Rapport

Monitor Open standaarden: rapportage 2017

Onderzoek naar het gebruik van open standaarden van de ‘pas toe of leg uit’-lijst van het Forum Standaardisatie door overheidsorganisaties:

bij aanbestedingen (juli 2016 - juni 2017), in overheidsbrede voorzieningen (zomer 2017) en per standaard (zomer 2017)

Van Jaap Korpel & Joost Vreuls

Versie Versie 1.2

Datum 8-3-2018

Inhoudsopgave

Bijlagen

1. Managementsamenvatting

Het daadwerkelijk gebruik van open standaarden is voor goed en veilig functionerende ICT van de overheid zó belangrijk, dat sinds 2009 het Forum Standaardisatie een lijst beheert van open standaarden die verplicht toegepast moeten worden: de open standaarden van de 'pas toe of leg uit'-lijst.

De kernvraag van de jaarlijkse Monitor Open standaarden is of, en zo ja in welke mate, overheden deze open standaarden daadwerkelijk gebruiken wanneer ze van toepassing zijn.

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 in 2017 nog niet bereikt.
- Bij 81% 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 33% van de aanbestedingen werd om alle of tenminste om alle cruciale relevante open standaarden gevraagd.
- De 35 onderzochte overheidsbrede voorzieningen voldoen in belangrijke mate aan de relevante open standaarden: van de 418 gevallen waarin een open standaard relevant was wordt in 67% van de gevallen daaraan voldaan en in 16% van de gevallen wordt deels voldaan of er zijn concrete plannen om er binnenkort aan te voldoen.
- De beheerorganisaties van veel open standaarden hebben geen goed beeld over het feitelijk gebruik van hun standaarden. Voor de standaarden waarover wèl cijfers beschikbaar zijn blijkt het gebruik in de meeste gevallen tussen 50% en 75% te liggen.

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 2017 waren dit er 40) is het 'pas toe of leg uit'-regime van toepassing.

[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.

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

Monitor Open standaarden 2017 (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 2016 t/m juni 2017 ('pas toe of leg uit' bij feitelijke aanbestedingen), respectievelijk de situatie in de zomer van 2017 (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 2016/2017;
- onderzoek naar de toepassing van open standaarden bij overheidsbrede voorzieningen;
- onderzoek naar gebruiksgegevens van open standaarden, voorzover beschikbaar.

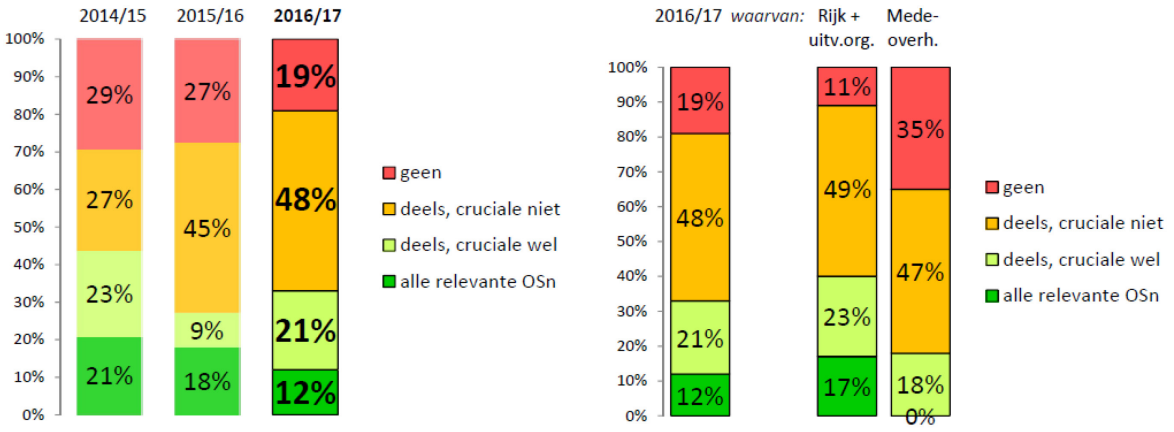
In het navolgende worden de voornaamste bevindingen per deelonderzoek samengevat. De positieve bevindingen hebben een groen blokje (+), de minder positieve een oranje (-).

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 35 aanbestedingen van de rijksoverheid en uitvoeringsorganisaties en 17 aanbestedingen van mede-overheden onderzocht, in totaal 52 aanbestedingen (uit het 3e en 4e kwartaal van 2016 en 1e en 2e kwartaal van 2017). De resultaten worden beschreven in hoofdstuk 3.



Het percentage aanbestedingen waarbij *niet* om een open standaard is gevraagd daalde van 27% vorig jaar naar 19% dit jaar. In 12% van de onderzochte aanbestedingen is gevraagd om alle relevante open standaarden, en in 21% van de aanbestedingen is tenminste om de cruciale standaarden gevraagd. Samen is dat 33%, en dat is meer dan vorig jaar (27%) maar nog wel iets minder dan het jaar dáárvoor. Het percentage

aanbestedingen waarbij om één of meer cruciale standaarden niet is gevraagd – de middencategorie – is licht gestegen: van 45% vorig jaar tot 48% dit jaar.

Rijk en uitvoeringsorganisaties deden het in 2016/2017 een stuk beter dan de mede-overheden: slechts bij 11% van de Rijks-aanbestedingen werd om geen enkele standaard gevraagd (mede-overheden: 35%), bij 17% werd om alle relevante standaarden gevraagd (mede-overheden: 0%) en daarnaast bij nog 23% om tenminste alle cruciale standaarden (mede-overheden: 18%).

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

+	Bij 6 aanbestedingen (12%) is om alle relevante standaarden gevraagd. Hierbij gaat het alleen om aanbestedingen Rijk en uitvoeringsorganisaties: van het Ministerie van V&J, het Ministerie van BZK (twee keer), de Belastingdienst, het RIVM en het CIZ.
-	Het aandeel aanbestedingen waarbij om alle relevante standaarden is gevraagd, is ten opzichte van vorig jaar afgenomen van 18% naar 12%. Deze daling komt vooral voor rekening van de mede-overheden: bij geen enkele van die aanbestedingen werd om alle relevante standaarden gevraagd. Bij Rijk en uitvoeringsinstanties loopt de score slechts licht terug in vergelijking met vorig jaar, van 19% naar 17%.
+	Naast de 6 aanbestedingen (12%) waarbij om alle relevante standaarden is gevraagd, werd bij 36 aanbestedingen (69%) om een deel van de relevante open standaarden gevraagd. Dat is meer dan vorig jaar (55%).
+	Van de 36 aanbestedingen waarbij om *een deel van* de standaarden is gevraagd, werd bij 11 aanbestedingen (21% 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 19% van alle aanbestedingen om geen enkele van de relevante open standaarden werd gevraagd. Dat is overigens een betere score dan vorig jaar (27%). Het Rijk scoort hier duidelijk beter (11% tegen 29% vorig jaar) dan de mede-overheden (35% tegen 26% vorig jaar).
+	Sommige standaarden (vooral NEN-ISO/IEC 27001 en 27002, PDF, ODF en TLS, en daarnaast – in wat mindere mate – SAML, IPv6, DNSSEC en Digitoegankelijk) 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, PDF, Digitoegankelijk, TLS en StUF).
-	Twee standaarden werden relatief weinig gevraagd: DNSSEC en ODF zijn frequent als relevant aangemerkt, maar in slechts 21% respectievelijk 12% van die gevallen werd om de standaard gevraagd. Drie standaarden werden ongeveer 10 keer als relevant aangemerkt, maar zijn in het geheel niet uitgevraagd: DKIM, SPF en STARTTLS & DANE.
+	De mate waarin om standaarden werd gevraagd is voor sommige standaarden dit jaar toegenomen, en bij ongeveer evenveel standaarden juist afgenomen. Het valt op dat IPv6 steeds beter wordt uitgevraagd: het percentage steeg van 8% naar 42%.

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

- Ministerie van BZK (raamovereenkomst voor een SMS-gateway voor het versturen van SMS-berichten). De relevant geachte standaarden (NEN-ISO/IEC 27001 en 27002, IPv4 & IPv6, DNSSEC, TLS en – minder cruciaal – DKIM en SPF) zijn allemaal uitgevraagd, en er is een apart hoofdstuk over open standaarden opgenomen.
- Gemeente Tilburg (gezamenlijk klantregiesysteem voor de 'Tilburgse Toegang'). Voor deze aanbesteding is een groot aantal open standaarden relevant: TLS, Digikoppeling,

StUF, ODF, PDF, SAML, NEN-ISO/IEC 27001 en 27002, CMIS, HTTPS & HSTS en – minder cruciaal – Digitoegankelijk, XBRL, DKIM, SPF en STARTTLS & DANE. Hoewel niet al deze standaarden zijn uitgevraagd, oordeelt de expert positief vanwege de complexiteit van de casus en het feit dat veel aandacht bestaat aan standaarden is besteed, inclusief een verwijzing naar de 'pas-toe-of-leg-uit'-lijst.

- Centrum Indicatiestelling Zorg (dataverbindingen voor alle locaties van het CIZ en een managed IP VPN-dienst). Alle standaarden (IPv4 & IPv6 en NEN-ISO/IEC 27001 en 27002) zijn uitgevraagd. Verder wordt vermeld dat de netwerkcomponenten dienen te voldoen aan de thans geldende Europese normen en voorschriften m.b.t. veiligheid, elektrische installatie en overheidsreglementen en -bepalingen.
- Kamer van Koophandel (digitaal opgevoerde wijzigingsverzoeken ook digitaal kunnen ondertekenen en opsturen). Van de acht relevante geachte standaarden (AdES, PDF, NEN-ISO/IEC 27001 en 27002, HTTPS & HSTS, TLS, Digitoegankelijk en DNSSEC) wordt alleen de laatste niet gevraagd (deze is overigens ingeschat als niet-cruciaal).

'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 2016 (over 2017 zal door overheden pas verantwoording afgelegd worden in het jaarverslag dat in het voorjaar van 2018 verschijnt).

Voor 20 van de aanbestedingen in het 3e en 4e kwartaal van 2016 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 6 ministeries) geen sprake: nergens wordt een concrete afwijking van de 'pas toe of leg uit'-lijst genoemd.
-	In het jaarverslag over 2016 hebben 4 van de 11 ministeries een alinea over 'pas toe of leg uit' opgenomen (vorig jaar eveneens 4).
+	Het ministerie van BZK 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 haar ICT-producten en -diensten en bedrijfsvoering.

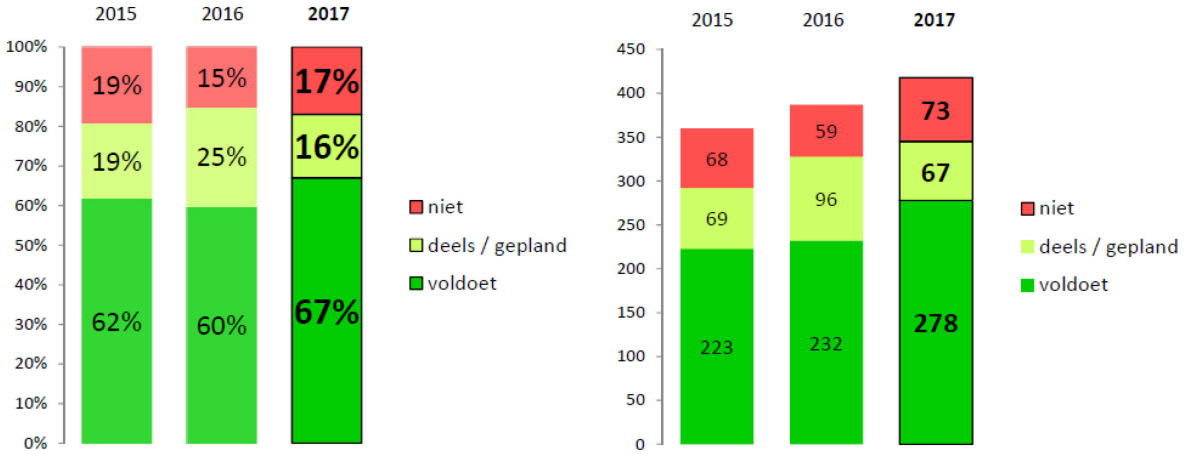
Toepassing van open standaarden via overheidsbrede voorzieningen (H4)

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 418 gevallen waarbij een open standaard voor een voorziening relevant was, voldoet in 67% de voorziening daar aan (vorig jaar 60%). Het aantal gevallen waarin de voorziening deels aan de standaard voldoet of daarvoor concrete plannen heeft is afgenomen: van 25% vorig jaar naar 16% dit jaar. Samen is dat 83%.



In absolute aantallen (zie rechter figuur hierboven) is te zien dat het aantal gevallen waarin aan open standaarden wordt voldaan is gestegen van 223 in 2015 tot 278 dit jaar.

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

+	Voor veel voorzieningen is een flink aantal open standaarden relevant: 12 standaarden gemiddeld per voorziening. Van de 40 standaarden op de lijst voor 'pas toe of leg uit' zijn er 27 relevant voor één of meer overheidsbrede voorzieningen.
+	Voor 9 van deze 27 open standaarden geldt dat 80% of meer van de voorzieningen aan die standaard – indien relevant – voldoet. Een belangrijk deel van deze standaarden staat al vijf jaar of langer op de lijst.
-	Zes standaarden scoren relatief laag: van de voorzieningen waarvoor deze relevant zijn voldoet er geen enkele aan CMIS, en voldoet 29% aan STARTTLS & DANE, 36% aan SKOS, 39% aan IPv4&IPv6, 40% aan AdES Baseline Profiles, en 46% aan HTTPS & HSTS. Drie van deze zes standaarden staan overigens minder dan een jaar op de lijst (AdES Baseline Profiles, STARTTLS & DANE en HTTPS & HSTS).
+	In de meeste gevallen voldoen de onderzochte voorzieningen aan (de meeste) daarvoor relevante open standaarden: aan 67% wordt voldaan, aan 16% voldoet de

[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.

	voorziening deels of dit is gepland en in 17% 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 12) 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.
+	Het kostte ook dit jaar de nodige moeite om de gevraagde informatie boven tafel te krijgen. Positieve uitzondering is Logius, beheerder van een groot aantal voorzieningen: jaarlijks publiceren zij hierover een helder overzicht. Daarnaast bleek een deel van de andere beheerders dit jaar sneller in staat de gevraagde informatie te leveren.

Enkele voorzieningen onderscheiden zich in positieve zin:

- Rijksoverheid.nl voldoet aan alle 16 relevante standaarden;
- DigiD voldoet aan alle 11 relevante standaarden;
- BRI (inkomen) voldoet aan alle 5 relevante standaarden;
- Samenwerkende Catalogi voldoet aan alle 2 relevante standaarden;
- PKI Overheid voldoet voldoet aan 9 van de 10 relevante standaarden en voor de resterende standaard is dat gepland;
- Overheid.nl voldoet aan 11 van de 14 relevante standaarden en voor de resterende 3 is dat gepland.

De eerste vijf voorzieningen werden ook in de vorige monitor vermeld omdat zij zich positief onderscheidden, de eerste drie hebben hun score vergeleken met vorig jaar nog verbeterd.

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. Voor 34 open standaarden van de lijst bleek dat wèl mogelijk[4], op één of meer van de volgende manieren:

- door met behulp van internet.nl na te gaan in hoeverre domeinnamen van overheden aan de standaard voldoen: DKIM, DNSSEC, IPv4/v6, SPF en TLS;
- door (met Google) na te gaan hoeveel ODF- en PDF-documenten[5] op websites van overheden te vinden zijn;
- door gegevens op te vragen bij de betreffende beheerorganisaties: dit leverde gegevens of meer globale informatie op voor de meeste andere open standaarden.

De gebruiksgegevens zijn verzameld in de zomer van 2017, met de volgende uitkomsten:

[4] Drie standaarden zijn niet onderzocht omdat die recent op de lijst geplaatst zijn: AdES Baseline Profiles, HTTPS & HSTS en STARTTLS & DANE. Voor drie standaarden is geen bruikbare informatie ontvangen: Aquo, E-Portfolio en STOSAG.

[5] Het is niet mogelijk om daarbij onderscheid te maken tussen PDF/A-1, PDF/A-2, PDF1.7 en andere versies.

+	Over 15 van de 37 onderzochte open standaarden zijn gegevens gevonden, die op zijn minst een indicatie geven van het gebruik van de betreffende standaard. Voor de andere open standaarden moest genoegen genomen worden met meer globale informatie, en voor enkele standaarden is geen informatie beschikbaar.
+	Bij 18 van de 37 onderzochte standaarden kan – al dan niet onderbouwd met harde gegevens – worden vastgesteld dat sprake is van toename van het gebruik. Voor 11 van deze standaarden is sprake van een duidelijk zichtbare stijging van het gebruik, die ook onderbouwd is met cijfers.
+	Van 6 van deze 18 standaarden geven de cijfers een duidelijk en direct beeld van het aandeel gebruikers. Voor elk van deze zes geldt: het gebruik neemt toe. Dit betreft de vijf standaarden waarvan het gebruik is gemeten met behulp van internet.nl (DKIM, DNSSEC, IPv6, SPF en TLS) en Digikoppeling.
+	Negen open standaarden worden op redelijk brede schaal door overheden gebruikt: StUF (100%, binnengemeentelijk echter minder), EMN_NL (alle gemeenten), Digikoppeling (76%), vier IV-standaarden namelijk DKIM (65%), DNSSEC (66%), SPF (76%) en TLS (93%), en twee onderwijsstandaarden: NL_LOM en OAI-PMH.
-	Voorzover wel cijfers beschikbaar zijn blijkt bij een aantal andere standaarden het gebruik over het algemeen nog aan de lage kant te zijn, bijvoorbeeld bij IPv6 en ODF. De implementatie van IPv6 verloopt nog steeds traag, afgezet tegen de ambities. De toepassing is dit jaar wel weer gestegen, tot 15%, bij de Rijksoverheid tot 33%.
-	Bij verschillende beheerorganisaties of anderszins bij open standaarden betrokken organisaties bestaat geen goed zicht op 'harde' gegevens over het gebruik; in zijn algemeenheid niet en in het bijzonder niet als het gaat om het gebruik door overheidsinstellingen. De intentie om dit gebruik in de toekomst wel in kaart te gaan brengen, is er vaak niet.
+	Enkele beheerorganisaties hebben de moeite genomen om apart voor deze monitor in kaart te brengen hoe het staat met het gebruik (door overheden). Voor enkele standaarden zijn initiatieven genomen voor een meer structurele vorm van monitoring (bij Digitoegankelijk, bij elk van de categorieën overheden voor de beide NEN-ISO-standaarden en de Compliancy-monitor van KING. Voor ODF zijn er ambities in die richting, maar financiering ontbreekt vooralsnog.
-	Bij de uitvraag van gebruiksgegevens blijken enkele andere beheerorganisaties weinig waarde te hechten aan inzicht in het gebruik en (dus) aan de monitor.
+	Bij enkele standaarden is sprake van (beginnend) beleid in de richting van gerichte sturing op de aanbodkant. StUF vormt hiervan een mooi voorbeeld, met o.a. een testplatform voor leveranciers en informatie over de compliance aan standaarden in de GEMMA Softwarecatalogus.

Algemene uitspraken over het feitelijk gebruik van open standaarden zijn buitengewoon moeilijk te doen, daarvoor is de verscheidenheid te groot:

- sommige standaarden betreffen een hele familie van deelstandaarden (Geo, StUF);
- bij de ene standaard is de doelgroep en dus het potentiële gebruik veel groter dan bij de andere; het vergelijken van percentages is daardoor niet altijd zinvol mogelijk;
- sommige standaarden betreffen een relatieve niche-toepassing, andere hebben juist een zeer brede toepassing (organisatorisch en/of functioneel);
- sommige standaarden zijn ook vanuit hun aard al verplichtend (voor EML_NL bijvoorbeeld is geen andere optie), bij andere is in principe sprake van 'keuzevrijheid' – afgezien van de verplichtingen uit Rijksinstructie e.d.

Halfjaarlijkse meting Internetveiligheidsstandaarden (Bijlage G)

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. Daarom worden de cijfers van de halfjaarlijkse meting opgenomen in de Monitor Open standaarden.

Het gaat om vijf internetveiligheidsstandaarden: DNSSEC (domeinnaambeveiliging), TLS (beveiligde verbinding), DKIM, SPF en DMARC[6] (alle drie anti-phishing). Voor een set van 544 domeinen is in 2017 met behulp van Internet.nl getoetst of zij voldoen aan de vijf internet-veiligheidsstandaarden. De cijfers zijn bij wijze van prognose ook lineair geëxtrapoleerd tot een percentage eind 2017.

+	TLS wordt het meest toegepast (92%), het aantal domeinen waarbij geconfigureerd is op de door het NCSC voorgeschreven veilige manier is lager maar is het afgelopen jaar wel verder gestegen van 26% naar 76%. De toepassing van DNSSEC en SPF is gegroeid tot respectievelijk 66% en 76% en de toepassing van DKIM groeide naar 65%.
+	Bij de eerste meting medio 2015 was de gemiddelde adoptiegraad van de vijf standaarden 35 %. Medio 2016 stond dit percentage op 49 % en medio 2017 op 71 %.
+	Alle onderzochte standaarden delen in deze verdere groei. En hetzelfde geldt voor de onderscheiden categorieën overheden: in elke sector is sprake van groei.
-	Als dit groeipercentage wordt geëxtrapoleerd naar het einde van 2017, dan blijkt dat zonder aanvullende acties geen van de overheidscategorieën de ambitie waarmaakt om deze standaarden eind 2017 te hebben geïmplementeerd.
-	Gemeenten komen in het kader van die extrapolatie met 83% nog het dichtst in de buurt van het streefbeeld en laten het afgelopen jaar ook de sterkste adoptiegroei zien. De andere overheidscategorieën komen bij die extrapolatie uit op ongeveer 70%.

De drie deel-onderzoeken naast elkaar

Elk van de drie deel-onderzoeken brengt een ander aspect van het proces van adoptie van open standaarden in beeld. Dergelijke gegevens kunnen niet zomaar naast elkaar gelegd worden. Tegelijkertijd komen in alle drie de deel-onderzoeken dezelfde open standaarden van de lijst voor ‘pas toe of leg uit’ voor. Wat levert het gecombineerde beeld uit deze drie bronnen op? In de onderstaande tabel is dat in beeld gebracht.

In de rechterkolom ‘Overall beeld’ zijn de volgende indicaties gebruikt:

●●	het beeld is bij alledrie de deelonderzoeken positief
●	verschillen tussen de deelonderzoeken: gemiddeld redelijk positief
●	verschillen tussen de deelonderzoeken: deels positief, deels matig
●●	het beeld is bij alledrie de deelonderzoeken matig
[?]	beperkte gegevens en/of verschillen tussen deelonderzoeken: geen duidelijk beeld

Voor vier standaarden is het overall beeld positief: SAML, TLS, Digikoppeling en EMN_NL. Bij drie van deze vier blijft overigens vooral de mate waarin om deze standaarden bij aanbestedingen wordt gevraagd achter. En voor acht standaarden is het beeld hoopgevend: HTTPS & HSTS, IPv4 & IPv6, NEN-ISO\IEC 27001:2005nl, 27002:2007nl,

[6] DMARC is op dit moment nog niet op de lijst geplaatst.

Digitoegankelijk, OWMS, de PDF-standaarden en StUF. De andere standaarden staan er op dit moment nog minder goed voor (oranje), of daarover is onvoldoende informatie (22x vraagteken).

Overzicht: bevindingen per standaard, uit de verschillende deel-onderzoeken

≥ 75 %
25-75 %
< 25 %

	Aanbestedingen	Voorzieningen	Gebruiksgegevens	Overall beeld	
indicator:	*# aanbestedingen gevraagd in % van # aanbestedingen waarbij OS relevant is*	*# voorzieningen dat voldoet + deels + gepland in % van # waarvoor de OS relevant is*	*# overheidsorganisaties dat de standaard gebruikt in % van alle overheidsorganisaties*		
bron:	*tabel 6 (H3)*	*o.b.v. tabel 9ab (H4)*	*tabel 10 (H5)*		
Internet & beveiliging:					
DKIM	0 %	86 %	65 % (Rijk 52 %)	●	
DNSSEC	21 %	89 %	66 % (Rijk 70 %)	●	
HTTPS & HSTS	*[niet gemeten]*	82 %	*[niet gemeten]*	●	
IPv6 en IPv4	42 %	48 %	15 % (Rijk 33 %)	●	
NEN-ISO\IEC 27001:2005nl	63 %	96 %		●	
NEN-ISO\IEC 27002:2007nl	62 %	96 %		●	
SAML	40 %	93 %	48 % (DigiD)	●●	
SPF	0 %	70 %	76 % (Rijk 60 %)	●	
STARTTLS en DANE	0 %	67 %	*[niet gemeten]*	●	
TLS	57 %	93 %	93 % (Rijk 83 %)	●●	
WPA2 Enterprise	(0 %)	(100 %)			[?]
Document & (web)content:					
AdEs Baseline Profiles	*[niet gemeten]*	60 %	*[niet gemeten]*		[?]
CMIS	(20 %)	(25 %)			[?]
Digitoegankelijk *)	58 %	68 %		●	
ODF 1.2	12 %	67 %		●	
OWMS	(100 %)	67 %		●	
PDF **)	50 %	100 %		●	
SKOS		73 %			[?]
E-facturatie &					
Sem. Model e-Factureren	(33 %)	(0 %)			[?]
SETU		(100 %)			[?]
WDO Datamodel					[?]
XBRL v2.1	(33 %)	(100 %)			[?]
Stelselstandaarden:					
Digikoppeling	33 %	84 %	76 % (Rijk 67 %)	●●	
Geo−standaarden	(0 %)	(100 %)			[?]
StUF	50 %	78 %		●	
Water & Bodem:					
Aquo Standaard	(0 %)				[?]
SIKB 0101					[?]
SIKB0102					[?]
Bouw:					
IFC					[?]
Visi					[?]
Juridische verwijzingen:					
BWB	(100 %)	(100 %)			[?]
ECLI					[?]
JCDR					[?]
Onderwijs & loopbaan:					
E−portfolio	(0 %)				[?]
NL LOM	(0 %)				[?]
OAI−PMH					[?]
Overig:					[?]
EMN_NL			alle gemeenten	●●	
STOSAG	(0 %)				[?]

Aanbestedingen en Voorzieningen: tussen haakjes indien aantal ≤ 5.
Gebruiksgegevens: grijs indien geen bruikbare gegevens ontvangen.

2. Inleiding en beleidscontext

2.1. Waarom open standaarden?

Het daadwerkelijk gebruik van open standaarden is voor goede ICT van de overheid zó belangrijk, dat sinds 2009 het Forum Standaardisatie een lijst beheert van open standaarden, die overheidsbreed verplicht toegepast moeten worden: de open standaarden van de 'pas toe of leg uit'-lijst. Het gebruik van deze standaarden is nodig om

- het digitale verkeer binnen en tussen overheden en tussen overheden en burgers en bedrijven goed te laten doorstromen (interoperabiliteit),
- grip te krijgen op de kosten voor ICT (door leveranciersafhankelijkheid terug te dringen)
- en om te zorgen voor veiligheid en betrouwbaarheid in het digitale verkeer met en tussen overheidsorganisaties. Niet in de laatste plaats 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[7]. 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 A voor een stroomschema.

[7] "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"*.

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[8] 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 1 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

[8] *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).

bovendien valt binnen het organisatorische werkingsgebied van de betreffende standaard.[9] 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[10] 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.*

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.*

2.4. Monitor Open standaarden

Het Forum Standaardisatie beheert de lijst met verplichte open standaarden die gelden voor de (semi-) publieke sector en stimuleert de adoptie van deze standaarden. Op deze wijze bevordert het Forum de interoperabiliteit van de overheid.

Het Bureau Forum Standaardisatie heeft ICTU gevraagd om jaarlijks, gebruikmakend van verschillende bronnen, een integrale beleidsgerichte rapportage te verzorgen. Die moet

[9] 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.
[10] 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.

inzicht geven in de vorderingen van het open standaarden-beleid en de voortgang in de adoptie van de standaarden op de lijst voor 'pas toe of leg uit'.

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 2016/2017,
- onderzoek toepassing open standaarden bij overheidsbrede voorzieningen,
- onderzoek gebruiksgegevens van een aantal open standaarden.

Onderzoek feitelijke aanbestedingen in 2016/2017

Dit jaar zijn aanbestedingen onderzocht van de rijksoverheid (en uitvoerings-organisaties) en van mede-overheden uit de periode juli 2016-juni 2017. 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 gebruiksgegevens van een aantal open standaarden

Om na te gaan in welke mate open standaarden daadwerkelijk worden toegepast zijn gebruiks-gegevens verzameld voor 37 open standaarden. Deels door met behulp van een webtool na te gaan in hoeverre domeinnamen van overheden aan de standaard voldoen. Deels door (met Google) na te gaan hoeveel ODF- en PDF-documenten op websites van overheden te vinden zijn. En deels door gebruiks- of aansluit-gegevens op te vragen bij de betreffende beheerorganisaties.

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 2017 is nu voor het zesde 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 5.1. De resultaten komen aan bod in paragrafen 5.2 (‘pas toe’ bij aanbestedingen), 5.3 (mate van ‘pas toe’ per open standaard), 5.4 (‘leg uit’ in jaarverslagen) en 5.5 (mate waarin open standaarden relevant waren bij de onderzochte aanbestedingen). Met ingang van 2014 wordt een deel van de aanbestedingen bij wijze van second opinion door een tweede expert beoordeeld. In paragraaf 5.6 gaan wij in op de meerwaarde en de algemene bevindingen daarvan.

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 2016 en Q1 en Q2 2017). Dit jaar is de rol van eerste en tweede expert omgewisseld ten opzichte van vorig jaar en is de beoordeling van aanbestedingen uitgevoerd door Wouter van den Berg MSc en Linda Oosterheert MSc (beiden TNO), met de eerdergenoemde mr.dr. Mathieu Paapst en mr. Arend-Jan Wiersma (beiden ICTRecht) als ‘tegen-beoordelaars’ in het kader van de second opinion.

Onderzocht zijn aanbestedingen die op tenderned.nl zijn gepubliceerd. Het betreft daardoor voornamelijk Europese aanbestedingen (drempelwaarden voor Europese aanbestedingen: voor de rijksoverheid > € 135.000 en voor decentrale overheden > € 209.000; deze drempelwaarden gelden voor de periode 2016 - 2017). 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.

Vorig jaar was het totale aantal beoordeelde aanbestedingen wat lager, met name het aantal aanbestedingen van de Rijksoverheid bleef achter bij eerdere jaren. Verder viel vorig jaar op dat er meer dan voorheen ook raamovereenkomsten werden aanbesteed.

Dit jaar is het aantal beoordeelde aanbestedingen van de Rijksoverheid weer 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 om de volgende casuïstiek uit de aanbestedingspraktijk:

- een aanbesteding waarbij geen concreet product of concrete dienst gevraagd is maar een 'open' vraag naar een voorstel voor een innovatieve toepassing;
- een aanbesteding waarbij sprake is van vernieuwing en (door)ontwikkeling van bestaande software waarbij onduidelijk is in hoeverre open standaarden relevant zijn;
- een aanbesteding betreft een soort prijsvraag, gericht op onderzoek en ontwikkeling;
- enkele aanbestedingen blijken in een later stadium alsnog te zijn ingetrokken;
- ook dit jaar blijkt in een enkel geval sprake van een raamovereenkomst die onvoldoende gedetailleerd uitgewerkt is om een oordeel te kunnen geven over de relevantie van open standaarden.

De beoordeling heeft plaatsgevonden in twee tranches: aanbestedingen uit juli tot en met december 2016 en uit januari tot en met juni 2017. Uiteindelijk zijn 52 aanbestedingen beoordeeld: 35 van het Rijk (departementen en uitvoeringsorganisaties, agentschappen, ZBO's) en een steekproef van 17 aanbestedingen van mede-overheden. Het aandeel aanbestedingen van de Rijksoverheid (67%) is beduidend hoger dan in de achterliggende jaren (in 2016 48%, in 2015 52% en 35% in 2014 en 33% in 2013). De 52 beoordeelde aanbestedingen vormen een goede afspiegeling van de overheids-ICT-aanbestedingen, voor zover die binnen de hiervoor 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-) mantel-overeenkomsten, die voor langere periode van kracht zijn en/of verlengd worden (meestal een aantal jaren). Aanbestedingen binnen de mantel-overeenkomst worden direct bij de mantel-partijen 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 waar geen sprake is van enige 'massa' van (ICT-) aanbestedingen 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).

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:

- monitoring en analyse van trends op sociale media, in combinatie met een mogelijkheid om vervolgens te communiceren met de klant (uitvoeringsorganisatie / Rijk);
- technisch beheer, hosting en doorontwikkeling van een landelijk digitaal dossier waarin zorgverleners gegevens vastleggen (agentschap / Rijk);
- procesautomatiseringssystemen op rioolwaterzuiveringsinstallaties met inbegrip van alle hardware en software (waterschap);
- een (nieuw) handhaafsysteem waarmee op basis van kentekenregistratie controle plaatsvindt op het recht om met het voertuig de binnenstad te betreden (gemeente);
- levering, onderhoud en beheer van een centrale voorziening voor langdurige opslag van digitaal (bewijs-)materiaal (politie);
- levering van een collateral management system (CMS) waar financiele instanties zoals banken maar ook het betreffende agentschap zelf de financiele risisco's managen (agentschap / Rijk);
- digitalisering aanvraagprocessen, met name intelligente e-formulieren voor het doen van online aanvragen voor bijzondere bijstand en levensonderhoud en de afhandeling daarvan (gemeente);
- dataverbindingen voor alle locaties van de opdrachtgever, met daarbij een managed IP VPN dienst (ZBO / Rijk);
- integrale backoffice software in combinatie met de levering van toegang- en vulgraad-systemen die de bedrijfsprocessen van de regionale grondstoffen- en afvalstoffendienst ondersteunen (gemeenten);
- leveren, implementeren en onderhouden van brug-management-systeem (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. Dit jaar is –in tegenstelling tot in eerdere jaren- deze kwestie van informatie uit de Nota van Inlichtingen in het geheel niet aan de orde geweest bij het bespreken van de beoordelingen in het kader van de second opinion.

Daarnaast is onderzocht op welke wijze de verantwoording ('leg uit') over 2016 heeft plaatsgevonden[11]*.*

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

[11] Voor twee sets van beoordeelde aanbestedingen is nagegaan in hoeverre 'leg uit' plaatsgevonden heeft: de set aanbestedingen uit Q3 en Q4 2016 die in deze Monitor 2017 zijn beoordeeld èn de set aanbestedingen uit Q1 en Q2 2016 die vorig jaar zijn beoordeeld (in het kader van de Monitor 2016).

argumenten, die mogelijk een rol hebben gespeeld bij de aanbestedingen, vallen buiten de scope van dit onderzoek.

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 2016/2017

In totaal had in de beoordeelde 52 aanbestedingen om 317 open standaarden gevraagd moeten worden, feitelijk werd er echter 142 keer om een open standaard gevraagd - dat is dus 45% daarvan (zie tabel 1), vergelijkbaar met het percentages van de afgelopen jaren (2014/2015: 43% en 2015/2016: 44%). Over de jaren 2012 en 2013 lag dit percentage beduidend lager, op respectievelijk 30% en 25%.

Bij 6 van de 52 aanbestedingen (12%; vorig jaar 18%) werd om alle relevante open standaarden gevraagd, dat is 'pas toe' in strikte zin: 3 aanbestedingen door een ministerie, 1 door een uitvoeringsorganisatie, 1 door een agentschap en 1 door een ZBO.

Daarnaast werd bij 36 aanbestedingen (69%; vorig jaar 55%) gevraagd om een deel van de voor die aanbesteding relevante standaarden.

Bij de resterende 10 aanbestedingen (19%; vorig jaar 27%) - waarbij één of meer open standaarden relevant waren - werd om geen enkele open standaard gevraagd.

De aanbestedingen zijn nader beoordeeld op de mate waarin zij voldoen aan het open standaardenbeleid: zijn alle relevante standaarden gevraagd, is om een deel daarvan gevraagd of is er in het geheel niet om relevante open standaarden gevraagd. Deze driedeling is in twee opzichten nog verder genuanceerd.

Enerzijds kan nog een onderscheid worden gemaakt tussen de voor een bepaalde aanbesteding cruciale open standaarden en eventuele andere relevante open standaarden. Anderzijds kan bij de aanbesteding ook op andere, bijvoorbeeld meer algemene wijze aandacht besteed zijn aan open standaarden. Dit heeft geleid tot zeven categorieën voor de mate waarin aanbestedingen voldoen aan het open standaardenbeleid:

- er is om alle relevante open standaarden gevraagd (12%),
- 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 (21%),
    - er is om open standaarden gevraagd, maar om minimaal één cruciale niet (48%),
- er zijn geen relevante open standaarden gevraagd, onder te verdelen in:
    - er wordt alleen verwezen naar architectuur-kaders (0%),
    - er wordt in algemene zin aandacht besteed aan open standaardenbeleid (0%),
    - er is geen aandacht voor open standaardenbeleid (15%),
    - de aanbesteding is strijdig met het open standaardenbeleid (4%)[12].

Vorig jaar waren de verschillen in scores in tabel 1 tussen Rijk en decentrale overheden heel klein, en terug te voeren tot de score van een enkele aanbesteding. Dit jaar zijn de verschillen beduidend groter. Het aandeel aanbestedingen waarbij om alle relevante standaarden werd gevraagd ligt bij het Rijk op 17% (vorig jaar nog 19%). Bij de decentrale overheden is bij geen enkele onderzochte aanbesteding om alle relevante standaarden gevraagd (vorig jaar: 17%). Ook bij de twee andere hoofdcategorieën zijn de verschillen groot in vergelijking met vorig jaar: bij 71% van de Rijks-aanbestedingen tegen 65% voor de decantrale overheden is om een deel van de relevante open standaarden gevraagd; en bij 11% van de Rijks-aanbestedingen tegen 35% voor de decantrale overheden werd om geen enkele relevante standaard gevraagd. Met name bij deze laatste categorie is het verschil met vorig jaar opmerkelijk: het percentage Rijks-aanbestedingen waarbij om geen enkele open standaard werd gevraagd is teruggelopen van 29% vorig jaar naar 11% dit jaar, het percentage voor de decentrale overheden is juist opgelopen, van 26% naar 35%.

[12] Dit jaar krijgen twee aanbestedingen het predicaat 'strijdig met open standaarden beleid', net als twee jaar geleden. Vorig jaar was volgens de experts geen enkele aanbesteding 'strijdig met open standaarden beleid', met daarbij de kanttekening dat toen bij enkele raamovereenkomsten een kwalificatie 'strijdig met open standaarden beleid' dichtbij was. Deze aanbestedingen zijn toen niet in de beoordeling meegenomen.

Tabel 1: 'Pas toe' en 'leg uit' bij feitelijke aanbestedingen 2016/2017

(Bron: onderzoek feitelijke aanbestedingen juli 2016 t/m juni 2017, uitgevoerd zomer 2017)

	Ministeries + Uitvoerings-organisaties		Gemeenten + Provincies + Waterschappen		**Totaal 2016 / 2017**		Totaal 2015 / 2016	
	totaal	in %	totaal	in %	**totaal**	in %	totaal	in %
aanbestedingen waarbij OS relevant	*35*	*100 %*	*17*	*100 %*	***52***	*100 %*	*44*	*100 %*
alle relevante OSn gevraagd	**6**	**17 %**	**0**	**0 %**	**6**	**12 %**	**8**	**18 %**
deel van relevante OSn gevraagd	**25**	**71 %**	**11**	**65 %**	**36**	**69 %**	**24**	**55 %**
* cruciale OSn gevraagd	8	(23 %)	3	(18 %)	**11**	(21 %)	4	(9 %)
* OSn gevraagd, maar cruciale niet	17	(49 %)	8	(47 %)	**25**	(48 %)	20	(45 %)
geen relevante OSn gevraagd	**4**	**11 %**	**6**	**35 %**	**10**	**19 %**	**12**	**27 %**
* alleen architectuur-kaders	0	(0 %)	0	(0 %)	**0**	(0 %)	1	(2 %)
* algemene aandacht aan OSn-beleid	0	(0 %)	0	(0 %)	**0**	(0 %)	1	(2 %)
* geen aandacht voor OSn-beleid	4	(11 %)	4	(24 %)	**8**	(15 %)	10	(23 %)
* strijdig met OSn-beleid	0	(0 %)	2	(12 %)	**2**	(4 %)	0	(0 %)
totaal aantal relevante OSn	208	100 %	109	100 %	**317**	100 %	257	100 %
* aantal cruciale relevante OSn	138	66 %	60	55 %	**198**	62 %	202	79 %
totaal aantal gevraagde relevante OSn	112	54 %	30	28 %	**142**	45 %	113	44 %
* niet alle OSn gevraagd => Leg Uit vereist	29	(83 %)	17	(100 %)	**46**	(88 %)	36	(82 %)
cruciale OSn wel gevraagd	8		3		**11**		4	
Leg Uit in jaarverslag beslist vereist	21		14		**35**		32	
- idem, maar beperkt tot Q3+Q4 2016 [13]	*15*	*(100 %)*	*5*	*(100 %)*	***20***	*(100 %)*	*15*	*(100 %)*
- concrete verantwoording in jaarverslag	*0*	*(0 %)*	*0*	*(0 %)*	***0***	*(0 %)*	*0*	*(0 %)*
- beperkte verantwoording in jaarverslag	*3*	*(20 %)*	*0*	*(0 %)*	***3***	*(15 %)*	*3*	*(20 %)*
- geen Leg Uit in jaarverslag	*12*	*(80 %)*	*5*	*(100 %)*	***17***	*(85 %)*	*12*	*(80 %)*
Totaal	35	100 %	17	100 %	**52**	100 %	44	100 %

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

Uit het horizontaal met groen gemarkeerde blok in de tabel valt op dat iets meer dan 3 op de 5 relevante standaarden door de beoordelaars als cruciaal worden aangemerkt. Dat is het geval als de kern van de applicatie raakvlakken heeft met de betreffende standaard. Vorig jaar lag deze score anders, toen was bijna 4 op de 5 relevante standaarden cruciaal. Met betrekking tot dit verschil het volgende:

- het aantal standaarden dat per aanbesteding relevant wordt geacht, ligt dit jaar slechts fractioneel hoger dan vorig jaar dus dat is geen factor van belang;

[13] Controle op de toepassing van 'leg uit' heeft alleen kunnen plaatsvinden over de aanbestedingen uit 2016, waarover verantwoording had moeten worden afgelegd in het Jaarverslag 2016.

- het verschil met vorig jaar manifesteert zich vooral bij de beoordeling van de aanbestedingen van de decentrale overheden: 55% cruciaal (vorig jaar: 81%).

Tot slot is opvallend aan tabel 1 dat het aandeel bevraagde standaarden voor het Rijk dit jaar bijna twee keer zo hoog ligt als bij de overige overheden: 54% tegenover 28%. Vorig jaar scoorden Rijk en andere overheden gelijk, met 44%. Bij Rijk is derhalve sprake van een duidelijke verbetering terwijl de score voor de andere overheden flink terugvalt.

Vorig jaar bleek dat – na een jaar met een duidelijke verbetering van de scores in 2015 – er sprake was van een consolidering van die ontwikkeling, met enige nuancering. Op basis van de beoordelingen van de experts dit jaar kan worden vastgesteld dat in vergelijking met vorig jaar sprake is van een lichte verdere verbetering van 'pas toe' bij de onderzochte aanbestedingen, met daarbij ook weer enige nuancering omdat het beeld niet over de volle breedte eenzelfde kant op wijst. Op basis van tabel 1 kan het volgende worden geconcludeerd:

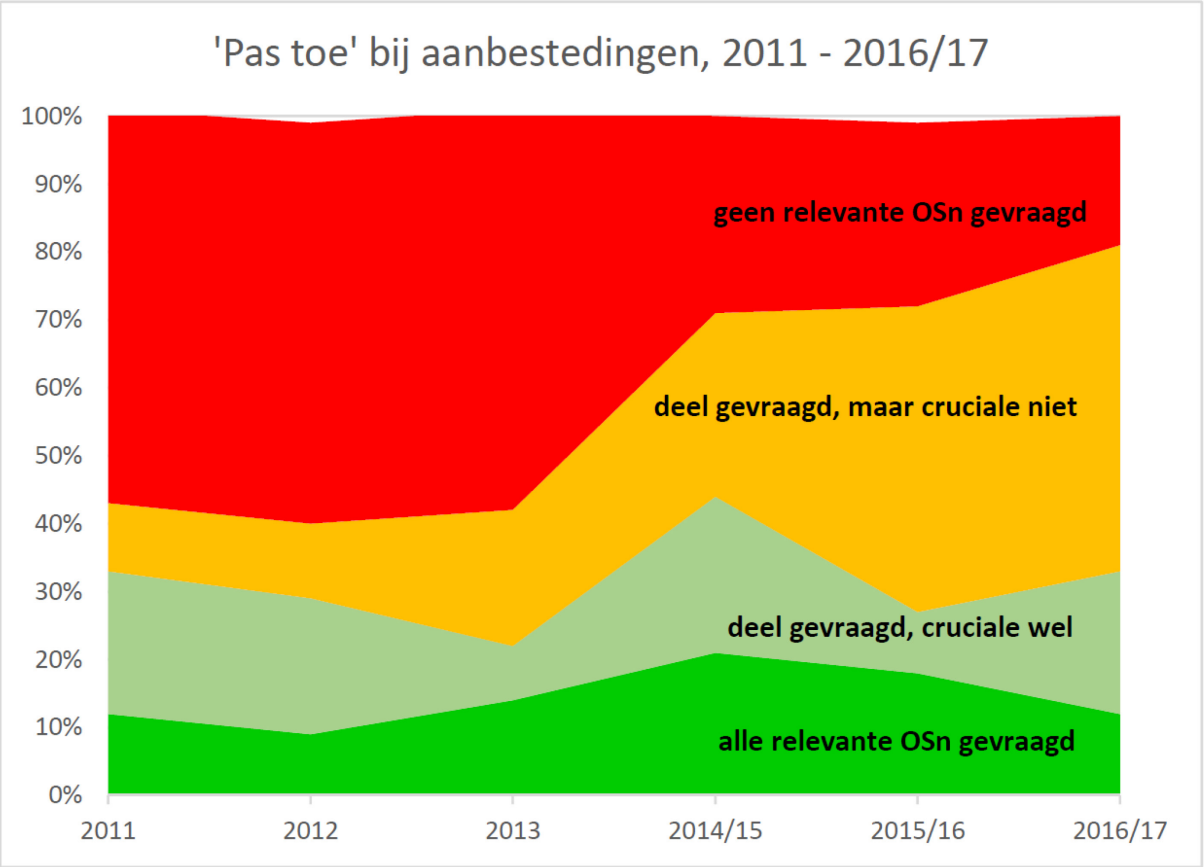
- Het aantal aanbestedingen waarbij om alle relevante standaarden is gevraagd is iets afgenomen, van 18% naar 12%; ook vorig jaar was er al een geringe afname (van 21% naar 18%). De daling dit jaar is vrijwel geheel toe te schrijven aan het feit dat in de categorie andere overheden bij geen enkele aanbesteding naar alle relevant geachte standaarden is gevraagd.
- Voor het aantal aanbestedingen waarbij om geen enkele standaard is gevraagd is sprake van een duidelijke verbetering: een daling 27% naar 19%. Eerder is al opgemerkt dat deze verbetering volledig wordt gerealiseerd bij het Rijk. De verbetering die zich daar voordoet weegt ruimschoots op tegen het minder gunstige beeld dit jaar bij de andere overheden. Daar is het aandeel 'geen aandacht voor open standaarden beleid' of 'strijdig met het open standaarden beleid' verdubbeld en opgelopen van 17% vorig jaar tot 35% dit jaar.
- De middencategorie – een deel van de relevante standaarden gevraagd – laat dan ook een oplopend percentage zien: een stijging van 55% naar 69%. De verschuiving binnen deze middencategorie is bovendien gunstig:
  - wel gevraagd om alle cruciale open standaarden maar om één of meer andere niet: van 9% vorig jaar naar 21% nu en daarmee bijna weer terug op het niveau van twee jaar geleden (toen 23%);
  - gevraagd om open standaarden, maar om minimaal één cruciale niet: van 45% vorig jaar naar 48% dit jaar.

In Figuur 2 is deze verschuiving in een breder tijdsperspectief geplaatst, vanaf de monitor over 2011.

Na de consolidatie die vorig jaar zichtbaar werd, blijkt nu weer sprake van enige verdere verbeteringen. Dat geldt nog niet voor 'alle standaarden gevraagd' (donkergroen): dat loopt net als vorig jaar enigszins terug. Het percentage aanbestedingen waarbij om alle relevante standaarden is gevraagd, heeft zich de afgelopen jaren als volgt ontwikkeld: van 9% (2012) naar 14% (2013) naar 21% (2014/2015), 18% (2016) tot 12% dit jaar.

Het aantal aanbestedingen waarvoor geen enkele standaard is gevraagd (rood) is gedaald in vergelijking met vorig jaar. Het daalde van 27% vorig jaar naar 19% 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%.

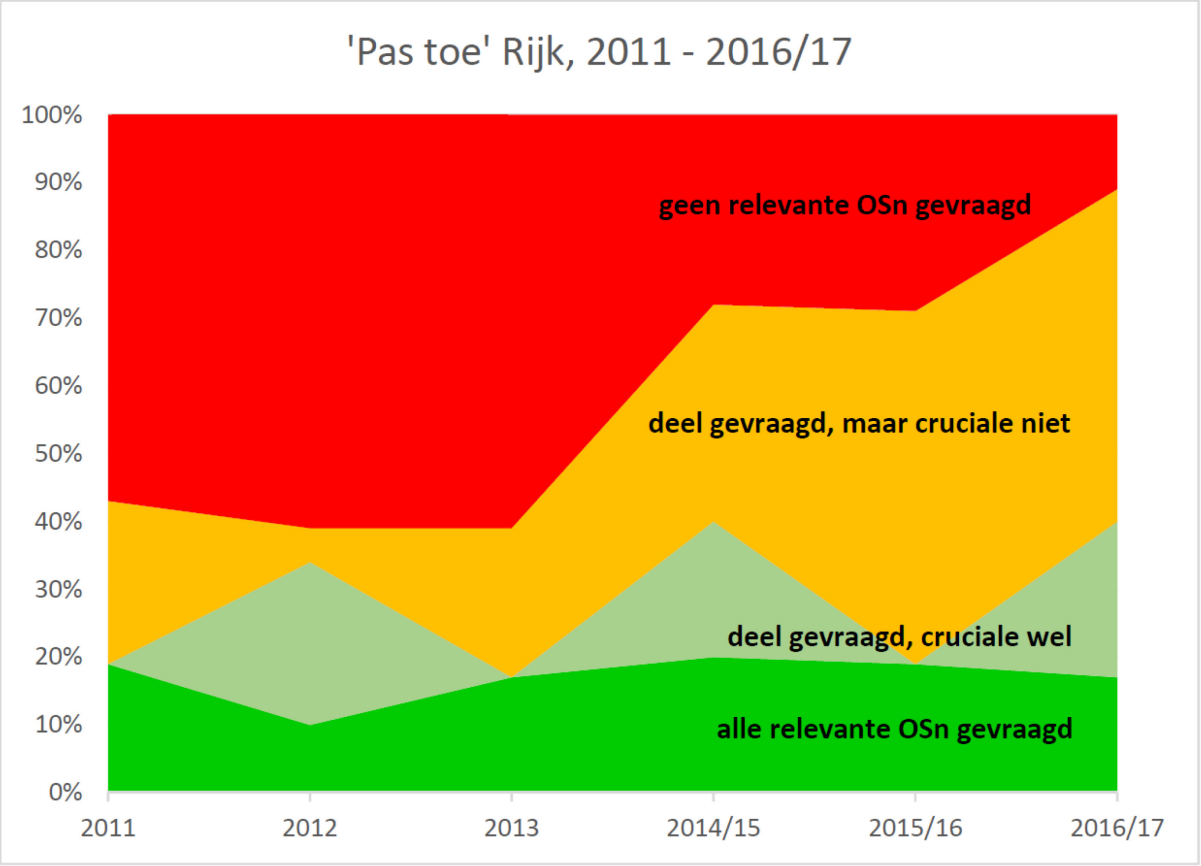
Figuur 2: 'Pas toe' bij feitelijke aanbestedingen 2011 - 2016/2017



In het midden-gedeelte van de figuur is de verschuiving waar te nemen zoals eerder al is verwoord: het gele gedeelte (deels gevraagd, maar tenminste één cruciale niet) is iets groter geworden maar met name het lichtgroene deel (deels gevraagd, maar alle cruciale wèl) is duidelijk in omvang toegenomen. Als het lichtgroene en het groene deel worden samengenomen – alle cruciale open standaarden zijn gevraagd – dan gaat de score dit jaar (33%) weer de goede kant op, in de richting van de piek tot nu toe in de monitor 2014/2015 (44%) na een terugval vorig jaar naar 27%.

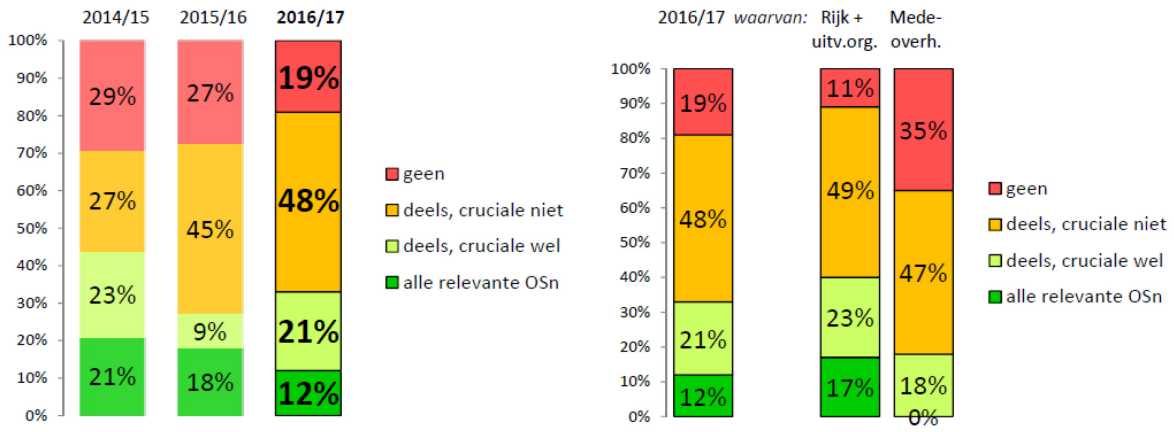
Eerder is al opgemerkt dat de score dit jaar voor de andere overheden duidelijk van invloed is op het totaalbeeld. Om in de terminologie te blijven van de kleuren uit bovenstaande tabel: het groene deel is bij de andere overheden helemaal verdwenen, het lichtgroene deel is gelijk gebleven en zowel het gele deel als (met name) het rode deel zijn groter geworden. Dat betekent dat het beeld voor de Rijksoverheid (zie Figuur 3) nog iets gunstiger is dan het landelijke totaalbeeld.

Figuur 3: 'Pas toe' bij aanbestedingen Rijk 2011 - 2016/2017



In onderstaande figuur zijn (rechts) de percentages voor 2016/2017 uitgesplitst naar Rijk en mede-overheden. Duidelijk is te zien dat Rijk en uitvoeringsorganisaties het in 2016/2017 een stuk beter deden dan de mede-overheden: slechts bij 11% van de Rijks-aanbestedingen werd om geen enkele standaard gevraagd (mede-overheden: 35%), bij 17% werd om alle relevante standaarden gevraagd (mede-overheden: 0%) en daarnaast bij nog 23% om tenminste alle cruciale standaarden (mede-overheden: 18%).

Figuur 4: 'Pas toe' bij aanbestedingen: uitsplitsing Rijk vs. mede-overheden 2016/2017



3.3. Overzicht van beoordeelde aanbestedingen Rijk en uitvoeringsorganisaties

De 35 aanbestedingen van Rijk en uitvoeringsorganisaties die dit jaar zijn beoordeeld zijn in Tabel 5 opgesomd, met een korte omschrijving van het onderwerp van de aanbesteding, met de open standaarden die de beoordelaars relavant achten (uitgesplitst in cruciale en niet-cruciale) en met de uiteindelijke beoordeling. Hiervoor is de volgende indeling gehanteerd (conform Tabel 1):

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 gevraagd is zijn groen gemarkeerd, relevante standaarden waarom niet is gevraagd geel.

Tabel 5: Overzicht van beoordeelde aanbestedingen Rijk en uitvoeringsorganisaties

aanbesteder	inhoud aanbesteding	standaarden[14] cruciaal	standaarden niet-cruciaal	oordeel
Belasting-dienst	Onderhoud en support van programmatuur voor de documentenstromen waarmee o.a. de opmaak en structuur van de documenten beheerst wordt.	ISO 27001/27002 PDF 1.7/PDF A1	-	A
CIZ	Dataverbindingen voor alle locaties van CIZ. Er wordt ook gevraagd om een managed IP VPN dienst.	IPv6 en IPv4 ISO 27001/27002	-	A
Min. BZK	De housing en hosting van de ICT-infrastructuur van KOOP. Hieronder vallen de installatie, servercapaciteit, het volledige beheer, onderhoud, certificaten ontwikkeling en alle aanvullende dienstverlening van de (dedicated) managed hosting (en housing) services.	BWB DNSSEC IPv6 en IPv4 ISO 27001/27002 OWMS TLS	SMeF 2.0	A
Min. BZK	Het leveren, implementeren en onderhouden van oplossingen voor het inrichten van de generieke kopieer-, print- en scanvoorzieningen binnen ICT-werkomgevingen en het realiseren van rijksbreed printen en scannen.	IPv4 en IPv6 ISO 27001/27002 ODF PDF TLS	-	A
Min. V&J	Het leveren van standaardprogrammatuur, onderhoud en support plus dienstverlening in de vorm van adviezen en ondersteuning, ten behoeve van de rechtspraak.	ODF	ISO 27001/27002	A
RIVM	De behoefte om voor 2 jaar oude / nieuwe, bestaande / komende websites en sociale media kanalen, inclusief content middels een goede (bestaande) archiverings-methodiek extern te beleggen (conform de archiefwet).	ISO 27001/27002	-	A
Belasting-dienst	Er is gekozen voor de inzet van nieuwe software op het mainframe van de dienst (Business Proces Manager (BPM) van IBM). Dat betekent de introductie van een Linux	ISO 27001/27002	IPv4 en IPv6	B

[14] 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[14] cruciaal	standaarden niet-cruciaal	oordeel
	operating system voor de IBM System z mainframe(s) van de Belastingsdienst.			
Belasting-dienst	Het leveren van een SaaS-oplossing ter ondersteuning van de in-, door- en uitstroom van medewerkers van de Belastingdienst. Het gaat om functionaliteiten voor Werving & Selectie, Loopbaanbegeleiding en Assessment.	ISO 27001/27002 SAML TLS	Digitoegankelijk E-portfolio ODF PDF	B
KvK	Het hosten van een nieuwe dienst waarbij de ondernemer het op KvK.nl digitaal opgevoerde wijzigingsverzoek ook digitaal kan ondertekenen en opsturen, zonder de noodzaak (nu) tot afdrukken en versturen per post.	Digitoegankelijk ISO 27001/27002 PDF	DNSSEC TLS	B
KvK	Een nieuwe applicatie voor drie afdelingen die gericht zijn op interne dienstverlening. Elke afdeling gebruikt nu een ander systeem, de nieuwe applicatie moet zorgen voor een 'single point of contact' voor de KvK medewerkers.	Digitoegankelijk ISO 27001/27002 TLS	ODF PDF SAML	B
Min. BZK	Het verwerven van apparatuur voor vaste ICT-Werkplekken. Onderdeel van de aanbesteding is het realiseren van een uitgebreide webshop.	ISO 27001/27002	IPv4 en IPv6 SAML TLS	B
Min. BZK	Als onderdeel van de dienstverlening verzorgt FMH het vervoer van personen voor BZK, VenJ, OCW, EZ, en andere organisaties behorend tot de Rijksoverheid. Er is behoefte aan een nieuw planningssysteem voor personenvervoer vanwege het aflopen van de huidige overeenkomst.	ISO 27001/27002 SAML TLS	ODF PDF	B
Min. BZK	Het leveren van een SMS-Gateway. Hierbij gaat het om het afhandelen van het versturen van SMS berichten, waarbij de opdracht voor het versturen via een applicatie of een webservice kan worden verstuurd.	DNSSEC IPv4 en IPv6 ISO 27001/27002 TLS	DKIM SPF	B
OM	Kantoorautomatisering-diensten.	ISO 27001/27002	TLS	B
Belasting-dienst	Een tool voor monitoring en analyse van social media en een tool om met de klanten te kunnen communiceren waarbij alle door de Belastingdienst gebruikte accounts geïntegreerd zijn zodat dienstverlening platform-onafhankelijk centraal plaats kan vinden.	ISO 27001/27002 ODF PDF TLS	DKIM SAML SPF STARTTLS & DANE	C
Belasting-dienst	Een Documentgenerator, waarmee gebruikers gemakkelijk documenten kunnen samenstellen, gebruik makend van modellen, teksten en gegevens, zonder dat deze gegevens moeten worden overgetypt uit administraties.	Digitoegankelijk ODF PDF TLS	CMIS ISO 27001/27002 SAML	C
Belasting-dienst	Een Learning Management Systeem (LMS) gekoppeld aan een Elektronische Leeromgeving (Moodle) ten behoeve van de ministeries van Infrastructuur en Milieu, Buitenlandse Zaken en Economische Zaken. De oplossing moet de uitvoering van activiteiten rondom Leren en Ontwikkelen ondersteunen.	E-Portfolio HTTPS & HSTS ISO 27001/27002 SAML TLS	Digitoegankelijk DKIM NL-LOM ODF PDF SPF STARTTLS & DANE	C
CIZ	Het technisch onderhoud van de applicatie voor de ondersteuning van het primaire proces, Portero, en het technisch onderhoud van de datawarehouse (DWH) omgeving.	Digikoppeling 2.0 ISO 27001/27002 ODF PDF A1 TLS	CMIS Digitoegankelijk SMeF 2.0 StUF XBRL	C
CIZ	Het leveren van diensten voor vaste en mobiele telefonie. Onderdeel hiervan is het Skype for Business platform dat bij de opdrachtnemer geïmplementeerd dient te worden.	IPv4 en IPv6 ISO 27001/27002 TLS	ODF PDF	C
DJI	Het leveren van (onderhouds-)diensten en componenten voor de huidige Telehoren –dienst (gebruikt bij het vreemdelingenrecht en het strafrecht).	ISO 27001/27002	IPv4 en IPv6 TLS	C
ICTU	Hosten, beheer, onderhoud en doorontwikkeling van een kennisbank: een webportaal, gericht op kennisuitwisseling	Digitoegankelijk DNSSEC ISO 27001/27002	IPv4 en IPv6 ODF	C

aanbesteder	inhoud aanbesteding	standaarden[14] cruciaal	standaarden niet-cruciaal	oordeel
	binnen BZK, met andere actoren in het openbaar bestuur en met wetenschappers, onderzoekers en studenten.	TLS	PDF	
Min. BZK	Een Collateral Management Systeem (CMS): een software systeem waarmee het Agentschap van de Generale Thesaurie haar financiële risico's kan managen. Het beoogde CMS moet zo'n 2500 transacties ondersteunen, waarbij gedacht moet worden aan interest rate swaps, cross currency swaps en FX swaps.	ISO 27001/27002 ODF	DKIM DNSSEC SPF STARTTLS & DANE TLS	C
Min. OCW	Transitie, applicatiebeheer en appl;icatieontwikkeling van het huidige Document Management Portfolio.	ISO 27001/27002 ODF PDF TLS	DNSSEC	C
Min. V&J	De aanschaf, implementatie en het onderhoud van twee AFIS-en (Automated Fingerprint Identification Systems) ten behoeve van een nieuwe biometrievoorziening voor de Vreemdelingenketen (DGVz).	ISO 27001/27002 TLS	StUF	C
Min. VWS	Managed hosting en storage services waarbij de installatie, migratie servercapaciteit (hardware en virtueel), het volledige beheer (server, netwerk, opslag, backup), onderhoud, certificaten, ontwikkeling, alle aanvullende dienstverlening, storage en retransitie tot de opdracht behoort.	Digikoppeling DKIM DNSSEC HTTPS IPv4 en IPv6 ISO 27001/27002 SPF STARTTLS & DANE	-	C
Politie	Levering, onderhoud en beheer van een centrale voorziening voor langdurige opslag van digitaal (bewijs-) materiaal.	DNSSEC IPv4 en IPv6 ISO 27001/27002 SAML TLS	-	C
Politie	Het afhandelen van alle mobiele spraak/data en data-only verkeer via vaste en mobiele telefonie, levering van klantspecifieke SIM-kaarten en aanvullende dienstverlening.	ISO 27001/27002 TLS	IPv4 en IPv6	C
RDW	Levering, installatie, onderhoud en support van nieuwe Hardware Security Modules (HSM's) voor de RDW, en onderhoud, support en overige dienstverlening op de huidige installed base HSM's. RDW exploiteert diverse PKI's voor de uitgifte van o.a. kentekenkaarten en rijbewijzen. Daarnaast geeft de RDW eigen authenticatiemiddelen uit. Voor de bescherming van het cryptografisch materiaal gebruikt de RDW HSM's.	IPv6 en IPv4 ISO 27001/27002	HTTPS & HSTS TLS	C
RIVM	Technisch beheer, hosting en doorontwikkeling van Peridos, het landelijke digitale dossier waarin zorgverleners in het kader van de screening op Downsyndroom en het structureel echoscopisch onderzoek (SEO) gegevens vastleggen.	Digikoppeling 2.0 ISO 27001/27002 ODF PDF TLS	Digitoegankelijk	C
RWS	De vervanging van bedienwerkplekken en bijbehorende ICT-systemen in de Verkeerscentrale NW Nederland, daarbij inbegrepen de vervanging van de koppelingen van de Verkeerscentrale met objecten -tunnels, brug, wisselbaan en kunstwerken - in het beheergebied.	IPv4 en IPv6 ISO 27001/27002 TLS	WPA2 Enterprise	C
SVB	Onderhoud en support op de functionaliteit waarvoor het LAN, WLAN, de netwerk security en de tokens worden ingezet. Meer specifiek: de beschikbaarheid en het functioneren van de betreffende netwerken optimaliseren.	DNSSEC IPv6 en IPv4 ISO 27001/27002 TLS WPA2 Enterprise	-	C

aanbesteder	inhoud aanbesteding	standaarden[14] cruciaal	standaarden niet-cruciaal	oordeel
KvK	Een raamovereenkomst voor het uitbreiden, aanpassen en onderhouden van de centrale IT-infrastructuur (met name serverapparatuur, storageapparatuur, LAN-apparatuur en bijbehorende systeemsoftware).	**DNSSEC** **IPv6 en IPv4** **ISO 27001/27002**	**TLS**	**F**
Min. BZK	Implementatie en onderhoud van een web based applicatie waarmee eindgebruikers binnen het BZ-domein in een persoonlijk dashboard met behulp van de nieuwsmonitoring-tool, op basis van nieuwsberichten uit vele internationale nieuwsbronnen, ontwikkelingen over voor hun relevante thema's of regio's kunnen raadplegen.	**HTTPS** **ISO 27001/27002** **TLS**	**DKIM** **SPF** **STARTTLS & DANE**	**F**
Min. Def	Het beheer van en ondersteuning bij het Facilitair Management Informatie Systeem, plus 'aanvullende diensten'.	**DNSSEC** **ISO 27001/27002** **TLS**	**ODF** **PDF**	**F**
Min. I&M	Locatiemanagement: systeembeheer (van simulatoren) en ontwikkeling en beheer (van een nieuwe website) voor de betreffende locatie voor training en opleiding.	-	**IPv4 en IPv6** **ISO 27001/27002** **ODF** **PDF** **TLS**	**F**

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. Met name het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties springt er dit jaar uit, met een drietal aanbestedingen dat het predikaat 'taart-kandidaat' krijgt op voorspraak van de geraadpleegde experts. In dit kadertje komt er van die drie aanbestedingen maar één aan bod, om ook ruimte te bieden aan andere aanbestedende partijen met een positieve waardering van hun uitvraag van relevante standaarden.

Ministerie van BZK: een openbare aanbesteding van het sluiten van een raamovereenkomst voor het leveren van een SMS-gateway. Hierbij gaat het om het afhandelen van het versturen van SMS-berichten, waarbij de opdracht voor het versturen via een applicatie of een webservice kan worden verstuurd. De relevant geachte standaarden (NEN-ISO/IEC 27001 en 27002, IPv4 en IPv6, DNSSEC, TLS en – minder cruciaal – DKIM en SPF) zijn allemaal uitgevraagd, zij het dat de uitvraag op de niet-cruciale standaarden DKIM en SPF te licht wordt bevonden door de experts. In de specificatie van de prestatie staat een apart hoofdstuk over open standaarden.

Gemeente Tilburg: de vijf partners in de 'Tilburgse Toegang' werken momenteel met eigen systemen om hun werk in de ondersteunende zorgverlening te verrichten waardoor informatie niet automatisch deelbaar is tussen de systemen. In de praktijk betekent dat onder andere dubbele invoer in de verschillende systemen en een uiteenlopende manier van registreren. In het kader van een verdere doorontwikkeling wil de opdrachtgever een gezamenlijk klantregiesysteem voor de Toegang aanschaffen. Bij deze aanbesteding is een complex aan open standaarden als relevant aangemerkt: TLS, Digikoppeling, StUF, ODF, PDF, SAML, NEN-ISO/IEC 27001 en 27002, CMIS, HTTPS en HSTS* en – minder cruciaal – Digitoegankelijk, XBRL, DKIM, SPF en STARTTLS en DANE. Hoewel niet al deze standaarden zijn uitgevraagd, oordeelt de expert positief gezien de complexiteit van de casus en het feit dat in de aanbestedingsdocumenten veel aandacht bestaat voor standaarden met daarbij ook een expliciet verwijzing naar de 'pas-toe-of-leg-uit'-lijst.

Centrum Indicatiestelling Zorg: een openbare aanbesteding voor dataverbindingen voor alle locaties van het CIZ. Er wordt ook gevraagd om een managed IP VPN dienst. Alle relevante standaarden worden als cruciaal gezien (IPv4 en IPv6 en NEN-ISO/IEC 27001 en 27002) en zijn ook alle uitgevraagd. Verder wordt in de aanbestedingsdocumenten vermeld dat de in de oplossing opgenomen netwerkcomponenten dienen te voldoen aan de thans geldende Europese normen en voorschriften m.b.t. veiligheid, elektrische installatie en overheidsreglementen en –bepalingen.

Kamer van Koophandel: de KvK ontvangt jaarlijks 1,5 miljoen verzoeken om ondernemingsgegevens te wijzigen in het Handelsregister. In verband met autorisatiecontrole worden deze verzoeken na invulling van een webformulier op KvK.nl op papier met handtekening via de post ingediend. In de gewenste situatie wil de KvK de ondernemer in staat stellen het op KvK.nl digitaal opgevoerde wijzigingsverzoek ook digitaal te ondertekenen en op te sturen, zonder de noodzaak tot afdrukken en versturen per post. Van de acht relevante geachte standaarden (AdES*, PDF, NEN-ISO/IEC 27001 en 27002, HTTPS en HSTS*, TLS, Digitoegankelijk en DNSSEC) wordt alleen de laatste niet gevraagd (deze is overigens ingeschat als niet-cruciaal).

*De met een * gemarkeerde standaarden stonden op het moment van de aanbesteding nog niet op de 'Pas-toe-of-leg-uit'-lijst. Dat neemt niet weg dat in enkele gevallen door de aanbestedende partij wel al is uitgevraagd op deze standaarden.*

3.4. '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 de relevant geachte standaarden (bij de in totaal 52 aanbestedingen was 317 keer een open standaard relevant) is in 142 gevallen (45%) 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 gemiddeld iets hoger dan vorig jaar (6,1 dit jaar tegen 5,8 standaarden per aanbesteding vorig jaar[15]);
- het percentage uitgevraagd ligt met 45% fractioneel hoger dan vorig jaar (2016: 44%)[16];
- combinatie van bovenstaande twee punten duidt erop dat er dit jaar per aanbesteding iets meer standaarden zijn uitgevraagd dan vorig jaar (2,7 versus 2,6).

Dat is terug te zien in de scores voor 'Pas toe' per afzonderlijke standaard. 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. Zie tabel 6.

Een aantal standaarden werd vaker dan gemiddeld gevraagd bij de onderzochte aanbestedingen: ISO 27001/02, PDF, StUF, Digitoegankelijk (voorheen: Webrichtlijnen) en TLS, en – kort daar achter – IPv4/IPv6 en SAML. OWMS scoort in de tabel weliswaar een uitvraagpercentage van 100% maar voor deze standaard geldt dat die slechts één maal als relevant is aangemerkt.

[15] Het aantal standaarden op de lijst voor 'pas toe of leg uit' is min of meer vergelijkbaar met vorig jaar.
[16] In 2015 was dit 43%; dat was toen een flinke verbetering ten opzichte van het jaar daarvoor (25%).

Tabel 6: 'Pas toe' bij feitelijke aanbestedingen in 2016 / 2017, per standaard

(Bron: onderzoek feitelijke aanbestedingen juli 2016 t/m juni 2017, uitgevoerd zomer 2017)

2 x ≥ 75 % 11 x 25-75 % 12 x < 25 %	Ministeries + Uitvoerings-Organisaties		Gemeenten + Provincies + Waterschappen		**Totaal 2016/2017**		*Totaal 2015/2016*
aantal aanbestedingen: n =	*35*		*17*		*52*		*44*
	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	6	0 %	3	0 %	9	0 %	50 %
DNSSEC	10	20 %	4	25 %	14	21 %	0 %
IPv6 en IPv4	17	41 %	2	50 %	19	42 %	8 %
NEN-ISO\IEC 27001:2005nl	35	80 %	13	38 %	48	63 %	60 %
NEN-ISO\IEC 27002:2007nl	35	77 %	13	38 %	48	62 %	48 %
SAML	8	75 %	7	0 %	15	40 %	29 %
SPF	6	0 %	3	0 %	9	0 %	
STARTTLS en DANE	5	0 %	3	0 %	8	0 %	
TLS	29	66 %	13	38 %	42	57 %	54 %
WPA2 Enterprise	2	0 %			2	0 %	
Document & (web)content:							
CMIS	2	50 %	3	0 %	5	20 %	45 %
Digitoegankelijk *)	8	63 %	4	50 %	12	58 %	56 %
ODF 1.2	16	19 %	10	0 %	26	12 %	30 %
OWMS	1	100 %			1	100 %	0 %
PDF **)	16	63 %	10	30 %	26	50 %	65 %
SKOS							
E-facturatie & administratie:							
Sem. Model e-Factureren	2	50 %	1	0 %	3	33 %	50 %
SETU							
WDO Datamodel							
XBRL v2.1	1	0 %	2	50 %	3	33 %	0 %
Stelselstandaarden:							
Digikoppeling	3	67 %	6	17 %	9	33 %	33 %
Geo−standaarden			4	0 %	4	0 %	33 %
StUF	2	0 %	6	67 %	8	50 %	73 %
Water & Bodem:							
Aquo Standaard			1	0 %	1	0 %	
SIKB 0101							
SIKB0102							
Bouw:							
IFC							0 %
Visi							
Juridische verwijzingen:							
BWB	1	100 %			1	100 %	
ECLI							
JCDR							0 %
Onderwijs & loopbaan:							
E−portfolio	2	0 %			2	0 %	0 %
NL LOM	1	0 %			1	0 %	
OAI−PMH							0 %
Overig:							
EMN_NL							
STOSAG			1	0 %	1	0 %	0 %
Totaal	**208**	**54 %**	**109**	**28 %**	**317**	**45 %**	**44 %**

**) Voorheen: Webrichtlijnen. Net als voorgaande jaren alleen beoordeeld voor externe webapplicaties.*
***) Bij de beoordelingen is geen onderscheid gemaakt tussen de verschillende PDF-varianten.*
Ades Baseline Profiles en HTTPS & HSTS zijn pas in mei 2017 op de lijst geplaatst, en daarom buiten de beoordelingen gelaten.

Eerder is al opgemerkt dat stijgers en dalers elkaar min of meer in evenwicht houden. Als we ons beperken tot de standaarden die relatief vaak relevant waren, vallen enkele verschillen ten opzichte van vorig jaar op:

- met name de uitvraag bij IPv4/IPv6 is sterk verbeterd, zowel bij het Rijk als bij de andere overheden, en herstelt zich daarmee van een flinke terugval vorig jaar. Verder valt de uitvraag op DNSSEC op. Waar de afgelopen jaren 0% werd gescoord, wordt deze standaard nu wel bij enkele aanbestedingen uitgevraagd. Wat verder opvalt is dat het aandeel uitgevraagd bij ISO 27002 weer vrijwel gelijk aan de uitvraag van ISO 27001;
- een drietal standaarden laat een tegenovergesteld beeld zien met een relatief flinke daling: hiervan is met name sprake bij DKIM, StUF en ODF. Voor een veel voorkomende standaard als ODF is een uitvraag-score van 12% laag. Bij DKIM valt op dat deze standaard dit jaar geen enkele keer is uitgevraagd, terwijl deze standaard voor 9 van de 52 aanbestedingen als relevant is aangemerkt.

3.5. 'Leg uit' bij feitelijke aanbestedingen

Bij 6 aanbestedingen die in het kader van deze monitor 2017 zijn beoordeeld, is om alle relevante standaarden gevraagd. Bij de andere 46 aanbestedingen had dus in het jaarverslag verantwoording afgelegd moeten worden ('Leg uit') voor het niet toepassen van de betreffende relevante standaard(en). Bij 11 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 35 aanbestedingen (door 29 verschillende overheidsorganisaties) is 'Leg uit' zonder twijfel vereist, omdat hierbij niet gevraagd werd om één of meer van de relevante cruciale open standaarden (25 aanbestedingen) of zelfs om geen enkele relevante standaard gevraagd is (10 aanbestedingen).

Van deze 35 aanbestedingen is het voor 20 aanbestedingen (door 18 overheidsorganisaties, waarvan 6 ministeries) op dit moment mogelijk om in het Jaarverslag 2016 te controleren of 'leg-uit' is toegepast; deze 20 aanbestedingen dateren uit Q3 – Q4 12016. Voor de resterende 15 aanbestedingen kan dat pas na het verschijnen van de jaarverslagen over 2017. Van 'Leg uit' was in de jaarverslagen van de 18 overheidsorganisaties 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.

Bij de decentrale overheden waarvan aanbestedingen zijn onderzocht is in de jaarverslagen geen enkele verwijzing naar het onderliggende beleid teruggevonden[17].

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),

[17] Ook in de gehanteerde (lokale / regionale) beleidskaders met betrekking tot inkoop en aanbesteding is geen verwijzing gevonden naar het hier bedoelde onderliggende beleid.

Infrastructuur en Milieu, VWS, OCW, Binnenlandse Zaken en Veiligheid en Justitie. Van deze zes departementen zijn namelijk aanbestedingen beoordeeld uit Q3+Q4 2016, met een beoordeling die noodzaakt tot 'leg uit'. In onderstaand schema zijn deze zes 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 2016;
- 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';
- daaronder ook het ministerie van Sociale Zaken en Werkgelegenheid; dit departement gaat (als enige) expliciet in op een afwijking van de open standaarden, het betreft een contract-uitbreiding die niet binnen de zoek-criteria viel voor dit onderzoek;
- in het jaarverslag van Wonen en Rijksdienst wordt voor de rijksbrede bedrijfsvoerings-onderwerpen (daaronder: open standaarden) verwezen naar het jaarverslag van 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	**Uitvoering 'leg uit'**
AZ	Het Ministerie van Algemene Zaken heeft geen grote ICT-projecten van meer dan € 5 miljoen uitgevoerd in 2016. Gebruik open standaarden en open source software. Er zijn geen bijzonderheden te melden. *(Bron: B Beleidsverslag onder 3: bedrijfsvoeringsparagraaf, onder 2)*
BZK	Afwijkingen instructie rijksdienst bij aanschaf ICT diensten of ICT producten Het Ministerie van BZK heeft in 2016 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 MijnOverheid, e-Herkenning en DigiD. Jaarlijks publiceert Logius in zijn online jaaroverzicht een overzicht van de toepassing van open standaarden *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf, onder 2)*
BUZA	[Geen]
DEF	[Geen]
EZ	[Geen]
FIN	Gebruik open standaarden en open source software. Voldaan is aan de verplichting van artikel 3, eerste lid van de Instructie rijksdienst bij de aanschaf van ICT-diensten of -producten. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf, onder 2)*
IM	[Geen. NB: vorig jaar nog wel]
OCW	[Geen]
SZW	Gebruik open standaarden In 2016 is een aantal ICT-producten en -diensten van boven de € 50.000 ingekocht of aanbesteed. Procedureel is in die gevallen in het inkoop- en aanbestedingsproces geborgd dat wordt voldaan aan de eis van voldoen aan de open-standaarden volgens het pas-toe-of-leg-uit-principe. In 2016 is op een punt afgeweken van de open standaarden. Het contract

	voor de financiële administratie is uitgebreid. SAP maakt gebruik van open standaarden op 1 uitzondering na. SAP maakt gebruik van iDoc in plaats van de EDIFACT-standaard. *(Bron: B Beleidsverslag onder 6: Bedrijfsvoeringsparagraaf onder 2)*
V&J	[Geen]
VWS	[Geen]
WR	Niet anders dan de volgende verwijzing: Voor de rijksbrede bedrijfsvoeringsonderwerpen wordt u verwezen naar de bedrijfsvoeringsparagraaf van het jaarverslag van begrotingshoofdstuk VII Binnenlandse Zaken en Koninkrijksrelaties.

'Leg uit' voor aanbestedingen uit Q1+Q2 2016 (vorig jaar beoordeeld)

In de vorig jaar verschenen Monitor 2016 zijn onder andere aanbestedingen beoordeeld uit Q1+Q2 2016. Voor 17 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 2016 nu wèl beschikbaar zijn.

Deze 17 aanbestedingen (door 16 overheidsorganisaties, waarvan 2 ministeries) zijn vrijwel gelijk verdeeld over 'Rijk' en 'mede-overheden'. Van 'Leg uit' was in de jaarverslagen van deze 16 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 2015 in de monitor 2016 valt op dat bij één departement de verwijzing naar het beleid rond de toepassing van open standaarden is komen te vervallen (het ministerie van I&M).

De bevindingen rond het toepassen van het 'Leg uit' principe in 2016 zijn min of meer gelijk aan de voorgaande jaren (2011 tot en met 2015), met de nuancering zoals hierboven beschreven.

3.6. Welke open standaarden waren relevant bij feitelijke aanbestedingen

In het onderzoek van feitelijke aanbestedingen is van elke aanbesteding vastgesteld welke open standaard(en) van de 'pas-toe-of-leg-uit'-lijst daarvoor relevant was. Dat levert ook interessante informatie op vanuit het perspectief van de adoptie van standaarden. In Tabel 7 is weergegeven hoe vaak elk van de standaarden van de lijst relevant is gebleken bij een aanbesteding. Van de 38 standaarden[18] op de lijst voor 'pas toe of leg uit' waren er 25 standaarden[19] minimaal bij één aanbesteding relevant (in 2016: 27 van de 37), de andere 11 waren dus voor geen van de 52 onderzochte aanbestedingen in 2016 relevant. Daarvan

[18] Op de lijst staan in juni 2017 40 standaarden, maar zoals eerder aangegeven zijn HTTPS en HSTS en Ades Baseline Profiles niet meegenomen in de beoordeling omdat deze pas sinds mei op de lijst staan.
[19] 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.

waren er 6 ook vorig jaar voor geen enkele onderzochte aanbesteding relevant: ECLI, EMN_NL, WDO Datamodel, SIKB0101, VISI en SKOS.

Een vijftal standaarden steekt er met kop en schouders bovenuit als het gaat om de mate waarin zij relevant worden geacht, getuige tabel 7: ISO 27001/02, TLS, PDF en ODF, met scores vanaf 50% (ODF en PDF) oplopend tot bijna altijd relevant voor ISO 27001/02 (92%). Deze zelfde standaarden stonden ook vorig jaar bovenaan en zijn bij 26 tot 48 (van de 52) aanbestedingen als relevant aangemerkt. Daarna volgt een groep van vier standaarden die bij meer dan 10 aanbestedingen als relevant zijn aangemerkt: SAML, IPv4/IPv6, Digitoegankelijk (voorheen: webrichtlijnen) en DNSSEC. In vergelijking met vorig jaar zijn er twee standaarden uit dit rijtje weggevallen (StUF en CMIS) en is DNSSEC er aan toegevoegd. Dit laatste is opvallend; vorig jaar werd DNSSEC vrijwel niet als een relevante standaard aangemerkt bij de toen beoordeelde aanbestedingen.

Aan de andere kant: van de 25 standaarden die bij de beoordeelde aanbestedingen relevant werden geacht, zijn er dit jaar 7 slechts incidenteel als relevant aangemerkt (vorig jaar waren dat er nog 8):

- E-portfolio en WPA2 Enterprise twee keer, en
- de Aquo-standaarden, NL_LOM, OWMS, STOSAG en BWB één keer.

Alleen STOSAG stond ook vorig jaar in deze opsomming.

Eerder in dit hoofdstuk - bij tabel 1 - is al opgemerkt dat het aantal relevant geachte standaarden per aanbesteding min of meer vergelijkbaar is met vorig jaar en slechts fractioneel hoger ligt. Naar aanleiding van tabel 7 kan daar nog aan worden toegevoegd dat op het niveau van de afzonderlijke standaarden van de lijst iets meer standaarden een hoger percentage 'relevant' scoren dan vorig jaar. Uitschieters daarbij zijn NEN-ISO/IEC 27001 en 27002, DNSSEC en – in iets mindere mate – TLS. 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 68% vorig jaar naar 50% nu.

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

Daar staat tegenover dat ook enkele standaarden dit jaar wel relevant waren (en vorig jaar niet). Ook hier gaat het meestal om standaarden die weinig als relevant worden aangemerkt (Aquo, NL_LOM en JCDR).

In vergelijking met de vorige monitor zijn er dit jaar enkele duidelijke verschuivingen in de mate waarin standaarden relevant waren voor de onderzochte aanbestedingen:

- vier standaarden waren dit jaar veel vaker relevant dan vorig jaar: ISO27001 (+ 24%), ISO 27002 (+26%), DNSSEC (+22%) en TLS (+17%);
- één standaard was dit jaar duidelijk minder vaak relevant: ODF (-18%).

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 6.2 is er dit jaar bij aanbestedingen ongeveer even vaak om de relevante standaarden gevraagd als vorig jaar: 45% dit jaar tegen 44% vorig jaar. In tabel 7 is voor de afzonderlijke standaarden berekend hoe vaak daar om 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 (63% respectievelijk 62%), TLS (46%) en PDF (25%). Bij de vorige monitor stonden dezelfde vier standaarden op dit punt bovenaan.

Na dit rijtje koplopers volgt nog een drietal standaarden met een score van boven de 10%: SAML (12%), IPv4/IPv6 (15%) en Digitoegankelijk (voorheen: Webrichtlijnen) met 13% . Om de andere standaarden is slechts bij enkele aanbestedingen gevraagd of - ten onrechte - zelfs in het geheel niet. Dit laatste is het geval bij E-portfolio, Aquo, NL_LOM, DKIM, GEO-standaarden, SPF, STARTTLS en DANE en WPA2 Enterprise. Deze 0%-scores doen zich meestal voor bij standaarden die slechts incidenteel (meestal 1 of 2 keer, in een enkel geval 3 en 4 keer) als relevant zijn aangemerkt. Wat dit jaar opvalt is dat bij een drietal standaarden de uitvraag-score op 0% staat terwijl de standaarden toch een behoorlijk aantal keren relevant waren. Hierbij gaat het om de volgende standaarden: DKIM (bij 9 aanbestedingen relevant), SPF (ook 9 keer relevant geacht) en STARTTLS en DANE (8 keer relevant).

Tabel 7: Open standaarden relevant / gevraagd bij feitelijke aanbestedingen in 2016/2017

(Bron: onderzoek feitelijke aanbestedingen juli 2016 t/m juni 2017, uitgevoerd zomer 2017)

	Ministeries + Uitvoerings-organisaties		Gemeenten + Provincies + Waterschappen		**Totaal 2016/2017**	
aantal aanbestedingen: n =	*35*		*17*		***52***	
	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	17 %	0 %	18 %	0 %	**17 %**	**0 %**
DNSSEC	29 %	6 %	24 %	6 %	**27 %**	**6 %**
IPv6 en IPv4	49 %	20 %	12 %	6 %	**37 %**	**15 %**
NEN-ISO\IEC 27001:2005nl	100 %	80 %	76 %	29 %	**92 %**	**63 %**
NEN-ISO\IEC 27002:2007nl	100 %	77 %	76 %	29 %	**92 %**	**62 %**
SAML	23 %	17 %	41 %	0 %	**29 %**	**12 %**
SPF	17 %	0 %	18 %	0 %	**17 %**	**0 %**
STARTTLS en DANE	14 %	0 %	18 %	0 %	**15 %**	**0 %**
TLS	83 %	54 %	76 %	29 %	**81 %**	**46 %**
WPA2 Enterprise	6 %	0 %			**4 %**	**0 %**
Document & (web)content:						
CMIS	6 %	3 %	18 %	0 %	**10 %**	**2 %**
Digitoegankelijk *)	23 %	14 %	24 %	12 %	**23 %**	**13 %**
ODF 1.2	46 %	9 %	59 %	0 %	**50 %**	**6 %**
OWMS	3 %	3 %			**2 %**	**2 %**
PDF **)	46 %	29 %	59 %	18 %	**50 %**	**25 %**
SKOS						
E-facturatie & administratie:						
Sem. Model e-factureren	6 %	3 %	6 %	0 %	**6 %**	**2 %**
SETU						
WDO Datamodel						
XBRL v2.1	3 %	0 %	12 %	6 %	**6 %**	**2 %**
Stelselstandaarden:						
Digikoppeling	9 %	6 %	35 %	6 %	**17 %**	**6 %**
Geo−standaarden			24 %	0 %	**8 %**	**0 %**
StUF	6 %	0 %	35 %	24 %	**15 %**	**8 %**
Water & Bodem:						
Aquo Standaard			6 %	0 %	**2 %**	**0 %**
SIKB 0101						
SIKB0102						
Bouw:						
IFC						
Visi						
Juridische verwijzingen:						
BWB	3 %	3 %			**2 %**	**2 %**
ECLI						
JCDR						
Onderwijs & loopbaan:						
E−portfolio	6 %	0 %			**4 %**	**0 %**
NL LOM	3 %	0 %			**2 %**	**0 %**
OAI−PMH						
Overig:						
EMN_NL						
STOSAG			6 %	6 %	**2 %**	**2 %**
Totaal	**208**	**54%**	**109**	**28 %**	**317**	**45 %**

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

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[20]. Hiervoor zijn enerzijds 26 voorzieningen onderzocht die samen de GDI (Generieke Digitale Infrastructuur) vormen[21] . Anderzijds zijn dit jaar ook 9 (andere) voorzieningen die vorige jaren zijn onderzocht nogmaals onderzocht.

Dit deel-onderzoek is uitgevoerd door Piet Hein Minnecré en Florian Henning van PBLQ. In Bijlage E 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 16 juni 2017. 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

[20] Zie ook EAR Online, voor een overzicht van voorzieningen geordend naar informatiseringsdomeinen.
[21] 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.

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 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. Daarbij is ondermeer gebruik gemaakt van een aantal bronnen:

- https://internet.nl - test overzicht van overheidsvoorzieningen op IPv6, DNSSEC,TLS, DKIM en SPF;
- het website-register van de Rijksoverheid (https://www.communicatierijk.nl/vakkennis/r/rijkswebsites-verplichte-richtlijnen/websiteregister).

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 daarvan is voorgelegd aan de opdrachtgever en vervolgens in een definitieve versie toegestuurd aan de vertegenwoordigers van de voorzieningen en opgenomen in de rapportage[22]. 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 duidelijk 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. Daaraan is een status gekoppeld. Deze is door de onderzoekers toegekend. De status kan de volgende waarden hebben:

- Ja: De voorziening is compliant[23] met de standaard,
- Nee: De voorziening is niet compliant met de standaard,
- Deels: Onderdelen van de voorziening zijn compliant maar niet alle onderdelen[24],
- Gepland: Er zijn concrete plannen (gekoppeld aan een datum) om de voorziening op korte termijn compliant te maken met de standaard.

Relevant of niet relevant

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

[22] Zie Bijlage E.

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

[24] 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.

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.

Webrichtlijnen en Digitoegankelijk

De Webrichtlijnen-standaard is het afgelopen jaar vervangen door de Digitoegankelijk-standaard. Het toepassingsgebied van Digitoegankelijk is (nog) niet veranderd ten opzichte van de Webrichtlijnen. Het voornemen is om wetgeving te introduceren (de Wet GDI), waarin de standaard verplicht wordt gesteld. Voorlopig geldt het pas-toe-of-leg-uit regime voor de standaard. BZK en Logius werken momenteel aan een nieuw model voor monitoring en rapportage, dat aansluit bij de verplichtingen die vanuit de Europese Unie voor deze standaard worden gesteld. In deze monitor zijn we, bij afwezigheid van een nieuwe toetsingssystematiek, nog uitgegaan van de systematiek voor Webrichtlijnen. Concreet: is er een toets uitgevoerd en is er een onderbouwing in de vorm van een toetsrapport, 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'.

Ondernemingsdossier / MijnOverheid voor Ondernemers

Het Ondernemingsdossier is niet meer in gebruik, en wordt vervangen door MijnOverheid voor Ondernemers. Deze nieuwe voorziening is vanaf eind 2017 in test en naar verwachting in 2018 operationeel. Daarom is deze voorziening dit jaar niet getoetst in dit onderzoek.

4.2. Overzicht: open standaarden in overheidsbrede voorzieningen

In Tabel 9a + 9b zijn de bevindingen over de 35 onderzochte overheidsbrede voorzieningen in één overzicht samengebracht. In de rapportage van PBLQ, opgenomen in Bijlage E, 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 40 open standaarden op de 'pas toe of leg uit'-lijst zijn er 27 relevant voor één of meer overheidsbrede voorzieningen. Er zijn 13 open standaarden die voor meer dan 20 voorzieningen relevant zijn: IPv6/IPv4 (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), SPF (23), DKIM, Digitoegankelijk, PDF/A-1, PDF/A-2 en PDF 1.7 (22) en STARTTLS+DANE (21).

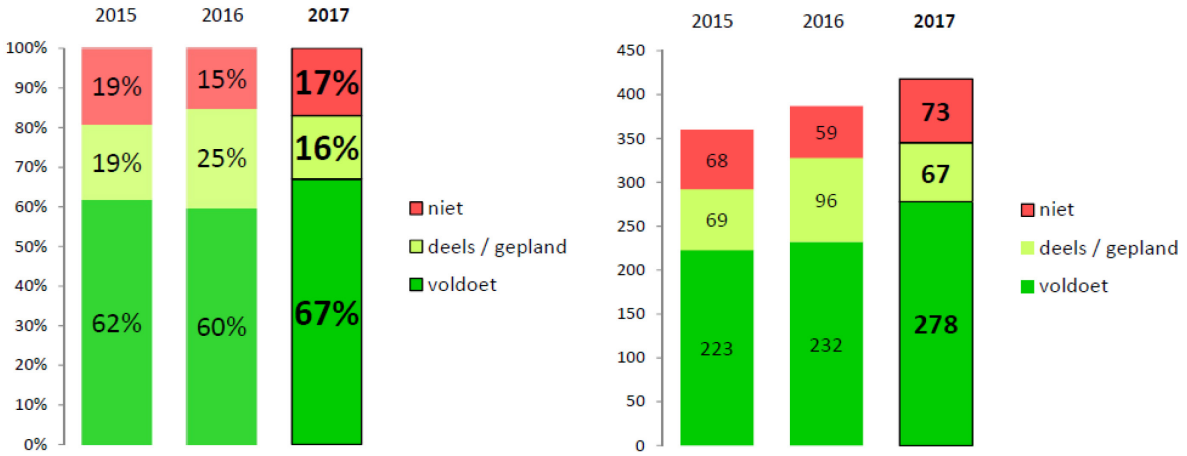
De mate waarin voorzieningen aan de standaard (als die relevant is) voldoen is hoog: voor 9 van de 24 open standaarden geldt dat tenminste 80% van de voorzieningen aan die standaard voldoet. Het gaat om de volgende negen open standaarden: TLS (25 van de 28 voorzieningen voldoet daaraan), NEN-ISO\IEC 27001 en 27002 (25 van de 27 voorzieningen), SAML (13 van de 15), Geo-standaarden (alle 5 de voorzieningen), BWB (alle 4), WPA2 Enterprise (alle 3), SETU en XBRL & Dimensions (alle 2).

Per voorziening beschouwd

Voor een deel van de voorzieningen zijn relatief veel open standaarden relevant, zoals voor de NHR (Basisregistratie Handelsregister: 19 standaarden), de basisregistraties BAG, BRK, WOZ en BGT en Digitale Werkomgeving Rijk (17 standaarden), de BRV, MijnOverheid en P-Direct (17) en Doc-Direct, ODC Noord en Rijksoverheid.nl (16). Voor andere voorzieningen, zoals BRI en Diginetwerk (5), Samenwerkende Catalogi (2) en e-Factureren (1) zijn slechts enkele open standaarden relevant.

Gemiddeld zijn voor een voorziening 12 open standaarden relevant. Vorig jaar waren dat er bijna 11 per voorziening (toen stonden er iets minder standaarden op de lijst) en het jaar daarvoor 9 per voorziening (toen zijn meer voorzieningen onderzocht en stonden er minder open standaarden op de lijst).

Figuur 8: Toepassing open standaarden in 35 voorzieningen: in % en absolute aantallen



In de meeste gevallen voldoen deze voorzieningen ook aan de relevante open standaarden (zie Figuur 8): in 418 gevallen (combinaties van voorziening en relevante standaard) is een

standaard van de lijst relevant, in 278 gevallen (67%, vorig jaar 60%) voldoet de voorziening daar aan en in 67 gevallen (16%, vorig jaar was dat nog 25%) voldoet de voorziening daar deels aan of is dat gepland. In 73 gevallen (17%, vorig jaar 15%) voldoet de voorziening op dit moment nog niet aan een relevante open standaard.

In absolute aantallen (zie rechts in Figuur 8) is het aantal gevallen waarin aan open standaarden wordt voldaan gestegen van 223 in 2015 tot 278 dit jaar.

Bekijken we de voorzieningen apart, dan blijkt dat vier voorzieningen voldoen aan alle relevante standaarden: Rijksoverheid.nl (16 standaarden), DigiD (11 standaarden) BasisRegistratie Inkomen (5 standaarden) en Samenwerkende Catalogi (2 standaarden). Daarnaast zijn er zes 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 nog 9). 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).

Tabel 9a: Toepassing open standaarden in 35 voorzieningen

		Dienstverlening							Gegevens								
	V = voldoet *D = voldoet deels* *G = gepland* *N = voldoet niet* *(leeg = n.v.t.)*	Berichtenbox bedrijven	e-Factureren	MijnOverheid	Ondernemersplein	Overheid.nl	Samenwerkende Catalogi	SBR (Standard Bus. Rep.)	BAG, BRK, WOZ en BGT	BRI (inkomen)	BRT (topografie)	BRV (voertuigen)	BSN Beheervz + GBA-V	Digilevering	Digimelding	NHR (Nieuw HandelsReg.)	Stelselcatalogus
	aantal relevante OSn:	*13*	*1*	*17*	*14*	*14*	*2*	*12*	*68*	*5*	*9*	*17*	*14*	*7*	*7*	*19*	*9*
Internet & beveiliging	DKIM	N		V	V	V		N	V					V	V	V	
	DNSSEC	V		V	G	V		N	V			V		V	V	G	V
	HTTPS & HSTS	N		V	V	G			G		G	G	V	V	V	G	N
	IPv4 & IPv6	N		N	V	V		V	V			N	N	N	N	N	V
	NEN-ISO\IEC 27001			V	V	V			V	V	V	V	V			V	
	NEN-ISO\IEC 27002			V	V	V			V	V	V	V	V			V	
	SAML	V		V								V				V	
	SPF	N		V	V			N	V			V		V	V	V	
	STARTTLS & DANE			V	N	V		N	G		G	G		V	V	N	
	TLS	V		V	N	G		V	V	V	V	V	V			V	
	WPA2 Enterprise									V							
Document & (web)content	AdES Baseline Profiles							V								V	
	CMIS				N							N				D	
	Digitoegankelijk	N		G	V	G	V	N	V		V	D				N	V
	ODF 1.2																
	OWMS			N	N	V	V				N	V					
	PDF 1.7	V		V		V		V	D			V				V	V
	PDF/A-1	V		V		V		V	D			V				V	V
	PDF/A-2	V		V		V		V	D			V				V	V
	SKOS				N	V			D		V	V				N	V
E-facturatie	SMeF		N														
	SETU																
	WDO Datamodel																
	XBRL & Dimensions							V									
Stelselsta	Digikoppeling 2.0	V		D					V	V		D	N	V	V	V	
	Geo-standaarden								V		V						
	StUF	V		V					V				N			V	
Water &	Aquo-standaarden																
	SIKB 0101																
	SIKB 0102																
Bouw	IFC																
	VISI																
Juridisch	BWB				V												V
	ECLI																
	JCDR																
Onderwij	e-Portfolio																
	NL_LOM																
	OAI-PMH																
Overij	EML_NL																
	STOSAG																

Tabel 9b: Toepassing open standaarden in 35 voorzieningen

		Identificatie & Au			Interconnectivite			Overige centrale voorzieningen (niet GDI)								
	V = voldoet *D = voldoet deels* *G = gepland* *N = voldoet niet* *(leeg = n.v.t.)*	DigiD	DigiD Machtigen	ETD (eHerkenning en Idensys)	Diginetwerk	DigiPoort	PKI Overheid	Digi-Inkoop	Dig. Werkomgeving Rijk	Doc-Direct	ODC Noord	P-Direct	Rijksoverheid.nl	Rijkspas	Rijksportaal	TenderNed
	aantal relevante OSn:	*11*	*13*	*14*	*5*	*12*	*10*	*12*	*18*	*16*	*16*	*17*	*16*	*10*	*6*	*14*
Internet & beveiliging	DKIM	V		V		V			D	V	G	V	V	G		N
	DNSSEC	V	V	V	V	N	V	V	D		V	N	V	G		V
	HTTPS & HSTS	V	V	V		V	V	N	D	N	D	N	V			V
	IPv4 & IPv6	V	V	G	N	N	G	N	D	N	D	N	V	N	N	N
	NEN-ISO\IEC 27001	V	V	V	V	V	V	V	V	V	N	D	V	V		V
	NEN-ISO\IEC 27002	V	V	V	V	V	V	V	V	V	N	D	V	V		V
	SAML	V	D	V					V	V	N	V	V	V	V	V
	SPF	V	V	V		N		N	D	N		N	V	V		N
	STARTTLS & DANE	V		N	G	V			N		G			N		N
	TLS	V	V	V		V	V	V	V	N	V	V	V	V		V
	WPA2 Enterprise								V		V					
Document & (web)content	AdES Baseline Profiles								D	N		N				
	CMIS									N						
	Digitoegankelijk	V	N	V					D		N	N	V			N
	ODF 1.2								V	N	V	N	V		V	
	OWMS						V				G		V			
	PDF 1.7		V	V			V	V	V	V	D	D	V		V	V
	PDF/A-1		V	V			V	V	V	V	D	D	V		V	V
	PDF/A-2		V	V			V	V	V	V	D	D	V		V	V
	SKOS									N						
E-facturatie	SMeF							N								
	SETU					V		V								
	WDO Datamodel															
	XBRL & Dimensions					V										
Stelselsta	Digikoppeling 2.0		D			V			D	N		V		V		
	Geo-standaarden															
	StUF															
Water &	Aquo-standaarden															
	SIKB 0101															
	SIKB 0102															
Bouw	IFC															
	VISI															
Juridisch	BWB											V	V			
	ECLI															
	JCDR															
Onderwij	e-Portfolio															
	NL_LOM															
	OAI-PMH															
Overig	EML_NL															
	STOSAG															

5. Open standaarden: gebruiksgegevens

Het uiteindelijke doel van het open standaardenbeleid is 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.

Dit deel-onderzoek is uitgevoerd door Joost Vreuls en Joris Dirks van ICTU.

Voor een completer beeld is het feitelijk gebruik dus een interessante indicator. Helaas is het in het kader van dit deel van het onderzoek lang niet altijd even eenvoudig gebleken om (voor alle open standaarden) vast te stellen in welke mate die feitelijk gebruikt worden.

Van 34 van de 40 standaarden[25] op de 'pas-toe-of-leg-uit' lijst (peildatum: zomer 2017) is informatie verzameld over het feitelijk gebruik. De open standaarden van de lijst voor 'pas toe of leg uit' zijn zeer verschillend, en de mate waarin het feitelijk gebruik van de standaard kan worden vastgesteld loopt sterk uiteen. Langs drie wegen hebben wij in het kader van dit deelonderzoek informatie verzameld:

- door gebruik te maken van de webtool 'internet.nl';
- door een Google-zoekopdracht, in combinatie met een in ontwikkeling zijnde 'crawler';
- door gegevens op te vragen bij de betreffende beheerorganisaties of aanverwante organisaties die over relevante informatie beschikken.

Slechts bij een beperkt aantal standaarden is een met relevante cijfers onderbouwd beeld verkregen van het gebruik van de standaard. Daar waar dergelijke gegevens niet voorhanden waren hebben we ons noodgedwongen gebaseerd op meer kwalitatief gerichte uitspraken of op inschattingen die door onze respondenten zijn gemaakt.

Er is bij deze monitor 2017 een poging gedaan om de uitvraag op de gebruiksgegevens meer te stroomlijnen door een strakkere indeling van de vraagstelling, met als doel om meer uniformiteit te realiseren in de rapportage over het gebruik van de verschillende standaarden. Hierin zijn we maar zeer ten dele geslaagd. Dit komt vooral door de grote onderlinge verscheidenheid aan de standaarden, elk met hun 'eigen verhaal':

- sommige standaarden betreffen een hele familie van deelstandaarden (Geo, StUF);
- bij de ene standaard is de doelgroep en dus het potentiële gebruik veel groter dan bij de andere;

[25] Voor een drietal standaarden is geen navraag gedaan omdat deze nog te kort op de lijst staan. Van drie andere standaarden is geen (relevante) informatie ontvangen.

- sommige standaarden betreffen een relatieve niche-toepassing, andere hebben juist een zeer brede toepassing (organisatorisch en/of functioneel);
- sommige standaarden zijn vanuit hun aard veel meer verplichtend (denk aan EML_NL) in de zin dat je zonder de standaard eigenlijk niet verder kan, bij andere is veel meer sprake van 'keuzevrijheid' – afgezien van de verplichtingen uit Rijksinstructie e.d.

Tenslotte: voor veel standaarden wordt het gebruik niet gemonitord. Gezien het belang van de standaarden (die immers met reden op de lijst zijn geplaatst) is dat op zijn minst bijzonder.

5.1. Gebruiksgegevens 2017 op hoofdlijnen

De gebruiksgegevens zijn verzameld in de zomer van 2017. Uit de aldus verkregen informatie kunnen de volgende algemene bevindingen worden afgeleid:

- voor 14 van de onderzochte standaarden zijn redelijk harde gegevens gevonden die op zijn minst een indicatie geven van het gebruik van de betreffende standaard. Voor de andere open standaarden moest genoegen genomen worden met meer globale informatie (18 standaarden), of was er helemaal geen relevante informatie beschikbaar (5 standaarden);
- bij 18 van de onderzochte standaarden kan – al dan niet onderbouwd met harde gegevens – op basis van de verkregen informatie worden vastgesteld dat sprake is van toename van het gebruik.

In onderstaande tabel staat per standaard vermeld hoe het staat met het gebruik door overheden. Kijkend naar de afzonderlijke standaarden, kan worden vastgesteld:

- van zes standaarden geven de cijfers een duidelijk en direct beeld van het aandeel gebruikers binnen de overheid, de kernvraag van dit deel van de monitor. Dit betreft de vijf standaarden waarvan het gebruik is gemeten met behulp van internet.nl (DKIM, DNSSEC, IPv6, SPF en TLS) en Digikoppeling;
- bij andere standaarden waar cijfermatige informatie is aangeleverd, geven deze cijfers een indicatief en afgeleid beeld van het gebruik, bijvoorbeeld door inzicht in de omvang van het berichtenverkeer;
- zeven open standaarden worden op redelijk brede schaal door overheden gebruikt: StUF (100%, binnengemeentelijk echter minder), EMN_NL (alle gemeenten), Digikoppeling (76%) en een viertal IV-standaarden: DKIM (65%), DNSSEC (66%), SPF (76%) en TLS (93%);
- deze zelfde standaarden[26] vinden we ook terug in de opsomming van standaarden waar sprake is van een duidelijk zichtbare stijging van het gebruik (onderbouwd met cijfers). Andere standaarden waar een met cijfers onderbouwde stijging zichtbaar is zijn: de Geo-standaarden, SAML, WPA2 Enterprise, XBRL en ook de opgave van het Waterschapshuis voor wat betreft de NEN/ISO-standaarden;
- er zijn ook enkele standaarden waarbij door onze bronnen melding wordt gemaakt van een stijging van het gebruik, maar zonder enige vorm van cijfermatige onderbouwing;
- voor zover cijfers beschikbaar zijn blijkt bij een aantal andere standaarden het gebruik over het algemeen (nog) aan de lage kant te zijn, bijvoorbeeld bij IPv6 en ODF.

[26] De enige uitzondering is EML_NL: alle gemeenten gebruiken deze standaard al, net als vorig jaar.

Tabel 10: Gebruiksgegevens 2017, per standaard

(Bron: onderzoek Gebruiksgegevens zomer 2017, zie Bijlage F)

≥ 75 % 25-75 % < 25 %	**Gebruik door overheden 2017**		***Ontwikkeling in gebruik***
	TOTAAL	waarvan Rijk / Uitv.	
Internet & beveiliging:			
DKIM	65 %	52 %	totaal verdubbeld, grootste toename bij mede-overheden
DNSSEC	66 %	70 %	totaal gegroeid van 45% tot 66%, Rijk van 59% tot 70%
HTTPS en HSTS			dit jaar nog niet onderzocht
IPv6 en IPv4	15 %	33 %	implementatie verloopt traag, wel verbetering t.o.v. vorig jaar
NEN-ISO\IEC 27001:2005nl NEN-ISO\IEC 27002:2007nl			implementatie via BIR (Rijk) en BIG/BIWA/IBI (mede-overheden)
SAML	48 % (DigiD)		verdubbeld van 24% tot 48% (aandeel aansluitingen DigiD)
SPF	76 %	60 %	flinke toename van 54% tot 76%, vooral bij mede-overheden
STARTTLS en DANE			dit jaar nog niet onderzocht
TLS	93 %	83 %	flinke stijging van 79% naar 93%, en veel meer cf. richtlijn NCSC
WPA2 Enterprise	[beperkt]		gebruik neemt toe (via federatieve diensten als GovRoam)
Document & (web)content:			
AdEs Baseline Profiles			dit jaar nog niet onderzocht
CMIS		alle ministeries (?)	feitelijk gebruik onduidelijk
Digitoegankelijk *)		alle ministeries (?)	feitelijk gebruik nog onduidelijk (vervangt Webrichtlijnen)
ODF 1.2			indicatief beeld: gebruik waarschijnlijk zeer beperkt
OWMS		Min AZ + I-raad	feitelijk gebruik onduidelijk
PDF **)			indicatief beeld: wordt breed gebruikt
SKOS			feitelijk gebruik onduidelijk
E-facturatie & administratie:			
Sem. Model e-Factureren			gebruik neemt toe, Rijk loopt voorop
SETU			feitelijk gebruik onduidelijk
WDO Datamodel			gebruik neemt toe
XBRL v2.1		uitvoeringsorg.s	gebruik neemt toe
Stelselstandaarden:			
Digikoppeling	76 %	67 %	totaal gegroeid van 64% tot 76%, Rijk van 40% tot 67%
Geo−standaarden			gebruik sommige (deel)standaarden neemt toe
StUF			alle gemeenten gebruiken StUF in meer of mindere mate
Water & Bodem:			
Aquo Standaard			geen bruikbare gegevens ontvangen
SIKB 0101			door mede-overheden breed gebruikt, geen harde gegevens
SIKB0102			feitelijk gebruik onduidelijk
Bouw:			
IFC			feitelijk gebruik onduidelijk, lijkt beperkt
Visi			gebruik nog niet groot, maar neemt toe
Juridische verwijzingen:			
BWB ECLI JCDR	in diverse voorzieningen geïmplementeerd, geen harde gebruiksgegevens		geen harde gegevens beschikbaar
Onderwijs & loopbaan:			
E−portfolio			geen bruikbare gegevens ontvangen
NL LOM			binnen sector onderwijs breed gebruikt, geen harde gegevens
OAI−PMH			breed gebruikt (onderwijs, erfgoed), geen harde gegevens
Overig:			
EMN_NL		alle gemeenten	volledige adoptie bereikt
STOSAG			geen bruikbare gegevens ontvangen

Gedetailleerde gegevens over het gebruik per standaard (voor zover beschikbaar) zijn te vinden in Bijlage F. In de navolgende paragrafen worden de onderzochte standaarden per domein kort omschreven en wordt de conclusie over het gebruik weergegeven.

5.2. Domein internet en beveiliging

DKIM (Anti-phishing)

DKIM koppelt een e-mail aan een domeinnaam met behulp van een digitale handtekening. Het stelt de ontvanger in staat om te bepalen welke domeinnaam (en daarmee welke achterliggende organisatie) verantwoordelijk is voor het zenden van de e-mail. Daardoor kunnen spam- en phishing-mails beter worden gefilterd.

Ongeveer twee op de drie domeinnamen van overheden is in 2017 voorzien van een DKIM-configuratie (vorig jaar: een op de drie). De relatieve 'achterblijvers' uit de vorige meting (gemeenten en waterschappen) hebben een duidelijke inhaalslag gemaakt, met dit jaar een hoogste procentuele score bij de gemeenten. In vergelijking met de meting vorig jaar is sprake van een stijging die zich bij alle overheden voordoet.

DNSSEC (Domeinnaambeveiliging)

Het Domain Name System (DNS) is kwetsbaar, waardoor kwaadwillenden een domeinnaam kunnen koppelen aan een ander IP-adres ('DNS spoofing'). Gebruikers kunnen hierdoor bijvoorbeeld worden misleid naar een frauduleuze website. DNS Security Extensions (DNSSEC) lost dit op. DNSSEC is een cryptografische beveiliging die een digitale handtekening toevoegt aan DNS-informatie. Op die manier wordt de integriteit van deze DNS-informatie beschermd. Aan de hand van de digitale handtekening kan een internetgebruiker (onderwater en volledig automatisch m.b.v. speciale software) controleren of een gegeven DNS-antwoord authentiek is en afkomstig is van de juiste bron. Zodoende is met grote waarschijnlijkheid vast te stellen dat het antwoord onderweg niet is gemanipuleerd.

Het aandeel websites van overheden dat voldoet aan DNSSEC ligt inmiddels op twee op de drie (66%). Het aantal is nog steeds groeiende. De overheden zijn met hun score inmiddels beland boven het landelijk gemiddelde.

IPv6 en IPv4 (Internetnummers)

Internet Protocol versie 6 (IPv6) maakt communicatie van data tussen ICT-systemen binnen een netwerk, zoals internet, mogelijk. De standaard bepaalt dat ieder ICT-systeem binnen het netwerk een uniek nummer (IP-adres) heeft. De belangrijkste motivatie voor de ontwikkeling van IPv6 was het vergroten van de hoeveelheid beschikbare adressen ten opzichte van de tegenwoordig gangbare voorganger IPv4. De aanvankelijke ambitie van het kabinet was om websites en email van de overheid per 2014 toegankelijk te hebben via IPv6. Om interoperabiliteit maximaal te waarborgen heeft het College Standaardisatie 'pas toe of leg uit' van toepassing verklaard op de combinatie van IPv4 en IPv6. Een organisatie moet dus beide versies vragen bij de aanschaf van een ICT-product of -dienst.

De implementatie van IPv6 door overheden verloopt traag, afgezet tegen de ambities, maar er is het tweede achtereenvolgende jaar sprake van een ontwikkeling de goede kant op, nu met een score van 15%.

NEN-ISO/IEC 27001 / 27002 (Managementsysteem / Richtlijnen informatiebeveiliging)

De NEN-ISO/IEC 27001 standaard ISO 27001 specificeert eisen voor het vaststellen, implementeren, uitvoeren, bewaken, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie. Het ISMS is ontworpen met het oog op adequate en proportionele beveiligingsmaatregelen die de informatie afdoende beveiligen en vertrouwen bieden.

De NEN-ISO/IEC 27002 standaard 'Code voor informatiebeveiliging' (versie 2013) is een nadere specificatie van NEN-ISO/IEC 27001 en geeft richtlijnen en principes voor het initiëren, implementeren, onderhouden en verbeteren van informatiebeveiliging binnen een organisatie. NEN-ISO/IEC 27002 kan dienen als praktische richtlijn voor het ontwerpen van veiligheids-standaarden binnen een organisatie en effectieve methoden voor het bereiken van deze veiligheid.

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) zijn toegepast. Daarover hebben alle 11 departementen medio februari 2017 een ICV (in control verklaring) afgegeven. Daarnaast is in 2017 gewerkt aan een nieuwe BIR, die is gebaseerd op de meest recente versies van relevante ISO normatiek en andere normen van de pas-toe-of-leg-uit lijst.
Alle Nederlandse gemeenten hanteren inmiddels de BIG als normenkader voor informatiebeveiliging, deze is gebaseerd op de BIR / ISO27001/2.
Bij de provincies worden de standaarden ISO/IEC 27001 en 27002 geïmplementeerd via de IBI. Op dit moment zijn geen nadere gegevens over de voortgang van de implementatie beschikbaar.
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%). Eind 2017 vindt wederom een sectorbrede meting plaats naar de voortgang op de implementatie van informatie-beveiliging (self assessment). Dit jaar komt daar nog een beoordeling bij door een onafhankelijke externe partij op compliancy met de BIWA.

SAML (uitwisseling inloggegevens)

De Security Assertion Markup Language (SAML) is een XML-gebaseerd raamwerk voor het communiceren van gebruikers authenticatie, rechten, en attribuut informatie. SAML biedt organisatie entiteiten de mogelijkheid om claims te maken over de identiteit, attributen en rechten van een subject (een entiteit welke vaak een menselijke gebruiker is) aan andere entiteiten zoals Internet applicaties of diensten.

SAML is de standaard geworden voor (nieuwe) aansluitingen waarbij burgers of bedrijven inloggen bij de overheid. Het is onbekend hoeveel organisaties SAML gebruiken voor de authenticatie van medewerkers.

SPF (E-mailbeveiliging)

SPF controleert of de mailserver die een e-mail wil versturen namens het e-maildomein deze e-mail mag verzenden. SPF specificeert een technische methode om afzenderadres-vervalsing detecteerbaar te maken. SPF biedt de mogelijkheid te controleren of een bericht aangeleverd wordt vanaf een server die daartoe gerechtigd is. Dit doet SPF door de authenticiteit van de domeinnaam in het afzenderadres van de ontvangen mail herleidbaar te maken via de in DNS gepubliceerde IP-adressen van de verzendende mailserver(s). Indien een mailserver niet in de lijst met gepubliceerde IP-adressen staat (de zogeheten SPF-records) maar toch mail verstuurt met het betreffende domein als afzender, dan wordt de mail als niet geauthenticeerd beschouwd.

Het aandeel websites van overheden dat voldoet aan SPF ligt inmiddels boven op driekwart en laat in vergelijking met vorig jaar (wederom) een behoorlijke stijging zien. De groei is in alle

onderscheiden categorieën overheden terug te vinden, maar bij het Rijk blijft de groei dit jaar wel wat achter in vergelijking met de andere overheden.

TLS (Beveiligde internetverbinding)

TLS is een protocol, dat tot doel heeft om beveiligde verbindingen op de transportlaag over het internet te verzorgen. De standaard wordt gebruikt bovenop standaard internet transport protocollen (TCP/IP) en biedt een beveiligde basis, waar applicatie protocollen als HTTP (webverkeer) of SMTP en IMAP (mailuitwisseling) op hun beurt weer op kunnen bouwen en gebruik van kunnen maken.

De standaard TLS komen we veel tegen bij overheidswebsites (93%) en het gebruik is ook gegroeid in vergelijking met vorig jaar (in 2016: 79%). De aanpak conform de richtlijn van het NCSC komt ook steeds meer voor: inmiddels bij driekwart (77%) van de hier onderzochte websites (vorig jaar: 26%).

WPA2 Enterprise (Toegang tot een wifi-netwerk met een account)

Steeds meer komt het voor dat medewerkers van overheidsorganisaties WiFi-toegang nodig hebben op andere locaties dan hun eigen werkplek. Als de gastlocatie WiFi-toegang biedt met een gedeeld wachtwoord, dan moeten zij handmatig een verbinding maken met het WiFi-netwerk door het gedeelde wachtwoord in te geven. Dit is onveilig en inefficiënt.
WPA2 Enterprise maakt het mogelijk dat gebruikers automatisch en veilig toegang krijgen tot aangesloten WiFi-netwerken via authenticatie op basis van bestaande identiteitsgegevens. Diensten zoals Govroam, Rijk2Air en Eduroam maken al gebruik van WPA2 Enterprise, en bieden WiFi-toegang met een hoog beveiligingsniveau zonder dat de gebruiker extra handelingen hoeft te verrichten.

Govroam maakt een flinke ontwikkeling mee en lijkt daarmee een inhaalslag te voeren op de educatieve sector. Er lijkt nog veel ruimte te zijn voor groei in adoptie. Buiten de federatieve diensten voor WPA2 Enterprise is er geen stimulans hiervoor; gezien het doel van de standaard, lijkt het ook vooral wenselijk dat adoptiebevordering gebeurt via federatieve diensten.

5.3. Domein document en (web/app)content

CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)

Content Management Interoperability Services (CMIS) is een open standaard die een scheiding mogelijk maakt tussen zogenaamde 'content repositories' en content applicaties. Hierdoor kunnen content (ongestructureerde data, zoals documenten en e-mails) en bijbehorende metadata (beschrijvende data) gemakkelijker worden uitgewisseld. Met behulp van CMIS kunnen applicaties als Content Management Systemen (CMS) en Document Management Systemen (DMS) werken met content die afkomstig is uit verschillende repositories (een soort van opslagplaats voor ongestructureerde data), zonder nieuwe koppelingen te hoeven bouwen of gebruik te hoeven maken van leverancierseigen oplossingen. Het is hierdoor eenvoudiger om informatie en de bijbehorende metadata uit verschillende databases en over organisatiegrenzen heen uit te wisselen. Bovendien is het met CMIS eenvoudiger om te migreren van een systeem naar een ander systeem.

Alle departementen zijn 'in beeld' als het gaat om het gebruik van CMIS. Harde gegevens over gebruik zijn evenwel niet beschikbaar. Van andere overheden en instellingen uit de publieke sector is geen informatie bekend.

Digitoegankelijk (Toegankelijkheid websites)

De standaard EN 301 549 voorziet in het toegankelijk maken van overheidswebsites. EN 301 549 bevat de internationale toegankelijkheidsstandaard WCAG 2.0, die ervoor zorgt dat content op websites en in webapplicaties ook toegankelijk is voor mensen met een functiebeperking.
Deze standaard heeft grote overeenkomsten met Webrichtlijnen (niveau AA); het belangrijkste verschil zit in het schrappen van het principe 'Universeel' uit de Webrichtlijnen met achterliggende normen voor systeem-onafhankelijke websites. De Europese standaard is sinds december 2016 per Europese richtlijn verplicht en wordt in Nederland 'Digitoegankelijk' genoemd.

De adoptie van Digitoegankelijk is maar beperkt inzichtelijk. Op basis van de voorhanden zijnde informatie lijkt het er op dat een groot aantal organisaties wel zich bewust is van het bestaan van de standaard (of de voorloper daarvan), maar dat waarschijnlijk de meeste er niet aan voldoen. Mede afhankelijk van de inrichting (en consequenties) van de verplichtende wetgeving in Nederland, is de verwachting dat de adoptie flink zal toenemen.

ODF 1.2 / PDF 1.7 / PDF/A-1 en PDF A-2 (Documentbewerking / Documentpublicatie)

De lijst voor 'pas toe of leg uit' telt op dit moment vier open documentstandaarden: ODF, gericht op bewerkbare documenten, en drie varianten van PDF voor niet-bewerkbare documenten. ODF 1.2 (versie: 1.2) is een open standaard voor tekstdocumenten, (vector-)tekeningen, presentaties en rekenbladen (spreadsheets). PDF/A-1 (versie: NEN-ISO 19005-1:2005). Dit deel van ISO 19005 specificeert hoe Portable Document Format (PDF) 1.4 voor lange termijn archivering van elektronische documenten dient te worden gebruikt. Het heeft betrekking op documenten met combinaties van data in de vorm van karakters, rasters en vectoren. PDF/A-2 (versie: ISO 19005-2). Deze standaard slaat de brug tussen PDF/A-1 en PDF 1.7 waarbij PDF/A-2 een betere geschiktheid heeft voor langdurig archiveren van documenten waar 'elementen' inzitten die niet door PDF/A-1 worden ondersteund en waarbij PDF 1.7 kan worden gebruikt voor 'elementen' die niet door PDF/A-2 ondersteund worden. PDF 1.7 (versie: ISO 32000-1:2008). Deze standaard specificeert een bestandsformaat voor het weergeven van elektronische documenten. Het uitgangspunt van de standaard is dat het gebruikers mogelijk wordt gemaakt documenten uit te wisselen en te bekijken, zowel onafhankelijk van de omgeving waarin ze zijn gecreëerd, alsook de omgeving waarin ze worden uitgeprint of bekeken. Elk PDF v1.7 document bevat een complete beschrijving van een document, inclusief tekst, font objects (embedded of met typeface beschrijving), afbeeldingen, audio, video, en 2D/3D graphics.

ODF lijkt nauwelijks gebruikt te worden. Een aantal sites biedt nog wel een hoeveelheid MS Office-documenten aan, maar van de drie formaten is PDF het meest gebruikt. Van deze PDF-documenten is een klein gedeelte in PDF/A-formaat; hoeveel documenten voldoen aan de eisen van de PDF 1.7-standaard is niet bekend.

OWMS 4.0 (Metadata overheidsinformatie)

OWMS is een semantische standaard voor metadata, de eigenschappen om informatieobjecten mee te beschrijven. Het voorschrijven van een semantische standaard voor metadata verhoogt de vindbaarheid en de samenhang van informatie die door overheidsorganisaties wordt aangeboden op internet.

Het aantal directe toepassers van OWMS 4.0 beperkt zich binnen de overheid tot het Ministerie van Algemene Zaken en de Inspectieraad. Toepassing van een contentmodel dat is gebaseerd op OWMS 4.0 kan wijd verspreid zijn binnen de overheid, afhankelijk van het type contentmodel waarnaar wordt gekeken. Deze conclusie is (wederom) gelijkluidend als die van vorig jaar.

SKOS (Thesauri en begrippenwoordenboek)

SKOS is een uitwisselbaar gegevensmodel voor het delen en linken van systemen voor kennisrepresentatie via het Web. Veel systemen voor kennisrepresentatie zijn gegrondvest op eenzelfde conceptueel kader. Voorbeelden zijn thesauri, taxonomieën, begrippenwoordenboeken, classificatieschema's en systemen voor trefwoordtoekenning. Ze worden vaak gebruikt in vergelijkbare applicaties. SKOS maakt de overeenkomstige structuurelementen expliciet volgens een generieke standaard. Doordat SKOS voortbouwt op de standaarden RDF, RDFS en OWL (zie hierboven) zijn de kennisrepresentaties bruikbaar voor computerprogramma's ("machine readable") en kunnen deze uitgewisseld worden tussen applicaties en gepubliceerd worden op het Web.

Harde gegevens over gebruik door overheden zijn niet beschikbaar.

5.4. Domein E-facturatie en administratie.

Semantisch model e-factureren (Elektronische facturen)

Het Semanitische factuurmodel is een standaard voor electronisch 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). De standaard beschrijft welke gegevenselementen er in een elektronische factuur opgenomen dienen en kunnen worden, wat de samenhang is tussen deze elementen en wat de betekenis is van deze elementen. Daarnaast bevat de standaard mappings van de gegevenselementen naar SETU (staat op de 'pas toe of leg uit' –lijst) en de internationale UBL standaard zoals UBL SI (Simpler Invoicing) en UBL OHNL. Dit zijn twee veelgebruikte standaarden voor elektronisch factureren. Dankzij de mappings kunnen gebruikers van deze standaarden op een eenvoudige uniforme wijze elektronisch naar de overheid factureren. Mappings naar andere standaarden zijn bovendien ook mogelijk.

Hoewel exacte gegevens ontbreken, lijkt het dat adoptie groeiende is. Daarbij is de Rijksoverheid een duidelijke voorloper terwijl decentrale overheden nog duidelijk aan het begin staan.

SETU-standaarden (Informatie flexibele arbeidskrachten)

De SETU-standaard is de Nederlandse implementatie van de internationale HR-XML standaard en is ontwikkeld door de grote uitzendorganisaties. Door toepassing van de SETU standaard ontstaat uniformering van het elektronisch berichtenverkeer tussen aanbieders en afnemers (inleners) van tijdelijk personeel (flexibele arbeid). Dit leidt tot vereenvoudiging van het inhuurproces.

Over de mate waarin van overheidszijde gebruik wordt gemaakt van de SETU-standaard bij het inlenen van personeel zijn geen harde gegevens beschikbaar.

WDO Datamodel (Douane-informatie)

Het WDO Datamodel is in 1997 opgezet vanuit de G7 naar aanleiding van de wens van het bedrijfsleven om gegevensaanlevering van het bedrijfsleven naar de overheid op het gebied van grensoverschrijdend personen- en goederenverkeer meer te simplificeren en te harmoniseren. Aangevers worden op dit moment geconfronteerd met het feit dat men dezelfde gegevens vaak meerdere keren moet aanleveren, op verschillende manieren, aan verschillende overheidsinstanties en in verschillende landen. Het WDO Datamodel bevat zogenaamde 'informatiepakketten' voor gegevensuitwisseling. Deze beschrijven de semantiek van de uitgewisselde informatie: gegevens- en

procesmodellen en hiervan afgeleide berichtspecificaties, de zogenaamde Message Implementation Guidelines (MIG's). Informatiepakketten kunnen aan elkaar gerelateerd worden, waardoor samenhang ontstaat. Het WDO Datamodel integreert op deze manier de semantiek voor verschillende toepassingsdomeinen. Hierbij gaat het niet alleen om de Douane, maar ook om tal van andere overheidsinstellingen die betrokken zijn bij grensoverschrijdend verkeer (Voedsel en Waren Autoriteit, Havenautoriteiten etc.).

Met betrekking tot het gebruik van deze standaard zijn geen harde gegevens bekend omdat het feitelijke gebruik niet wordt geregistreerd. Er is sprake van een stijging van het gebruik.

XBRL en Dimensions (Bedrijfsrapportages)

Organisaties wisselen bedrijfsinformatie uit op de meest uiteenlopende manieren (op papier of elektronisch, als Word-document, als Pdf, als spreadsheet, etc.). XBRL, eXtensible Business Reporting Language, is een internationale open standaard om deze gegevens op eenvoudige wijze te verzamelen, elektronisch uit te wisselen, te analyseren en zo nodig nader te bewerken.

Het gebruik van deze standaard is groeiende.

5.5. Domein Stelselstandaarden

Digikoppeling versie 2.0 (Veilige berichtuitwisseling)

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

- *bevragingen: een vraag waar direct een reactie op wordt verwacht. Hierbij is snelheid van afleveren belangrijk. Als een service niet beschikbaar is, dan hoeft de vraag niet opnieuw te worden aangeboden;*
- *meldingen: men levert een bericht en (pas) veel later komt eventueel een reactie terug. In dat geval is snelheid van afleveren minder belangrijk. Als een partij even niet beschikbaar is om het bericht aan te nemen, dan is het juist wel gewenst dat het bericht nogmaals wordt aangeboden.*

Aan versie 2.0 van Digikoppeling (deze versie staat op de lijst 'pas toe of leg uit') is o.a. de specificatie voor grote berichten toegevoegd, de mogelijkheid om attachments toe te voegen en om security op berichtniveau toe te passen. In 2016 is vooral onderhoud aan de standaard doorgevoerd. De belangrijkste wijziging is dat het wijzigingsvoorstel om het OIN beleid aan te passen is goedgekeurd door de Regieraad Gegevens. Het OIN, het Organisatie Identificatie nummer is een essentieel onderdeel van de Digikoppeling standaard en wordt binnen het berichtenverkeer van de Overheid veelvuldig toegepast. Dit nieuwe beleid zal in 2017 worden uitgewerkt en gerealiseerd.

Een substantieel deel van de overheden is op Digikoppeling aangesloten. Er is sprake van een verdere stijging, van 64% naar een aandeel van 76%. Vorig jaar hebben met name provincies en waterschappen een inhaalslag gemaakt en groeiden relatief hard. Dit jaar blijft de groei daar achter en is met name bij Rijk en gemeenten sprake van groei.

Geo-standaarden (Geografische informatie)

In Nederland (en ook daarbuiten) zijn veel organisaties betrokken bij 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 aardoppervlakte. 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 Geo-standaarden voorziet hierin. 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 v1.3.1*
- *Nederlands metadataprofiel op ISO 19119 voor services v1.2.1*
- *webserviceprofielen voor Web Feature Service (WFS) en Web Map Service (WMS)*

Omdat sprake is van een set deelstandaarden, is het beeld complex en lastig te duiden. Daar waar sprake is van (indicatieve) gegevens over gebruik, is sprake van duidelijke stijgingen. Dit geldt voor het gebruik van NEN3610, zowel qua aantal implementaties (o.a. uitbreiding naar BAG) als qua aantal bevragingen van data die gestructureerd is conform de NEN3610-familie van informatiemodellen. Met het steeds verder gevuld raken van de BGT neemt ook het gebruik van GML steeds verder toe. GML is een onmisbare bouwsteen in het stelsel van (geo)basisregistraties. Op metadata gebied zien we een groei van het aanbieden van metadata van datasets conform de standaarden (+10%), terwijl het aanbod van metadata van services constant blijft. Het gebruik in de vorm van afnemen (doorzoeken) van metadata is fors gegroeid (+500%). Voor het gebruik van WMS en WFS geven gebruikscijfers van PDOK een goede indicatie van het gebruik binnen overheidscontext. Het gebruik van deze services laat voor bijv. WMS een groei van 250% zien.

StUF (Uitwisseling administratieve overheidsgegevens)

De StUF-standaard is een familie van samenhangende gegevens- en berichtenstandaarden. StUF staat sinds eind 2008 op de pas-toe-of-leg-uit-lijst en richt zich op de standaardisatie van de inhoud van informatie, berichten en services. StUF is als open standaard vastgesteld voor :

- *uitwisseling 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 diensten-portfolio van gemeenten;*
- *uitwisseling van domein- of sector-specifieke gegevens waarin ook basis- en/of zaak-gegevens voorkomen en waarvoor geen andere (inter)nationale (XML-gebaseerde) berichtenstandaard is vastgesteld.*

Samengevat blijkt uit de cijfers en de analyse dat gemeenten, ketenpartners en hun leveranciers goede stappen hebben gezet op het vlak van interoperabiliteit en het gebruik van StUF: er ligt een stevige basis. Het aantal gemeentelijke ketens waarin StUF wordt gebruikt, is uitgebreid. Er is veel pakketsoftware op de markt of dit komt binnenkort op de markt. Om de baten van de StUF-standaard te benutten is meer aandacht nodig voor vernieuwing van de standaard en voor verbreding van het gebruik in andere gemeentelijke ketens, processen en systemen. Bij deze vernieuwing is goed opdrachtgeverschap van gemeenten cruciaal. Het verminderen van tempo-verschillen en het afdwingen van compliancy (testrapporten) draagt bij aan soepeler implementaties en meer transparantie over de kwaliteit van het aanbod van software. De verwachting is dat de ingezette vernieuwing van de StUF Familie en de borging van Open Standaarden in de uniforme ICT inkoopvoorwaarden (GIBIT) daar aan bijdraagt. Datzelfde geldt voor de beweging dat gemeenten steeds meer van hun informatievoorziening collectief willen organiseren.

5.6. Domein Water en bodem

Aquo-standaarden (uitwisseling gegevens waterbeheer)

Over het gebruik van deze standaarden is geen bruikbare informatie beschikbaar.

SIKB0101 (Milieutechnische bodeminformatie)

SIKB0101 is een 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. Een onderdeel van het gebruik is het aanleveren van bodemkwaliteitgegevens aan landelijke registratiesystemen voor bodemkwaliteit (GLOBIS), aan lokale systemen (bodem informatiesystemen provincies en gemeenten) en aan TOWABO, het landelijke systeem voor de toetsing van waterbodems (o.a. vervuild slib). GLOBIS wordt decentraal beheerd en er zijn meerdere implementaties van dit systeem in gebruik. Daarvoor is SIKB0101 de facto de standaard. De verplichting geldt bij de investering in een systeem of dienst waarmee kwaliteitsgegevens van bodems uitgewisseld worden.

Rijkswaterstaat Leefomgeving en vrijwel alle gemeenten, provincies en omgevingsdiensten beschikken over systemen waarin SIKB0101 is toegepast. Harde gegevens over de mate waarin overheden digitaal gegevens delen zijn evenwel niet beschikbaar.

SIKB0102 (Archeologische bodeminformatie)

Met SIKB0102 kunnen overheden en bedrijven gestandaardiseerde archeologische informatie uitwisselen. Dankzij het gebruik van de SIKB0102-uitwisselingsstandaard zijn archeologische onderzoeksgegevens voor iedereen online beschikbaar. Deze gegevens zijn transparant opgezet en beschreven, wat ten goede komt aan het vertrouwen in de kwaliteit van de beschikbare digitale documentaties. Het koppelen van verschillende datasets - bijvoorbeeld in het kader van een synthetiserend onderzoek - wordt vereenvoudigd. Hierdoor kan er met minder inspanning meer kenniswinst worden geboekt. Bedrijfsprocessen lopen efficiënter in een digitaal traject dan in een analoog traject. Een opgravende instantie, overheidsorganisatie of een bedrijf dat archeologisch onderzoek en/of vondsten doet heeft een wettelijke plicht om binnen twee jaar na afronding van de opgraving de verzamelde informatie beschikbaar te stellen aan een aantal depots (landelijk, provinciaal en/of gemeentelijk). De structuur, het formaat en de waarden voor de digitale uitwisseling van deze informatie wordt beschreven in de SIKB0102-standaard. De verplichting geldt bij een investering in een systeem of dienst dat wordt gebruikt voor de uitwisseling van archeologische informatie, verzameld tijdens het uitvoeren van archeologisch onderzoek en/of bij een archeologische vondst.

Over de mate waarin van overheidszijde gebruik wordt gemaakt van de SIKB0102l zijn geen harde gegevens beschikbaar.

5.7. Domein Bouw

IFC (Bouwwerkinformatiemodellen)

Bij de IFC-standaard draait het om de uitwisseling van 3D-bouwinformatiemodellen.

Hoewel sprake is van een stijging van het gebruik, zijn er nog veel partijen die IFC niet toepassen. Harde gegevens omtrent het gebruik ontbreken.

VISI (Bouwprocesinformatie)

De VISI standaard richt zich op de formele communicatie tussen partijen in de bouwsector, zowel grond- weg en waterbouw, de burger & utiliteitsbouw als de installatiebranche.

Enkele harde gegevens over gebruik door overheden zijn voor het eerst beschikbaar. Een vergelijking met de vorige monitor is nog niet mogelijk. Het algemene beeld is dat sprake is van een toename van het gebruik.

5.8. Domein Juridische verwijzingen

BWB, ECLI en JCDR (Juridische identificatie en verwijzing)

De drie Juriconnect standaarden BWB, ECLI en JCDR zijn gericht op standaardisatie van identificatie met het doel om de geïdentificeerde inhoud te delen. Voor verwijzing naar wet- en regelgeving of onderdelen daarvan in wetten.overheid.nl, is aan elke regeling een uniek identificatienummer (BWBID) toegekend. De Juriconnect-BWB-standaard standaard beschrijft hoe deze verwijzing wordt vormgegeven. Citeren, vinden en verbinden van wet- en regelgeving gaat door toepassing van de BWB standaard sneller, eenvoudiger en geeft minder kans op fouten. Gebruik van de standaard biedt daardoor verbetering van interoperabiliteit. De open standaard BWB biedt een eenduidige manier van verwijzen naar (onderdelen van) wet- en regelgeving. De laatste versie (versie 1.3.1) maakt het mogelijk om in wet- en regelgeving te kunnen verwijzen naar: taalversies en onderdelen van internationale verdragen, wet- en regelgeving waarvan de indeling niet voldoet aan de gebruikelijke nummering van hoofdstukken en paragrafen, en ruime begrippen zoals "enig artikel". Met de ECLI-standaard (versie 1.0) kunnen:

- *alle rechterlijke uitspraken in de Europese Unie (zowel van nationale als van Europese gerechten) worden voorzien van een gelijkaardige, unieke en persistente identifier. Deze identifier kan worden gebruikt voor identificatie en citatie van rechterlijke uitspraken en derhalve om deze te vinden in binnenlandse of buitenlandse, Europese of internationale jurisprudentie-databanken;*
- *alle rechterlijke uitspraken worden voorzien van uniforme metadata, gebaseerd op de Dublin Core standaard. Het zoeken van uitspraken in allerlei databanken wordt daardoor gefaciliteerd.*

De JCDR-standaard (versie 1.0) biedt een eenduidige manier van verwijzen naar (onderdelen van) decentrale regelgeving waarmee de interoperabiliteit van juridische documenten en systemen die veel verwijzingen kennen naar decentrale regelgeving wordt bevorderd.

Over het gebruik van deze standaarden zijn op dit moment geen harde gegevens beschikbaar, evenmin als voorgaande jaren.

5.9. Domein Onderwijs en loopbaan

e-Portfolio

Over het gebruik van deze standaard is geen bruikbare informatie beschikbaar.

NL_LOM

NL LOM is een standaard die voorschrijft welke metadata toegekend moeten worden aan educatieve materialen om de vindbaarheid en vergelijkbaarheid te vergroten. Met metadata worden extra kenmerken van een document of ander object bedoeld. Te denken valt aan auteursgegevens, titel, uitgever, taal, etc. NL LOM is een Nederlands profiel op de internationale standaard IEEE LOM (Learning Object Metadata). NL LOM is gemaakt voor de sectoren primair onderwijs, voortgezet onderwijs, middelbaar beroepsonderwijs en hoger onderwijs.

Onder aanbieders en afnemers van leermaterialen binnen het onderwijsveld is het gebruik van NL LOM zeer hoog. NL LOM kent geen gebruik buiten de onderwijssector. Een ontwikkeling in de tijd kunnen we met de beschikbare gegevens niet maken.

OAI-PMH

OAI-PMH is een standaard voor harvesting van metadata uit repositories. Een repository is een bibliotheek met documenten/objecten (ook wel 'content' genoemd), bijvoorbeeld een (digitaal) archief. OAI-PMH maakt het mogelijk om deze metadata (dus niet de documenten / objecten zelf) uit verschillende repositories te verzamelen. Vanuit een centraal systeem kan dan gezocht worden naar documenten/objecten in de verschillende aangesloten repositories.

Onder aanbieders en afnemers van leermaterialen binnen het onderwijsveld is het gebruik van OAI-PMH zeer hoog. OAI-PMH kent tevens een brede adoptie binnen de erfgoedsector. Een ontwikkeling in de tijd kunnen we met de beschikbare gegevens niet maken.

5.10. Domein Overig

EML_NL (Verkiezingsgegevens)

De EML_NL standaard versie 1.0 is het Nederlands toepassingsprofiel op de Election Markup Standard en 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.

De EML_NL wordt toegepast door alle gemeenten in Nederland.

STOSAG (afvalbranche)

Over het gebruik van deze standaard is geen bruikbare informatie beschikbaar.

Bijlagen

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)*	Het faciliteren van het vaststellen van organisatorische herkomst voor e-mail afkomstig van overheidsdomeinen, als deze over een onbeveiligde, publieke internetverbinding wordt verstuurd wanneer verdere authenticatie ontbreekt.	Overheden en instellingen uit de publieke sector.
DNSSEC RFC 4033, RFC 4034, RFC 4035 *(15 juni 2012)*	- Het registreren en in DNS publiceren van internet-domeinnamen ('signing'). De registratieverplichting geldt enkel indien 'signed domain names' bij een registerhouder van een top-level domein (zoals SIDN voor .NL) geautomatiseerd aangevraagd kunnen worden; - Het vertalen van domeinnamen naar internetadressen en vice versa ('validation enabled resolving'). Validatie is niet verplicht voor systemen die niet direct aan het publieke internet gekoppeld zijn (bijvoorbeeld clients/werkplekken binnen een LAN en interne DNS-systemen).	Overheden en instellingen uit de (semi-) publieke sector.
HTTPS en HSTS RFC 2818, RFC 6797 *(9 mei 2017)*	Het beveiligen van de communicatie tussen clients (zoals browsers) en servers voor alle via het Internet benaderbare websites en webservices. Voor webservices is het functioneel toepassingsgebied alleen van toepassing bij 'server to client'-interactie, niet voor 'server to server'-interactie.	Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.
IPv6 en IPv4 v4 en v6 *(25 november 2010)*	Voor de communicatie op netwerkniveau over organisatiegrenzen heen tussen organisaties, individuele eindgebruikers, apparaten, diensten en sensoren.	Overheden en instellingen uit de (semi) publieke sector.
NEN-ISO\IEC 27001 2013 *(18 mei 2015)*	Specificeren van eisen voor het vaststellen, implementeren, uitvoeren, bewaken, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie.	Overheden en instellingen uit de publieke sector.
NEN-ISO\IEC 27002 2013 *(18 mei 2015)*	De standaard omvat "best practices" op het gebied van het organiseren van informatiebeveiliging voor een organisatie, bestaande uit het beheer van bedrijfsmiddelen, veilig personeel, toegangsbeveiliging, cryptografie, fysieke beveiliging en beveiliging van de omgeving, beveiliging in de bedrijfsvoering, communicatiebeveiliging, leveranciersrelaties, beheer van informatiebeveiligingsincidenten, informatie-beveiligingsaspecten van bedrijfscontinuïteitsbeheer, naleving en de acquisitie, ontwikkeling en het onderhoud van informatiesystemen.	Overheden en instellingen uit de publieke sector.
SAML 2.0 *(20 mei 2009)*	Federatieve (web)browser-based single-sign-on (SSO) en single-sign-off. Dat wil zeggen dat een gebruiker na eenmalig inloggen via zijn browser toegang krijgt tot verschillende diensten van verschillende partijen.	Overheden en instellingen uit de publieke sector.
SPF RFC 7208 *(18 mei 2015)*	Het controleren of een e-mailserver gerechtigd is om namens een domeinnaam e-mail te mogen verzenden	Overheden en instellingen uit de publieke sector.
STARTTLS en DANE RFC 3207, RFC 7672 *(19 september 2016)*	Inkomende mailservers passen STARTTLS (SMTP over STARTTLS, oftewel ESMTPS) in combinatie met DANE toe, zodat verzendende mailservers daarmee een versleutelde verbinding over een onvertrouwd netwerk (zoals internet) kunnen opzetten. Dit voorkomt dat aanvallers het mailverkeer kunnen afluisteren (passieve aanvallers) en/of kunnen manipuleren (actieve aanvallers). Dit functioneel toepassingsgebied geldt voor alle mailverbindingen buiten de (interne) infrastructuur die onder eigen beheer valt.	Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-)publieke sector.
TLS 1.2, 1.1 en 1.0 *(16 september 2014)*	Het met behulp van certificaten beveiligen van de verbinding (op de transportlaag) tussen client- en serversystemen of tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internettechnologie.	Overheden (Rijk, provincies, gemeenten, en waterschappen) en instellingen uit de publieke sector.
WPA2 Enterprise versie 2 [802.11] *(2 februari 2016)*	Veilige, met behulp van een account geauthentiseerde toegang tot een wifi-netwerk van een (semi-) overheidsorganisatie. Toegang tot publieke wifi-netwerken van overheden voor gasten zonder account is uitgesloten van de verplichting	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 zijn van toepassing op documenten in de vorm van een XML-, PDF-, CMS-, en ZIP-bestand dat is voorzien van een geavanceerde en/of gekwalificeerde elektronische handtekening of zegel (inclusief tijdstempels).	Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.
CMIS 1.0 *(9 december 2014)*	Het toegankelijk maken van ongestructureerde gegevens in content repositories van Content Management Systemen (CMS) en Document Management Systemen (DMS) met als doel deze gegevens uit te wisselen met andere CMS en DMS systemen.	Overheden (Rijk, provincies, gemeenten en waterschappen) en overige instellingen uit de publieke sector.
Digitoegankelijk 1.1.2 *(19 oktober 2016)*	EN 301 549 is van toepassing op 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)*	Metadateren van publieke overheidsinformatie op internet.	Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.
PDF/A-1 NEN-ISO 19005-1:2005 *(15 juni 2012)*	Het uitwisselen en publiceren van niet- of beperkt-reviseerbare documenten, waarbij duurzame toegankelijkheid van belang is.	Overheden, semi-overheden en instellingen in de publieke sector.
PDF/A-2 ISO-19005-2 *(15 juni 2012)*	Het uitwisselen en publiceren van niet- of beperkt-reviseerbare documenten, waarbij duurzame toegankelijkheid van belang is en waarbij PDF/A-1 als standaard niet voldoet vanwege gebrek aan functionaliteit.	Overheden, semi-overheden en instellingen in de publieke sector.
PDF 1.7 ISO 32000-1:2008 *(18 november 2009)*	Het uitwisselen en publiceren van niet- of beperkt-reviseerbare documenten, waarbij duiding van oorsprong of functierijkheid onderdeel zijn van het document en waarbij PDF/A-1 als standaard niet kan worden ingezet.	Overheden en instellingen uit de (semi-) publieke sector.
SKOS SKOS W3C Recommandation 18 august 2009 *(18 mei 2015)*	Het in een gestructureerde vorm op het Web publiek beschikbaar stellen van een 'niet geformaliseerd' Knowledge Organization System (KOS), met als doel kennis over de betekenissen en samenhang van de onderliggende begrippen te ordenen en toegankelijk te maken.	Overheden en instellingen uit de publieke sector.
Stelselstandaarden		
Digikoppeling 2.0 *(17 juni 2013)*	Geautomatiseerde gegevensuitwisseling tussen informatiesystemen voor sectoroverstijgend berichtenverkeer, op basis van drie koppelvlakstandaarden: * DK ebMS standaard voor meldingen tussen informatiesystemen * DK WUS standaard voor de bevraging van informatiesystemen * DK GB standaard voor de uitwisseling van grote berichten	Overheden (Rijk, provincies, gemeenten, waterschappen) en instellingen uit de publieke sector. Het werkingsgebied van de standaard is bedoeld voor intersectoraal verkeer en verkeer met basisregistraties en kent geen verplichting binnen sectoren. Het Forum is wel van mening, dat gebruik binnen sectoren ook aanbevelens-waardig is en roept de beheerder van de standaard dan ook op dit gebruik te promoten.
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		
Semantisch model e-Factureren 2.0 *(15 november 2016)*	De verzending van elektronische facturen door organisaties die deelnemen aan het economisch verkeer in Nederland (waaronder overheden) en de ontvangst hiervan door overheden.	Overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit publieke sector. M.u.v. vertegenwoordigingen van

		de Nederlandse overheid in het buitenland.
SETU resp. 1.2, 1.2, 1.3, 1.3 *(februari 2015)*	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: Elektronisch verkeer dat te kenmerken is als verant-woordingsverkeer waarin financiële informatie de kern vormt. * Dimensions: Bij gebruikmaking van "contextuele informatie" binnen het voornoemde toepassingsgebied voor XBRL.	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 ontwikkelings-voortgang 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.
OAI–PMH 2.0 *(21 december 2010)*	Het vraaggestuurd aanbieden en ophalen van verzamelingen metadata uit bibliotheken met (digitale) documenten of andere objecten, met als doel het opnemen van deze metadata in een centrale bibliotheek. Uitgezonderd zijn die toepassingen waarvoor op basis van de lijst voor 'pas toe of leg uit' het gebruik van OSB (nu: Digikoppeling) verplicht is.	Overheden en instellingen uit de publieke sector.
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.
Water & bodem		
Aquo Standaard Aquo 2016-12 *(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 13.3.0 *(9 december 2014)*	Uitwisselen van onderzoeksgegevens over de milieu-hygiënische 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.	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, 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, 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, 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)*	De standaard moet ingezet worden voor: 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 digitale 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?

Een wettelijke verplichting gaat juridisch gezien in hiërarchie boven het 'pas toe of leg uit' beleid. Om hier geen misverstanden over te laten bestaan, staan er geen wettelijk verplichte open standaarden 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 ZBOs 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.

1. De benodigde documentatie moet laagdrempelig beschikbaar zijn.
2. Er mogen geen hindernissen zijn op het terrein van intellectueel eigendomsrecht.
3. Belanghebbenden moeten voldoende inspraakmogelijkheden hebben tijdens de (door)ontwikkeling van de standaard.
4. 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-mail adres 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.

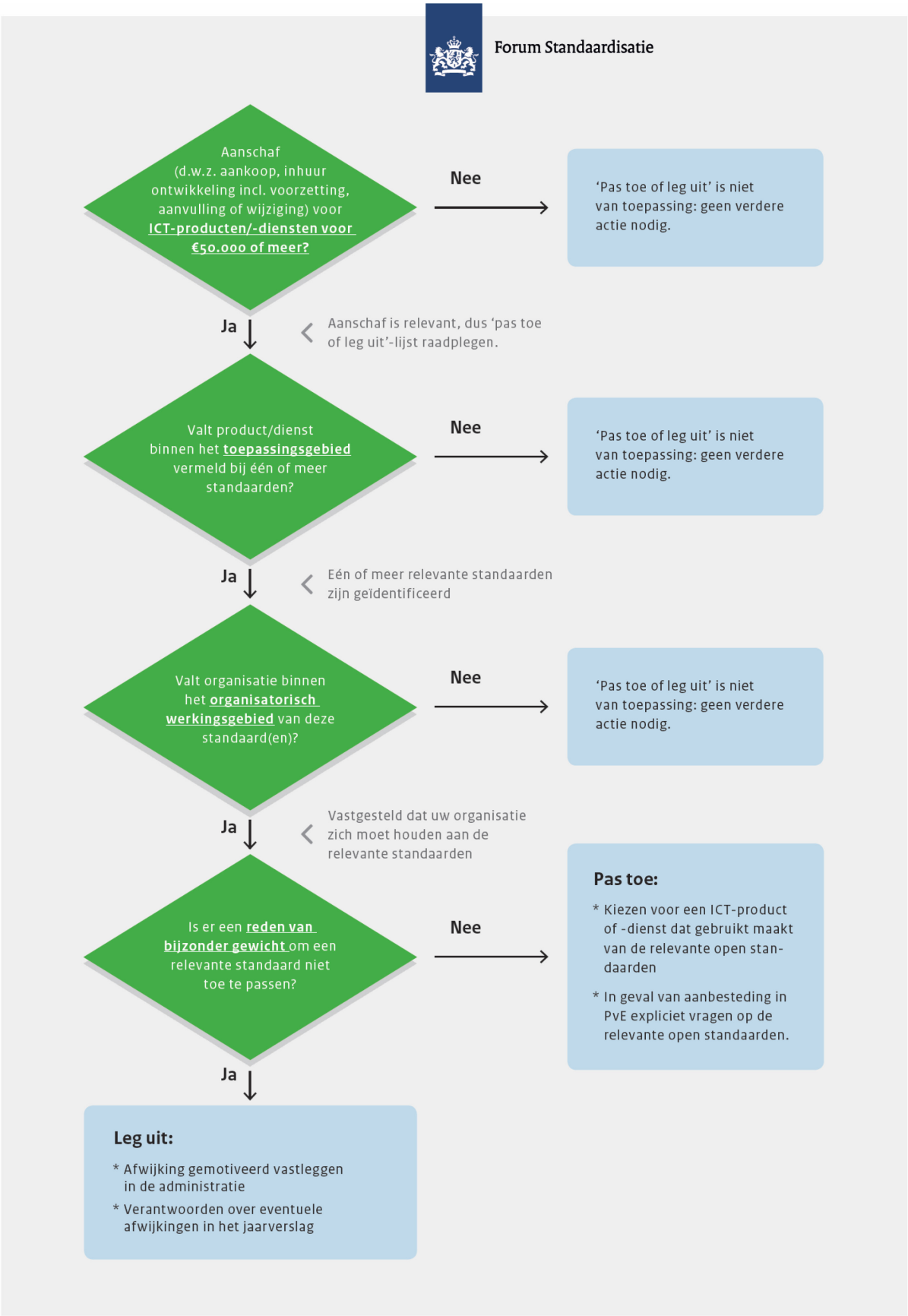
17. Waar kan ik hulp krijgen bij het uitvragen en toepassen van een standaard?

    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. Aanbestedingen: ervaringen met tweede beoordeling

In de onderzoeksopzet is net als vorig jaar plaats ingeruimd voor een tweede beoordeling voor een deel van de door dhr. Van den Berg en mw. Oosterheert beoordeelde aanbestedingen. Deze is verricht door dhr. Paapst in samenwerking met dhr. Wiersma. Het doel van deze tweede beoordeling was drieledig:

- een toets op de beoordeling van de 'eerste beoordelaar';
- eventuele aanscherping van het aanvankelijke oordeel op basis van onderlinge discussie tussen beide beoordelaars:
    - aanvullende standaarden worden als relevant benoemd of standaarden die aanvankelijk relevant werden geacht worden toch niet als relevant beoordeeld;
    - eventueel een andere conclusie over de vraag of er bij de aanbesteding om de relevante standaarden is gevraagd;
    - aanpassing van het eindoordeel, vooral vanwege beide voorgaande punten;
- zicht krijgen op de 'grijze gebieden' waarover de discussie gaat of kan gaan in de praktijk van aanbestedingen.

De beoordelaars hebben in het kader van de second opinion elk 42 aanbestedingen Rijk bestudeerd[27], onafhankelijk van elkaar bepaald welke standaarden in hun optiek relevant waren en op basis van de interpretatie van de uitvraag van standaarden door de aanbestedende partij een waarde-oordeel gegeven. Voorafgaand aan deze beoordeling zijn de gezamenlijke uitgangspunten voor de beoordelingen met elkaar te besproken en waar nodig aangescherpt.

Na de beoordeling in eerste aanleg zijn per aanbesteding de beide zienswijzen onderling uitgewisseld en uitgebreid besproken. Die gesprekken hebben plaatsgevonden in juni en augustus. De focus in die gesprekken lag logischerwijze op de punten waar de afzonderlijke beoordelingen een verschil lieten zien.

De beide beoordelaars hadden dit jaar aanvankelijk voor 26 van de 42 aanbestedingen een meer of minder verschillend oordeel. Dat is eenzelfde aandeel aanvankelijke verschillen als vorig jaar (16 van de 25 aanbestedingen). Daarvoor waren vier oorzaken:

- een andere inschatting of de aanbesteding (voldoende) beoordeelbaar is;
- een andere kijk op de relevantie van één of meer standaarden voor de aanbesteding;
- een andere conclusie over het vragen om de relevante standaarden;
- nuance-verschillen bij het toekennen van een waarde-oordeel.

De discussie tussen de beide beoordelaars leidde overigens voor alle aanbestedingen redelijk snel en eenduidig tot consensus over de uiteindelijke beoordeling. Sommige van de aanbestedingen door de eerste beoordelaar naar aanleiding van de discussie uiteindelijk 'hoger' beoordeeld (6) en een aantal andere juist lager (4). De meeste verschuivingen op de schaal van beoordelings-waarden waren marginaal.

[27] Dit zijn er meer dan het aantal uiteindelijke beoordeelde en gewaardeerde aanbestedingen (35). Gedurende het proces van (gezamenlijk) beoordelen is een aantal aanbestedingen afgevallen als zijnde niet beoordeelbaar.

Dat de experts aanvankelijk verschillend oordeelden lijkt een indicatie dat de lijst voor 'pas toe of leg uit' wellicht niet altijd eenvoudig of eenduidig toegepast kan worden op aanbestedingen. Voor functionarissen die slechts incidenteel bij aanbestedingen betrokken zijn zou het moeilijk kunnen zijn om de lijst voor 'pas toe of leg uit'goed in praktijk te brengen.

Gezien het bovenstaande heeft de tweede beoordeling zijn waarde bewezen. Uitwisseling van inzichten en ervaringen heeft ertoe geleid dat er consensus ontstond. Tijdens dat proces heeft de second opinion tot een aantal inhoudelijke discussies tussen de experts geleid die ook inzicht geven in mogelijke onduidelijkheden in de aanbestedingspraktijk bij – in dit geval – een overheidsinstelling[28].

[28] Er is ook op onderdelen discussie ontstaan over de inrichting en de vormgeving van de second opinion. Deze meer procesmatige aspecten passen niet in deze monitor maar worden meegenomen in geval er bij een eventuele volgende monitor weer wordt besloten tot een second opinion.

Bijlage E. Voorzieningen: rapport PBLQ met detail-informatie per voorziening

E.1. Inleiding

E.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.

E.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.

E.1.3 Werkwijze

Voor dit onderzoek is gebruik gemaakt van de 'pas toe of leg uit'-lijst van 16 juni 2017. 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 duidelijk aangegeven.

Op basis van publiek beschikbare informatie en kennis van experts en van de onderzoekers is een eerste inschatting gemaakt of de voorziening de standaard ook daadwerkelijk ondersteunt. Daarbij is ondermeer gebruik gemaakt van een aantal bronnen:

- https://internet.nl - test overzicht van overheidsvoorzieningen op IPv6, DNSSEC,TLS, DKIM en SPF
- Het website register van de Rijksoverheid (https://www.communicatierijk.nl/vakkennis/r/rijkswebsites-verplichte-richtlijnen/websiteregister)

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 daarvan is voorgelegd aan de opdrachtgever en vervolgens in een definitieve versie toegestuurd aan de vertegenwoordigers van de voorzieningen en opgenomen in de rapportage. 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 duidelijk opgenomen in de rapportage.

E.1.4 Aandachtspunten voor de lezer

Status
In de rapportage is per voorziening een tabel opgenomen. Daarin staan de standaarden genoemd die relevant zijn voor de voorzieningen. Daaraan is een status gekoppeld. Deze is door de onderzoekers toegekend. De status kan de volgende waarden hebben:

- Ja: De voorziening is conform[29] met de standaard,
- Nee: De voorziening is niet conform met de standaard,
- Deels: Onderdelen van de voorziening zijn conform maar niet alle onderdelen[30],
- Gepland: Er zijn concrete plannen (gekoppeld aan een datum) om de voorziening op korte termijn conform te maken met 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.[31] 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.

Webrichtlijnen en Digitoegankelijk
De Webrichtlijnenstandaard is het afgelopen jaar vervangen door de Digitoegankelijkstandaard. Het toepassingsgebied van Digitoegankelijk is (nog) niet veranderd ten opzichte van de Webrichtlijnen. Momenteel is het voornemen om wetgeving te introduceren, waarin de standaard verplicht wordt gesteld. Voorlopig geldt het pas-toe-of-leg-uit regime voor de standaard. BZK en Logius werken momenteel aan een nieuw model voor monitoring en rapportage, dat aansluit bij de verplichtingen die vanuit de Europese Unie voor deze standaard worden gesteld. In deze monitor zijn we, bij afwezigheid van een nieuwe toetsingssystematiek, nog uitgegaan van de systematiek voor Webrichtlijnen. Concreet: is er een toets uitgevoed en is er een onderbouwing in de vorm van een toetsrapport, 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:

[29] Met "conform" wordt in dit onderzoek bedoeld dat de standaard door de eindgebruiker te gebruiken is.
[30] 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.
[31] Zie: https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht

"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 partijen die versie 1.2 (nog) niet ondersteunen de score 'nee'.

Ondernemingsdossier/MijnOverheid voor Ondernemers
Het Ondernemingsdossier is per 1-8 niet meer in gebruik, en gaat vervangen worden door MijnOverheid voor Ondernemers. Deze nieuwe voorziening is vanaf eind 2017 in test en naar verwachting in 2018 operationeel. Daarom is deze voorziening dit jaar niet getoetst in dit onderzoek.

E.2. Gebruik standaarden per voorziening

E.2.1. BAG, BRK, WOZ en BGT

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.

Standaard	Status	Toelichting
Digikoppeling 2.0	Ja	Vrijwel alle koppelingen met afnemers, andere basisregistraties en evtl. 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.
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Ja	Het Kadaster voldeed vorig jaar al aan de Webrichtlijnen en heeft een toegankelijkheidsverklaring gepubliceerd op kadaster.nl.
DKIM	Ja	De implementatie van DKIM wordt is 8 september 2017 afgerond.
DNSSEC	Ja	De website www.kadaster.nl ondersteunt DNSSEC (zie https://internet.nl/domain/www.kadaster.nl/87074)
Geo-Standaarden	Ja	Naast de INSPIRE richtlijnen, maakt het Kadaster gebruik van NEN3610 en de meest gangbare Geo standaarden voor de betreffende basisregistraties.

HTTPS/HSTS	Gepland	HTTPS is correct geconfigureerd (en wordt afgedwongen) en alleen HSTS ontbreekt nog (zie https://internet.nl/domain/www.kadaster.nl/87074). Dit wordt na 8 september opgepakt, met verwachte implementatie per Q1 2018.
IPv4 en IPv6	Ja	Zowel IPv4 als IPv6 worden ondersteund door het Kadaster. (zie https://internet.nl/domain/www.kadaster.nl/87074)
NEN-ISO/IEC 27001/27002	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.
PDF 1.7, PDF/A-1 en PDF/A-2	Deels	Uittreksels worden verstrekt in PDF 1.4-formaat. Databestanden worden vooral in GML uitgewisseld. GML is een standaard XML-formaat voor Geo-data, gebaseerd op de Geo-standaarden. Afnemers melden geen problemen met het huidige PDF formaat. Daarom geeft het Kadaster geen prioriteit aan het vervangen van PDF 1.4. Voor het archiveren van kennisgevingen wordt gebruik gemaakt van PDF/A-1.
SKOS	Deels	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. Voor de WOZ moet deze slag nog worden gemaakt. (4 van de 5 BR's)
SPF	Ja	Is geïmplementeerd per 8 september. (zie https://internet.nl/mail/kadaster.nl/36502)
STARTTLS/DANE	Gepland	STARTTLS is geïmplementeerd, maar DANE wordt na 8 september opgepakt, met verwachte implementatie per Q1 2018. (zie https://internet.nl/domain/www.kadaster.nl/87074)
StUF	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.
TLS v1.2, v1.1 en v1.0.	Ja	Deze standaard wordt volledig door het Kadaster ondersteund. (zie https://internet.nl/domain/www.kadaster.nl/87074)

Ten opzichte van vorig jaar zijn er enkele ontwikkelingen te vermelden. Zo zijn DKIM, IPV4/IPv6, TLS en SPF inmiddels geïmplementeerd.

Een aantal standaarden zijn ten opzichte van het vorige onderzoek nieuw op de PTOLU lijst. Hiervan zijn STARTTLS/DANE en HTTPS/HSTS relevant, maar nog niet geïmplementeerd. Voor HTTPS/HSTS en STARTTLS/DANE bestaat wel een planning.

Concluderend, moeten voor deze voorziening nog de volgende standaarden (volledig) geïmplementeerd worden DANE, HSTS, PDF, en SKOS.

E.2.2. Berichtenbox voor bedrijven

Beheerorganisatie: Rijksdienst voor Ondernemend Nederland (RVO).

De Berichtenbox voor bedrijven is een beveiligd e-mailsysteem. Hiermee wisselen ondernemers digitaal berichten uit met overheidsorganisaties. 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
Digikoppeling 2.0	Ja	Overheden kunnen via Digikoppeling geautomatiseerd berichten verzenden en ontvangen. Ondernemers kunnen alleen handmatig (via de website) hun Berichtenbox gegevens opvragen.
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Nee	Dictu heeft een webrichtlijnen toets gedaan, zie meegezonden stuk. Een concrete planning is nog niet bekend.
DKIM	Nee	DKIM is niet geïmplementeerd (zie https://internet.nl/mail/berichtenbox.antwoordvoorbedrijven.nl/34865).[32]
DNSSEC	Ja	Volgens internet.nl voldoet het domein berichtenbox.antwoordvoorbedrijven.nl (zie https://internet.nl/mail/berichtenbox.antwoordvoorbedrijven.nl/34865).
HTTPS/HSTS	Nee	HTTPS is geïmplementeerd, maar HSTS wordt niet afgedwongen (zie https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/91865).
IPv4 en IPv6	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/91865). 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.
PDF 1.7, PDF A/1, PDF A/2	Ja	Alle berichten kunnen worden gedownload (vanaf de Berichtenbox website) in PDF/A formaat. PDF-documenten worden gegenereerd in PDF A/1.
SAML	Ja	eHerkenning is SAML-based en wordt toegepast voor het inloggen op de Berichtenbox.
SPF	Nee	SPF is niet geïmplementeerd (zie https://internet.nl/mail/berichtenbox.antwoordvoorbedrijven.nl/34865).[33]
STuF	Ja	Wordt in combinatie met Digikoppeling gebruikt voor de uitwisseling met alle partijen die via digikoppeling op de berichtenbox zijn aangesloten.
TLS v1.2, v1.1 en v1.	Ja	De Berichtenbox maakt gebruik van TLS (1.2, 1.1 en 1.0). Zie https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/87107.

Ten opzichte van het onderzoek uit 2016 zijn er een aantal ontwikkelingen. Bij de oude standaarden is DNSSEC van Nee naar Ja gegaan. Bij de standaarden DKIM en SPF geeft de test via internet.nl geeft aan dat er nog niet voldaan wordt aan de standaard. Bij de beheerorganisatie is nog onduidelijk wat de status is van de toepassing, en er kon in de looptijd van het onderzoek geen definitieve antwoord gegeven worden. Daarom is dit jaar ervoor gekozen om de test van internet.nl als leidend te hanteren.

Van de standaarden die dit jaar nieuw op de lijst staan, is alleen HTTPS/HSTS relevant. Hiervan moet HSTS nog geïmplementeerd worden. STARTTLS/DANE is niet relevant, omdat de Berichtenbox geen inkomend email heeft, alleen uitgaande email (bijvoorbeeld notificaties). De Berichtenbox zelf kan niet als email gezien worden. Toch wordt STARTTLS door de Berichtenbox gebruikt (DANE wordt niet gebruikt, omdat de DNS van de Berichtenbox hiervoor eerst ge-upgraded worden voordat een DANE record toegevoegd kan worden).

[32] Bij de beheerorganisatie is nog onduidelijk wat de status van deze standaard moet zijn. Voor deze reden is in de rapportage de zichtwijze op basis van de internet.nl toets gehanteerd.
[33] Idem.

Concluderend, moet deze voorziening nog de volgende standaarden implementeren: Digitoegankelijk, DKIM, HSTS, IPv4 en IPv6, en SPF.

E.2.3. BRI

Beheerorganisatie: Belastingdienst

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.

Let op: binnen het beschikbare tijdsbestek voor deze opdracht is het niet gelukt een bevestiging te krijgen van de Belastingdienst op deze inschatting. Met de Belastingdienst is afgesproken dat de inschatting van de onderzoekers opgenomen wordt.

Standaard	Status	Toelichting
Digikoppeling 2.0	Ja	Digikoppeling wordt toegepast in de rol van afnemer van berichten van basisregistraties(HR). De ebms-koppeling met Digilevering is operationeel in de produktie-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 vorig jaar niet eerder dan 2017-2018 gepland.
NEN-ISO/IEC 27001/27002	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.	Ja	De actuele versies van TLS maken deel uit van de standaard beveiligingsrichtlijnen van de Belastingdienst.
WPA2 Enterprise	Ja	WPA2 wordt toegepast door de Belastingdienst.

Ten opzichte van vorig jaar zijn er de volgende wijzigingen: SKOS en CMIS worden dit jaar niet meer als relevant gezien voor deze voorziening. Verder staan een aantal nieuwe standaarden op de lijst: Ades Baseline Profiles, Digitoegankelijk, HTTPS/HSTS, en STARTTLS/DANE. Echter, volgens onze inschatting is deze standaard niet relevant binnen de scope van deze voorziening.

E.2.4. BRT

Beheerorganisatie: Kadaster

De Basis Registratie Topografie (BRT) wordt beheerd door het Kadaster. De BRT bestaat uit digitale topografische bestanden op verschillende schaalniveaus. Deze verzameling topografische bestanden is beschikbaar als open data. Dat betekent dat het Kadaster deze gegevensbestanden kosteloos en met minimale leveringsvoorwaarden ter beschikking stelt. Voor het uitwisselen van gegevens gebaseerd op een geografische ondergrond zijn alle overheidsorganisaties verplicht gebruik te maken van gegevens uit de BRT, als deze gegevens beschikbaar zijn.

Standaard	Status	Toelichting
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Ja	Het Kadaster voldeed al aan de Webrichtlijnen en heeft daarnaast een toegankelijkheidsverklaring gepubliceerd op kadaster.nl, waarin zij verklaart z.s.m. te willen voldoen aan Digitoegankelijk.
Geo-Standaarden	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).
HTTPS/HSTS	Gepland	HTTPS wordt al toegepast, HSTS nog niet (zie https://internet.nl/domain/www.kadaster.nl/87074). Dit wordt na 8 september 2017 opgepakt, met verwachte implementatie per Q1 2018.
NEN-ISO/IEC 27001/27002	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.
OWMS	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	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.
STARTTLS/DANE	Gepland	STARTTLS is al geïmplementeerd (zie https://internet.nl/domain/www.kadaster.nl/87074). DANE zal na 8 september opgepakt worden, met verwachte implementatie per Q1 2018.
TLS v1.2, v1.1 en v1.	Ja	Deze standaard wordt volledig door het Kadaster ondersteund (zie https://internet.nl/domain/www.kadaster.nl/87074)

Ten opzichte van het onderzoek van vorig jaar zijn er geen wijzigingen. Wel zijn er een aantal nieuwe standaarden op de lijst, waarvan HTTPS/HSTS en STARTTLS/DANE relevant zijn. STARTTLS is al geïmplementeerd, maar HTTPS/HSTS en DANE zullen na 8 september 2017 opgepakt worden.

Concluderend, moet deze voorziening nog volgende standaarden (volledig) implementeren: HTTPS/HSTS, DANE, en OWMS.

E.2.5. BRV

Beheerorganisatie: RDW (Rijksdienst Wegverkeer)

In de Basisregistratie Voertuigen (BRV) worden gegevens vastgelegd over gekentekende voertuigen en de eigenaren en/of houders van deze voertuigen. Uit de registratie verstrekt de RDW gegevens aan overheden, burgers, bedrijven en andere belanghebbenden.

Standaard	Status	Toelichting
CMIS	Nee	RDW doet aan verschillende vormen van document management. De RDW consolideert daarvoor op het Sharepoint platform. Dat platform kan CMIS ondersteunen, maar het staat per default uit. Er is op dit moment geen aanleiding, zowel intern als extern, om CMIS toe te passen.
Digikoppeling 2.0	Deels	RDW maakt voor alle nieuwe uitwisselingen gebruik van Digikoppeling. Dat is onder meer het geval in de uitwisseling met MijnOverheid (Berichtenbox), CJIB, Politie, ILT, CBR, de Belastingdienst, etc.
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Deels	De RDW heeft de toegankelijkheidsverklaring op de site geplaatst. Zie: https://www.rdw.nl/overrdw/Paginas/Toegankelijkheidsverklaring.aspx?path=Portal/Over RDW/Kwaliteit. De website van de RDW voldoet nog niet volledig aan Digitoegankelijk. Wel loopt een project voor volledige herbouw van RDW.nl. Hierin is aandacht voor Digitoegankelijk. Wanneer de site wordt opgeleverd zal een audit hierop worden gedaan.
DNSSEC	Ja	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. Alle overige domeinen (.eu, .info, .com) staan binnen het programma RIT op de planning voor eind 2017, maar maken geen deel uit van de BRV.
HTTPS en HSTS	Gepland	HSTS gaat Fujitsu activeren voor de HTTPS ingangen die onderdeel zijn van de nieuwe werkplek omgeving. Voor de RDW diensten omgeving wordt HSTS geactiveerd bij de overgang van TMG naar F5. Dit wordt voor 1 juli 2018 gerealiseerd.
IPv4 en IPv6	Nee	IPv4 wordt gesupport, 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	Ja	RDW is ISO 27001/2 gecertificeerd. RDW voldoet niet aan alle extra voorschriften van de BIR, dat hoeft ook niet want RDW is gehouden aan de VIR (en met auditor is afgesproken dat voldoen aan de 27001/27002 norm gelijk staat aan voldoen aan de VIR). Er is een in control statement van de 27001/27002 en de BKR-audit.
OWMS	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	Ja	Bij digitale dienstverlening worden uittreksels en informatie uit de BRV in PDF/A vorm verstrekt.
SAML	Ja	Op 4 juli 2017 is de SAML2.0 koppeling actief geworden.
SKOS	Ja	Socrata verzorgt de open data omgeving van de RDW (https://opendata.rdw.nl/browse). Het RDF-XML formaat wordt ondersteund en de beheerder geeft aan dat zeer waarschijnlijk ook de SKOS standaard wordt ondersteund.
SPF	Ja	RDW ondersteunt en gebruikt de SPF standaard voor email verkeer.
STARTTLS en DANE	Gepland	STARTTLS, DANE, DKIM en SPF wordt bij de overgang naar Fujitsu voor alle DNS domeinen geïmplementeerd. Dit wordt voor 1 juli 2018 gerealiseerd.
TLS v1.2, v1.1 en v1.	Ja	RDW ondersteunt en gebruikt de TLS protocollen op de e-mail servers en Digikoppeling.

Ten opzichte van het onderzoek uit 2016 zijn er enkele ontwikkelingen. SAML was vorig jaar nog alleen in SAML 1.1 geïmplementeerd, maar sinds juli 2017 is versie 2.0 geïmplementeerd. Digitoegankelijk (vorig jaar nog Webrichtlijnen) staat nog steeds op status "Deels", maar er loopt inmiddels een project voor de herbouw van rdw.nl, waarin ook aandacht voor

Digitoegankelijk besteed zal worden. De SKOS standaard is dit jaar geïmplementeerd door het RDF-XML formaat te ondersteunen. Inmiddels is ook de TLS standaard toegepast op rdw.nl.

Van de standaarden die dit jaar nieuw op de lijst staan zijn HTTPS/HSTS, en STARTTLS/DANE relevant voor de voorziening. De voorzieningen voldoet nog niet aan deze standaarden, maar voor de eerste twee is de implementatie wel gepland.

Concluderend voor deze voorziening, moeten de volgende standaarden nog (volledig) geïmplementeerd worden: CMIS, Digikoppeling, Digitoegankelijk, HTTPS en HSTS, IPv4 en IPv6, STARTTLS en DANE.

E.2.6. BSN Beheervoorziening en GBA-V

Beheerorganisatie: Rijksdienst voor Identiteitsgegevens (RvIG), Ministerie BZK

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

Standaard	Status	Toelichting
Digikoppeling 2.0	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 worden richting gemeenten en afnemers gecommuniceerd.
HTTPS/HSTS	Ja	Alle aangeboden webservices draaien HTTPS en HSTS.
IPv4 en IPV6	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	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.
StUF	Nee	De voorziening spreekt de WSI standaard XML/SOAP met haar gebruikers. Er is geen concrete planning voor de invoering van StUF.
TLS v1.2, v1.1 en v1.0	Ja	De voorziening ondersteunt zowel TLS 1.2, 1.1 als 1.0.

Ten opzichte van het onderzoek uit 2016 zijn er enkele veranderingen. Digikoppeling is van Gepland naar Nee gegaan. Daarnaast zijn een aantal standaarden ten opzichte van het vorige onderzoek nieuw op de PTOLU lijst, waaronder de HTTPS/HSTS standaard die relevant voor de voorziening is en inmiddels ook geïmplementeerd.

Concluderend voor deze voorziening, moeten de volgende standaarden nog (volledig) geïmplementeerd worden: Digikoppeling 2.0, IPv4 en IPV6, en StUF.

E.2.7. 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
DNSSEC	Ja	Digi-Inkoop voldoet aan DNSSEC (zie https://internet.nl/mail/digiinkoop.nl/36515).
HTTPS/HSTS	Nee	De voorziening voldoet aan HTTPS, maar niet aan HSTS[34]. Hiervoor bestaat nog geen planning.
IPv4 en IPV6	Nee	IPv6 werd vorig jaar 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 ook https://internet.nl/mail/digiinkoop.nl/36515)
NEN-ISO/IEC 27001/27002	Ja	Digi-Inkoop voldoet aan de BIR. Er is een in control statement afgegeven. Leveranciers voldoen aan ISO 27001.
PDF/A en PDF 1.7	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 berichtenverkeer-standaarden 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).
SETU	Ja	Digi-Inkoop ondersteunt de uitwisseling van SETU-hr-XML berichten
SMeF 2.0	Nee	Digi-Inkoop gebruikt de OHNL standaard voor berichtenuitwisseling en voldoet daarmee aan SMeF 1.3. Digi-Inkoop maakt gebruik van de specificaties van het semantisch model. Echter, er is geen opdracht om een upgrade naar 2.0 uit te voeren.
SPF	Nee	Digi-Inkoop voldoet nog niet aan deze standaard, en er bestaan op dit moment ook nog geen plannen om dit in de toekomst te implementeren. Digiinkoop.nl is alleen een applicatie domein, er wordt niet gemaild vanaf dit domein.
TLS v1.2, v1.1 en v1.0	Ja	Digi-Inkoop is 1.2 compliant (zie https://internet.nl/mail/digiinkoop.nl/36515).

Ten opzichte van het onderzoek uit 2016 zijn er enkele ontwikkelingen. Vorig jaar werd gemeld dat de voorziening voldeed aan SMEF, door het update van de versie van de standaard naar 2.0 voldoet de voorziening echter niet meer hieraan. Wel voldoet de voorziening inmiddels aan TLS v1.2.

Van de standaarden die dit jaar nieuw op de lijst staan is alleen HTTPS en HSTS relevant. De voorziening voldoet wel aan HTTPS, maar niet aan HSTS (hiervoor bestaan ook nog geen plannen).

Concluderend voor Digi Inkoop, moeten de volgende standaarden nog geïmplementeerd worden: HSTS, IPv4 en IPV6, en SMeF 2.0.

[34] Volgens https://internet.nl/mail/digiinkoop.nl/36515 voldoet de voorziening naast HTTPS ook wel aan HSTS.

E.2.8. DigiD

Beheerorganisatie: Logius

DigiD is de generieke identificatievoorziening voor burgers voor de dienstverlening van de overheid. DigiD wordt beheerd door Logius. De huidige versienummer van DigiD is 5.3.

Standaard	Status	Toelichting
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Ja	Als overgangsperiode voldoet DigiD nu nog aan de Webrichtlijnen, een externe toets ten behoeve hiervan heeft plaatsgevonden (https://www.accessibility.nl/ondersteuning/inspectie/site-981 en https://www.digid.nl/help). Echter, tijdens dit onderzoek vond er een toets plaats WCAG2.0 AA t.b.v. de nog op te stellen Digitoegankelijk verklaring.
DKIM	Ja	DigiD mail wordt verstuurd met een DKIM signature (zie https://internet.nl/mail/digid.nl/34847).
DNSSEC	Ja	DNSSEC is doorgevoerd in release 4.5 van DigiD en inmiddels operationeel. Ook de mailservers voldoen aan de standaard (zie https://internet.nl/domain/digid.nl/87081).
HTTPS en HSTS	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/domain/digid.nl/87081).
IPv4 en IPv6	Ja	De website DigiD.nl is via IPv6 toegankelijk. Inmiddels verlopen ook de mailstromen via IPv6 (zie https://www.internet.nl/mail/digid.nl/17054).
NEN-ISO/IEC 27001/27002	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Rijk (BIR) van toepassing die is gebaseerd op NEN-ISO27001. Logius heeft zich over toepassing van deze norm verantwoord door het afgeven van In Control Verklaringen (ICV's) aan de eigenaar (BZK/DGOBR).
SAML	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	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/34847)
STARTTLS/DANE	Ja	De mailserver van DigiD passen STARTTLS en DANE toe (zie https://www.internet.nl/mail/digid.nl/41975).
TLS	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.

Ten opzichte van vorig jaar zijn er een aantal ontwikkelingen. DNSSEC en IPv4/IPv6 zijn van Deels naar Ja gegaan. De Digikoppeling en SKOS standaarden worden niet relevant gezien voor DigiD, en staan daarom niet meer in de tabel. Van de nieuw aan de lijst toegevoegde standaarden zijn HTTPS/HSTS en STARTTLS/DANE relevant voor DigiD. Aan HTTPS/HSTS zowel als aan STARTTLS/DANE wordt voldaan.

Concluderend, worden bij deze voorziening alle relevanten standaarden toegepast.

E.2.9. DigiD Machtigen

Beheerorganisatie: Logius

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. De huidige versie van DigiD Machtigen is 4.10

Standaard	Status	Toelichting
Digikoppeling 2.0	Deels	Het huidige PBS koppelvlak kan niet zomaar Digikoppeling compliant gemaakt worden, onder andere omdat er klanten op zijn aangesloten. De insteek van Logius is dat nieuwe koppelvlakken zoals het DVS of nieuwe versies van koppelvlakken Digikoppeling compliant worden uitgevoerd, en dat reeds aangesloten partijen overgaan naar deze koppelvlakken. Het huidige PBS koppelvlak stamt nog uit de tijd dat de Digikoppeling standaard in ontwikkeling was, en voldoet deels aan de uiteindelijke ontstane Digikoppeling standaard. Een nieuwe versie van het PBS koppelvlak is nog niet ontwikkeld maar zal Digikoppeling compliant uitgevoerd worden.
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Nee	De voorziening voldoet nu niet aan deze standaard. Bij de laatste test in 2016 zijn enkele bevindingen geconstateerd (mede als gevolg van een andere interpretatie van enkele normen).
DNSSEC	Ja	Volgens internet.nl voldoet het domein https://machtigen.digid.nl aan DNSSEC (zie https://internet.nl/site/machtigen.digid.nl/91888).
HTTPS/HSTS	Ja	Deze standaarden zijn geimplementeerd (zie https://internet.nl/site/machtigen.digid.nl/91888).
IPv4 en IPV6	Ja	Zowel IPv6 als IPv4 worden ondersteund (zie https://internet.nl/site/machtigen.digid.nl/91888).
NEN-ISO/IEC 27001/27002	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Rijk (BIR) van toepassing die is gebaseerd op NEN-ISO27001. Logius heeft zich over toepassing van deze norm verantwoord door het afgeven van In Control Verklaringen (ICV's) aan de eigenaar (BZK/DGOBR).
PDF/A en PDF 1.7	Ja	De voorziening voldoet aan deze standaard.
SAML v2.0	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. Wanneer er meer duidelijkheid komt over eID wordt een keuze gemaakt over de implementatie van SAML. Logius gaat die keuze nu nog niet maken om desinvesteringen tegen te gaan. Naast authenticatie gebruikt DigiD Machtigen de SAML standaard ook om een getekend machtigingsbewijs af te geven, namelijk als een SAML assertion.
SPF	Ja	De voorziening voldoet aan deze standaard, zie ook de toelichting bij DigiD.
TLS v1.2, v1.1 en v1.0	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. Tijdens dit onderzoek is DDM aangepast zodat de site ook compliant is met de alle eisen die door de toets via internet.nl gehanteerd worden.

Ten opzichte van vorig jaar zijn er een aantal ontwikkelingen. De voorziening voldoet dit jaar niet aan de Digitoegankelijk en/of de Webrichtlijnen standaard omdat in de laatste toets nog een aantal onvolkomenheden geregistreerd zijn die nog niet opgelost zijn.

Ook zijn er een aantal nieuwe standaarden op de lisjt ten opzichte van vorig jaar. Hiervan is HTTPS/HSTS relevant, en de voorziening voldoet hier ook aan.

Concluderend, moet DigiD Machtigen nog volgende standaarden (volledig) implementeren: Digitoegankelijk, en Digikoppeling, en SAML v2.0.

E.2.10. Digilevering

Beheerorganisatie: Logius

Digilevering is een generieke abonnementenvoorziening voor het verstrekken van gebeurtenisberichten. Aangesloten basisregistraties kunnen in Digilevering abonnementen voor hun afnemers vastleggen om hen op de hoogte te houden van wijzigingen.

Standaard	Status	Toelichting
Digikoppeling 2.0	Ja	Digilevering maakt gebruik van Digikoppeling
DKIM[35]	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.
DNSSEC[36]	Ja	DNSSEC is geïmplementeerd op de centrale voorziening DNS.
HTTPS/HSTS[37]	Ja	Digilevering voldoet aan de HTTPS standaard. Aan HSTS wordt niet voldaan.
IPv4 en IPv6	Nee	Digilevering gebruikt het Logius infrastructuur platform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik. Digilevering ondersteunt op dit moment alleen IPv4.
SPF[38]	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[39]	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

[35] 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.
[36] idem
[37] idem
[38] idem
[39] idem

	spam/malware verstuurder wordt aan-gemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen.

Ten opzichte van het onderzoek uit 2016 zijn er een aantal ontwikkelingen: DKIM, DNSSEC, IPv4/IPv6 zijn inmiddels geïmplementeerd. Daarnaast is SPF van Nee naar Ja gegaan.

Ook zijn er een aantal standaarden nieuw op de lijst. Hiervan zijn alleen de STARTTLS/DANE en HTTPS/HSTS relevant voor Digilevering. Beide standaarden worden toegepast (behalve HSTS).

Concluderend, is er voor deze voorziening maar één standaard die nog toegepast moet worden, de HSTS standaard.

E.2.11. Digimelding

Beheerorganisatie: Logius

Met Digimelding kunnen overheden bij gerede twijfel vermeende onjuistheden in de gegevens van Basisregistraties uniform en efficiënt terugmelden aan de bronhouders van die Basisregistraties.

Standaard	Status	Toelichting
Digikoppeling 2.0	Ja	Digimelding maakt gebruik van Digikoppeling
DKIM[40]	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.
DNSSEC[41]	Ja	DNSSEC is geïmplementeerd op de centrale voorziening DNS.
HTTPS/HSTS[42]	Ja	Digilevering voldoet aan de HTTPS standaard. HSTS wordt niet toegepast.
IPv4 en IPv6	Nee	Digimelding gebruikt het Logius infrastructuur platform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik. Digimelding ondersteunt op dit moment alleen IPv4.
SPF[43]	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[44]	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.

[40] idem
[41] idem
[42] idem
[43] idem
[44] idem

Ten opzichte van de Monitor van 2016 zijn een aantal dingen veranderd. Zo voldoet Digimelding inmiddels aan de standaarden DKIM, DNSSEC, IPv4/IPv6, en SPF.

Van de standaarden die dit jaar nieuw op de lijst staan, zijn HTTPS/HSTS en STARTTLS/DANE relevant. De laatste wordt volledig toegepast door de voorziening, maar bij de eerste wordt alleen HTTPS toegepast.

Concluderend, moet bij deze voorziening alleen nog HSTS geïmplementeerd worden.

E.2.12. 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
DNSSEC	Ja	DNSSEC validatie wordt toegepast op Rijks-DNS.
IPv4 en IPV6	Nee	Binnen Diginetwerk wordt alleen IPv4 gebruikt, binnen het nummerplan is voldoende IPv4 ruimte beschikbaar. Er zijn geen specifieke plannen voor IPv6, maar er is een beleidsvoorstel om in tijdsperiode 2017/2018 plannen te gaan ontwikkelen.
NEN-ISO/IEC 27001/27002	Ja	Deze standaard is onderdeel van het algemene beveiligingsbeleid van Logius. Logius voldoet aan deze standaard en Diginetwerk is ook gebaseerd op deze standaard.
STARTTLS/DANE	Gepland	Om STARTTLS/DANE op Diginetwerk te kunnen faciliteren dient de RijksDNS het DANE TLSA-record te ondersteunen. Dat is op dit moment nog niet het geval, maar ondersteuning voor het TLSA-record zal in 2017 gerealiseerd worden. Het gebruik van de standaard STARTTLS/DANE wordt bepaald door de toepassingen en niet door Diginetwerk.

Sinds het onderzoek van vorig jaar is er een nieuwe ontwikkeling, namelijk is van de standaarden die nieuw op de lijst staan, de STARTTLS/DANE relevant. Deze standaard is nog niet geïmplementeerd, maar zal dat voor het eind van het jaar nog zijn.

Concluderend, moeten bij Diginetwerk nog de IPv6 standaard en het faciliteren van de STARTTLS/DANE standaard geïmplementeerd worden.

E.2.13. 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 zijn is deze voorziening niet getoetst met de toetsen van internet.nl.

Standaard	Status	Toelichting
Digikoppeling	Ja	Zie de koppelvlakspecificaties op http://www.logius.nl/producten/gegevensuitwisseling/digitpoort/koppelvlakken
DKIM	Ja	DigiPoort voldoet aan DKIM. Dit is ook relevant omdat de voorziening een SMTP koppelvlak heeft.
DNSSEC	Nee	Hoewel DigiPoort werkt met PKI certificaten ter authenticatie, zou DNSSEC ook ingericht moeten zijn. Er zijn geen plannen om dit in te richten, omdat de voorziening geen businesscase hiervoor ziet omdat het risico nihil is.
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 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	Nee	Digipoort gebruikt het Logius infrastructuur platform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik. Digipoort ondersteunt IPv4
NEN-ISO/IEC 27001/27002	Ja	DigiPoort voldoet aan de BIR. Leveranciers voldoen aan ISO 27001 of vergelijkbare standaard.
SETU	Ja	DigiPoort ondersteunt de uitwisseling van SETU-hr-XML berichten
SPF	Nee	DigiPoort heeft geen SPF-records. Er wordt niet gemaild vanuit dit domein, maar SPF zou wel ingericht moeten worden. Er wordt op dit moment naar gekeken, maar er liggen nog geen formele plannen deze stap te maken.
STARTTLS/DANE	Ja	Zowel STARTTLS als DANE zijn beide ingericht.
TLS v1.2, v1.1 en v1.	Ja	Digipoort ondersteunt v1.2, maar niet meer de verouderde versies.
XBRL en Dimensions	Ja	Wordt ondersteund door Digipoort.

Ten opzichte van vorig jaar zijn er een aantal ontwikkelingen geweest. Toen was de voorziening nog opgesplitst in DigiPoort/OTP en Digipoort/PI. Inmiddels is DigiPoort/OTP gemigreerd naar Digipoort/PI en bestaat dus niet meer als separate voorziening. Verder wijst een vergelijking van bovenstaande tabel met die van Digipoort / PI van vorig jaar uit dat er voor de meeste 'oude' standaarden geen wijzigingen zijn als het om de status gaat. Uitzondering daarop is IPv6. Daarvoor is vorig jaar aangegeven dat dit jaar de migratie naar de nieuwe Logius infrastructuur plaats zou vinden en dat daarmee aan IPv6 voldaan zou worden. De beoogde migratie heeft plaatsgevonden, maar dat heeft er nog niet toe geleid dat IPv6 ondersteund wordt. Er is nog geen concrete planning afgegeven dus dit jaar is de status van Gepland in Nee veranderd.

Ook staan dit jaar een aantal nieuwe standaarden op de lijst. Hiervan zijn HTTPS en HSTS relevant, waarbij er aan HTTPS formeel wordt voldaan en aan HSTS alleen maar impliciet. Daarnaast zijn ook STARTTLS en DANE nieuw op de lijst. Howel deze standarden niet in het functionele toepassingsgebeid van de voorziening vallen, worden ze beide toegepast door de voorziening.

Concluderend, voor deze voorziening moeten nog de volgende standaarden geïmplementeerd worden: IPv6, DNSSEC en SPF.

E.2.14. Digitale Werkomgeving Rijksdienst (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 de DWR-werkomgeving. De nieuwe digitale werkomgeving bestaat uit verschillende onderdelen voor infrastructuur en connectiviteit. De drie belangrijkste zijn de uniforme digitale werkomgeving voor alle ambtenaren (DWR Next client), één website voor alle 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.

Standaard	Status	Toelichting
Ades Baseline Profiles	Deels	SSC-ICT is in staat om dit te leveren waar het door een afnemer gevraagd wordt. Voor een aantal klanten wordt dit geleverd.
Digikoppeling 2.0	Deels	Binnen VenJ vindt elektronisch berichtenverkeer interdepartementaal plaats via de Justitie Berichten Service (JUBES). JUBES is vanuit VenJ het koppelvlak voor de Digikoppeling dienst van Logius. De open standaarden eBMS en WUS zijn de daarbij gebruikte protocollen om de berichten veilig te versturen. Verder nemen alle departementen uit het verzorgingsgebied van SSC-ICT deel aan eFacturatie.
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 eigenaar van alle websites van haar klanten, bij deze websites ligt de verantwoordelijkheid bij de klant zelf.
DKIM	Deels	DKIM is geïmplementeerd voor 72 van de 90 domeinen die SSC-ICT in beheer heeft. Het is geïmplementeerd in combinatie met SPF en DMARC (DMARC is begin 2015 aangemeld voor opname op de pas-toe-of-leg-uit-lijst).
DNSSEC	Deels	De domeinen van de klanten van SSC-ICT die via de DNS van AZ lopen, voldoen. De domeinen van de klanten van SSC-ICT die via de DNS van SSC-ICT lopen, voldoen eind 2017. SSC-ICT geeft aan dat de cliënt DNSSEC-validatie ondersteunt, en dat RijksDNS DNSSEC-validatie ondersteunt.
HTTPS/HSTS	Deels	HTTPS wordt gebruikt, maar HSTS wordt niet standaard aangezet voor websites die SSC-ICT host voor klanten. Andere webgebaseerde voorzieningen maken wel gebruik van HSTS.
IPv4 en IPV6	Deels	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. Het is de bedoeling dat de internet facing kant van de DMZ IPv6 gaat ondersteunen, maar een concrete tijdlijn staat nog niet vast.
NEN-ISO/IEC 27001/27002	Ja	DWR voldoet aan de BIR en wordt hier ook op ge-audit. De laatste audit heeft plaatsgevonden in de periode 2015/2016.
ODF 1.2	Ja	De DWR Next client wordt geleverd met zowel Libreoffice 5.0 als Office 2016. Beide softwaresuites ondersteunen het lezen en schrijven van ODF bestanden.
PDF 1.7 / PDF A/1 en PDF A/2	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.
SAML	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	Deels	SPF wordt op 72 van de 90 domeinen toegepast.
STARTTLS/DANE	Nee	De internet mailvoorziening werkt met STARTTLS. Implementatie van onder meer DANE is in onderzoek in het verlengde van het initiatief 'Veilige E-mail Coalitie'. DANE wordt niet meer in 2017 geimplementeerd, maar waarschijnlijk pas in 2018.
TLS v1.2, v1.1 en v1.0	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	Ja	Op de wifivoorziening van DWR wordt deze standaard toegepast. Dit is een kantoorvoorziening.

Ten opzichte van de Monitor 2016 zijn enkele ontwikkelingen te benoemen. Zo is de status van IPv4/IPv6 gewijzigd van 'Nee' naar 'Deels'. Digitoegankelijk kent een ontwikkeling in de andere richting, waar de status nu op 'Deels' staat.

Ook zijn er een aantal standaarden nieuw op de lijst. Hiervan is Ades Baseline relevant en wordt toegepast waar het expliciet door een klant gevraagd wordt, maar niet overal. Hetzelfde geldt voor HTTPS/HSTS, waarbij HTTPS overal toegepast wordt, maar HSTS alleen bij sommige webgebaseerde voorzieningen. Ook STARTTLS/DANE is relevant en STARTTLS wordt in de internet mailvoorziening ook toegepast, maar voor de toepassing van DANE loopt nog een onderzoek.

Concluderen, moeten bij deze voorziening nog een aantal standaarden (volledig) geïmplementeerd worden: Ades Baseline Profiles, Digikoppeling, DKIM, Digitoegankelijk, DNSSEC, HSTS, IPv4 en IPV6 , SPF , en STARTTLS/DANE.

E.2.15. 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
Ades Baseline Profiles	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 2018 bekend.
CMIS	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.
Digikoppeling 2.0	Nee	Op dit moment wordt geen gebruik gemaakt van Digikoppeling
DKIM	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.
HTTPS/HSTS	Nee	Ook hierover loopt een onderzoek over de mogelijke toepassing van deze standaard in de toekomst. De uitkomsten daarvan zijn naar verwachting in het eerste kwartaal van 2018 bekend.
IPv4 en IPv6	Nee	De Haagse ring, waarover praktisch al het verkeer naar de Doc-Direkt voorzieningen loopt, ondersteunt geen IPv6. Het is bij Doc-Direkt niet bekend wanneer IPv6 gebruikt gaat worden. De beheerder van de Haagse Ring is Logius. De Haagse Ring is onderdeel van Diginetwerk. Binnen Diginetwerk wordt alleen IPv4 gebruikt, binnen het nummerplan is nu nog voldoende IPv4 ruimte beschikbaar.

NEN-ISO/IEC 27001/27002	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.
ODF	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	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.
SAML	Ja	Via de werkplek DWR kunnen medewerkers via SSO inloggen op de door Doc-Direkt beheerde DMS applicatie.
SKOS	Nee	SKOS wordt op dit moment niet toegepast. Er zijn nog geen plannen bekend of en wanneer SKOS geïmplementeerd zal worden.
SPF	Nee	Ook SPF wordt op dit moment niet toegepast, en het is nog niet bekend of en wanneer SPF geïmplementeerd zal worden.
TLS v1.2, v1.1 en v1.0	Nee	Het is bij Doc-Direkt niet bekend of TLS van toepassing is en daarmee ook niet wanneer dit geïmplementeerd is.

Ten opzichte van vorig jaar zijn er geen veranderingen. Wel zijn er dit jaar twee nieuwe standaarden op de lijst: Ades Baseline Profiles en HTTPS/HSTS. Deze zijn nog niet toegepast maar er loopt een onderzoek hierover dat naar verwachting in Q1 2018 afgerond is.

Concluderend, moet deze voorziening nog de volgende standaarden implementeren: Digikoppeling, IPv4 en IPv6 , ODF , SKOS , SPF , TLS , CMIS, Ades Baseline Profiles, en HTTPS/HSTS.

E.2.16. 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
SMEF 2.0	Nee	De OHNL e-factuur berichten voldoen aan de SMEF 1.3 specificaties. Voor het uitvoeren van de upgrade naar SMEF 2.0 heeft Logius geen opdracht gekregen van EZ.

Ten opzichte van vorig jaar zijn er een aantal dingen veranderd, zowel bij de voorziening zelf als ook bij de toetsing. Met betrekking tot de toetsing zijn er een aantal standaarden waarop de voorziening vorig jaar getoetst werd niet meer meegenomen. De reden is dat eFactureren geen (infrastructuur) voorziening in de typische zin is, veeleer is het een standaard bestaande uit semantische en syntactische afspraken. Om deze reden wordt de voorziening niet meer op de volgende infrastructuur-relevante standaarden getoetst: DNSSEC, IPv4 en IPv6, SPF, en PDF/A en PDF1.7. Voor dezelfde reden zijn ook Digitoegankelijk (voorheen Webrichtlijnen), en NEN 27001/27002 dit jaar niet meer getoetst.

Sinds vorig jaar zijn er ook een aantal nieuwe standaarden op de lijst. Echter, geen van deze standaarden is relevant voor eFactureren.

Concluderend, de berichten moeten nog een upgrade naar de nieuwe versie van de standaard krijgen.

E.2.17. MijnOverheid

Beheerorganisatie: Logius

MijnOverheid is de persoonlijke internetpagina voor overheidszaken voor de burger. MijnOverheid biedt burgers toegang tot de functionaliteiten 'uw post', 'uw persoonlijke gegevens' en 'uw lopende zaken' van overheidsdiensten. Overheidsinstellingen, zoals de Belastingdienst, Kadaster, RDW, SVB, UWV en gemeenten zijn aangesloten en maken voor delen van hun digitale dienstverlening gebruik van MijnOverheid. Logius is verantwoordelijk voor het portaal, de aangesloten partijen zijn verantwoordelijk voor hun eigen dienstverlening die via MijnOverheid benaderd kan worden.

Standaard	Status	Toelichting
Digikoppeling 2.0	Deels	Nieuwe koppelingen worden conform Digikoppeling 2.0 ingericht. Nagenoeg alle koppelingen voldoen aan de standaard, alleen in het uitzonderlijke geval dat een afnemer dit niet ondersteunt, dan niet.
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Gepland	De laatste Webrichtlijnen toets is door Stichting Accessibility uitgevoerd (niet meer door Centric zoals voorheen) en hieruit zijn een aantal issues naar voren gekomen. Deze issues zijn opgelost en er is een nieuwe toets aangevraagd. Pas daarna kan worden vastgesteld of MijnOverheid volledig voldoet aan deze standaard.
DKIM	Ja	MijnOverheid voldoet aan DKIM (conform https://internet.nl)
DNSSEC	Ja	MijnOverheid voldoet aan DNSSEC (conform https://internet.nl)
HTTPS en HSTS	Ja	Deze standaard wordt toegepast.
IPv4 en IPV6	Nee	Mijnoverheid gebruikt het Logius infrastructuur platform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik. Mijnoverheid ondersteunt op dit moment alleen IPv4. (Er zijn plannen om IPv6 te activeren, maar er is nog geen concrete datum aan deze plannen gekoppeld)
NEN-ISO/IEC 27001/27002	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Rijk (BIR) van toepassing die is gebaseerd op NEN-ISO27001. Logius heeft zich over toepassing van deze norm verantwoord door het afgeven van In Control Verklaringen (ICV's) aan de eigenaar (BZK/DGOBR). De ICV's zijn nog up-to-date.
OWMS	Nee	OWMS wordt niet ondersteund, want de web content van MijnOverheid is specifiek voor MijnOverheid en wordt dus niet uitgewisseld met andere partijen.
PDF 1.7, PDF/A-1 of PDF/A-2	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 besloten om niet op formaat te gaan controleren
SAML	Ja	Authenticatie loopt via SAML
SPF	Ja	SPF is relevant en inmiddels geïmplementeerd.

STARTTLS en DANE	Ja	Deze standaard relevant en wordt toegepast.
StUF	Ja	MijnOverheid heeft waar relevant de koppeling op basis van StUF. Dit is alleen relevant voor WOZ en Lopende Zaken
TLS v1.2, v1.1 en v1.	Ja	In de dienstverlening aan burgers maakt MijnOverheid gebruik van een TLS 1.2-verbinding (https://internet.nl/site/mijn.overheid.nl). De koppelingen met afnemers (overheidsorganisaties) lopen ook via TLS op basis van PKIoverheid-certificaten.

Ten opzichte van vorig jaar zijn er de volgende ontwikkelingen. Vorig jaar waren de webrichtlijnen nog op Deels, maar digitoegankelijk staat dit jaar op Gepland. Ook OWMS stond vorig jaar op Deels, en dit jaar op Nee. Bij de PDF standaard stond vorig jaar nog Deels, en inmiddels wordt hieraan voldaan.

Verder zijn van de standaarden die nieuw op de lijst staan, de STARTTLS/DANE en HTTPS/HSTS standaarden relevant. Beiden worden toegepast.

Concluderend, moet deze voorziening nog de volgende standaarden implementeren: Digikoppeling, Digitoegankelijk, IPV6, en OWMS.

E.2.18. NHR

Beheerorganisatie: Kamer van Koophandel

Het Nationaal Handels Register (NHR) is een door de Kamer van Koophandel (KvK) gehouden register, waarin rechtspersonen en ondernemingen vermeld staan met hun gegevens.

Standaard	Status	Toelichting
Ades Baseline Profiles	Ja	De NHR voldoet aan de Ades Baseline Profiles standaard.
CMIS	Deels	De bij de KvK in gebruik zijn de content management systemen Tridion en Documentum zijn compliant aan de CMIS standaard. Nog niet alle interne koppelingen op deze systemen zijn al gemigreerd naar deze standaard, daar zijn op ook nog geen plannen voor.
Digikoppeling 2.0	Ja	Ongeveer 10% van het verkeer van het NHR gaat naar mede-overheden. Die uitwisselingen vinden allemaal plaats via Digikoppeling en StUF.
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Nee	De KvK voldoet voor een groot deel aan Digitoegankelijk. In 2016 werd gepland om in 2017 een scan op de planning om de status te herijken en van daaruit noodzakelijke verbeteringen door te voeren, maar dit is nog niet gebeurd. De huidige planning is Q4 2017.
DKIM	Ja	Het domein kvk.nl voldoet aan DKIM (zie https://internet.nl/mail/kvk.nl/34914).
DNSSEC	Gepland	DNSSEC wordt nog niet toegepast (zie https://internet.nl/site/www.kvk.nl/87180). De planning voor implementatie van de DNSSEC is Q4 2017.
HTTPS/HSTS	Gepland	De voorziening gebruikt beide HTTPS, maar nog niet HSTS (zie https://internet.nl/site/www.kvk.nl/87180). De planning is om HSTS Q4 2017 nog te gaan ondersteunen.

IPv4 en IPv6	Nee	De website kvk.nl ondersteunt IPv4, maar is niet toegankelijk via IPv6 (zie https://internet.nl/site/www.kvk.nl/87180). Het project om over te stappen naar IPv6 project is door de KvK nog niet ingepland. De KvK had in 2016 wel voorbereidingen getroffen, waaronder de overstap naar een andere ISP provider, zodat de KvK een migratie naar IPv6 uit kan gaan voeren. Deze situatie was in augustus 2017 nog niet veranderd.
NEN-ISO/IEC 27001/27002	Ja	De KvK is sinds 2016 ISO 27001 gecertificeerd en hanteert ISO27002.
PDF 1.7, PDF A/1, PDF A/2	Ja	Alle uittreksels en informatie uit het NHR wordt in PDF/A-vorm verstrekt. Het betreft PDF A/1.
SAML	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. Er liep in 2016 een traject waarbij de authenticatieprocedures en infrastructuur werden vervangen. Hierdoor kan SAML inmiddels voor elke dienst ingezet worden voor authenticatie.
SKOS	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. Voor deze standaard zou in 2016 een impactscan uitgezet worden, maar dit is nog niet gebeurd. Wanneer dit wel gaat gebeuren kan door de KvK nog niet aangegeven worden.
SPF	Ja	SPF is ten opzichte van het vorige onderzoek nieuw op de lijst en inmiddels geïmplementeerd door NHR.
STARTTLS/DANE	Nee	De voorziening past alleen STARTTLS toe, DANE nog niet (zie https://internet.nl/mail/kvk.nl/34914). De planning is om HSTS Q4 2017 te gaan ondersteunen.
STuF	Ja	Ongeveer 10% van het verkeer van het NHR gaat naar medeoverheden. Die uitwisselingen vinden allemaal plaats via Digikoppeling en StuF.
TLS v1.2, v1.1 en v1.	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/87180).

Er zijn een aantal ontwikkelingen sinds het onderzoek van vorig jaar. Een aantal standaarden zijn ten opzichte van het vorige onderzoek nieuw op de PTOLU lijst. De Ades Baseline Profiles, HTTPS/HSTS en STARTTLS/DANE standaarden zijn hiervan relevant. Echter, tot nu toe worden alleen Ades Baseline Profiles, HTTPS en STARTTLS toegepast.

Concluderend, moet deze voorziening nog aan de volgende standaarden voldoen: CMIS, DANE, Digitoegankelijk, DNSSEC, HSTS, IPv6, en SKOS.

E.2.19. 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
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Nee	Websites van ODC-Noord die aan het internet ontsloten zijn, voldoen in principe aan Digitoegankelijk, dit is een inrichtingseis. ODC heeft de website niet laten toetsen. Het waarmerk drempelvrij is dan ook niet behaald. De WCAG checker op http://checkers.eiii.eu/ geeft bijvoorbeeld bij https://www.odc-noord.nl/over-odc-noord een hoge, maar onvolledige, score van 107/112.
DKIM	Gepland	DKIM is nog niet geïmplementeerd voor ODC-Noord. Voor e-mail maakt ODC-Noord vooralsnog gebruik van de mail-faciliteiten van DUO. Er zou een eigen e-mailinfrastructuur vanaf eind 2015 komen, maar dit is nog niet in gang gebracht. In het kader van de beweging van OCW naar één werkplekconcept is het mogelijk dat op termijn een multi-tenant mail-oplossing aangeboden wordt, maar dit is nog niet in gang. Planning is om dit eind 2018 afgerond te hebben.
DNSSEC	Ja	ODC-Noord heeft sinds het onderzoek uit 2015 een eigen DNS ingericht, die DNSSEC gebruikt.
HTTPS/HSTS	Deels	De cloud dashboards zijn allemaal uitsluitend via HTTPS benaderbaar een aantal websites draaien op HSTS. De overige websites worden in de loop van 2017 aangepast.
IPv6 en IPv4	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 de systemen die vanaf het internet benaderbaar zijn ook worden ontsloten via IPv6.
NEN-ISO/IEC 27001/27002	Nee	ODC-Noord implementeert op dit moment de BIR. Er is nog geen in control statement. De leveranciers van de rekencentra voldoen beide aan ISO 27001. Een BIR-audit op housing is uitgevoerd eind 2014. Er werd in 2016 een ADR (Audit Dienst Rijk) onderzoek uitgevoerd per departement. Dit richt zich o.a. op de opvolging die de departementen hebben gegeven aan nog uit te voeren activiteiten genoemd o.a. in de bevindingen uit het BIR onderzoek van de ADR over 2015 (bijvoorbeeld in de vorm van verbeterplannen verankerd in jaarplannen), en op de onderbouwing (dossiervorming) bij de systemen voor het wel of niet voldoen aan de BIR. Het onderzoek is in januari 2017 gepubliceerd, en er loopt op dit moment een verbeterplan met betrekking tot de ADR bevindingen. Er is echter nog geen concrete datum bekend.
ODF 1.2	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	Gepland	Hier is nog aandacht voor geweest in versie 1.0 van de ODC-Noord website. OWMS wordt meegenomen in de volgende versie. De update hiervoor is voor 2018 verwacht.
PDF 1.7, PDF A/1, PDF A/2	Deels	V.w.b. uitwisseling van (definitieve) documenten met externe partijen wordt gebruik gemaakt van PDF. PDFCreator van Windows wordt als printoptie in de kantoorautomatiserings-omgeving 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.
SAML	Nee	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.
STARTTLS/DANE	Gepland	De implementatie van STARTTLS en DANE loopt op dit moment. Afronding is voor eind 2018 gepland.
TLS 1.2, 1.1 en 1.0	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	Ja	Deze standaard is toegepast waar ODC-Noord wifi gebruikt.

Ten opzichte van het onderzoek van 2016 zijn er een aantal ontwikkelingen. De NEN-ISO/IEC 27001/27002 standaard is gewijzigd van Gepland naar Nee. Bij OWMS bestaat inmiddels een planning voor het update voor de website om hieraan te voldoen en de status is dus naar 'Gepland' gewijzigd. De Webrichtlijnen standaard stond vorig jaar nog op Deels, maar de opvolger Digitoegankelijk staat nu op Nee.

Daarnaast zijn er een aantal nieuwe standaarden op de lijst, waarvan HTTPS/HSTS en STARTTLS/DANE relevant zijn voor de voorziening. HTTPS/HSTS wordt deels toegepast op dit moment en de volledige implementatie van HSTS is gepland, en ook de implementatie van STARTTLS/DANE is gepland.

Concluderend op deze voorziening, moeten nog de volgende standaarden (volledig) worden geïmplementeerd: Digitoegankelijk, DKIM, HTTPS/HSTS, IPv6 en IPv4 , NEN-ISO/IEC 27001/27002 , OWMS, PDF, SAML, en STARTTLS/DANE.

E.2.20. Ondernemersplein

Beheerorganisatie: Kamer van Koophandel

Ondernemersplein.nl is het informatiepunt voor ondernemers bij iedere (nieuwe) stap als ondernemer. Onder andere de RVO, de KvK, de Belastingdienst, Antwoord voor Bedrijven, UVW, RDW en het CBS werken samen om informatie voor ondernemers te bundelen en makkelijk toegankelijk te maken. Ook de producten en diensten van de gemeenten en provincies worden ontsloten. De website www.antwoordvoorbedrijven.nl is in 2014 opgegaan in www.ondernemersplein.nl.

Standaard	Status	Toelichting
BWB	Ja	Binnen de website, de content van AvB, wordt verwezen naar wetgeving conform de BWB standaard
CMIS	Nee	De tooling (CMS/ESB) ondersteunt de standaard wel, maar deze wordt niet actief gebruikt. Er zijn er 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)	Ja	Verklaring is beschikbaar. Meer informatie beschikbaar op: https://www.ondernemersplein.nl/toegankelijkheid/
DKIM	Ja	DKIM is geïmplementeerd (zie https://internet.nl/mail/ondernemersplein.nl/34765)
DNSSEC	Gepland	Wordt geïmplementeerd dit jaar op de nieuwe DNS omgeving.
HTTPS/HSTS	Ja	Aan deze standaard wordt voldaan (zie https://internet.nl/site/www.ondernemersplein.nl/86899).
IPv4 en IPV6	Ja	De website ondersteunt IPv4 en is toegankelijk via IPv6 (zie https://internet.nl/site/www.ondernemersplein.nl/86899).
NEN-ISO/IEC 27001/27002	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 ook gecertificeerd hierop.
OWMS	Nee	De informatie op de website is gemetadateerd volgens een eigen model die past bij de metadatering van de partners.
SKOS	Nee	Er wordt niet aan deze standaard voldaan. Het moet nog onderzocht worden of hieraan voldaan zal worden en plannen gemaakt worden.

SPF	Ja	Er wordt aan deze standaard voldaan (zie https://internet.nl/mail/ondernemersplein.nl/34765).
STARTTLS/DANE	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.
TLS v1.2, v1.1 en v1.	Nee	Technisch kan er worden overgestapt naar alleen TLS 1.2 echter plannen zijn uitgesteld door slechte browser ondersteuning aan eindgebruiker.

Sinds het onderzoek van 2016 zijn een aantal ontwikkelingen te vermelden. Bij DNSSEC is de status veranderd van 'Nee' naar 'Gepland'. Bij DKIM is de status naar 'Ja' gegaan. Bij Digitoegankelijk is de status van 'Gepland' naar 'Ja' veranderd. Bij CMIS is de status van 'Ja' naar 'Nee' veranderd, op basis van voortschrijdend inzicht bij de beheerpartij. Bij SPF is de status van 'Nee' naar 'Ja' gewijzigd, en bij TLS van 'Gepland' naar 'Nee'.

Van de standaarden die nieuw op de lijst staan, zijn de volgende standaarden relevant: HTTPS/HSTS, en STARTTLS/DANE. Aan de eerste wordt voldaan, maar voor STARTTLS/DANE moet nog onderzocht worden of hieraan voldaan zal worden.

Concluderend, moeten bij deze voorziening nog de volgende standaarden geïmplementeerd worden:, CMIS, DNSSEC, OWMS, SKOS, STARTTLS/DANE, en TLS.

E.2.21. Overheid.nl

Beheerorganisatie: Kennis- en Exploitatiecentrum Officiële Overheidspublicaties (KOOP)

De website Overheid.nl is de toegang tot alle informatie van de Nederlandse overheid op internet. Deze website werd in opdracht van het ministerie van Binnenlandse Zaken en Koninkrijksrelaties gemaakt door Logius. Per 1 augustus 2016 is het beheer van Overheid.nl overgedragen van Logius aan KOOP. KOOP heeft de toepassing van een aantal standaarden direct in gang gezet bij de hostingpartij.

Standaard	Status	Toelichting
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Gepland	Er is een toegankelijkheidsverklaring conform EN 301459. De nieuwe eisen van deze nieuwe richtlijn zijn meegenomen in de vernieuwing van Overheid.nl, die eind 2017 staat gepland.
DKIM	Ja	DKIM is geïmplementeerd (zie https://internet.nl/domain/www.overheid.nl/87086).
DNSSEC	Ja	Overheid.nl voldoet sinds Q2 2015 aan DNSSEC (zie https://internet.nl/domain/www.overheid.nl/87086).
HTTPS en HSTS	Gepland	Het portaal-gedeelte (www.overheid.nl) voldoet aan de standaard (zie https://internet.nl/domain/www.overheid.nl/87086). Een aantal sub-sites staat nog gepland om in 2017 aan deze standaarden te laten voldoen.
IPv4 en IPV6	Ja	Er wordt voldaan aan IPv4 en IPv6 (zie https://internet.nl/domain/www.overheid.nl/87086).
NEN-ISO/IEC 27001/27002	Ja	Vanaf 2015 staat overheid.nl niet meer op die risicokaart van BZK en hoeft geen ICV meer worden afgegeven.
OWMS	Ja	Overheid.nl is gemetadateerd conform OWMS.
PDF 1.7 PDF/A-1 PDF/A-2	Ja	Alle PDF's van Officiële bekendmakingen zijn PDF/A-1a zoals wettelijk bepaald is.
SKOS	Ja	SKOS is geïmplementeerd voor de waardelijsten van OWMS.
STARTTLS en DANE	Ja	STARTTLS en DANE zijn geheel geïmplementeerd (zie https://internet.nl/mail/overheid.nl/34850).

TLS v1.2, v1.1 en v1.0	Gepland	De aanpassingen in deze standaard staan ingepland voor tweede helft 2017.

Ten opzichte van het onderzoek van vorig jaar zijn er een aantal ontwikkelingen. Zo zijn DKIM, IPv4/IPv6 inmiddels geïmplementeerd. Bij TLS, die vorig jaar nog op 'Ja' stond, moeten nog aanpassingen gedaan worden om te voldoen.

Van de standaarden die nieuw op de lijst staan, zijn de volgende relevant: HTTPS/HSTS en STARTTLS/DANE. HTTPS/HSTS wordt deels geïmplementeerd en volledige implementatie is gepland. Aan STARTTLS/DANE wordt al voldaan.

Concluderend, moet deze voorzieningen nog (volledig) voldoen aan Digitoegankelijk, HTTPS/HSTS, en TLS.

E.2.22. 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
Ades Baseline Profiles	Nee	De implementatie van deze standaard is nog niet gestart.
BWB	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.
Digikoppeling 2.0	Ja	P-Direkt heeft vele interfaces met partijen binnen de overheid, Identity management, hr-data, arbo-diensten, ziekmeldingen, koppelingen met BD. 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.
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Nee	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.
DKIM	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.
DNSSEC	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.

HTTPS/HSTS	Nee	HTTPS is 100% doorgevoerd voor alle communicatie met klanten. HSTS is nog niet geïmplementeerd.
IPv4 en IPv6	Nee	De Haagse ring, waarover eigenlijk al het verkeer naar de P-Direkt loopt, ondersteunt geen IPv6. De P-Direkt voorzieningen, zoals gehost bij Match, ondersteunen in theorie momenteel al IPv6. In de praktijk is nog geen enkele afnemer op IPv6 aangesloten. Op het aanbieden van IPv6 door de Haagse Ring heeft P-Direkt geen invloed.
NEN-ISO/IEC 27001/27002	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, er bestaat bij de beheerorganisatie nog onduidelijkheid of de beheerorganisatie ook aan de BIR voldoet. Daarom staat de status hier op Deels.
ODF	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, 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. Het proces dat brieven genereert is het niet mogelijk ODF bestanden te genereren.
PDF 1.7 – PDF A/1 of PDF A/2	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.
SAML	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	Nee	SPF moet nog geïmplementeerd worden door de beheerder van de mail dienst (in het geval van P-Direkt is dat SSC-ICT).
TLS v1.2, v1.1 en v1.0	Ja	Alle diensten van P-Direkt die door middel van HTTP worden ontsloten, worden enkel aangeboden via TLS v1.0 of hoger.

Ten opzichte van het onderzoek uit 2016 zijn er een aantal ontwikkelingen. De SPF standaard stond vorig jaar nog op Gepland, maar staat dit jaar op Nee omdat er geen concreet datum gepland is. De NEN-ISO/IEC 27001/27002 standaard staat dit jaar op Deels in plaats van Ja. Van de standaarden die nieuw op de lijst staan, zijn de volgende standaarden relevant: HTTPS/HSTS en Ades Baseline Profiles. Deze standaarden worden nog niet toegepast.

Concluderend, moet deze voorziening nog aan volgende standaarden voldoen: Ades Baseline Profiles, Digitoegankelijk, DNSSEC, HSTS, IPv6, NEN-ISO/IEC 27001/27002, ODF, PDF, en SPF.

E.2.23. PKIoverheid

Beheerorganisatie: Logius

Het PKIoverheid-certificaat is een computerbestand dat fungeert als een digitaal paspoort. Certificaten worden gebruikt bij onder meer het bezoeken van beveiligde websites, het controleren van de elektronische ondertekening van berichten of documenten, en het bekijken van versleutelde informatie. Logius heeft meegewerkt aan de ontwikkeling van het normenkader dat aan PKIoverheid-certificaten ten grondslag ligt, en is betrokken bij het beheer ervan. Zo beheert Logius ondermeer de website http://crl.pkioverheid.nl waarop de status van de certificaten terug te vinden is. Daarnaast bevat de algemene Logius webpagina meer informatie over PKI overheid.

Standaard	Status	Toelichting
DNSSEC	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/87088 en https://internet.nl/domain/www.logius.nl/87089).
HTTPS/HSTS	Ja	Deze standaard wordt toegepast door de voorziening (zie https://internet.nl/domain/crl.pkioverheid.nl/87088 en https://internet.nl/domain/www.logius.nl/87089).
IPv4 en IPV6	Gepland	IPv6 is geïmplementeerd voor de informatiepagina's van PKIoverheid op de Logius website (zie https://internet.nl/domain/www.logius.nl/87089). De PKIoverheid specifieke applicatiepagina's zijn op dit moment nog niet geschikt voor IPv6 (zie https://internet.nl/domain/crl.pkioverheid.nl/87088). Navraag bij de leverancier leert dat dit wel is opgenomen op de roadmap maar (nog) niet voor 2017.
NEN-ISO/IEC 27001/27002	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.
OWMS	Ja	Op website van Logius ja, maar niet op de website van PKIoverheid (info is niet bedoeld voor hergebruik van overheidsinformatie).
PDF 1.7, PDF A/1, PDF A/2	Ja	Documenten die via de websites beschikbaar worden gesteld worden volgens PDF/A opgesteld.
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/87088 en https://internet.nl/domain/www.logius.nl/87089).

Sinds het onderzoek van 2016 zijn er de volgende ontwikkelingen. De status van IPv6 is gewijzigd naar Gepland. Digitoegankelijk wordt als niet relevant voor de voorziening geacht, omdat de PKIoverheid specifieke applicatiepagina's (cert.pkioverheid.nl, crl.pkioverheid.nl en cps.pkioverheid.nl) voornamelijk bedoeld zijn voor machinale verwerking en het dus ook niet nodig geacht wordt om deze toegankelijk te maken (conform Webrichtlijnen of opvolgers).
Een aantal standaarden zijn ten opzichte van het vorige onderzoek nieuw op de PTOLU lijst. Hiervan is alleen de HTTPS/HSTS standaard relevant voor de voorziening, en deze standaard wordt ook toegepast.

Concluderend, moet bij de voorziening alleen nog de IPv6 standaard toegepast worden.

E.2.24. 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
BWB	Ja	Binnen de website wordt verwezen naar wetgeving conform de BWB standaard. BWB wordt dus toegepast.
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Ja	De website voldoet aan Digitoegankelijk (WCAG 2.0). Zie ook de verantwoording daarover op: http://www.rijksoverheid.nl/toegankelijkheid.

DKIM	Ja	DKIM is geïmplementeerd voor de bulk van het mailverkeer. Dit heeft 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. DKIM is niet ingericht voor andere DPC-mailstromen, zoals de persoonlijke @rijksoverheid.nl mailboxen (niet in gebruik bij DPC), omdat deze lopen via de SSC-ICT mailservers. Dat betekent dat e-mailverkeer gebruikmakend van @rijksoverheid.nl niet onder beheer van DPC valt. Ook de domain @rijksoverheid.nl voldoet aan DKIM (zie https://internet.nl/mail/rijksoverheid.nl/34858).
DNSSEC	Ja	Rijksoverheid.nl is ondertekend met DNSSEC (zie https://internet.nl/site/www.rijksoverheid.nl/86909). DPC biedt DNSSEC ook aan al haar klanten die domeinen via haar registrar-functie afnemen.
HTTPS/HSTS	Ja	De voorziening voldoet aan deze standaard (zie https://internet.nl/site/www.rijksoverheid.nl/86909).
IPv4 en IPV6	Ja	Rijksoverheid.nl ondersteunt zowel IPv6 als IPv4 (zie https://internet.nl/site/www.rijksoverheid.nl/86909).
NEN-ISO/IEC 27001/27002	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. AZ is het enige departement dat zonder bevindingen door de ADR audits is gekomen.
ODF 1.2	Ja	Het CMS van het Platform Rijksoverheid Online accepteert slechts PDF en ODF (open standaard) formaten. Er zijn wel 'legacy'-bestanden in alleen .doc of .xls formaat. Nieuwe documenten zijn echter altijd tenminste in PDF- of indien bewerkbaar, in ODF-formaat beschikbaar. De PDF-generator die men gebruikt is goed voor het leeuwendeel van de PDF's op de website en genereert PDF-bestanden in PDF/A-1a.
OWMS	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	Ja	DPC publiceert zelf geen PDF's, maar departementen kunnen PDFs op Rijksoverheid plaatsen. Vooralsnog kan de Rijksoverheid praktisch niet aan deze richtlijn voldoen. DPC is daarover met BZK in gesprek.
SAML	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	Ja	Het e-maildomein @rijksoverheid.nl is integraal van SPF voorzien (zie https://internet.nl/mail/rijksoverheid.nl/34768).
TLS v1.2, v1.1 en v1.0	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/87100) .

Er zijn een aantal ontwikkelingen sinds de Monitor 2016. De PDF standaard is van Deels naar Ja gegaan. Een aantal standaarden zijn ten opzichte van het vorige onderzoek nieuw op de PTOLU lijst. Hiervan zijn HTTPS/HSTS en STARTTLS/DANE relevant, en de voorziening voldoet ook aan beide standaarden.

Concluderend, zijn alle relevante standaarden bij deze voorziening geïmplementeerd.

E.2.25. 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
Digikoppeling 2.0	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.
DKIM	Gepland	Voor Rijkspas worden mails verstuurd vanaf de applicatie voor Interdepartementale Toegang (IdT). In de huidige infrastructuur is dit niet toegepast. Uiterlijk Q3 2018 worden de Rijkspassystemen verhuisd naar een nieuw datacenter waar DKIM wel toegepast zal worden.
DNSSEC	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, maar de leverancier geeft aan dat de verwachting is DNSSEC eind 2017 wel geïmplementeerd gaat worden.
IPv4 en IPV6	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	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	Ja	De Interdepartementale Toegang applicatie (IDT) is per 2015 aangesloten op de Single Sign On voorziening via SAML.
SPF	Ja	SPF is geïmplementeerd.
STARTTLS/DANE	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 einde 2017 verwacht wordt. Na deze implementatie zal SSC-ICT opnieuw de mogelijkheden van STARTTLS en DANE analyseren.
TLS v1.2, v1.1 en v1.0	Ja	TLS wordt gebruikt voor het veilig ontsluiten van de website voor IdT.

Er zijn een aantal veranderingen ten opzichte van het onderzoek uit 2016. Voor DKIM en voor DNSSEC is de status gewijzigd naar 'Gepland'. Verder is SPF inmiddels geïmplementeerd.

Van de standaarden die dit jaar nieuw op de lijst staan is alleen STARTTLS/DANE relevant. Voorlopig voldoet de Rijkspas nog niet aan deze standaard.

Concluderend, moeten bij deze voorziening nog de volgende standaarden geïmplementeerd worden: DKIM, DNSSEC, IPV6, en STARTTLS/DANE.

E.2.26. Rijksportaal

Beheer organisatie: Ministerie BZK

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
IPv4 & IPv6	Nee	Het huidige Rijksportaal (versie 1.6.5) is alleen ingericht voor IPv4. Om performance redenen wordt IPv6 momenteel nog niet toegepast. Oplossing van de oorzaken van de performance-issues is onderwerp van onderzoek.
ODF	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	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.
SAML	Ja	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.

Ten opzichte van 2016 zijn er een aantal ontwikkelingen. IPv4/IPv6 was vorig jaar nog Gepland, maar staat nu op Nee. OWMS wordt inmiddels door de beheerorganisatie niet meer als relevant beschouwd (omdat het functioneel toepassingsgebied van deze standaard beschreven is als 'Metadateren van publieke overheidsinformatie op internet', en het Rijksportaal niet bereikbaar is via het internet en geen overheidsinformatie bevat die bedoeld is voor een algemeen publiek). ODF stond vorig jaar nog op Ja, maar inmiddels op Deels.

De Digitoegankelijk standaard is niet van toepassing voor "websites die alleen intern binnen een overheidsorganisatie worden gebruik ('intranet')." Echter, uit de Europese toegankelijkheidsrichtlijn blijkt dat de verplichting op termijn ook voor intranetten gaat gelden. De beheerorganisatie geeft aan dat daarom voor het nieuwe Rijksportaal toegankelijkheid een belangrijk criterium is en tegen die tijd wordt onderzocht hoe de toegankelijkheid het beste kan worden geborgd.

Geen van de standaarden die nieuw op de lijst staan (Ades Baseline Profiles, HTTPS/HSTS, STARTTLS/DANE) zijn van toepassing voor deze voorziening.

Concluderend, moet het Rijksportaal alleen nog de IPv6implementeren.

E.2.27. Samenwerkende Catalogi

Beheerorganisatie: Logius

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 doorzoekbaar door middel van de Zoekdienst van KOOP. 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
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Ja	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)
OWMS	Ja	Samenwerkende catalogi is volledig gebaseerd op OWMS.

Bij Samenwerkende Catalogi zijn ten opzichte van het onderzoek uit 2016 geen wijzigingen te vermelden.

E.2.28. SBR (Standard Business Reporting)

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)[45]. De voorziening voor de e-dienstverlening is Digipoort. SBR heeft een eigen website.

Standaard	Status	Toelichting
Ades Baseline Profiles	Ja	Binnen SBR (Assurance) waarbij bijvoorbeeld jaarverslagen worden ondertekend door een accountant, wordt binnen DigiPoort gebruik gemaakt van XAdES als EU standaard.
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Nee	Voor SBR-NL.nl werd nog niet op Digitoegankelijk getoetst dus er is nog geen verklaring, vandaar voldoet de website nog niet aan het toetsingbeleid van deze standaard.

[45] 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.

DKIM	Nee	De website van SBR (http://www.sbr-nl.nl) heeft ook een mailserver. In het verleden voldeed deze aan DKIM, maar 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).
DNSSEC	Nee	De website van SBR (http://www.sbr-nl.nl) is ondergebracht bij een derde partij. Ook het technisch DNS-beheer is daar ondergebracht, maar nog niet alle domeinen maken gebruik van DNSSEC.
IPv4 en IPv6	Ja	De website van SBR wordt bij een derde partij gehost en is bereikbaar met IPv6.
PDF 1.7, PDF A/1, PDF A/2	Ja	Bij het publiceren van documenten houdt Logius voor SBR PDF/A aan bij publicatie.
SPF	Nee	De website van SBR (http://www.sbr-nl.nl) heeft ook een mailserver. Deze voldoet niet aan SPF (zie https://internet.nl/mail/sbr-nl.nl/results). De SBR website is hierin afhankelijk van de 'moederwebsite' www.logius.nl.
STARTTLS/DANE	Nee	Aan STARTTLS wordt voldaan, door de voorziening. Aan DANE wordt nog niet voldaan, hiervoor is ook nog geen planning bekend omdat de SBR website hierbij afhankelijk is van de 'moederwebsite' www.logius.nl.
TLS 1.0, 1.1 en 1.2	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.
XBRL	Ja	SBR maakt gebruik van XBRL.

Ten opzichte van het onderzoek uit 2016 zijn er een aantal ontwikkelingen. Omdat SBR geen infrastructuur voorziening in de typische zin is maar veeleer een standaard die op de DigiPoort voorziening draait, staat Digikoppeling niet meer als relevante standaard in de tabel voor SBR maar bij DigiPoort. Omdat DigiPoort dit jaar geheel aan de IPv6 standaard voldoet, staat deze standaard nu ook bij SBR op "Ja". Aan DKIM wordt in tegenstelling tot vorig jaar niet voldaan, omdat de website recent is overgezet naar een nieuwe beheerder.

Een aantal standaarden zijn ten opzichte van het vorige onderzoek nieuw op de PTOLU lijst. Hiervan zijn Ades Baseline Profiles en STARTTLS en DANE relevant. Aan Ades Baseline Profiles wordt door de voorziening voldaan. Aan STARTTLS wordt ook voldaan, maar nog niet aan DANE.

Concluderend, moeten bij deze voorziening nog de volgende standaarden geïmplementeerd worden: Digitoegankelijk, DKIM, DNSSEC, SPF, en STARTTLS/DANE.

E.2.29. Stelsel Elektronische Toegangsdiensten

Beheerorganisatie: Logius

Sinds vorig jaar 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 er aan 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
Digitoegankelijk (EN 301 549 met WCAG 2.0)	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).
DKIM	Ja	Bij verstuurde email wordt DKIM toegepast, bij ontvangst gebeurd dit door de centrale email voorzieningen van Logius (SSC-ICT).
DNSSEC	Ja	DNSSEC werd in 2015 in de productieomgeving opgenomen.
HTTPS en HSTS	Ja	HTTPS en HSTS wordt toegepast op alle websites en webapplicaties onder beheer van de beheerorganisatie.
IPv4 en IPv6	Gepland	Aan de ondersteuning van IPv6 voor alle (publiek toegankelijke) systemen wordt gewerkt. De plandatum om IPv6 geheel geïmplementeerd te hebben is eind 2017.
NEN-ISO/IEC 27001/27002	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.
PDF 1.7, PDF/A-1 of PDF/A-2	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.
SAML	Ja	SAML is een verplichte eis vanuit het stelsel.
SPF	Ja	SPF wordt toegepast bij de voorziening, maar wordt vooralsnog niet vereist als toe te passen techniek voor deelnemers.
STARTTLS en DANE	Nee	STARTTLS is geïmplementeerd voor eherkenning.nl en idensys.nl. De implementatie van DANE is nog onderwerp van onderzoek.
TLS v1.2, v1.1 en v1.	Ja	Het afsprakenstelsel stelt het gebruik van TLS1.x verplicht.

Ten opzichte van de Monitor van 2016 zijn er een aantal ontwikkelingen. Zo wordt inmiddels DKIM toegepast; deze standaard werd vorig jaar nog niet als relevant beschouwd. Ook IPv4 en IPv6 worden dit jaar als relevant beschouwd en meegenomen in de toetsing. Van de standaarden die sinds vorig jaar nieuw op de lijst staan, zijn HTTPS/HSTS en STARTTLS/DANE relevant. Hiervan wordt aan de eerste, en STARTTLS voldaan, aan DANE nog niet.

Concluderend, moeten bij deze voorziening nog DANE enIPv6 geïmplementeerd worden.

E.2.30. Stelselcatalogus

Beheerorganisatie: Logius

De Stelselcatalogus is een online catalogus die inzicht geeft in welke gegevens het Stelsel van Basisregistraties bevat, wat ze betekenen en hoe ze met elkaar verbonden zijn. Met die

informatie kunnen overheden bepalen of de gegevens uit de basisregistratie(s) makkelijk zijn in te passen in hun eigen werkprocessen. De Stelselcatalogus wordt beheerd door Logius.

Standaard	Status	Toelichting
BWB	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.
Digitoegankelijk (EN 301 549 met WCAG 2.0)	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
DNSSEC	Ja	DNSSEC is geïmplementeerd op de centrale voorziening DNS (zie https://internet.nl/site/www.stelselcatalogus.nl/92837).
HTTPS / HSTS	Nee	De HTTPS implementatie staat gepland voor medio Q4 2017. HSTS wordt nog niet geïmplementeerd.
IPv4 en IPv6	Ja	Stelselcatalogus gebruikt het Logius infrastructuur platform. 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).
PDF 1.7, PDF A/1, PDF A/2	Ja	Documenten worden als PDF-A/1 aangeboden via de website.
SKOS	Ja	SKOS wordt toegepast door de voorziening.

Sinds de Monitor 2016 zijn er enkele veranderingen. Zo is DKIM niet meer relevant, omdat mail relay niet toegepast wordt binnen de Stelselcatalogus. Ook OWMS wordt niet meer als relevant beschouwd door de voorziening. DNSSEC stond vorig jaar nog op Gepland, en is inmiddels geïmplementeerd. Daarnaast is de IPv4/6 standaard van gepland naar Ja gegaan.

Ook zijn er een aantal nieuwe standaarden op de lijst. Hiervan is alleen HTTPS/HSTS relevant, en zal nog voor het einde van 2017 geïmplementeerd worden.

Concluderend op deze voorziening, is het alleen de HTTPS/HSTS standaard die nog geïmplementeerd moet worden.

E.2.31. 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
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Nee	TenderNed wordt momenteel gerenoveerd. Daarbij worden de schermen deels vernieuwd. Bij de implementatie van nieuwe schermen worden de richtlijnen uit EN 301 539 toegepast.
DKIM	Nee	E-mails verzonden vanuit TenderNed zijn niet beveiligd met DKIM (zie https://internet.nl/mail/tenderned.nl/34863).
DNSSEC	Ja	Het domein is gesigned met DNSSEC (zie https://internet.nl/site/www.tenderned.nl/86922).
HTTPS en HSTS	Ja	De client-server communicatie van TenderNed is beveiligd met HTTPS en HSTS (zie https://internet.nl/site/www.tenderned.nl/86922).
IPv4 en IPV6	Nee	Tenderned.nl is niet voorbereid op IPv6 (zie https://internet.nl/site/www.tenderned.nl/86922). TenderNed is afhankelijk van de hostingpartij. Wanneer deze een transitie door maakt naar IPv6 zal TenderNed daar in mee gaan.
NEN-ISO/IEC 27001/27002	Ja	TenderNed is ISO27001/2 gecertificeerd. Dit wordt jaarlijks geaudit.
PDF 1.7, PDF/A-1, PDF/A-2	Ja	Geautomatiseerd gecreëerde PDF's (bij de aankondigingen) zijn gemaakt in versie 1.7.
SAML	Ja	Per 1 juli 2014 is het mogelijk voor gebruikers om, naast de huidige registreer- en inlogmogelijkheden, gebruik te maken van inloggen via eHerkenning. De huidige mogelijkheden worden vanaf deze datum uitgefaseerd. (Bron: http://www.tenderned.nl/eherkenning-en-tenderned-0)
SPF	Nee	TenderNed past de SPF standaard niet toe (zie https://internet.nl/mail/tenderned.nl/34863). In het verleden is SPF wel actief geweest voor tenderned.nl. Dit leverde echter problemen op na een migratie van mailservers bij de DICTU. Daarom is deze functionaliteit uitgezet.
STARTTLS en DANE	Nee	STARTTLS wordt ondersteund. DANE nog niet.
TLS v1.2, v1.1 en v1.0	Ja	TenderNed past TLS 1.2 toe (zie https://internet.nl/site/www.tenderned.nl/86922). Voor een aantal koppelingen wordt nog TLS 1.0 gebruikt voor compatibiliteit.

Ten opzichte van het onderzoek van 2016 zijn er een aantal ontwikkelingen. Zo wordt inmiddels voldaan aan DNSSEC. SPF bleek niet goed te werken en is weer uitgeschakeld. Digitoegankelijk staat nu op Nee, terwijl de Webrichtlijnen standaard vorig jaar op Ja stond.

Van de standaarden die dit jaar nieuw toegevoegd zijn aan de lijst, zijn HTTPS/HSTS en STARTTLS/DANE relevant. Aan de HTTPS/HSTS en STARTTLS wordt ook voldaan, aan DANE nog niet.

Concluderend, moet deze voorziening nog (volledig) voldoen aan Digitoegankelijk, DKIM, IPv6, STARTTLS/DANE, en SPF.

Geïnterviewde personen

Naam voorziening	Contactpersoon
BAG, WOZ, BGT, BRK	Harrie van Leeuwen / Piet van der Krieke
Berichtenbox voor bedrijven	Laura Ouwehand
BRI	Henk Heerink (tot 2017, daarna via CIO office)
BRT	Harrie van Leeuwen / Piet van der Krieke
BRV	Gert Stel, Walter Huberts
BSN en GBA-V	Bob te Riele
Digi-Inkoop	Victor den Toom
DigiD	Joris Joosten, David Kamp
DigiD Machtigen	Wim Geurts, Joris Joosten
Digilevering	Ed van der Ark
Digimelding	Ed van der Ark
Diginetwerk	Glenn Lutke Schipholt
DigiPoort	Victor den Toom
Doc-Direkt	Ali Amin Shahidi
DWR	Rein Hennen
eFactureren	Victor den Toom
Stelsel elektronische toegangsdiensten	Joris Joosten, Remco Schaar
MijnOverheid	Louis Stevens
NHR	Erik Goos, Rob Spoelstra
ODC Noord	Fijtse Vos
Ondernemersplein	Milla van der Have, Wouter Nieuwenhuis
Overheid.nl	Lucien de Moor, Hans Overbeek)
P-Direkt	Jos van Vlimmeren
PKI Overheid	Jochem van den Berge
Rijksoverheid.nl	Marc van de Graaf, Cees den Heijer
Rijkspas	Jacqueline Vlietland, Stefano Sacceddu
Rijksportaal	Raph Rooij
Samenwerkende Catalogi	Kristian Mul
SBR	Victor den Toom
Stelselcatalogus	Ed van der Ark
Tenderned	Rudi van Eijck

Bijlage F. Gebruiksgegevens: rapport ICTU met detail-informatie per open standaard

F.1. Inleiding

In het kader van de Monitor Open standaarden wordt nu voor het vijfde opeenvolgende jaar aandacht besteed aan gegevens over het feitelijk gebruik door overheden van standaarden van de lijst voor 'pas toe of leg uit'. Deze gegevens zijn relatief objectief en geven een goede indicatie van de huidige technische adoptie van standaarden. In dit hoofdstuk worden de gegevens gepresenteerd.

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 in het kader van dit deel van het onderzoek lang niet altijd even eenvoudig gebleken om (voor alle open standaarden) vast te stellen in welke mate die feitelijk gebruikt worden.

In augustus 2017 stonden er 40 (al dan niet samengestelde) standaarden op de lijst voor 'pas toe of leg uit'. In vergelijking met de lijst van een jaar geleden zijn er 3 nieuwe standaarden aan toegevoegd: Ades Baseline Profiles, HTTPS en HSTS en STARTTLS en DANE. Deze drie nieuwe standaarden zijn dit jaar nog niet meegenomen in het deelonderzoek ‘gebruiksgegevens’ omdat het besluit tot plaatsing op de lijst dateert van mei van dit jaar (voor de eerste twee) en van september 2016 (STARTTLS en DANE). Bij een eventuele volgende monitor worden deze standaarden wel meegenomen. Zodoende hebben wij voor 37 standaarden van de huidige lijst het gebruik onderzocht.

Slechts bij een beperkt aantal standaarden is een met relevante cijfers onderbouwd beeld verkregen van het gebruik van de standaard. Daar waar dergelijke gegevens niet voorhanden waren hebben we ons noodgedwongen gebaseerd op meer kwalitatief gerichte uitspraken of op inschattingen die door onze respondenten zijn gemaakt. In paragraaf 3.3 tot en met 3.11 wordt een beeld geschetst van de gebruiksgegevens die wij hebben gevonden. Daarbij wordt de indeling in domeinen aangehouden die Bureau Forum Standaardisatie aanhoudt bij de ordening van de betreffende standaarden.

F.2. Gebruiksgegevens per standaard

De open standaarden van de lijst voor ‘pas toe of leg uit’ zijn zeer verschillend, en de mate waarin het feitelijk gebruik van de standaard kan worden vastgesteld loopt sterk uiteen. Langs drie wegen hebben wij in het kader van dit deelonderzoek informatie verzameld: door

gebruik te maken van een webtool, van een Google-zoekopdracht en door benadering van de betreffende beheerorganisatie.

Webtool / internet.nl: DKIM, DNSSEC, IPv4/v6, SPF en TLS

Tot twee jaar terug is voor drie open standaarden gebruik gemaakt van een webtool (DKIM, DNSSEC en IPv4/v6). Zo doende kon voor deze drie standaarden op zijn minst een goede indicatie worden verkregen van het gebruik. Sinds 2015 biedt het Platform Internet Standaarden[46] de mogelijkheid om via de website internet.nl domeinen te toetsen op het gebruik van de internet- en beveiligings-standaarden die op de 'pas toe of leg uit' lijst van Forum Standaardisatie staan[47]. In datzelfde jaar is Forum Standaardisatie gestart met een halfjaarlijkse evaluatie van overheidsdomeinen op het voldoen aan deze standaarden. In 2015 is daarom - op verzoek van het Forum Standaardisatie - overgestapt op deze nieuwe tool als bron om het gebruik van internet- en beveiligingsstandaarden in kaart te brengen. Deze tool is ook geschikt voor SPF en TLS[48]. De overstap leidde met name in de monitor van 2015 eenmalig tot complicaties bij het vergelijken van gegevens in de tijd door een andere manier van testen. Toch is besloten om de overstap te ondernemen, in de veronderstelling dat internet.nl een betrouwbare en breed (in de zin van: op meerdere standaarden van toepassing) inzetbare mogelijkheid tot meten biedt.

Voor deze monitor is gebruik gemaakt van data uit de halfjaarlijkse Meting Internetveiligheids-standaarden van Forum Standaardisatie. De meest recente rapportage daarover van Bureau Forum Standaardisatie is opgenomen in bijlage D. Bureau Forum hanteert een andere indeling van de overheidscategorieen door op rijksniveau een onderscheid te maken tussen Rijk & GDI enerzijds en uitvoerders anderzijds. Ten behoeve van het thans voorliggende hoofdstuk gebruiksgegevens waar sprake is van een vierdeling (rijk-provincies-gemeenten-waterschappen) is een herberekening van de scores gemaakt, gebaseerd op de ruwe data die aan de basis liggen van de rapportage van Bureau Forum.

Google-zoekopdracht en crawler: ODF, PDF/A-1, PDF/A-2 en PDF1.7

Voor de vier open documentstandaarden (ODF, PDF/A-1, PDF/A-2 en PDF1.7) is - tot op zekere hoogte - een test mogelijk, namelijk door na te gaan hoeveel ODF- en PDF-documenten op websites van overheden te vinden zijn, in vergelijking met het aantal .doc-bestanden. Voor deze meting is net als bij de vorige metingen volstaan met een selectie van acht websites: van de rijksoverheid (rijksoverheid.nl), van drie van de vier G4-gemeenten, van twee provincies en van het Forum Standaardisatie en ICTU. Aanvullend hierop is gebruik gemaakt van een crawler die het Forum Standaardisatie in ontwikkeling heeft. Deze crawler zoekt de bovengenoemde websites af en enkele andere veelbezochte sites en geeft naast een ondersteunend beeld, ook informatie over de mate waarin PDF/A wordt toegepast binnen PDF-bestanden.

Informatie van beheer-organisatie: andere standaarden

[46] Platform Internet Standaarden is een gezamenlijk initiatief van Forum Standaardisatie, het Ministerie van Economische zaken en de Nederlandse internetgemeenschap. Zie https://internet.nl/about/
[47] Uitgezonderd NEN-ISO\IEC 27001 en 27002.
[48] Ook voor DMARC. Deze standaard is weliswaar al positief getoetst maar is nog niet opgenomen op de pas-toe-of-leg-uit lijst en daarom nog niet meegenomen in deze rapportage.

Voor de andere open standaarden die in het onderzoek zijn meegenomen hebben wij de beheer-organisaties benaderd of partijen die anderszins zijn betrokken. Van een aantal van deze organisaties is – in uiteenlopende mate van concreetheid – informatie ontvangen die gebruikt kon worden voor dit onderzoek.

Geen informatie: Aquo-standaard, E-portfolio, NL LOM, OAI-PMH en Stosag
Voor een vijftal standaarden kon de beheer-organisatie geen informatie verstrekken of heeft in het geheel niet gereageerd. Dit betreft de Aquo-standaard, E-portfolio, NL LOM, OAI-PMH en STOSAG. Deze vijf standaarden komen in het vervolg van dit hoofdstuk dan ook niet meer aan bod.

In de paragrafen 3.3. tot en met 3.11 worden de gebruiksgegevens van de open standaarden (binnen de paragrafen in alfabetische volgorde) gepresenteerd. Elk van deze passages is ter verificatie voorgelegd aan de bron, en op basis van een eventuele reactie heeft dat geleid tot enkele aanpassingen.

F.3. Domein internet en beveiliging

In deze paragraaf komen achtereenvolgens de volgende standaarden aan bod: DKIM, DNSSEC, IPv4 & IPv6, ISO-27001 en ISO 27002, SAML, SPF, TLS en WPA2 Enterprirse. Een deel van deze standaarden komt tevens terug in bijlage B waar de rapportage van Bureau Forum Standaardisatie met betrekking tot de IV-standaarden integraal is opgenomen. Een tweetal standaarden uit dit domein (HTTPS en HSTS en STARTTLS en DANE) komt in een eventuele volgende monitor pas aan bod.

F.3.1. DKIM (Anti-phishing)

DKIM koppelt een e-mail aan een domeinnaam met behulp van een digitale handtekening. Het stelt de ontvanger in staat om te bepalen welke domeinnaam (en daarmee welke achterliggende organisatie) verantwoordelijk is voor het zenden van de e-mail. Daardoor kunnen spam- en phishing-mails beter worden gefilterd.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
DKIM	juni 2012	overall: 65 % w.v. Rijk: 52 %	toename van 32% naar 65%

Het overall percentage in bovenstaand kader is het gewogen gemiddelde van twee domeinen: gemeenten (69%) en niet-gemeentelijke overheden (39%). Deze laatste categorie is nader uitgesplitst in: Rijk, provincies en waterschappen. Zie voor meer details tabel F1.

De meting is gedaan medio 2017, nu voor de derde keer met behulp van internet.nl[49]. In de huidige meting voor DKIM wordt gekeken of de DNS-server aangeeft dat er al dan niet een DKIM-configuratie is voor de betreffende domeinnaam. Dit garandeert overigens nog niet dat alle mailservers van de organisatie ook daadwerkelijk mails versturen die aan DKIM voldoen.

[49] Voorheen gebeurde dat met behulp van Phishing scorecard van Measuremail.

Tabel F1: Domeinnamen die aan DKIM voldoen (in %)

(Bron: internet.nl)

DKIM (versie: RFC 6376)	Rijk		Gemeenten		Provincies		Waterschappen		**Totaal**	
	Voldoet aan DKIM	*(n)*	*Voldoet aan DKIM*	*(n)*	*Voldoet aan DKIM*	*(n)*	*Voldoet aan DKIM*	*(n)*	*Voldoet aan DKIM*	*(n)*
Medio 2015	28%	(170)	19%	(411)	38%	(16)	14%	(29)	22%	(626)
Medio 2016	45%	(100)	30%	(398)	41%	(17)	20%	(35)	32%	(550)
Medio 2017	52%	(98)	69%	(396)	50%	(16)	50%	(34)	65%	(544)

Conclusie:

Ongeveer twee op de drie domeinnamen van overheden is in 2017 voorzien van een DKIM-configuratie (vorig jaar: een op de drie). De relatieve 'achterblijvers' uit de vorige meting (gemeenten en waterschappen) hebben een duidelijke inhaalslag gemaakt, met dit jaar een hoogste procentuele score bij de gemeenten. In vergelijking met de meting vorig jaar is sprake van een stijging die zich bij alle overheden voordoet.

F.3.2. DNSSEC (Domeinnaambeveiliging)

Het Domain Name System (DNS) is kwetsbaar, waardoor kwaadwillenden een domeinnaam kunnen koppelen aan een ander IP-adres ('DNS spoofing'). Gebruikers kunnen hierdoor bijvoorbeeld worden misleid naar een frauduleuze website. DNS Security Extensions (DNSSEC) lost dit op. DNSSEC is een cryptografische beveiliging die een digitale handtekening toevoegt aan DNS-informatie. Op die manier wordt de integriteit van deze DNS-informatie beschermd. Aan de hand van de digitale handtekening kan een internetgebruiker (onderwater en volledig automatisch m.b.v. speciale software) controleren of een gegeven DNS-antwoord authentiek is en afkomstig is van de juiste bron. Zodoende is met grote waarschijnlijkheid vast te stellen dat het antwoord onderweg niet is gemanipuleerd.

Standaard	*op lijst sinds*	*gebruik door overheden (%)*		*ontwikkeling in gebruik*
		totaal	*w.v. Rijk*	
DNSSEC	juni 2012	66 %	70 %	groei van 45% naar 66%

In het kader van de Monitor open standaarden is medio 2017 een lijst met 544 domeinnamen van overheden en uitvoeringsorganisaties gecontroleerd, dit jaar voor de derde keer met behulp van de Internet.nl[50]. Met deze test kan het eerste deel van het functioneel

[50] Bij vorige metingen is gebruik gemaakt van de DNNSEC portfolio checker van SIDN Labs (Stichting Internet Domeinregistratie Nederland). De functionaliteit van dat instrument is opgenomen in internet.nl

toepassingsgebied van de standaard gemeten worden: het registreren en in DNS publiceren van internet-domein-namen ('signing'). Of de overheden ook validatie doen wanneer zij andere systemen benaderen (het tweede deel van het functionele toepassingsgebied), is niet getest.

Deze check leverde de volgende resultaten op voor 2016. Het gebruik van DNSSEC ligt binnen de overheid inmiddels op 66% en is gestegen ten opzichte van de meting vorig jaar (in 2016: 45%). In onderstaand overzicht is de ontwikkeling uitgesplitst naar de sectoren binnen de overheid.

Tabel F2: Domeinnamen overheid die voldoen aan DNSSEC
(Bron: Internet.nl)

DNSSEC	Rijk	Gemeenten	Provincies	Waterschappen	**Totaal**
Zomer 2015	28 %	25 %	25 %	17 %	**25 %**
Zomer 2016	59 %	42 %	35 %	37 %	**45 %**
Zomer 2017	70 %	68 %	40 %	50 %	**66 %**

Uit tabel F2 is af te lezen dat de stijging van het gebruik van DNSSEC zich in alle geledingen binnen de overheid voordoet. Bij de gemeenten is de stijging het grootst.

Op de website www.dnsssec.nl valt af te lezen dat thans (september 2017) bijna 49% van de 5,8 miljoen .nl-domeinen zijn voorzien van DNSSEC (vorig jaar: 45%). Inmiddels ligt de overheid derhalve duidelijk boven het landelijk gemiddelde als het gaat om het voldoen aan DNSSEC.

Conclusie:
Het aandeel websites van overheden dat voldoet aan DNSSEC ligt inmiddels op twee op de drie (66%). Het aantal is nog steeds groeiende. De overheden zijn met hun score inmiddels beland boven het landelijk gemiddelde.

F.3.3. IPv6 en IPv4 (Internetnummers)

Internet Protocol versie 6 (IPv6) maakt communicatie van data tussen ICT-systemen binnen een netwerk, zoals internet, mogelijk. De standaard bepaalt dat ieder ICT-systeem binnen het netwerk een uniek nummer (IP-adres) heeft. De belangrijkste motivatie voor de ontwikkeling van IPv6 was het vergroten van de hoeveelheid beschikbare adressen ten opzichte van de tegenwoordig gangbare voorganger IPv4. De aanvankelijke ambitie van het kabinet was om websites en email van de overheid per 2014 toegankelijk te hebben via IPv6.

dat door dezelfde organisatie wordt beheerd. De totaal-percentages gebaseerd op deze eerdere wijze van meten zijn: 5% (voorjaar 2013), 10% (najaar 2013) en 14% (zomer 2014).

Om interoperabiliteit maximaal te waarborgen heeft het College Standaardisatie 'pas toe of leg uit' van toepassing verklaard op de combinatie van IPv4 en IPv6. Een organisatie moet dus beide versies vragen bij de aanschaf van een ICT-product of -dienst.

Standaard	*op lijst sinds*	*gebruik door overheden (%)*		*ontwikkeling in gebruik*
		totaal	*w.v. Rijk*	
IPv6 en IPv4	nov 2010	15 %	33 %	implementatie verloopt traag maar wel verbetering t.o.v. vorig jaar

In het kader van de Monitor open standaarden is zomer 2017 een lijst met 544 domeinnamen van overheden en uitvoeringsorganisaties getest met behulp van Internet.nl (in 2015 en eerdere jaren was de meting gebaseerd op de IPv6 domain readiness tester op ip6.nl). Deze check leverde de volgende resultaten op voor 2017: het gebruik van IPv6 ligt binnen de overheid op 15, tegen 6% vorig jaar[51]. Ook al is het percentage nog laag, afgezet tegen de ambitie, er is wel sprake van een verdere beweging in de gewenste richting. Vorig jaar was ook al sprake van een dergelijke beweging (van 2% naar 6%). Een nadere precisering van levert een volgend beeld op.

Tabel F3: Websites die voldoen aan IPv6 [52]
(Bron: Internet.nl voor 2016 [herberekend] en 2017)

IPv6 *gemeten in de zomerperiode van 2016 en 2017*	Rijk		Gemeenten		Provincies		Waterschappen		**Totaal**	
Zomer 2016	16 %	(152	3 %	(398	6 %	(18)	3 %	(37)	**6 %**	**(605)**
Zomer 2017	33 %	(98)	11 %	(396)	25 %	(16)	9 %	(34)	**15 %**	**(544)**

Conclusie:
De implementatie van IPv6 door overheden verloopt traag, afgezet tegen de ambities, maar er is het tweede achtereenvolgende jaar sprake van een ontwikkeling de goede kant op, nu met een score van 15%.

F.3.4. NEN-ISO/IEC 27001/27002 (Managementsysteem / Richtlijnen en principes informatiebeveiliging)

De NEN-ISO/IEC 27001 standaard ISO 27001 specificeert eisen voor het vaststellen, implementeren, uitvoeren, bewaken, beoordelen, bijhouden en verbeteren van een

[51] Deze 6% voor 2016 is gebaseerd op internet.nl waarna een herberekening heeft plaatsgevonden om de cijfers 2016 vergelijkbaar te maken met de cijfers van daaraan voorafgaande jaren. De onderlinge vergelijkbaarheid tussen de jaren 2016 en 2017 is daardoor niet optimaal. Bij een eventuele volgende monitor zullen de gegevens van 2016 en eerder niet meer in de monitor worden opgenomen.
[52] Bij gemeenten, provincies en waterschappen zijn in de meting 2016 ook de respectievelijke koepelorganisaties meegenomen.

gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie. Het ISMS is ontworpen met het oog op adequate en proportionele beveiligingsmaatregelen die de informatie afdoende beveiligen en vertrouwen bieden.

De NEN-ISO/IEC 27002 standaard 'Code voor informatiebeveiliging' (versie 2013) is een nadere specificatie van NEN-ISO/IEC 27001 en geeft richtlijnen en principes voor het initiëren, implementeren, onderhouden en verbeteren van informatiebeveiliging binnen een organisatie. NEN-ISO/IEC 27002 kan dienen als praktische richtlijn voor het ontwerpen van veiligheids-standaarden binnen een organisatie en effectieve methoden voor het bereiken van deze veiligheid.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
NEN-ISO/IEC 27001 en 27002	mei 2015	Rijk: implementatie via de BIR Alle gemeenten hanteren de BIG als normenkader Waterschappen: implementatie via BIWA Provincies: implementatie via IBI	Rijk: afgerond Alle gemeenten, provincies en waterschappen: vergaande ontwikkeling

Bronnen: Ministerie van BZK / DGOO, KING-gemeenten, IPO en Waterschapshuis

De kaders die gelden voor de Nederlandse overheid (diverse Baselines Informatiebeveiliging: BIG, BIR, IBI, BIWA) zijn afgeleid van de NEN-ISO/IEC 27001- en 27002-norm.

VIR en BIR

Alle departementen en daaraan gelieerde uitvoeringsorganisaties zijn gehouden aan de toepassing van het VIR (Voorschrift Informatiebeveiliging Rijksdienst) en de BIR (Baseline Informatiebeveiliging Rijksdienst). Via VIR en BIR past de Rijksdienst de ISO IEC 27001- en 27002-norm toe. Het voldoen aan het VIR en de BIR vraagt blijvend om aandacht. Daarover leggen de departementen jaarlijks verantwoording af door middel van een ICV (in control verklaring). Alle 11 departementen hebben medio februari 2017 zo'n ICV afgegeven. Die verantwoording legt men af aan de directeur-generaal Overheidsorganisatie (DGOO). Intentie is dat ook in de toekomst DGOO de naleving van VIR en BIR zal blijven monitoren. In 2017 is gewerkt aan een nieuwe versie van de BIR. Deze is gebaseerd op de meest recente versies van relevante ISO normatiek en andere normen van de pas-toe-of-leg-uit lijst.

BIG

Alle Nederlandse gemeenten hanteren de BIG als normenkader voor informatiebeveiliging, deze is gebaseerd op de BIR / ISO27001/2. De implementatie van de BIG loopt sinds 2013.

Gemeenten verantwoorden zich elk jaar over de kwaliteit van de informatieveiligheid van diverse informatiesystemen. In 2017 gebeurt dit voor het eerst met een nieuwe Audit systematiek: de Eenduidige Normatiek Single Information Audit (ENSIA). ENSIA maakt het beantwoorden van de uitvraag over informatieveiligheid beter en efficiënter. Met ENSIA verantwoordt de gemeente zich vanaf 2017 ook horizontaal aan de gemeenteraad. ENSIA sluit aan op de gemeentelijke planning en control-cyclus. Zo krijgt het gemeentebestuur

meer overzicht over de informatieveiligheid van hun gemeente. Voorheen waren er aparte verantwoordingsprocedures voor de Basisregistratie Personen (BRP), Paspoortuitvoeringsregeling (PUN), Digitale persoonsidentificatie (DigiD), Basisregistratie Adressen en Gebouwen (BAG), Basisregistratie Grootschalige Topografie (BGT) en de Structuur uitvoeringsorganisatie Werk en Inkomen (Suwinet). Met ENSIA is dit nu gebundeld. Dat wil zeggen dat gemeenten in één keer slim verantwoording afleggen over het gebruik van de registratiesystemen. Kortom, met ENSIA:

- heeft het gemeentebestuur meer overzicht over de stand van zaken van de informatieveiligheid en kan het hier beter op sturen;
- sluit het verantwoordingsproces over informatieveiligheid aan op de gemeentelijke planning & control-cyclus;
- vermindert de verantwoordingsdruk bij gemeenten, omdat zes verantwoordingsprocedures zijn samengevoegd.

De ENSIA-vragenlijst is gebaseerd op de volledige vragenlijst van de BIG (ISO27001/2). De ENSIA-tool wordt op 1 juli 2017 beschikbaar gesteld aan gemeenten. Afronding van de vragenlijsten is uiterlijk 31 december 2018. Gemeenten zijn positief over de introductie van ENSIA. Op dit moment, eind juni 2017, zijn vrijwel alle gemeenten klaar om met de implementatie te starten.

ENSIA is niet bedoeld voor integrale monitoring op het feitelijk gebruik. Echter, bijna 80 procent van de vragen die in de vragenlijst zijn opgenomen, worden door verticale toezichthouders hergebruikt. De ministeries van SZW, I&M en BZK monitoren daardoor het feitelijke gebruik van dat deel van de BIG dat voor de eigen basisregistratie van belang is.

IBI

De provincies hebben dit jaar de monitoringstool ten behoeve van de IBI, gebaseerd op de 27001/27002 en zoals afgesproken in het convenant interprovinciale regulering informatieveiligheid, weer ingevuld. De monitor laat een positieve tendens zien. Provincies werken gestaag door aan implementatie van de standaard.

Ook hebben de provincies voor hun organisaties een gezamenlijke doorontwikkeling van de 2700x afgesproken. Dit vergt interprovinciaal op strategisch niveau nog besluitvorming. Het einddoel wordt afgestemd. De weg er naar toe geeft ruimte voor maatwerk per provincie.

BIWA

De Waterschappen hebben in 2013 afgesproken de Baseline Informatiebeveiliging Waterschappen (BIWA) door te voeren. De BIWA is gebaseerd op de NEN-ISO/IEC 27001 / 27002. Behalve dat elk waterschap een eigen groeipad heeft om te voldoen aan de BIWA worden onder regie van Het Waterschapshuis via een landelijk programma Informatieveiligheid diverse thema's van informatiebeveiliging collectief uitgewerkt en worden kennis en ervaringen actief uitgewisseld. Jaarlijks vindt sectorbreed een inventarisatie plaats naar de voortgang en volwassenheid van informatiebeveiliging middels een self assessment. Daarnaast zullen in oktober en november 2017 alle waterschappen door een onafhankelijk partij extern beoordeeld worden op compliance met de BIWA.

De meest recente waterschapsectorbrede uitvraag naar de voortgang van de BIWA-implementatie (cijfers juni 2017 over 2016) brengt het volgende beeld naar voren:

- 100% heeft een gap- en/of een risico-analyse uitgevoerd op conformiteit met de BIWA
- 100% heeft het Beleid Informatiebeveiliging laten goedkeuren door het bestuur
- 86% heeft activiteiten voor informatiebeveiliging gebudgetteerd voor 2017
- 96% heeft een BIWA-implementatieplan opgesteld
- 77% heeft in het jaarverslag gerapporteerd over informatiebeveiliging
- 91% heeft bewustzijnsactiviteiten rond informatiebeveiliging ontplooid

Daarnaast zijn alle waterschappen in 2017 in samenwerking met Rijkswaterstaat aangesloten bij het CERT Watermanagement.

Conclusie:
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) zijn toegepast. Daarover hebben alle 11 departementen medio februari 2017 een ICV (in control verklaring) afgegeven. Daarnaast is in 2017 gewerkt aan een nieuwe BIR, die is gebaseerd op de meest recente versies van relevante ISO normatiek en andere normen van de pas-toe-of-leg-uit lijst.

Alle Nederlandse gemeenten hanteren inmiddels de BIG als normenkader voor informatie-beveiliging, deze is gebaseerd op de BIR / ISO27001/2.

Bij de provincies worden de standaarden ISO/IEC 27001 en 27002 geïmplementeerd via de IBI. Op dit moment zijn geen nadere gegevens over de voortgang van de implementatie beschikbaar.

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%). Eind 2017 vindt wederom een sectorbrede meting plaats naar de voortgang op de implementatie van informatie-beveiliging (self assessment). Dit jaar komt daar nog een beoordeling bij door een onafhankelijke externe partij op compliancy met de BIWA.

F.3.5. SAML (uitwisseling inloggegevens)

De Security Assertion Markup Language (SAML) is een XML-gebaseerd raamwerk voor het communiceren van gebruikers authenticatie, rechten, en attribuut informatie. SAML biedt organisatie entiteiten de mogelijkheid om claims te maken over de identiteit, attributen en rechten van een subject (een entiteit welke vaak een menselijke gebruiker is) aan andere entiteiten zoals Internet applicaties of diensten.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
SAML	mei 2009	DigiD: 48% eHerkenning: 100%	doorzettende groei bij DigiD

Twee belangrijke toepassingen van SAML in Nederland zijn eHerkenning en DigiD, waarmee bedrijven respectievelijk burgers zich kunnen authentiseren en identificeren bij overheden. Beide kennen hun eigen toepassingsprofiel ('verbijzondering') van SAML. Daarnaast kunnen overheden intern SAML toepassen, bij voorbeeld voor authenticatie van personeel binnen het eigen applicatielandschap.

Logius heeft inzicht in de aansluitingen op eHerkenning en DigiD. Dit zijn functionerende koppelingen van overheid naar Logius. Vanuit eHerkenning loopt de koppeling op basis van SAML naar aanbieders van authenticatie voor bedrijven. In het geval van eHerkenning lopen aansluitingen exclusief via SAML; alternatieven zijn er niet[53]. Bij DigiD is SAML ingevoerd als alternatief voor twee andere koppelvlakken.

Overheden (en andere partijen) kunnen op DigiD aansluiten via een ouder koppelvlak of via SAML. In drie jaar tijd is het percentage SAML-aansluitingen opgelopen van 17% naar 24%, naar 48% dit jaar[54].

Van alle eHerkenning-aansluitingen loopt 100% via SAML. In onderstaand overzicht is uitgesplitst naar overheidssectoren. De absolute aantallen lopen gestaag op.

Tabel F4: Aansluitingen bij eHerkenning en DigiD, gebaseerd op SAML
(Bron: opgave Logius; eherkenning.nl[55])

SAML *gecheckt: augustus 2014, augustus 2015, augsutus 2016, oktober 2017*	Rijk + Uitvoerings-organisaties / ZBO's + OOV + eOverheid				Gemeenten				Provincies				Waterschappen				**Totaal**			
	2014	*2015*	*2016*	*2017*	*2014*	*2015*	*2016*	*2017*	*2014*	*2015*	*2016*	*2017*	*2014*	*2015*	*2016*	*2017*	*2014*	*2015*	*2016*	*2017*
SAML bij eHerkenning	19	20	17	26	75	126	142	167	5	5	8	9	0	1	1	1	99	152	168	203
SAML bij DigiD	4	12	17	21	54	80	109	266	1	1	2	2	0	0	0	1	59	93	128	290
Totaal	*23*	*32*	*34*	*47*	*129*	*206*	*251*	*433*	*6*	*6*	*10*	*11*	*0*	*1*	*1*	*2*	*158*	*245*	*296*	*493*

Conclusie:
SAML is de standaard geworden voor (nieuwe) aansluitingen waarbij burgers of bedrijven inloggen bij de overheid. Het is onbekend hoeveel organisaties SAML gebruiken voor de authenticatie van medewerkers.

[53] Niet al het berichtenverkeer verloopt via SAML; voor enkele andere toepassingsgebieden worden andere standaarden gebruikt.
[54] Dit zijn de percentages voor de onderzochte deelnemers; voor alle deelnemers zijn de percentages respectievelijk 19%, 28% en ook 48%.
[55] https://www.eherkenning.nl/aansluiten-op-eherkenning/wie-zijn-aangesloten/

F.3.6. SPF (E-mailbeveiliging)

SPF controleert of de mailserver die een e-mail wil versturen namens het e-maildomein deze e-mail mag verzenden. SPF specificeert een technische methode om afzenderadres-vervalsing detecteerbaar te maken. SPF biedt de mogelijkheid te controleren of een bericht aangeleverd wordt vanaf een server die daartoe gerechtigd is. Dit doet SPF door de authenticiteit van de domeinnaam in het afzenderadres van de ontvangen mail herleidbaar te maken via de in DNS gepubliceerde IP-adressen van de verzendende mailserver(s). Indien een mailserver niet in de lijst met gepubliceerde IP-adressen staat (de zogeheten SPF-records) maar toch mail verstuurt met het betreffende domein als afzender, dan wordt de mail als niet geauthenticeerd beschouwd.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
SPF	mei 2015	76% w.v. Rijk: 60%	flinke toename (2016: 54%)

SPF was nog niet opgenomen in de monitor 2015 vanwege plaatsing op de pas-toe-of-leg-uit lijst in mei van dat jaar. In de zomer 2015 is wel een meting gedaan over de toepassing van SPF, ook toen met behulp van internet.nl. Dat biedt de mogelijkheid om de ontwikkeling van het gebruik op drie meetmomenten te vergelijken. Uit het overzicht blijkt dat sprake is van een toename, van 32% in 2015 naar 54% in 2016 en nu 76%.

In deze meting wordt alleen getest of de domeinnaamserver via SPF vertelt welke e-mail-servers gerechtigd zijn. Er wordt niet getest of deze 'SPF-record' strikt genoeg is. Zo kan het zijn dat hier in staat dat alle e-mailservers ter wereld gerechtigd zijn. Het kan zelfs zijn dat ten onrechte eigen mailservers niet in de SPF-lijst staan en daarmee mogelijk als spam worden gezien door anderen. In de meting wordt niet getest of binnenkomende mail bij deze organisaties ook getoetst wordt middels de SPF-standaard.

Uitgesplitst naar categorieën overheden ziet het beeld er als volgt uit.

Tabel F5: Mailservers overheid die voldoen aan SPF
(Bron: Internet.nl)

SPF	Rijk	Gemeenten	Provincies	Waterschappen	**Totaal**
Zomer 2015	35 %*	31 %	35 %*	35 %*	**32 %**
Zomer 2016	55 %	55 %	59 %	46 %	**54 %**
Zomer 2017	60 %	80 %	88 %	68 %	**76 %**

** Over 2015 is alleen een gecombineerd percentage bekend voor Rijk, provincies èn waterschappen.*

Conclusie:
Het aandeel websites van overheden dat voldoet aan SPF ligt inmiddels boven op driekwart en laat in vergelijking met vorig jaar (wederom) een behoorlijke stijging zien. De groei is in alle onderscheiden categorieën overheden terug te vinden, maar bij het Rijk blijft de groei dit jaar wel wat achter in vergelijking met de andere overheden.

F.3.7. TLS (Beveiligde internetverbinding)

TLS is een protocol, dat tot doel heeft om beveiligde verbindingen op de transportlaag over het internet te verzorgen. De standaard wordt gebruikt bovenop standaard internet transport protocollen (TCP/IP) en biedt een beveiligde basis, waar applicatie protocollen als HTTP (webverkeer) of SMTP en IMAP (mailuitwisseling) op hun beurt weer op kunnen bouwen en gebruik van kunnen maken.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
TLS	sept 2014	93%; daarvan ruim 4 op de 5 cf. richtlijn NCSC Rijk: 83 %	verdere flinke stijging, ook al was score vorig jaar al hoog

Voor TLS heeft het Nationaal Cyber Security Centrum (NCSC) voorgeschreven hoe overheden hun webservers moeten inrichten[56]. Door te werken conform deze richtlijn, verkleint de overheid de kans dat beveiligde gegevensstromen alsnog worden gemanipuleerd of afgelezen door kwaadwillenden. Op de lijst voor 'pas toe of leg uit' staat dat bij beveiligde verbindingen gebruik moet worden gemaakt van TLS, maar niet wanneer er een beveiligde verbinding gebruikt moet worden. De eigenaar van een webserver kan daarom een reden hebben waarom hij niet TLS ondersteunt.

Met behulp van Internet.nl is getoetst of de website ('HTTPS') ondersteuning biedt aan TLS. In deze test is derhalve alleen de website getest; er is niet gekeken naar andere verbindingen via TLS. Het is bijvoorbeeld ook mogelijk om diensten als mail (IMAP, SMTP) en berichten (XMPP) via TLS te laten lopen. Zie tabel F6 voor de uitsplitsing naar categorieën overheden.

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

Tabel F6: Websites die ondersteuning bieden aan TLS
(Bron: Internet.nl)

TLS	Rijk		Gemeenten		Provincies		Waterschappen		**Totaal**	
	Wel, en cf. richtlijn NCSC	*Wel maar niet cf. richtlijn NCSC*	*Wel, en cf. richtlijn NCSC*	*Wel maar niet cf. richtlijn NCSC*	*Wel, en cf. richtlijn NCSC*	*Wel maar niet cf. richtlijn NCSC*	*Wel, en cf. richtlijn NCSC*	*Wel maar niet cf. richtlijn NCSC*	*Wel, en cf. richtlijn NCSC*	*Wel maar niet cf. richtlijn NCSC*
Zomer 2015	11 %	40 %	4 %	69 %	0 %	69 %	0 %	72 %	**6 %**	**61 %**
Zomer 2016	43 %	22 %	21 %	61 %	24 %	53 %	40 %	43 %	**26 %**	**53 %**
Zomer 2017	52 %	31 %	83 %	12 %	53 %	27 %	79 %	12 %	**77 %**	**16 %**
Ondersteunt TLS niet in 2017	*18 %*		*5%*		*20%*		*9%*		***8%***	

Meer dan 9 op de 10 websites van overheden (93%) biedt ondersteuning aan TLS. Daarbij laat elk van de te onderscheiden categorieën overheden groei zien in vergelijking met vorig jaar (in 2016: 79%). De volgende zaken vallen op:

- de categorie Rijk (brede definitie) blijft –net als vorig jaar- achter bij het gemiddelde beeld met 83% maar is wederom wel bezig met een (beperkte) inhaalslag; de groei is daar het grootst;
- er is sprake van een duidelijke verschuiving, richting toepassing van TLS conform de richtlijn van het NCSC;
- vorig jaar scoorde de categorie Rijk nog relatief hoog op inpassing van TLS conform de richtlijn van het NCSC. Dit jaar is Rijk door de andere overheden op dit punt ingehaald. Met name de inhaalslag bij gemeenten en waterschappen is groot met scores rond de 80% waar Rijk en provincies rond de 50% scoren.

Conclusie:
De standaard TLS komen we veel tegen bij overheidswebsites (93%) en het gebruik is ook gegroeid in vergelijking met vorig jaar (in 2016: 79%). De aanpak conform de richtlijn van het NCSC komt ook steeds meer voor: inmiddels bij driekwart (77%) van de hier onderzochte websites (vorig jaar: 26%).

F.3.8. WPA2 Enterprise (Toegang tot een wifi-netwerk met een account)

Steeds meer komt het voor dat medewerkers van overheidsorganisaties WiFi-toegang nodig hebben op andere locaties dan hun eigen werkplek. Als de gastlocatie WiFi-toegang biedt met een gedeeld wachtwoord, dan moeten zij handmatig een verbinding maken met het WiFi-netwerk door het gedeelde wachtwoord in te geven. Dit is onveilig en inefficiënt.

WPA2 Enterprise maakt het mogelijk dat gebruikers automatisch en veilig toegang krijgen tot aangesloten WiFi-netwerken via authenticatie op basis van bestaande identiteitsgegevens.

Diensten zoals Govroam, Rijk2Air en Eduroam maken al gebruik van WPA2 Enterprise, en bieden WiFi-toegang met een hoog beveiligingsniveau zonder dat de gebruiker extra handelingen hoeft te verrichten.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
WPA Enterprise	februari 2016	Beperkt	Stijging

De enige indicator voor gebruik van WPA2 Enterprise is het gebruik van federatieve diensten als Govroam en Eduroam. Als organisaties daarop aangesloten zijn, passen zij WPA2 Enterprise toe voor hun gebruikers èn de gebruikers van andere deelnemers aan de federatie. Het is waarschijnlijk dat er ook organisaties WPA2 Enterprise toepassen zonder dat zij aansluiten bij een federatieve dienst. In die zin is WPA2 Enterprise vergelijkbaar met SAML.

Op 1 sept 2016 had Govroam 49 deelnemers. Op 1 september 2017 waren dat er 132. Een aantal van deze deelnemers is nog bezig de aansluiting te realiseren maar heeft wel een overeenkomst ondertekend met de Stichting Govroam.

Op 1 september 2017 had Eduroam 199 deelnemers in de educatieve sector[57]. Hieronder vallen bijna alle instellingen voor hoger onderwijs, een groot deel van de mbo-instellingen en medisch centra, bibliotheken en instituten. In mei 2016 waren dit er nog 157[58].

Bij de onderzoeker en de beheerder van Govroam zijn geen nadere ontwikkelingen bekend die de adoptie van de standaard verder stimuleren. Zij zien wel een bredere beweging binnen de overheid om inloggen op gastnetwerken van andere overheden aan te pakken.

Conclusie:
Govroam maakt een flinke ontwikkeling mee en lijkt daarmee een inhaalslag te voeren op de educatieve sector. Er lijkt nog veel ruimte te zijn voor groei in adoptie. Buiten de federatieve diensten voor WPA2 Enterprise is er geen stimulans hiervoor; gezien het doel van de standaard, lijkt het ook vooral wenselijk dat adoptiebevordering gebeurt via federatieve diensten.

F.4. Domein document en (web/app)content

In deze paragraaf komen achtereenvolgens aan bod: CMIS, Digitoegankelijk, ODF in combinatie met PDF 1.7, PDF/A1 en PDF/A2 en SKOS. Ades Baseline Profiles komt bij deze monitor nog niet aan bod.

F.4.1. CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)

Content Management Interoperability Services (CMIS) is een open standaard die een scheiding mogelijk maakt tussen zogenaamde 'content repositories' en content applicaties. Hierdoor kunnen content (ongestructureerde data, zoals documenten en e-mails) en

[57] https://www.eduroam.nl/instellingen/
[58] https://web.archive.org/web/20160520065015/https://www.eduroam.nl/instellingen/

bijbehorende metadata (beschrijvende data) gemakkelijker worden uitgewisseld. Met behulp van CMIS kunnen applicaties als Content Management Systemen (CMS) en Document Management Systemen (DMS) werken met content die afkomstig is uit verschillende repositories (een soort van opslagplaats voor ongestructureerde data), zonder nieuwe koppelingen te hoeven bouwen of gebruik te hoeven maken van leverancierseigen oplossingen. Het is hierdoor eenvoudiger om informatie en de bijbehorende metadata uit verschillende databases en over organisatiegrenzen heen uit te wisselen. Bovendien is het met CMIS eenvoudiger om te migreren van een systeem naar een ander systeem.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
CMIS	dec 2014	Rijk: alle departementen, maar gebruik onduidelijk	n.v.t.

Bron: Ministerie van BZK

Het beeld ten aanzien van de gebruiksgegevens met betrekking tot CMIS is vergelijkbaar met dat van het vorige jaar. Ook vorig jaar was dat al het geval (vergelijkbaar met 2015). Voor wat betreft het Rijk is er sprake van twee grote toepassingen van CMIS:

- de websites van de Rijksoverheid, meer specifiek via het platform van de Ministeries van Algemene Zaken en van Veiligheid en Justitie;
- de doc-diensten van de 11 ministeries; acht daarvan worden geleverd door SSC-ICT, drie departementen hebben aparte documentsystemen.

Mogelijk is er daarnaast nog sprake van kleinere toepassingen; het zicht daarop ontbreekt.

Kanttekening bij het bovenstaande is dat CMIS wel wordt ondersteund, maar dat niet wordt bijgehouden of er daadwerkelijk gebruik gemaakt wordt van de mogelijkheden die CMIS biedt. Er wordt evenmin getoetst of CMIS volledig conform de specificatie wordt toegepast. CMIS is vaak standaard aanwezig in doc-systemen maar toepassing in de praktijk is laag omdat er relatief weinig documenten worden uitgewisseld tussen de systemen.

Conclusie:
Alle departementen zijn 'in beeld' als het gaat om het gebruik van CMIS. Harde gegevens over gebruik zijn evenwel niet beschikbaar. Van andere overheden en instellingen uit de publieke sector is geen informatie bekend.

F.4.2. Digitoegankelijk (Toegankelijkheid websites)

De standaard EN 301 549 voorziet in het toegankelijk maken van overheidswebsites. EN 301 549 bevat de internationale toegankelijkheidsstandaard WCAG 2.0, die ervoor zorgt dat content op websites en in webapplicaties ook toegankelijk is voor mensen met een functiebeperking.

Deze standaard heeft grote overeenkomsten met Webrichtlijnen (niveau AA); het belangrijkste verschil is het schrappen van het principe 'Universeel' uit de Webrichtlijnen met achterliggende normen voor systeem-onafhankelijke websites. De Europese standaard is sinds december 2016 per Europese richtlijn verplicht en wordt in Nederland 'Digitoegankelijk' genoemd.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
Digitoegankelijk	oktober 2016	Beperkt	Nieuw

De Dienst Logius beheert het dossier Digitoegankelijk voor het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. De organisatie meldt:

"Eind 2015 / begin 2016 is door middel van een belronde langs relevante organisaties geïnventariseerd hoe het er voor stond met het toepassen van de Webrichtlijnen. Deze organisaties is gevraagd om dat weer te geven in een 'toegankelijkheidsverklaring' en om deze verklaring vervolgens te publiceren op de website. Dat leverde het volgende resultaat op:
Op 18 maart 2016 hadden 178 van de 390 Nederlandse gemeenten een actuele verklaring op de website staan. Dit was op dat moment 46 procent van alle gemeenten. Van de 12 provincies hadden 2 provincies een verklaring. Van de 22 waterschappen waren er 9 die een verklaring op de website hadden staan.
Er zijn op dit moment geen nieuwere cijfers beschikbaar. Die zouden dan betrekking moeten hebben op Digitoegankelijk en niet langer op Webrichtlijnen. Er wordt nu gewerkt aan een automatische manier van monitoring. Tegelijkertijd zal in 2018 vanuit Europa een nieuwe toegankelijkheidsverklaring worden geïntroduceerd. De implementatie hiervan alsmede van een geautomatiseerde monitor zal dan gaan zorgen voor een gestructureerde manier van rapporteren van gegevens rond digitale toegankelijkheid."

Er is niet gekeken naar de inhoud van de verklaring. Andere soorten overheden zijn niet opgenomen in deze inventarisatie.

De vorige monitor-rapportages gebruikten het Waarmerk Drempelvrij als indicator voor het toepassen van Webrichtlijnen. Daarbij werd gekeken uit een lijst van ruim 600 overheden, welke er een afdoende waarmerk hadden behaald. Dit aantal daalde de afgelopen jaren sterk, waarschijnlijk voornamelijk doordat het Ministerie van BZK (en de VNG) is gaan vragen om zelfverklaringen. Het aantal verklaringen was een stuk hoger dan het aantal behaalde waarmerken. Ter illustratie; in de zomer van 2016 waren er totaal 13 overheden uit de lijst, die met een waarmerk aantoonden de Webrichtlijnen te implementeren. Dit aantal lijkt bij een quick scan, (zeer licht) gedaald in de zomer van 2017.

In november 2016 publiceerde Stichting Accessibility een rapport over de toegankelijkheid van Nederlandse websites[59]. Zonder kwantitatieve uitspraken te doen, signaleerde dit rapport dat overheidswebsites voorloper zijn als het gaat om toegankelijkheid.

De Europese richtlijn wordt in Nederlandse wetgeving geëffectueerd uiterlijk 23 september 2018. Dit zal de adoptie van de standaard waarschijnlijk stimuleren. Daarnaast wordt het toepassingsgebied van Digitoegankelijk mogelijk verbreed. In dat geval zullen ook documenten en mobiele applicaties aan vergelijkbare toegankelijkheidseisen moeten gaan voldoen.

[59] https://www.accessibility.nl/nieuws/2016/11/veel-websites-nog-steeds-slecht-toegankelijk

Conclusie:
De adoptie van Digitoegankelijk is maar beperkt inzichtelijk. Op basis van de voorhanden zijnde informatie lijkt het er op dat een groot aantal organisaties wel zich bewust is van het bestaan van de standaard (of de voorloper daarvan), maar dat waarschijnlijk de meeste er niet aan voldoen. Mede afhankelijk van de inrichting (en consequenties) van de verplichtende wetgeving in Nederland, is de verwachting dat de adoptie flink zal toenemen.

F.4.3. ODF 1.2 / PDF 1.7 / PDF/A-1 en PDF A-2 (Documentbewerking / Documentpublicatie)

De lijst voor 'pas toe of leg uit' telt op dit moment vier open document-standaarden: ODF, voor bewerkbare documenten, en drie varianten van PDF voor niet-bewerkbare documenten.

- ODF 1.2 (versie: 1.2) is een open standaard voor tekstdocumenten, (vector-)tekeningen, presentaties en rekenbladen (spreadsheets).
- PDF/A-1 (versie: NEN-ISO 19005-1:2005). Dit deel van ISO 19005 specificeert hoe Portable Document Format (PDF) 1.4 voor lange termijn archivering van elektronische documenten dient te worden gebruikt. Het heeft betrekking op documenten met combinaties van data in de vorm van karakters, rasters en vectoren.
- PDF/A-2 (versie: ISO 19005-2). Deze standaard slaat de brug tussen PDF/A-1 en PDF 1.7 waarbij PDF/A-2 een betere geschiktheid heeft voor langdurig archiveren van documenten waar 'elementen' inzitten die niet door PDF/A-1 worden ondersteund en waarbij PDF 1.7 kan worden gebruikt voor 'elementen' die niet door PDF/A-2 ondersteund worden.
- PDF 1.7 (versie: ISO 32000-1:2008). Deze standaard specificeert een bestandsformaat voor het weergeven van elektronische documenten. Het uitgangspunt van de standaard is dat het gebruikers mogelijk wordt gemaakt documenten uit te wisselen en te bekijken, zowel onafhankelijk van de omgeving waarin ze zijn gecreëerd, alsook de omgeving waarin ze worden uitgeprint of bekeken. Elk PDF v1.7 document bevat een complete beschrijving van een document, inclusief tekst, font objects (embedded of met typeface beschrijving), afbeeldingen, audio, video, en 2D/3D graphics.

Standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
ODF 1.2	juni 2012	geen overheidsbrede cijfers	
PDF/A-1	nov 2008	(enkele websites gecheckt: daarop PDF veel gebruikt, maar ook meer .doc dan .odt-documenten).	geen eenduidige conclusie te trekken
PDF/A-2	juni 2012		
PDF 1.7	nov 2009	Weinig PDF/A.	

In het onderzoek beperken wij ons tot gebruik van documentstandaarden op websites. Daarbij zien we dat PDF veel gebruikt wordt – het formaat dat het breedst ondersteund door ontvangende apparaten – van Linux desktop tot Windows tablet, en de opmaak in hoge mate garandeert.

Omdat ODF een formaat is voor bewerkbare (en herbruikbare) documenten, kan het vooral als volwaardig alternatief gezien worden voor documenten in een leveranciersafhankelijk formaat als het doel is dat de ontvanger het document verder kan bewerken. Voor gegevenssets die herbruikbaar moeten zijn (als hoogwaardige open data) is naast ODF (spreadsheet), het ook mogelijk om de CSV, XML en RDF-standaarden te gebruiken. Deze drie staan op de lijst van het Forum Standaardisatie als aanbevolen standaarden. Een alternatief voor documenten is daarnaast in veel situaties, het plaatsen van de tekst in een webpagina.

Binnen PDF zijn veel extra mogelijkheden (/specificaties). Om compatibiliteit en duurzaamheid het best te garanderen is bij het toepassen van PDF het daarom het beste de standaarden PDF/A-1, PDF/A-2 of PDF 1.7 te gebruiken.

Ten opzichte van vorige jaren is het beeld weinig veranderd. Wel is er voor het eerst een tweede meetmethode toegepast waarmee te zien is hoeveel documenten aan de PDF/A-standaarden.

Stakeholdergegevens: ODF
OpenDoc Society geeft aan wel de ambitie maar geen financiering te hebben voor het monitoren van het gebruik van ODF in Nederland.
Verder meldt zij: *"De ondersteuning in de markt van de ODF standaard is een genuanceerd verhaal, omdat er in de markt van officetoepassingen nogal een complexe marktsituatie (feitelijk: marktfalen) is. Met name Microsoft opereert zeer strategisch voor wat betreft het ondersteunen van standaarden, waarbij cruciale delen van de standaard in de publieke sector niet of niet goed worden ondersteund. Er zijn voldoende producten in de markt te vinden die ODF goed ondersteunen, en er komen nog steeds nieuwe implementaties bij. De ODF plugfests die we vanuit OpenDoc Society organiseren voldoen daarbij in een behoefte om aan te sturen op aantoonbare interoperabiliteit. [..]*
Tijdens het ODF plugfest in Rome zal oa. de Britse overheid rapporteren over hun voortgang. Op gov.uk staan alleen nog ODF-documenten."
Wat betreft ontwikkelingen meldt OpenDoc Society: "Er zou eigenlijk een extra (ook financiele) stimulans gegeven moeten worden aan het versnellen van de totstandkoming van ODF 1.3, en aan de ontwikkeling van belangrijke features zoals collaboration. Er zijn waardevolle en strategische open source-projecten zoals WebODF, die doordat voldoende middelen ontbreken niet het herstel van het evenwicht van de markt kunnen bewerkstelligen. Met een beperkte impuls zouden die voor een enorme doorbraak kunnen zorgen."

Stakeholderinformatie: PDF
Het Nationaal Archief geeft aan: geen gegevens bijhouden over kwantitatief en kwalitatief gebruik van PDF in Nederland. Over de interne organisatie meldt zij dat: *"alle inkomende en uitgaande documentatie gescand wordt volgens de PDF/A 1b-standaard. Deze scanners zijn ingericht volgens 19005-ISO-standaard. Alle documentatie die via de onofficiële wijze wordt gescand en/of opgeslagen (via reguliere MFP's) (door medewerkers zelf) krijgen geen specifiek PDF/A-formaat."*

In gesprekken in voorgaande jaren heeft Adobe, belangrijkste leverancier van PDF-software en contribuant aan de specificatie, aangegeven geen gegevens over gebruik te hebben.

Zoekresultaten

Met behulp van Google is het aantal zoekresultaten per site opgevraagd van bestandstype .pdf, met de extensies .ods/.odt/.odp en met de extensies .doc/.docx/.xls/.xlsx/.ppt/.pptx. Dit is gedaan op 8 verschillende websites. Dit geeft geen uitsluitsel over de PDF-versie, zodat op deze manier niet nagegaan kan worden hoeveel bestanden voldoen aan PDF/A-1, PDF/A-2 of PDF 1.7.[60]

Tabel F7: PDF-, ODF- en MS office-bestanden op enkele websites

(Bron: Google)

	.pdf (incl. andere pdf-versies)			**.odt** *)			**.doc** **)		
	Zomer 2015	*Zomer 2016*	Zomer 2017	*Zomer 2015*	*Zomer 2016*	*Zomer 2017*	*Zomer 2015*	*Zomer 2016*	*Zomer 2017*
rijksoverheid.nl	118.000	122.000	118.000	209	197	110	564	512	566
amsterdam.nl	36.500	28.500	25.200	0	0	0	3.940	3.940	4.240
rotterdam.nl	40.900	19.600	6.010	0	0	0	903	587	263
utrecht.nl	27.000	20.200	6.390	0	0	0	247	142	17
drenthe.nl	6.310	7.580	6.310	0	0	0	248	215	179
zuid-holland.nl	2.080	15.600	11.000	0	0	0	110	189	201
forumstandaardisatie.nl	1.430	446	1.270	22	11	13	54	14	14
ictu.nl	863	236	56	18	4	0	46	7	0
Totaal	***233.083***	***214.162***	***174.236***	***249***	***212***	***113***	***6.112***	***5.606***	***5480***

**) alle ODF-formaten, namelijk .odt, .ods en .odp*
***) en verwante formaten, dus .doc, .docx, .xls, .xlsx, .ppt, .pptx*

	.pdf + .odt *) **als % van alle bestanden**			**verhouding .odt** *) **/ .doc** **)		
	Zomer 2015	*Zomer 2016*	Zomer 2017	*Zomer 2015*	*Zomer 2016*	*Zomer 2017*
rijksoverheid.nl	99,5 %	99,6 %	99,5 %	0,37:1	1:1	0,72:1
amsterdam.nl	94,2 %	87,9 %	85,6 %	0:1	0:1	0:1
rotterdam.nl	89,7 %	97,1 %	95,8 %	0:1	0:1	0:1
utrecht.nl	96,4 %	99,3 %	99,7 %	0:1	0:1	0:1
drenthe.nl	94,6 %	97,2 %	97,2 %	0:1	0:1	0:1
zuid-holland.nl	97,4 %	98,8 %	98,2 %	0:1	0:1	0:1
forumstandaardisatie.nl	97,6 %	97,0 %	98,9 %	0,40:1	0,69:1	0,93:1
ictu.nl	95,5 %	97,2 %	100 %	0,50:1	0,55:1	:0***)
Totaal	***97,4 %***	***97,5 %***	***97,0 %***			

**) alle ODF-formaten, namelijk .odt, .ods en .odp*
***) en verwante formaten, dus .doc, .docx, .xls, .xlsx, .ppt, .pptx*
****) geen ODF, .doc of aanverwante documenten*

[60] Door de werking van zoekmachines is het aantal documenten slechts een schatting door de zoekmachine van het werkelijke aantal documenten. Bij grotere aantallen lijkt de inschatting hoger uit te vallen.

Uit bovenstaande tabel kunnen de volgende conclusies worden getrokken:[61]

- voor alle onderzochte websites (rijksoverheid: alle departementen zijn ondergebracht op www.rijksoverheid.nl) blijkt het overgrote deel van alle documenten op de website in een PDF-format te zijn.
- ODF (.ods/.odt/.odp) treft Google net als bij de vorige metingen alleen aan in beperkte mate op www.rijksoverheid.nl en op de websites van het Forum Standaardisatie.
- het aantal MS office-bestanden (.doc/.docx/.xls/.xlsx/.ppt/.pptx) is beperkt maar nog wel beduidend hoger het aantal ODF-bestanden. De gemeente Amsterdam laat zowel relatief als in absolute aantallen elk jaar een hoger aantal zien, terwijl Rotterdam en Utrecht duidelijk minder MS Office-bestanden op hun sites hebben – maar ook het aantal PDF-documenten daalt daar.

Crawler

Bureau Forum Standaardisatie is bezig met de ontwikkeling van een *crawler* die systematisch websites afzoekt naar documenten, en valideert of deze aan de documenstandaarden voldoen. Deze crawler verkeert in bèta; de resultaten hiervan hebben we daarom slechts als indicatie meegenomen. Door de techniek kan deze crawler niet alle pagina's afzoeken (vooral afhankelijk van de website) en wijken de aantallen daarom af van die van de zoekresultaten-methode. Door de bank genomen lijkt de crawler de bevindingen uit de bestaande methode te bevestigen.

Deze crawler geeft verder een beeld of de documenten voldoen aan één van de PDF/A standaarden, maar niet of PDF 1.7 wordt toegepast. Bij de zeven via Google onderzochte websites, en ook bij andere websites, is te zien dat een bescheiden aantal pagina's voldoet aan PDF/A.

De crawler heeft meer websites bezocht en laat ook daar zien dat in ongeveer één op de zes websites, er nog een behoorlijk aantal documenten in het formaat van MS Office is gedeeld en dus niet voor alle bezoekers te openen.

Conclusie:

ODF lijkt nauwelijks gebruikt te worden. Een aantal sites biedt nog wel een hoeveelheid MS Office-documenten aan, waarvan sommige sites zelfs een groei laten zien van dit niet-open formaat. Van de drie formaten is PDF het meest gebruikt. Van deze PDF-documenten is een een klein gedeelte in PDF/A-formaat; hoeveel documenten voldoen aan de eisen van de PDF 1.7-standaard is niet bekend.

[61] Bij deze cijfers moeten enkele kanttekeningen geplaatst worden:

- het aantal bestanden in een bepaald formaat op de website zegt nog niets over het gebruik van deze bestandsformaten in directe (andere) contacten met burgers, bedrijven en mede-overheden;
- daarnaast zegt het bestandsformaten op de website weinig over het gebruik van de verschillende formaten binnen de organisatie

F.4.4. OWMS 4.0 (Metadata overheidsinformatie)

OWMS is een semantische standaard voor metadata, de eigenschappen om informatieobjecten mee te beschrijven. Het voorschrijven van een semantische standaard voor metadata verhoogt de vindbaarheid en de samenhang van informatie die door overheidsorganisaties wordt aangeboden op internet.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
OWMS	nov 2011	Ministerie van AZ, Inspectieraad (directe toepassing)	n.v.t.

Beheerorganisatie: KOOP

Er wordt niet structureel informatie verzameld over de directe toepassing van OWMS op overheidswebsites; van actieve monitoring van het gebruik van de standaard is geen sprake (evenmin als in voorgaande jaren). Met betrekking tot de adoptie van OWMS is het volgens onze bron zinvoller om te kijken naar de toepassing van OWMS in contentmodellen van de centrale voorzieningen.

Onze bron geeft inzicht in aantallen gebruikers van vier toepassings-profielen: een categorie van directe toepassers en drie categorieën van toepassers van een contentmodel dat op OWMS is gebaseerd. Ook die laatste toepassingen zijn immers OWMS-conform.

1. Organisaties die zelf OWMS direct toepassen in hun eigen informatiesystemen. Behalve op de collecties van KOOP is bekend dat het Ministerie van AZ op rijksoverheid.nl OWMS toepast op content van alle ministeries. Ook de inspectieraad past OWMS direct toe op inspectieloket.nl voor alle 11 rijksinspecties. Verder komen met enige regelmaat vragen binnen over OWMS van leveranciers van contentpublicatiesystemen van gemeenten en gemeenschappelijke regelingen. Aantallen hiervan ontbreken. Er is geen reden om te veronderstellen dat OWMS op een meerderheid van de overheidswebsites direct wordt toegepast. Daar is ook geen sterke business case voor.
2. Organisaties die zelf een contentmodel toepassen dat op OWMS is gebaseerd. In dit verband wordt alleen gekeken naar de contentmodellen die zijn gepubliceerd op http://standaarden.overheid.nl/contentmodellen. Vrijwel alle organisaties leveren content aan voor Officiële Bekendmakingen in de Staatscourant, staatsblad, tractatenblad en parlementaire informatie. Die publicaties zijn allen gebaseerd op varianten van het model voor Officiële Publicaties (http://standaarden.overheid.nl/oep/technische-documentatie). Alleen de 40 organisaties van de rechterlijke macht leveren via rechtspraak.nl direct aan in het technische formaat van het contentmodel voor officiële publicaties. Twee andere veel toegepaste contentmodellen zijn die van CVDR en Samenwerkende Catalogi (SC). SC staat ook op de 'pas toe of leg uit'- lijst en wordt door leveranciers van productcatalogi geïmplementeerd, volgens onze bron voor vrijwel alle gemeenten, provincies en waterschappen. Zij tellen mee in deze categorie. CVDR is verplicht voor geconsolideerde regelgeving van gemeenten.
3. Organisaties die een voorziening bij KOOP gebruiken die een OWMS-compliant content-model afdwingt. Naast de hiervoor onder 2. genoemde decentrale overheden die CVDR

gebruiken, maakt een groot aantal (overheids)organisaties voor hun Officiële Bekendmakingen gebruik van het Digitaal Loket dat metadata verzamelt in het formaat van het contentmodel voor Officiële Publicaties. Zij passen dus niet zelf het technische OWMS-formaat toe, maar leveren wel alle door OWMS gevraagde informatie.

4. Organisaties die content aanleveren die KOOP van metadata voorziet conform een contentmodel. De publicatie van wet- en regelgeving in het Staatsblad wordt doorgaans door de ministeries aangeleverd in verschillende formaten en vervolgens door SDU van metadata voorzien.

Conclusie:
Het aantal directe toepassers van OWMS 4.0 beperkt zich binnen de overheid tot het Ministerie van Algemene Zaken en de Inspectieraad. Toepassing van een contentmodel dat is gebaseerd op OWMS 4.0 kan wijd verspreid zijn binnen de overheid, afhankelijk van het type contentmodel waarnaar wordt gekeken. Deze conclusie is (wederom) gelijkluidend als die van vorig jaar.

F.4.5. SKOS (Thesauri en begrippenwoordenboek)

SKOS is een uitwisselbaar gegevensmodel voor het delen en linken van systemen voor kennisrepresentatie via het Web. Veel systemen voor kennisrepresentatie zijn gegrondvest op eenzelfde conceptueel kader. Voorbeelden zijn thesauri, taxonomieën, begrippenwoordenboeken, classificatieschema's en systemen voor trefwoordtoekenning. Ze worden vaak gebruikt in vergelijkbare applicaties. SKOS maakt de overeenkomstige structuurelementen expliciet volgens een generieke standaard. Doordat SKOS voortbouwt op de standaarden RDF, RDFS en OWL (zie hierboven) zijn de kennisrepresentaties bruikbaar voor computerprogramma's ("machine readable") en kunnen deze uitgewisseld worden tussen applicaties en gepubliceerd worden op het Web.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
SKOS	mei 2015	onbekend, gebruik onduidelijk	n.v.t.

Bron: Taxonic

Navraag bij onze bron wijst uit dat er geen kwantitatieve gegevens over het gebruik van SKOS beschikbaar zijn, en dat er ook geen orgaan is dat ontwikkelingen rond deze standaard cijfermatig bijhoudt. Men neemt wel veel belangstelling voor de standaard waar. Vorig jaar zijn in de monitor enkele concrete ontwikkelingen uit het daaraan voorafgaande jaar benoemd. Deze bevindingen van vorig jaar staan nog steeds en voor elk van de resultaten geldt dat deze de afgelopen 12 maanden verder uitgebreid en bestendigd zijn.

Over het afgelopen jaar zijn de volgende ontwikkelingen te melden:

- Bij Alliander is een pilot afgerond om bedrijfswoordenboeken met SKOS te ontsluiten als eerste stap naar brede toepassing van SKOS en andere Linked Data-standaarden;
- Bij Wolters Kluwer is de NFLT omgezet naar SKOS; deze zal ook als LD beschikbaar komen;

- Bij de Politie loopt een groot project rondom Linked Data waarbinnen SKOS ook een belangrijke rol speelt;
- Het Ministerie van OCW gaat de Digitale Erfgoed Referentie Architectuur uitbreiden met Linked Data-standaarden. SKOS gaat daarin een rol spelen;
- Beeld en Geluid is druk doende een aantal thesauri beschikbaar te maken via SKOS. Diverse partijen binnen de Erfgoed-sector zijn met soortgelijke initiatieven bezig.

Conclusie:
Harde gegevens over gebruik door overheden zijn niet beschikbaar.

F.5. Domein E-facturatie en administratie

In deze paragraaf worden de volgende vier standaarden nader beschouwd: Semantisch Model eFactuur, SETU, XBRL en Dimensions en WDO Datamodel.

F.5.1. Semantisch model e-factureren (Elektronische facturen)

Het Semantische factuurmodel is een standaard voor electronisch 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). De standaard beschrijft welke gegevenselementen er in een elektronische factuur opgenomen dienen en kunnen worden, wat de samenhang is tussen deze elementen en wat de betekenis is van deze elementen. Daarnaast bevat de standaard mappings van de gegevenselementen naar SETU (staat op de 'pas toe of leg uit' –lijst) en de internationale UBL standaard zoals UBL SI (Simpler Invoicing) en UBL OHNL. Dit zijn twee veelgebruikte standaarden voor elektronisch factureren. Dankzij de mappings kunnen gebruikers van deze standaarden op een eenvoudige uniforme wijze elektronisch naar de overheid factureren. Mappings naar andere standaarden zijn bovendien ook mogelijk.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
SMeF 2.0	nov 2016	In alle relevante e-Factuurstandaarden	groeiend

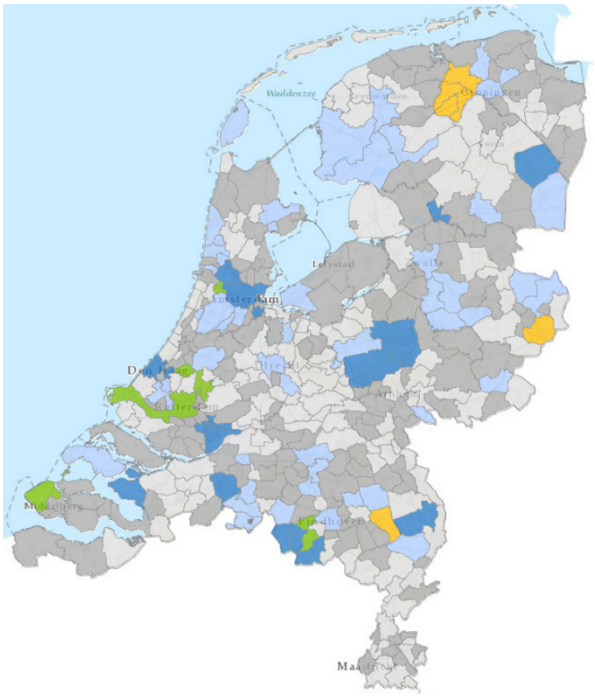
De beheerorganisatie van SMeF 2.0 (NEN en TNO) heeft geen kwantitatieve indicatoren van diens adoptie in daadwerkelijke e-facturen. Dat komt omdat de adoptie van SMeF 2.0 in de praktijk indirect gebeurt via het adopteren van andere e-factuurstandaarden, zoals OHNL of SETU, die voldoen aan SMeF 2.0.

Volgens een analyse van de beheerorganisatie voldeden eind 2016 de volgende factuurstandaarden aan SMeF 2.0:
- SALES 2.0 (ketenstandaard Bouw & Installatie)
- SI-UBL 1.1 (Simplerinvoicing)
- OHNL 1.9 (Digipoort)
- Standaard Energie eFactuur (Nederlandse energiebranche)
- SETU invoice 2.0 (Nederlandse uitzendbranche)

Voor het gebruik van de afgeleide factuurstandaarden, zijn er gegevens van verschillende organisaties.

De actuele (gemodereerde) zelfrapportage van overheden bij Pianoo[62] geeft in september 2017 het volgende beeld:

- Bij gemeenten geven zes aan gereed te zijn. Een tiental is bezig met implementatie, zo'n twintig met voorbereiding; de overige gemeenten is niet bezig, is gestopt met implementatie of heeft geen informatie aangeleverd.
- Twee waterschappen hebben e-facturen geïmplementeerd. Vier zijn nog niet gestart of al gestopt; de overige is bezig met implementatie of in voorbereiding
- Gelderland is de enige provincie die e-Facturen geïmplementeerd heeft. Twee zijn bezig met implementatie; vijf zijn in verkennende fase.



Zelfrapportage gemeenten aan Pianoo, geplot op kaart

Één van de technische oplossingen voor e-factureren is DigiInkoop. Hieraan doen 7 gemeenten, de provincie Zuid-Holland en het UWV mee, alle kerndepartementen en verschillende diensten van de Rijksoverheid[63]. Niet alle deelnemende organisaties hebben ook bij de hierboven genoemde rapportage bij Pianoo aangegeven e-Factureren in gebruik te hebben.

Het CBS houdt in een trendrapportage de adoptie van elektronische facturen bij; zij beschikken in hun 2016-rapportage niet over nieuwe gegevens ten opzichte van vorig jaar. In

[62] Kaartoverzicht bij het Pianoo programmabureau e-factureren: http://ez.maps.arcgis.com/apps/webappviewer/index.html?id=17a412116fbf409584682a671e878f6e
[63] https://www.logius.nl/ondersteuning/gegevensuitwisseling/welke-overheden-doen-mee/

2014 was 2/3e van de facturen digitaal, waarbij niet onderzocht is of deze voldoen aan een van de SMeF-afgeleide standaarden[64].

De nieuwe versie 2.0 het semantisch model standaard is snel geadopteerd door de onderliggende factuurstandaarden. Voor de adoptie van de factuurstandaarden is het programmabureau e-factureren opgericht binnen Pianoo, het expertisecentrum voor aanbestedingen. Dit programmabureau ondersteunt bij de implementatie[65].

De Europese richtlijn 2014/55/EU bepaalt dat alle aanbestedende diensten in de EU landen eind 2018 e-facturen moeten kunnen ontvangen en verwerken. Die verplichting wordt bovendien vastgelegd in de Aanbestedingswet 2012. Dit jaar is daarbij ook de Europese norm voor de semantiek van efactureren[66] gepubliceerd, die binnenkort verplicht is voor overheden. De beheerorganisatie verwacht dat dit een stimulans zal geven in de adoptie, ook in de private sector.

Vanaf 1 januari 2017 moeten leveranciers van de Rijksoverheid e-factureren. De verplichting tot e-facturatie geldt voor nieuwe inkoopovereenkomsten[67].

Conclusie:
Hoewel exacte gegevens ontbreken, lijkt het dat adoptie groeiende is. Daarbij is de Rijksoverheid een duidelijke voorloper terwijl decentrale overheden nog duidelijk aan het begin staan.

F.5.2. SETU-standaarden (Informatie flexibele arbeidskrachten)

De SETU-standaard is de Nederlandse implementatie van de internationale HR-XML standaard en is ontwikkeld door de grote uitzendorganisaties. Door toepassing van de SETU standaard ontstaat uniformering van het elektronisch berichtenverkeer tussen aanbieders en afnemers (inleners) van tijdelijk personeel (flexibele arbeid). Dit leidt tot vereenvoudiging van het inhuurproces.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
SETU	feb 2015	geen harde gegevens	Licht stijgende trend

De SETU-standaarden zijn Nederlandse implementaties van internationaal geldende standaarden, namelijk HR-XML en sinds kort ook UBL. De SETU-standaarden worden ontwikkeld en beheerd door de stichting SETU waarin alle grote uitzendorganisaties in Nederland betrokken zijn. Ook softwareleveranciers voor de branche voor flexibele arbeid kunnen actief participeren in de ontwikkeling.

[64] Bron: ICT, kennis en economie in cijfers 2016, paragraaf 5.4, CBS, Den Haag / Heerlen/ Bonaire.
[65] https://www.pianoo.nl/themas/elektronisch-factureren/e-factureren-toegelicht
[66] EN 16931-1:2017: https://standards.cen.eu/dyn/www/f?p=204:110:0::::FSP_PROJECT:60602&cs=1B61B766636F9FB34B7DBD72CE9026C72
[67] https://www.rijksoverheid.nl/onderwerpen/digitale-overheid/digitaal-zaken-doen-met-de-overheid/e-factureren-aan-de-overheid

SETU beschikt, in lijn met voorgaande jaren, niet over kwantitatieve gegevens over het feitelijke gebruik van de standaarden. De gebruiksgegevens zijn lastig te bepalen, aangezien het berichtenverkeer niet via een centraal platform geregeld wordt en er recent ook geen metingen of enquêtes zijn uitgevoerd. Er zijn ook geen andere partijen die wel zicht hebben op de adoptie in de gehele branche voor flexibele arbeid. Enkel de individuele organisaties die de SETU-standaarden hebben geïmplementeerd kunnen een indicatie geven van het volume van het berichtverkeer.

Gebaseerd op onderzoek van TNO in augustus 2014 en kwalitatieve informatie is het volgende te zeggen over de adoptie van SETU:

- Alle grote spelers in markt voor flexibele arbeid zijn aangesloten bij SETU en gebruiken de SETU-standaarden voor hun berichtuitwisseling. Deze spelers vertegenwoordigen 85% van de markt in termen van marktvolume. Uit informele uitvraag bij werkgroepen blijkt dat deze spelers gestaag nieuwe koppelingen ontwikkelen met behulp van de SETU-standaarden, dus dit betekent een lichte stijging ten opzichte van de vorige monitor.
- Voor de kleinere spelers in deze markt geldt dat zij afhankelijk zijn van hun softwareleveranciers voor het implementeren van de SETU-standaarden. Er zijn bij SETU 16 softwareleveranciers bekend die één of meerdere van de SETU-standaarden ondersteunen, hierin is dus een licht stijgende lijn te zien ten opzichte van de vorige monitor.

Er wordt voor de komende tijd een toename van de adoptie van de SETU-standaard voor de factuur verwacht, de stimulans hiervoor is de 2.0 versie van deze standaard die dit jaar is ontwikkeld. Deze 2.0 versie is een implementatie van de Europese norm voor e-Facturatie en gebaseerd op UBL in plaats van op HR-XML.

Conclusie:
Over de mate waarin van overheidszijde gebruik wordt gemaakt van de SETU-standaard bij het inlenen van personeel zijn geen harde gegevens beschikbaar.

F.5.3. WDO Datamodel (Douane-informatie)

Het WDO Datamodel is in 1997 opgezet vanuit de G7 naar aanleiding van de wens van het bedrijfsleven om gegevensaanlevering van het bedrijfsleven naar de overheid op het gebied van grensoverschrijdend personen- en goederenverkeer meer te simplificeren en te harmoniseren. Aangevers worden op dit moment geconfronteerd met het feit dat men dezelfde gegevens vaak meerdere keren moet aanleveren, op verschillende manieren, aan verschillende overheidsinstanties en in verschillende landen.

Het WDO Datamodel bevat zogenaamde ‘informatiepakketten’ voor gegevensuitwisseling. Deze beschrijven de semantiek van de uitgewisselde informatie: gegevens- en procesmodellen en hiervan afgeleide berichtspecificaties, de zogenaamde Message Implementation Guidelines (MIG’s). Informatiepakketten kunnen aan elkaar gerelateerd worden, waardoor samenhang ontstaat. Het WDO Datamodel integreert op deze manier de semantiek voor verschillende toepassingsdomeinen. Hierbij gaat het niet alleen om de Douane, maar ook om tal van andere overheidsinstellingen die betrokken zijn bij grensoverschrijdend verkeer (Voedsel en Waren Autoriteit, Havenautoriteiten etc.).

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
WDO Datamodel	april 2014	In elk geval Douane, Rijkswaterstaat, Zeehavenpolitie/Koninklijke Marechaussee en Havenautoriteiten	Stijgend

Aangezien het Nationaal Platform Data Model (NPDM) in 2016 is opgehouden te bestaan is het beheer en de coördinatie van het WDO datamodel belegd bij de Douane. Het beheer van de MIG 's blijft de verantwoordelijkheid van de ontwikkelaars. Op dit moment zijn er meerdere MIG 's in gebruik en in ontwikkeling, die gebaseerd zijn op het Datamodel. De Nederlandse Douane publiceert vijf MIG 's gebaseerd op het Datamodel, namelijk de MIG 's AGS (Import, Export en Opslag), AIS/ICS, AES/ECS en Comfort info. De MIG 's zijn functionele- en technische specificaties waarmee organisaties hun systemen kunnen ontwikkelen. De MIG 's worden gepubliceerd op de OSWO omgeving (https://www.oswo.nl/swodouane/). Ook is de NVWA, samen met de Nederlandse Douane bezig met de ontwikkeling van MIG 's voor de applicaties VGC en CLIENT Import gebaseerd op het WDO Datamodel.

Tevens is de Single Window-MIG voor Single Window Maritiem en Lucht (SWML), die gezamenlijk is ontwikkeld door de organisaties Douane, Rijkswaterstaat, Zeehavenpolitie/Koninklijke Marechaussee en Havenautoriteiten, geheel gebaseerd op het Data Model. De MIG bestaat uit de berichten behorende bij de implementatie van het SWML voortvloeiend uit de Europese Richtlijn 2010/65 en overige Douane-berichten behorend tot de Douaneprocessen Binnenbrengen, Uitgaan en Proviand. Deze MIG is tevens gepubliceerd op de OSWO omgeving.

Een belangrijke ontwikkeling is de introductie van het EU Customs Data model (EU CDM) wat is gebaseerd 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. Dit geeft aan dat de Europese Commissie belang hecht aan het gebruik van het WDO datamodel als tool om de beoogde harmonisatie en standaardisatie te realiseren. Dit feit alleen is al een indicatie dat het gebruik van het datamodel zal toenemen.

Een andere belangrijke ontwikkeling waarvan de verwachting bestaat dat deze het gebruik zal doen toenemen is de voorgenomen plaatsing van het WDO Datamodel op de Europese lijst van open standaarden.

Conclusie:
Met betrekking tot het gebruik van deze standaard zijn geen harde gegevens bekend omdat het feitelijke gebruik niet wordt geregistreerd. Er is sprake van een stijging van het gebruik.

F.5.4. XBRL en Dimensions (Bedrijfsrapportages)

Organisaties wisselen bedrijfsinformatie uit op de meest uiteenlopende manieren (op papier of elektronisch, als Word-document, als Pdf, als spreadsheet, etc.). XBRL, eXtensible Business Reporting Language, is een internationale open standaard om deze gegevens op eenvoudige wijze te verzamelen, elektronisch uit te wisselen, te analyseren en zo nodig nader te bewerken.

Standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
XBRL	april 2010	Belastingdienst, KvK, CBS, MinOCW/DUO en MinVWS	stijgende lijn; over-all

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.

De SBR-roadmap[68] heeft als primair doel om voor alle betrokken partijen helder te krijgen welke activiteiten cruciaal zijn om dit publiek-private samenwerkingsverband echt tot een breed en doorslaand succes te maken, en in welk tempo een en ander vorm kan krijgen. Doordat de partijen zich daaraan committeren, ontstaat een gemeenschappelijke agenda voor de komende jaren en daarmee ook een basis van onderling vertrouwen. Dat kan een extra impuls aan het SBR-programma geven.

In de afgelopen jaren zijn belangrijke vorderingen geboekt en is een breed draagvlak gecreëerd voor SBR als dé rapportagestandaard voor gestructureerd digitaal gegevens-verkeer. SBR is daarmee een (grootschalig) werkende oplossing en "proven technology". Door SBR breed in te gaan zetten wordt bereikt dat een ondernemer minder tijd hoeft te besteden aan zaken als administreren en rapporteren, en daardoor des te meer datgene kan doen dat hij wil en moet doen: ondernemen. Daarnaast kan via SBR de digitale dienstverlening vanuit de overheid richting ondernemend Nederland verbeteren. Daarmee past de roadmap ook naadloos in de kabinetsagenda. Binnen het (semi)overheidsdomein wordt gebruik gemaakt van SBR bij de Belastingdienst, de Kamer van Koophandel (KvK), het Centraal Bureau voor de Statistiek (CBS), de Dienst Uitvoering Onderwijs (MinOCW/DUO) en in pilotvorm ook de Autoriteit Woningcorporaties.[69]
Daar waar nu enkele tientallen berichtstromen gebruik maken van SBR, zijn er meer dan 1000 potentiele informatieketens ingeschat. In het kader van het project 'Acceleratie SBR' worden (semi)overheidspartijen gestimuleerd hun informatieketens aan te sluiten op SBR (inclusief XBRL) met als doel administratieve lasten te verlagen, betrouwbaarder gegevens te kunnen uitwisselen en informatie transparanter te maken.

[68] Roadmap SBR op weg naar 2020, 3e herijkte versie, juli 2017. Deze versie bouwt voort op de 1e versie en de 2e herijkte versie. De roadmap wordt in deze paragraaf als bron gebruikt, aangevuld met cijfers die vanuit Logius zijn aangeleverd.
[69] Naast deze (semi)overheidsinstellingen wordt nog een categorie gebruikers onderscheiden: een viertal grootbanken, specifiek gericht op het digitaliseren van de processen rond aanvragen en het beheer van zakelijke kredieten.

De concrete vorderingen zijn het meest evident bij aangiftes die ondernemingen en instellingen doen bij de Belastingdienst. De berichtuitwisseling beloopt al vele miljoenen per jaar en dat aantal blijft stijgen. De Belastingdienst past SBR (incl. XBRL) toe met betrekking tot de inkomstenbelasting, vennootschapsbelasting, omzetbelasting, intracommunautaire prestaties en toeslagen. In 2017 is er een toename van het berichtenverkeer voor de suppletie omzetbelasting, serviceberichten uitstel en het aantal machtigingen en verzoeken voor de vooraf ingevulde aangifte (VIA).
De KvK heeft zich tot doel gesteld om de komende jaren haar dienstverlening, waaronder de Handelsregisterprocessen, zoveel mogelijk te digitaliseren. Dit betekent dat ook het deponeringsproces van de jaarrekening volledig wordt gedigitaliseerd. Bij de Kamer van Koophandel is SBR in een vergevorderd stadium. Enkele honderdduizenden jaarrekeningen van micro-ondernemingen en kleine ondernemingen worden nu jaarlijks via SBR ontvangen. Vanaf 2018 komen hier de jaarrekeningen, inclusief accountantsverklaring, van middelgrote ondernemingen bij. De Nederlandse Beroepsorganisatie voor Accountants (NBA) heeft het mogelijk gemaakt om de accountantsverklaringen voortaan in SBR-formaat te kunnen afgeven.
CBS heeft een verplichtstellingsagenda geadopteerd voor drie statistieken. Het is al geruime tijd mogelijk deze statistieken via SBR aan te leveren bij CBS. CBS heeft in 2017 eerste berichten ontvangen via SBR.
Het doel van OCW/DUO is om de verantwoording door onderwijsinstellingen aan te laten leveren in XBRL, voorzien van een assuranceverklaring in XBRL van de accountant en getekend met het beroepscertificaat. De aanleveringen aan het ministerie OCW/DUO gebeurt grotendeels via het XBRL Onderwijsportaal. Vanaf 2017 wordt de jaarverantwoording, in pilotvorm, system-to-system aangeleverd.
De partijen (woningcorporaties, softwareleveranciers en accountants) die hebben deelgenomen aan de pilot woningcorporaties onderkennen het belang en de toegevoegde waarde van de invoering van SBR voor gegevensuitwisseling. Komende jaren zal een gefaseerde implementatie van SBR plaatsvinden.

In onderstaande tabel staat het aantal XBRL- berichten dat jaarlijks per partij is uitgewisseld.

		2014	2015	2016	2017*
Belastingdienst	Aangifte Inkomstenbelasting en vennootschapsbelasting	7.097.378	10.393.408	13.550.654	10.737.500
	Aangifte omzetbelasting en opgaaf intracommunautaire prestaties	2.729.865	3.725.467	4.077.407	3.200.819
	Toeslagen	18.489	374.464	1.044.417	829.332
	Loonheffingen**	28	729	1.474	825
Kamer van Koophandel	Deponeren Jaarverantwoording	106.730	175.581	277.410	368.638
CBS	Statistiekopgaven	-	-	224	248
DUO	Jaarverantwoording	-	-	-	2.304
Woningcorporaties	Jaarverantwoording	-	-	pilot	pilot
Totaal* **		**9.952.490**	**14.669.649**	**18.951.586**	**15.139.666**

* *2017 t/m augustus.*

** *Momenteel alleen verklaringen uitsluitend zakelijk gebruik bestelauto (UZGB).*

*** *Machtigingen worden ten opzichte van de vorige rapportage niet meer meegerekend.*

Het draagvlak voor SBR is duidelijk toegenomen. Alle relevante "stakeholders" participeren in het publiek-private samenwerkingsverband waarin SBR wordt (door)ontwikkeld. Daarbij gaat het om publieke organisaties die informatie uitvragen (zoals de BD, de KvK, CBS en MinOCW/DUO), om private organisaties die informatie uitvragen (zoals de banken), om intermediaire partijen die een belangrijke rol spelen bij het tot stand komen van rapportages (zoals accountants, fiscale adviseurs, softwareleveranciers en hun koepelorganisaties), hun relevante beroepsorganisaties (zoals de NBA) en om ondernemers zelf, vertegenwoordigd door hun koepels (VNO-NCW en MKB-NL). Het toenemende draagvlak blijkt ook uit het feit dat er tal van (publieke en private) partijen zeer geïnteresseerd zijn om toe te treden tot het SBR-samenwerkingsverband.

Conclusie:
Het gebruik van deze standaard is groeiende.

F.6. Stelselstandaarden

In deze paragraaf staan drie standaarden centraal: Digikoppeling, StUF en Geo-standaarden.

F.6.1. Digikoppeling versie 2.0 (Veilige berichtuitwisseling)

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

- bevragingen: een vraag waar direct een reactie op wordt verwacht. Hierbij is snelheid van afleveren belangrijk. Als een service niet beschikbaar is, dan hoeft de vraag niet opnieuw te worden aangeboden;
- meldingen: men levert een bericht en (pas) veel later komt eventueel een reactie terug. In dat geval is snelheid van afleveren minder belangrijk. Als een partij even niet beschikbaar is om het bericht aan te nemen, dan is het juist wel gewenst dat het bericht nogmaals wordt aangeboden.

Aan versie 2.0 van Digikoppeling (deze versie staat op de lijst 'pas toe of leg uit') is o.a. de specificatie voor grote berichten toegevoegd, de mogelijkheid om attachments toe te voegen en om security op berichtniveau toe te passen.

In 2016 is vooral onderhoud aan de standaard doorgevoerd. De belangrijkste wijziging is dat het wijzigingsvoorstel om het OIN beleid aan te passen is goedgekeurd door de Regieraad Gegevens. Het OIN, het Organisatie Identificatie nummer is een essentieel onderdeel van de Digikoppeling standaard en wordt binnen het berichtenverkeer van de Overheid veelvuldig toegepast. Dit nieuwe beleid zal in 2017 worden uitgewerkt en gerealiseerd.

Standaard	*op lijst sinds*	*gebruik door overheden*		*ontwikkeling in gebruik*
		totaal	*w.v. Rijk*[70]	
Digikoppeling	juni 2013	76 %	67 %	aantal aansluitingen verder gestegen, in vergelijking met vorig jaar

Bron: beheerorganisatie Logius

[70] Waar in deze en overeenkomstige tabellen wordt gesproken over Rijk wordt bedoeld: inclusief uitvoeringsorganisaties, ZBO's + OOV + eOverheid.

Logius (Stelselvoorzieningen) heeft op verschillende peilmomenten (maart 2013, augustus 2013, augustus 2014, augustus 2015, zomer 2016 en zomer 2017) 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 toegevoegd uit de OOV-sector die niet zijn aangesloten op Digikoppeling.

Tabel F8: Overheden aangesloten op Digikoppeling
(Bron: opgave Logius)

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 % [71]	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 %

Conclusie:
Een substantieel deel van de overheden is op Digikoppeling aangesloten. Er is sprake van een verdere stijging, van 64% naar een aandeel van 76%. Vorig jaar hebben met name provincies en waterschappen een inhaalslag gemaakt en groeiden relatief hard. Dit jaar blijft de groei daar achter en is met name bij Rijk en gemeenten sprake van groei.

F.6.2. Geo-standaarden (Geografische informatie)

In Nederland (en ook daarbuiten) zijn veel organisaties betrokken bij 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 aardoppervlakte. 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

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

worden, zijn afspraken nodig over de te gebruiken standaarden. De set Geo-standaarden voorziet hierin. 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 v1.3.1
- Nederlands metadataprofiel op ISO 19119 voor services v1.2.1
- webserviceprofielen voor Web Feature Service (WFS) en Web Map Service (WMS)

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
Geo-standaarden	dec 2014	op onderdelen harde gegevens	op onderdelen: stijgend

Er is sprake van een set van deel-standaarden. Dat maakt het krijgen van overzicht met betrekking tot het gebruik complex. Bij Geonovum is wederom navraag gedaan met betrekking tot het gebruik. De basisset geo-standaarden staat op de lijst voor 'pas toe of leg uit' en bestaat uit de volgende 5 componenten:

- het basis-model geo-informatie NEN3610: een generiek model op basis waarvan sectorspecifieke informatiemodellen zijn en worden ontwikkeld. Momenteel zijn er 16 van dergelijke informatiemodellen (nog niet alle in gebruik genomen) en aan twee nieuwe informatiemodellen (IMBAG / Informatiemodel Basisregistratie Adressen en Gebouwen en IMWV / Informatiemodel Wegen en Verkeer) wordt gewerkt . Naar verluidt is bij een zestal informatiemodellen (vier in de context van basisregistraties [BGT, BRT, Kadaster en BRO] en twee in het kader van overige wetgeving[72]) het bereik maximaal, in de zin dat alle bronhouders de betreffende modellen verplicht gebruiken waarbij de software deze modellen derhalve ook ondersteunt. Bij enkele informatiemodellen heeft zijn concrete cijfers te geven:
    - Basisregistratie Grootschalige Topografie: alle 428 bronhouders aangesloten: 390 gemeenten, 12 provincies, 22 waterschappen, ProRail, Rijkswaterstaat en de Ministeries van Defensie en Economische Zaken. In 2016 waren er 100 miljoen views en downloads via PDOK op de BGT (2015: 11,1 miljoen, een stijging van 800%);
    - In 2016 heeft de Basisregistratie Kadaster 2,5 miljoen informatieproducten geleverd conform dit model (in 2015: 1,9 miljoen, een stijging van ruim 30%);
    - Basisregistratie Topgrafie. Het gebruik van dit bestand is in 2016 ruimschoots verdubbeld: in 2016 werden er ruim 2.1 miljard hits (2015: bijna 900 miljoen, een stijging van 130%) hits op de officiële distributie-services geregistreerd;
    - Ruimtelijkje Ordening: Inmiddels bijna 64.000 (2015: ruim 58.000) plannen conform IMRO gepubliceerd in de landelijke voorziening ruimtelijkeplannen.nl. Ruim 400 bevoegd gezagen (o.a. gemeenten, provincies en een aantal departementen) gebruiken het model voor het opbouwen van hun ruimtelijke plannen. Deze opbouw wordt door acht softwareleveranciers ondersteund.
- de Geography Markup Language (GML). De Geography Markup Language (GML) is een op XML gebaseerd formaat, specifiek ontwikkeld voor geo-informatie. Veel

[72] Te weten de Wet Ruimtelijke Ordening en de Wet Informatie-uitwisseling Ondergrondse Netwerken.

uitwisselingsstandaarden in het geo-domein zijn gebaseerd op GML. Zo horen bij alle in de vorige paragraaf beschreven informatiemodellen (behalve informatiemodel Landelijk Gebied) ook uitwisselingsprofielen op basis van GML. Dit omvat dus ook de hiervoor genoemde basisregistraties en andere landelijke registraties met bijv. ruimtelijke plannen. GML wordt zowel vereist als formaat waarin bronhouders data aanleveren aan landelijke voorzieningen en registraties (zoals voor bestemmingsplannen en -verpakt in een Stuf-envelop- voor grootschalige topografie i.h.k.v. de BGT) als veelgebruikt als formele uitleverformaat waarin afnemers data kunnen afnemen. Voor het afnemen van open overheidsinformatie in bijv. de BGT, BRT en de Basisregistratie Kadaster is GML zelfs het enige uitleverformaat. In 2016 zijn zo'n 750.000 (2015: 350.000) BGT-opvragingen gedaan. Dit zijn grotendeels opvragingen door niet-bronhouders omdat bronhouders ook via de productieketen voorzien worden van updates.

- metadataprofiel op ISO 19115 voor geografie. Het Nederlandse profiel op ISO19115 is een aanscherping van de metadatarichtlijnen voor datasets, waarmee dataproviders zowel aan ISO19115 als aan INSPIRE- en nationale vereisten voldoen. Het belangrijkste gebruik van deze standaard vindt plaats binnen het Nationaal Georegister, het nationale metadata portaal voor geodata en geo-services. Door de metadata van datasets conform deze standaard in dit portaal te registreren, zijn (open) geodatasets goed vindbaar en is de bruikbaarheid goed te beoordelen door de gebruikers. Momenteel zijn ruim 9.500 (2015: 8.500) geodatasets geregistreerd in het Nationaal Georegister, waarbij gebruik gemaakt wordt van deze standaard.
- metadataprofiel op ISO 19119 voor services. Het Nederlandse profiel op ISO19119 is een aanscherping van de metadatarichtlijnen voor geo-webservices, waarmee dataproviders zowel aan ISO19119 als aan INSPIRE- en nationale vereisten voldoen. Het belangrijkste gebruik van deze standaard vindt plaats binnen het Nationaal Georegister, het nationale metadata portaal voor geodata en geo-services. Het aantal geregistreerde services (ruim 500 services) in het Nationaal Georegister is stabiel. Voor het registreren van webservices die in het kader van de Europese INSPIRE-richtlijn in de lucht worden gebracht, is registratie in dit register verplicht. Het gebruik van deze standaard binnen de INSPIRE-context is hiermee maximaal. Voor beide profielen gezamenlijk is nog het aantal hits op het Nationaal Georegister nog een indicatie van het gebruik: in 2016 is het NGR ruim 26 miljoen (2015: 5,8 miljoen) keer bevraagd.
- webserviceprofielen voor Web Feature Service (WFS) en Web Map Service (WMS), bedoeld voor het ontsluiten en daadwerkelijk verzenden van geografische data als afbeelding (kaartmateriaal). Het gebruik van deze profielen is moeilijk te kwantificeren omdat sprake is van veel verschillende aanbieders en veel verschillende softwareleveranciers. Op een aantal punten zijn er echter wel degelijk uitspraken te doen en nuttige indicaties te geven. Zo kan gekeken worden naar het gebruik van deze services bij de ontsluiting van (geo)basisregistraties en andere registraties met een wettelijke grondslag, zoals INSPIRE. Hierbij is het gebruik van de Nederlandse profielen op WFS en WMS maximaal: de formele distributieservices zijn allen gebaseerd op deze open standaarden. Een andere benadering is door bij de WMS-standaard te kijken naar indicatoren voor het gebruik van WMS en alternatieven. De volgende indicaties zijn beschikbaar:
    - de gezamenlijke WMS-services van Publieke Dienstverlening Op de Kaart (PDOK) zijn in 2016 1,3 miljard keer bevraagd (2015 ruim 514 miljoen);

- de WMTS-services kregen ruim 1,5 miljard (2015: 349 miljoen) en WMSC-services 230 (2015: 225 miljoen) hits te verwerken. In totaal krijgen de varianten dus net als in 2015 meer hits dan de WMS zelf;
- Voor WFS is een dergelijke benadering beperkt mogelijk. Het niet-standaard alternatief dat wordt aangeboden door PDOK zijn de zgn. Atom feeds. Deze feeds kregen in 2016 3,5 miljoen hits, terwijl WFS ruim 350 miljoen hits had; het honderdvoudige dus.

Conclusie:
Omdat sprake is van een set deelstandaarden, is het beeld complex en lastig te duiden. Daar waar sprake is van (indicatieve) gegevens over gebruik, is sprake van duidelijke stijgingen.

Dit geldt voor het gebruik van NEN3610, zowel qua aantal implementaties (o.a. uitbreiding naar BAG) als qua aantal bevragingen van data die gestructureerd is conform de NEN3610-familie van informatiemodellen. Met het steeds verder gevuld raken van de BGT neemt ook het gebruik van GML steeds verder toe. GML is een onmisbare bouwsteen in het stelsel van (geo)basisregistraties. Op metadata gebied zien we een groei van het aanbieden van metadata van datasets conform de standaarden (+10%), terwijl het aanbod van metadata van services constant blijft. Het gebruik in de vorm van afnemen (doorzoeken) van metadata is fors gegroeid (+500%). Voor het gebruik van WMS en WFS geven gebruikscijfers van PDOK een goede indicatie van het gebruik binnen overheidscontext. Het gebruik van deze services laat voor bijv. WMS een groei van 250% zien.

F.6.3. StUF (Uitwisseling administratieve overheidsgegevens)

De StUF-standaard is een familie van samenhangende gegevens- en berichtenstandaarden. StUF staat sinds eind 2008 op de pas-toe-of-leg-uit-lijst en richt zich op de standaardisatie van de inhoud van informatie, berichten en services. StUF is als open standaard vastgesteld voor :

- uitwisseling 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 diensten-portfolio van gemeenten;
- uitwisseling van domein- of sector-specifieke gegevens waarin ook basis- en/of zaak-gegevens voorkomen en waarvoor geen andere (inter)nationale (XML-gebaseerde) berichtenstandaard is vastgesteld.

Het organisatorische werkingsgebied van StUF is gemeenten en de ketens waarbinnen gemeenten participeren. In de periode 2012-2014 is naast de uitvoering van het reguliere beheer de StUF-familie verder ontwikkeld en uitgebreid zowel op de inhoud, de standaardisatie-methodiek en het instrumentarium. De adoptie en de toepassing van StUF zijn aanzienlijk toegenomen.

Verbeterde standaardisatiemethodiek en vernieuwing
Een belangrijke impuls in het toepassen en de doorontwikkeling van StUF is gerealiseerd in het kader van OperatieNUP, het meerjarige programma dat KING uitgevoerd heeft in opdracht van de VNG. Na beëindiging van OperatieNUP in december 2014, zijn genoemde

activiteiten gecontinueerd. Het betekent dat al tijdens het standaardisatieproces, vroegtijdig met leveranciers, afspraken worden gemaakt over het inbouwen van de standaarden, het preventief testen ervan en het publiceren van informatie over softwareproducten en testresultaten in de Softwarecatalogus.
De basis van de actuele versie van de StUF familie (3.x) is al gelegd in 2008. Om aan te sluiten op nieuwe behoeften, snellere ICT ontwikkeling, lagere kosten, complexiteitsreductie en technische ontwikkelingen is in 2015 gestart met verkenningen en analyses naar een grondige vernieuwing van de StUF familie. Binnen deze vernieuwing wordt zowel in de inhoud van de standaard, de ontwikkelaanpak en tooling vernieuwd. In 2017 zijn de eerste twee standaarden gerealiseerd.
Er is onderzoek gedaan naar een grondige vernieuwing van de StUF familie. Naast nieuwe versies van informatiemodellen is er samen met Kadaster, Geonovum een nieuw metamodel ontwikkeld. Dat is een randvoorwaarde voor harmonisatie van semantiek. Verder is een nieuwe modelgedreven werkwijze en tooling gerealiseerd waarmee snel en efficiënt compacte berichtstandaarden gegenereerd kunnen worden.
In diezelfde periode zijn met 197 softwareleveranciers nieuwe convenanten afgesloten (vorig jaar: 186). In dit convenant voor de periode 2016 t/m 2018 is de set van afspraken tussen KING en leveranciers verder uitgebreid (ten opzichte van het convenant dat tot 2016 gold) en aangescherpt in het kader van de doelstellingen van de gemeentelijke Digitale Agenda 2020.

Compliancy en StUF Testplatform
Om er voor te zorgen dat leveranciers tijdig en aantoonbaar aan de standaarden voldoen (=compliancy) is het StUF Testplatform beschikbaar. Met deze online testomgeving kunnen leveranciers hun softwareproducten preventief en objectief testen op de juiste toepassing van StUF. Een foutloze test geeft een goede kwaliteitsindicatie over interoperabiliteit middels StUF. De adoptie van het StUF Testplatform, dat nu 5,5 jaar beschikbaar is, door leveranciers verliep in eerste instantie traag. Door aanhoudende druk neemt het gebruik gestaag toe. In 2017 is het aantal leveranciers van gemeentelijke software dat een account op het StUF Testplatform gelijk gebleven ten opzichte van 2016: 56 leveranciers. Maandelijks worden enkele duizenden StUF-berichten getest. Het testplatform wordt ook gebruikt voor de StUF (deel)standaarden van de Waarderingskamer, het Zorginstituut Nederland, Geonovum en het Ministerie van V&J.
Sinds september 2014 publiceert KING driemaandelijks een Compliancy monitor. Deze monitor is bedoeld om gemeenten, samenwerkingsverbanden en ketenpartijen op een overzichtelijke manier te informeren over welke software-producten wel en niet voldoen aan tien actuele standaarden. Uit deze monitor komt een beeld naar voren dat veel softwareproducten niet compliant zijn. Om de effecten van StUF te benutten is en blijft het voor gemeenten van belang het toepassen van StUF goed mee te nemen in alle fasen van een ICT product en foutloze testrapporten te eisen.

Uniforme Inkoopvoorwaarden - GIBIT
Om het ICT opdrachtgeverschap verder te versterken en het duurzaam toepassen van (open) standaarden beter te borgen zijn inmiddels binnen de gemeentelijke Digitale Agenda 2020 uniforme ICT inkoopvoorwaarden, de **GIBIT,** gerealiseerd. (zie www.gibit.nl). Daartoe zijn Gemeentelijke ICT Kwaliteitsnormen uit de GIBIT wettelijke standaarden, standaarden op de Pas-toe-of-leg-uit lijst en landelijke gemeentelijke standaarden opgenomen. Het toepassen

ervan geldt over de gehele levensduur van een ICT-product/dienst. In december 2016 is de GIBIT door het VNG Bestuur vastgesteld. In 2017 is de grootschalige invoering ervan uitgevoerd. De adoptie van de GIBIT verloopt tot nu toe soepel en snel. Per augustus 2017 maakt al 50% van de gemeenten of gemeentelijke samenwerkingsverbanden gebruik van de GIBIT en/of is deze opgenomen in het aanbestedingsbeleid.

Uitbreidingen van de StUF familie

Voor de aansluiting op basisregistraties en andere landelijke voorzieningen is afgelopen jaren de StUF-familie uitgebreid voor het Handelsregister van de Kamer van Koophandel, de aansluiting op de LV-WOZ van de Waarderingskamer, op MijnOverheid Lopende Zaken met Logius en voor de BGT (StUF-GEO-IMGEO) met GEONOVUM. Ook voor het berichtenverkeer voor het nieuwe jeugdstelsel (CORV) van het Ministerie van V&J en ketens voor de decentralisaties in samenwerking met Zorg Instituut Nederland wordt StUF gebruikt. In deze trajecten wordt voorgebouwd op StUF en waar mogelijk combinatie gemaakt met andere standaarden (iWMO en iJW) . Deze uitbreidingen op StUF zijn ontwikkeld door of in nauwe samenwerking met de betreffende organisaties. In enkele gevallen lukte dat na nadrukkelijk aandringen door de VNG en KING en op grond van uitgevoerde impact-analyses.
Naast de uitbreiding van StUF voor externe koppelingen zijn nieuwe aangescherpte standaarden opgesteld voor een selectie van binnengemeentelijke ketens. Binnen deze standaarden is het gebruik van authentieke basisgegevens en zaakgegevens meegenomen. Naast de voorbeelden zoals genoemd in de monitor 2016 (voor betalen en invorderen, BAG-WOZ, BAG-GBA, documentcreatie, voorinvullen van digitale (e-)formulieren, zaakgericht werken (Zaak- en Documentservices, StUF-ZTC), toezicht en handhaven en WABO-BAG), zijn inmiddels nog standaarden vastgesteld voor de koppelvlakken Regie- en Zaakservices, en BGT-BAG. Deze standaarden worden momenteel door meerdere ICT-leveranciers ingebouwd.

Markttransparantie door GEMMA Softwarecatalogus

In het najaar van 2012 is de eerste versie van de GEMMA Softwarecatalogus (www.softwarecatalogus.nl) in gebruik genomen. Deze online softwarecatalogus biedt transparantie en inzicht over welke leveranciers gemeentelijke softwareproducten aanbieden, wat de productplanning is en welke (open) standaarden worden ondersteund. In het voorjaar van 2013 waren daarin ruim 400 softwareproducten van circa 60 leveranciers opgenomen. In maart 2014 is versie 2 van de catalogus geïntroduceerd. Een belangrijke uitbreiding is de functionaliteit waarmee gemeenten het eigen applicatieportfolio kunnen bijhouden. Gemeenten gebruiken de softwarecatalogus voor hun ICT-management en voor onderlinge kennisdeling. Inmiddels maken alle gemeenten er gebruik van. Ruim 225 gemeenten hebben hun applicatieportfolio er redelijk compleet in opgenomen. Inmiddels gebruiken ook steeds meer samenwerkingsverbanden de Softwarecatalogus. Ook daar worden de StUF-standaarden gebruikt, zodat het beeld van het gebruik steeds completer wordt. Het aanbod van software in de catalogus neemt steeds verder toe. In de software staan meer dan 2300 softwareproducten (incl. versies; vorig jaar 2000) van 197 ICT-leveranciers (vorig jaar: 186). In de softwarecatalogus kunnen leveranciers ook hun testrapportages publiceren. Dit is van belang voor gemeenten en andere overheden om inzicht te krijgen in de juiste toepassing van StUF of andere (open) standaarden. Voorts helpt het bij het verhogen van de betrouwbaarheid van de door leveranciers geregistreerde

productinformatie. Het aantal gepubliceerde testrapporten (vorig jaar 720) is flink gestegen tot inmiddels ruim 1000.
De GEMMA Architectuur is in 2017 flink uitgebreid met nadere detailleringen van domeinen, applicatiefuncties en bijbehorende standaarden. In de Softwarecatalogus moeten de leveranciers, gemeenten en samenwerkingsverbanden een migratie uitvoeren van GEMMA1 naar GEMMA2. Dit migratieproces is inmiddels door ongeveer 60% uitgevoerd. De verwachting is dat de migratie eind 2017 afgerond wordt.
In overleg met het Bureau Forum Standaardisatie zijn afspraken gemaakt over het gebruik van de softwarecatalogus als informatiebron voor onderliggende monitor.

Adoptiegraad van StUF
Kijken we naar het aanbod van pakketsoftware dat StUF ondersteunt (volgens opgave van leveranciers), dan blijkt dat het volgende:

Tabel F9: Marktadoptie StUF

Adoptiegraad	**Totaal**	**StUF-BG 3.10**	**StUF-ZKN 3.10**
Aantal leveranciers	197 (186)	57 (56)	50 (50)
Aantal softwareproducten (incl. versies)	2358 (2043)	718 (645)	505 (384)
waarvan beschikbaar/in gebruik	1223 (1346)	320 (349)	204 (193)
waarvan gepland/in ontwikkeling	78 (153)	50 (104)	28 (37)

(bron KING: www.softwarecatalogus.nl - peildatum september 2017; tussen haakjes de cijfers van de vorige monitor)

Op dit moment bieden 57 softwareleveranciers 320 softwareproducten (incl. versies) aan die StUF BG ondersteunen. Voor StUF ZKN (Zaken) gaat het om 50 leveranciers en 204 producten. Voor tientallen softwareproducten is de (door)ontwikkeling gepland.
Alle gemeenten (100%) gebruiken de StUF standaard. De intensiteit van de adoptie neemt gestaag steeds verder toe. Het aantal softwareproducten dat bijv. StUF BG ondersteunt is t.o.v. 2015 met 125 toegenomen. De relatieve adoptiegraad t.o.v. het totaal aantal geregistreerde producten blijft ongeveer gelijk. Een vergelijkbaar beeld geldt voor StUF ZKN.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
StUF	nov 2008	gemeenten: 100% (voor de afdekking van alle binnengemeentelijke ketens geldt een lager percentage)	op meerdere prestatie-indicatoren duidelijke vooruitgang

Dit positieve beeld wil niet zeggen dat gegevensuitwisseling van basisgegevens- en/of zaakgegevens in alle afnemende processen en informatiesystemen optimaal is en conform StUF verloopt. Er wordt nog steeds gebruik gemaakt van verouderde versies (StUF 2.x) en/of maatwerk koppelingen, maar er is daarin wel afname, en dus groei naar gebruik van de nieuwere StUF-versies. Ook zijn veel binnengemeentelijke informatie- of procesketens (nog) niet of slechts deels gedigitaliseerd. Dit belemmert niet alleen de invoering van zaakgericht werken, optimale online diensten en het breder gebruik van authentieke gegevens, ook een

verdere doorontwikkeling en grootschalige digitalisering van processen zoals bijvoorbeeld geautomatiseerde processturing op basis van mutaties en signalen uit systemen is niet goed uitvoerbaar.
Voorts blijkt er een groot verschil tussen de afspraken die via convenanten met leveranciers zijn gemaakt en het daadwerkelijk en tijdig nakomen ervan. Sommige leveranciers spelen niet of te laat in op de vraag. Deels is dat te wijten aan het achterblijven van een gebundelde vraag en gerichte opdrachtverstrekking door gemeenten. Een ander deel wordt veroorzaakt door tempo-verschillen tussen leveranciers onderling. Voor gemeenten zijn dit belemmeringen bij het kunnen doorvoeren van procesverbeteringen.

Conclusie:
Samengevat blijkt uit de cijfers en de analyse dat gemeenten, ketenpartners en hun leveranciers goede stappen hebben gezet op het vlak van interoperabiliteit en het gebruik van StUF: er ligt een stevige basis. Het aantal gemeentelijke ketens waarin StUF wordt gebruikt, is uitgebreid. Er is veel pakketsoftware op de markt of dit komt binnenkort op de markt.

Om de baten van de StUF-standaard te benutten is meer aandacht nodig voor vernieuwing van de standaard en voor verbreding van het gebruik in andere gemeentelijke ketens, processen en systemen.

Bij deze vernieuwing is goed opdrachtgeverschap van gemeenten cruciaal. Het verminderen van tempo-verschillen en het afdwingen van compliancy (testrapporten) draagt bij aan soepeler implementaties en meer transparantie over de kwaliteit van het aanbod van software. De verwachting is dat de ingezette vernieuwing van de StUF Familie en de borging van Open Standaarden in de uniforme ICT inkoopvoorwaarden (GIBIT) daar aan bijdraagt. Datzelfde geldt voor de beweging dat gemeenten steeds meer van hun informatievoorziening collectief willen organiseren.

F.7. Water en bodem

Er vallen drie standaarden binnen dit domein: de Aquo-standaarden en SIKB0101 respectievelijk SIKB 0102. Over de Aquo-standaarden is geen informatie ontvangen. In het vervolg van deze paragraaf staan derhalve de beide SIKB-standaarden centraal.

F.7.1. SIKB0101 (Milieutechnische bodeminformatie)

SIKB0101 is een 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. Een onderdeel van het gebruik is het aanleveren van bodemkwaliteitgegevens aan landelijke registratiesystemen voor bodemkwaliteit (GLOBIS), aan lokale systemen (bodem informatiesystemen provincies en gemeenten) en aan TOWABO, het landelijke systeem voor de toetsing van waterbodems (o.a. vervuild slib). GLOBIS wordt decentraal beheerd en er zijn meerdere implementaties van dit systeem in gebruik. Daarvoor is SIKB0101 de facto de

standaard. De verplichting geldt bij de investering in een systeem of dienst waarmee kwaliteitsgegevens van bodems uitgewisseld worden.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
SIKB0101	dec 2014	decentrale overheden die een BIS gebruiken; Rijkswaterstaat Leefomgeving (Bodemloket)	n.v.t.

Beheerorganisatie: SIKB

Alle overheden die een BodemInformatieSysteem (BIS) gebruiken, passen ook SIKB0101 toe. Aangezien veruit de meeste provincies, omgevingsdiensten en gemeenten een BIS gebruiken, kan worden afgeleid dat zij daarmee ook de standaard toepassen. Tevens wordt SIKB0101 ondersteund door het landelijke waterbodeminformatiesysteem WAB-Info (RWS) en gebruiken enkele waterschapslaboratoria SIKB0101 voor gegevensuitwisseling. Ook Rijkswaterstaat Leefomgeving is gebruiker van de SIKB-standaard in diverse applicaties (zoals Meldpunt Besluit Bodemkwaliteit, BoToVa, Bodemloket). Naast bovengenoemde overheidsorganisaties passen ook bodem-adviesbureaus en (milieu-) laboratoria SIKB0101 toe. De facto is er derhalve sprake van 100% toepassing in de keten. Waar milieu-hygiënische data over de bodem worden uitgewisseld vindt dit plaats middels de standaard SIKB0101.

Toepassing van SIKB0101 vindt zowel plaats binnen standaardsoftware (o.a. BIS-systemen bij overheden) als in maatwerkapplicaties. De leveranciers en ontwikkelaars die SIKB0101 hebben geïmplementeerd zijn gepubliceerd op de website van SIKB.

Binnen het domein van de standaard SIKB0101 zijn de komende jaren twee belangrijke ontwikkelingen relevant: de Basis Registratie Ondergrond (BRO) en het Digitaal Stelsel Omgevingswet (DSO). Er vindt met enige regelmaat constructief overleg plaats om (her-)gebruik van de standaard SIKB0101 onder de aandacht te brengen en te kijken op welke wijze vanuit de beheerorganisatie ondersteuning kan worden verleend. Ook binnen het Centraal College van Deskundigen (CCvD) is zijn deze ontwikkelingen regelmatig onderwerp van gesprek.

Conclusie:
Rijkswaterstaat Leefomgeving en vrijwel alle gemeenten, provincies en omgevingsdiensten beschikken over systemen waarin SIKB0101 is toegepast. Harde gegevens over de mate waarin overheden digitaal gegevens delen zijn evenwel niet beschikbaar.

F.7.2. SIKB0102 (Archeologische bodeminformatie)

Met SIKB0102 kunnen overheden en bedrijven gestandaardiseerde archeologische informatie uitwisselen. Dankzij het gebruik van de SIKB0102-uitwisselingsstandaard zijn archeologische onderzoeksgegevens voor iedereen online beschikbaar. Deze gegevens zijn transparant opgezet en beschreven, wat ten goede komt aan het vertrouwen in de kwaliteit van de beschikbare digitale documentaties. Het koppelen van verschillende datasets - bijvoorbeeld in het kader van een synthetiserend onderzoek - wordt vereenvoudigd. Hierdoor kan er met minder inspanning meer kenniswinst worden geboekt. Bedrijfsprocessen lopen efficiënter in

een digitaal traject dan in een analoog traject. Een opgravende instantie, overheidsorganisatie of een bedrijf dat archeologisch onderzoek en/of vondsten doet heeft een wettelijke plicht om binnen twee jaar na afronding van de opgraving de verzamelde informatie beschikbaar te stellen aan een aantal depots (landelijk, provinciaal en/of gemeentelijk). De structuur, het formaat en de waarden voor de digitale uitwisseling van deze informatie wordt beschreven in de SIKB0102-standaard.

De verplichting geldt bij een investering in een systeem of dienst dat wordt gebruikt voor de uitwisseling van archeologische informatie, verzameld tijdens het uitvoeren van archeologisch onderzoek en/of bij een archeologische vondst.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
SIKB0102	feb 2016	Decentrale overheden met een archeologisch depot	n.v.t.

Beheerorganisatie: SIKB

Ten opzichte van voorgaande jaren zijn in 2016 goede stappen gezet bij de implementatie van de standaard SIKB0102. Koppelingen zijn gerealiseerd in het nieuwe Provinciale Depot Beheer Systeem (PDBS). Ook bij partijen die archeologisch onderzoek uitvoeren wordt digitale uitwisseling langzaam maar zeker gemeengoed. E-depot (DANS) heeft SIKB0102 geïmplementeerd. Archis had SIKB0102 geïmplementeerd maar bij het vernieuwde Archis 3 is de mogelijkheid tot digitale aanlevering tijdelijk buiten werking. Eind 2017 zal dit worden hersteld. Achter blijven de gemeentelijk depots die veelal intern gericht zijn met hun data en weinig delen met partijen buiten de eigen organisatie.

Implementatie van de standaard SIKB0102 zal ook de komende jaren de nodige ondersteuning en stimulering vragen. Dit wordt door SIKB geleverd. Onder meer middels een landelijke bijeenkomst ‘digitaal werken in de Archeologie’.

Binnen het domein van de standaard SIKB0102 is de komende jaren de ontwikkelingen van het informatiehuis Cultureel Erfgoed van belang: Afstemming over het gebruik van de standaard SIKB0102 bevindt zich in de opstartfase.

De leveranciers en ontwikkelaars die SIKB0102 hebben geïmplementeerd zijn gepubliceerd op de website van SIKB.

Conclusie:
Over de mate waarin van overheidszijde gebruik wordt gemaakt van de SIKB0102l zijn geen harde gegevens beschikbaar.

F.8. Bouw

Binnen dit domein gaat het om twee standaarden: IFC en VISI.

F.8.1. IFC (Bouwwerkinformatiemodellen)

Bij de IFC-standaard draait het om de uitwisseling van 3D-bouwinformatiemodellen.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
IFC	nov 2011	lijkt nog beperkt; geen harde gegevens	n.v.t.

De IFC-standaard is vrijelijk toepasbaar, zonder dat hiervoor enige vorm van registratie nodig is. Om die reden kan de beheerorganisatie lastig een beeld krijgen van de toepassing van de standaard. In zijn algemeenheid werd vorig jaar door buildingSMART het volgende gesteld:

- dat sprake is van toename van het gebruik;
- dat er –gestoeld op de RVB BIM Norm- een stelsel van basisafspraken uitgebracht is (basis-ILS), dat inmiddels ondersteund wordt door ca. 200 partijen;
- dat er nog veel partijen zijn die de standaard niet toepassen;
- dat alle grote leveranciers van BIM-software (Bouwwerk Informatie Model) IFC in meer of mindere mate ondersteunen. Dit is echter al lange tijd zo en om die reden kan dat niet als maatstaf voor de adoptie van de standaard in de sector worden beschouwd;
- om de adoptie van de standaard goed in kaart te brengen zou een breed marktonderzoek noodzakelijk zijn. Op korte termijn is daarvoor evenwel geen budget.

Dit geeft nog steeds een goed beeld van het gebruik van IFC.

Het Rijksvastgoedbedrijf (RVB, fusie van onder meer Rijksgebouwendienst, Dienst Vastgoed Defensie) schrijft sinds 2011 het gebruik van IFC voor via de RVB BIM Norm in alle PPS-projecten. In de huidige RVB BIM Norm staat onder meer dat opdrachtnemers de informatie uit het gebouwmodel moeten aanleveren in de vorm van 2D-CAD-tekeningen[73] en als 3D-modellen in het open bestandsformaat IFC. Maar omdat het RVB in haar primaire processen vooralsnog berust op het gebruik van 2D-CAD tekeningen, is het interne gebruik van BIM (en dus ook van IFC) nog beperkt. Het afgelopen jaar is hier evenwel een aanzet tot verandering in gekomen met diverse BIM pilots die het enthousiasme van de toepassing van BIM als een olievlek doorheen de organisatie dienen te verspreiden, maar ook door bv. het beschikbaar stellen van een IFC-viewer in de grafische omgeving.

Het feit dat consortia de modellen aan het RVB aanleveren in IFC-formaat zegt overigens niets over het gebruik van IFC door de consortia in den brede; dat is aan de consortia zelf. De ervaring bij het RVB is dat consortia voor hun interne processen veelal gebruik maken van een merkspecifiek bronformaat. Dat staat IFC als uitwisselingsformaat evenwel niet in de weg. Het breed ondersteund initiatief van de basis-ILS met basisafspraken omtrent IFC geeft immers de groeiende acceptatie van IFC aan, vooral in het gebruik van IFC in de onderlinge communicatie met, en de coördinatie van BIM modellen. De ervaring bij het RVB wijst uit dat de ondersteuning van het IFC-formaat vanuit sterk in Nederland vertegenwoordigde modelleerapplicaties sinds 2011 flink is verbeterd, en zich nog continu aan het verbeteren is. Het RVB zal bij de eerstvolgende update van de RVB BIM Norm uitgaan van de “nieuwe”

[73] Reden hiervoor: de interne processen binnen het RVB zijn nog helemaal gestoeld op 2D-informatie.

versie van IFC, zijnde IFC4, om hiermee als vliegwiel ook de doorontwikkeling en verbetering van de software te stimuleren.

Conclusie:
Hoewel sprake is van een stijging van het gebruik, zijn er nog veel partijen die IFC niet toepassen. Harde gegevens omtrent het gebruik ontbreken.

F.8.2. VISI (Bouwprocesinformatie)

De VISI standaard richt zich op de formele communicatie tussen partijen in de bouwsector, zowel grond- weg en waterbouw, de burger & utiliteitsbouw als de installatiebranche.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
VISI	dec 2014	Eerste kencijfers beschikbaar	Stijgende trend

Bron: BIM loket

Bij BIM-loket is navraag gedaan over het gebruik van VISI. Zij beschikken over totaalgegevens van het aantal organisaties dat op servers van softwareleveranciers draait, alsmede het aantal accounts, het aantal transacties, het aantal berichten en het aantal bijlagen dat wordt gewisseld. Dit jaar is een eerste poging gedaan om het gebruik door overheden zichtbaar te maken. Onderstaande gegevens hebben betrekking op de periode 2017 tot en met september:

- aantal publieke opdrachtgevers die VISI hebben gebruikt (gemeenten, provincies, waterschappen en landelijke overheid samen): 90;
- aantal transacties verstuurd door deze opdrachtgevers: 169.465;
- aantal verstuurde berichten: 260.891;
- aantal verstuurde bijlagen: 224.739.

Het daadwerkelijke gebruik van VISI bouwbreed ligt nog veel hoger. Tegenwoordig worden veel UAV-GC projecten met VISI gedaan waarbij opdrachtnemers de meeste communicatie initieren. Verder zijn ook commerciële opdrachtgevers (denk aan woningcorporaties) niet in onderstaande data meegenomen. Het geheel overziend geeft onze bron aan dat in vergelijking met vorig jaar sector-breed (GWW) sprake is van een stijging van het gebruik van VISI met 70%. Dat percentage staat overigens los van het gebruik specifiek door overheden.

Conclusie:
Enkele harde gegevens over gebruik door overheden zijn voor het eerst beschikbaar. Een vergelijking met de vorige monitor is nog niet mogelijk. Het algemene beeld is dat sprake is van een toename van het gebruik.

F.9. Juridische identificatie en verwijzing

De drie Juriconnect standaarden BWB, ECLI en JCDR zijn gericht op standaardisatie van identificatie met het doel om de geïdentificeerde inhoud te delen.

Voor verwijzing naar wet- en regelgeving of onderdelen daarvan in wetten.overheid.nl is aan elke regeling een uniek identificatienummer (BWBID) toegekend. De Juriconnect-**BWB**-standaard beschrijft hoe deze verwijzing wordt vormgegeven. Citeren, vinden en verbinden van wet- en regelgeving gaat door toepassing van de BWB standaard sneller, eenvoudiger en geeft minder kans op fouten. Gebruik van de standaard biedt daardoor verbetering van interoperabiliteit. De open standaard BWB biedt een eenduidige manier van verwijzen naar (onderdelen van) wet- en regelgeving. De laatste versie (versie 1.3.1) maakt het mogelijk om in wet- en regelgeving te kunnen verwijzen naar:

- taalversies en onderdelen van internationale verdragen,
- wet- en regelgeving waarvan de indeling niet voldoet aan de gebruikelijke nummering van hoofdstukken en paragrafen, en
- ruime begrippen zoals "enig artikel".

Met de **ECLI**-standaard (versie 1.0) kunnen:

- alle rechterlijke uitspraken in de Europese Unie (zowel van nationale als van Europese gerechten) worden voorzien van een gelijkaardige, unieke en persistente identifier. Deze identifier kan worden gebruikt voor identificatie en citatie van rechterlijke uitspraken en derhalve om deze te vinden in binnenlandse of buitenlandse, Europese of internationale jurisprudentie-databanken;
- alle rechterlijke uitspraken worden voorzien van uniforme metadata, gebaseerd op de Dublin Core standaard. Het zoeken van uitspraken in allerlei databanken wordt daardoor gefaciliteerd.

De **JCDR**-standaard (versie 1.0) biedt een eenduidige manier van verwijzen naar (onderdelen van) decentrale regelgeving waarmee de interoperabiliteit van juridische documenten en systemen die veel verwijzingen kennen naar decentrale regelgeving wordt bevorderd.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
BWB, ECLI en JCDR	BWB feb 2016, ECLI en JCDR nov 2013	in diverse voorzieningen geïmplementeerd, geen harde gebruiksgegevens	geen harde gegevens beschikbaar

Bron: KOOP (Kennis- en Exploitatiecentrum Officiële Overheidspublicaties)

Bij de servicedesk van het KOOP (Kennis- en Exploitatiecentrum Officiële Overheidspublicaties) is in de zomer van 2017 wederom navraag gedaan naar gebruiksgegevens. Net als bij de vorige monitor geeft men aan niet over harde gegevens te beschikken. Er wordt namelijk niet actief gemonitord op het gebruik van de standaarden. In algemene termen geeft men aan dat de situatie niet anders is dan vorig jaar (en daarmee ook in 2015 en 2014). Het beeld is – indicatief – als volgt:

- De Juriconnect-BWB-standaard is geïmplementeerd in het BasisWettenBestand van de overheid dat zowel via de internetsite wetten.overheid.nl als via diverse services als open data beschikbaar is gemaakt. Zowel door de diverse hergebruikers van de open data van dit BasisWettenBestand in het juridisch domein als door in het platform Juriconnect deelnemende partijen wordt voor het verwijzen naar de verdragen, wetten en regelingen geconformeerd aan de standaard. Hierbij gaat het om de overheid (centraal

en decentraal), uitgevers van juridische informatie, content integrators, uitvoeringsorganisaties en individuele aanbieders van juridische informatie.
- De JCDR-standaard is geïmplementeerd in de Centrale Voorziening voor Decentrale Regelgeving.
- De ECLI wordt toegekend aan alle uitspraken van (tucht)rechterlijke instanties die in Nederland worden gepubliceerd. Deze ECLI's zijn alle terug te vinden in het ECLI-register op Rechtspraak.nl. Bij het citeren van uitspraken wordt tegenwoordig vrijwel altijd gebruik gemaakt van ECLI; door rechters in vonnissen en arresten, door rechtsgeleerden en door ambtenaren (beleidsnotities e.d.). Er is sprake van toenemend gebruik in andere landen van ECLI alsmede door het Europees Hof van Justitie en het Europees Patentbureau. Dit bevordert de acceptatie van de standaard. Uitbreiding van het gebruik ligt in het verschiet; door het Europees Hof voor de Rechten van de Mens en door een achttal extra landen.

Conclusie:
Over het gebruik van deze standaarden zijn op dit moment geen harde gegevens beschikbaar, evenmin als voorgaande jaren.

F.10. Onderwijs en loopbaan

Over e-Portfolio is niet (voldoende) relevante informatie ontvangen om te kunnen rapporteren.

F.10.1. NL LOM (Vindbaarheid van leermaterialen)

NL LOM is een standaard die voorschrijft welke metadata toegekend moeten worden aan educatieve materialen om de vindbaarheid en vergelijkbaarheid te vergroten. Met metadata worden extra kenmerken van een document of ander object bedoeld. Te denken valt aan auteursgegevens, titel, uitgever, taal, etc. NL LOM is een Nederlands profiel op de internationale standaard IEEE LOM (Learning Object Metadata). NL LOM is gemaakt voor de sectoren primair onderwijs, voortgezet onderwijs, middelbaar beroepsonderwijs en hoger onderwijs.

NL LOM is nauw verweven met de OAI-PMH-standaard bij het ontsluiten en metadateren van educatieve content. Er is daarvoor een centrale repository gecreëerd waarin alle metadata en verwijzingen naar educatieve content vanuit diverse bronnen bijeen worden gebracht: Edurep, ook wel aangeduid als educatieve zoekmachine. Gebruikers (m.n. docenten) hoeven maar in één repository te kijken als ze onderwijsmateriaal zoeken. Edurep maakt gebruik van NL LOM en OAI-PMH. Plaatsing van beide standaarden op de lijst met de verplichte status was een middel om de belangstelling, het draagvlak en het aantal gebruikers te vergroten.

standaard	*op lijst sinds*	*gebruik door overheden*	*ontwikkeling in gebruik*
NL LOM	mei 2011	Publieke en private aanbieders van onderwijsmaterialen. Indirect (voor zoeken van onderwijs-materiaal): publieke en private partijen en individuen binnen het onderwijsveld	niet bekend

Binnen het toepassingsgebied van 'leermaterialen in het onderwijsveld' hebben OAI-PMH en NL LOM de gewenste positie verworven, de standaarden worden breed gebruikt (zie verder de paragraaf over OAI PMH). NL LOM wordt niet buiten de onderwijssector gebruikt.

In een eerdere monitor is het gebruik van NL LOM in een percentage uitgedrukt. Die gegevens waren gebaseerd op onderzoek naar het gebruik van open standaarden in de sector onderwijs (2013, in opdracht van het Ministerie van OCW). Later is een dergelijk onderzoek niet meer uitgevoerd zodat een tijdlijn niet is te maken.

Conclusie
Voor wat betreft aanbieders en afnemers van leermaterialen binnen het onderwijsveld is het gebruik van NL LOM zeer hoog. NL LOM kent geen gebruik buiten de onderwijssector. Een ontwikkeling in de tijd kunnen we met de beschikbare gegevens niet maken.

F.10.2. OAI-PMH (Vindbaarheid van leermaterialen)

OAI-PMH is een standaard voor harvesting van metadata uit repositories. Een repository is een bibliotheek met documenten/objecten (ook wel 'content' genoemd), bijvoorbeeld een (digitaal) archief. OAI-PMH maakt het mogelijk om deze metadata (dus niet de documenten / objecten zelf) uit verschillende repositories te verzamelen. Vanuit een centraal systeem kan dan gezocht worden naar documenten/objecten in de verschillende aangesloten repositories.

OAI-PMH is nauw verweven met de NL-LOM-standaard bij het ontsluiten en metadateren van educatieve content. Er is daarvoor een centrale repository gecreëerd waarin alle metadata en verwijzingen naar educatieve content vanuit diverse bronnen bijeen worden gebracht: Edurep, ook wel aangeduid als educatieve zoekmachine. Gebruikers (m.n. docenten) hoeven maar in één repository te kijken als ze onderwijsmateriaal zoeken. Edurep maakt gebruik van NL LOM en OAI-PMH. Plaatsing van beide standaarden op de lijst met de verplichte status was een middel om de belangstelling, het draagvlak en het aantal gebruikers te vergroten.

standaard	*op lijst sinds*	*gebruik door overheden*	*ontwikkeling in gebruik*
OAI-PMH	dec. 2010	Hetzelfde als NL LOM voor wat betreft de onderwijssector. Daarnaast zeer breed gebruik binnen erfgoedsector.	

Binnen het toepassingsgebied van 'leermaterialen in het onderwijsveld' hebben OAI-PMH en NL LOM de gewenste positie verworven, de standaarden worden breed gebruikt. Er is voor het onderwijsveld een afspraak gebaseerd op het OAI-protocol opgesteld, die wordt beheerd door Kennisnet (Platform Edustandaard). Kennisnet biedt handleidingen en verwijzingen voor implementatie en gebruik van NL LOM en OAI-PMH. Veel partijen gebruiken Edurep, het biedt toegang tot meer dan 1.400.000 leermaterialen en verwerkt

maandelijks meer dan 2.000.000 zoekvragen. Aangesloten partijen maken daarbij gebruik van beide standaarden. Binnen de groep aangesloten partijen kan een onderscheid worden gemaakt tussen aanbieders (meer dan 50) en afnemers (bijna 20 partijen).

OAI-PMH wordt ook buiten de onderwijssector gebruikt[74]. OAI-PMH wordt namelijk breed gebruikt binnen de erfgoedsector, het wordt beschouwd als de norm voor de samenwerking van instellingen in de erfgoedsector. De standaard kent dan ook een hoge adoptiegraad binnen de sector. Vrijwel alle middelgrote en grote instellingen (bijv. de Koninklijke Bibliotheek, het Nationaal Archief, het Rijksmuseum en Beeld en Geluid) passen OAI-PMH toe voor de uitwisseling van metadatasets.

Ook bij kleinere instellingen is het gebruik van OAI-PMH gangbaar, al is de adoptiegraad hier minder hoog. Bij kleinere instellingen kan o.a. gedacht worden aan gemeenten en organisaties die specifieke collecties beheren zoals Stichting Papua Cultureel Erfgoed en de Vereniging De Hollandsche Molen. De lagere adoptiegraad komt voornamelijk voort uit het feit dat er doorgaans minder middelen beschikbaar zijn voor OAI-implementaties. Hierdoor wordt bij deze instellingen vaker gekozen voor goedkopere en traditionelere oplossingen zoals CSV-dumps. Dit is een ad-hoc oplossing waarbij een kopie van de gegevens wordt gemaakt in een zeer eenvoudige bestandsindeling.

De hoge adoptiegraad is geleidelijk ontstaan en ook op dit moment zijn OAI-PMH implementatietrajecten nog aan de orde. Belangrijke aanjagers van OAI-PMH zijn aggregatieplatformen als Europeana geweest die OAI-PMH vereisen. Dergelijke aggregatieplatforms zijn een soort verzamelbibliotheken waar gegevens van andere collecties bij elkaar worden gevoegd. Hier zit een gelaagdheid in waarbij grote platforms als Europeana beschouwd kunnen worden als de top van een piramide.

Alle grote leveranciers (o.a. Picturae en DE REE en DEVENTit) van collectiebeheersystemen in Nederland hebben de implementatie van het protocol opgenomen in hun software.

In een eerdere monitor is het gebruik van de standaarden in een percentage uitgedrukt. Die gegevens waren gebaseerd op onderzoek naar het gebruik van open standaarden in de sector onderwijs (2013, in opdracht van het Ministerie van OCW). Later is een dergelijk onderzoek niet meer uitgevoerd zodat een tijdlijn niet is te maken.

Conclusie
Voor wat betreft aanbieders en afnemers van leermaterialen binnen het onderwijsveld is het gebruik van OAI-PMH zeer hoog. OAI-PMH kent tevens een brede adoptie binnen de erfgoedsector. Een ontwikkeling in de tijd kunnen we met de beschikbare gegevens niet maken.

F.11. Overig

Binnen deze 'restcategorie' valt een tweetal standaarden: EMN_NL en STOSAG. Van STOSAG is geen informatie ontvangen.

[74] Kennisnet ambieert daar geen rol als beheerder; dat past namelijk niet bij de missie van Kennisnet: 'Laat ICT werken voor het onderwijs'.

F.11.1. EML_NL (Verkiezingsgegevens)

De EML_NL standaard versie 1.0 is het Nederlands toepassingsprofiel op de Election Markup Standard en 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.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
EML_NL	nov 2013	elke gemeente	n.v.t.

Beheerorganisatie: Kiesraad

De standaard EML_NL is de vertaling van de internationale EML-standaard naar de Nederlandse situatie. De totstandkoming van de EML_NL standaard liep samen op met de ontwikkeling van Ondersteunende Software Verkiezingen (OSV) en daarin opgenomen. De software (OSV en daarmee ook het gebruik van de EML_NL standaard) wordt door de Kiesraad ter beschikking gesteld voor gebruik tijdens verkiezingen. De voornaamste gebruikers zijn politieke partijen, gemeenten, hoofdstembureaus en centraal stembureaus.

Gedurende 2016 heeft een referendum en een verkiezing plaatsgevonden:

- Referendum over het Associatieovereenkomst tussen de Europese Unie en Oekraïne (6 april). OSV-software is beschikbaar gesteld aan:
    - 19 hoofdstembureau gemeenten;
    - 393 gemeenten (alle gemeenten hebben ook daadwerkelijk gebruik gemaakt van de software);
- Gemeentelijke herindelingsverkiezingen (23 november; één nieuw te vormen gemeente). De OSV-software is beschikbaar gesteld aan:
    - de nieuw te vormen gemeente;
    - ongeveer 15 politieke partijen (lokale afdelingen; onbekend hoeveel er daadwerkelijk gebruik hebben gemaakt van de software).

De EML-bestanden met de uitslaggegevens van de gehouden verkiezing en referendum zijn als open data beschikbaar op data.overheid.nl[75].

Conclusie:
De standaard EML_NL wordt toegepast door alle gemeenten in Nederland.

[75] https://data.overheid.nl/data/dataset?q=eml

Bijlage G. Meting IV-standaarden Forum Standaardisatie medio 2017

Halfjaarlijkse meting **Informatieveiligheidsstandaarden** Forum Standaardisatie

= Medio 2017 =

Samenvatting

Uit de meest recente meting (juli 2017) van overheidsdomeinen op gebruik van de IV-standaarden blijkt dat de adoptie van deze standaarden weer is gegroeid. De groei zwakt echter wel af. Bovendien verschilt de groei aanzienlijk per 'overheidslaag'. Gemeenten doen het net als bij de vorige meting relatief goed, maar ook bij hen is de groei in 2017 afgezwakt ten opzichte van de tweede helft van 2016. Als de groeipercentages van de eerste helft 2017 doorzetten, dan haalt **geen** van de 'overheidslagen' het in 2016 uitgesproken streefbeeld om eind 2017 de standaarden te hebben geïmplementeerd.

Achtergrond

Sinds 2015 biedt het Platform Internet Standaarden[1] de mogelijkheid om via de website internet.nl[2] domeinen te toetsten op het gebruik van internet- en beveligingsstandaarden die op de 'pas toe of leg uit' -lijst van Forum Standaardisatie staan. In datzelfde jaar is Forum Standaardisatie gestart met een halfjaarlijkse meting van overheidsdomeinen op het voldoen aan deze standaarden.

Die metingen hebben ertoe geleid dat het Nationaal Beraad in februari 2016 de ambitie uitsprak deze standaarden versneld te willen adopteren[3]. Dit betekent concreet dat voor deze standaarden niet het tempo van 'pas-toe-of-leg-uit' wordt gevolgd (i.e. wachten op een volgend investeringmoment en dan de strandaarden implementeren) maar dat actief wordt ingezet op implementatie van de standaarden op de korte termijn[4]. Voorliggende notitie bevat de resultaten van de meest recente meting van juli 2107.

Om welke standaarden gaat het

Het Nationaal Beraad heeft bovengenoemde afspraken gemaakt met betrekking tot de volgende standaarden[5]:

- DNSSEC: Domeinnaambeveiliging
- TLS[6] : Beveiligde verbinding
- DKIM: Anti-Phishing
- SPF: Anti-Phishing
- DMARC[7]: Anti-Phishing (rapportages)

---

[1] Platform Internet Standaarden is een gezamenlijk initiatief van Forum Standaardisatie, het Ministerie van Economische zaken en het Nederlandse internet gemeenschap. Zie https://internet.nl/about/

[2] Om vergelijking tussen de verschillende metingen mogelijk te maken, worden hier *dezelfde* elementen gemeten als in de 0-meting. Het is dus niet zo dat de meting ondertussen 'strenger' is geworden (in tegenstelling tot het scoringspercentage op internet.nl)

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

[4] Onderdeel van deze afspraak is dat Forum Standaardisatie de voortgang van de adoptie meet en inzichtelijk maakt. Om die reden is de halfjaarlijkse meting vanaf dit jaar onderdeel van de Monitor Open standaarden beleid.

[5] Zie: https://www.forumstandaardisatie.nl/lijst-open-standaarden/in_lijst/verplicht-pas-toe-leg-uit

[6] Voor TLS geldt dat het Nationaal Beraad de ambitie uitsprak deze eind 2017 tenminste voor die domeinen toe te passen waar burgers en bedrijven mogelijk privacy -gevoelige gegevens invoeren (een zogenaamde transactiesite). Overheden worden opgeroepen om dergelijke domeinen, die nog niet getoetst worden, bij Forum Standaardisatie te melden, zodat deze onderdeel kunnen worden van de halfjaarlijkse toetsing. Onlangs sprak het Nationaal Beraad het streefbeeld af om https/hsts eind 2018 in alle overheidswebsites te hebben toegepast.

Om welke domeinen gaat het

In totaal zijn in deze meting 544 domeinen getoetst, bestaande uit:

- Domeinen die horen bij de deelnemers van het Nationaal Beraad
- De domeinen die horen bij voorzieningen van de Generieke Digitale Infrastructuur.
- De 25 best bezochte domeinen van Rijksoverheden (en uitvoerders

- De domeinen van de andere partijen die direct of indirect vertegenwoordigd zijn in het nationaal beraad, zoals:
    - Uitvoerders (de Manifestpartijen)
    - Gemeenten
    - Provincies en Waterschappen
    - Partijen die behorend tot Klein LEF

Hoe wordt gemeten

De meting geeft de stand van zaken weer eind juli 2017. De meting laat zien of een domein de standaarden toepast. 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.

Ten aanzien van de meting van specifieke standaarden merken wij het volgende op:

- Wij 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)[8].
- Wij meten het gebruik van TLS op alle (website)domeinen omdat wij onvoldoende informatie hebben over individuele domeinen om te weten of er op een website vertrouwelijke gegevens worden uitgewisseld.
- Bij gemeenten meten wij het gebruik van TLS alleen op het hoofddomein, omdat wij geen inzicht hebben in de overige domeinen die een gemeente voor verschillende doeleinden gebruikt. Wij roepen u daarom op om ons te wijzen op aanvullende transactiedomeinen die aanvullend gemeten zouden moeten worden.
- Wij meten het gebruik van e-mail beveiligingsstandaarden ook op domeinen waarvan een organisatie geen e-mail verstuurt. Dit is relevant, omdat ook die domeinen worden misbruikt (burgers weten vaak niet of deze domeinen door de organisatie worden gebruikt), en juist domeinen waarvandaan niet gemaild wordt, makkelijk kunnen worden geblokkeerd met SPF.
- TLS: Als een domein bereikbaar is via ipv6 dan wordt de toepassing van TLS getoetst via IPv4 én IPv6. De slechtste configuratie bepaald de eindscore.

---

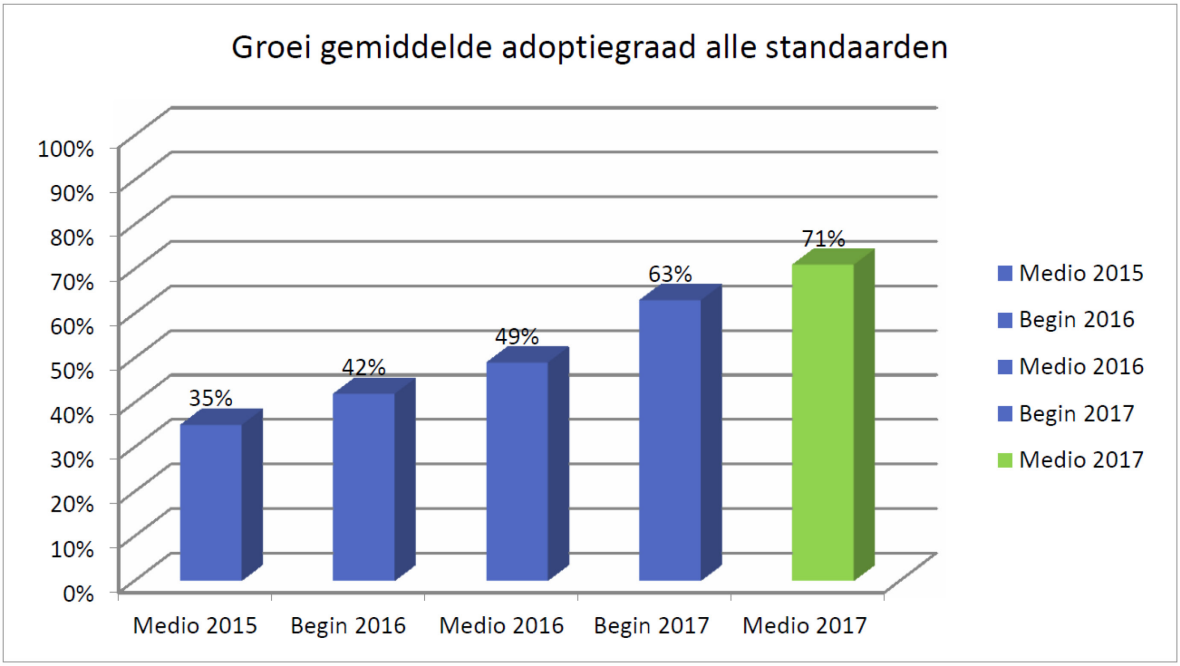
[7] DMARC is positief getoetst maar nog niet opgenomen op de pas-toe-of-leg-uit lijst. DMARC hangt echter dermate sterk samen met de toepassing van DKIM en SPF, dat het Nationaal Beraad besloot DMARC alvast onderdeel te maken van de 'versnelde adoptie set'.

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

- De gemeten 544 domeinen zijn bij lange na niet alle domeinen waar het Nationaal Beraad direct en indirect voor verantwoordelijk is. Een goede score op deze domeinen garandeert geenszins dat hiermee alle overheidsdomeinen beschermt zijn tegen bijvoorbeeld phising.
- DKIM: Als van weergegeven (sub-)domeinen geen mail wordt verstuurd, is de toepassing van DKIM weinig zinvol en daarom ook niet verplicht. Voor dergelijke (sub-)domeinen moet DMARC wel worden toegepast met een policy *"p=reject"* en SPF ook met als policy "*-all*" *(hard fail)*. Forum Standaardisatie vraagt u als domeinnaam-eigenaar/-beheerder om door te geven als van uw (sub-)domein niet wordt gemaild, zodat wij hier bij onze volgende meting rekening mee kunnen houden

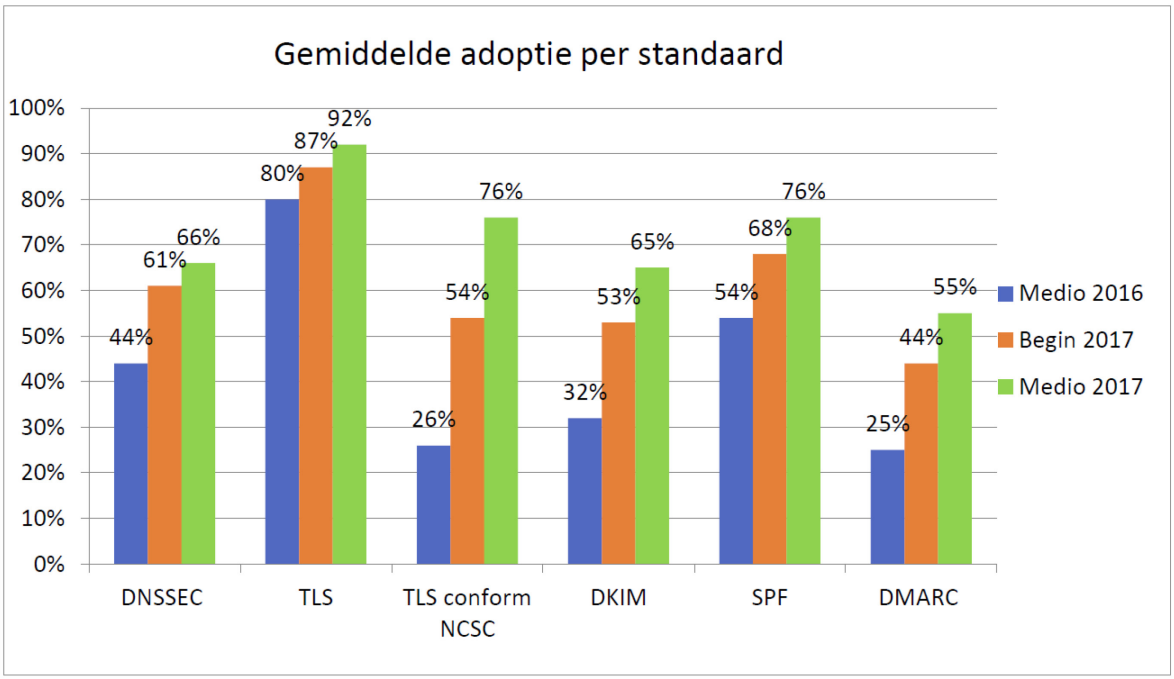
In bijlage 1 worden alle individuele scores op de vijf genoemde standaarden weergegeven. Bij deze rapportage wordt de score van de webstandaarden DNSSEC en TLS weergegeven zoals getoetst op het 'www. -domein' De mailstandaarden (DKIM,SPF&DMARC) zijn getoetst op hetzelfde domein zonder 'www.' .

Resultaten



Figuur 1: De groei van de gemiddelde adoptiegraad van alle standaarden sinds medio 2015.

Zoals te zien in bovenstaande figuur, groeit de gemiddelde adoptiegraad van de vijf getoetste standaarden gestaag. Binnen een tijdsbestek van 2 jaar is het gemiddelde ruim verdubbeld. Tegelijk is het, gegeven de ambitie om eind 2017 de 100% te hebben bereikt, nodig om in het komende half jaar een enorme versnelling in te zetten. De gemiddelden verschillen per overheidslaag. Figuur 3 laat zien wat de gemiddelden zijn per overheidlaag.



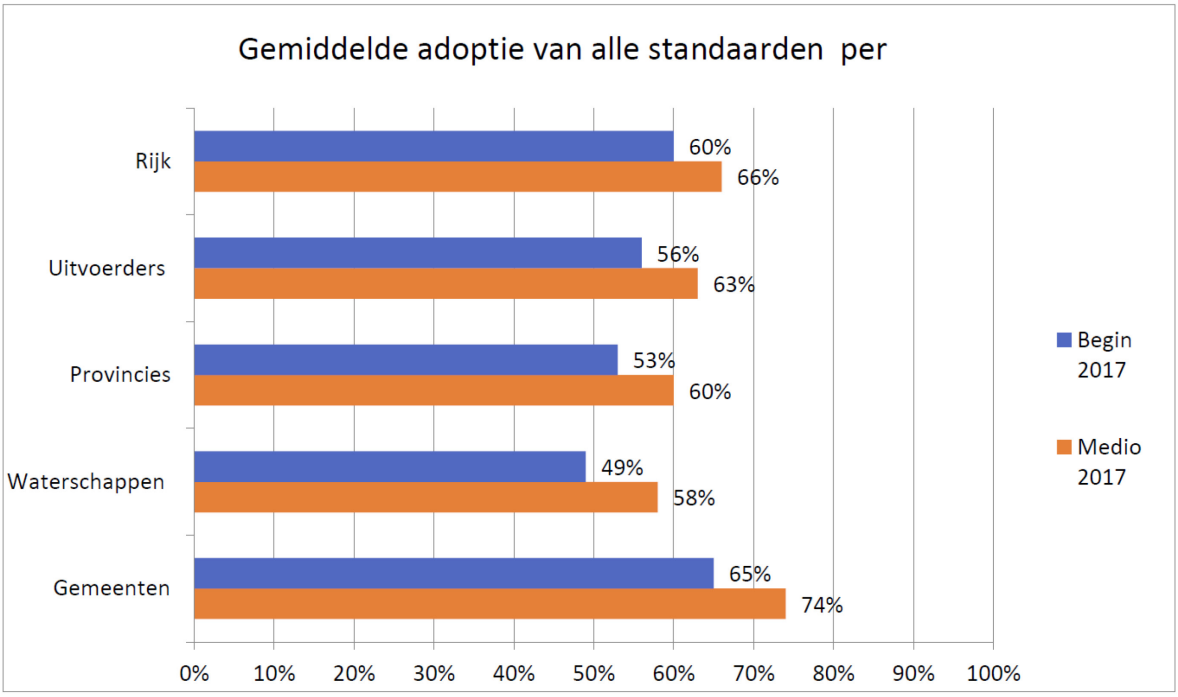
Figuur 2. Adoptiegraad van de individuele standaarden over alle getoetste domeinen.

Wat valt op:

- De Toepassing van alle standaarden is wederom gegroeid in het afgelopen half jaar, maar de groei zwakt wel af.
- De groei is met name bij DNSSEC beperkt. Een duidelijke verklaring hiervoor is niet te geven.
- De groei van TLS is ook beperkt, maar niet vreemd, want tegelijk is de adoptiegraad van TLS het hoogst van alle standaarden (92%). Gemeenten, Uitvoerders en Waterschappen hebben allen een TLS-adoptiegraad hoger dan 90%.
- Het aantal keer dat TLS conform de richtlijnen van het NCSC wordt toegepast is het afgelopen halve jaar wederom flink toegenomen.
- De toepassing van DMARC blijft achter bij de overige standaarden.

Hoe scoren de verschillende 'overheidslagen'?

In deze rapportage wordt een onderscheid gemaakt tussen de 'overheidslagen' : Rijk, uitvoerders, provincies, waterschappen en gemeenten.

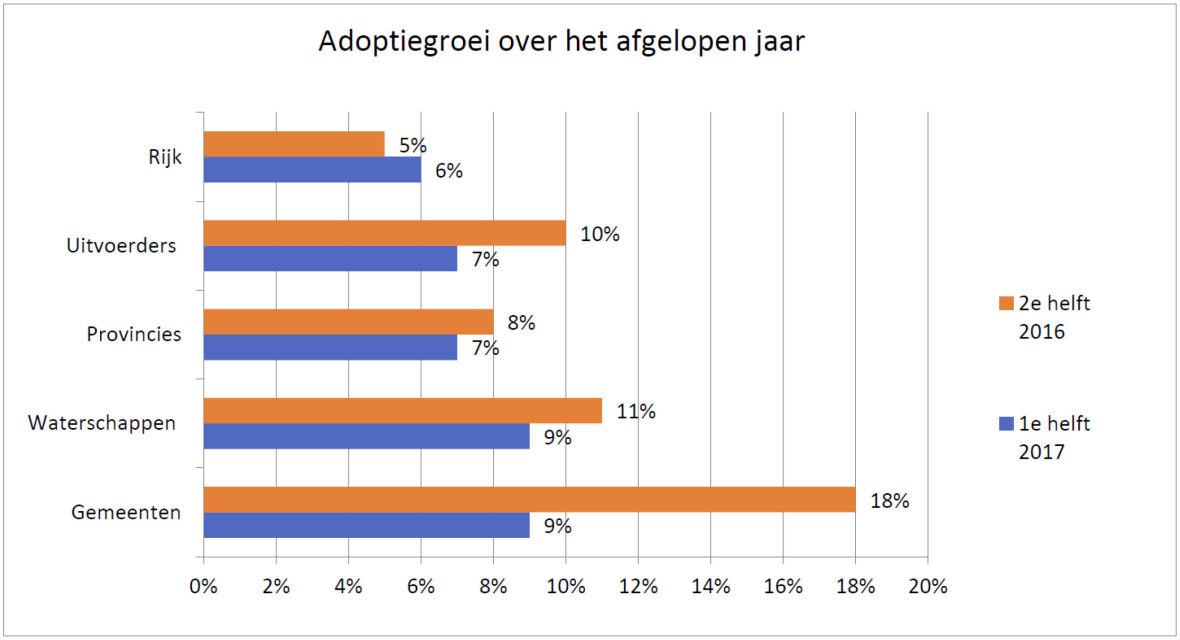


Figuur 3. De gemiddelde adoptiegraad van alle vijf de standaarden per 'overheidslaag'.

Wat valt op:

- Medio 2017 is de gemiddelde adoptiegraad bij gemeenten wederom het hoogst.
- De het groeipercentage 9 %-punt is (samen met de waterschappen) het hoogst. Gezien het enorme aantal gemeentedomeinen waar het hier om gaat (396) is de groei extra indrukwekkend.
- Het Rijk (begin 2016 nog koploper) blijft een goede tweede, maar het verschil met de vorige meting is beperkt.
- De waterschappen blijven hangen op een gemiddelde adoptie van alle standaarden van 58% en scoren daarmee het laagst.

Groei sinds Begin 2017



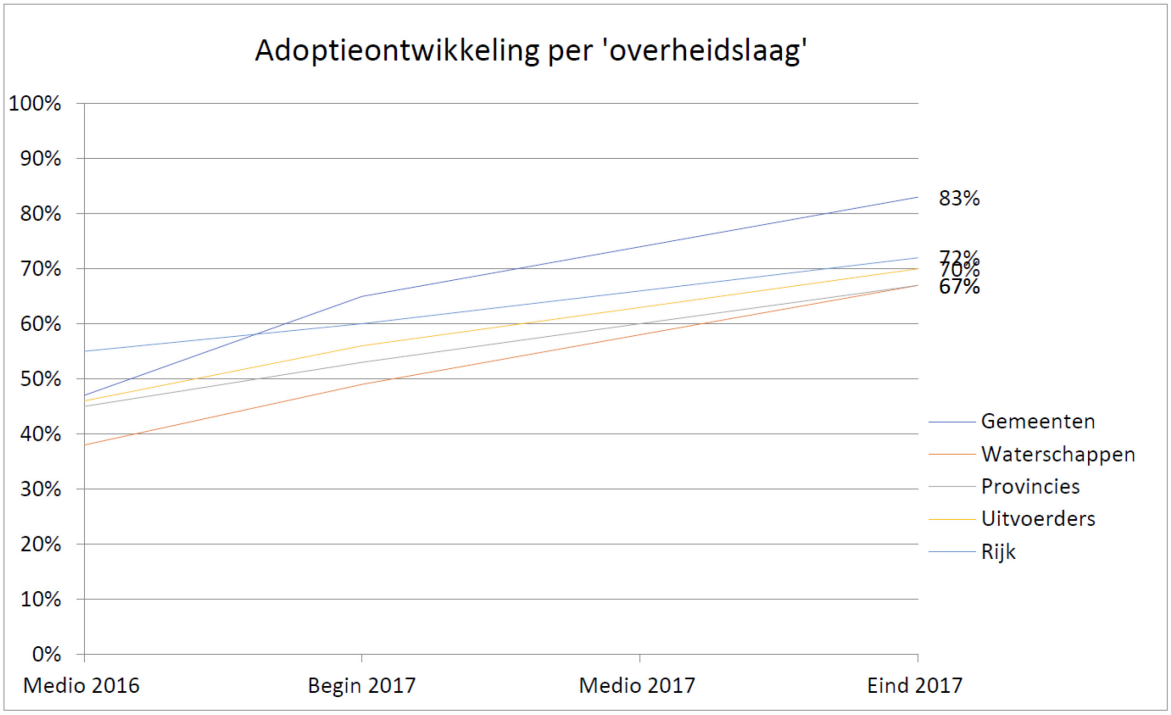
Figuur 4: De ontwikkeling van de gemiddelde adoptiegraad over het afgelopen jaar

Wat valt op:

- Alleen het rijk laat een lichte versnelling van de groei zien over de afgelopen zes maanden.
- De enorme groei van gemeenten in de tweede helft van 2016 is niet op hetzelfde tempo doorgezet in de eerste helft van 2017 en is helaas gehalveerd.
- Daarbij moet worden opgemerkt dat een groeipercentage van 9%-punt over 396 domeinen alsnog indrukwekkend is.
- Het groeipercentage bij de provincies en uitvoerders is het laagst. Bij provincies betreft het de kleinste groep domeinen (16) waardoor het percentage extra teleurstellend is. Tegelijkertijd ligt er een kans om met de verbetering van een aantal domeinnamen een flinke percentuele verbetering te realiseren.
- Voor alle overheidslagen geldt dat zij het streefbeeld voor eind 2017 niet zullen halen als de groei over de eerste helft van 2017 doorzet (zie de volgende alinea en figuur 5).

Verwachting voor eind 2017

Net als bij voorgaande rapportages hebben we de groei over de afgelopen periode genomen en deze geëxtrapoleerd naar eind 2017. Per 'overheidslaag' is gekeken of zij met hun huidige adoptiegraad en groei over de afgelopen zes maanden, de ambitie kunnen verwezenlijken om eind 2017 alle standaarden – daar waar van toepassing- te hebben geïmplementeerd.



Figuur 5: Extrapolatie gemiddelde groei verschillende overheden. Naar eind 2017.

Wat valt op:

- Als de groei over het afgelopen halve jaar wordt doorgezet in de tweede helft 2017 haalt **geen** van de 'overheidslagen' het genoemde streefbeeld.
- Gemeenten scoren met een verwachte gemiddelde van 83% het best.
- Het Rijk is tweede met 72%. Het Rijk had aan het begin van van de metingen de beste uitgangspositie..
- Provincies en waterschappen blijven in de extrapolatie steken op een gemiddelde adoptiegraad van 67%.

Score verbeteren?

Zoals bij eerdere rapportages bevat deze rapportage een bijlage met de scores van de vijf standaarden per getoetst domein. Als uw domeinen nog niet goed scoren op alle standaarden, bevelen wij aan gebruikt te maken van https://internet.nl/ Deze site geeft per standaard in detail aan waar het eventueel aan schort en wat er verbeterd dient te worden voor een positieve score.

Daarnaast biedt de site automatisch een toets op een aantal aanpalende informatieveiligheidsstandaarden aan, die het Forum Standaardisatie, het NCSC en Platform Internet standaarden aanbevelen om toe te passen. Mocht u vragen hebben over de site en aangeboden toets, dan kunt u terecht bij vraag@internet.nl

Heeft u vragen over voorliggende rapportage of scores, dan kunt u het best contact opnemen via info@forumstandaardisatie.nl