd.
DNSSEC (Beveiligde domeinnamen)	Ja	Rijksoverheid.nl is ondertekend met DNSSEC (zie: https://internet.nl/site/www.rijksoverheid.nl/). DPC biedt DNSSEC ook aan al haar klanten die domeinen via haar registrar-functie afnemen.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening voldoet aan deze standaard (zie: https://internet.nl/site/www.rijksoverheid.nl/).
IPv4 en IPV6 (Internetnummers)	Ja	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	Hosting leverancier Ordina heeft een NEN 27001/2 implementatie waarin de beveiliging van rijksoverheid.nl meegaat. DPC zelf valt onder de VIR/BIR-implementatie van het moederdepartement AZ.
SAML (Inloggegevens)	Ja	Er is een soort WeTransfer app binnen het Rijksoverheid online platform. Deze maakt gebruik van SAML voor het authentiseren van gebruikers. Er zijn geen andere diensten die via Rijksoverheid worden aangeboden en inloggen vereisen (met SAML).
SPF (Preventie van mailspoofing/phishing)	Ja	Het e-maildomein @rijksoverheid.nl is integraal van SPF voorzien (zie: https://internet.nl/mail/rijksoverheid.nl/).
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Gepland	Verzendende mailservers die STARTTLS ondersteunen, kunnen met ontvangende mailserver(s) een beveiligde verbinding opzetten. Tenminste één van de mailserverdomeinen bevat geen TLSA-record voor DANE (zie:

		https://internet.nl/mail/rijksoverheid.nl/). SSC-ICT geeft aan dat de planning voor implementatie van DANE Q4 2018 is.
TLS v1.2, v1.1 en v1.0 (Beveiligde, versleutelde verbindingen)	Ja	Rijksoverheid.nl maakt gebruik van het Platform Rijksoverheid Online en daardoor geheel voorzien van https door middel van PKIo EV certificaten (zie: https://internet.nl/site/www.rijksoverheid.nl/).
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Ja	De website voldoet aan Digitoegankelijk (WCAG 2.0). Zie ook de verantwoording daarover op: http://www.rijksoverheid.nl/toegankelijkheid.
ODF 1.2 (Documentbewerkingen)	Ja	Het CMS van het Platform Rijksoverheid Online accepteert slechts ODF (open standaard) formaten. Er zijn wel 'legacy'-bestanden in alleen .doc of .xls formaat.
OWMS (Metadata overheidsinformatie)	Ja	De beleidskeuzes (contentmodellen) zijn in te zien in het Informatie Publicatie Model (IPM) bij het OWMS (zie: http://standaarden.overheid.nl/rijksoverheid).
PDF 1.7 / PDF A/1 en PDF A/2 (Documentpublicatie/ archivering)	Nee	DPC publiceert zelf geen PDF's, maar departementen kunnen PDF's op Rijksoverheid plaatsen. Vooralsnog kan de Rijksoverheid praktisch niet aan deze richtlijn voldoen. DPC is daarover met BZK in gesprek.
		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 2017 is de PDF standaard op nee gezet. En is de STARTTLS/DANE standaard opgenomen en op gepland gezet. SSC-ICT is voornemens DANE te implementeren in Q4 2018.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Rijksoverheid.nl voldoet aan DMARC.

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

4. Gegevens en registreren

4.1 Basisregistraties

4.1.1 NHR (Handelsregister)

Beheerorganisatie: Kamer van Koophandel

Werking en inhoud NHR (bron: Monitor GDI 2018)
Het Handelsregister is de basisregistratie waarin alle rechtspersonen en ondernemingen in Nederland zijn opgenomen. Aansluiten op de Basisregistratie Handelsregister gaat om het tot stand brengen van een elektronische verbinding tussen het Handelsregister en de afnemer. Actuele gegevens uit het Handelsregister kunnen worden overgebracht via de informatieproducten van het Handelsregister.

Standaard	Status	Toelichting
		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 zowel website als mailservers aan DMARC (zie: https://internet.nl/mail/kvk.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC wordt volledig toegepast (zie: https://en.internet.nl/site/kvk.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels	De voorziening gebruikt zowel HTTPS als HSTS. Eén subdomein (kvk.nl zonder www) gebruikt nog geen HSTS, dit wordt hersteld.
IPv4 en IPv6 (Internetnummers)	Deels	Mailservers e.d. zijn bereikbaar via zowel IPv4 als IPv6 maar de website van KvK nog niet, De website kvk.nl ondersteunt IPv4, maar is niet toegankelijk via IPv6 (zie: https://internet.nl/site/www.kvk.nl/). Het project om over te stappen naar IPv6 voor de website hangt samen met de wisseling van provider die KvK wil gaan doen, die wisseling is in 2017 uitgesteld tot 2018 maar nog niet ingepland.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De KvK is sinds 2016 ISO 27001 gecertificeerd en hanteert ISO27002.
SAML (Inloggegevens)	Ja	eHerkenning is SAML-based en wordt toegepast voor het aanleveren van jaarrekeningen en informatieverstrekking. In de

		notarisapplicatie kan de notaris van achter zijn computer rechtstreeks opgave doen. Ook hier wordt gebruik gemaakt van SAML als authenticatieprocedure. Omdat gebruik wordt gemaakt van een generiek identificatie- en authenticatiesysteem voor alle diensten van KvK kan SAML voor elke dienst ingezet worden voor authenticatie.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd voor NHR.
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Gepland	De voorziening past alleen STARTTLS toe, DANE nog niet (zie: https://internet.nl/mail/kvk.nl/). KvK heeft inmiddels de middelen in huis om DANE op DNS-servers te gaan ondersteunen. De beheerder geeft echter aan dat dit een lastige, risicovolle operatie is. De start ervan is voorzien in 2018.
TLS v1.2, v1.1 en v1. (Beveiligde, versleutelde verbindingen)	Ja	De KvK gebruikt TLS op de verbindingen waar voorheen SSL werd gebruikt. De kamer is inmiddels overgegaan op TLS1.2 (zie: https://internet.nl/site/www.kvk.nl/).
		Document en (web/app)content
Ades Baseline Profiles (Digitaal ondertekenen van documenten)	Ja	De NHR voldoet aan de Ades Baseline Profiles standaard.
CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)	Deels	De bij de KvK in gebruik zijnde content management systemen Tridion, Sharepoint en Documentum zijn compliant aan de CMIS standaard. Nog niet alle interne koppelingen op deze systemen zijn gemigreerd naar deze standaard, daar zijn ook nog geen plannen voor. Koppelingen met Sharepoint worden CMIS compliant uitgevoerd.
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Deels	De KvK voldoet volledig aan de eisen van Digitoegankelijk voor alle nieuwe onderdelen. Voor oudere onderdelen van de website wordt getracht compliant te zijn in 2019. Voor nieuwe app's geldt inmiddels standaard de Digitoegankelijk eis.
Open API Specification (Beschrijven van REST API's)	Gepland	KvK zal in 2018 een start maken om aan deze standaard te voldoen. Reeds operationele API's worden echter hierop niet aangepast.
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/ archivering)	Ja	Alle uittreksels en informatie uit het NHR wordt in PDF/A-vorm verstrekt. Het betreft PDF A/1.
SKOS (Thesauri en begrippen-woordenboeken)	Nee	SKOS is nog niet geïmplementeerd in Gegevenscatalogus NHR. De standaard wordt wel voorzien door diverse ondersteunende software pakketten in gebruik bij de KVK rondom het NHR. Implementatie van SKOS in de Gegevenscatalogus HR is nog niet ingepland.
		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	KvK migreert haar financiële systeem in 2018 naar ProFiT van AFAS, UBL 2.1 en SMeF 2.0 worden wel ondersteund maar de modelfactuur nog niet.

Ten opzichte van 2017 zijn er een aantal ontwikkelingen. Alle nieuwe onderdelen van NHR voldoen aan Digitoegankelijk (EN 301 549 met WCAG 2.0). Voor oudere onderdelen van de website wordt getracht compliant te zijn in 2019. DNSSEC wordt volledig toegepast. HTTPS/HSTS is van de status gepland naar de status deels gegaan. Mailservers e.d. zijn bereikbaar via zowel IPv4 als IPv6. De website kvk.nl ondersteunt IPv4, maar is niet toegankelijk via IPv6. Dit was gepland voor 2017, maar is verzet naar 2018. De voorziening past alleen STARTTLS toe, DANE nog niet (zie https://internet.nl/mail/kvk.nl/). KvK heeft inmiddels de middelen in huis om DANE op DNS-servers te gaan ondersteunen, de start ervan is vertraagd (Q4 2017) en voorzien in 2018.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) zijn DMARC, NLCIUS en Open API relevant. Volgens KVK voldoen zowel website als mailservers aan DMARC. Implementatie van Open API staat gepland voor 2018. NHR voldoet nog niet aan NLCIUS.

Concluderend, moeten voor NHR nog de volgende standaarden (volledig) worden geïmplementeerd: CMIS, Digitoegankelijk (EN 301 549 met WCAG 2.0), HTTPS/HSTS, IPv4 en IPv6, SKOS, STARTTLS/DANE, NLCIUS, Open API.

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

Beheerorganisatie: Kadaster

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

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

Werking en inhoud BAG (bron: Monitor GDI 2018)
De Basisregistraties Adressen en Gebouwen (BAG) zijn de registraties waarin gemeentelijke basisgegevens over alle gebouwen en adressen in Nederland zijn vastgelegd.

Werking en inhoud BRK (bron: Monitor GDI 2018)

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

Werking en inhoud WOZ (bron: Monitor GDI 2018)
De Basisregistratie Waarde Onroerende Zaken (WOZ) maakt het mogelijk dat de in de WOZ-beschikking vastgestelde WOZ-waarde door alle overheidsorganisaties, die daarvoor een wettelijke taak hebben, gebruikt kan worden. De Landelijke Voorziening WOZ (LV WOZ) maakt het mogelijk dat afnemers (mits daartoe geautoriseerd) via een centraal loket alle WOZ-gegevens kunnen krijgen.

Werking en inhoud BGT (bron: Monitor GDI 2018)
De Basisregistratie Grootschalige Topografie (BGT) is de gedetailleerde grootschalige digitale kaart van heel Nederland. Alle fysieke objecten zoals gebouwen, wegen, water en natuur worden hierin vastgelegd. De opbouw van de BGT is sinds 10 oktober 2017 gereed. Voor overheden en andere wettelijke gebruikers is het gebruik van de BGT vanaf 1 juli 2017 verplicht.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/ phishing)	Ja	Het Kadaster voldoet aan DKIM.
DMARC (Anti-phishing)	Ja	Deze standaard is geïmplementeerd.
DNSSEC (Beveiligde domeinnamen)	Ja	De website www.kadaster.nl ondersteunt DNSSEC (zie: https://internet.nl/domain/www.kadaster.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Gepland	HTTPS is correct geconfigureerd (en wordt afgedwongen). HSTS is deels geïmplementeerd en is gepland in Q3 en 4 verder geïmplementeerd te worden (zie: https://internet.nl/domain/www.kadaster.nl/)De verwachte implementatie per Q1 2018 is niet gehaald.
IPv4 en IPv6 (Internetnummers)	Ja	Zowel IPv4 als IPv6 worden ondersteund door het Kadaster (zie: https://internet.nl/domain/www.kadaster.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Het Kadaster is gecertificeerd voor NEN-ISO/IEC 27001 en hanteert 27002. Het Handboek Beveiliging Kadaster is volledig op de BIR gebaseerd. In het jaarverslag is een in control statement opgenomen.
SPF (Preventie van mailspoofing/ phishing)	Ja	SPF is geïmplementeerd (zie: https://internet.nl/mail/kadaster.nl/).

STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Gepland	STARTTLS is geïmplementeerd, maar de verwachte implementatie van DANE is gepland per Q1 2019 te zijn geïmplementeerd (zie: https://internet.nl/domain/www.kadaster.nl/).De verwachte implementatie van DANE per Q1 2018 is niet behaald.
TLS v1.2, v1.1 en v1.0. (Beveiligde, versleutelde verbindingen)	Ja	Deze standaard wordt volledig door het Kadaster ondersteund (zie: https://internet.nl/domain/www.kadaster.nl/).
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Ja	Het Kadaster voldoet aan de Webrichtlijnen en heeft een toegankelijkheidsverklaring gepubliceerd op kadaster.nl.
Open API Specification (Beschrijven van REST API's)	Ja	Deze standaard is geïmplementeerd.
PDF 1.7, PDF/A-1 en PDF/A-2 (Documentpublicatie/ archivering)	Ja	Uittreksels worden verstrekt in PDF 1.4-formaat. Databestanden worden vooral in GML uitgewisseld. GML is een standaard XML-formaat voor Geo-data, gebaseerd op de Geo-standaarden. Afnemers melden geen problemen met het huidige PDF formaat. Daarom geeft het Kadaster geen prioriteit aan het vervangen van PDF 1.4. Voor het archiveren van kennisgevingen wordt gebruik gemaakt van PDF/A-1.
SKOS (Thesauri en begrippen-woordenboeken)	Deels	Het Kadaster hanteert SKOS voor de beschikbaarstelling van begrippenkaders van basisregistraties. De begrippenkaders voor de BRK zoals gepubliceerd op brk.basisregistraties.nl, de BAG zoals gepubliceerd op bag.basisregistraties.nl en de BGT (IMgeo) en BRT op definities.geostandaarden.nl zijn allemaal conform SKOS. Voor de WOZ moet deze slag nog worden gemaakt. (4 van de 5 BR's). Hiervoor is nog geen planning.
		E-facturatie en administratie
NLCIUS (Elektronisch factureren)	Nee	Invoering van elektronisch factureren is onderhanden en daarop zal gebruik gemaakt gaan worden van de NLCIUS standaard.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichten-uitwisselingen)	Deels	Vrijwel alle koppelingen met afnemers, andere basisregistraties en evt. front-office systemen worden gelegd op basis van Digikoppeling: - de koppelingen voor het aanleveren van gegevens aan LV-BAG, LV-WOZ en LV-BGT zijn gebaseerd op Digikoppeling standaarden; - het aanleveren door bronhouders (o.a. notariaat) van gegevens aan de BRK is niet gebaseerd op Digikoppeling;

		- de koppelingen voor het verkrijgen van informatie van gegevens uit LV BAG en LV WOZ en BRK zijn gebaseerd op Digikoppeling. Daarnaast kan informatie uit LV's worden verkregen via PDOK (Publieke Dienstverlening op de Kaart) die gebruik maakt van de Open GEO-standaarden. Ook de informatie uit de BRT wordt op deze wijze geleverd. Gegevens uit de BGT zijn beschikbaar via PDOK.
Geo-Standaarden (Geografische informatie)	Ja	Naast de INSPIRE richtlijnen, maakt het Kadaster gebruik van NEN3610 en de meest gangbare Geo standaarden voor de betreffende basisregistraties.
StUF (Uitwisseling administratieve overheidsgegevens)	Ja	Het Kadaster maakt deels gebruik van StUF en is deels volgens de Geo-standaarden (GML) opgemaakt. StUF wordt gebruikt voor aanlevering van bronhouder naar LV-BAG, LV-WOZ en LV-BGT. WOZ en BGT worden ook geleverd in StUF.

Ten opzichte van 2017 is de Digikoppeling 2.0 standaard van status 'ja' op status 'deels' gezet, omdat een aantal koppelingen niet op Digikoppeling gebaseerd zijn. De PDF 1.7, PDF/A-1 en PDF/A-2 standaard is volledig geïmplementeerd.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) zijn DMARC, NLCIUS en Open API relevant. DMARC en Open API zijn geïmplementeerd. Invoering van elektronisch factureren is onderhanden en daarop zal gebruik gemaakt gaan worden van de NLCIUS standaard.

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

4.1.3 BRT (Basisregistratie Topografie)

Beheerorganisatie: Kadaster

Werking en inhoud BRT (bron: Monitor GDI 2018)
De Basisregistratie Topografie (BRT) bestaat uit digitale topografische bestanden, veelal kaarten, op verschillende schaal niveaus.

Standaard	Status	Toelichting
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	DMARC is geïmplementeerd.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Gepland	HTTPS wordt al toegepast, HSTS is deels geïmplementeerd (zie: https://internet.nl/domain/www.kadaster.nl/). Verdere implementatie is gepland in Q3 en Q4 2018. Implementatie per Q1 2018 is niet gehaald.

NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Het Kadaster is gecertificeerd voor NEN-ISO/IEC 27001 en hanteert 27002. Het Handboek Beveiliging Kadaster is volledig op de BIR gebaseerd. In het jaarverslag is een in control statement opgenomen.
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Gepland	STARTTLS is geïmplementeerd (zie: https://internet.nl/domain/www.kadaster.nl/). DANE is gepland per Q1 2019 te zijn geïmplementeerd. Verwachte implementatie van DANE per Q1 2018 is niet gehaald.
TLS v1.2, v1.1 en v1. (Beveiligde, versleutelde verbindingen)	Ja	Deze standaard wordt volledig door het Kadaster ondersteund (zie: https://internet.nl/domain/www.kadaster.nl/).
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Nee	Het Kadaster voldoet aan de Webrichtlijnen en heeft een toegankelijkheidsverklaring gepubliceerd op kadaster.nl. Naar verwachting voldoet het Kadaster in Q4 2018 volledig aan de toegankelijkheidsrichtlijn.
OWMS (Metadata overheidsinformatie)	Nee	OWMS is wel van toepassing, maar PDOK hanteert via het Nationaal GEO Register de wettelijk vastgelegde standaarden, gebaseerd op Inspire en ISO volgens het zogenaamde NL profiel. Data.overheid.nl harvest het NGR met behulp van de CSW standaard (Catalogue Services for the Web' een OGC-Geostandaard (Open Geospatial Consortium), ook onderdeel van INSPIRE). De BRT voldoet dus niet aan de standaard maar voldoet wel aan alternatieve internationale standaarden. Er zijn geen interoperabiliteitsproblemen hierdoor.
SKOS (Thesauri en begrippen-woordenboeken)	Ja	Het Kadaster hanteert SKOS voor de beschikbaarstelling van begrippenkaders van basisregistraties. De begrippenkaders voor de BRK zoals gepubliceerd op brk.kadaster.nl, de BAG zoals gepubliceerd op bag.kadaster.nl en de BGT (IMgeo) en BRT op definities.geostandaarden.nl zijn allemaal conform SKOS.
		Stelselstandaarden
Geo-Standaarden (Geografische informatie)	Ja	De BRT wordt zowel geleverd via PDOK (Wat biedt Publieke Dienstverlening Op de Kaart) in GML (Objectdata), als via internationale Geo-standaarden. Daarnaast wordt de BRT geleverd via PDOK in rasterformaat in GEO, tiff formaat en WMTS (Web Map Tile Service).

Ten opzichte van 2017 is de status van de standaard Digitoegankelijk (EN 301 549 met WCAG 2.0) van de status 'ja' naar 'nee' gegaan. De verwachting van de beheerder is dat het kadaster wat Digitoegankelijk (EN 301 549 met WCAG 2.0) betreft in Q4 2018 volledig aan de toegankelijkheidsrichtlijn voldoet.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. DMARC is reeds geïmplementeerd.

Concluderend moet de BRT nog de volgende standaarden (volledig) implementeren: Digitoegankelijk (EN 301 549 met WCAG 2.0), HTTPS/HSTS, OWMS, STARTTLS/DANE. Ten aanzien van OWMS moet opgemerkt worden dat wel wordt voldaan aan overige en verplichte internationale standaarden. Daarmee wordt bewust afgeweken van de OWMS standaard.

4.1.4 BRV (Basisregistratie Voertuigen)

Beheerorganisatie: RDW (Rijksdienst Wegverkeer)

Werking en inhoud van BRV (Bron: Monitor GDI 2018)
In de Basisregistratie Voertuigen (BRV) staan gegevens van voertuigen, kentekenbewijzen en personen aan wie het kentekenbewijs is afgegeven. Een organisatie is aangesloten op de Basisregistratie Voertuigen wanneer op een gestructureerde wijze (niet incidenteel) informatie wordt afgenomen uit het Kentekenregister. Alle gemeenten, provincies, waterschappen, (relevante) departementen, manifestpartijen en andere overheidsorganisaties in de voertuigenketen zijn aan gesloten op de BRV.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	De BRV voldoet aan DKIM.
DMARC (Anti-phishing)	Ja	De BRV voldoet aan DMARC.
DNSSEC (Beveiligde domeinnamen)	Ja	De BRV voldoet aan DNSSEC. De niet-gevoelige (technische) gegevens uit de BRV zijn te bevragen via www.rdw.nl. Die site is volgens internet.nl gesigned met DNSSEC. Alle .nl rdw domeinen zijn gesigned met DNSSEC.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Gepland	Implementatie wordt medio 2018 gerealiseerd.
IPv4 en IPv6 (Internetnummers)	Nee	IPv4 wordt ondersteund, IPv6 wordt nog niet ingezet. De BRV is te bevragen via www.rdw.nl. Op dit moment ziet de RDW voor de BRV nog geen noodzaak om op IPv6 over te gaan.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging)	Ja	De BRV voldoet aan deze standaard.

(Richtlijnen en principes informatiebeveiliging)		
SAML (Inloggegevens)	Ja	De BRV voldoet aan SAML.
SPF (Preventie van mailspoofing/phishing)	Ja	RDW ondersteunt en gebruikt de SPF standaard voor email verkeer.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	De BRV voldoet aan STARTTLS, DANE, DKIM en SPF.
TLS v1.2, v1.1 en v1. (Beveiligde, versleutelde verbindingen)	Ja	RDW ondersteunt en gebruikt de TLS protocollen op de e-mail servers en Digikoppeling.
		Document en (web/app)content
CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)	Nee	Het bij RDW gebruikte platform voor document management ondersteunt CMIS maar er is voor RDW op dit moment geen aanleiding, zowel intern als extern, om CMIS toe te passen.
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Deels	De website van de RDW voldoet nog niet volledig aan de Webrichtlijnen (versie 2, niveau AA). Voor de status wordt verwezen naar: https://www.rdw.nl/over-rdw/dienstverlening/kwaliteits--en-servicenormen/toegankelijkheidsverklaring.
Open API Specification (Beschrijven van REST API's)	Ja	De BRV voldoet aan Open API Specification.
OWMS (Metadata overheidsinformatie)	Ja	De toegang tot BRV-data is op data.overheid.nl in overeenstemming met OWMS gemetadateerd beschikbaar.
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/archivering)	Ja	Bij digitale dienstverlening worden uittreksels en informatie uit de BRV in PDF/A vorm verstrekt.
SKOS (Thesauri en begrippenwoordenboeken)	Ja	De BRV voldoet aan SKOS.
		Stelselstandaarden
Digikoppeling 2.0	Deels	RDW maakt voor alle nieuwe uitwisselingen gebruik van Digikoppeling. Dat is onder meer het geval in de uitwisseling met

(Veilige berichtenuitwisseling en)	MijnOverheid (Berichtenbox), CJIB, Politie, ILT, CBR, de Belastingdienst, etc. Bestaande koppelingen blijven via bestaande middelen lopen, tenzij onderhoud of wijzigingen de mogelijkheid bieden om de digikoppeling mee te nemen.

Ten opzichte van 2017 voldoet de BRV aan STARTTLS/DANE. Verder is DKIM toegevoegd, de BRV voldoet aan deze standaard.

Van de standaarden die in 2018 nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) zijn DMARC en Open API Specification relevant. BRV voldoet aan beide standaarden.

Concluderend moeten voor de BRV nog (volledig) worden geïmplementeerd: CMIS, Digikoppeling 2.0, Digitoegankelijk (EN 301 549 met WCAG 2.0), HTTPS en HSTS en IPv4 en IPv6.

4.1.5 BRI (Basisregistratie Inkomen)

Beheerorganisatie: Belastingdienst

Werking en inhoud BRI (bron: Monitor GDI 2018)
In de Basisregistratie Inkomen staat van ongeveer 13 miljoen burgers per jaar het authentiek inkomen gegeven dat gebaseerd is op het verzamelinkomen of het belastbaar jaarloon. Overheidsorganisaties gebruiken de BRI om toeslagen, subsidies of uitkeringen te bepalen.

Standaard	Status	Toelichting
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	De voorziening voldoet aan de DMARC standaard.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De BRI voldoet aan de standaard beveiligingseisen van de Belastingdienst. Deze eisen zijn conform VIR met classificatie departementaal vertrouwelijk. Voor opsporingsgegevens (FIOD) geldt een strakker regime. Aangezien het beveiligingskader voor de gehele Belastingdienst geldt, is er geen apart in control statement voor de BRI.
TLS v1.2, v1.1 en v1. (Beveiligde, versleutelde verbindingen)	Ja	De actuele versies van TLS maken deel uit van de standaard beveiligingsrichtlijnen van de Belastingdienst.
WPA2 Enterprise (Toegang tot een WiFi-netwerk met account)	Ja	WPA2 wordt toegepast door de Belastingdienst.
		Stelselstandaarden
Digikoppeling 2.0	Ja	Digikoppeling wordt toegepast in de rol van afnemer van berichten van basisregistraties(HR). De ebMS-koppeling met

(Veilige berichtenuitwisselingen)	Digilevering is operationeel in de productie-omgeving. De aansluiting op Digilevering wordt nu alleen gebruikt in de rol van afnemer van het stelsel van basisregistraties. Het aansluiten van de BRI als Basisregistratie/leverancier op Digilevering was niet eerder dan 2017-2018 gepland.

Ten opzichte van 2017 zijn er ten aanzien van reeds opgenomen standaarden geen wijzigingen.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. BRI voldoet aan DMARC.

Concluderend voldoet BRI (volledig) aan de verplichte standaarden.

4.2 Digilevering

Beheerorganisatie: Logius

Inhoud en werking van Digilevering (Bron: Monitor GDI 2018)
Digilevering is een abonnementenvoorziening voor het automatisch verstrekken van gebeurtenisberichten vanuit een basisregistratie. Een gebeurtenisbericht is bijvoorbeeld het starten van een bedrijf of een verandering in iemands inkomen. Afnemers van basisregistraties ontvangen via Digilevering wijzigingen in de vorm van automatisch gegenereerde berichten waarop zij geabonneerd zijn.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM[6] (Preventie van mailspoofing/phishing)	Ja	Digilevering draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. DKIM is geïmplementeerd op de centrale voorziening mail relay.
DMARC (Anti-phishing)	Gepland	Implementatie van DMARC staat gepland voor Q1 2019.
DNSSEC[7] (Beveiligde domeinnamen)	Ja	DNSSEC is geïmplementeerd op de centrale voorziening DNS.

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

[7] idem

HTTPS/HSTS[8] (Beveiligd, versleuteld webverkeer)	Nee	Digilevering voldoet aan de HTTPS standaard. Aan HSTS wordt niet voldaan.
IPv4 en IPv6 (Internetnummers)	Gepland	Implementatie van IPv6 staat gepland voor Q1 2019. Digilevering gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik.
SPF[9] (Preventie van mailspoofing/phishing)	Ja	Digilevering draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. SPF is geïmplementeerd op de centrale voorziening mail relay.
STARTTLS/DANE[10] (Beveiligd, versleuteld mailverkeer)	Ja	Digilevering draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Digilevering maakt gebruik van Digikoppeling.

Ten opzichte van 2017 staat de implementatie van IPv6 gepland voor Q1 2019. De status van HTTPS/HSTS is van ‘ja’ naar ‘nee’ gegaan, omdat niet voldaan wordt aan HSTS.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Implementatie van de standaard staat gepland voor Q1 2019.

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

4.3 Digimelding

Beheerorganisatie: Logius

Inhoud en werking van Digimelding (bron: Monitor GDI 2018)

[8] idem

[9] idem

[10] idem

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

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	DKIM draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. DKIM is geïmplementeerd op de centrale voorziening mail relay.
DMARC (Anti-phishing)	Gepland	Implementatie van DMARC staat gepland voor Q1 2019.
DNSSEC[11] (Beveiligde domeinnamen)	Ja	DNSSEC is geïmplementeerd op de centrale voorziening DNS.
HTTPS/HSTS[12] (Beveiligd, versleuteld webverkeer)	Nee	Digilevering voldoet aan de HTTPS standaard. HSTS wordt niet toegepast.
IPv4 en IPv6 (Internetnummers)	Nee	Digimelding gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik. Digimelding ondersteunt op dit moment alleen IPv4.
SPF[13] (Preventie van mailspoofing/phishing)	Ja	Digimelding draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. SPF is geïmplementeerd op de centrale voorziening mail relay.
STARTTLS/DANE[14]	Ja	Digimelding draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar

[11] [11] Digimelding en Digilevering zijn op het Equinix platform geïmplementeerd, de applicaties kunnen alleen via de mail-relay server van het platform e-mail versturen. Deze mail –relay server is niet van buitenaf benaderbaar, daarom kan dit met internet.nl niet getoetst worden.

[12] idem

[13] idem

[14] idem

(Beveiligd, versleuteld mailverkeer)		buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Digimelding maakt gebruik van Digikoppeling.

Ten opzichte van 2017 is de status van HTTPS/HSTS van ‘ja’ naar ‘nee’ gegaan, omdat niet voldaan wordt aan HSTS.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Implementatie van DMARC staat gepland voor Q1 2019.

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

4.4 Stelselcatalogus

Beheerorganisatie: Logius

Inhoud en werking van stelselcatalogus (bron: Monitor GDI 2018)
De Stelselcatalogus geeft inzicht in de begrippen en definities die worden gebruikt binnen het stelsel van Basisregistraties. De Stelselcatalogus geeft gebruikers, afnemers, leveranciers en anderen een zo volledig mogelijk beeld van de beschikbare gegevens, begrippen en hun betekenis binnen het Stelsel van Basisregistraties. De Stelselcatalogus helpt op die manier om de overheidsdoelstelling van ’eenmalige gegevensaanlevering en meervoudig gebruik’ te realiseren.

Standaard	Status	Toelichting
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	De Stelselcatalogus voldoet aan DMARC (zie: https://internet.nl/mail/stelselcatalogus.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC is geïmplementeerd op de centrale voorziening DNS (zie: https://internet.nl/site/www.stelselcatalogus.nl/).
HTTPS/ HSTS (Beveiligd, versleuteld webverkeer)	Nee	HTTPS is in 2017 geïmplementeerd. HSTS wordt nog niet ondersteund (zie: https://internet.nl/site/www.stelselcatalogus.nl/).

IPv4 en IPv6 (Internetnummers)	Ja	De Stelselcatalogus gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik. Stelselcatalogus ondersteunt IPv4 en IPv6 (zie: https://internet.nl/site/www.stelselcatalogus.nl/92837).
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Ja	De webpagina's van de Stelselcatalogus vallen binnen de website van digitaleoverheid.nl. Zie certificaat van toegankelijkheid van Accessibility.nl. Zie: https://www.digitaleoverheid.nl/toegankelijkheidsverklaring.
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/ archivering)	Ja	Documenten worden als PDF-A/1 aangeboden via de website.
SKOS (Thesauri en begrippen-woordenboeken)	Ja	SKOS wordt toegepast door de voorziening.
		Juridische identificatie en verwijzing
BWB (Wet- en regelgeving)	Ja	De Stelselcatalogus gebruikt het Basis Wetten Bestand (BWB) via Juriconnect als open standaard voor de link naar de wetgeving als bron. De Juriconnect Id's worden gebruikt om per gegeven of begrip in de Stelselcatalogus de link te leggen naar de wet en het artikel in het Basis Wetten Bestand.

Ten opzichte van 2017 is HTTPS geïmplementeerd. HSTS wordt nog niet ondersteund.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. De Stelselcatalogus voldoet aan DMARC.

Concluderend, moet de Stelselcatalogus nog de volgende standaard (volledig) implementeren: HTTPS/ HSTS.

4.5 P-Direkt

Beheerorganisatie: P-Direkt

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

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

Standaard	Status	Toelichting

		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	P-Direkt maakt gebruik van de mailservers van SSC-ICT, onder andere voor het versturen van de loonstroken aan de medewerkers. P-Direkt heeft aangegeven dat het initiatief voor de adoptie van dit soort standaarden dan ook bij SSC-ICT ligt. Navraag bij SSC-ICT leert dat DKIM actief gemaakt is voor deze mailservice van P-Direkt.
DMARC (Anti-phishing)	Ja	De Rijksbrede mail voorziening waarvan P-Direkt gebruik maakt, ondersteunt DMARC.
DNSSEC (Beveiligde domeinnamen)	Nee	Op de Haagse ring maakt het netwerk van SSC-ICT, waar P-Direkt gebruik van maakt, geen gebruik van DNSSEC. Ook hier geldt dat P-Direkt een afnemer is van een Rijksbrede dienst en het initiatief voor het implementeren van DNSSEC bij de SSC-ICT ligt. SSC-ICT gaf in 2016 aan dat zij op hun beurt weer afhankelijk zijn van de leverancier van de Haagse ring, namelijk Logius. Inmiddels is DNSSEC nog niet geïmplementeerd en is er geen verdere informatie voorhanden.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Gepland	HTTPS is 100% doorgevoerd voor alle communicatie met klanten. HSTS is nog niet geïmplementeerd. De externe sites P-Direkt.nl en sciorijk.nl voldoen beide aan HSTS. Eén interne site voldoet hier niet aan. Planning voor implementatie is Q1 2019.
IPv4 en IPv6 (Internetnummers)	Nee	De Haagse ring, waarover eigenlijk al het verkeer naar P-Direkt loopt, ondersteunt geen IPv6. De P-Direkt voorzieningen, zoals gehost bij Match, ondersteunen in theorie momenteel al IPv6.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Deels	De hosting van de dienstverleningssystemen van P-Direkt voldoet aan de BIR (BIR compliancy is integraal onderdeel van de inrichting van het ODC, en als zodanig daarmee ook voor P-Direkt). Echter, de beheersorganisatie voldoet niet volledig aan de BIR en zit in een proces/project om aan de BIR te voldoen.
SAML (Inloggegevens)	Ja	P-Direkt gebruikt SAML om Single Sign-On in te vullen. Verbinding naar de kerndepartementen is gelegd, maar een gedeelte van de rijksambtenaren van onderliggende organisatieonderdelen, moeten nog handmatig inloggen. P-Direkt heeft met de kerndepartementen de afspraak gemaakt dat de kerndepartementen verantwoordelijk zijn voor het implementeren van de Single Sign-on functie bij de onderliggende organisatieonderdelen.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd door de beheerder van de maildienst (in het geval van P-Direkt is dat SSC-ICT).
TLS v1.2, v1.1 en v1.0 (Beveiligde, versleutelde verbindingen)	Ja	Alle diensten van P-Direkt die door middel van HTTP worden ontsloten, worden enkel aangeboden via TLS v1.0 of hoger.
		Document en (web/app)content
Ades Baseline Profiles (Digitaal ondertekenen van documenten)	Nee	De implementatie van deze standaard is nog niet gestart en hiervoor is nog geen concrete planning. P-Direkt doet onderzoek naar geavanceerde en gekwalificeerde digitale handtekeningen.

Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Gepland	Het Portal is nog altijd in ontwikkeling. Er is op dit portal nog geen Webrichtlijnen toets geweest. P-Direkt is zich ervan bewust dat er nog geen volledige compliancy is met de Webrichtlijnen. P-Direkt is in het proces van de impactanalyse van het (tijdelijke) besluit Digitoegankelijk. Hieruit vloeit voor P-Direkt de eis voort om te voldoen aan WCAG 2.x. Voor nieuwe websites streeft P-direkt naar implementatie voor 23 september 2019. Bestaande websites hoopt P-direkt voor 23 september 2020 te hebben omgebouwd. De 2 mobiele apps zijn aangepast voor 23 juni 2021.
ODF (Document-bewerkingen)	Nee	Veel brieven die automatisch gegenereerd worden, worden in Word gemaakt en naar managers verstuurd, die deze dan zelf nog aanpassen. P-Direkt gebruikt .doc(x), omdat dit voor de doelgroep het meest gangbaar is. De ontvanger van de brieven zou dit zelf moeten omzetten met de aanwezige KA software die ODF ondersteunt. In het proces dat brieven genereert is het niet mogelijk ODF bestanden te genereren.
PDF 1.7 – PDF A/1 of PDF A/2 (Documentpublicatie/ archivering)	Deels	De meeste zaken die het digitale personeelsdossier ingaan zijn PFD/A. De grootste uitzondering/afwijking zijn de digitale loonstroken, die zijn nog altijd PDF 1.3. Reden/oorzaak is dat deze aangemaakt worden met een standaard SAP conversieroutine die niet anders dan PDF 1.3 kan genereren. Er is momenteel geen concreet plan de loonstroken in PDF A/x te genereren. PDF A/2 wordt nog niet gebruikt binnen P-Direkt.
		Stelselstandaarde
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	P-Direkt heeft vele interfaces met partijen binnen de overheid, Identity management, hr-data, arbo-diensten, ziekmeldingen, koppelingen met BD. Het salarisverwerkingssysteem werkt op basis van Digikoppeling. Alle nieuwe koppelingen die P-Direkt ontwikkelt, worden gebouwd op basis van Digikoppeling. Richting 2018 migreert de voorziening naar de rijksdatacenters, Digikoppeling krijgt dan een nog belangrijkere rol. Nieuwe interfaces zoals TEM2W, IDM2 en de ARBO interface zijn conform Digikoppeling 2.0.
		Juridische identificatie en verwijzing
BWB (Wet- en regelgeving)	Ja	Alle verwijzingen naar wetten worden conform de BWB-standaard gemaakt. De redactie heeft de richtlijn dat ze altijd op deze manier handelt bij verwijzingen naar wetsteksten of andere regels en richtlijnen die op wetten.overheid.nl te vinden zijn.

Ten opzichte van 2017 is de SPF standaard geïmplementeerd. Bovendien zijn er concrete planningen afgegeven voor de implementatie van Digitoegankelijk (EN 301 549 met WCAG 2.0) en HTTPS/HSTS.

Van de standaarden die in 2018 nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. P-direkt voldoet aan deze standaard.

Concluderend moet voor P-direkt nog (volledig) worden geïmplementeerd: Ades Baseline Profiles, Digitoegankelijk (EN 301 549 met WCAG 2.0), DNSSEC, HTTPS/HSTS, IPv4 en IPv6, NEN-ISO/IEC 27001/27002, ODF, PDF 1.7 – PDF A/1 of PDF A/2.

5. Dienstverlening en verbinden

5.1 eFactureren

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting
		E-facturatie en administratie
NLCIUS (Elektronisch factureren)	Gepland	De SMEF 2.0 standaard was nog niet geïmplementeerd maar wordt opgevolgd door de NLCIUS. Per 19 april 2019 is de NLCIUS verplicht voor overheden, volgens Europese richtlijn 2014/55. Implementatie staat gepland voor Q2 2019.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen NLCIUS relevant. NLCIUS vervangt standaard SMEF 2.0. Implementatie van deze standaard staat gepland voor Q2 2019.

Concluderend, moet voor eFactureren nog de volgende standaarden (volledig) worden geïmplementeerd: NLCIUS.

5.2 SBR

Beheerorganisatie: Logius

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

Dienst Uitvoering Onderwijs (DUO)[15]. De voorziening voor de e-dienstverlening is Digipoort. SBR heeft een eigen website.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/ phishing)	Gepland	De website van SBR (http://www.sbr-nl.nl) heeft ook een mailserver. Omdat de website overgezet wordt naar het Ministerie van AZ, moet DKIM (naast DMARC en SPF) nog ingesteld worden. Daardoor voldoet de website momenteel niet aan DKIM. Planning voor implementatie is Q1, 2019.
DMARC (Anti-phishing)	Gepland	SBR voldoet niet aan DMARC. Dit staat gepland voor Q1 2019.
DNSSEC (Beveiligde domeinnamen)	Ja	De website van SBR (http://www.sbr-nl.nl) Voldoet zowel op het web als het maildomein aan DNSSEC.
IPv4 en IPv6 (Internetnummers)	Ja	De website van SBR wordt bij een derde partij gehost en is bereikbaar met IPv6.
SPF (Preventie van mailspoofing/phis hing)	Ja	De website van SBR (http://www.sbr-nl.nl) heeft ook een mailserver. Deze voldoet aan SPF (zie: https://internet.nl/mail/sbr-nl.nl/).
STARTTLS/ DANE (Beveiligd, versleuteld mailverkeer)	Gepland	Aan STARTTLS wordt voldaan, door de voorziening. Aan DANE wordt nog niet voldaan. Dit is opgenomen in de planning voor Q1 2019.
TLS 1.0, 1.1 en 1.2 (Beveiligde, versleutelde verbindingen)	Ja	De verbinding alleen mogelijk voor voldoende veilige TLS-versies (zie: https://internet.nl/site/www.sbr-nl.nl/#). In geval van Digipoort geldt voor de markt bij koppelvlak WUS en ebMS dat TLS 1.2 de standaard is. TLS 1.0 (en mogelijk ook 1.1) is uitgefaseerd. SSL v3 en v3.1 zijn in 2015 uitgefaseerd. Het koppelvlak Grote Berichten 3.0 worden op TLS 1.0 en TLS 1.1 aangeboden. TLS 1.0 en TLS 1.1 worden nog uitgefaseerd.
		Document en (web/app)content
Ades Baseline Profiles (Digitaal ondertekenen van documenten)	Ja	Binnen SBR (Assurance) waarbij bijvoorbeeld jaarverslagen worden ondertekend door een accountant, wordt binnen DigiPoort gebruik gemaakt van XAdES als EU standaard.

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

Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Gepland	Voor SBR-NL.nl is op Digitoegankelijk getoetst en op zes punten na voldoet deze, er is nog geen verklaring. Per oktober 2018 wordt een nieuw CMS geïmplementeerd.
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/archivering)	Ja	Bij het publiceren van documenten houdt Logius voor SBR PDF/A aan bij publicatie.
		E-facturatie en administratie
XBRL (Bedrijfs-rapportages)	Ja	SBR maakt gebruik van XBRL.

Ten opzichte van 2017 is de implementatie van Digitoegankelijk (EN 301 549 met WCAG 2.0), DKIM en STARTTLS/DANE gepland voor Q1 2019. Verder wordt voldaan aan DNSSEC en SPF.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Implementatie van DMARC staat gepland voor Q1 2019.

Concluderend, moeten voor de SBR nog de volgende standaarden (volledig) worden geïmplementeerd: Digitoegankelijk (EN 301 549 met WCAG 2.0), DKIM, DMARC, STARTTLS/DANE.

5.3 Digipoort

Beheerorganisatie: Logius

DigiPoort is een ICT-centrale waar berichtenverkeer voor de overheid afgehandeld wordt. Overheden kunnen DigiPoort inzetten om bedrijfs- en ketenprocessen te automatiseren. Omdat Digipoort slechts machine-naar-machine koppelingen levert en niet toegankelijk is vanaf het openbare internet, is deze voorziening niet getoetst met de toetsen van internet.nl.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	DigiPoort voldoet aan DKIM. Dit is ook relevant omdat de voorziening een SMTP koppelvlak heeft.
DMARC (Anti-phishing)	Gepland	Planning voor de implementatie van DMARC is Q1 2019, als onderdeel van een Logius breed project voor Domein verhuizing.
DNSSEC (Beveiligde domeinnamen)	Gepland	Implementatie van DNSSEC vindt plaats in Q1 2019.
HTTPS/HSTS	Ja	De voorziening voldoet aan HTTPS. Formeel wordt niet aan HSTS voldaan, maar de standaard HTTP (poort 80) is bij de voorziening helemaal niet

(Beveiligd, versleuteld webverkeer)		ontsloten, zodat feitelijk alleen via HTTPS een verbinding gemaakt kan worden. In de geest voldoet de voorziening dus impliciet wel aan HSTS.
IPv4 en IPV6 (Internetnummers)	Gepland	Digipoort gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik. Digipoort ondersteunt IPv4. Implementatie van IPv6 staat gepland voor Q1 2019.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	DigiPoort voldoet aan de BIR. Leveranciers voldoen aan ISO 27001 of een vergelijkbare standaard.
SPF (Preventie van mailspoofing/phishing)	Gepland	DigiPoort heeft geen SPF-records. Er wordt niet gemaild vanuit dit domein, maar SPF zou wel ingericht moeten worden. Dit is opgenomen in de planning voor Q1 2019.
TLS v1.2, v1.1 en v1. (Beveiligde, versleutelde verbindingen)	Ja	Digipoort ondersteunt TLS v1.2, maar niet meer de verouderde versies.
		Stelselstandaarden
Digikoppeling (Veilige berichten-uitwisselingen)	Ja	Digipoort voldoet aan deze standaard. Zie de koppelvlakspecificaties op http://www.logius.nl/producten/gegevensuitwisseling/digitpoort/koppelvlakken.
		E-facturatie en administratie
SETU (Informatie flexibele arbeidskrachten)	Ja	DigiPoort ondersteunt de uitwisseling van SETU-hr-XML berichten.
XBRL en Dimensions (Bedrijfsrapportages)	Ja	De standaard wordt ondersteund door Digipoort.

Ten opzichte van 2017 is een concrete planning afgegeven voor de implementatie voor DNSSEC, IPv6 en SPF. Verder is de standaard STARTTLS/DANE afgevoerd, omdat de voorziening niet over een eigen emailvoorziening beschikt.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Planning voor de implementatie van DMARC is Q1 2019.

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

5.4 Diginetwerk

Beheerorganisatie: Logius

Diginetwerk is het besloten netwerk van de overheid. Via Diginetwerk kunnen overheden gegevens die een hoge mate van beveiliging vereisen, veilig uitwisselen met andere overheden. Diginetwerk is opgebouwd uit een aantal aan elkaar gekoppelde, specifieke besloten overheidsnetwerken.

Standaard	Status	Toelichting
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	Diginetwerk.nl voldoet aan DMARC
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC validatie wordt toegepast op Rijks-DNS.
IPv4 en IPV6 (Internetnummers)	Gepland	IPv4 is geïmplementeerd voor Diginetwerk. De implementatie van IPv6 staat gepland voor Q4 2018.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Deze standaard is onderdeel van het algemene beveiligingsbeleid van Logius. Logius voldoet aan deze standaard en Diginetwerk is ook gebaseerd op deze standaard.

Ten opzichte van 2017 is er een concrete planning voor de implementatie van IPv6, namelijk Q4 2018. Verder is de standaard STARTTLS/DANE afgevoerd, omdat de voorziening niet over een eigen emailvoorziening beschikt.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Diginetwerk voldoet aan DMARC.

Concluderend, moet Diginetwerk nog de volgende standaard (volledig) implementeren: IPv4 en IPV6.

5.5 Tenderned

Beheerorganisatie: PIANOo/DICTU

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
		Internet en beveiliging
DKIM	Nee	E-mails verzonden vanuit TenderNed zijn niet beveiligd met DKIM (zie: https://internet.nl/mail/tenderned.nl/).

(Preventie van mailspoofing/phishing)		
DMARC (Anti-phishing)	Nee	Tenderned voldoet niet aan DMARC.
DNSSEC (Beveiligde domeinnamen)	Ja	Het domein is gesigned met DNSSEC (zie: https://internet.nl/site/www.tenderned.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	De client-server communicatie van TenderNed is beveiligd met HTTPS en HSTS (zie: https://internet.nl/site/www.tenderned.nl/).
IPv4 en IPV6 (Internetnummers)	Nee	Tenderned.nl is niet voorbereid op IPv6 (zie: https://internet.nl/site/www.tenderned.nl/). TenderNed is afhankelijk van de hostingpartij. Wanneer deze een transitie door maakt naar IPv6 zal TenderNed daarin mee gaan.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	TenderNed is ISO27001/2 gecertificeerd. Dit wordt jaarlijks geaudit.
SAML (Inloggegevens)	Ja	Per 1 juli 2014 is het mogelijk voor gebruikers om, naast de huidige registreer- en inlogmogelijkheden, gebruik te maken van inloggen via eHerkenning. (Bron: http://www.tenderned.nl/eherkenning-en-tenderned-0)
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is inmiddels aangezet door de technisch dienstverlener DICTU. (Zie: https://internet.nl/mail/tenderned.nl/140321/#mailauth).
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Nee	STARTTLS wordt ondersteund. DANE nog niet.
TLS v1.2, v1.1 en v1.0 (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 2.0) (Toegankelijkheid web content)	Nee	TenderNed wordt vanaf 2017 gerenoveerd. Daarbij worden de schermen deels vernieuwd. De beheerder heeft aangegeven nog tot in 2019 te renoveren. Bij de implementatie van nieuwe schermen worden de richtlijnen uit EN 301 539 toegepast.
Open API Specification (Beschrijven van REST API's)	Nee	De publieke API's worden beschreven door middel van Swagger. Swagger kan je zien als OAS versie 2.0. Swagger als API Specificatie bestaat niet meer en is opgegaan in OAS. Tenderned voldoet daarmee niet aan OAS 3.0. Deze versie is belangrijk

		omdat deze samenhang aanbrengt in de verschillende manieren om API specificaties op te stellen.
PDF 1.7, PDF/A-1, PDF/A-2 (Documentpublicatie/ archivering)	Ja	Geautomatiseerd gecreëerde PDF's (bij de aankondigingen) zijn gemaakt in versie 1.7.

Ten opzichte van 2017 is inmiddels SPF geïmplementeerd door de technische dienstverlener. De renovatie van Tenderned is nog gaande en gaat nog tot in 2019 door.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) zijn DMARC en Open API relevant. Echter voldoet Tenderned aan beide standaarden niet.

Concluderend, moet Tenderned nog de volgende standaarden (volledig) implementeren: Digitoegankelijk (EN 301 549 met WCAG 2.0), DKIM, DMARC, IPv4 en IPV6, Open API Specification, STARTTLS en DANE.

5.6 DWR

Beheerorganisatie: Ministerie BZK

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

Binnen SSC-ICT loopt momenteel een project om relevante, voor DWR van toepassing zijnde Open Standaarden te implementeren zover deze nog niet geïmplementeerd waren.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Deels	De implementatie van DKIM en DMARC is voor SSC-ICT zelf voor 90% afgerond. Open staat nog het aanbieden van een dienst voor externe applicaties die mailen of klanten die gebruik maken van externe mailingdiensten. SSC-ICT is voor realisatie van deze dienst afhankelijk van de betreffende klanten.
DMARC (Anti-phishing)	Deels	De implementatie van DKIM en DMARC is voor SSC-ICT zelf voor 90% afgerond. Open staat nog het aanbieden van een dienst voor externe applicaties die mailen of klanten die gebruik maken van externe mailingdiensten. SSC-ICT is voor realisatie van deze dienst afhankelijk van de betreffende klanten.

DNSSEC (Beveiligde domeinnamen)	Deels	De domeinen van de klanten van SSC-ICT die via de DNS van AZ lopen voldoen reeds. De domeinen van de klanten van SSC-ICT die via de DNS van SSC-ICT lopen voldoen eind 2018 i.p.v. eind 2017. SSC-ICT geeft aan dat de cliënt zelf DNSSEC-validatie ondersteunt, er is alleen nog een issue met de Proxy die niet om kan gaan met de validatie. Dit issue is belegd bij de leverancier. RijksDNS tenslotte ondersteunt DNSSEC-validatie.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Gepland	HTTPS wordt gebruikt, maar HSTS wordt nog niet standaard aangezet voor websites die SSC-ICT host voor klanten. Andere webgebaseerde voorzieningen maken wel gebruik van HSTS. Implementatie van deze standaarden is voor eind 2018 voorzien.
IPv4 en IPV6 (Internetnummers)	Gepland	IPv4 is in gebruik. De gebruikte technische componenten van DWR ondersteunen wel IPv6. IPv6 is een onderdeel van de infrastructuur en IPv6 reeksen worden uitgedeeld door Logius. De internet facing kant van de DMZ gaat IPv6 eind 2018 ondersteunen.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	SSC-ICT werkt via deze standaard en wordt hier ook op ge-audit. De laatste audit heeft plaatsgevonden in 2017.
SAML (Inloggegevens)	Ja	Single Sign-on (SSO) op basis van SAML 2.0 wordt aangeboden als dienst in de Servicecatalogus van SSC-ICT. Het SSO-koppelvlak is een generieke dienst. Het project DOorontwikkeling Single Sign-On (DOrSSOn) voorziet internet facing aanvulling van de huidige oplossing met open source componenten gebaseerd op de standaarden SAML 2.0 en OAuth 2.0 in opdracht van de CIO Rijk.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF wordt op alle domeinen toegepast.
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Gepland	De internet mailvoorziening werkt met STARTTLS. Implementatie van DANE in Q4 2018 is in voorbereiding in het verlengde van het initiatief ‘Veilige E-mail Coalitie’. De implementatie van DANE is afhankelijk van DNSSEC, welke ook in Q4 2018 voorzien is (zie hierboven onder “DNSSEC”).
TLS v1.2, v1.1 en v1.0 (Beveiligde, versleutelde verbindingen)	Ja	De op de werkplek aangeboden browsers ondersteunen deze versies van TLS. De internet mailvoorziening werkt met STARTTLS. Voor webservers met applicaties van klanten wordt dit toegepast voor de klanten die dit hebben aangevraagd.
WPA2 Enterprise (Toegang tot een WiFi-netwerk met account)	Ja	Op de wifivoorziening wordt deze standaard toegepast. Wifi wordt door SSC-ICT als voorziening geleverd in de kantoorpanden waar SSC-ICT IT-dienstverlener voor het pand is (IDV-P).
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Deels	Niet alle websites waar SSC-ICT zelf eigenaar is, voldoen op dit moment aan Digitoegankelijk. SSC-ICT is niet de eigenaar van alle websites van haar klanten, bij deze websites ligt de verantwoordelijkheid derhalve bij de klant zelf.

(Toegankelijkheid web content)		
ODF 1.2 (Documentbewerkingen)	Ja	De DWR Next client wordt geleverd met zowel Libreoffice 5.x als Office 2016. Beide softwaresuites ondersteunen het lezen en schrijven van ODF-bestanden.
PDF 1.7 / PDF A/1 en PDF A/2 (Documentpublicatie/ archivering)	Ja	De DWR Next client kan alle types PDF lezen. Schrijven van PDF kan op meerdere manieren. Alle types worden ondersteund, al is daarvoor soms wel het installeren van Adobe Acrobat Professional benodigd. PDF A/2 is mogelijk voor klanten die Adobe Acrobat Pro afnemen. De regulier verstrekte Adobe Acrobat Standard ondersteunt PDF A/2 niet, maar wel PDF 1.7 en PDF A/1. De scanfunctionaliteit in het reguliere multifunctional printplatform voor de werkomgeving ondersteunt PDF 1.7 en PDF A/1.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Deels	Binnen JenV vindt elektronisch berichtenverkeer interdepartementaal plaats via de Justitie Berichten Service (JUBES). JUBES is vanuit JenV het koppelvlak voor de Digikoppelingdienst van Logius. De open standaarden eBMS en WUS zijn de daarbij gebruikte protocollen om de berichten veilig te versturen. Binnen BZ wordt deze standaard gebruikt voor de Mule koppeling. Verder nemen alle departementen uit het verzorgingsgebied van SSC-ICT deel aan eFacturatie. Op deze standaard wordt waar van toepassing aangesloten bij nieuwe koppelingen.

Ten opzichte van 2017 is een concrete planning afgegeven voor implementatie van HTTPS/HSTS, IPv6 en DANE. Inmiddels wordt SPF voor alle domeinen toegepast. Ten opzichte van vorig jaar is de standaard Ades Baseline Profiles verwijderd als relevante standaard. De reden daarvoor is dat dit jaar de beheerder van de voorziening heeft aangegeven dat het onderdeel waarop de standaard van toepassing is niet onder de scope van de DWR voorziening valt. PBLQ kan zich hierin vinden. Overigens is SSC-ICT wel in staat de standaard te leveren en voldoen zij in die zin dus wel.

Van de standaarden die in 2018 nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. DWR voldoet deels aan deze standaard.

Concluderend moeten voor DWR nog (volledig) worden geïmplementeerd: Digitoegankelijk (EN 301 549 met WCAG 2.0), DKIM, DMARC, DNSSEC, HTTPS/HSTS, IPv4 en IPV6, STARTTLS/DANE. De beheerder geeft aan dat SSC-ICT voor de implementatie van sommige standaarden afhankelijk is van haar klanten en zich derhalve niet verantwoordelijk voelt voor het gebruik van de standaard door de klant.

5.7 Digi-Inkoop

Beheerorganisatie: Logius

Digi-Inkoop is een rijksbreed geautomatiseerd inkoopsysteem dat het inkoopproces vereenvoudigt. Digi-Inkoop is er voor de inkoop van alle producten en diensten, van kantoorartikelen tot inhuur van personeel.

Standaard	Status	Toelichting

		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Gepland	Implementatie is opgenomen in de planning (Q1, 2019).
DMARC (Anti-phishing)	Gepland	Implementatie is opgenomen in de planning (Q1, 2019).
DNSSEC (Beveiligde domeinnamen)	Ja	Digi-Inkoop voldoet aan DNSSEC (zie: https://internet.nl/mail/digiinkoop.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening voldoet aan HTTPS/HSTS.
IPv4 en IPV6 (Internet-nummers)	Nee	IPv6 werd in 2016 en 2017 niet ondersteunt door de hoster van Digi-Inkoop. Er zijn geen plannen dit te realiseren, en er is geen opdracht om dit aan te passen (zie: https://internet.nl/mail/digiinkoop.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Digi-Inkoop voldoet aan de BIR. Er is een in control statement afgegeven. Leveranciers voldoen aan ISO 27001.
SPF (Preventie van mailspoofing/phishing)	Gepland	Digi-Inkoop voldoet nog niet aan deze standaard, implementatie is opgenomen in de planning voor Q2 2019.
TLS v1.2, v1.1 en v1.0 (Beveiligde, versleutelde verbindingen)	Ja	Digi-Inkoop is TLS 1.2 compliant (zie: https://internet.nl/mail/digiinkoop.nl/).
		Document en (web/app)content
PDF/A en PDF 1.7 (Documentpublicatie/archivering)	Ja	De Digi-Inkoop 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 Digi-Inkoop gebruik van maakt: https://www.logius.nl/ondersteuning/gegevensuitwisseling/ubl-ohnl en https://www.logius.nl/ondersteuning/gegevensuitwisseling/setu-hr-xml-ohnl).
		E-facturatie en administratie
NLCIUS (Elektronisch factureren)	Gepland	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 staat gepland voor Q2 2019.
SETU (Informatie flexibele arbeidskrachten)	Ja	Digi-Inkoop ondersteunt de uitwisseling van SETU-hr-XML berichten.

Ten opzichte van 2017 zijn implementatie van DKIM en SPF opgenomen in de planning. DKIM is nieuw opgenomen ten opzichte van vorig jaar. Digi-Inkoop voldoet aan HTTPS/HSTS. De status van HTTPS/HSTS is verhoogd van nee naar ja.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) zijn DMARC en NLCIUS relevant. Implementatie van beiden worden opgenomen in de planning.

Concluderend, moeten voor Digi-Inkoop nog de volgende standaarden (volledig) worden geïmplementeerd: DKIM, DMARC, IPv4 en IPV6, NLCIUS, SPF.

Bijlage A Geïnterviewde personen

Naam voorziening	Contactpersoon
BAG, WOZ, BGT, BRK	Harrie van Leeuwen / Piet van der Krieke
Berichtenbox voor bedrijven	Dick Bruinsma, Laura Ouwehand
BRI	Harry Roumen
BRT	Harrie van Leeuwen / Piet van der Krieke
BRV	Walter Huberts, Gert Stel
BSN en GBA-V	Bob te Riele, Hans van Laar
Digi-Inkoop	Peter Haasnoot, Erwin Kaats
DigiD	Peter Haasnoot, Erwin Kaats
DigiD Machtigen	Peter Haasnoot, Erwin Kaats
Digilevering	Peter Haasnoot, Erwin Kaats
Digimelding	Peter Haasnoot, Erwin Kaats
Diginetwerk	Peter Haasnoot, Erwin Kaats
DigiPoort	Peter Haasnoot, Erwin Kaats
Doc-Direkt	Ali Amin Shahidi
DWR	Rein Hennen
eFactureren	Peter Haasnoot, Erwin Kaats
Stelsel elektronische toegangsdiensten	Peter Haasnoot, Erwin Kaats
MijnOverheid	Peter Haasnoot, Erwin Kaats
NHR	Rob Spoelstra
ODC Noord	Jaap Jansma
Ondernemersplein	Milla van der Have, Wouter Nieuwenhuis
Overheid.nl	Lucien de Moor, Hans Overbeek
P-Direkt	Jos van Vlimmeren
PKI Overheid	Peter Haasnoot, Erwin Kaats
Rijksoverheid.nl	Marc van de Graaf, Cees den Heijer
Rijkspas	Stefano Sacceddu
Rijksportaal	Leon Boender
Samenwerkende Catalogi	Peter Haasnoot, Erwin Kaats
SBR	Peter Haasnoot, Erwin Kaats
Stelselcatalogus	Peter Haasnoot, Erwin Kaats
Tenderned	Rudi van Eijck