FS-20171213.04A

Rapport

Monitor Open standaardenbeleid: 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 1.0

Datum 30-11-2017

Inhoudsopgave

Bijlagen

1. Managementsamenvatting

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 standaardenbeleid 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'

[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.

geplaatst. Op deze open standaarden (zomer 2017 waren dit er 40) is het 'pas toe of leg uit'-regime van toepassing.

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

Monitor Open standaardenbeleid 2017 (H2)

In opdracht van het Bureau Forum Standaardisatie voert ICTU jaarlijks de Monitor Open standaardenbeleid 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.

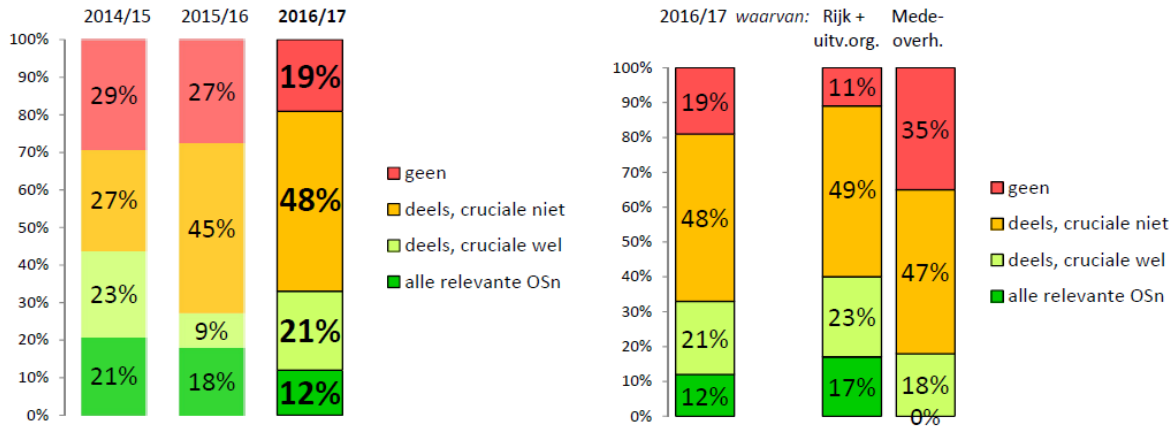
In het navolgende worden de voornaamste bevindingen per deelonderzoek samengevat. De positieve bevindingen hebben een groen blokje (+), de minder positieve een oranje (-).

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 -

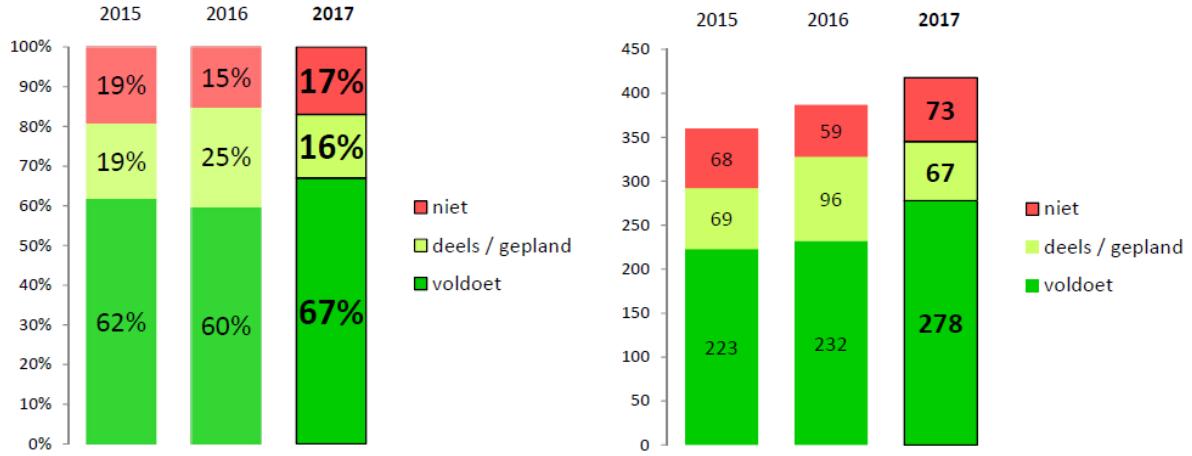
	diensten en bedrijfsvoering.

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.

[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.

+	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 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:

+	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

[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.

	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 standaardenbeleid.

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

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

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, 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. 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.

[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."

Zie Bijlage A voor een stroomschema.

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.

[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).

Een open standaard van de lijst is altijd relevant als het betreffende ICT-product of -dienst valt binnen het functionele toepassingsgebied van die open standaard, als de organisatie bovendien valt binnen het organisatorische werkingsgebied van de betreffende standaard.[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 standaardenbeleid

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.

[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.

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

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 standaardenbeleid 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].

[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).

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

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:

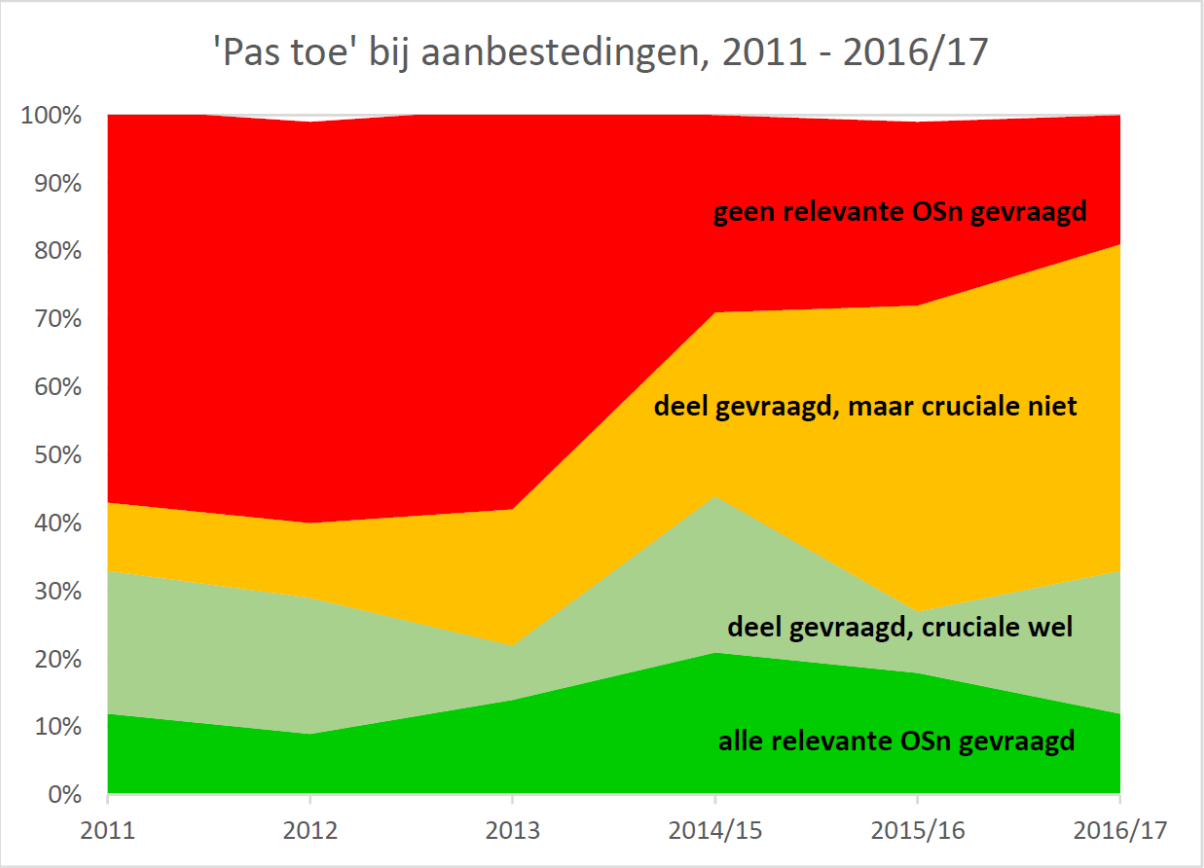
- Het aantal aanbestedingen waarbij om alle relevante standaarden is gevraagd is iets afgenomen, van 18% naar 12%; ook vorig jaar was er al een geringe afname (van 21% naar 18%). De daling dit jaar is vrijwel geheel toe te schrijven aan het feit dat in de categorie andere overheden bij geen enkele aanbesteding 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%.

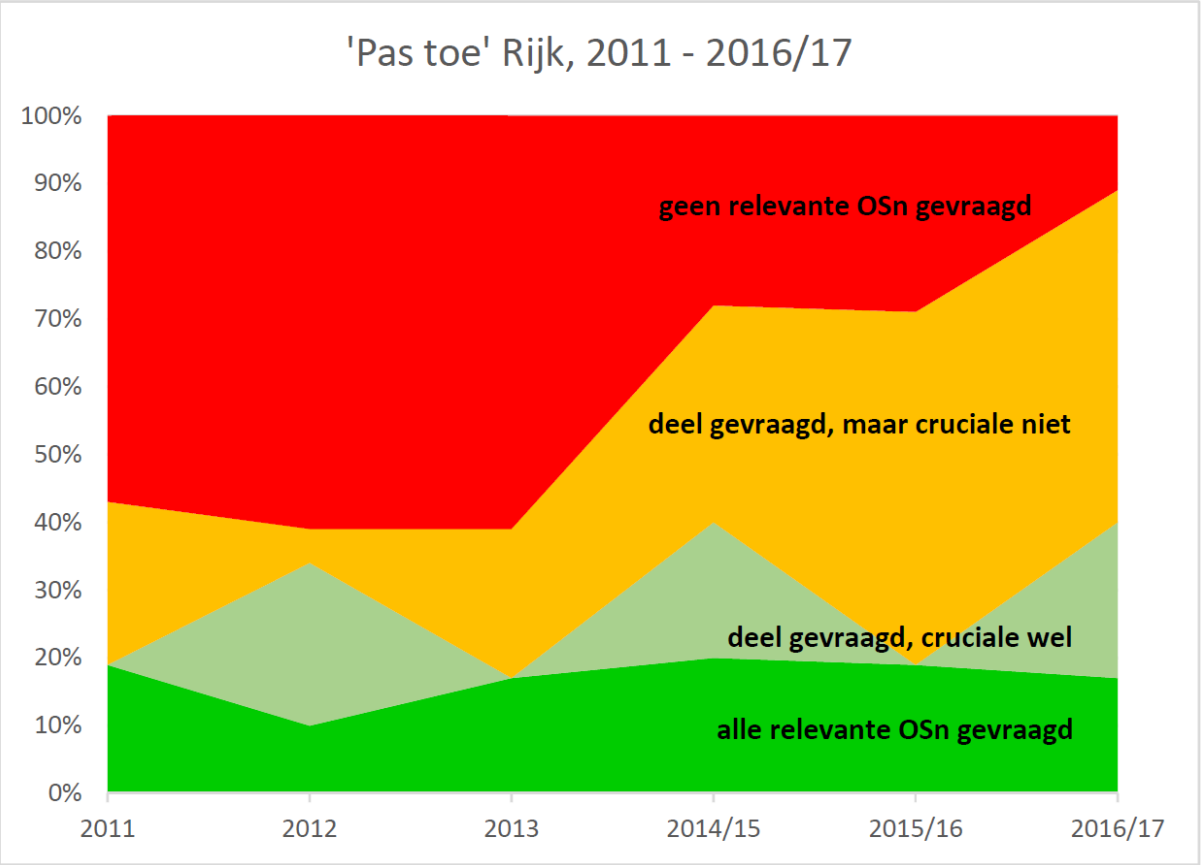
Figuur 2: 'Pas toe' bij feitelijke aanbestedingen 2011 - 2016/2017



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%.

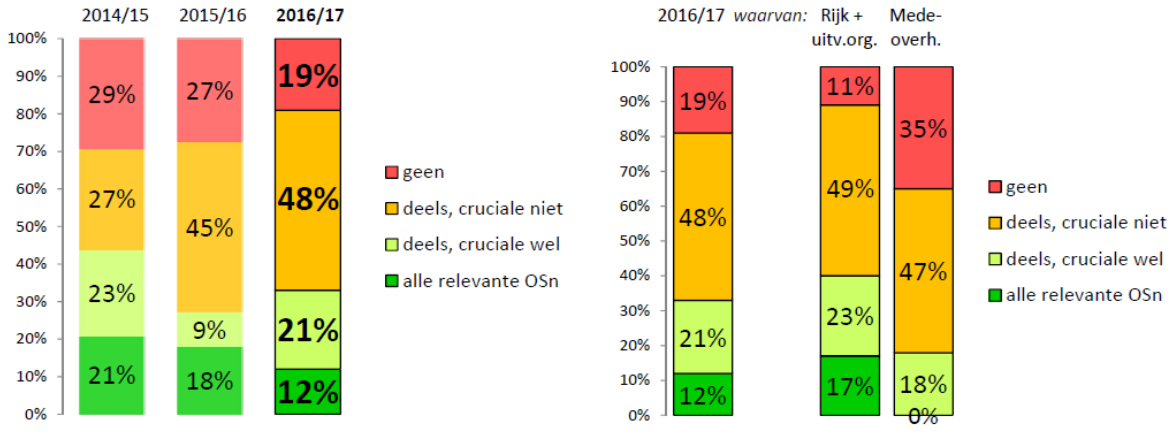
Eerder is al opgemerkt dat de score dit jaar voor de andere overheden duidelijk van invloed is op het totaalbeeld. Om in de terminologie te blijven van de kleuren uit bovenstaande tabel: het groene deel is bij de andere overheden helemaal verdwenen, het lichtgroene deel is gelijk gebleven en zowel het 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

[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
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 operating system voor de IBM System z mainframe(s) van de Belastingsdienst.	ISO 27001/27002	IPv4 en IPv6	B
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

aanbesteder	inhoud aanbesteding	standaarden[14] cruciaal	standaarden niet-cruciaal	oordeel
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 binnen BZK, met andere actoren in het openbaar bestuur en met wetenschappers, onderzoekers en studenten.	Digitoegankelijk DNSSEC ISO 27001/27002 TLS	IPv4 en IPv6 ODF PDF	C
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	IPv4 en IPv6 ISO 27001/27002 TLS	WPA2 Enterprise	C

aanbesteder	inhoud aanbesteding	standaarden[14] cruciaal	standaarden niet-cruciaal	oordeel
	en kunstwerken - in het beheergebied.			
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
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.

[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%).

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 uitvraag-percentage van 100% maar voor deze standaard geldt dat die slechts één maal als relevant is aangemerkt.

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].

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

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), 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 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).

[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.

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. 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:

BAG, BRK, WOZ en BGT
Berichtenbox bedrijven
BRI (inkomen)
BRT (topografie)
BRV (voertuigen)
BSN Beheervoorz. + GBA-V
DigiD
DigiD Machtigen
Digilevering
Digimelding
Diginetwerk
DigiPoort
Afsprakenstelsel ETD
e-Factureren
MijnOverheid
NHR (Nieuw HandelsRegister)
Ondernemersplein
Overheid.nl
PKI Overheid
Samenwerkende Catalogi
SBR (Standard Business Rep.)
Stelselcatalogus

Andere voorzieningen:

Digi-Inkoop
Digitale Werkomgeving Rijk
Doc-Direct
ODC Noord
P-Direct
Rijksoverheid.nl
Rijkspas
Rijksportaal
TenderNed

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

[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.

uitgegaan van de eindgebruiker. Dat is diegene die in de keten baat zou moet hebben bij het gebruik van open standaarden. Dit is expliciet zo gekozen, omdat het beleid gericht is op het stimuleren van interoperabiliteit. In eerdere onderzoeken is gebleken dat beheerders van voorzieningen soms 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.

[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.

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 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).

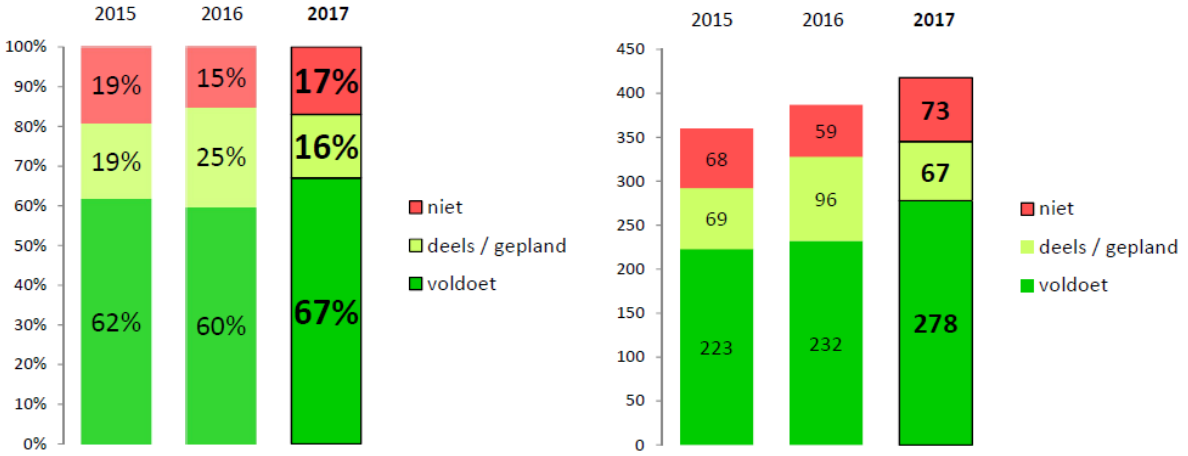
De mate waarin voorzieningen aan de standaard (als die relevant is) voldoen is hoog: voor 9 van de 24 open standaarden geldt dat tenminste 80% van de voorzieningen aan die standaard voldoet. Het gaat om de volgende negen open standaarden: TLS (25 van de 28 voorzieningen voldoet daaraan), NEN-ISO\IEC 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																
Onderwi	e-Portfolio																
	NL_LOM																
	OAI-PMH																
Overi	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

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 32 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);

[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.

- bij de ene standaard is de doelgroep en dus het potentiële gebruik veel groter dan bij de andere;
- 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 19 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;

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

- 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.

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]	Veilige, met behulp van een account geauthentiseerde toegang tot een wifi-netwerk van een (semi-) overheidsorganisatie.	Nederlandse overheden (Rijk, provincies, gemeenten en

(2 februari 2016)	Toegang tot publieke wifi-netwerken van overheden voor gasten zonder account is uitgesloten van de verplichting	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 standaardenbeleid

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.

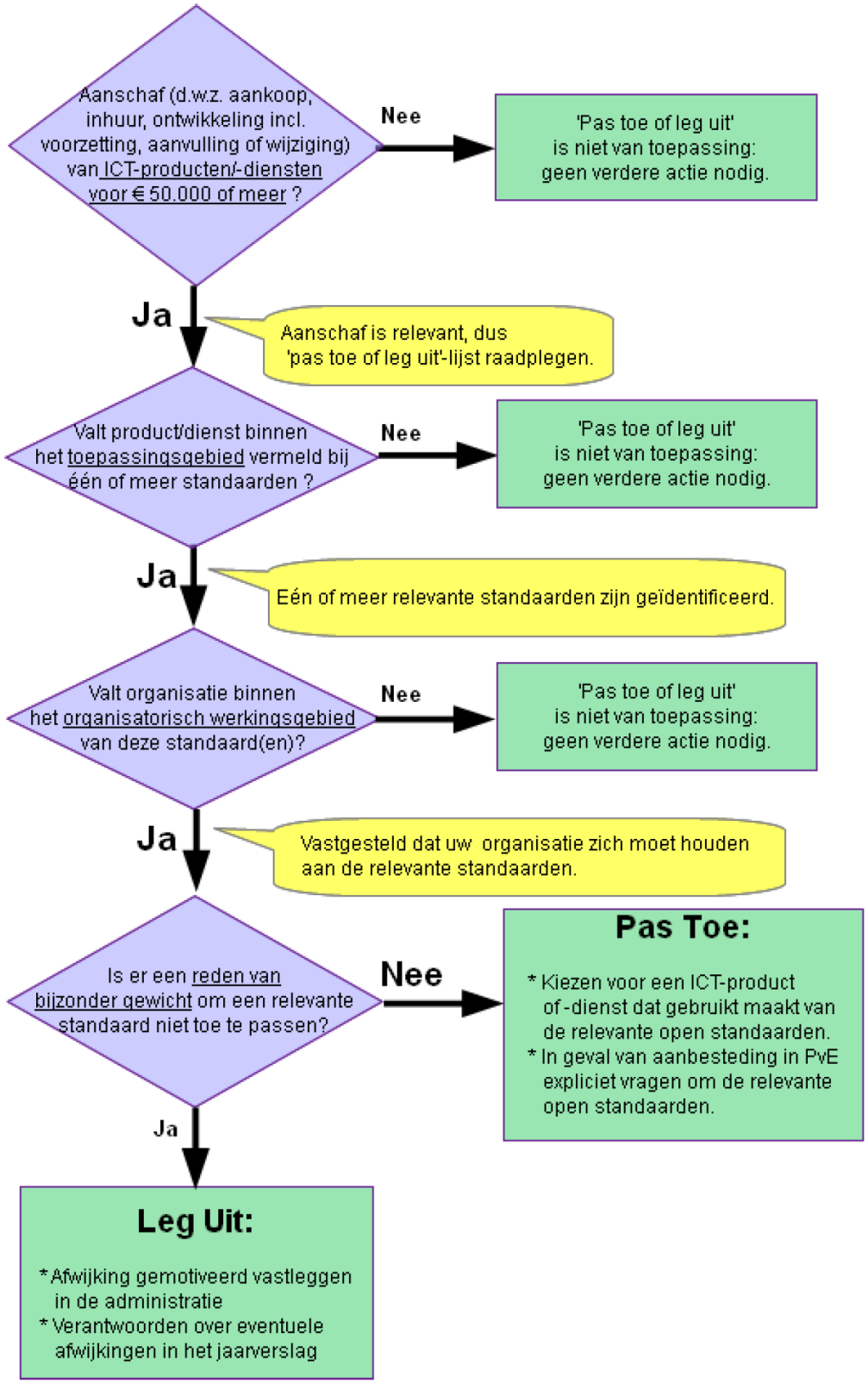
15. Ik ben het niet eens met het toepassingsgebied van een standaard. Wat kan ik doen?
    Als u denkt dat het toepassingsgebied van een standaard niet juist gedocumenteerd is, dan kan u bij het Forum Standaardisatie een verzoek tot wijziging indienen. Het Forum Standaardisatie heeft een procedure voor 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

@@ PBLQ-rapport wordt t.z.t. toevoegd in definitieve versie monitor @@


PBLQ
Monitor Open Standaarden Voorzieningen
Versie 1.0
25-10-2017

PBLQ
verbinders in de informatiesamenleving

Inhoudsopgave

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

@@ nu nog separaat, wordt t.z.t. toevoegd in definitieve versie monitor @@

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.

---

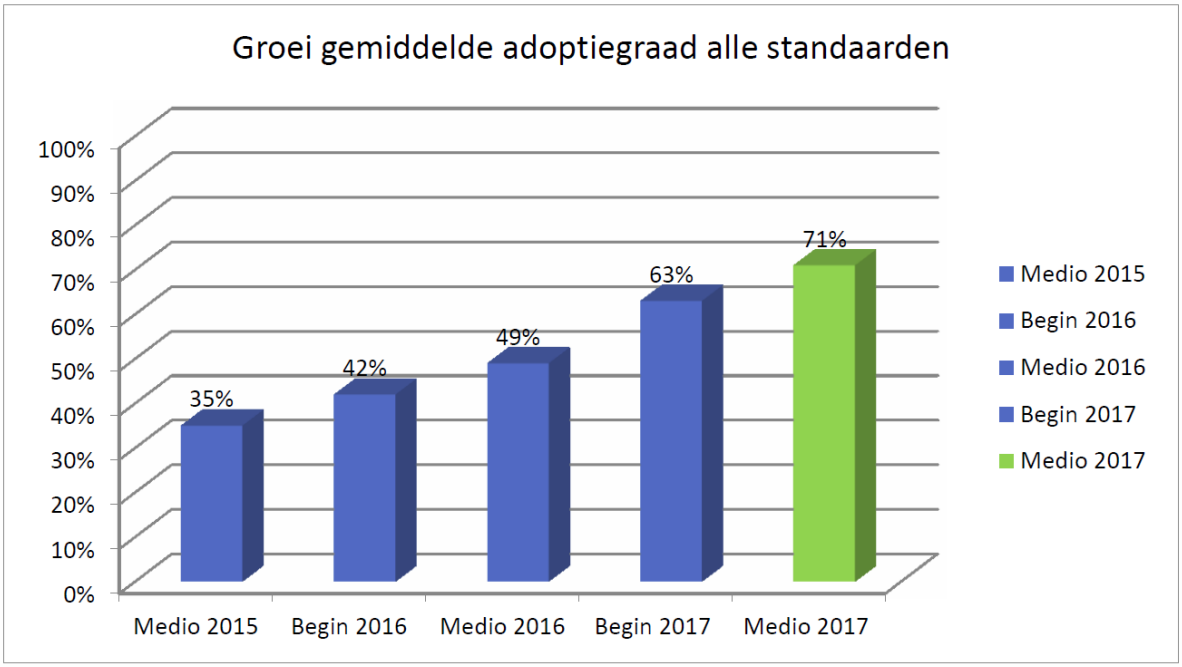
[7] DMARC is positief getoetst maar nog niet opgenomen op de pas-toe-of-leg-uit lijst. DMARC hangt echter dermate sterk samen met de toepassing van DKIM en SPF, dat het Nationaal Beraad besloot DMARC alvast onderdeel te maken van de 'versnelde adoptie set'.

[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

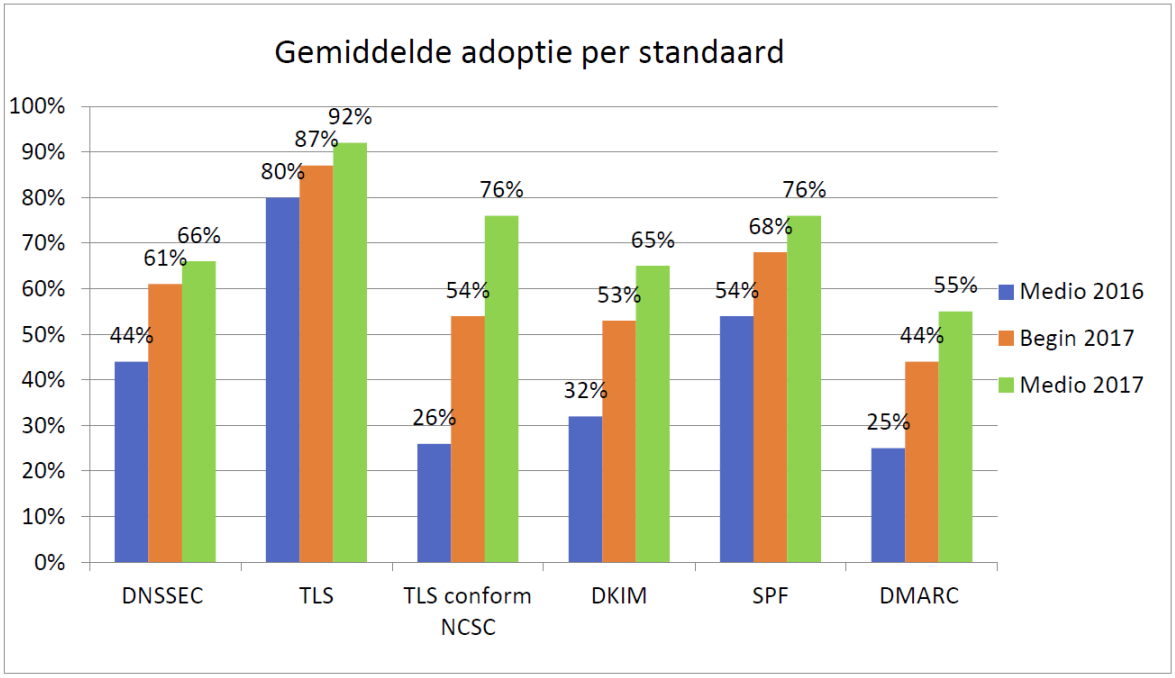
In bijlage 1 worden alle individuele scores op de vijf genoemde standaarden weergegeven. Bij deze rapportage wordt de score van de webstandaarden DNSSEC en TLS weergegeven zoals getoetst op het 'www. -domein' De mailstandaarden (DKIM,SPF&DMARC) zijn getoetst op hetzelfde domein zonder 'www.' .

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.



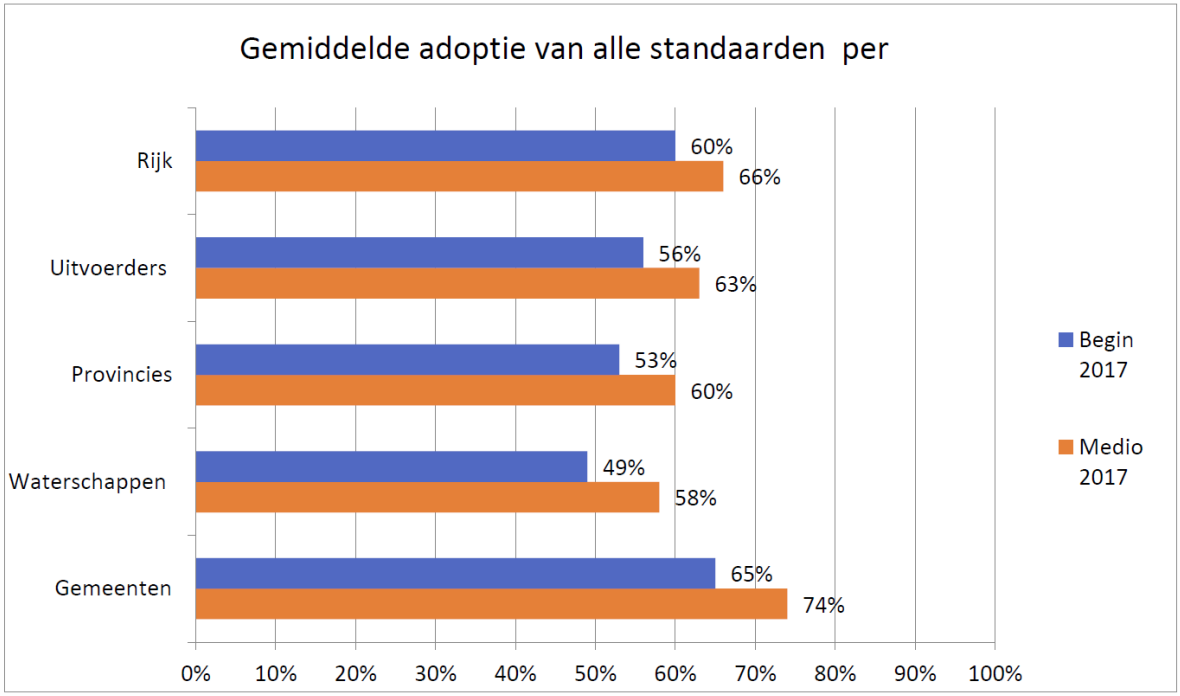
Figuur 2. Adoptiegraad van de individuele standaarden over alle getoetste domeinen.

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.

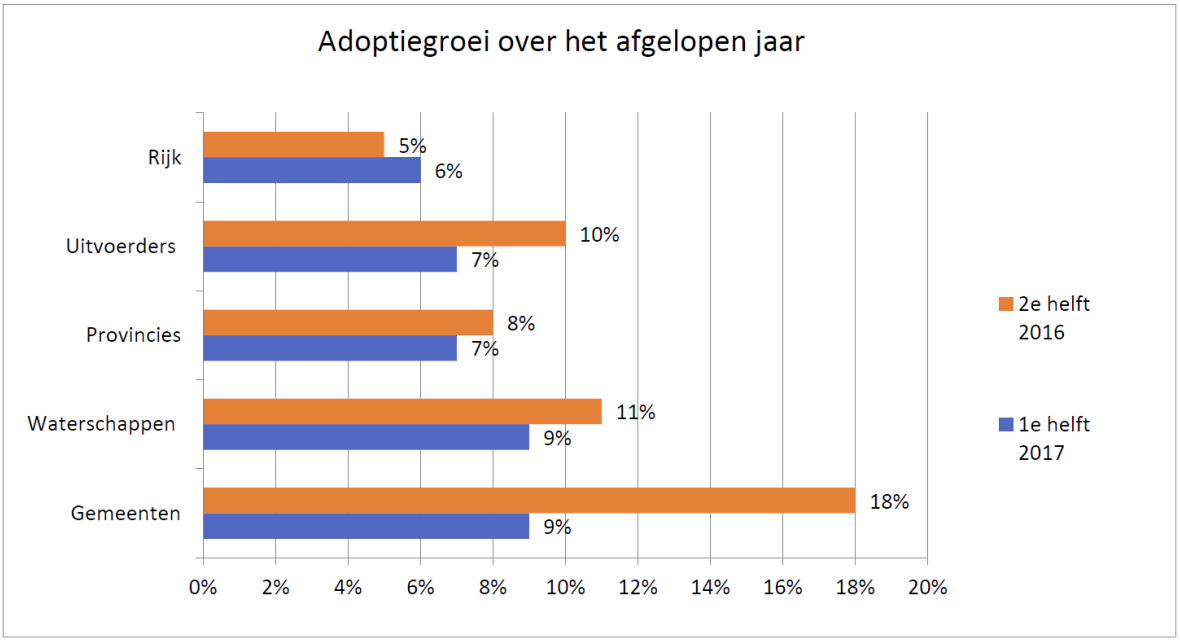


Figuur 3. De gemiddelde adoptiegraad van alle vijf de standaarden per 'overheidslaag'.

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



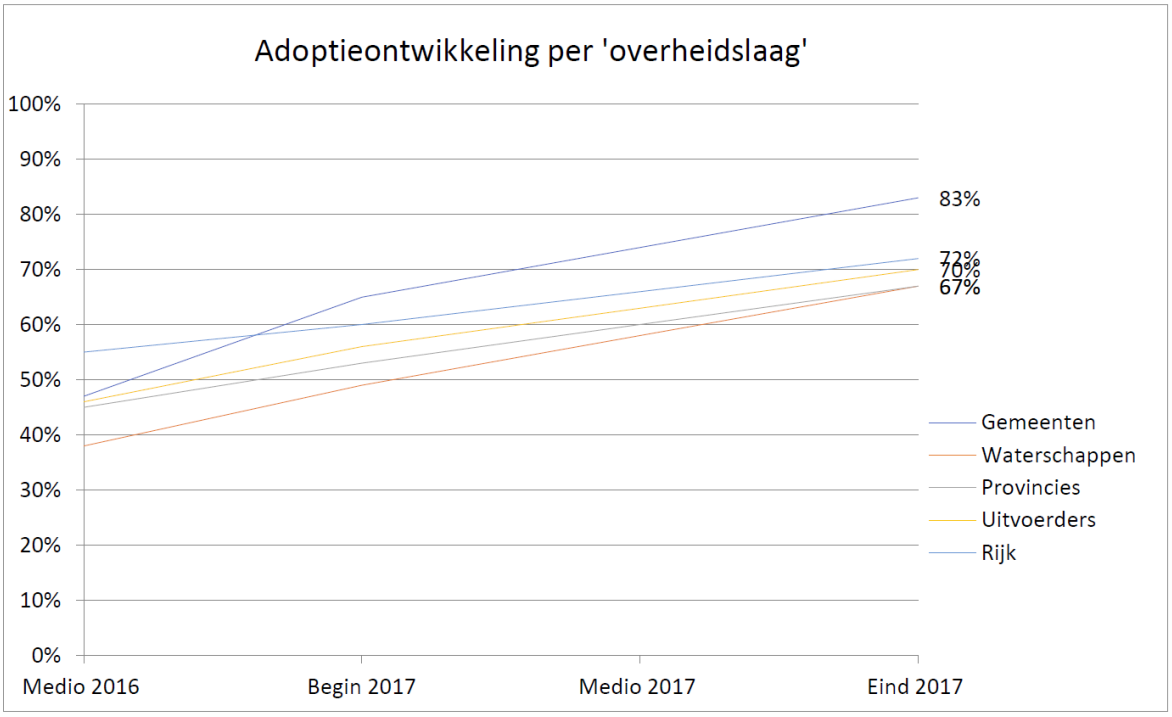
Figuur 4: De ontwikkeling van de gemiddelde adoptiegraad over het afgelopen jaar

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

Na de Forumvergadering van 13 december 2017 nader in te voegen bijlagen E en F

NB: Twee bijlagen zijn apart bijgevoegd, deze worden t.z.t. in de definitieve versie in het document geïntegreerd. Het gaat over bijlage E, het PBLQ rapport met de onderzoeksresultaten per voorziening -waarin nog een laatste aanpassing verwerkt moet worden m.b.t. AdES Baseline Profiles voor BAG – en om bijlage F, met de onderzoeksresultaten over het gebruik per standaard.