Monitor Open standaardenbeleid - rapportage 2016

De toepassing van open standaarden bij aanbestedingen (juli 2015-juni 2016) en in centrale voorzieningen (zomer 2016) en gebruiksgegevens van open standaarden (zomer 2016)

Auteur	Jaap Korpel & Joost Vreuls
Versie	1.0
Datum	15 december 2016
Omvang	128 pagina's

Inhoudsopgave

1 Managementsamenvatting

In opdracht van het Bureau Forum Standaardisatie en het ministerie van Economische Zaken voert ICTU jaarlijks de Monitor Open standaardenbeleid uit. Voor u ligt de rapportage die betrekking heeft op de periode juli 2015 t/m juni 2016 ('pas toe of leg uit' bij feitelijke aanbestedingen), respectievelijk de situatie in de zomer van 2016 (gebruiksgegevens van open standaarden en toepassing van open standaarden via generieke voorzieningen).

Open standaardenbeleid (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 en tegelijk kostenefficiënte 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. Meer informatie over de beleidscontext is te vinden in hoofdstuk 2.

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 gerechtvaardigd: 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 toetsing, door het College en Forum Standaardisatie op de lijst voor 'pas toe of leg uit' geplaatst. Op deze open standaarden (zomer 2016 waren dit er 37) is het 'pas toe of leg uit'-regime van toepassing.

Monitor Open standaardenbeleid

De Monitor Open standaardenbeleid is gebaseerd op gegevens uit een aantal bronnen:

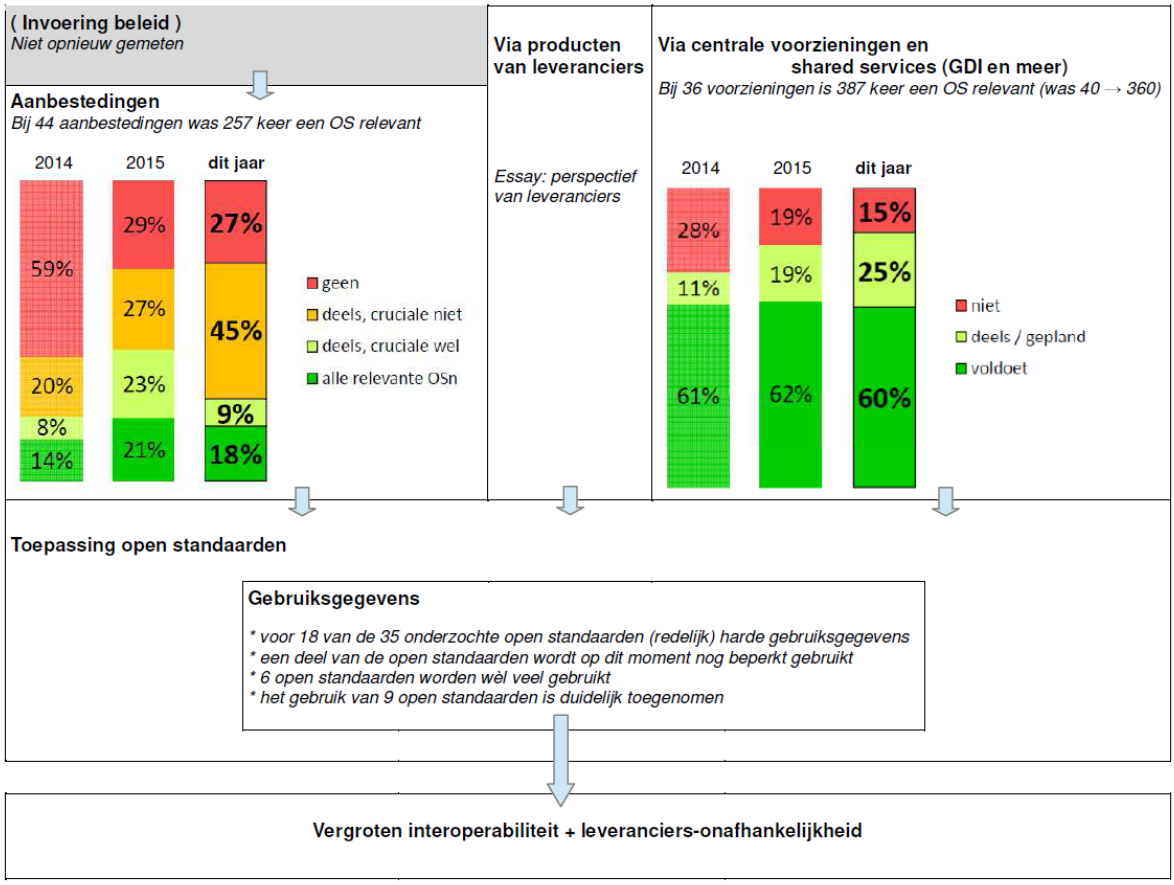
- onderzoek naar gebruiksgegevens van open standaarden, aangevuld met een korte enquête onder beheerorganisaties over hun activiteiten;
- onderzoek naar de toepassing van open standaarden bij een groot aantal voorzieningen, aangevuld met een essay over het perspectief van leveranciers;
- onderzoek van 'pas toe of leg uit' bij feitelijke aanbestedingen in 2015/2016, aangevuld met bevindingen uit enkele gesprekken met aanbestedende partijen.

Samen bieden deze bronnen een beeld van de voortgang van het open standaardenbeleid. In de onderstaande figuur (zie volgende pagina) is de samenhang tussen de deelonderzoeken weergegeven, met enkele van de voornaamste bevindingen.

Het onderzoek van feitelijke aanbestedingen liet vorig jaar een opvallende verbetering zien: bij aanbestedingen werd veel vaker gevraagd om alle relevante open standaarden (21%) of tenminste om de cruciale standaarden (23%). Samen was dat 44%, twee keer zo vaak als het jaar daarvoor (22%). Het aantal aanbestedingen waarbij helemaal niet om open standaarden gevraagd werd was bovendien sterk gedaald (van 59% tot 29%).

[1] Het open standaardenbeleid gaat er van uit, dat overheden en andere organisaties in de publieke sector uit zichzelf de 'gangbare' open standaarden toepassen. Zie de 'lijst met gangbare open standaarden' van het Forum Standaardisatie. De toepassing van deze 'gangbare' open standaarden wordt voor deze monitor niet onderzocht.

Open standaardenbeleid



Dit jaar zijn de resultaten niet verder verbeterd: in 18% van de onderzochte aanbestedingen is gevraagd om alle relevante open standaarden, en in 9% van de aanbestedingen is tenminste om de cruciale standaarden gevraagd. Samen is dat 27%, minder dan vorig jaar (maar nog wel iets meer dan het jaar dáárvoor). Vooral het percentage aanbestedingen waarbij om één of meer cruciale standaarden niet is gevraagd blijkt gestegen: van 27% vorig jaar tot 45% dit jaar. Van 'leg uit' (verantwoording van de redenen om dat bewust niet te doen) is dit jaar, net als in voorgaande jaren, niet of nauwelijks sprake geweest.

Het 'pas toe of leg uit'-principe heeft betrekking op aanbestedingen, en daarmee alleen op de uitbreiding of vernieuwing van de ICT èn alleen op de opdrachten die de betreffende organisatie zelf verstrekt. Daarnaast maken overheden op grote schaal en in toenemende mate gebruik van generieke voorzieningen (shared services, I-voorzieningen, basisregistraties etc.). Een belangrijk deel daarvan blijkt te voldoen aan de relevante open standaarden, en de mate waarin voorzieningen voldoen aan relevante open standaarden neemt bovendien toe. Van alle 387 gevallen waarbij een open standaard voor een voorziening relevant was, voldoet in 60% de voorziening daar aan (vorig jaar 62%). Het aantal gevallen waarin de voorziening deels aan de standaard voldoet of daarvoor concrete plannen heeft is verder gestegen: van 19% vorig jaar naar 25% dit jaar. Overheden voldoen op deze manier, soms mogelijk zonder het te weten, voor dat deel van hun ICT aan open standaarden.

Het resultaat van open standaardenbeleid, aanbestedingen en toepassing van generieke voorzieningen zou (uiteindelijk) terug te zien moeten zijn in de gebruiksgegevens van open standaarden. Dergelijke gegevens zijn helaas slechts in beperkte mate voorhanden. Enkele open standaarden blijken breder toegepast te worden, bij verschillende open standaarden is het gebruik nog beperkt. Bij een aantal open standaarden is wel een duidelijke groei van het gebruik te zien. Hierbij dient bedacht te worden, dat een open standaard op de lijst geplaatst wordt omdat het gebruik een

extra stimulans nodig heeft. Het is dus logisch dat het gebruik aanvankelijk (nog) beperkt is en (hopelijk) vervolgens in een aantal jaren geleidelijk toeneemt.

In het vervolg van dit hoofdstuk worden de voornaamste bevindingen per deelonderzoek kort samengevat. De positieve bevindingen hebben een groen blokje, de minder positieve oranje.

Gebruiksgegevens van een aantal open standaarden (H3)

Het uiteindelijk 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 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 31 open standaarden van de lijst bleek dat wèl mogelijk, op één 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[2] op websites van overheden te vinden zijn;
- door gebruik te maken van een openbaar register: op de site van Stichting drempelvrij.nl staat een overzicht van alle websites die voldoen aan de Webrichtlijnen;
- door gegevens op te vragen bij de betreffende beheerorganisaties: dit leverde gegevens of meer globale informatie op voor de meeste andere onderzochte open standaarden.

De gebruiksgegevens zijn verzameld in de zomer van 2016, met in grote lijnen de volgende uitkomsten.

	Over 18 van de 35 onderzochte[3] open standaarden zijn redelijk harde gebruiksgegevens gevonden. Voor de andere open standaarden moest genoegen genomen worden met meer globale informatie, en voor enkele standaarden is geen informatie beschikbaar.
	Bij verschillende beheerorganisaties of anderszins bij open standaarden betrokken organisaties bestaat geen goed zicht op 'harde' gegevens over het gebruik door overheidsinstellingen.
	Voor enkele standaarden zijn initiatieven gesignaleerd voor een vorm van monitoring (van de BIR door BZK en de IBI door provincies, en de Compliance monitor van KING).
	Zes open standaarden worden op redelijk brede schaal door overheden gebruikt: StUF (100%, binnengemeentelijk echter minder), EMN_NL (alle gemeenten), Digikoppeling (64%), Semantisch Model e-Factureren (62% bij de rijksoverheid), SPF (54%) en DNSSEC (45%, rijksoverheid 59%).
	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, Webrichtlijnen en ODF.
	Positief is de groei van het gebruik door overheden van zeven standaarden: Digikoppeling (in drie jaar van 29% naar 64%), DNSSEC (in drie jaar van 10% naar 45%), DKIM (van 22% vorig jaar naar 32% dit jaar), Semantisch model e-Factureren (van 53% naar 62%), TLS (van 67% naar 79%), SPF (van 32% naar 54%) en SAML (gestage groei, nu 28% resp. 100%). Daarnaast lijkt ook het gebruik van STOSAG en XBRL toe te nemen.
	De implementatie van IPv6 verloopt nog steeds traag. De toepassing is dit jaar licht gestegen tot 6%, bij de Rijksoverheid tot 16%.
	Bij enkele standaarden is sprake van (beginnend) beleid in de richting van gerichte sturing op de aanbodkant. StUF vormt hiervan een mooi voorbeeld, met o.a. een testplatform voor leveranciers en informatie over de compliance aan standaarden in de GEMMA Softwarecatalogus.

Halfjaarlijkse meting Internetveiligheidsstandaarden (paragraaf 3.3)

In 2015 is het Forum Standaardisatie gestart met een halfjaarlijkse evaluatie van 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.

[2] Het is niet mogelijk om daarbij onderscheid te maken tussen PDF/A-1, PDF/A-2, PDF1.7 en andere versies.
[3] Niet onderzocht zijn: SIKB0102 en WPA2 Enterprise (sinds kort op de lijst).

Het gaat om vijf internetveiligheidsstandaarden: DNSSEC (domeinnaambeveiliging), TLS (beveiligde verbinding), DKIM, SPF en DMARC[4] (alledrie anti-phishing). Voor een set van 152 domeinen wordt met behulp van Internet.nl getoetst of zij voldoen aan de vijf internetveiligheidsstandaarden. De cijfers worden bij wijze van prognose ook lineair geëxtrapoleerd tot een percentage eind 2017.

	TLS wordt het meest toegepast (75%), het aantal domeinen waarbij geconfigureerd is op de door het NCSC voorgeschreven veilige manier is lager maar is het afgelopen jaar wel gestegen van 23% naar 40%. De toepassing van DNSSEC en SPF is gegroeid tot respectievelijk 51% en 53%, de toepassing van DKIM groeide naar 39% en van DMARC naar 29%.
	Bij de eerste meting medio 2015 was de gemiddelde adoptiegraad van de vijf standaarden 35 %. Eind 2015 stond dit percentage op 42 % en medio 2016 op 49 %.
	Als dit groeipercentage wordt geëxtrapoleerd naar het einde van 2017, dan blijkt dat zonder aanvullende acties de adoptiegraad op dat moment zal blijven steken op 71% en daarmee achterblijft bij de ambitie om deze standaarden eind 2017 te hebben geïmplementeerd.
	Volgens deze extrapolatie komt de toepassing van DNSSEC, SPF en TLS eind 2017 uit op rond 80%, en TLS conform NCSC, DKIM, DMARC eindigen iets boven 50%.

Toepassing van open standaarden via generieke voorzieningen (H4)

Het toepassen van open standaarden is de verantwoordelijkheid van de afzonderlijke overheids-organisaties. Maar voor een deel van hun informatiesystemen maken overheden gebruik van generieke 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, leidt dat tot breder gebruik van open standaarden. Daarom is ook dit jaar onderzocht in hoeverre de belangrijkste voorzieningen (36 in totaal) voldoen aan de relevante open standaarden. Hiervoor zijn enerzijds 27 voorzieningen onderzocht die samen de GDI (Generieke Digitale Infrastructuur) vormen[5]. Anderzijds zijn dit jaar ook 9 (andere) voorzieningen die vorig jaar zijn onderzocht nogmaals onderzocht[6].

	Voor veel voorzieningen is een flink aantal standaarden relevant, gemiddeld bijna 11 standaarden per voorziening. Van de 37 standaarden op de lijst voor 'pas toe of leg uit' zijn er 24 relevant voor één of meer generieke voorzieningen, per standaard gemiddeld relevant voor 16 voorzieningen.
	De mate waarin voorzieningen aan de standaard (als die relevant is) voldoen is redelijk hoog: voor 9 van de 24 open standaarden geldt dat tenminste 80% van de voorzieningen aan die standaard voldoet. Een belangrijk deel van deze standaarden staat al vijf jaar of langer op de lijst. Alleen IPv4/IPv6 (13%) scoort relatief laag.
	In de meeste gevallen voldoen de onderzochte voorzieningen aan (de meeste) daarvoor relevante open standaarden: aan 60% wordt voldaan, 25% voldoet deels of dit is gepland en in 15% van de gevallen wordt op dit moment (nog) niet voldaan aan een relevante open standaard. Uitgangspunt van het open standaardenbeleid is, dat aanpassing plaatsvindt op het moment dat een voorziening ontwikkeld, vernieuwd of vervangen wordt.
	Op dit moment voldoen 11 van de 36 voorzieningen geheel of gedeeltelijk aan alle (gemiddeld 11) relevante open standaarden en/of hebben concrete plannen om daaraan op korte termijn te voldoen. Bijna allemaal (10 van de 11) zijn dit GDI-voorzieningen.
	Veel voorzieningen hebben ten opzichte van de vorige meting vooruitgang geboekt, met als positieve voorbeelden BRT, Digi-Inkoop, DigiD Machtigen en Ondernemersplein.
	Uit de gesprekken blijkt, dat het open standaardenbeleid beter bekend wordt en dat er meer aandacht komt (en meer plannen zijn) voor het voldoen aan de relevante open standaarden.
	Voor het uiteindelijk effect moeten alle schakels in de keten meewerken: naast de beheerders van de voorzieningen bijvoorbeeld ook de beheerders van het netwerk waarvan deze gebruikmaken. In een aantal gevallen laten echter op dit moment nog één of enkele partijen verstek gaan.

[4] DMARC is op dit moment nog niet op de lijst geplaatst.
[5] 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.
[6] Namelijk: ODC Noord, Digi-Inkoop, Doc-Direct, DWR, P-Direct, Rijksoverheid.nl, Rijkspas, Rijksportaal en TenderNed.

	Het kostte ook dit jaar veel moeite om de gevraagde informatie boven tafel te krijgen, de transparantie over het voldoen aan open standaarden is voor veel voorzieningen nog beperkt.
	Positieve uitzondering daarop is Logius, beheerder van een groot aantal voorzieningen: jaarlijks publiceren zij hierover een helder overzicht. Daarnaast bleek een deel van de beheerders dit jaar sneller in staat de gevraagde informatie te leveren, de ervaring is (wederzijds) toegenomen.

Enkele generieke voorzieningen onderscheiden zich in positieve zin:

- Afsprakenstelsel Elektronische Toegangdiensten voldoet aan alle 10 relevante standaarden.
- Samenwerkende Catalogi voldoet aan alle 2 relevante standaarden.
- Rijksoverheid.nl voldoet aan 12 van de 15 relevante standaarden en voldoet aan de andere 3 standaarden deels.
- DigiD Machtigen voldoet aan 10 van de 12 relevante standaarden en voldoet aan de andere 2 standaarden deels.
- PKI Overheid voldoet aan 9 van de 10 relevante standaarden en aan de tiende standaard deels.
- Basisregistraties BRI (inkomen) en BRT (topografie) voldoen aan 6 van de 7 relevante standaarden.
- Digipoort PI voldoet aan 8 van de 10 relevante standaarden.

Open standaarden bij aanbestedingen (H6)

Het 'pas toe of leg uit'-principe is een centraal beleidsinstrument binnen het open standaarden-beleid: overheden moeten bij ICT-aanbestedingen van € 50.000 of meer de relevante open standaarden van de lijst toepassen, of verantwoording afleggen in hun jaarverslag. Dat blijkt in de praktijk minder eenvoudig dan het op het eerste gezicht lijkt. Veel (vooral kleine) overheden doen maar één keer per jaar of zelfs nog minder vaak een aanbesteding waarvoor één of meer open standaarden relevant zijn. En òf een open standaard voor die aanbesteding relevant is spreekt niet vanzelf: dat hangt (per standaard) af van het toepassingsgebied en organisatorisch werkgebied. Die informatie is voor elk van de standaarden van de lijst voor 'pas toe of leg uit' te vinden op de website van het Bureau Standaardisatie.

'Pas toe' bij feitelijke aanbestedingen

Voor de monitor is, net als vorig jaar, een groot aantal aanbestedingen onderzocht. Dit keer zijn 21 aanbestedingen van de rijksoverheid (incl. uitvoeringsorganisaties) en 23 aanbestedingen van mede-overheden onderzocht, in totaal 44 aanbestedingen uit het 3e en 4e kwartaal van 2015 en het 1e en 2e kwartaal van 2016.

	Bij 8 aanbestedingen (18%) is om alle relevante standaarden gevraagd, dit is een lichte daling ten opzichte van vorig jaar (21%), zowel bij het Rijk als bij decentrale overheden. Het gaat hierbij om aanbestedingen van het Ministerie van V&J, de Belastingdienst, de Politie, de Veiligheidsregio Utrecht en de gemeenten Almere, Hollands Kroon en Vlissingen.
	Naast de 8 aanbestedingen (18%) waarbij om alle relevante standaarden is gevraagd, werd bij 24 aanbestedingen (55%) om een deel van de relevante open standaarden gevraagd. Dat is nog iets meer dan vorig jaar (50%).
	De keerzijde hiervan is uiteraard, dat nog altijd bij 27% van alle aanbestedingen om geen enkele van de relevante open standaarden wordt gevraagd, dat is iets minder en dus iets beter dan vorig jaar (29%). Er is hierin nauwelijks verschil tussen het Rijk en de decentrale overheden. Daarnaast werd van de 24 eerder genoemde aanbestedingen waarbij om *een deel van* de open standaarden is gevraagd bij 20 aanbestedingen (45% van alle aanbestedingen) niet om cruciale open standaarden gevraagd. Dat betekent dat in totaal bij 72% van de aanbestedingen *niet om cruciale* open standaarden is gevraagd, een slechtere score dan vorig jaar (56%).
	Bij de in totaal 44 aanbestedingen was in totaal 257 keer een open standaard relevant. Sommige standaarden (vooral NEN-ISO/IEC 27001 en 27002, PDF, ODF en TLS, en daarnaast SAML, IPv6 en Webrichtlijnen) 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 27002, PDF/A-1, PDF 1.7, PDF/A-2 en StUF).
	Wanneer we niet kijken naar het aantal aanbestedingen (44) maar naar het aantal keer dat bij deze aanbestedingen een open standaard relevant was (257, dus per aanbesteding was gemiddeld 5,8 keer een open standaard relevant), dan is de verbetering van vorig jaar gehandhaafd. In 113 gevallen (44%) werd om de relevante open standaard gevraagd (vorig jaar: 43%).
	Enkele standaarden worden relatief weinig gevraagd, met name SAML, IPv6 en ODF. Deze drie zijn frequent als relevant aangemerkt, maar in slechts ongeveer 10 à 30% van die gevallen werd om de standaard gevraagd.
	Bij een aantal standaarden is de mate waarin daarom werd gevraagd (als die standaard relevant was voor een aanbesteding) dit jaar toegenomen, bij ongeveer evenveel standaarden is de mate waarin daarom werd gevraagd dit jaar afgenomen.

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

- Veiligheidsregio Utrecht (werkprocesapplicatie met een zaakgerichte, een objectgerichte en een DMS-functionaliteit). De relevante standaarden (PDF, ODF, StUF, CMIS, Webrichtlijnen, ISO 27001/02, SAML en Digikoppeling en ook PNG en JPEG) worden alle uitgevraagd.
- Belastingdienst (mid-volume scan-oplossingen en aanverwante dienstverlening). Het bestek bevat een uitgebreide verwijzing naar de BIR (ISO 27001/02 is als relevant aangemerkt) en er is expliciet opgenomen dat gescand moet kunnen worden in onder andere PDF-formaat.
- Gemeente Breda (standaardapplicatie voor bijhouding van de BAG). Alle standaarden die relevant en cruciaal worden geacht (StUF, PDF, ODF, IPv4/v6, GEO-standaarden en TLS) worden in de bevraging door de opdrachtgever meegenomen. Alleen SAML - door de beoordelaars ook relevant geacht, zij het niet cruciaal - wordt niet uitgevraagd.
- Ministerie van V&J (standaardprogrammatuur en daaraan gerelateerde dienstverlening). Alle relevante (en cruciale) standaarden zijn gevraagd: PDF, ODF, ISO27001/02, JPEG, PNG, SMeF, TLS en SETU. Daarnaast wordt ook expliciet het open standaardenbeleid genoemd.

'Leg uit' in jaarverslagen

'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 2015 (over 2016 kan door overheden pas verantwoording afgelegd worden in het jaarverslag dat in het voorjaar van 2017 verschijnt).

Voor 15 van de aanbestedingen in het 3e en 4e kwartaal van 2014 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 lijst voor 'pas toe of leg uit' genoemd.
	In het jaarverslag over 2015 hebben 4 van de 11 ministeries een alinea over 'pas toe of leg uit' opgenomen (vorig jaar: 6).
	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.

De drie deel-onderzoeken naast elkaar

Elk van de drie deel-onderzoeken brengt een ander aspect van het proces van adoptie van open standaarden in beeld. Dergelijke gegevens kunnen niet zomaar naast elkaar gelegd worden.

Tegelijkertijd komen in alle drie de deel-onderzoeken dezelfde open standaarden van de lijst voor ‘pas toe of leg uit’ voor. Wat levert het gecombineerde beeld uit deze drie bronnen op ? In de onderstaande tabel is dat in beeld gebracht.

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

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

Voor een aantal standaarden is het overall beeld positief: NEN-ISO\IEC 27001:2005nl en 27002:2007nl, Digikoppeling, Semantisch Model e-Factureren, PDF/A-1, PDF/A-2, PDF 1.7, TLS en StUF. En voor zeven standaarden is het beeld hoopvol: SAML, DNSSEC, DKIM, ODF 1.2, CMIS, de Geo-standaarden en SPF. De andere standaarden staan er op dit moment nog minder goed voor (oranje), of daarover is onvoldoende informatie (17x vraagteken).

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

≥ 75 % past toe 25-75 % past toe < 25 % past toe	Gebruiks-gegevens	Generieke voorzieningen	Onderzoek aanbestedingen	Overall beeld	
indicator: *(): minder dan 5 cases*		# voorzieningen dat voldoet + deels + gepland in % van # waarvoor de OS relevant is	# aanbestedingen gevraagd in % van # aanbestedingen waarbij OS relevant is		
bron:	*hoofdstuk 3*	*o.b.v. tabel 15ab*	*tabel 18*		
Sinds 2008 op de lijst:					
NEN-ISO\IEC 27001 + 27002	hoog ? (Rijk, gem.n)	97 %	60 % / 48 %	●●	
PDF/A-1	hoog ? (Google)	65 %	65 %	●●	
StUF	hoog (gem.n)	78 %	73 %	●●	
Sinds 2009 op de lijst:					
SETU	onbekend	(100 %)	(33 %)		[?]
SAML	28 / 100 % + stijgt	80 %	29 %	●	
PDF 1.7	hoog ? (Google)	65 %	65 %	●●	
Sinds 2010 op de lijst:					
XBRL en Dimensions	redelijk + stijgt	(100 %)	(0 %)		[?]
E−portfolio	*[geen gegevens]*		(0 %)		[?]
Aquo Standaard	*[geen gegevens]*				[?]
IPv6 en IPv4	6 à 16 % + stijgt	13 %	8 %	●●	
OAI−PMH	*[geen gegevens]*		(0 %)		[?]
Sinds 2011 op de lijst:					
NL LOM	*[geen gegevens]*				[?]
Webrichtlijnen	2 à 3 % + daalt	42 %	56 %	●	
OWMS	onbekend	55 %			[?]
IFC	onbekend				[?]
STOSAG	redelijk + stijgt				[?]
Sinds 2012 op de lijst:					
DNSSEC	45 à 59 % + stijgt	48 %	(0 %)	●	
DKIM	32 % + stijgt	41 %	(50 %)	●	
ODF 1.2	beperkt ? (Google)	67 %	30 %	●	
PDF/A-2	hoog ? (Google)	65 %	65 %	●●	
Sinds 2013 op de lijst:					
Digikoppeling 2.0	64 à 40 % + stijgt	59 %	33 %	●●	
Sem. model e-Factureren	62 % (Rijk) + stijgt	(100 %)	(50 %)	●●	
BWB	onbekend	(100 %)			[?]
ECLI	onbekend				[?]
EMN_NL	alle gemeenten				[?]
JCDR	onbekend		(0 %)		[?]
Sinds 2014 op de lijst:					
WDO Datamodel	onbekend				[?]
TLS	26 % (NCSC) + stijgt	69 %	54 %	●●	
CMIS	onduidelijk	40 %	45 %	●	
Geo−standaarden	onduidelijk	100 %	(33 %)	●	
SIKB 0101 v11	onbekend				[?]
VISI 1.4	onbekend				[?]
Sinds 2015 op de lijst:					
SKOS	onbekend	31 %			[?]
SPF	54 % + stijgt	32 %		●	

2 Inleiding en beleidscontext

2.1 Beleid open standaarden

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

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 overheidsorganisatie 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. 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.

Eind 2011 kondigde het kabinet 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.

Vorig jaar nam de Tweede Kamer 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 heeft in mei 2015 de bestaande overheidsbrede verplichting voor het toepassen van open standaarden herbevestigd en verlengd tot eind 2017.

Dit nam de Tweede Kamer bovendien de motie Oosenbrug (11 oktober 2016) aan, waarin de regering onder andere gevraagd werd om *"(…) het gebruik van open standaarden te verplichten bij wet"*.

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[7] van kracht:

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

Deze verplichting geldt voor de aanbesteding, inkoop of ontwikkeling van ICT-producten en -diensten ter waarde van € 50.000 en meer. Niet alleen voor nieuwe producten of diensten, maar ook als het gaat om aanpassing van bestaande producten of diensten. In Bijlage 1 is een schema opgenomen waarin het 'pas toe of leg uit'-principe in het kort wordt toegelicht.

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

[7] *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).

het organisatorische werkingsgebied van de betreffende standaard.[8] 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[9] 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.*

2.2 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.

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.

[8] Het functionele toepassingsgebied en het organisatorische werkingsgebied van elke standaard zijn vermeld in de lijst voor 'pas toe of leg uit'.
[9] De Rijksbegrotingsvoorschriften zijn opgesteld door het Ministerie van Financiën en bevatten de voorschriften voor de verantwoording over de begroting, de uitvoering van de begroting en de begroting.

2.3 Bronnen van de gepresenteerde gegevens

In deze rapportage worden gegevens gepresenteerd die afkomstig zijn uit een aantal bronnen:

- onderzoek gebruiksgegevens van een aantal open standaarden,
- onderzoek toepassing open standaarden bij rijksbrede voorzieningen en shared services,
- onderzoek van feitelijke aanbestedingen in 2015/2016.

Onderzoek gebruiksgegevens van een aantal open standaarden

Om na te gaan in welke mate open standaarden daadwerkelijk worden toegepast zijn gebruiks-gegevens verzameld voor 34 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. Deels door gebruik te maken van een openbaar register (Waarmerk drempelvrij.nl). En deels door gebruiks- of aansluit-gegevens op te vragen bij de betreffende beheerorganisaties.

Onderzoek open standaarden bij rijksbrede voorzieningen en shared services

Dit jaar is een onderzoek uitgevoerd naar de mate waarin 36 voorzieningen voldoen aan de open standaarden die daarvoor relevant zijn: 27 voorzieningen van de GDI (Generieke Digitale Infrastructuur) en 9 andere voorzieningen die in de voorgaande jaren ook onderzocht zijn. Hiervoor zijn de betreffende beheerorganisaties benaderd.

Onderzoek feitelijke aanbestedingen in 2015/2016

Dit jaar zijn aanbestedingen onderzocht van de rijksoverheid (en uitvoerings-organisaties) en van mede-overheden uit de periode juli 2015-juni 2016. 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.

3 Gebruiksgegevens van open standaarden

3.1 Inleiding

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

Het 'pas toe of leg uit'-regime is gericht op aanbestedingen, en daarmee op het toepassen van open standaarden bij afzonderlijke toevoegingen aan en vernieuwing van het ICT-systeem van overheden. Gegevens over het feitelijk gebruik geven een beeld voor het gehele ICT-systeem. Bovendien gaat het bij het 'pas toe of leg uit'-regime om het vragen om open standaarden, en wordt niet gemeten in hoeverre het gevraagde ook (volledig) is geleverd. Tenslotte kunnen overheden open standaarden ook toepassen, mogelijk zelfs zonder zich daarvan bewust te zijn, doordat zij voorzieningen of producten gebruiken waarin deze open standaarden toegepast zijn.

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

In augustus 2016 stonden er 37 (al dan niet samengestelde) standaarden op de lijst voor 'pas toe of leg uit'. In vergelijking met de lijst van een jaar eerder is één standaard van de lijst afgevoerd (NTA 9040)[10] en zijn er 2 nieuwe aan toegevoegd: SIKB0102 en WPA2 Enterprise. Deze twee nieuwe standaarden zijn dit jaar nog niet meegenomen in het deelonderzoek 'gebruiksgegevens' omdat het besluit tot plaatsing op de lijst dateert van februari van dit jaar. Bij een eventuele volgende monitor worden deze standaarden wel meegenomen[11]. Zodoende hebben wij voor 35 standaarden van de huidige lijst het gebruik onderzocht.

Slechts bij een beperkt aantal standaarden is een met relevante cijfers onderbouwd beeld verkregen van het gebruik van de standaard. Daar waar dergelijke gegevens niet voorhanden waren hebben we ons noodgedwongen gebaseerd op meer kwalitatief gerichte uitspraken of op inschattingen die door onze respondenten zijn gemaakt. In paragraaf 3.4 tot en met 3.34 wordt een beeld geschetst van de gebruiksgegevens die wij hebben gevonden.

3.2 Gebruiksgegevens per standaard

De open standaarden van de lijst voor 'pas toe of leg uit' zijn zeer verschillend, en de mate waarin het feitelijk gebruik van de standaard kan worden vastgesteld loopt sterk uiteen. Langs vier wegen hebben wij in het kader van dit deelonderzoek informatie verzameld: door gebruik te maken van een webtool, van een openbaar register, van een Google-zoekopdracht en door benadering van de betreffende beheerorganisatie.

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

Tot vorig jaar is voor drie open standaarden gebruik gemaakt van een webtool (DKIM, DNSSEC en IPv4/v6). Zo doende kon voor deze drie standaarden op zijn minst een goede indicatie worden

[10] JPEG en PNG staan niet meer als afzonderlijke standaard op de lijst maar zijn ondergebracht bij ODF. In die zin zijn ook deze standaarden vergeleken met vorig jaar afgevoerd van de lijst.
[11] Ook de standaard STARTTLS & DANE waarover het besluit tot plaatsing heel recent is genomen (september 2016), zal volgend jaar voor het eerst in de monitor worden meegenomen.

verkregen van het gebruik. Sinds 2015 biedt het Platform Internet Standaarden[12] de mogelijkheid om via de website internet.nl domeinen te toetsten op het gebruik van de internet- en beveiligings-standaarden die op de 'pas toe of leg uit' lijst van Forum Standaardisatie staan[13]. In datzelfde jaar is Forum Standaardisatie gestart met een halfjaarlijkse evaluatie van overheidsdomeinen op het voldoen aan deze standaarden. Vorig jaar is daarom - op verzoek van het Forum Standaardisatie - overgestapt op deze nieuwe tool als bron om het gebruik van internet- en beveiligingsstandaarden in kaart te brengen. Deze tool is ook geschikt voor SPF en TLS[14]. De overstap leidde met name in de monitor van vorig jaar eenmalig tot complicaties bij het vergelijken van gegevens in de tijd door een andere manier van testen. Toch is besloten om de overstap te ondernemen, in de veronderstelling dat internet.nl een betrouwbare en breed (in de zin van: op meerdere standaarden van toepassing) inzetbare mogelijkheid tot meten biedt.

Voor deze monitor is gebruik gemaakt van data uit de halfjaarlijkse Meting Internetveiligheids-standaarden van Forum Standaardisatie. Daarin is de categorie Rijk gedefinieerd als: de domeinen die horen bij de deelnemers van het Nationaal Beraad[15], de domeinen behorende bij de voorzieningen van de Generieke Digitale Infrastructuur, de 25 best bezochte domeinen van Rijksoverheden (en uitvoerders), die van de Manifestpartijen èn die van de partijen behorend tot Klein LEF.

Openbaar register: Webrichtlijnen
Voor één van de open standaarden is een openbaar gebruikersregister beschikbaar: webrichtlijnen.

Voor die standaard is er een officieel waarmerk dat verleend wordt door een geaccrediteerde inspectie-instelling. Op de website van Stichting drempelvrij.nl staat het overzicht van alle websites die bewezen-voldoen aan de Webrichtlijnen, dan wel aan de lagere niveaus van toegankelijkheid.

Google-zoekopdracht: ODF, PDF/A-1, PDF/A-2 en PDF1.7
Voor de vier open documentstandaarden (ODF, PDF/A-1, PDF/A-2 en PDF1.7) is - tot op zekere hoogte - een test mogelijk, namelijk door na te gaan hoeveel ODF- en PDF-documenten op websites van overheden te vinden zijn, in vergelijking met het aantal .doc-bestanden. Voor deze meting is net als bij de vorige metingen volstaan met een selectie van acht websites: van de rijksoverheid (rijksoverheid.nl), van drie van de vier G4-gemeenten, van twee provincies en van het Forum Standaardisatie en ICTU.

Informatie van beheer-organisatie: 21 andere standaarden
Voor de andere open standaarden die in het onderzoek zijn meegenomen hebben wij de beheer-organisaties benaderd of partijen die anderszins zijn betrokken. Van een aantal van deze organisaties is – in uiteenlopende mate van concreetheid – informatie ontvangen die gebruikt kon worden voor dit onderzoek.

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

In de paragrafen 3.4 tot en met 3.32 worden de gebruiksgegevens van de open standaarden (in alfabetische volgorde) gepresenteerd. Elk van deze paragrafen is ter verificatie voorgelegd, en op basis van een eventuele reactie heeft dat geleid tot enkele aanpassingen.

Maar eerst presenteren wij in paragraaf 3.3 de voornaamste bevindingen uit de halfjaarlijkse Meting Informatieveiligheidsstandaarden van het Forum Standaardisatie.

[12] Platform Internet Standaarden is een gezamenlijk initiatief van Forum Standaardisatie, het Ministerie van Economische zaken en de Nederlandse internetgemeenschap. Zie https://internet.nl/about/
[13] Uitgezonderd de Webrichtlijnen en NEN-ISO\IEC 27001 en 27002.
[14] Ook voor DMARC. Deze standaard is weliswaar al positief getoetst maar is nog niet opgenomen op de pas-toe-of-leg-uit lijst en daarom nog niet meegenomen in deze rapportage.
[15] VNG, IPO en de Unie van Waterschappen nemen ook deel aan dit Nationaal Beraad. Bij het berekenen van de scores voor 'Rijk' in de eerder genoemde metingen van het Forum Standaardisatie zijn de websites www.vng.nl, www.ipo.nl en www.uwv.nl meegenomen. Deze drie websites zijn eveneens meegenomen bij het berekenen van de afzonderlijke scores voor de andere overheidssectoren. In die zin is derhalve sprake van een beperkte dubbeling.

3.3 Meting Informatieveiligheidsstandaarden Forum Standaardisatie

Sinds 2015 biedt het Platform Internet Standaarden[16] de mogelijkheid om via de website internet.nl domeinen te toetsten op het gebruik van de internet- en beveiligingsstandaarden die op de 'pas toe of leg uit' lijst van Forum Standaardisatie staan[17]. In datzelfde jaar is Forum Standaardisatie gestart met een halfjaarlijkse evaluatie van overheidsdomeinen op het voldoen aan deze standaarden.

Aanvullende adoptieafspraken voor de internet en beveiligingsstandaarden

De evaluatierapportages hebben ertoe geleid dat het Nationaal Beraad eind 2015 de ambitie uitsprak deze standaarden versneld te willen adopteren. Dit betekent concreet dat voor deze standaarden niet het tempo van pas-toe-of-leg-uit wordt gevolgd – wachten op een volgend investeringmoment en dan de strandaarden implementeren – maar dat actief wordt ingezet op implementatie van de standaarden op de korte termijn. Onderdeel van deze afspraak is dat Forum Standaardisatie de voortgang van de adoptie meet en inzichtelijk maakt. Daarom wordt vanaf dit jaar de halfjaarlijkse voortgangsrapportage onderdeel van de Monitor Open standaardenbeleid. Daarnaast zal het Forum Standaardisatie de resultaten vanaf december via de website beschikbaar maken[18].

Welke standaarden en welke domeinen ?

Het Nationaal Beraad heeft bovengenoemde afspraken gemaakt met betrekking tot de volgende standaarden[19]:

- DNSSEC: domeinnaambeveiliging
- TLS[20]: beveiligde verbinding
- DKIM: anti-phishing
- SPF: anti-phishing
- DMARC[21]: anti-phishing (rapportages)

De volgende groepen met domeinen zijn getoetst (in totaal 152 unieke domeinen):

- domeinen die horen bij de deelnemers van het Nationaal Beraad
- 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 (398 domeinen)
    - provincies en Waterschappen
    - partijen die behoren tot Klein LEF

[16] Platform Internet Standaarden is een gezamenlijk initiatief van Forum Standaardisatie, het Ministerie van Economische zaken en de Nederlandse internetgemeenschap (zie https://internet.nl/about).
[17] Met uitzondering van de Webrichtlijnen en NEN-ISO/IEC 27001 en 27002.
[18] Zie https://www.forumstandaardisatie.nl/thema/internet-en-beveiliging
[19] Zie: https://www.forumstandaardisatie.nl/lijst-open-standaarden/in_lijst/verplicht-pas-toe-leg-uit
[20] Voor TLS geldt dat het Nationaal Beraad de ambitie uitsprak deze 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.
[21] 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'.

Tabel 1: Adoptie internetveiligheidsstandaarden bij halfjaarlijkse metingen Forum Standaardisatie

	Medio 2015 *(Nulmeting)*	Eind 2015 *(Eenmeting)*	**Medio 2016** *(Meest recente meting)*
[aantal domeinen Nationaal Beraad]	*[140]*	*[140]*	*[152]*
DKIM	28 %	35 %	**39 %**
DMARC	11 %	22 %	**29 %**
DNSSEC	28 %	33 %	**51 %**
SPF	35 %	46 %	**53 %**
TLS	73 %	76 %	**75 %**
Waarvan conform NCSC	23 %	40 %	**40 %**

TLS wordt van de vijf standaarden het al sinds 2015 meest toegepast (medio 2016: 75%), het aantal domeinen waarbij geconfigureerd is op de door het NCSC voorgeschreven veilige manier is lager maar is het afgelopen jaar wel gestegen van 23% naar 40%. De toepassing van DNSSEC en SPF is gegroeid: DNSSEC van 28% tot 51% en SPF van 35% tot 53%. De toepassing van DKIM groeide iets minder snel: van 28% tot 39%. De toepassing van DMARC (nog niet op de lijst voor 'pas toe of leg uit') groeide van 11% naar 29%.

Bij de eerste meting medio 2015 was de gemiddelde adoptiegraad van de 5 standaarden op de toen getoetste set van grofweg 150 Nationaal Beraad domeinen 34,8 %. Aan het einde van het jaar stond dit percentage op 42,2 % en medio 2016 op 49,4 % . Dit betekent dat ondanks de uitgesproken ambitie van het Nationaal Beraad de groei het afgelopen halve jaar iets is afgenomen (7,4% naar 7,2%).

Extrapolatie van de adoptiegraad naar eind 2017

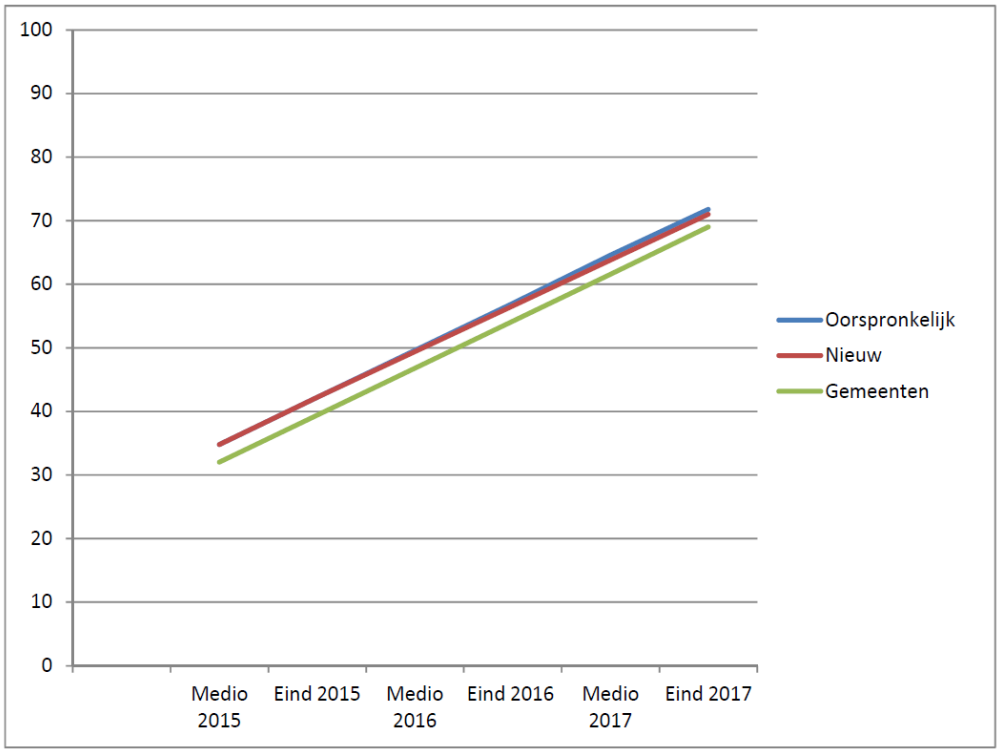
Als dit groeipercentage wordt geëxtrapoleerd naar het einde van 2017 (einde mandaatperiode van Forum Standaardisatie), dan blijkt dat zonder aanvullende acties, de adoptiegraad op dat moment zal blijven steken op 71% en daarmee achterblijft op het afgesproken streefbeeld om de standaarden eind 2017 – daar waar van toepassing – te hebben geïmplementeerd.

Daarbij valt op dat de groei bij gemeenten bijna praktisch hetzelfde is (7% per half jaar) t.o.v. de domeinen van de overige partijen in het Nationaal Beraad. Door de iets lagere adoptiegraad bij de eerste meting (32%) zal de adoptie bij gemeenten eind 2017 naar verwachting uitkomen op 68%.

In onderstaande figuur is dat weergegeven:

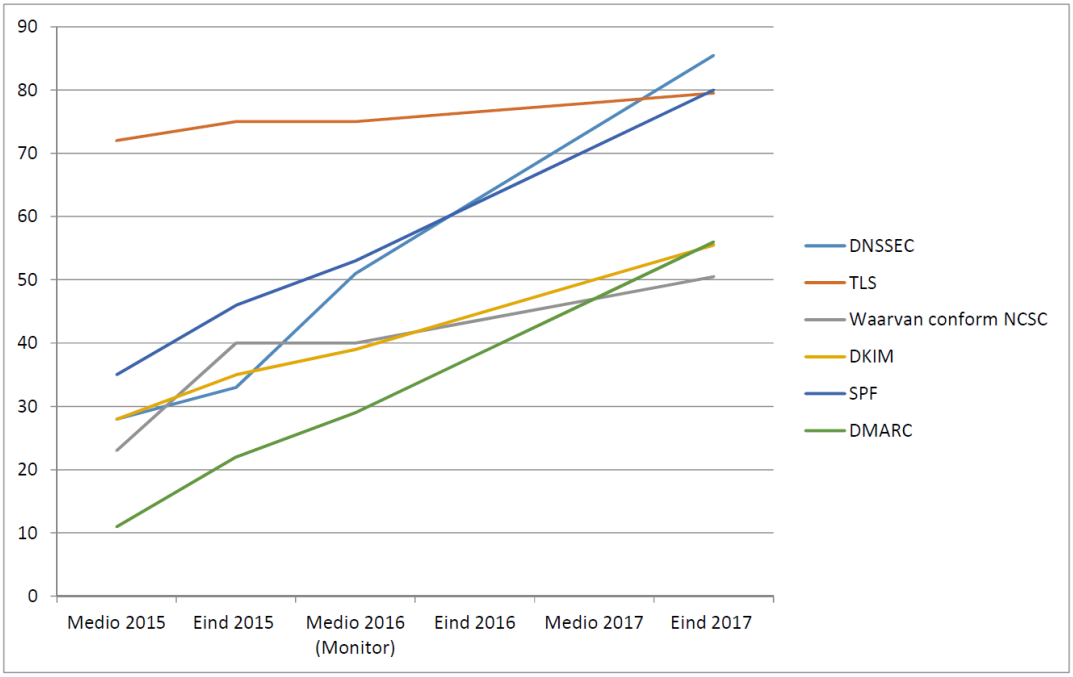
- Oorspronkelijk: verwachte groei adoptiegraad tot eind 2017 op basis van groei 2e helft 2015
- Nieuw: verwachte groei adoptiegraad tot eind 2017 op basis van groei 1e helft 2016
- Gemeenten: verwachte groei adoptiegraad op basis van groei afgelopen jaar.

Figuur 2: Gemiddeld adoptieniveau internetveiligheidsstandaarden: extrapolatie groei tot eind 2017



Per standaard ziet de extrapolatie van de groei naar eind 2017 er als volgt uit:

Figuur 3: Gemiddelde groei per standaard geëxtrapoleerd naar eind 2017 (zonder gemeenten)



Volgens deze extrapolatie komt de toepassing van DNSSEC, SPF en TLS eind 2017 uit op rond 80%, en TLS conform NCSC, DKIM, DMARC eindigen iets boven 50%.

De volledige rapportage aan het Nationaal Beraad Digitale Overheid is als Bijlage C bijgevoegd.

3.4 BWB, ECLI en JCDR (Juriconnect): juridische standaarden

De Juriconnect-**BWB**-standaard (versie 1.3.1) biedt een eenduidige manier van verwijzen naar (onderdelen van) wet- en regelgeving waarmee de interoperabiliteit van juridische documenten en systemen die veel verwijzingen kennen naar wet- en regelgeving wordt bevorderd.

Met de **ECLI**-standaard 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 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.

Deze drie juridische standaarden staan sinds 2013 op de 'pas toe of leg uit'-lijst.

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

Bron: KOOP (Kennis- en Exploitatiecentrum Officiële Overheidspublicaties)

Bij de servicedesk van het KOOP (Kennis- en Exploitatiecentrum Officiële Overheidspublicaties) is in de zomer van 2016 wederom navraag gedaan naar gebruiksgegevens. Net als bij de vorige monitor geeft men aan niet over harde gegevens te beschikken. Er wordt namelijk niet actief gemonitord op het gebruik van de standaarden. In algemene termen geeft men aan dat de situatie niet wezenlijk anders is dan in 2015 en 2014. Het beeld is – indicatief – als volgt:
- De Juriconnect-BWB-standaard is geïmplementeerd in het BasisWettenBestand van de overheid dat zowel via de internetsite wetten.overheid.nl als via diverse services als open data beschikbaar is gemaakt. Zowel door de diverse hergebruikers van de open data van dit BasisWettenBestand in het juridisch domein als door in het platform Juriconnect deelnemende partijen wordt voor het verwijzen naar de verdragen, wetten en regelingen geconformeerd aan de standaard. Hierbij gaat het om de overheid (centraal en decentraal), uitgevers van juridische informatie, content integrators, uitvoeringsorganisaties en individuele aanbieders van juridische informatie.
- De JCDR-standaard is geïmplementeerd in de Centrale Voorziening voor Decentrale Regelgeving.
- De ECLI wordt toegekend aan alle uitspraken van (tucht)rechterlijke instanties die in Nederland worden gepubliceerd. Deze ECLI's zijn alle terug te vinden in het ECLI-register op Rechtspraak.nl. Bij het citeren van uitspraken wordt tegenwoordig vrijwel altijd gebruik gemaakt van ECLI; door rechters in vonnissen en arresten, door rechtsgeleerden en door ambtenaren (beleidsnotities e.d.). Er is sprake van toenemend gebruik in andere landen van ECLI alsmede door het Europees Hof van Justitie en het Europees Patentbureau. Dit bevordert de acceptatie van de standaard. Uitbreiding van het gebruik ligt in het verschiet; door het Europees Hof voor de Rechten van de Mens en door een achttal extra landen.

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

3.5 CMIS (content-uitwisseling)

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.

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

Bron: Ministerie van BZK

Het beeld ten aanzien van de gebruiksgegevens met betrekking tot CMIS is vergelijkbaar met dat van het vorige jaar. Voor wat betreft het Rijk is er sprake van twee grote toepassingen van CMIS:

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

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

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

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

3.6 Digikoppeling versie 2.0 (berichtenverkeer)

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 is o.a. de specificatie voor grote berichten toegevoegd, de mogelijkheid om attachments toe te voegen en om security op berichtniveau toe te passen. Digikoppeling versie 2 is backward compatible met versie 1. Digikoppeling versie 3.0 is op dit moment in behandeling bij het Forum Standaardisatie voor opname, 2.0 is de versie die op de lijst voor 'pas toe of leg uit' staat.

Standaard	*op lijst sinds*	*gebruik door overheden*		*ontwikkeling in gebruik*
		totaal	*w.v. Rijk*[22]	
Digikoppeling	juni 2013	64 %	40 %	aantal aansluitingen verder gestegen, in vergelijking met vorig jaar

Bron: beheerorganisatie Logius

Logius (project Aansluitingsondersteuning Stelselvoorzieningen) heeft op verschillende peilmomenten (maart 2013, augustus 2013, augustus 2014, augustus 2015 en zomer 2016) lijsten aangeleverd waarop (onderdelen van) overheden en uitvoeringsorganisaties stonden die op Digikoppeling zeggen te zijn aangesloten. Daaruit is het onderstaande overzicht af te leiden dat laat zien dat gedurende een reeks van jaren sprake is van een gestage groei van het gebruik van Digikoppeling. De ontwikkeling in de tijd bij de categorie 'Rijk' moet met het nodige voorbehoud worden bekeken want deze categorie is gevoelig voor veranderingen in de samenstelling van de populatie. Zo zijn dit jaar veel organisaties toegevoegd uit de OOV-sector die niet zijn aangesloten op Digikoppeling. Dit drukt het percentage.

Tabel 4: Overheden aangesloten op Digikoppeling
(Bron: opgave Logius)

Digikoppeling	Rijk + Uitvoerings-organisaties / ZBO's + OOV + eOverheid	Gemeenten	Provincies	Waterschappen	**Totaal**
Voorjaar 2013	3 %	31 %	8 %	14 %	22 %
Zomer 2013	4 %	42 %	15 %	14 %	29 %
Zomer 2014	5 %[23]	57 %	23 %	14 %	40 %
Zomer 2015	64 %	63 %	42 %	24 %	58 %
Zomer 2016	40 %	75 %	67 %	46 %	64 %

[22] Waar in deze en overeenkomstige tabellen wordt gesproken over Rijk wordt bedoeld: inclusief uitvoeringsorganisaties, ZBO's + OOV + eOverheid.
[23] In 2013 en 2014 is het aantal aansluitingen gedeeld op het aantal overheidsinstellingen. In 2015 en 2016 is aansluiting gezocht bij de rekenwijze van Logius waarbij alleen de overheidsorganisaties zijn betrokken waar uitwisseling via digikoppeling aan de orde zou moeten zijn.

Conclusie:
Een substantieel deel van de overheden is op Digikoppeling aangesloten. Er is sprake van een verdere stijging, van 58% naar een aandeel van 64%. Met name provincies en waterschappen die voorheen nog relatief beperkt waren aangesloten, hebben een inhaalslag gemaakt. Het aandeel gemeenten is nog steeds relatief groot.

3.7 DKIM (email-authenticatie)

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

standaard	*op lijst sinds*	*gebruik door overheden*	*ontwikkeling in gebruik*
DKIM	juni 2012	overall: 32 %	toename van 22% naar 32%

Het overall percentage in bovenstaand kader is een gewogen gemiddelde van een tweetal groepen domeinen: gemeenten (30%) en niet-gemeentelijke overheden (39%)[24]. Deze laatste categorie is nader uitgesplitst in: Rijk, provincies en waterschappen. Zie voor meer details tabel 2.

De meting is gedaan medio 2016, nu voor de tweede keer met behulp van internet.nl[25]. In de huidige meting voor DKIM wordt gekeken of de DNS server aangeeft dat er al dan niet een DKIM-configuratie is voor de betreffende domeinnaam. Dit garandeert overigens nog niet dat alle mailservers van deze organisatie ook daadwerkelijk mails versturen die aan DKIM voldoen.

Tabel 5: Domeinnamen die aan DKIM voldoen (in %)
(Bron: internet.nl)

DKIM (versie: RFC 6376)	Rijk	*overeenkomstig definitie BFS (zie par. 3.2)*		Gemeenten		Provincies		Waterschappen		**Totaal**	
	medio 2015	*medio 2016*	*medio 2015*	*medio 2016*	*medio 2015*	*medio 2016*	*medio 2015*	*medio 2016*	*medio 2015*	*medio 2016*
voldoet aan DKIM	28%	45%	19%	30%	38%	41%	14%	20%	22%	32%
voldoet *niet* aan DKIM	72%	55%	81%	70%	62%	59%	86%	80%	78%	68%
Totaal (n)	*170*	*100*	*411*	*398*	*16*	*17*	*29*	*35*	626	*550*

Conclusie:
Ongeveer één op de drie domeinnamen van overheden is in 2016 voorzien van een DKIM-configuratie. De verschillen tussen de overheden zijn niet groot, met dien verstande dat de waterschappen relatief

[24] Zie toelichting in paragraaf 3.2.
[25] Voorheen gebeurde dat met behulp van Phishing scorecard van Measuremail.

nog wat achterblijven. In vergelijking met de meting vorig jaar is sprake van een substantiële stijging. Deze doet zich bij alle overheden voor.

3.8 DNSSEC (beveiliging domeinnamen)

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.

Standaard	*op lijst sinds*	*gebruik door overheden*		*ontwikkeling in gebruik*
		totaal	*w.v. Rijk*	
DNSSEC	juni 2012	45 %	59 %	groei van 25% naar 45%

In het kader van de monitor open standaardenbeleid 2016 is medio 2016 een lijst met 550 domeinnamen van overheden en uitvoeringsorganisaties gecontroleerd, dit jaar voor de tweede keer met behulp van de Internet.nl[26]. Met deze test kan het eerste deel van het functioneel toepassingsgebied van de standaard gemeten worden: het registreren en in DNS publiceren van internet-domein-namen ('signing'). Of de overheden ook validatie doen wanneer zij andere systemen benaderen (het tweede deel van het functionele toepassingsgebied), is niet getest.

Deze check leverde de volgende resultaten op voor 2016. Het gebruik van DNSSEC ligt binnen de overheid inmiddels op 45% en is gestegen ten opzichte van de meting vorig jaar (in 2015: 25%). In onderstaand overzicht is de ontwikkeling uitgesplitst naar de sectoren binnen de overheid.

Tabel 6: Domeinnamen overheid die voldoen aan DNSSEC
(Bron: Internet.nl)

DNSSEC	Rijk	*overeenkomstig definitie BFS (zie par. 3.2)*	Gemeenten	Provincies	Waterschappen	**Totaal**
Zomer 2015		28 %	25 %	25 %	17 %	**25 %**
Zomer 2016		59 %	42 %	35 %	37 %	**45 %**

Uit tabel 3 is af te lezen dat de stijging van het gebruik van DNSSEC zich in alle geledingen binnen de overheid voordoet. Daarbij valt op dat de inhaalslag die de categorie Rijk en uitvoeringsorganisaties vorig jaar heeft gemaakt (cijfers uit de monitor 2015 vergeleken met die uit de monitor 2014) zich verder heeft doorgezet. Deze categorie scoort nu als enige bovengemiddeld.

Op de website www.dnsssec.nl valt af te lezen dat thans (oktober 2016) bijna 45% van de 5,7 miljoen .nl-domeinen zijn voorzien van DNSSEC (vorig jaar: 44%). Inmiddels ligt de overheid derhalve op het landelijk gemiddelde als het gaat om het voldoen aan DNSSEC.

[26] Bij vorige metingen is gebruik gemaakt van de DNNSEC portfolio checker van SIDN Labs (Stichting Internet Domeinregistratie Nederland). De functionaliteit van dat instrument is opgenomen in internet.nl dat door dezelfde organisatie wordt beheerd. De totaal-percentages gebaseerd op deze eerdere wijze van meten zijn: 5% (voorjaar 2013), 10% (najaar 2013) en 14% (zomer 2014).

Conclusie:
Het aandeel websites van overheden dat voldoet aan DNSSEC gaat inmiddels richting de helft (45%). Het aantal is nog steeds groeiende. De overheden zijn met hun score inmiddels beland op het landelijk gemiddelde.

3.9 EML_NL (verkiezingen)

De EML_NL standaard versie 1.0 is het Nederlands toepassingsprofiel op de Election Markup Standard en definieert de gegevens en de uitwisseling van gegevens bij verkiezingen die vallen onder de Nederlandse Kieswet. Het gaat daarbij om de uitwisseling van kandidaatgegevens en uitslaggegevens.

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

Beheerorganisatie: Kiesraad

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

Gedurende 2015 hebben drie verkiezingen plaatsgevonden:
- Provinciale Staten en waterschapsverkiezingen (18 maart). OSV-software is beschikbaar gesteld aan:
  - 34 centraal stembureaus (provincies en waterschappen opgeteld);
  - 20 hoofdstembureaus gemeenten;
  - rond de 390 gemeenten (alle gemeenten hebben ook daadwerkelijk gebruik gemaakt van de software);
  - ongeveer 360 politieke partijen (lokale afdelingen; onbekend hoeveel er daadwerkelijk gebruik hebben gemaakt van de software);
- Eerste Kamerverkiezing (26 mei). OSV-software werd gebruikt voor uitwisseling van gegevens door:
  - 1 centraal stembureau;
  - 12 hoofdstembureaus (provincies);
  - zo'n 13 politieke partijen:
- Gemeentelijke herindelingsverkiezingen (18 november; twee nieuw te vormen gemeenten). De OSV-software is beschikbaar gesteld aan:
  - de 2 nieuw te vormen gemeenten;
  - ongeveer 20 politieke partijen (lokale afdelingen; onbekend hoeveel er daadwerkelijk gebruik hebben gemaakt van de software).

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

3.10 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:

- ISO 19136;
- NEN 3610;
- Nederlands metadataprofiel op ISO 19115;
- Nederlands profiel op ISO 19142.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
Geo-standaarden	mrt 2011	op onderdelen harde gegevens	op onderdelen: stijgend of stabiel

Er is sprake van een set van deel-standaarden. Dat maakt het krijgen van overzicht met betrekking tot het gebruik complex. Bij Geonovum is navraag gedaan met betrekking tot het gebruik. De basisset geo-standaarden staat op de lijst voor 'pas toe of leg uit' en bestaat uit de volgende 4 componenten:

- het basis-model geo-informatie NEN3610: een generiek model op basis waarvan sectorspecifieke informatiemodellen worden ontwikkeld (momenteel 16 van dergelijke informatiemodellen, nog niet alle in gebruik genomen). Naar verluidt is bij een zestal informatiemodellen (vier in de context van basisregistraties [BGT, BRT, Kadaster en BRO] en twee in het kader van overige wetgeving[27]) het bereik maximaal, in de zin dat alle bronhouders de betreffende modellen verplicht gebruiken waarbij de software deze modellen derhalve ook ondersteunt. Concrete cijfers:
    - Basisregistratie Grootschalige Topografie: alle 428 bronhouders;
    - Basisregistratie Topgrafie: 898 mln. hits in 2015;
    - Ruimtelijkje Ordening: 58.000 plannen RO op het landelijke portaal ruimtelijkeplannen.nl geplaatst conform de RO-standaarden (vorig jaar augustus 50.000).
- de Geography Markup Language (GML).GML is een formaat, speciaal ontwikkeld voor de uitwisseling van geo-informatie (aanleveren en uitleveren). Een met harde gegevens onderbouwd voorbeeld: in 2015 zijn ongeveer 350.000 BGT-opvragingen gedaan. Op basis van extrapolatie van de groeicurve zal het gebruik in 2016 in de miljoenen bevragingen gaan komen.
- metadataprofielen voor geografie en webservices. Het belangrijkste gebruik van deze standaard vindt plaats binnen het Nationaal Georegister. Huidige stand:
    - geografie: ruim 8.500 geodatasets geregistreerd waarbij gebruik gemaakt wordt van deze standaard (ter vergelijking: vorig jaar eenzelfde aantal);
    - webservices: ruim 500 services geregistreerd;
    - voor beide profielen samen is het aantal hits op het Nationaal Register een indicatie van het gebruik: in 2015 ruim 5.8 miljoen keer bevraagd.
- webserviceprofielen voor Web Feature Service (WFS) en Web Map Service (WMS), bedoeld voor het ontsluiten en daadwerkelijk verzenden van geografische data als afbeelding (kaartmateriaal). Het gebruik van deze profielen is moeilijk te kwantificeren omdat sprake is van veel verschillende aanbieders en veel verschillende softwareleveranciers. De volgende indicaties zijn wel beschikbaar:
    - WMS-services van Publieke Dienstverlening Op de Kaart (PDOK) in 2015 ruim 514 miljoen keer bevraagd;
    - de beide varianten WMTS-services 349 miljoen en WMSC-services 225 miljoen hits;
    - totaal een kleine 1,1 miljard hits, vergelijkbaar met de cijfers over 2014.

Conclusie:
Over de mate waarin vanuit overheidsorganisaties gebruik wordt gemaakt van Geo-standaarden zijn sinds dit jaar op onderdelen gegevens bekend, vooral bij het basis-model geo-informatie NEN3610. Voor het overige zijn indirecte en indicatieve cijfers beschikbaar.

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

3.11 IFC (bouw)

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

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

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

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

Dit geeft nog steeds een goed beeld van wat gaande is met betrekking tot het gebruik van IFC.

Het Rijksvastgoedbedrijf (RVB, voorheen de Rijksgebouwendienst) schrijft sinds 2011 het gebruik van IFC voor via de RVB BIM Norm in alle PPS-projecten. In de huidige RVB BIM Norm staat onder meer dat opdrachtnemers de informatie uit het gebouwmodel moeten aanleveren in de vorm van 2D-CAD-tekeningen[28] en als 3D-modellen in het open bestandsformaat IFC. Maar omdat het RVB in haar primaire processen vooralsnog berust op het gebruik van 2D-CAD tekeningen, is het interne gebruik van BIM (en dus ook van IFC) nog beperkt tot de personen die zich bezig houden met de ontwikkeling van BIM.

Het feit dat consortia de modellen aan de RVB aanleveren in IFC-formaat zegt overigens niets over het gebruik van IFC door de consortia in den brede; dat is aan de consortia zelf. De ervaring bij het RVB is dat consortia voor hun interne processen veelal gebruik maken van een merkspecifiek bronformaat. Dat staat IFC als uitwisselingsformaat evenwel niet in de weg. De ervaring bij de RVB wijst uit dat de ondersteuning van het IFC-formaat vanuit sterk in Nederland vertegenwoordigde modelleerapplicaties sinds 2011 flink is verbeterd.

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

3.12 IPv6 en IPv4 (internetprotocol IP-adressen)

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.

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

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

Standaard	*op lijst sinds*	*gebruik door overheden (%)*		*ontwikkeling in gebruik*
		totaal	*w.v. Rijk*	
IPv6 en IPv4	nov 2010	6 %	16 %	implementatie verloopt traag maar wel verbetering t.o.v. vorig jaar

In het kader van de monitor open standaardenbeleid is in juni 2016 een lijst met 605 domeinnamen van overheden en uitvoeringsorganisaties getest met behulp van Internet.nl (voorheen was de meting gebaseerd op de IPv6 domain readiness tester op ip6.nl). Deze check leverde de volgende resultaten op voor 2016: het gebruik van IPv6 ligt binnen de overheid op 6%, tegen 2% vorig jaar. Ook al is het percentage nog laag, afgezet tegen de ambitie, er is wel sprake van een beweging in de gewenste richting. Vorig jaar was nog sprake van een stabilisatie op 2%. Een nadere precisering van levert een volgend beeld op.

Tabel 7: Websites die voldoen aan IPv6 [29]
(Bron: Internet.nl voor 2015 en 2016, daarvoor: IPv6 domain readiness tester)

IPv6 *gemeten in de zomerperiode van 2014, 2015 en 2016*	Rijk + Uitvoerings-organisaties / ZBO's + OOV + eOverheid			Gemeenten			Provincies			Waterschappen			**Totaal**		
	2014	*2015*	*2016*	*2014*	*2015*	*2016*	*2014*	*2015*	*2016*	*2014*	*2015*	*2016*	*2014*	*2015*	*2016*
4 sterren	9	6	25	6	4	11	1	1	1	0	0	1	**16**	**11**	**38**
0,5 t/m 3,5 sterren	42	67	5	158	154	169	7	8	8	8	7	8	**215**	**236**	**190**
0 sterren	116	83	121	259	252	218	8	6	9	21	22	28	**404**	**363**	**376**
niet controleerbaar	13	22	0	0	1	0	0	1	0	0	1	0	**13**	**25**	**0**
totaal	***180***	***178***	***152***	***423***	***411***	***398***	***16***	***16***	***18***	***29***	***30***	***37***	***648***	***635***	***605***

Bij metingen voor 2015 werd getest op vijf functionaliteiten van domeinnaamservers op het ondersteunen van IPv6: of de DNS via een enkel-IPv6-netwerk is op te bevragen en of er IPv6-adressen gegeven worden voor DNS-servers (SOA-record), mail (MX-record), web en de 'root' van het domein. Met de test via Internet.nl (dit jaar en vorig jaar) wordt niet meer getest of de DNS-server ook antwoordt als alleen IPv6 wordt gebruikt. Wel wordt voor de websites getest of de getoonde site via IPv6 respectievelijk IPv4 dezelfde zijn. Een herberekening heeft ervoor gezorgd dat de scores van de huidige test vergelijkbaar zijn met de scores gebaseerd op de IPv6 domain readiness tester (2014).

Conclusie:
De implementatie van IPv6 door overheden verloopt traag, maar na een stabilisatie op 2% in de periode tot en met 2015 is nu wel de nodige voortgang geboekt met een score van 6%. Deze winst wordt met name geboekt bij de sectoren Rijk en Gemeenten.

[29] Bij gemeenten, provincies en waterschappen zijn in de meting 2016 ook de respectievelijke koepelorganisaties meegenomen.

3.13 NEN-ISO/IEC 27001 / 27002 (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 beide standaarden staat sinds mei 2015 een nieuwe versie 2013 op de lijst voor 'pas toe of leg uit'.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
NEN-ISO/IEC 27001 en 27002	mei 2008	Rijk: implementatie via de BIR gemeenten: 90% (implementatie via BIG / NEN-ISO/IEC 27001) waterschappen: implementatie via BIWA	Rijk: afgerond gemeenten: stijgend provincies en waterschappen: verdaande ontwikkelina

Bronnen: Ministerie van BZK / DGOBR en VNG

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

BIR

Alle departementen en daaraan gelieerde uitvoeringsorganisaties zijn gehouden aan de invoering van de VIR (Voorschrift Informatiebeveiliging Rijksdienst). De BIR (Baseline Informatiebeveiliging Rijksdienst) is daarbij de leidraad in termen van beveiligingsmaatregelen. De BIR omvat de gehele ISO/IEC 27001- en 27002-norm. De departementen en hun uitvoerings-organisaties hebben de BIR inmiddels alle geïmplementeerd. Het voldoen aan de BIR vraagt blijvend om aandacht. Daarover leggen de departementen jaarlijks door middel van een ICV (in control verklaring) verantwoording af. Alle 11 departementen hebben medio februari 2016 zo'n ICV afgegeven. Die verantwoording legt men af aan de directeur-generaal Overheidsorganisatie. De Rijksdienst geeft aan dat daarmee het gebruik en de toepassing van de standaarden NEN-ISO/IEC 27001- en 27002-norm is geborgd. Intentie is dat ook in de toekomst DGOO de naleving van VIR en BIR zal blijven monitoren.

BIG

Voor wat betreft BIG (de gemeente-variant van de BIR) is navraag gedaan bij KING (Kwaliteits-instituut Nederlandse Gemeenten). Eind november 2013 hebben gemeenten in de resolutie 'Informatieveiligheid, randvoorwaarde voor de professionele gemeente' aangegeven dat elke gemeente beleid zal vaststellen aan de hand van de BIG. Via Waarstaatjegemeente.nl wordt met enige regelmaat een uitvraag gedaan over de mate waarin gemeenten op dit vlak vorderingen hebben gemaakt.

Die uitvraag levert onder meer de volgende uitspraken op (cijfers over 2016):

- 54% (vorig jaar: 42%) van de gemeenten heeft informatieveiligheid als onderdeel van de collegeambities opgenomen. Hierbij zij aangetekend dat collegeambities voor meerdere jaren worden vastgesteld en in de regel niet tussentijds worden aangepast;

- 90% (vorig jaar: 56%) van de gemeenten heeft op bestuurlijk niveau informatiebeveiligingsbeleid vastgesteld dat is gebaseerd op de BIG (83%) of op basis van de Code voor informatiebeveiliging NEN ISO 27001 en 27002 (7%);
- 30% (vorig jaar: 12%) van de gemeenten heeft in het jaarverslag een paragraaf over informatieveiligheid opgenomen.

IBI

De provincies hebben de interprovinciale baseline informatiebeveiliging (IBI) opgesteld als uitgangspunt om informatiebeveiliging adequaat te organiseren. Deze IBI is gebaseerd op de NEN-ISO/IEC 27001 / 27002 en is in mei 2016 geactualiseerd vanwege wijzigingen in diezelfde NEN-normen. Alle provincies hebben zich geconformeerd om de IBI te implementeren en toe te passen en hebben het convenant interprovinciale regulering informatieveiligheid vastgesteld waarin staat aangeven dat de IBI het uitgangspunt is voor de provincie. Via een eigen monitoringtool rapporteren provincies hoe ver ze zijn met de implementatie van de IBI. Op basis van de nieuwe IBI voert elke provincie een gap analyse uit waardoor een accuraat en actueel beeld van de stand van zaken met betrekking tot de implementatie van de IBI beschikbaar komt.

BIWA

De Waterschappen hebben in 2013 afgesproken de Baseline Informatiebeveiliging Waterschappen (BIWA) door te voeren. De BIWA is gebaseerd op de NEN-ISO/IEC 27001 / 27002. Behalve dat elk waterschap een eigen groeipad heeft om te voldoen aan de BIWA worden onder regie van Het Waterschapshuis via een landelijk programma Informatieveiligheid diverse thema's van informatiebeveiliging collectief uitgewerkt en worden kennis en ervaringen actief uitgewisseld. Eind 2016 zullen naar verwachting de eerste 3, en mogelijk 5, waterschappen BIWA-compliant zijn. Jaarlijks vindt sectorbreed een inventarisatie plaats naar de voortgang en volwassenheid van informatiebeveiliging.

De meest recente waterschapsectorbrede uitvraag naar de voortgang van de BIWA-implementatie (cijfers december 2015) brengt het volgende beeld naar voren:

- 100% heeft een gap- en/of een risico-analyse uitgevoerd op conformiteit met de BIWA
- 87% heeft het Beleid Informatiebeveiliging laten goedkeuren door het bestuur
- 83% heeft activiteiten voor informatiebeveiliging gebudgetteerd voor 2016
- 96% heeft een BIWA-implementatieplan opgesteld
- 61% heeft in het jaarverslag gerapporteerd over informatiebeveiliging
- 87% heeft bewustzijnsactiviteiten rond informatiebeveiliging ontplooid

In het najaar van 2016 is besluitvorming in voorbereiding om alle waterschappen in 2017 te auditen en certificeren. Naar verwachting zullen eind 2017 dan ook een groot aantal waterschappen BIWA-compliant zijn.

Conclusie:

Voor de Rijksdienst (departementen en uitvoeringsorganisaties) geldt dat de standaarden ISO/IEC 27001 en 27002 zijn geïmplementeerd via de BIR (Baseline Informatie-beveiliging Rijksdienst). Daarover hebben alle 11 departementen medio februari 2016 een ICV (in control verklaring) afgegeven.

Bij de gemeenten zijn in 2014 de eerste concrete stappen gezet om zicht te krijgen op de adoptiegraad van de standaarden 27001en 27002, door implementatie van de BIG. Op basis van de meest recente peiling blijkt dat 90% van de gemeenten informatieveiligheid cq. informatie-beveiligingsbeleid heeft vastgesteld dat is gebaseerd op de BIG (83%) of op basis van de Code voor informatiebeveiliging NEN ISO 27001 en 27002 (7%). Dat betekent een flinke stijging ten opzichte van vorig jaar.

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 2015 heeft het merendeel van de waterschappen (87%) de governance op informatiebeveiliging ingericht, werken zij planmatig (96%) aan de implementatie van de BIWA en wordt het onderwerp actief onder de aandacht gebracht (87%). Eind 2016 vind wederom een sectorbrede meting plaats naar de voortgang op de implementatie van informatiebeveiliging. Naar verwachting zullen de eerste 3 tot 5 waterschappen dan BIWA-compliant zijn

3.14 ODF 1.2 / PDF 1.7 / PDF/A-1 en PDF/A-2 (documentstandaarden)

De lijst voor 'pas toe of leg uit' telt op dit moment vier open document-standaarden:

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

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

Het beeld uit bovenstaand overzicht is hetzelfde als bij de vorige monitor. Met behulp van Google is het aantal documenten bepaald met de extensie .pdf, met de extensies .ods/.odt/.odp en met de extensies .doc/.docx/.xls/.xlsx/.ppt/.pptx op 8 verschillende websites. De extensie .pdf op zichzelf geeft geen uitsluitsel over de PDF-versie, zodat op deze manier niet nagegaan kan worden hoeveel bestanden voldoen aan PDF/A-1, PDF/A-2 of PDF 1.7 en hoeveel aan een andere PDF-variant.

Tabel 8: PDF-, ODF- en MS office-bestanden op enkele websites
(Bron: Google)

	.pdf (inclusief andere pdf-versies)			**.odt** *)			**.doc** **)		
	Zomer 2014	*Zomer 2015*	*Zomer 2016*	*Zomer 2014*	*Zomer 2015*	*Zomer 2016*	*Zomer 2014*	*Zomer 2015*	*Zomer 2016*
rijksoverheid.nl	110.000	118.000	122.000	306	209	197	414	564	512
amsterdam.nl	47.200	36.500	28.500	0	0	0	1.090	3.940	3.940
rotterdam.nl	204.000	40.900	19.600	0	0	0	355	903	587
utrecht.nl	25.400	27.000	20.200	0	0	0	43	247	142
drenthe.nl	4.810	6.310	7.580	0	0	0	108	248	215
zuid-holland.nl	1.950	2.080	15.600	0	0	0	27	110	189
forumstandaardisatie.nl	1.630	1.430	446	28	22	11	8	54	14
ictu.nl	834	863	236	24	18	4	15	46	7
Totaal	***395.824***	***233.083***	***214.162***	***358***	***249***	***212***	***2.060***	***6.112***	***5.606***

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

	.pdf + .odt *) **als % van alle bestanden**			**verhouding .odt** *) **/ .doc** **)		
	Zomer 2014	*Zomer 2015*	*Zomer 2016*	*Zomer 2014*	*Zomer 2015*	*Zomer 2016*
rijksoverheid.nl	99,6 %	99,5 %	99,6 %	0,74	0,37	0,30
amsterdam.nl	97.7 %	94,2 %	87,9 %	0	0	0
rotterdam.nl	99.8 %	89,7 %	97,1 %	0	0	0
utrecht.nl	99,8 %	96,4 %	99,3 %	0	0	0
drenthe.nl	97,8 %	94,6 %	97,2 %	0	0	0
zuid-holland.nl	98,6 %	97,4 %	98,8 %	0	0	0
forumstandaardisatie.nl	99,5 %	97,6 %	97,0 %	3,50	0,40	0,69
ictu.nl	98,3 %	95,5 %	97,2 %	1,60	0,50	0,55
Totaal	***99,5 %***	***97,4 %***	***97,5 %***			

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

Gemeente Den Haag is net als vorig jaar uit de tabel verwijderd; door de configuratie van de website kan Google het document-type MS-office niet herkennen.

Uit bovenstaande tabel kunnen de volgende conclusies worden getrokken:

- voor alle onderzochte websites (rijksoverheid: alle departementen zijn ondergebracht op www.rijksoverheid.nl) blijkt het overgrote deel van alle documenten op de website in een PDF-format te zijn. Onbekend is of dit ook conform de standaarden 1.7 of A is.
- ODF (.ods/.odt/.odp) treft Google net als bij de vorige metingen alleen aan in beperkte mate op www.rijksoverheid.nl en op de websites van het Forum Standaardisatie. Op de vernieuwde site van ICTU wordt dit niet meer aangetroffen, behalve in het archief van de oude NOiV website. De aantallen schommelen, een duidelijke trend is niet zichtbaar. In vergelijking met vorig jaar liggen de aantallen lager. Een document op een website kan in ODF worden aangeboden in plaats van PDF als het bedoeld is om te hergebruiken of te bewerken.

- het aantal MS office-bestanden (.doc/.docx/.xls/.xlsx/.ppt/.pptx) is beperkt maar nog wel beduidend hoger het aantal ODF-bestanden. De gemeente Amsterdam laat zowel relatief als in absolute aantallen een hoge score zien, net als in voorgaande jaren.

Bij deze cijfers moeten wel enkele kanttekeningen geplaatst worden:
- het aantal bestanden in een bepaald formaat op de website zegt nog niets over het gebruik van deze bestandsformaten in directe (andere) contacten met burgers en bedrijven;
- daarnaast zegt het bestandsformaten op de website weinig over het gebruik van de verschillende formaten binnen de organisatie;
- de aantallen bestanden die Google bij deze zoekopdrachten vermeldt zijn niet exact. Bij grote aantallen wordt het aantal geschat, en dezelfde zoekopdracht levert niet altijd (ongeveer) het zelfde aantal op. Dit kan per Google-server tot wel 15% verschillen;
- deze zoekopdrachten geven alleen een totaal aantal bestanden met pdf-extensie, daardoor bieden de zoekopdrachten geen uitsluitsel over verschillende PDF-standaarden (PDF/A-1, PDF/A-2, PDF 1.7) en evenmin over de vraag of die in de goede gevallen zijn toegepast.

Conclusie:
Op enkele belangrijke overheidswebsites is het overgrote deel van de bestanden in een PDF-format (maar niet noodzakelijkerwijs één van de PDF-formats van de lijst voor 'pas toe of leg uit'). Bestanden in ODF-format zijn bij de acht onderzochte websites alleen bij rijksoverheid.nl, forumstandaardisatie.nl en ictu.nl in zeer beperkte mate aangetroffen.

3.15 OWMS 4.0 (metadata informatie overheid)

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

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

Beheerorganisatie: KOOP

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

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

1. Organisaties die zelf OWMS direct toepassen in hun eigen informatiesystemen. Behalve op de collecties van KOOP is bekend dat het Ministerie van AZ op rijksoverheid.nl OWMS toepast op content van alle ministeries. Ook de inspectieraad past OWMS direct toe op inspectieloket.nl voor alle 11 rijksinspecties. Verder komen met enige regelmaat vragen binnen over OWMS van leveranciers van contentpublicatiesystemen van gemeenten en gemeenschappelijke regelingen. Aantallen hiervan ontbreken. Er is geen reden om te veronderstellen dat OWMS op een meerderheid van de overheidwebsites direct wordt toegepast. Daar is ook geen sterke business case voor.

2. Organisaties die zelf een contentmodel toepassen dat op OWMS is gebaseerd. In dit verband wordt alleen gekeken naar de contentmodellen die zijn gepubliceerd op http://standaarden.overheid.nl/contentmodellen. Vrijwel alle organisaties leveren content aan voor Officiële Bekendmakingen in de Staatscourant, staatsblad, tractatenblad en parlementaire informatie. Die publicaties zijn allen gebaseerd op varianten van het model voor Officiële Publicaties (http://standaarden.overheid.nl/oep/technische-documentatie). Alleen de 40 organisaties van de rechterlijke macht leveren via rechtspraak.nl direct aan in het technische formaat van het contentmodel voor officiële publicaties. Twee andere veel toegepaste contentmodellen zijn die van CVDR en Samenwerkende Catalogi (SC). SC staat ook op de 'pas toe of leg uit'- lijst en wordt door leveranciers van productcatalogi geïmplementeerd, volgens onze bron voor vrijwel alle gemeenten, provincies en waterschappen. Zij tellen mee in deze categorie. CVDR is verplicht voor geconsolideerde regelgeving van gemeenten.
3. Organisaties die een voorziening bij KOOP gebruiken die een OWMS-compliant content-model afdwingt. Naast de hiervoor onder 2. genoemde decentrale overheden die CVDR gebruiken, maakt een groot aantal (overheids)organisaties voor hun Officiële Bekendmakingen gebruik van het Digitaal Loket dat metadata verzamelt in het formaat van het contentmodel voor Officiële Publicaties. Zij passen dus niet zelf het technische OWMS-formaat toe, maar leveren wel alle door OWMS gevraagde informatie.
4. Organisaties die content aanleveren die KOOP van metadata voorziet conform een contentmodel. De publicatie van wet- en regelgeving in het Staatsblad wordt doorgaans door de ministeries aangeleverd in verschillende formaten en vervolgens door SDU van metadata voorzien.

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

3.16 SAML (uitwisseling inloggegevens)

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

standaard	*op lijst sinds*	*gebruik door overheden*	*ontwikkeling in gebruik*
SAML	mei 2009	DigiD: 28% eHerkenning: 100%	gestage groei zichtbaar

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

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

Logius geeft aan dat 28% van alle DigiD-aansluitingen op dit moment via SAML loopt. Ter vergelijking: vorig jaar was dat nog 19%. In deze opgave van Logius zijn ook sectoren opgenomen zoals zorg, werk

& inkomen en software-ontwikkelaars. Als hierop wordt gecorrigeerd is het percentage opgelopen van 17% vorig jaar naar 24% dit jaar.

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

Tabel 9: Aansluitingen bij eHerkenning en DigiD, gebaseerd op SAML
(Bron: opgave Logius)

SAML *gechecked: augustus 2013, augustus 2014, en augustus 2015*	Rijk + Uitvoerings-organisaties / ZBO's + OOV + eOverheid				Gemeenten				Provincies				Waterschappen				**Totaal**			
	2013	*2014*	*2015*	*2016*	*2013*	*2014*	*2015*	*2016*	*2013*	*2014*	*2015*	*2016*	*2013*	*2014*	*2015*	*2016*	*2013*	*2014*	*2015*	*2016*
SAML bij eHerkenning	15	19	20	17	37	75	126	142	2	5	5	8	0	0	1	1	54	99	152	168
SAML bij DigiD	1	4	12	17	1	54	80	109	0	1	1	2	0	0	0	0	2	59	93	128
Totaal	*16*	*23*	*32*	*34*	*38*	*129*	*206*	*251*	*2*	*6*	*6*	*10*	*0*	*0*	*1*	*1*	*56*	*158*	*245*	*296*

Conclusie:
De invoering van SAML maakt een gestage ontwikkeling door in de goede richting. Het aantal aansluitingen op SAML loopt op, zowel bij DigiD als bij eHerkenning.

3.17 Semantisch model e-factureren (betalingsverkeer)

Het Semantische factuurmodel is een standaard voor elektronisch factureren. 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. 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. De opname van het semantische factuurmodel geeft duidelijkheid aan overheden en bedrijven (gebruikers en ICT-aanbieders) over de elementen die op facturen naar overheidsorganisaties gebruikt dienen te worden (specifiek voor de Nederlandse situatie).

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in*
Semantisch model e-factureren	juni 2013	62% facturen digitaal verwerkbaar; 25% facturen via digipoort (Rijk)	wisselend beeld

Het Semantisch model e-factureren (SMeF) is te gebruiken in uiteindelijke uitwisselformaten voor automatisch verwerkbare facturen. Daarnaast zijn er elektronische facturen die niet geautomatiseerd verwerkbaar zijn omdat ze niet in een verwerkbaar formaat worden aangeboden (maar bij voorbeeld

in PDF), of aangeboden worden via een webportaal. Ook facturen die niet conform een SmeF zijn opgesteld, kunnen door de ontvanger opgeslagen worden in een eigen database die ingericht is conform het Semantisch model. Voor de toekomst geldt als streven dat alle factuuraanmakers, -verzenders, -ontvangers en intermediaire partijen de Europese richtlijn voor de opmaak van eFacturen voor november 2018 opvolgen.

Digipoort is een ICT-portaal voor elektronische berichtenuitwisseling tussen bedrijfsleven en overheden. Voor e-Factureren gebruikt Digipoort de van het Semantisch model e-Factureren afgeleide SETU en NLOH. Op de peildatum augustus 2016 zijn de 58 financiële administraties van de Rijksdienst aangesloten op Digipoort, evenals het UWV en een zestal gemeenten. Een gemeente en één provincie zullen binnenkort op Digipoort aansluiten. Naast efactuur-ontvangst via Digipoort zijn andere ontvangstvoorzieningen in gebruik bij de Rijksdienst.

Alleen voor de overheidssector Rijk zijn gegevens beschikbaar over de mate van adoptie van elektronisch factureren. Volgens opgave van de Directie Inkoop, Faciliteiten, Huisvesting Rijk[30] zijn over 2015 de volgende kerncijfers beschikbaar:

- over 2015 zijn bij de Rijksdienst in totaal circa 1,6 mln. facturen binnengekomen;
- 62% van die facturen is digitaal verwerkbaar (bij de vorige monitor over 2014: 53%);
- hiervan is 42% e-Factuur, 20% PDF-factuur en 38% een papieren factuur;
- 25% van deze 1,6 mln. facturen is via Digipoort ontvangen (monitor over 2014: 19%);
- het is onbekend hoeveel van de facturen conform SETU zijn en hoeveel conform NLOH.

Het Kabinet heeft besloten om per 1 januari 2017 een eFactuurplicht aan leveranciers van de Rijksdienst op te leggen. Beoogd wordt om het percentage eFacturen naar de Rijksdienst verder te verhogen en het factuurproces binnen de rijksdienst verder te optimaliseren. Belangrijker nog is de impuls die met het voorbeeld van de Rijksdienst wordt gegeven aan [verdere] toepassing van eFacturatie door bedrijfsleven en andere overheden. Leveranciers kunnen met de meeste financiële pakketten beschikbaar in Nederland op gemakkelijke wijze een eFactuur aanmaken en aan de Rijksdienst versturen. E-Factuur berichten worden vanuit het netwerk van software leveranciers en factuurintermediairs verenigd in SimplerInvoicing via één van de factuurintermediairs via Digipoort bij de Rijksdienst ontvangen. Voor personen en organisaties die geen softwarepakket en/of factuurintermediair inzetten kan via het e-Factuurportaal van DigiInkoop handmatig een factuur ingelegd worden die als e-Factuur de juiste financiële administratie bij de Rijksdienst bereikt.

Andere overheden kunnen op dezelfde wijze via de SimplerInvoicing en Digipoort mits aangesloten op Digipoort eFactuur berichten in de afgesproken berichtformaten ontvangen. Andere overheden kunnen ook direct met SimplerInvoicing een connectie realiseren.

De Europese commissie is voornemens drie syntaxen te accorderen die door alle aanbestedende diensten moeten worden geadopteerd. SimplerInvoicing werkt met standaard en bijbehorende mapping SI-UBL. SI-UBL, NLOH en SETU zullen de in ontwikkeling zijnde Europese e-Factuurstandaarden en mappings moeten volgen. In NL is het voornemen om de EU-UBL voor de Rijksdienst verbindend te verklaren en de overige syntaxen naar EU-UBL te converteren. Voor de Rijksdienst wordt verwacht dat NLOH en SETU migreren naar EU-UBL. Aanzienlijke investeringen in ICT infrastructuur en ontvangende informatiesystemen zullen in de komende jaren noodzakelijk zijn.

Wanneer we het gebruik van de standaard in een breder perspectief plaatsen, blijkt dat in 2014 van alle rekeningen die het bedrijfsleven verzond bijna twee op de drie een elektronische factuur was: 64 %. Dit cijfer omvat zowel e-facturen als overige elektronische facturen[31]. De stijging blijft daarmee doorzetten. In 2012 bedroeg dit aandeel nog 45 % en in 2013 56%. Er is dus sprake van een gestage toename. Het aandeel van de ontvangen elektronische facturen laat ook een groei zien: in 2014 was 54% van de facturen niet op papier gedrukt, in 2013 was 47% van de ontvangen facturen elektronisch en in 2012 was dat 43%.

[30] Onderdeel van het Ministerie van BZK, DGOBR.

[31] Het onderscheid tussen e-Facturen enerzijds en elektronische facturen die niet geschikt zijn voor automatische verwerking anderzijds, is hier niet mogelijk vanwege onvoldoende betrouwbaarheid van de cijfers. Bron: ICT, kennis en economie in cijfers 2015, paragraaf 5.4, CBS, Den Haag / Heerlen/ Bonaire. De cijfers over 2012 wijken af van de gegevens uit de vorig jaar gepubliceerde monitor. Dat is toe te schrijven aan een andere wijze van presentatie van de cijfers door het CBS in bovengenoemde publicatie in vergelijking met die van vorig jaar.

Conclusie:
Voor wat betreft de adoptie van elektronisch factureren zijn alleen gegevens bekend over het Rijk. Daar loopt het inmiddels goed; ruim meer dan de helft van de facturen over 2015 (62%) is digitaal verwerkbaar (over 2014: 53%). Het aandeel facturen dat via Digipoort is ontvangen, vertoont ten opzicht van de vorige monitor ook een stijging (van 19% naar 25% over 2015). Voor andere overheden zijn geen gegevens bekend.

3.18 SETU-standaarden (elektronisch berichtenverkeer uitzendbranche)

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

standaard	*op lijst sinds*	*gebruik door overheden*	*ontwikkeling in gebruik*
SETU	mei 2009	geen harde gegevens	stijgende trend

Er zijn - net als in eerdere jaren - geen exacte gegevens beschikbaar over het gebruik van de SETU-standaard in termen van aantallen berichten. Met betrekking tot de adoptie van de SETU-standaard heeft onze bron[32] voor de monitor 2014 het volgende aangegeven met betrekking tot de aanbodzijde van dit deel van de arbeidsmarkt:

- 85% van de uitzendorganisaties in termen van marktvolume (omzet markt flexibele arbeid) is aangesloten bij SETU; deze paar grote spelers gebruiken de SETU-standaard voor berichtenuitwisseling;
- de rest van de markt is grotendeels afhankelijk van hun softwareleverancier; een recente inventarisatie onder deze softwareleveranciers wijst uit dat 12 (van de 14 geraadpleegde) leveranciers SETU ondersteunen.

Dit beeld is niet fundamenteel veranderd in de afgelopen periode, in elk geval niet voor zover dat valt te staven met (nieuwe) harde gegevens; berichtenverkeer wordt niet gemeten en in het afgelopen jaar zijn evenmin enquêtes gehouden. In de praktijk blijkt het lastig om de feitelijke adoptie van de SETU-standaard te meten. Zo nu en dan worden uitzenders wel eens bevraagd over de penetratie van SETU. De uitkomst daarvan onderschrijft het bovenstaande beeld. Er lopen bij uitzenders altijd wel een paar trajecten om klanten aan te sluiten via SETU; in die zin blijft de trend - net als vorig jaar - positief.

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

3.19 SIKB0101 (water/bodembeheer)

De SIKB-standaard richt zich op het uitwisselen van onderzoeksgegevens over de (milieu-hygiënische) kwaliteit van de bodem, inclusief geografische en administratieve gegevens, en de specifieke gegevens die direct voortkomen uit (of vooruitlopen op) de besluiten die het bevoegd gezag naar aanleiding daarvan heeft genomen.

[32] TNO (in augustus 2014).

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
SIKB0101	dec 2010	decentrale overheden die een BIS gebruiken; Rijkswaterstaat Leefomgeving (Bodemloket)	n.v.t.

Beheerorganisatie: SIKB

Alle overheden die een BodemInformatieSysteem (BIS) gebruiken, passen ook SIKB0101 toe. Aangezien veruit de meeste provincies, omgevingsdiensten en gemeenten een BIS gebruiken, kan worden afgeleid dat zij daarmee ook de standaard toepassen. Waterschappen gebruiken geen BIS en zijn bij SIKB dan ook beperkt in beeld. Wel wordt SIKB0101 ondersteund door het landelijke waterbodeminformatiesysteem WAB-Info (RWS) en gebruiken enkele waterschapslaboratoria SIKB0101 voor gegevensuitwisseling.

Ook Rijkswaterstaat Leefomgeving is gebruiker van de SIKB-standaard in diverse applicaties (o.a. Meldpunt Besluit Bodemkwaliteit, BoToVa, Bodemloket). RWS Leefomgeving trekt samen op met de beheerorganisatie om ondersteuning van SIKB0101 door leveranciers te stimuleren.

Naast bovengenoemde overheidsorganisaties passen ook bodem-adviesbureaus en (milieu-) laboratoria SIKB0101 toe.

Conclusie:
Rijkswaterstaat Leefomgeving en vrijwel alle gemeenten, provincies en omgevingsdiensten beschikken over systemen waarin SIKB0101 is toegepast. Harde gegevens over de mate waarin overheden digitaal gegevens delen zijn evenwel niet beschikbaar. Aandachtspunt is en blijft een tijdige update naar nieuwe versies van de standaard.

3.20 SKOS (linked data)

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

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

Bron: Taxonic / Kadaster.

Navraag bij onze bronnen wijst uit dat er geen kwantitatieve gegevens over het gebruik van SKOS beschikbaar zijn, en dat er ook geen orgaan is dat ontwikkelingen rond deze standaard cijfermatig bijhoudt. Men neemt wel veel belangstelling voor de standaard waar. De volgende concrete ontwikkelingen uit het afgelopen jaar zijn vermeldenswaardig:

- het kadaster heeft zijn begrippenwoordenboek via SKOS ontsloten (tax.kadaster.nl);
- ook is het kadaster bezig PDOK beschikbaar te maken in de vorm van Linked Data. Daarbij speelt SKOS ook een belangrijke rol;

- de hulpdiensten in Nederland hebben hun begrippenwoordenboeken conform SKOS gepubliceerd op www.firebrary.nl;
- Kennisnet is bezig met een serie projecten om taxonomieën met SKOS te ontsluiten;
- OWMS bevat ook twee thesauri conform SKOS;
- CBNL is een initiatief om begrippen in de bouw met RDFS/OWL te modelleren, daarbij speelt SKOS ook een rol.

Van de zijde van het Kadaster wordt hier nog aan toegevoegd dat SKOS veel gebruikt wordt voor de basisregistraties BRT en BRK, en in de nabije toekomst ook voor de BAG en BGT.

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

3.21 SPF (anti-phishing)

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

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
SPF	mei 2015	54%	flinke toename (2015: 32%)

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

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

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

Tabel 10: Mailservers overheid die voldoen aan SPF
(Bron: Internet.nl)

SPF

	Rijk	overeenkomstig definitie BFS (zie par. 3.2)	Gemeenten	Provincies	Waterschappen	**Totaal**
Zomer 2015	35 %*		31 %	35 %*	35 %*	**32 %**
Zomer 2016	55 %		55 %	59 %	46 %	**54 %**

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

Conclusie:
Het aandeel websites van overheden dat voldoet aan SPF ligt inmiddels boven de 50% en laat in vergelijking met vorig jaar een behoorlijke stijging zien. De onderscheiden categorieën overheden ontlopen elkaar qua score niet zoveel.

3.22 STOSAG (afvalbranche)

Door de beheerorganisatie van STOSAG zijn inmiddels vijf standaarden ontwikkeld. Hiervan hebben er vier betrekking op een afzonderlijk proces van informatie-uitwisseling en één op de technische informatie-uitwisseling. De processen die momenteel in de scope van de STOSAG-standaard zitten zijn:

- communicatie tussen chipkaarten en (ondergrondse) verzamelcontainers met toegangsidentificatie;
- communicatie tussen bechipte minicontainers en identificatiesystemen op de inzamelwagen;
- communicatie tussen verzamelcontainers en back-office systemen;
- communicatie tussen de systemen op de inzamelwagen en back-office systemen.

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
STOSAG	nov 2011	gemeenten > 40% lokale uitvoeringsorganisaties > 75%	stijging bij gemeenten van 30% naar 40%

Bron: Koninklijke Vereniging voor Afval- en Reinigingsmanagement (NVRD)

Door de in STOSAG participerende stuur- en werkgroepleden is in kwalitatieve zin het een en ander opgemerkt over het gebruik. Op diverse plekken zijn componenten uit de standaard geïmplementeerd door leveranciers van software in de afvalbranche. Een inschatting van de penetratiegraad bedraagt 75% (aandeel leveranciers dat in delen van de STOSAG-standaard compliant is). Delen van de standaard zijn ook daadwerkelijk en aantoonbaar geadopteerd door de markt (gebruikers). Dit is vooral af te lezen aan de standaardisatie van toegangspassen tot ondergrondse verzamelsystemen (MiFAre passen). Er wordt in 'afval-land' nauwelijks meer anders uitgerold behalve in sommige legacy-omgevingen. Dit geldt ook in toenemende mate voor chips in mini-containers (kliko's).

Analyse van recente aanbestedingen[33] heeft uitgewezen dat in nagenoeg alle aanbestedingen binnen het domein een verwijzing wordt gemaakt naar STOSAG (met name aangaande de chips in minicontainers en de pasjes). Daar waar geen vernieuwing plaatsvindt (legacy architectuur) is

[33] Een globale analyse door de NVRD van een 9-tal recente aanbestedingen van TenderNed wijst uit dat in 7 gevallen sprake is van STOSAG compliancy.

toepassing van STOSAG niet aan de orde. Omdat de markt van leveranciers in toenemende mate STOSAG standaard al compliant producten levert, zijn ook steeds meer afnemers zich niet bewust van het feit dat ze STOSAG-compliancy in huis hebben of halen.

Een inschatting van het gebruik van de standaard aan de zijde van de overheid:
- gemeenten: in elk geval 40%;
- lokale uitvoeringsorganisaties: in elk geval 75%.

Het doorontwikkelen van de standaard naar versie 2.0, het verder stimuleren van het gebruik binnen Nederland en het inbrengen van kennis vanuit de STOSAG in Europees verband zijn aandachtspunten voor 2015-2016.

Conclusie:
Op basis van enkele cijfermatige en kwalitatieve uitspraken bestaat het beeld dat de invoering van STOSAG een stijgende lijn laat zien bij de doelgroep: gemeenten en lokale uitvoeringsorganisaties.

3.23 StUF (berichtenstandaard)

De StUF-standaard is een familie van samenhangende gegevens- en berichtenstandaarden. StUF staat sinds eind 2008 op de pas-toe-of-leg-uit-lijst en richt zich op de standaardisatie van de inhoud van informatie, berichten en services. StUF is als open standaard vastgesteld voor :
- uitwisseling en bevraging van basisgegevens die behoren tot een aantal wettelijk vastgestelde basisregistraties, zoals Personen (GBA), Adressen (BRA), Gebouwen (BGA), Kadaster (BRK), Nieuw Handelsregister (NHR) en Waarde Onroerende Zaken (WOZ);
- uitwisseling en bevraging van zaakgegevens die behoren tot de producten- en diensten-portfolio van gemeenten;
- uitwisseling van domein- of sector-specifieke gegevens waarin ook basis- en/of zaak-gegevens voorkomen en waarvoor geen andere (inter)nationale (XML-gebaseerde) berichtenstandaard is vastgesteld.

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

Verbeterde standaardisatiemethodiek

Een belangrijke impuls in het toepassen en de doorontwikkeling van StUF is gerealiseerd in het kader van OperatieNUP, het meerjarige programma dat KING uitgevoerd heeft in opdracht van de VNG. Binnen Operatie NUP is een aantal standaardisatietrajecten uitgevoerd en een organisatie, methodiek en instrumentarium neergezet om toekomstige standaardisaties te ondersteunen. Na beëindiging van OperatieNUP in december 2014, zijn genoemde activiteiten gecontinueerd en ook elders toegepast. Het betekent dat al tijdens het standaardisatieproces, vroegtijdig met leveranciers, afspraken worden gemaakt over het inbouwen van de standaarden, het preventief testen ervan en het publiceren van informatie over softwareproducten en testresultaten in de Softwarecatalogus.

Met 155 softwareleveranciers zijn nieuwe convenanten en addenda afgesloten (vorig jaar: 167). De afname van het aantal leveranciers met een actueel convenant heeft te maken met het aflopen van het oude convenant per eind 2015 en de introductie van een nieuw convenant voor de periode 2016 t/m 2018 waarin de set van afspraken tussen KING en leveranciers verder uitgebreid en aangescherpt is in het kader van de doelstellingen van Digitale Agenda 2020. Sommige leveranciers hebben besloten niet verder te opereren op de gemeentelijke markt.

Compliancy en StUF Testplatform

Om er voor te zorgen dat leveranciers tijdig en aantoonbaar aan de standaarden voldoen (=compliancy) is het StUF Testplatform beschikbaar. Met deze online testomgeving kunnen leveranciers hun softwareproducten preventief en objectief testen op de juiste toepassing van StUF. Een foutloze test geeft een goede kwaliteitsindicatie over interoperabiliteit middels StUF. De adoptie van het StUF Testplatform, dat nu 4,5 jaar beschikbaar is, door leveranciers verliep in eerste instantie traag. Door aanhoudende druk neemt het gebruik gestaag toe. In de zomer van 2016 hadden 56 leveranciers van gemeentelijke software een account op het StUF Testplatform (vorig jaar: 52). Maandelijks worden enkele duizenden StUF-berichten getest. Het testplatform wordt ook gebruikt voor de StUF (deel)standaarden van de Waarderingskamer, het Zorginstituut Nederland, Geonovum en het Ministerie van V&J.

Sinds september 2014 publiceert KING driemaandelijks een Compliancy monitor. Deze monitor is bedoeld om gemeenten, samenwerkingsverbanden en ketenpartijen op een overzichtelijke manier te informeren over welke software-producten wel en niet voldoen aan de actuele standaarden. Zie verder http://kinggemeenten.nl/secties/leveranciersmanagement/producten/compliancy-monitor. Voor gemeenten is het van belang bij aanschaf en acceptatie van software of updates foutloze testrapporten te eisen. Om het ICT opdrachtgeverschap verder te versterken en het toepassen van standaarden beter te borgen worden binnen de Digitale Agenda 2020 uniforme ICT inkoopvoorwaarden gerealiseerd. (zie www.gibit.nl)

Uitbreidingen van de StUF familie

Voor de aansluiting op basisregistraties en andere landelijke voorzieningen is afgelopen jaren de StUF-familie uitgebreid voor het Handelsregister van de Kamer van Koophandel, de aansluiting op de LV-WOZ van de Waarderingskamer, op MijnOverheid Lopende Zaken met Logius en voor de BGT (StUF-GEO-IMGEO) met GEONOVUM. Ook voor het berichtenverkeer voor het nieuwe jeugdstelsel (CORV) van het Ministerie van V&J en ketens voor de decentralisaties in samenwerking met Zorg Instituut Nederland wordt StUF gebruikt. In deze trajecten wordt voorgebouwd op StUF en waar mogelijk combinatie gemaakt met andere standaarden (iWMO en iJW) . Deze uitbreidingen op StUF zijn ontwikkeld door of in nauwe samenwerking met de betreffende organisaties. In enkele gevallen lukte dat na nadrukkelijk aandringen door de VNG en KING en op grond van uitgevoerde impact-analyses.

Naast de uitbreiding van StUF voor externe koppelingen zijn nieuwe aangescherpte standaarden opgesteld voor een selectie van binnengemeentelijke ketens. Binnen deze standaarden is het gebruik van authentieke basisgegevens en zaakgegevens meegenomen. Voorbeelden zijn ketens voor betalen en invorderen, BAG-WOZ, BAG-GBA, documentcreatie, voorinvullen van digitale (e-)formulieren, zaakgericht werken (Zaak- en Documentservices, StUF-ZTC), toezicht en handhaven en WABO-BAG. Acht van deze standaarden zijn formeel vastgesteld en worden momenteel door meerdere ICT-leveranciers ingebouwd.

Markttransparantie door GEMMA Softwarecatalogus

In het najaar van 2012 is de eerste versie van de GEMMA Softwarecatalogus (www.softwarecatalogus.nl) in gebruik genomen. Deze online softwarecatalogus biedt transparantie en inzicht over welke leveranciers gemeentelijke softwareproducten aanbieden, wat de productplanning is en welke (open) standaarden worden ondersteund. In het voorjaar van 2013 waren daarin ruim 400 softwareproducten van circa 60 leveranciers opgenomen. In maart 2014 is versie 2 van de catalogus geïntroduceerd. Een belangrijke uitbreiding is de functionaliteit waarmee gemeenten het eigen applicatieportfolio kunnen bijhouden. Gemeenten gebruiken de softwarecatalogus voor hun ICT-management en voor onderlinge kennisdeling. Inmiddels maken alle gemeenten er gebruik van. Ruim 200 gemeenten hebben hun applicatieportfolio er redelijk compleet in opgenomen. Inmiddels gebruiken ook steeds meer samenwerkingsverbanden de Softwarecatalogus. Ook daar worden de StUF-standaarden gebruikt, zodat het beeld van het gebruik steeds completer wordt. Het aanbod van

software in de catalogus neemt steeds verder toe. In de software staan meer dan 2000 softwareproducten (incl. versies; vorig jaar 1500) van 186 ICT-leveranciers (vorig jaar: 167). In de softwarecatalogus kunnen leveranciers ook hun testrapportages publiceren. Dit is van belang voor gemeenten en andere overheden om inzicht te krijgen in de juiste toepassing van StUF of andere (open) standaarden. Voorts helpt het bij het verhogen van de betrouwbaarheid van de door leveranciers geregistreerde productinformatie. Het aantal gepubliceerde testrapporten (vorig jaar360) is flink gestegen tot inmiddels ruim 720.

In overleg met het Bureau Forum Standaardisatie zijn afspraken gemaakt over het gebruik van de softwarecatalogus als informatiebron voor onderliggende monitor.

Adoptiegraad van StUF

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

Tabel 11: Adoptiegegevens StUF

Adoptiegraad	**Totaal**	**StUF-BG 3.10**	**StUF-ZKN 3.10**
Aantal leveranciers	186 (167)	56 (46)	50 (41)
Aantal softwareproducten (incl. versies)	2043 (1568)	645 (340)	384 (244)
waarvan beschikbaar/in gebruik	1346 (1043)	349 (195)	193 (144)
waarvan gepland/in ontwikkeling	153 (238)	104 (65)	37 (36)
Verdeling softwareproducten naar functioneel gebied (status in gebruik en in ontwikkeling)			
Frontoffice	509 (498)	119 (107)	110 (119)
Midoffice	646 (671)	188 (163)	154 (165)
Backoffice	888 (920)	287 (255)	147 (147)
Bedrijfsvoering	428 (446)	138 (118)	111 (122)

(bron KING: www.softwarecatalogus.nl - peildatum augustus 2016; tussen haakjes de cijfers van de vorige monitor)

Op dit moment bieden 56 softwareleveranciers 349 softwareproducten (incl. versies) aan die StUF BG ondersteunen. Voor StUF ZKN (Zaken) gaat het om 50 leveranciers en 193 producten. Voor tientallen softwareproducten is de (door)ontwikkeling gepland.

Alle gemeenten (100%) gebruiken de StUF standaard. De adoptie neemt gestaag steeds verder toe. Het aantal softwareproducten dat bijv. StUF BG ondersteunt is t.o.v. 2015 met 154 toegenomen. De relatieve adoptiegraad t.o.v. het totaal aantal geregistreerde producten blijft ongeveer gelijk. Een vergelijkbaar beeld geldt voor StUF ZKN.

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

Dit positieve beeld wil niet zeggen dat gegevensuitwisseling van basisgegevens- en/of zaakgegevens in alle afnemende processen en informatiesystemen optimaal is en conform StUF verloopt. Er wordt nog veel gebruik gemaakt van oude versies (50% StUF 2.x) en/of maatwerk koppelingen. Ook zijn veel binnengemeentelijke informatie- of procesketens (nog) niet of slechts deels gedigitaliseerd. Dit belemmert niet alleen de invoering van zaakgericht werken, optimale online diensten en het breder

gebruik van authentieke gegevens, ook een verdere doorontwikkeling en grootschalige digitalisering van processen zoals bijvoorbeeld geautomatiseerde processturing op basis van mutaties en signalen uit systemen is niet goed uitvoerbaar.

Voorts blijkt er een groot verschil tussen de afspraken die via convenanten met leveranciers zijn gemaakt en het daadwerkelijk en tijdig nakomen ervan. Sommige leveranciers spelen niet of te laat in op de vraag. Deels is dat te wijten aan het achterblijven van een gebundelde vraag en gerichte opdrachtverstrekking door gemeenten. Een ander deel wordt veroorzaakt door tempo-verschillen tussen leveranciers onderling. Voor gemeenten zijn dit belemmeringen bij het kunnen doorvoeren van procesverbeteringen.

Vernieuwing StUF familie

De basis van de actuele versie van de StUF familie (3.x) is al gelegd in 2008. Om aan te sluiten op nieuwe behoeften, snellere ICT ontwikkeling en technische ontwikkelingen is in 2015 gestart met verkenningen en analyses naar een grondige vernieuwing van de StUF familie. Daarin wordt zowel in de inhoud van de standaard, de ontwikkelaanpak en tooling vernieuwd. De verwachting is dat in 2017 de eerste vernieuwde StUF onderdelen beschikbaar komen voor implementatie.

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

Om de baten van de StUF-standaard te benutten is meer aandacht nodig voor verbreding van het gebruik in andere gemeentelijke ketens, processen en systemen. Bij deze optimalisatie 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 vernieuwing van de StUF Familie en de borging van Open Standaarden in de uniforme ICT inkoopvoorwaarden (GIBIT) daar aan bijdraagt.

3.24 TLS (beveiliging)

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

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
TLS	sept 2014	79%; daarvan ruim een kwart cf. richtlijn NCSC	verdere stijging van vorig jaar al hoge score

Voor TLS heeft het Nationaal Cyber Security Centrum (NCSC) voorgeschreven hoe overheden hun webservers moeten inrichten[34]. Door te werken conform deze richtlijn, verkleint de overheid de kans dat beveiligde gegevensstromen alsnog worden gemanipuleerd of afgelezen door kwaadwillenden. Op de lijst voor 'pas toe of leg uit' staat dat bij beveiligde verbindingen gebruik moet worden gemaakt

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

van TLS, maar niet wanneer er een beveiligde verbinding gebruikt moet worden. De eigenaar van een webserver kan daarom een reden hebben waarom hij niet TLS ondersteunt.

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

Het overall percentage in bovenstaand kader is een gewogen gemiddelde van een tweetal groepen domeinen: gemeenten (82%) en niet-gemeentelijke overheden (79%)[35]. Deze laatste categorie is nader uitgesplitst in: Rijk, provincies en waterschappen. Zie voor meer details tabel 12.

Tabel 12: Websites die ondersteuning bieden aan TLS
(Bron: Internet.nl)

TLS	Rijk	*overeenkomstig definitie BFS (zie par. 3.2)*	Gemeenten		Provincies		Waterschappen		**Totaal**	
	2015	*2016*	*2015*	*2016*	*2015*	*2016*	*2015*	*2016*	***2015***	***2016***
Wel, en cf. richtlijn NCSC	11 %	43 %	4 %	21 %	0 %	24 %	0 %	40 %	**6 %**	**26 %**
Wel; niet cf. richtlijn NCSC	40 %	22 %	69 %	61 %	69 %	53 %	72 %	43 %	**61 %**	**53 %**
Ondersteunt TLS niet	49 %	35 %	27 %	18 %	31 %	24 %	28 %	17 %	**33 %**	**21 %**
Totaal (n)	*170*	*100*	*411*	*398*	*16*	*17*	*29*	*35*	***626***	***550***

Ongeveer 4 op de 5 websites van overheden biedt ondersteuning aan TLS. Daarbij laat elk van de te onderscheiden categorieën overheden groei zien in vergelijking met vorig jaar (in 2015: 67%). De volgende zaken vallen op:

- de categorie Rijk (brede definitie) blijft –net als vorig jaar- achter bij het gemiddelde beeld met 65% maar is wel bezig met een (beperkte) inhaalslag;
- er is sprake van een verschuiving, richting toepassing van TLS conform de richtlijn van het NCSC. Met name bij de waterschappen zijn hier flinke vorderingen gemaakt.
- net als vorig jaar scoort de categorie Rijk relatief hoog op inpassing van TLS conform de richtlijn van het NCSC.

Conclusie:
De standaard TLS komen we veel tegen bij overheidswebsites (79%) en is ook gegroeid in vergelijking met vorig jaar (in 2015: 67%). De aanpak conform de richtlijn van het NCSC komt ook steeds meer voor: inmiddels bij 26% van de hier onderzochte websites (vorig jaar: 6%).

[35] Zie toelichting in paragraaf 3.2.

3.25 VISI (bouwprocesinformatie)

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

standaard	*op lijst sinds*	*gebruik door overheden*	*ontwikkeling in gebruik*
VISI	dec 2014	onbekend, gebruik onduidelijk	n.v.t.

Bron: BIM loket

Bij BIM-loket is navraag gedaan over het gebruik van VISI. Zijn beschikken over totaalgegevens van het aantal organisaties dat op servers van softwareleveranciers draait, alsmede het aantal accounts, het aantal transacties, het aantal berichten en het aantal bijlagen dat wordt gewisseld[36]. Een opgave specifiek gericht op het gebruik door overheden is niet beschikbaar.

Op de website van BIM loket wordt melding gemaakt van het feit dat grote publieke opdrachtgevers het gebruik van VISI inmiddels voorschrijven in projecten die met BIM werken. Daarbij gaat het om ProRail, Rijkswaterstaat, de provincie Gelderland en de gemeenten Rotterdam, Amsterdam, Groningen, Leiden, Breda, 's Hertogenbosch, Haarlemmermeer en Heerlen.

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

3.26 WDO Datamodel (grensoverschrijdend verkeer)

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

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

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
WDO Datamodel	apr 2014	in elk geval RWS en Douane	stabiel

[36] Op servers B&S (stand september 2016): ongeveer 750 organisaties (gecorrigeerd voor dubbelingen) en ruim 11.000 accounts. Over de eerste 7 maanden van 2016: 99.000 transacties, 274.000 berichten en 227.000 bijlagen gewisseld. Een aantal organisaties (ongeveer 30, waarvan 3 gemeenten en 1 maal Rijk) werkt wel met VISI-software maar op eigen servers.

Het Nationaal Platform Data Model (NPDM) neemt in Nederland de communicatie over en de coördinatie rond het WDO Datamodel op zich. De organisatie van het NPDM is de afgelopen jaren uitgevoerd door Logius. Deze rol is gedurende 2016 overgedragen aan de Nederlandse Douane. Dit zal betekenen dat de taken van het NPDM wellicht in een aangepaste vorm zullen worden uitgevoerd.

Het beheer van de MIG's blijft de verantwoordelijkheid van de ontwikkelaars. Het Nationaal Platform Data Model (NPDM) geeft aan dat er op dit moment meerdere MIG's in gebruik en ontwikkeling zijn, die gebaseerd zijn op het Datamodel. De Nederlandse Douane publiceert vijf MIG's gebaseerd op het Datamodel, namelijk de MIG's AGS (Import, Opslag), AGS (Export), AIS/ICS, AES/ECS en Comfort info. De MIG's stellen organisaties in staat hun systemen aan te passen. De MIG's worden gepubliceerd op de OSWO omgeving (https://www.oswo.nl/swodouane/). Ook is de NVWA, samen met de Nederlandse Douane bezig met de ontwikkeling van MIG's voor de applicaties VGC en CLIENT Import gebaseerd op het WDO Datamodel.

Tevens is de Single Window-MIG voor het Maritiem Single Window (MSW, door Rijkswaterstaat, Douane en Grensbewaking) geheel gebaseerd op het Data Model. De MIG bestaat uit de berichten behorende bij de implementatie van het MSW voortvloeiend uit de Europese Richtlijn 2010/65 en overige Douane-berichten behorend tot de Douaneprocessen Binnenbrengen, Uitgaan en Proviand. Deze MIG wordt tevens gepubliceerd op de OSWO omgeving.

Een andere belangrijke ontwikkeling waarvan de verwachting bestaat dat deze het gebruik zal doen toenemen is de voorgenomen plaatsing van het WDO Datamodel op de Europese lijst van open standaarden. Dit wordt voorzien in het laatste kwartaal van 2016.

Conclusie:
Met betrekking tot het gebruik van deze standaard zijn geen verdere overall gegevens bekend.

3.27 Webrichtlijnen (toegankelijkheid websites)

Kern van de Webrichtlijnen is een set van 22 richtlijnen. Deze benoemen de eisen die moeten worden gesteld om een toegankelijke en kwalitatief hoogwaardige website te realiseren. De handleiding geeft aan hoe webbouwers deze eisen concreet kunnen toepassen en hoe opdrachtgevers de eisen kunnen controleren. Verder is er een automatische toets beschikbaar waarmee gedeeltelijk kan worden gecontroleerd in welke mate een webpagina aan de eisen voldoet. De Webrichtlijnen zijn opgesteld in opdracht van het Ministerie van Binnenlandse Zaken en Koninkrijksrelaties. Ze bouwen voort op de algemeen bekende webstandaarden en op de toegankelijkheidsrichtlijnen van het W3C (World Wide Web Consortium).

standaard	*op lijst sinds*	*gebruik door overheden (%)*	*ontwikkeling in gebruik*
Webrichtlijnen	apr 2007 (v1), juni 2011 (v2)	15 getoetste websites voldoen aan Webrichtlijnen v2 niveau AA of aan WCAG 2.0 niveau AA	sterke daling

Voor de Webrichtlijnen is de meest zekere indicator voor het voldoen aan de standaard het behalen van een certificering (waarmerk) bij de Stichting drempelvrij.nl[37]. Sinds april 2013 kan voor Webrichtlijnen versie 2 een waarmerk worden behaald. Een waarmerk voor Webrichtlijnen v1 is niet meer te verkrijgen en alle betreffende certificaten zijn inmiddels verlopen. Van de 635 domeinnamen[38] is in de zomer 2016 nagegaan welke daarvan waarmerkdrager zijn, zie onderstaande tabel.

[37] Zie www.drempelvrij.nl/waarmerkdragers/waarmerk-behaald.
[38] Bij de vorige metingen: 660 in 2013 en 648 in 2014.

Tabel 13: Websites met Waarmerk Drempelvrij (Webrichtlijnen) [39]
Bron: Stichting drempelvrij.nl)

Webrichtlijnen *Gechecked: zomer 2013, zomer 2014, en zomer 2015*	Rijk + Uitvoerings-organisaties / ZBO's + OOV + eOverheid			Gemeenten			Provincies			Waterschappen			**Totaal**			
	2014	*2015*	*2016*	*2014*	*2015*	*2016*	*2014*	*2015*	*2016*	*2014*	*2015*	*2016*	*2013*	*2014*	*2015*	*2016*
Webrichtlijnen v2 / niveau AA: volledig (groen, 3 ster)	*5*	*7*	*5* [40]	*27*	*22*	*7*	*0*	*1*	*1*	*0*	*2*	**0**	**1**	**32**	**32**	**13**
WCAG 2.0 niveau AA (groen, 2 ster)	1	2	1	4	1	1	0	0	0	0	0	**0**	**0**	**5**	**3**	**2**
Webrichtlijnen v2 / niveau A (groen, geen ster)	1	1	1	1	1	0	0	0	0	0	0	**0**	**0**	**2**	**2**	**1**
Webrichtlijnen v1 / volledig (95 ptn = groen, 3 ster)	3	1	**-**	17	2	-	2	0	**-**	0	0	**-**	**40**	**22**	**3**	**-**
Toegankelijkheid / prio 1+2 (≥ 46 ptn = groen, 2 ster)	1	0	-	7	0	-	0	0	-	1	0	-	**9**	**9**	**0**	**-**
Toegankelijkheid / prio 1 (≥ 16 ptn = groen, geen ster)	0	0	-	13	3	-	0	0	-	1	0	-	**57**	**14**	**3**	**-**
Voldoet deels, 'Goed op weg' (oranje)	1	4	0	4	15	2	0	0	0	0	0	**1**	**6**	**5**	**19**	**1**
subtotaal	*12*	*15*	*7*	*73*	*44*	*10*	*2*	*1*	*1*	*2*	*2*	***1***	***113***	***89***	***62***	***17***
Voldoen niet, of zijn (nog) niet getoetst	170	167	…	337	351	…	13	14	..	27	27	..	**547**	**559**	**573**	**603**
totaal	***185***	***179***	***…***	***428***	***424***	***…***	***16***	***16***	***..***	***31***	***29***	***..***	***660***	***648***	***635***	***620***

Er lijkt weinig interesse is in het behalen of verlengen van een waarmerk Drempelvrij. Het afgelopen jaar heeft de Rijksoverheid geen promotie meer gemaakt voor de Webrichtlijnen en ook de website van Webrichtlijnen offline gehaald, vooruit lopend op vervanging van de Webrichtlijnen[41]. Twee Europese richtlijnen schrijven in feite de EN 301 549 standaard voor, welke inhoudelijk gelijk is aan de WCAG 2.0. De WCAG 2.0 is op zijn beurt weer bron geweest voor de Nederlandse Webrichtlijnen, uitgebreid met een onderdeel over herbruikbaarheid van webcontent.

Het valt de onderzoekers op dat er ook bijna geen organisaties zijn die een waarmerk Drempelvrij hebben gehaald voor de WCAG 2.0. Het voldoen aan (de Europese vertaling van) deze standaard zal naar alle verwachting verplicht worden voor nieuwe en bestaande websites en applicaties van de overheid[42].

Bij het toekennen van het waarmerk kunnen enkele kanttekeningen worden geplaatst. Zo is het waarmerken altijd een momentopname, en op basis van een steekproef van willekeurige pagina's op de website, en de voorpagina. Wanneer nieuwe content toegevoegd wordt, kan het zijn dat deze niet conform de toegankelijkheidseisen is. Daarnaast kunnen websites in zijn geheel vervangen of aangepast worden waarbij het waarmerk gedateerd raakt. Tenslotte kan een website ook aan de norm van de standaard Webrichtlijnen voldoen zonder dat deze getoetst is voor het Waarmerk van de Stichting drempelvrij.nl.

[39] Omwille van de vergelijkbaarheid met voorgaande metingen is deze tabel gebaseerd op de cijfers van het Drempelvrij-waarmerkregister en niet op die van webrichtlijnen.nl.
[40] Naast de 6 (5+1) websites die hier bij Rijk (incl. andere partijen) staan, zijn er nog 12 sites in opdracht van de Rijksoverheid gemaakt en vijf sites van de Tweede Kamer die aan de Webrichtlijnen voldoen.
[41] https://www.digitoegankelijk.nl/beleid/inhoud/veranderingen-beleid
[42] http://eur-lex.europa.eu/legal-content/NL/TXT/?uri=CELEX:52016AG0013(01)#text

Nog een kanttekening bij de gevolgde aanpak en de interpretatie van de uitkomst. De gevolgde methode (testen op conformiteit aan de norm) geeft een goed beeld van de mate van doelbereiking maar minder van de intrinsieke adoptie. Data die inzicht bieden in de mate van adoptie zijn echter nog niet voorhanden.

Conclusie:
Het aantal 'waarmerkdragers' van Webrichtlijnen wordt minder; er is sprake van een flinke terugloop in de toepassing (of in ieder geval bewijsbaarheid) van voldoen aan Webrichtlijnen. Mogelijk is dit een gevolg van een vooruitlopen op vervanging van de Webrichtlijnen, maar dit is verre van zeker; er is niet te zien dat er geanticipeerd wordt op voldoen aan de nieuwe richtlijnen.

3.28 XBRL en Dimensions (financiële gegevens)

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

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

Standard Business Reporting (SBR) is de nationale standaard voor digitale uitwisseling van bedrijfsmatige rapportages. SBR wordt gebruikt voor het samenstellen, uitwisselen en verwerken van (financiële) rapportages in de publieke en private sector. Als basis voor het versturen van SBR-berichten wordt de internationale standaard XBRL gebruikt.

De SBR-roadmap[43] heeft als primair doel om voor alle betrokken partijen helder te krijgen welke activiteiten cruciaal zijn om dit publiek-private samenwerkingsverband echt tot een breed en doorslaand succes te maken, en in welk tempo een en ander vorm kan krijgen. Doordat de partijen zich daaraan committeren, ontstaat een gemeenschappelijke agenda voor de komende jaren en daarmee ook een basis van onderling vertrouwen. Dat kan een extra impuls aan het SBR-programma geven.

In de afgelopen jaren zijn belangrijke vorderingen geboekt en is een breed draagvlak gecreëerd voor SBR als dé rapportagestandaard voor gestructureerd digitaal gegevensverkeer. SBR is daarmee een (grootschalig) werkende oplossing en "proven technology". Door SBR breed in te gaan zetten wordt bereikt dat een ondernemer minder tijd hoeft te besteden aan zaken als administreren en rapporteren, en daardoor des te meer datgene kan doen dat hij wil en moet doen: ondernemen. Daarnaast kan via SBR de digitale dienstverlening vanuit de overheid richting ondernemend Nederland verbeteren. Daarmee past de roadmap ook naadloos in de kabinetsagenda. Binnen het (semi)overheidsdomein wordt gebruik gemaakt van SBR bij de Belastingdienst, de Kamer van Koophandel (KvK), het Centraal Bureau voor de Statistiek (CBS) en de Dienst Uitvoering Onderwijs (DUO)[44].

De concrete vorderingen zijn het meest evident bij aangiftes die ondernemingen en instellingen doen bij de Belastingdienst. Het aantal SBR-berichten richting Belastingdienst beloopt al vele miljoenen per jaar en dat aantal blijft alleen maar stijgen. De overgang op SBR is soepel verlopen, zowel aan de kant van de Belastingdienst als aan de kant van de ondernemers en hun intermediairs.

[43] *Roadmap SBR op weg naar 2020, 2e herijkte versie,* 19 juli 2016. Deze versie bouwt voort op de 1e herijkte versie d.d. 3 juli 2015 en de initiële SBR Roadmap d.d. juli 2014. De roadmap wordt in deze paragraaf als bron gebruikt, aangevuld met cijfers die vanuit Logius zijn aangeleverd.
[44] Naast deze (semi)overheidsinstellingen wordt nog een categorie gebruikers onderscheiden: een drietal grootbanken, specifiek gericht op het digitaliseren van de processen rond aanvragen en het beheer van zakelijke kredieten. Deze banken zijn naar verluidt klaar voor het ontvangen van kredietrapportages via SBR.

Bij de Kamer van Koophandel is SBR in een vergevorderd stadium. Vele tienduizenden jaarrekeningen worden nu jaarlijks via SBR ontvangen. Ook daar loopt de overgang soepel. Er wordt hard aan gewerkt om vanaf 2017 van SBR het enige nog toegestane aanlever-kanaal te maken. In dat licht heeft de Nederlandse Beroepsorganisatie voor Accountants (NBA) al verregaande stappen gezet om de accountantsverklaringen voortaan in SBR-formaat te kunnen afgeven.

De berichtenstroom van het CBS via SBR is voorzichtig op gang gekomen. Verder zijn drie grootbanken helemaal klaar voor het ontvangen van kredietrapportages via SBR en wordt SBR vanaf 2017 de standaard. Van groot belang is dat ook richting banken de aantallen SBR-berichten gaan toenemen. Ook het ministerie OCW/DUO is aangesloten op SBR. Naast de sectoren MBO, HBO en WO leveren ook de sectoren Primair Onderwijs en Voortgezet Onderwijs via SBR aan. Aanlevering door de instellingen zal grotendeels geschieden via een portaal. De planning is om in 2016 de mogelijkheid tot system-to-system aanleveren open te stellen.

In onderstaande tabel aantallen over de omvang van de berichtenstroom via Belastingdienst, KvK en CBS. Het aantal jaarrekeningen dat tussen juni 2016 t/m september 2016 in XBRL aan DUO is aangeleverd bedraagt ca. 1.600.

Tabel 14: Overzicht berichtenstroom [45]
(bron: Logius)

		2013	2014	2015	2016 *
Belastingdienst	Aangifte inkomstenbelasting en vennootschapsbelasting	3.198.841	7.097.378	10.393.408	8.442.189
	Aangifte omzetbelasting en opgaaf intracommunautaire prestaties	370.922	2.729.865	3.725.467	2.827.659
	Toeslagen		18.489	374.464	647.985
	Loonheffing **		28	729	967
	Machtigen	484.399	6.993.434	6.424.844	3.947.560
Kamer van Koophandel	Deponeren Jaarverantwoording	27.812	106.730	175.581	152.000
CBS	Statistiekopgaven	-	-	-	92
Totaal		**4.082.066**	**16.946.018**	**21.094.503**	**16.018.452**

** 2016 tot en met augustus*
*** Momenteel alleen verklaringen UZGB*

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

Het toenemende draagvlak blijkt ook uit het feit dat er tal van (publieke en private) partijen zeer geïnteresseerd zijn om toe te treden tot het SBR-samenwerkingsverband.

Conclusie:
Het gebruik van deze standaard is groeiende.

[45] Cijfers hebben betrekking op de omvang van berichtenverkeer; dit is niet gelijk aan het aantal aangesloten organisaties, hoewel tussen beide variabelen wel een verband bestaat.

4 Toepassing open standaarden via generieke 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 generieke 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 generieke voorzieningen (36 in totaal) voldoen aan de relevante open standaarden[46]. Hiervoor zijn enerzijds 27 voorzieningen onderzocht die samen de GDI (Generieke Digitale Infrastructuur) vormen[47]. Anderzijds zijn dit jaar ook 9 (andere) voorzieningen die vorig jaar zijn onderzocht nogmaals onderzocht[48]. Dit deel-onderzoek is uitgevoerd door Piet Hein Minnecré en Florian Henning van PBLQ.

Het gaat om de volgende 27 voorzieningen:

Generieke Digitale Infrastructuur:

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

Andere voorzieningen:

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

Ten opzichte van het onderzoek van de vorige monitor uit 2015 zijn dit jaar volgende voorzieningen niet meegenomen:

- Digikoppeling
- Ondernemingsdossier
- ON2013
- OT2010

De reden hiervoor is dat het Ondernemingsdossier in 2017 gestopt zal worden, Digikoppeling als standaard op de lijst staat en niet langer als voorziening gezien wordt, en dat ON2013 en OT2010 raamovereenkomsten zijn die met leveranciers eenmalig vastgesteld zijn. Er zijn na vaststelling geen wijzigingen meer te rapporteren.

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

[46] Zie ook EAR Online, voor een overzicht van voorzieningen geordend naar informatiseringsdomeinen.
[47] 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.
[48] Namelijk: ODC Noord, Digi-Inkoop, Doc-Direct, DWR, P-Direct, Rijksoverheid.nl, Rijkspas, Rijksportaal en TenderNed.

Werkwijze

Voor dit onderzoek is gebruik gemaakt van de 'pas toe of leg uit'-lijst van 8 juli 2016. Per voorziening is gekeken of de standaarden op deze lijst relevant zijn. Daarbij is telkens uitgegaan van de eindgebruiker. Dat is diegene die in de keten baat zou moet hebben bij het gebruik van open standaarden. Dit is expliciet zo gekozen, omdat het beleid van het College Standaardisatie 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. Wanneer er geen sprake is van interoperabiliteit hebben we dat in deze rapportage duidelijk aangegeven.

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

- https://internet.nl - test overzicht van overheidsvoorzieningen op IPv6, DNSSEC,TLS, DKIM en SPF
- http://checkers.eiii.eu/ voor Webrichtlijnen

Hiervan is een overzicht gemaakt dat is toegestuurd aan vertegenwoordigers van de voorzieningen. Op basis van hun reactie is de verzamelde informatie aangescherpt. Het resultaat daarvan is voorgelegd aan de opdrachtgever en vervolgens in een definitieve versie toegestuurd aan de vertegenwoordigers van de voorzieningen en opgenomen in de rapportage. Daar waar er verschillen van mening zijn over het al dan niet voldoen aan de voorzieningen zijn deze verschillen nader met elkaar besproken. In de gevallen waar de verschillen ook na de gesprekken bleven bestaan, is dit duidelijk opgenomen in de rapportage.

Ook dit jaar kostte het veel tijd om de informatie boven tafel te krijgen. Op de voorzieningen van Logius na zijn er weinig partijen die (bijvoorbeeld via hun website of hun jaarverslag) publiceren of en hoe ze aan de lijst met standaarden voldoen. Wel is het zo dat partijen beter dan vorig jaar in staat zijn om de gegevens na navraag snel te leveren. Dat is waarschijnlijk deels te verklaren door de gewenning aan het onderzoek bij zowel de onderzoekers als bij de geïnterviewden. Wij weten wie we moeten hebben, en zij zijn bekend met de vragen, en kennen de weg binnen hun eigen organisatie steeds beter. Daarnaast is onze indruk dat het onderwerp bij een groeiend aantal partijen meer aandacht te krijgen. Ook dit maakt de gesprekken eenvoudiger.

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 onderzoeker toegekend. De status kan de volgende waarden hebben:

Ja:	De voorziening is compliant[49] met de standaard,
Nee:	De voorziening is niet compliant met de standaard,
Deels:	Onderdelen van de voorziening zijn compliant maar niet alle onderdelen[50],
Gepland:	Er zijn concrete plannen (gekoppeld aan een datum) om de voorziening op korte termijn compliant te maken met de standaard.

[49] Met "compliant" wordt in dit onderzoek bedoeld dat de standaard door de eindgebruiker te gebruiken is.
[50] De bedoeling hiervan is dus niet dat een voorziening gedeeltelijk aan een standaard voldoet, maar dat een onderdeel van de voorziening helemaal aan de standaard voldoet. Voor dit onderdeel is dan in feite de status "Ja" van toepassing, maar niet voor de overige onderdelen. Idealiter zouden op termijn alle onderdelen van een voorziening aan de relevante standaard moeten voldoen.

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

Op grond van het College-besluit[51] hanteren we hier als toepassingsgebied van de Webrichtlijnen: websites waarmee overheden communiceren met burgers en/of bedrijven. Omdat de Webrichtlijnen daarnaast ook van waarde kunnen zijn voor overheidsinterne websites (bijv. intranettoepassingen) hebben we in dit onderzoek voor de volledigheid onderzocht of de voorzieningen waarbij (medewerkers van) overheden via een webinterface communiceren met andere overheden ook voldoen aan de Webrichtlijnen. Concreet betekent dit dat we bij Rijksportaal onder de tabel een aanvullende tekst over de Webrichtlijnen hebben opgenomen.

De BIR en ISO 27001/2

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

TLS

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

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

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

4.2 Essay #1: Van toetsen naar verleiden

Verleg de focus van het 'wat' naar het 'waarom' en het 'hoe'!

Op ons verzoek hebben de onderzoekers van PBLQ - Piet Hein Minnecré en Florian Henning - een essay geschreven. Hoewel dit onderdeel is van de Monitor Open Standaardenbeleid, heeft het een ander karakter. De Monitor richt zich op de kwantitatieve kenmerken van de adoptie van open standaarden, dit essay heeft meer een kwalitatief en explorerend karakter.

Daarbij staan drie vragen centraal:

- Waarom zijn sommige standaarden minder eenvoudig te adopteren dan andere?
- Waarom is het voor de ene voorziening makkelijker of lastiger dan voor de andere om standaarden te adopteren?
- Wat betekent dit voor mogelijke maatregelen die het Forum Standaardisatie kan nemen?

[51] In het College-besluit over de opname van de Webrichtlijnen is een aparte paragraaf opgenomen waarin het toepassingsgebied verder toegelicht en uitgewerkt wordt. Zie https://www.forumstandaardisatie.nl/standaard/webrichtlijnen.

Het essay is samengesteld op basis van de resultaten uit een enquête die onder de beheerders van de GDI-voorzieningen is uitgezet, de resultaten van de Monitor zelf, en een viertal gesprekken met beheerders van voorzieningen. De informatie die daaruit voorkomt is aan de hand de eigen expertise en ervaring met en onderzoeken naar de adoptie van standaarden geduid.

Sommige standaarden zijn lastiger dan andere

De oorspronkelijke vraag voor dit essay was om te onderzoeken of sommige standaarden (op basis van de resultaten van de Monitor) minder eenvoudig te adopteren blijken dan andere.

Het antwoord op deze vraag is ja, maar het gaat slechts om een beperkt aantal standaarden. Standaarden die voor een groot aantal voorzieningen lastig te implementeren blijken, zijn IPv6 en in mindere mate DNSSEC en de Webrichtlijnen. Uit gesprekken met beheerders van voorzieningen en uit de toelichting die bij beantwoording van de vragen uit de Monitor wordt gegeven komen vrij eenduidige verklaringen hiervoor. Voor de implementatie van DNSSEC en IPv6 zijn de beheerders van de voorzieningen afhankelijk van de leveranciers van het netwerk, in veel gevallen SSC-ICT. Dit bleek ook al uit eerdere onderzoeken.

Voor de Webrichtlijnen geldt dat het lastig is te voldoen aan de standaard doordat de standaard complex is (veel elementen kent), en de toetsing ook de nodige energie vergt. Daarnaast stellen de Webrichtlijnen eisen aan de inhoud van een website, en in de praktijk wordt deze vaak geleverd door andere partijen dan de beheerder van de website. Veel partijen hanteren de Webrichtlijnen wel degelijk als richtlijnen, maar vinden het niet noodzakelijk om er honderd procent aan te voldoen en dit te laten toetsen. Bij de Webrichtlijnen zie je dat in sommige gevallen wel in de geest gehandeld wordt, maar niet volgens de letter. De vraag is in hoeverre dit onwenselijk is, wellicht is het beter te kijken of de toetsing eenvoudiger te maken is.

Een belangrijke verklaring voor het verschil in de adoptie van standaarden is het verschil in de **perceptie van het belang en nut van standaarden**, zeker wanneer dit beoordeeld wordt ten opzichte van de kosten van implementatie. Veel beheerpartijen zien de internetbeveiligingsstandaarden als noodzaak, terwijl standaarden als ODF meer als een "extra" gezien worden, waarvan de urgentie niet gevoeld wordt. Voor partijen is niet helder welk probleem met de standaard wordt opgelost, partijen verwarren gebruik van de standaard met het gebruik van open source software en/of partijen beschouwen het geheel niet als hun probleem. De Microsoft DOCX standaard voldoet voor veel partijen prima, sterker nog: een overstap op ODF zou de interoperabiliteit met andere organisaties laten dalen.

Beheersorganisaties van voorzieningen geven aan dat het een sterk ondersteunende factor is als **standaardisatie past bij de missie of organisatiedoelstellingen** (openheid, samenwerken, voor ketenpartners etc.) en als dit ook in de organisatie naar een beleid is vertaald. Dit effect wordt versterkt door zogenaamde 'champions' die een centrale rol hebben en als ambassadeurs voor dit beleid fungeren.

Daarnaast blijkt tijd een belangrijke factor te zijn. Standaarden die relatief nieuw op de lijst staan, zijn vaak nog iets minder breed geïmplementeerd. Het kost beheerorganisaties tijd om standaarden daadwerkelijk te implementeren, en de periode tussen het landen van een standaard op de lijst en de daadwerkelijke implementatie kan jaren duren. Dat lijkt vooral te maken te hebben met **natuurlijke vervangings- en/of doorontwikkelingsprocessen bij voorzieningen**. Een gerelateerd punt is dat van de nieuwe 'relevante' standaarden in veel gevallen aangegeven wordt dat de implementatie nog wordt onderzocht of gepland. Partijen lijken het lastig te vinden om te bepalen of ze wat moeten met de standaard en zo ja, wat en wanneer. De vraag of het echt relevant is, is voor hen vaak lastig te bepalen. Het blijkt dat er vaak **te weinig deskundigen** zijn in de organisaties die dit goed kunnen beoordelen.

Samenvattend kunnen we stellen dat slechts een paar standaarden daadwerkelijk lastig implementeerbaar lijken, en dat voorzieningen daar vaak aannemelijke redenen voor opvoeren. In dit

soort gevallen kan verdere adoptie niet alleen worden geholpen door beheerders van voorzieningen hierop aan te spreken, maar is een bredere ketenaanpak vereist (zoals in het geval van IPv6). Daarbij moet nog eens goed worden gekeken naar de inhoud en het compliancemodel van de standaard (zoals in het geval van de Webrichtlijnen). Ten aanzien van dat tweede punt is er nog een onderscheid aan te brengen, namelijk de verdeling van het 'wat' (waaraan je moet voldoen) en het 'wie' (wie moet er aan voldoen). Toetsing van waaraan je moet voldoen is een zaak van de beheerder van de standaard. Die kan, bijvoorbeeld in het geval van de Webrichtlijnen, kijken of de toetsing laagdrempeliger in te richten is. Wie moet voldoen is een ander verhaal. Een voorbeeld hiervan is bijvoorbeeld de PDF standaard. Zo bestaat in dat geval vaker interpretatieverschil of met compliance is bedoeld dat een voorziening, zoals een portaal, alle eigen documenten aan een standaard laat voldoen, of ook de van derde partijen op het portaal geplaatste documenten hieronder vallen. In het laatste geval moet helder zijn wie hierop wordt aangesproken; de voorziening (omdat ze het niet afdwingen) of de derde partijen, die eigenlijk zelf hun documenten in PDF moeten aanleveren. Hierover zou het Forum meer duidelijkheid kunnen verschaffen.

Sommige voorzieningen vinden het makkelijker dan andere

Wie op een andere manier naar de tabel uit de Monitor kijkt, kan concluderen dat er voorzieningen zijn waarvoor de adoptie van standaarden makkelijker blijkt dan voor andere. Dat roept de vraag op hoe dit komt. Waarom is het voor de ene voorziening makkelijker of lastiger dan voor de andere, of wat doet de ene voorziening beter of slechter dan de andere? Uit de gesprekken komen bepalende factoren naar boven die we hier op een rij zetten.

Besef van het belang van open standaarden

Voorzieningen geven aan dat open standaarden steeds belangrijker worden in hun praktijk. Bij alle voorzieningen is de lijst met standaarden goed bekend en men geeft ook aan er rekening mee te houden.

Tegelijkertijd geeft men aan dat dit besef niet altijd bij iedereen aanwezig is. Zo stellen vijfentwintig procent van de deelnemende beheerorganisaties in de enquête dat opdrachtgevers "veel aandacht" aan open standaarden geven. Negen procent geeft aan dat hun opdrachtgever "nauwelijks aandacht" aan de adoptie van standaarden geeft. De voorzieningen geven ook aan dat de perceptie van het nut van open standaarden beperkt is. Men heeft wel gehoord dat het goed is, maar het is niet echt helder waar open standaarden aan bijdragen. Dat geldt zowel voor concrete voordelen, als voor de bijdrage die open standaarden leveren in brede zin, bijvoorbeeld aan het faciliteren van steeds toenemende ketensamenwerking of van transparantie door bijvoorbeeld open data en open overheid.

Ook bij de afnemers van voorzieningen blijkt niet altijd voldoende besef van de relevantie van standaarden te zijn. Zo geven in de enquête weliswaar 58 procent van de deelnemende beheerorganisaties aan dat hun afnemers open standaarden "enigszins" of "zeer" relevant vinden, maar daar tegenover staan wel 25% die vinden dat hun afnemers die "nauwelijks relevant" vinden.

Sturing op en beleid van de voorziening

Gelet op bovenstaande zal het niet verbazen dat het sturen vanuit opdrachtgevers op het gebruik van open standaarden beperkt is bij de meeste voorzieningen. Een voorbeeld van een organisatie die dat goed doet is Logius. Weliswaar is zij zelf geen opdrachtgever van de voorzieningen, maar er wordt wel centraal ingezet op het gebruik van de standaarden van de lijst. Deze aandacht van de directie van Logius blijkt voor voorzieningen een belangrijke drijfveer voor het gebruik van standaarden te zijn.

Bij voorzieningen waar het goed gaat met de adoptie van standaarden zien we dan ook vaak dat de opdrachtgever (bijvoorbeeld in het geval van Rijksoverheid.nl) belang hecht aan het gebruik van

standaarden. Tevens zien we dan dat standaarden ook in het beleid zijn opgenomen, terugkomen in de architectuur, en uiteindelijk hun weg vinden in het ontwerp en de verwerving.

Een belangrijke rem bij de adoptie van standaarden in voorzieningen is dat in de sturing op voorzieningen de samenhang ontbreekt. Er wordt te weinig in een totaalplaat (van de GDI-voorzieningen) gedacht. Zo zijn verantwoordelijkheden en budgetten versnipperd over veel voorzieningen en zijn er te veel afhankelijkheden van veel verschillende gremia. Infrastructuur en standaardisatie leggen het door de decentrale sturing af tegen verbetering van afzonderlijke voorzieningen. Er kan meer samenhang gecreëerd worden door de brede infrastructuur van voorzieningen meer in samenhang te ontwerpen, te ontwikkelen en te financieren.

Tegelijkertijd wordt aangegeven dat de aandacht voor standaarden niet alleen via deze formele lijnen tot stand komt. Er bestaat ook een informele lijn die grotendeels wordt bepaald door 'innovatoren' (met name architecten, technisch en proces specialisten). In deze lijn worden keuzes ten aanzien van standaarden gemaakt op basis van meritocratie. Deze 'innovatoren' zijn vaak de mensen in de uitvoeringsteams die een goed zicht hebben op wat er speelt en relevant is in de context van een organisatie. Zij spelen het spel op basis van hun eigen kennis en kunnen hiermee juist wel of juist niet bijdragen aan het succes van open standaarden. Het is vaak in het samenspel van deze mensen dat de keuzes worden gemaakt. De huidige instrumenten van het Forum, en dan vooral de Lijsten stuiten vaak op weerstand binnen deze groep, mede door de gedachte dat zij zelf beter geïnformeerd zijn dat het Forum. Dat kan een terechte gedachte zijn of niet, in beide gevallen is het nuttig voor zowel het Forum als de voorziening om het gesprek over het nut van relevante standaarden in een bredere groep experts te voeren. Tegenspraak is immers voor beide partijen een must.

De businesscase en de financiering

In de enquête geven beheersorganisaties aan dat ze aan de standaarden voldoen "waar mogelijk", maar ook dat dit "niet ten koste van alles" wordt gedaan. Er worden "prioriteitskeuzen" gemaakt. Een reden hiervoor, die in zowel de enquête als in de gesprekken veel terugkomt, is het geld dat beschikbaar moet zijn om open standaarden te implementeren. Budgetten hiervoor zijn vaak erg krap, en ruimte voor niet direct essentiële wijzigingen is dus beperkt.

En in dat niet direct essentiële zit vaak de crux. Bij de implementatie van standaarden vallen de kosten en baten zelden op dezelfde plek, of landen de baten pas veel later in de tijd terwijl de kosten zich nu direct aandienen. Dergelijke investeringen vergen dus een vooruitziende blik en een helder beeld van het overkoepelend belang.

Een treffend voorbeeld hiervan kwam voort uit een gesprek met één van de beheerders van voorzieningen. Daarin werd aangegeven dat de voorziening standaard tarieven hanteert voor haar dienstverlening. Gebruikers nemen naar gelang hun behoefte één of meerdere producten af tegen die tarieven. De totale rekening voor alle gebruikers en voor alle producten is immens, maar voor individuele afnemers gaat het telkens om zeer beperkte bedragen. Vernieuwing (met daarbij de invoering van open standaarden) om op termijn kosten omlaag te brengen is daarmee geen issue. Dat is het ook niet voor de opdrachtgever. De rekening wordt immers door de afnemers betaald.

Een gerelateerd punt is dat beheerorganisaties ook aangeven behoefte te hebben aan een soort roadmap over standaardenbeleid, waaruit duidelijk wordt welke verplichtingen (bijvoorbeeld domeinen of toepassingsgebieden) er aankomen.

Een oplossing zou zijn om beter duidelijk te maken hoe standaarden aansluiten op primaire drijfveren en doelen van organisaties, zoals vindbaarheid, openheid, en bereikbaarheid. Hierdoor kun je bereiken dat standaardisatie niet als een verplichting, maar als verantwoordelijkheid gezien wordt. In beheerorganisaties waar deze cultuur gevestigd is, wordt aangegeven dat dit besef de verantwoordelijke spelers de nodige motivatie geeft om het standaardisatiebeleid intern ook vorm te geven en toe te passen.

De voorziening zelf en haar omgeving

Beheerders van voorzieningen zijn in sterke mate afhankelijk van hun omgeving en andere spelers daarin. Dit heeft ook belangrijke gevolgen voor standaardisatie. Met name kleinere partijen hebben vaak weinig invloed op de andere spelers in hun ecosysteem en moeten de bewegingen daarin gewoon volgen. Dit geldt onder meer in de hierboven beschreven voorbeelden van minder eenvoudig te adopteren standaarden zoals IPv6.

Daarnaast geldt voor een aantal voorzieningen dat zij werken op basis van oude protocollen en daar ook moeilijk van af komen. Een complicerende factor voor voorzieningen is dat niet alleen zij op basis van oude protocollen werken, maar in de loop der jaren ook hun afnemers hebben overtuigd om hiermee te werken. Het belang van vernieuwingen en verbeteringen (waaronder de invoering van open standaarden) wordt misschien nog wel gezien, maar de gevraagde verandering kan (soms grote) investeringen vragen en brengt vaak ook risico's met zich mee. 'En het werkt nu toch ook?'

Het is dus belangrijk dat ook de gebruikers de nodige kennis in huis hebben en het belang onderkennen. Waar bijvoorbeeld trainingen gegeven worden over standaarden, is te zien dat de gebruikers van een voorziening ook sterker mee kunnen gaan in het invullen van het standaardisatiebeleid. Een voorbeeld daarvan is terug te vinden bij Rijksoverheid.nl, waar op het gebied van de Webrichtlijnen, maar ook ten aanzien van overige aspecten die raken aan de content, cursussen voor gebruikers worden georganiseerd. Dit zal natuurlijk niet bij alle voorzieningen mogelijk blijken of van toepassing zijn, maar het duidt wel op een mindset waarin de voorziening zich daadwerkelijk bezig houdt met het managen van haar omgeving.

Ook binnenshuis, bij de beheersorganisaties, is deze expertise belangrijk, en waar beheerorganisaties hierin investeren kan door de kennis in huis te hebben ook beter continuïteit van het standaardisatiebeleid worden geborgd. Het probleem bij veel voorzieningen is namelijk dat ze als project worden opgezet, en binnen dat project ook kennis en capaciteit wordt opgebouwd, maar na afloop weer verdwijnt.

Over de leveranciers van de voorzieningen (in dat geval doelen we op de bouwers, integrators, softwareontwikkelaars) is men eenduidig: deze vormen geen bottleneck voor de adoptie. In principe kan alles gemaakt worden, er hangt echter wel een prijskaartje aan. Hier heeft de opdrachtgever een belangrijke faciliterende en/of stimulerende rol. Als de eigenaar van een voorziening de nodige budgetten beschikbaar maakt, dan kan een leverancier een standaard in principe altijd inbouwen.

Aanbevelingen voor het Forum

Uit de gesprekken met de voorzieningen, maar ook uit de enquête kwamen verschillende aanbevelingen voor het Forum. Wat er duidelijk blijkt is dat de 'pas toe of leg uit' lijst als enig instrument een te beperkt handelsperspectief biedt, en dat aanvullende maatregelen en instrumenten noodzakelijk zijn. Op basis van de aangeleverde informatie van partijen, schetsen we hieronder een aantal aanbevelingen.

Schets het lonkend perspectief

Beter duiden van het nut. Geef een helder beeld waar open standaarden aan bijdragen en welke effecten ermee worden beoogd, zowel in algemene zin als concreet.

Werk daarbij in domeinen of sets van standaarden rond een thema. Toekomstige aandachtsgebieden voor standaardisatie die beheerorganisaties in de enquête noemen zijn o.a. internet & beveiliging, document en web content, uniforme betekenis en schrijfwijze, Europese standaarden, interoperabiliteit tussen (Rijks)overheid en bedrijven, en de geo-standaarden. Daarnaast kan gekeken worden naar brede thema's die momenteel politiek de aandacht zoals het sociaal domein, de Omgevingswet etc.

Maak het haalbaar. Focus niet op alle standaarden tegelijk. Het kan de beheerorganisaties helpen om prioriteringen aan te geven en meer helderheid te geven wat voor hen de relevante standaarden zijn.

Zet in op de spinnen in het web. Voorzieningen die een centrale rol spelen, of die de bulk van de bezoekers zien, kunnen een belangrijke voorbeeldrol als 'champion' spelen.

Geef duidelijk het migratiepad en de tijdslijnen aan: wat moet wanneer bereikt zijn?

Organiseer de verandering. Maak het concreet hoe we dit met elkaar gaan vormgeven, wat gedaan moet worden, wie welke rollen daarbij heeft, en wanneer welke resultaten te verwachten zijn. Breng hierbij politieke belang (druk van boven) en praktijkrelevantie (druk van beneden) bij elkaar om de nodige energie tot verandering tot stand te laten komen .

Geef een roadmap aan. Maak duidelijk wat de beheerorganisaties in de toekomst van het standaardenbeleid kunnen verwachten. Koppel dit duidelijk aan de baten.

Duidelijker aangeven van rollen en verantwoordelijkheden. Help partijen bij het bepalen of ze wat moeten met een standaard en zo ja, wat en wanneer. Geef daarnaast ook helderheid in het (vaak complexe) ecosysteem van spelers in de omgeving van beheersorganisaties. Wijs duidelijk de rollen toe en spreek met partijen helder tijdslijnen en verantwoordelijkheden af.

Zorg dat je aansluit bij waar de keuzes worden gemaakt: dat is niet altijd bij de voorziening zelf

Het is tijd om het bestuurlijk besef weer op te poetsen. Maak bij opdrachtgevers het belang van open standaarden duidelijk, en geef een helder beeld welke middelen het vereist om dit goed te waarborgen.

Wees zichtbaar. Geef het onderwerp standaardisatie meer zichtbaarheid en concentreer je hierbij op de essentiële knooppunten en spelers, bijvoorbeeld door aanwezigheid in de gremia waar keuzes worden gemaakt.

Richt je niet alleen op formele procedures. Zorg dat je ook aanwezig bent in het meer informele circuit van innovatoren. Deels kan het Forum daar een verbindende werking vervullen onder de innovatoren. Tegelijkertijd is het de vraag of je daar een geloofwaardige gesprekspartner of zelfs moderator kan zijn zonder zelf de noodzakelijke inhoudelijke kennis in huis te hebben.

4.3 Overzicht: open standaarden in generieke voorzieningen

In Tabel 15a + 15b zijn de bevindingen over de 36 onderzochte generieke voorzieningen in één overzicht samengebracht. In de paragrafen daarna wordt het beeld van de mate waarin elke voorziening aan de relevante open standaarden voldoet gedetailleerd besproken. Het gaat om de 27 onderzochte GDI-voorzieningen, plus de 9 andere onderzochte voorzieningen (deze laatsten zijn lila gemarkeerd).

Per standaard beschouwd

Van alle 36 open standaarden op de 'pas toe of leg uit'-lijst zijn er 24 relevant voor één of meer generieke voorzieningen. Er zijn 12 open standaarden die voor meer dan 20 voorzieningen relevant zijn: IPv6/IPv4 (relevant voor 32 voorzieningen), TLS en DNSSEC (beide relevant voor 29), NEN-ISO\IEC 27001

en NEN-ISO\IEC 27002 (beide relevant voor 29), SPF (25), Webrichtlijnen v2 (24), PDF/A-1, PDF/A-2 en PDF 1.7 (23) en Digikoppeling 2.0 en DKIM (beide 22).

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 9 standaarden: BWB, e-Factureren, Geo-standaarden, NEN-ISO\IEC 27001, NEN-ISO\IEC 27002, SAML, SETU, WPA2 en XBRL. Een belangrijk deel van deze standaarden staat al vijf jaar of langer op de lijst. Alleen IPv4/IPv6 (13%) scoort relatief laag.

Per voorziening beschouwd

Voor een deel van de voorzieningen zijn relatief veel open standaarden relevant, zoals voor en de NHR (Basisregistratie Handelsregister: 16 standaarden), de basisregistraties BAG, BRK, WOZ en BGT, de BRV, DWR, MijnOverheid, P-Direct en Rijksoverheid.nl (15). Voor andere voorzieningen, zoals Digilevering en Digimelding (5), Diginetwerk (4), en Samenwerkende Catalogi (2) zijn slechts enkele open standaarden relevant. Gemiddeld zijn voor een voorziening bijna 11 open standaarden relevant (vorig jaar – toen zijn meer voorzieningen onderzocht maar stonden er minder open standaarden op de lijst – waren dat er 9).

In de meeste gevallen voldoen deze voorzieningen ook aan de relevante open standaarden: in 387 gevallen (combinaties van voorziening en relevante standaard) is een standaard van de lijst relevant, in 232 gevallen (60%, vorig jaar 62%) voldoet de voorziening daar aan en in 96 gevallen (25%, vorig jaar was dat nog 19%) voldoet de voorziening daar deels aan of is dat gepland. In 59 gevallen (15%, vorig jaar 19%) voldoet de voorziening op dit moment nog niet aan een relevante open standaard.

Bekijken we de voorzieningen apart, dan blijkt dat twee voorzieningen voldoen aan alle relevante standaarden: Afsprakenstelsel Elektronische Toegangsdiensten (10 standaarden) en Samenwerkende Catalogi (2 standaarden). Daarnaast zijn er 9 voorzieningen die aan alle standaarden ofwel voldoen, danwel deels voldoen danwel concrete plannen hebben om daar op korte termijn aan te gaan voldoen.

Voor 11 van de 36 onderzochte voorzieningen geldt dus, dat zij aan alle standaarden voldoen, deels voldoen of gepland hebben daar op korte termijn aan te gaan voldoen. Dit zijn met name voorzieningen die deel uitmaken van de Generieke Digitale Infrastructuur: het gaat om 10 van de 27 onderzochte GDI-voorzieningen. Er zijn dit jaar geen voorzieningen die aan minder dan de helft van de standaarden voldoen, deels voldoen of dat hebben gepland (vorig jaar waren dat er nog twee).

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 15a: Toepassing open standaarden in 36 voorzieningen

V = voldoet *D = voldoet deels* *G = gepland* *N = voldoet niet* *(leeg = n.v.t.)*	BAG, BRK, WOZ en BGT	Berichtenbox bedrijven	BRI (inkomen)	BRT (topografie)	BRV (voertuigen)	BSN Beheervz + GBA-V	DigiD	DigiD Machtigen	Digi-Inkoop	Digilevering	Digimelding	Diginetwerk	DigiPoort/OTP	DigiPoort/PI	Dig. Werkomgeving Rijk	Doc-Direct
aantal relevante OSn:	*60*	*12*	*7*	*7*	*15*	*12*	*11*	*12*	*11*	*5*	*5*	*4*	*7*	*10*	*15*	*14*
Sinds 2008 op lijst																
NEN-ISO\IEC 27001+2	V		V	V	V	V	V	V	V			V	V	V	V	V
PDF/A-1	D	V			V			V	V						V	V
StUF	V	V				N										
Sinds 2009 op lijst																
SETU									V					V		
SAML		V			G		V	D							V	V
PDF 1.7	D	V			V			V	V						V	V
Sinds 2010 op lijst																
XBRL en Dimensions														V		
E-portfolio NL																
Aquo-standaard																
IPv6 en IPv4	G	N			N	N	D	V	N	G	G	N	G	V	N	N
OAI-PMH																
Sinds 2011 op lijst																
NL LOM																
Webrichtlijnen v2	G	G		V	D		V	V							V	
OWMS				N	V											
IFC																
STOSAG																
Sinds 2012 op lijst																
DNSSEC	V	N			V		D	V	V	G	G	V	G	N	D	
DKIM	G	V					V			G	G			V	D	V
ODF 1.2 (+ PNG/JPEG)															V	N
PDF/A-2	D	V			V			V	V						V	V
Sinds 2013 op lijst																
Digikoppeling 2.0	V	V	V		D	G	N	D		V	V		G	V	D	N
e-Factureren									V							
BWB																
ECLI																
EMN NL																
JCDR																
Sinds 2014 op lijst																
WDO Datamodel																
TLS	G	V	V	V	D	V	V	V	G				N	V	V	N
CMIS			V		N											N
Geo-standaarden	V			V												
SIKB 0101 v11																
VISI 1.4																
Sinds 2015 op lijst																
SKOS	D		N	V	N		V									N
SPF	G	N			V		V	V	N	N	N		N	N	D	N
WPA2			V												V	

Tabel 15b: Toepassing open standaarden in 36 voorzieningen

V = voldoet *D = voldoet deels* *G = gepland* *N = voldoet niet* *(leeg = n.v.t.)*	Afsprakenstelsel ETD	e-Factureren	MijnOverheid	NHR (Nieuw HandelsReg.)	ODC Noord	Ondernemersplein	Overheid.nl	P-Direct	PKI Overheid	Rijksoverheid.nl	Rijkspas	Rijksportaal	Samenwerkende Catalogi	SBR (Standard Bus. Rep.)	Stelselcatalogus	TenderNed
aantal relevante OSn:	*10*	*10*	*15*	*16*	*14*	*12*	*12*	*15*	*10*	*15*	*9*	*7*	*2*	*11*	*10*	*12*
Sinds 2008 op lijst																
NEN-ISO\IEC 27001+2	V	V	V	V	G	V	V	V	V	V	V					V
PDF/A-1	V	V	D	V	D		V	D	V	D		V		V	V	V
StUF			V	V												
Sinds 2009 op lijst																
SETU																
SAML	V		V	V	N			V		V	V	V				V
PDF 1.7	V	V	D	V	D		V	D	V	D		V		V	V	V
Sinds 2010 op lijst																
XBRL en Dimensions														V		
E-portfolio NL																
Aquo-standaard																
IPv6 en IPv4		N	N	N	D	V	G	N	D	V	N	G		D	G	N
OAI-PMH																
Sinds 2011 op lijst																
NL LOM																
Webrichtlijnen v2	V	N	D	D	D	G	G	N	V	V			V	N	V	V
OWMS			D		N	N	V		V	V		N	V		V	
IFC																
STOSAG																
Sinds 2012 op lijst																
DNSSEC	V	N	V	G	V	N	V	N	V	V	N			N	G	N
DKIM			V	V	G	N	G	V		V	N			V	G	N
ODF 1.2 (+PNG?JPEG)					V			N		V		V				
PDF/A-2	V	V	D	V	D		V	D	V	D		V		V	V	V
Sinds 2013 op lijst																
Digikoppeling 2.0			D	V				V			V			V		
e-Factureren		V														
BWB						V		V		V					V	
ECLI																
EMN NL																
JCDR																
Sinds 2014 op lijst																
WDO Datamodel																
TLS	V		V	V	V	G	V	V	V	V	V			V		V
CMIS				D		V										
Geo-standaarden																
SIKB 0101 v11																
VISI 1.4																
Sinds 2015 op lijst																
SKOS				N		N	V								V	
SPF	V	N	V	V		N		G		V	N			N		V
WPA2					V											

In de navolgende paragrafen worden de bevindingen voor elk van de generieke voorzieningen, op alfabetische volgorde, meer in detail besproken.

4.4 BAG, BRK, WOZ en BGT

Het Kadaster is de beherende partij voor deze vier basisregistraties. Het Kadaster heeft in één interview de standaarden voor allevier de voorzieningen beschreven. Het gaat om de volgende basisregistraties:

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

Standaard	Status	Toelichting
Digikoppeling	Ja	Vrijwel alle koppelingen met afnemers, andere basisregistraties en evt. front-office systemen worden gelegd op basis van Digikoppeling: - de koppelingen voor het aanleveren van gegevens aan LV-BAG, LV-WOZ en LV-BGT zijn gebaseerd op Digikoppeling standaarden; - het aanleveren door bronhouders (o.a. notariaat) van gegevens aan de BRK is niet gebaseerd op Digikoppeling; - de koppelingen voor het verkrijgen van informatie van gegevens uit LV BAG en LV WOZ en BRK zijn gebaseerd op Digikoppeling. Daarnaast kan informatie uit LV's worden verkregen via PDOK (Publieke Dienstverlening op de Kaart) die gebruik maakt van de Open GEO-standaarden. Ook de informatie uit de BRT wordt op deze wijze geleverd. Gegevens uit de BGT zijn beschikbaar via PDOK.
DKIM	Gepland	De webshop verstuurt opgevraagde uittreksels ook naar het e-mail adres van de afnemer. Aan de provider is opdracht verstrekt om DKIM te implementeren. Het project t.b.v. de implementatie van DKIM heeft vertraging opgelopen en de implementatie wordt nu verwacht in 2017.
DNSSEC	Ja	De website www.kadaster.nl ondersteunt DNSSEC. (Zie internet.nl)
Geo-Standaarden	Ja	Naast de INSPIRE richtlijnen, maakt het Kadaster gebruik van NEN3610. Alle geo-standaarden zijn verpakt in het interne IMKAD (InformatieModel Kadaster) dat ook de basis is voor de berichtuitwisseling
IPv4 en IPV6	Gepland	Het Kadaster ondersteunt vanaf eind 2016 zowel IPv4 als IPv6[52]. Project daarvoor loopt.
NEN-ISO/IEC 27001/27002	Ja	Het Kadaster is gecertificeerd voor NEN-ISO/IEC 27001 en hanteert 27002. Het Handboek Beveiliging Kadaster is volledig op de BIR gebaseerd. In het jaarverslag is een in control statement opgenomen.
PDF 1.7, PDF/A-1 en PDF/A-2	Deels	Uittreksels worden verstrekt in PDF 1.4-formaat. Databestanden worden vooral in GML uitgewisseld. GML is een standaard XML-formaat voor Geo-data, gebaseerd op de Geo-standaarden. Afnemers melden geen problemen met het huidige formaat. Daarom geeft het Kadaster geen prioriteit aan het vervangen van PDF 1.4. Voor het Archiveren van kennisgevingen wordt gebruik gemaakt van PDF/A-1.
SPF	Gepland	Zie DKIM
StUF	Ja	Het Kadaster maakt deels gebruik van StUF en is deels volgens de Geo-standaarden (GML) opgemaakt. StUF wordt gebruikt voor aanlevering van bronhouder naar LV-BAG, LV-WOZ en LV-BGT. WOZ wordt ook geleverd in StUF. Naar verwachting zal de BGT ook in StUFGEO-IMGEO worden geleverd.
Webrichtlijnen	Gepland	Kadaster.nl voldoet vanaf oktober 2016 (nieuwe release) aan de Webrichtlijnen[53]. Dit wordt vanaf dan wekelijks geautomatiseerd getoetst.

[52] Deze termijn werd door de beheersorganisatie aangegeven, maar was op het tijdpunt van de afronding van dit onderzoek nog niet geïmplementeerd om gecontroleerd te worden.

		De toegankelijkheidsverklaring is aanwezig.
TLS v1.2, v1.1 en v1.0	Gepland	Deze standaard wordt vanaf 1 oktober 2016[54] volledig door het Kadaster ondersteund. Het gaat om de standaard TLS 1.0, TLS 1.1 en 1.2.
SKOS	Deels	Het Kadaster hanteert SKOS voor de beschikbaarstelling van begrippen-kaders van basisregistraties. De begrippenkaders voor de BRK zoals gepubliceerd op brk.kadaster.nl, de BAG zoals gepubliceerd op bag.kadaster.nl en de BGT (IMgeo) en BRT op definities.geostandaarden.nl zijn allemaal conform SKOS. Voor de WOZ moet deze slag nog worden gemaakt.

Ten opzichte van vorig jaar zijn er enkele ontwikkelingen te vermelden. De implementatie van DKIM was in 2015 gepland maar is opgeschoven naar 2017 en zal dan volgens planning afgerond zijn. De implementatie van IPv6 is gevorderd en het Kadaster zal eind 2016 hieraan voldoen. In 2015 voldeed Kadaster.nl nog niet aan de Webrichtlijnen standaard, maar zal dit met het nieuwe release van oktober 2016 wel. Ook aan de TLS standaard zal vanaf oktober 2016 voldaan worden.

Van de nieuwe standaarden op de lijst zijn SIKB0102 en WPA2 Enterprise zin niet relevant voor de voorziening. SKOS is dat wel en de voorziening is grotendeels conform de standaard ingericht. Ook de implementatie van SPF is gepland voor 2017.

4.5 Berichtenbox voor bedrijven

De Berichtenbox voor bedrijven is een beveiligd e-mailsysteem. Hiermee wisselen ondernemers digitaal berichten uit met overheidsorganisaties. De Berichtenbox is speciaal gemaakt voor de Dienstenwet. Voor alle procedures die onder de Dienstenwet vallen, hebben ondernemers het recht om de Berichtenbox te gebruiken. Overheidsorganisaties zijn verplicht berichten via de Berichtenbox te beantwoorden.

Standaard	Status	Toelichting
Digikoppeling	Ja	Overheden kunnen via Digikoppeling geautomatiseerd berichten verzenden en ontvangen. Ondernemers kunnen alleen handmatig (via de website) hun Berichtenbox gegevens opvragen.
DKIM	Ja[55]	DKIM is geïmplementeerd.
DNSSEC	Nee	Volgens internet.nl ondersteunt de website geen DNSSEC. DICTU is verantwoordelijk voor de DNS-server die de domeinnaam antwoordvoorbedrijven.nl verzorgt. DNSSEC wordt nog niet voor de Berichtenbox voor bedrijven gebruikt, maar zij hebben de implementatie van DNSSEC wel in het vizier. Echter, een tijdsplanning voor de implementatie staat niet vast.
IPv4 en IPv6	Nee	De website van de Berichtenbox ondersteunt IPv4 maar is volgens internet.nl niet toegankelijk via IPv6. De Berichtenbox is wel IPv6 ready, maar nog niet de hele keten. AvB (beheerder van de Berichtenbox) is daarbij ook afhankelijk van leveranciers die hun IPv6 implementatie nog niet op orde hebben. De implementatie moet Dictu breed gebeuren voordat dit voor de Berichtenbox gedaan zal worden. Een datum voor de implementatie is niet bekend.

[53] Idem.
[54] Idem.
[55] Hier is na overleg met BFS de zienswijze van de voorziening gehanteerd. Volgens internet.nl is DKIM geïmplementeerd op het domein ondernemersplein.nl, maar niet op het domein berichtenbox.antwoordvoorbedrijven.nl. De beheerorganisatie geeft aan dat de voorziening aan DKIM voldoet. De oorzaak van de discrepantie was in de periode van dit onderzoek niet te achterhalen.

PDF 1.7, PDF A/1, PDF A/2	Ja	Alle berichten kunnen worden gedownload (vanaf de Berichtenbox website) in PDF/A formaat. PDF-documenten worden gegenereerd in PDF A/1.
SAML	Ja	eHerkenning is SAML-based en wordt toegepast voor het inloggen op de Berichtenbox.
SPF	Nee[56]	SPF is nog niet geïmplementeerd.
STuF	Ja	Wordt in combinatie met Digikoppeling gebruikt voor de uitwisseling met gemeenten.
Webrichtlijnen	Gepland	De website van de Berichtenbox is niet volledig conform de Webrichtlijnen. Er staan nog enkele punten open. De Berichtenbox zou volgens de planning eind 2015 / begin 2016 aan de Webrichtlijnen voldoen. Wegens migratie heeft dat stilgelegen, maar er is een nieuwe Webrichtlijnentoets gepland.
TLS v1.2, v1.1 en v1.0	Ja	De Berichtenbox maakt gebruik van TLS (1.2, 1.1 en 1.0).

Ten opzichte van vorig jaar zijn geen nieuwe ontwikkelingen gemaakt met het voldoen aan de standaarden die toen al op de lijst stonden. Bij Webrichtlijnen is wel inmiddels een planning voor een nieuwe toets. Vorig jaar stonden bij DENSSEC en IPv4/6 nog concrete planningen maar nu niet meer, vandaar is de status aangepast van Gepland naar Nee.

Er staan ook een aantal nieuwe standaarden op de lijst: SKOS, SPF, SIKB0102 en WPA2 Enterprise. Alleen SPF is hiervan relevant voor de voorziening, maar nog niet geïmplementeerd. SPF moet net als alle andere mailstandaarden door DICTU generiek worden ingevoerd op het mailverkeer.

4.6 BRI (inkomen)

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

Standaard	Status	Toelichting
Digikoppeling	Ja	Digikoppeling wordt toegepast in de rol van afnemer van berichten van basisregistraties(HR). De ebms-koppeling met Digilevering is operationeel in de produktie-omgeving. De aansluiting op Digilevering wordt nu alleen gebruikt in de rol van afnemer van het stelsel van basisregistraties. Het aansluiten van de BRI als Basisregistratie/leverancier op Digilevering staat niet eerder dan 2017-2018 gepland.
NEN-ISO/IEC 27001/27002	Ja	De BRI voldoet aan de standaard beveiligingseisen van de Belastingdienst. Deze eisen zijn conform VIR met classificatie departementaal vertrouwelijk. Voor opsporingsgegevens (FIOD) geldt een strakker regime. Aangezien het beveiligingskader voor de gehele Belastingdienst geldt, is er geen apart in control statement voor de BRI.
SKOS	Nee	De BRI voldoet nog niet aan SKOS. Er is bij de belastingdienst ook nog geen planning gemaakt of en wanneer de implementatie zal gebeuren.
TLS v1.2, v1.1 en v1.0	Ja	De actuele versies van TLS maken deel uit van de standaard beveiligingsrichtlijnen van de Belastingdienst.

[56] Hier is na overleg met BFS de zienswijze van de voorziening gehanteerd. Volgens internet.nl is SPF geïmplementeerd op het domein ondernemersplein.nl, maar niet op het domein berichtenbox.antwoordvoorbedrijven.nl. De beheerorganisatie geeft aan dat de voorziening niet aan SPF voldoet. De oorzaak van de discrepantie was in de periode van dit onderzoek niet te achterhalen.

CMIS v1.0	Ja	Voor toegang tot mijnbelastingdienst.nl, met ontsluiting van BRI gegevens, wordt CMIS als standaard ondersteund.
WPA2 Enterprise	Ja	WPA2 wordt toegepast door de Belastingdienst.

Ten opzichte van vorig jaar staat een aantal nieuwe standaarden op de lijst. SIKB102, SPF en WPA2 Enterprise zijn niet relevant voor de voorziening. Toch wordt WPA2 Enterprise wel door de Belastingdienst toegepast. Aangezien de BRI momenteel geen mail uitwisseling kent, is SPF voor de BRI niet van belang. (Voor de Belastingdienst als organisatie is dat wel zo en de mailservers van de Belastingdienst voldoen ook aan deze standaard.) SKOS is wel relevant voor de BRI, met name om een eenduidig zicht te geven op het begrip inkomen. Er wordt echter nog niet voldaan aan de standaard.

4.7 BRT (topografie)

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

Standaard	Status	Toelichting
Geo-Standaarden	Ja	De BRT wordt zowel geleverd via PDOK (Wat biedt Publieke Dienstverlening Op de Kaart) in GML (Objectdata), als via internationale Geo-standaarden. Daarnaast wordt de BRT geleverd via PDOK in rasterformaat in GEO, tiff formaat en WMTS (Web Map Tile Service).
NEN-ISO/IEC 27001/27002	Ja	Het Kadaster is gecertificeerd voor NEN-ISO/IEC 27001 en hanteert 27002. Het Handboek Beveiliging Kadaster is volledig op de BIR gebaseerd. In het jaarverslag is een in control statement opgenomen.
OWMS	Nee	OWMS is wel van toepassing, maar PDOK hanteert via het Nationaal GEO Register de wettelijk vastgelegde standaarden, gebaseerd op Inspire en ISO volgens het zogenaamde NL profiel. Data.overheid.nl harvest het NGR met behulp van de CSW standaard (Catalogue Services for the Web' een OGC-Geostandaard (Open Geospatial Consortium), ook onderdeel van INSPIRE). De BRT voldoet dus niet aan de standaard maar voldoet wel aan alternatieve internationale standaarden. Er zijn geen interoperabiliteitsproblemen hierdoor.
TLS v1.2, v1.1 en v1.0	Ja	Deze standaard wordt vanaf 1 oktober 2016 volledig door het Kadaster ondersteund[57]. Het gaat om de standaard TLS 1.0, TLS 1.1 en 1.2.
Webrichtlijnen	Ja	Kadaster.nl voldoet vanaf oktober 2016[58] (nieuwe release) aan de Webrichtlijnen. Wordt vanaf dan wekelijks geautomatiseerd getoetst. De toegankelijkheidsverklaring is reeds aanwezig.
SKOS	Ja	Het Kadaster hanteert SKOS voor de beschikbaarstelling van begrippenkaders van basisregistraties. De begrippenkaders voor de BRK zoals gepubliceerd op brk.kadaster.nl, de BAG zoals gepubliceerd op bag.kadaster.nl en de BGT (IMgeo) en BRT op definities.geostandaarden.nl zijn allemaal conform SKOS.

[57] Deze termijn werd door de beheersorganisatie aangegeven, maar was op het tijdpunt van de afronding van dit onderzoek nog niet geïmplementeerd om gecontroleerd te worden.
[58] Deze termijn werd door de beheersorganisatie aangegeven, maar was op het tijdpunt van de afronding van dit onderzoek nog niet geïmplementeerd om gecontroleerd te worden.

Ten opzichte van het onderzoek uit 2015 voldoet de voorziening vanaf oktober 2016 aan TLS. Ook aan de Webrichtlijnen wordt met de nieuwe release van Kadaster.nl inmiddels voldaan.

Van de nieuwe standaarden op de lijst zijn SPF, SIKB0102 en WPA2 Enterprise niet relevant voor de voorziening. SKOS is dat wel en is ook geïmplementeerd.

4.8 BRV (voertuigen)

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

Standaard	Status	Toelichting
Digikoppeling	Deels	RDW maakt voor alle nieuwe uitwisselingen gebruik van Digikoppeling. Dat is onder meer het geval in de uitwisseling met MijnOverheid (Berichtenbox), CJIB, Politie, ILT, CBR, de Belastingdienst, etc.
DNSSEC	Ja	De niet-gevoelige (technische) gegevens uit de BRV zijn te bevragen via www.rdw.nl. Die site is volgens internet.nl gesigned met DNSSEC. Alle .nl rdw domeinen zijn gesigned met DNSSEC. Alle overige domeinen (.eu, .info, .com) staan binnen het programma RIT op de planning voor eind 2017, maar maken geen deel uit van de BRV.
IPv4 en IPv6	Nee	IPv4 wordt gesupport, IPv6 wordt nog niet ingezet. De BRV is te bevragen via www.rdw.nl. Op dit moment is er voor de BRV nog geen noodzaak om op IPv6 over te gaan.
NEN-ISO/IEC 27001/27002	Ja	RDW is ISO 27001/2 gecertificeerd. RDW voldoet niet aan alle extra voorschriften van de BIR, dat hoeft ook niet want RDW is gehouden aan de VIR (en met auditor is afgesproken dat voldoen aan de 27001/27002 norm gelijk staat aan voldoen aan de VIR). Er is een in control statement van de 27001/27002 en de BKR-audit.
OWMS	Ja	De toegang tot BRV-data is op data.overheid.nl in overeenstemming met OWMS gemetadateerd beschikbaar.
PDF 1.7, PDF A/1, PDF A/2	Ja	Bij digitale dienstverlening worden uittreksels en informatie uit de BRV in PDF/A vorm verstrekt.
SAML	Gepland	De buitenkant is nu nog gestandaardiseerd op SAML 1.1. Implementatie van SAML 2,0 is onderdeel van het lopende programma MDT (Modernisering Digitale Toegang). Daarin zullen de koppelvlakken e-Herkenning en Digid4 worden ondersteund.
Webrichtlijnen	Deels	De RDW heeft de toegankelijkheidsverklaring op de site geplaatst. Zie: https://www.rdw.nl/overrdw/Paginas/Toegankelijkheidsverklaring.aspx?path=Portal/Over RDW/Kwaliteit. De website van de RDW voldoet nog niet volledig aan de Webrichtlijnen (versie 2, niveau AA). Zo is de videospeler nog niet toegankelijk zonder muis of touchscreen.
SKOS	Nee	Deze standaard lijkt relevant, maar RDW moet nog uitzoeken in hoeverre ze hieraan (kunnen) voldoen en wat dit betekent voor hun huidige Open Data publicaties.
SPF	Ja	RDW ondersteunt en gebruikt de SPF standaard voor email verkeer.

TLS v1.2, v1.1 en v1.0	Deels	RDW ondersteunt en gebruikt de TLS protocollen op de e-mail servers en Digikoppeling, maar volgens internet.nl niet op de www.rdw.nl website.
CMIS v1.0	Nee	RDW doet aan verschillende vormen van document management. De RDW consolideert daarvoor op het Sharepoint platform. Dat platform kan CMIS prima ondersteunen, maar het staat per default uit. De RDW moet nog beoordelen of deze standaard relevant is voor BRV.

Ten opzichte van het onderzoek uit 2015 is bij TLS is de status van Gepland naar Deels veranderd. Ook is de status dan DNSSEC veranderd van Nee naar Ja, en bij SAML bestaat inmiddels een concrete planning. Verder voldoet de website van de RDW inmiddels in onderdelen aan de Webrichtlijnen.

Van de sinds het vorige onderzoek nieuw op de lijst toegevoegde standaarden (SKOS, SPF, SIKB0102 en WPA2 Enterprise) is SPF relevant en ook al geïmplementeerd. SKOS is mogelijk relevant, maar de RDW moet nog uitzoeken in hoeverre deze standaard relevant is en of hij geïmplementeerd zal worden. De andere twee nieuwe standaarden zijn niet relevant.

4.9 BSN Beheervoorziening en GBA-V

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

Standaard	Status	Toelichting
Digikoppeling	Gepland	Gebruik van de voorzieningen verlopen via besloten netwerken, meer specifiek en voornamelijk Gemnet. Er ligt een integraal plan om in 2016 alle registers van RvIG te ontsluiten op Digikoppeling. De oplevering hiervan zal Q4 2016 zijn. Daarna kunnen de klanten van RvIG hierop koppelen.
IPv4 en IPV6	Nee	De voorzieningen zijn IPv6-ready in datacentrum, maar er wordt momenteel gebruik gemaakt van IPv4 adressen via Gemnet. Het is nog niet bekend wanneer er met het ontsluiten op IPv6 zal worden begonnen. Hier ligt een afhankelijkheid met de Gemnet transitie.
NEN-ISO/IEC 27001/27002	Ja	De Rijksdienst voor Identiteitsgegevens heeft een beveiligingsplan op basis van de BIR. Hier worden externe audits op gedaan. Er is een In Control Verklaring (ICV) aanwezig.
StUF	Nee	De voorziening spreekt de WSI standaard XML/SOAP met haar gebruikers. Er is geen concrete planning voor de invoering van StUF.
TLS v1.2, v1.1 en v1.0	Ja	De voorziening ondersteunt zowel TLS 1.2, 1.1 als 1.0.

Met betrekking tot de standaarden die al vorig jaar tijdens het onderzoek op de lijst stonden is er een ontwikkeling, namelijk dat bij de geplande implementatie van Digikoppeling een concrete datum staat voor oplevering (Q4 2016).

Sinds het vorige onderzoek zijn er een aantal nieuwe standaarden op de lijst (SKOS, SPF, SIKB0102, en WPA2 Enterprise). Geen van deze standaarden is relevant voor de voorziening, en ze zijn dus ook niet geïmplementeerd.

4.10 Digi-Inkoop

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

Standaard	Status	Toelichting
DNSSEC	Ja	Digi-Inkoop (domein digiinkoop.nl) voldoet aan DNSSEC.
IPv4 en IPV6	Nee	IPv6 wordt niet ondersteunt door de hoster van DigiInkoop. Er zijn geen plannen dit te realiseren.
NEN-ISO/IEC 27001/27002	Ja	DigiInkoop voldoet aan de BIR. Er is een in control statement afgegeven. Leveranciers voldoen aan ISO 27001.
Semantisch model e-factureren	Ja	DigiInkoop maakt gebruik van de specificaties van het semantisch model.
SETU	Ja	Digi-Inkoop ondersteunt de uitwisseling van SETU-hr-XML berichten
SPF	Nee	Digi-Inkoop voldoet nog niet aan deze standaard, en er bestaan op dit moment ook nog geen plannen om dit in de toekomst te implementeren. Digiinkoop.nl is alleen een applicatie domein, er wordt niet gemaild vanaf dit domein.
TLS v1.2, v1.1 en v1.0	Gepland	Digi-inkoop maakt gebruik van TLS 1.1 en 1.0 (met Forward Secrecy). Er loopt nu een migratie traject naar TLS V1.2. (verwachte release 10/9/16)
PDF/A en PDF 1.7	Ja	De Digi-Inkoop applicatie produceert inkooporders en facturen in PDF formaat. Documenten die op logius.nl beschikbaar worden gesteld zijn in PDF/A formaat (dit zijn de documenten over de berichtenverkeerstandaarden waar Digi-inkoop gebruik van maakt: https://www.logius.nl/ondersteuning/gegevensuitwisseling/ubl-ohnl en https://www.logius.nl/ondersteuning/gegevensuitwisseling/setu-hr-xml-ohnl).

Sinds het vorige onderzoek in 2015 zijn er een aantal ontwikkelingen geweest. DNSSEC is inmiddels geïmplementeerd. TLS v1.2 implementatie stond vorig jaar nog op Nee, maar hier worden inmiddels concrete stappen gezet om hier in het najaar 2016 aan te voldoen. Ook wordt inmiddels aan de PDF standaard voldaan, deze waren in het vorige jaar nog niet als relevante standaarden voor deze voorziening meegenomen.

Ook zijn sinds het vorige onderzoek een aantal nieuwe standaarden op de lijst (SKOS, SPF, SIKB0102, WPA2 Enterprise). Alleen SPF is hiervan relevant voor de voorziening. Echter, er zijn nog geen plannen om SPF te implementeren.

4.11 DigiD

DigiD is de generieke identificatievoorziening voor burgers voor de dienstverlening van de overheid. DigiD wordt beheerd door Logius.

Standaard	Status	Toelichting
Digikoppeling	Nee	Er zijn geen andere plannen aan te sluiten op Digikoppeling. DigiD richt zich voor berichtenverkeer op de SAML-standaard zoals ook opgenomen op de pas-toe-of-leg-uit-lijst.
DKIM	Ja	DigiD mail wordt verstuurd met een DKIM signature.

DNSSEC	Deels	DNSSEC is doorgevoerd in release 4.5 van DigiD en inmiddels operationeel. Dit jaar zijn in het onderzoek ook de mailservers meegenomen en die voldoen niet aan de standaard (zie https://www.internet.nl/mail/digid.nl/17054). Vandaar dat de status dit jaar naar Deels is gewijzigd.
IPv4 en IPV6	Deels	De website DigiD.nl is via IPv6 toegankelijk. De planning was om in 2015 ook de mailstromen via IPv6 te laten lopen. Deze is nog niet afgerond. Op dit moment lopen de mailstromen nog via IPv4 verkeer. Dit jaar zijn in het onderzoek ook de mailservers meegenomen en die voldoen niet aan de standaard (zie https://www.internet.nl/mail/digid.nl/17054). Vandaar dat de status dit jaar naar Deels is gewijzigd.
NEN-ISO/IEC 27001/27002	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Rijk (BIR) van toepassing die is gebaseerd op NEN-ISO27001. Logius heeft zich over toepassing van deze norm verantwoord door het afgeven van In Control Verklaringen (ICV's) aan de eigenaar (BZK/DGOBR).
SAML	Ja	DigiD biedt aan afnemers een SAML-koppelvlak. De meeste afnemers zitten nog op het A-select koppelvlak. SAML berichtuitwisseling in het eID stelsel (http://www.eid-stelsel.nl/) zal anders zijn die van DigiD. Om partijen niet tot meerdere migraties te dwingen houdt DigiD het A-select koppelvlak nog in stand.
SKOS	Ja	DigiD voldoet aan SKOS.
SPF	Ja	SPF is relevant voor DigiD bij alle mails vanuit de DigiD applicatie en DigiD voldoet ook aan deze standaard
Webrichtlijnen	Ja	Voldoet aan de Webrichtlijnen, externe toets heeft plaatsgevonden https://www.accessibility.nl/ondersteuning/inspectie/site-981 en https://www.digid.nl/help/
TLS v1.2, v1.1 en v1.0	Ja	DigiD Machtigen ondersteunt TLS v1.0 en TLS v1.2. TLS 1.1 wordt niet ondersteund, omdat Logius een sterke voorkeur heeft voor TLS 1.2. Om brede comptabiliteit mogelijk te maken wordt TLS 1.0 nog steeds ondersteund.

Ten opzichte van het onderzoek uit 2015 zijn er een aantal ontwikkelingen. De planning uit 2015 om ook de mailstromen via IPv6 te laten lopen is nog niet afgerond. Verder zijn in het onderzoek dit jaar ook de mailservers meegenomen en die voldoen niet aan IPv6 (zie https://www.internet.nl/mail/digid.nl/17054). Vandaar dat de status dit jaar naar Deels is gewijzigd. Dit betekent daarom niet dat het een terugval is, omdat hier gewoon de lat hoger gezet is maar feitelijk geen terugval bestaat. Deze redenering geldt ook voor DNSSEC.

Ook staan er een aantal nieuwe standaarden op de lijst (SKOS, SPF, SIKB0102 en WPA2 Enterprise), waarvan SKOS en SPF relevant zijn. Beide standaarden worden door de voorziening toegepast.

4.12 DigiD Machtigen

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

Standaard	Status	Toelichting
DNSSEC	Ja	Volgens internet.nl voldoet het domein https://machtigen.digid.nl aan DNSSEC.
IPv4 en IPV6	Ja	Zowel IPv6 als IPv4 worden ondersteund.

SAML	Deels	Twee van de drie koppelvlakken van DigiD Machtigen maakt gebruik van SAML. Het authenticatie koppelvlak met DigiD maakt nog gebruik van A-Select. Deze koppeling is ontworpen toen DigiD nog geen SAML koppelvlak hiervoor had en is nog niet vernieuwd. Wanneer er meer duidelijkheid komt over eID wordt een keuze gemaakt over de implementatie van SAML. Die keuze wordt nu nog niet gemaakt om desinvesteringen tegen te gaan
NEN-ISO/IEC 27001/27002	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Rijk (BIR) van toepassing die is gebaseerd op NEN-ISO27001. Logius heeft zich over toepassing van deze norm verantwoord door het afgeven van In Control Verklaringen (ICV's) aan de eigenaar (BZK/DGOBR).
Webrichtlijnen	Ja	De voorziening voldoet aan deze standaard.
TLS v1.2, v1.1 en v1.0	Ja	DigiD Machtigen ondersteunt TLS v1.0, TLS v1.1 en TLS v1.2. Om brede comptabiliteit mogelijk te maken wordt TLS 1.0 en 1.1 nog steeds ondersteund.
Digikoppeling	Deels	Het DVS koppelvlak is Digikoppeling compliant. PBS koppelvlak zal Digikoppeling compliant worden zodra daar een nieuwe versie voor gemaakt wordt.
PDF/A en PDF 1.7	Ja	De voorziening voldoet aan deze standaard.
SPF	Ja	De voorziening voldoet aan deze standaard, zie ook te toelichting bij DigiD.

Ten opzichte van het onderzoek uit 2015 zijn er enkele ontwikkelingen. IPv4/6 is van Gepland naar Ja veranderd. SAML staat nog steeds op de status 'Deels', maar inmiddels voldoen twee van de drie koppelvlakken aan de standaard (i.p.v. een koppelvlak in 2015). De Digikoppeling was vorig jaar nog niet als relevante standaard voor deze voorziening meegenomen. Dit is dit jaar veranderd en de status hiervan staat op 'Deels', omdat het DVS koppelvlak inmiddels Digikoppeling compliant is. OWMS stond vorig jaar wel in de tabel maar de relevantie van deze standaard was in 2015 nog niet bepaald; inmiddels wordt deze standaard als niet relevant beschouwd. De reden hiervoor is dat de OWMS standaard bedoeld is voor metadata om gepubliceeerde overheidsinformatie goed vindbaar te maken. Echter, DigiD Machtigen ontsluit geen overheidsinformatie waar metadata van toepassing op is. Bij de PDF standaard was de status in het vorige onderzoek nog onbekend, maar aan deze standaard wordt inmiddels voldaan. SAML staat dit jaar op Deels hoewel dit vorig jaar op Ja stond. Gezien de toelichting (maar twee van de drie koppelvlakken voldoen) had dit ook in 2015 op Deels moeten staan.

Van de standaarden die sinds het vorige onderzoek nieuw op de lijst erbij zijn gekomen (SKOS, SPF, SIKB0102, WPA2 Enterprise) is alleen SPF relevant, en hier wordt ook aan voldaan.

4.13 Digilevering

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

Standaard	Status	Toelichting
Digikoppeling	Ja	Digilevering maakt gebruik van Digikoppeling
DKIM	Gepland	Digilevering draait op het platform van Logius Managed Services. Aanpassingen op dit platform ter ondersteuning van de standaard worden Logius breed aangepakt. Het voldoen aan beveiligingsstandaarden, waaronder DKIM, wordt opgenomen in het jaarplan 2017. Dit wordt echter per dienst geïmplementeerd.

DNSSEC	Gepland	Digilevering draait op het platform van Logius Managed Services. Aanpassingen op dit platform ter ondersteuning van de standaard worden Logius breed aangepakt. Voor DNSSEC geldt dat een aantal diensten gebruik van maakt van DNSSEC en een aantal nog niet. Er loopt een traject om alle diensten van Logius te voorzien van DNSSEC. De planning hiervan is Q4 2016, Q1 2017.
IPv4 en IPv6	Gepland	Digilevering draait op het platform van Logius Managed Services. Aanpassingen op dit platform ter ondersteuning van de standaard worden Logius breed aangepakt. IPv6 wordt door de meeste diensten gebruikt. Enkele (legacy) implementaties gebruiken dit nog niet. De platformen ondersteunen dit en er is een IPv6 adresplan beschikbaar. Het omzetten wordt in het jaarplan 2017 meegenomen.
SPF	Nee	Hierover is ook na navraag bij meerdere personen is geen concrete planning vermeld.

Ten opzichte van het onderzoek uit 2015 zijn een aantal nieuwe standaarden in de tabel als relevant meegenomen: DKIM, DNSSEC, en IPv4/IPv6. Echter, deze standaarden zijn nog niet geïmplementeerd, maar hebben de status 'Gepland'.

Ook staan er een aantal nieuwe standaarden op de lijst ten opzichte van het vorige onderzoek (SKOS, SPF, SIKB0102 en WPA2 Enterprise), waarvan alleen SPF relevant is. Echter, hierover is ook na navraag bij meerdere personen is geen concrete planning vermeld.

4.14 Digimelding

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

Standaard	Status	Toelichting
Digikoppeling	Ja	Digimelding maakt gebruik van Digikoppeling
DKIM	Gepland	Digilevering draait op het platform van Logius Managed Services. Aanpassingen op dit platform ter ondersteuning van de standaard worden Logius breed aangepakt. Het voldoen aan beveiligingsstandaarden, waaronder DKIM, wordt opgenomen in het jaarplan 2017. Dit wordt echter per dienst geïmplementeerd.
DNSSEC	Gepland	Digilevering draait op het platform van Logius Managed Services. Aanpassingen op dit platform ter ondersteuning van de standaard worden Logius breed aangepakt. Voor DNSSEC geldt dat een aantal diensten gebruik van maakt van DNSSEC en een aantal nog niet. Er loopt een traject om alle diensten van Logius te voorzien van DNSSEC. De planning hiervan is Q4 2016, Q1 2017.
IPv4 en IPv6	Gepland	Digilevering draait op het platform van Logius Managed Services. Aanpassingen op dit platform ter ondersteuning van de standaard worden Logius breed aangepakt. IPv6 wordt door de meeste diensten gebruikt. Enkele (legacy) implementaties gebruiken dit nog niet. De platformen ondersteunen dit en er is een IPv6 adresplan beschikbaar. Het omzetten wordt in het jaarplan 2017 meegenomen.
SPF	Nee	Hierover is ook na navraag bij meerdere personen is geen concrete planning vermeld.

Ten opzichte van het onderzoek uit 2015 zijn een aantal nieuwe standaarden in de tabel als relevant meegenomen: DKIM, DNSSEC, en IPv4/IPv6. Echter, deze standaarden zijn nog niet geïmplementeerd, maar hebben de status 'Gepland'.

Ten opzichte van het onderzoek uit 2015 staan er een aantal nieuwe standaarden op de lijst (SKOS, SPF, SIKB0102 en WPA2 Enterprise), waarvan alleen SPF relevant is. Echter, hierover is ook na navraag bij meerdere personen is geen concrete planning vermeld.

4.15 Diginetwerk

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

Standaard	Status	Toelichting
IPv4 en IPV6	Nee	Binnen Diginetwerk wordt alleen IPv4 gebruikt, binnen het nummerplan is nu nog voldoende IPv4 ruimte beschikbaar. Er zijn geen specifieke plannen voor IPv6.
NEN-ISO/IEC 27001/27002	Ja	Deze standaard is onderdeel van het algemene beveiligingsbeleid van Logius. Logius voldoet aan deze standaard, daarmee voldoet ook Diginetwerk aan deze standaard.
DNSSEC	Ja	DNSSEC validatie wordt toegepast op Rijks-DNS.

Ten opzichte van vorig jaar is DNSSEC toegevoegd aan de tabel als relevante standaard en inmiddels ook geïmplementeerd.

Daarnaast is een andere ontwikkeling dat dit jaar een aantal nieuwe standaarden op de lijst staan: SKOS, SPF, SIKB0102 en WPA2 Enterprise. Geen van deze standaarden is relevant voor Diginetwerk en ze zijn dus ook niet geïmplementeerd.

4.16 DigiPoort

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

Digipoort is opgedeeld in twee, nochtans gescheiden, onderdelen: Digipoort OTP (voorheen Overheidstransactiepoort) en Digipoort Procesinfrastructuur (PI).

4.16.1 Digipoort / OTP

Standaard	Status	Toelichting
Digikoppeling	Gepland	Digikoppeling wordt in de huidige Digipoort OTP niet meer geïmplementeerd. Er loopt een migratie van Digipoort OTP naar het Keten Informatie Services | Manages Services-platform (KIS | MS platform). Dat is een nieuw platform dat voldoet aan alle standaarden (Digikoppeling, DNSSEC en IPv4 / IPv6). Einddatum van deze migratie is 2017.
DNSSEC	Gepland	DNSSEC wordt in de huidige Digipoort OTP niet meer geïmplementeerd. Er loopt een migratie van Digipoort OTP naar het Keten Informatie Services | Manages Services-platform (KIS | MS platform). Dat is een nieuw platform dat voldoet aan alle standaarden (Digikoppeling, DNSSEC en IPv4 / IPv6). Einddatum van deze migratie is 2017.

IPv4 en IPV6	Gepland	IPv6 wordt in de huidige Digipoort OTP niet meer geïmplementeerd. Er loopt een migratie van Digipoort OTP naar het Keten Informatie Services | Manages Services-platform (KIS|MS platform). Dat is een nieuw platform dat voldoet aan alle standaarden (Digikoppeling, DNSSEC en IPv4 / IPv6). Einddatum van deze migratie is 2017.
NEN-ISO/IEC 27001/27002	Ja	DigiPoort / OTP voldoet aan de BIR. Leveranciers voldoen aan ISO 27001 of vergelijkbare standaard.
SPF	Nee	Digipoort heeft geen SPF-records. Er wordt niet gemaild vanuit dit domein, maar SPF zou wel ingericht moeten worden.
TLS v1.2, v1.1 en v1.0	Nee	Digipoort ondersteunt TLS v1.1. TLS1.2 was gepland voor november 2015 maar er zijn nog geen nieuwe ontwikkelingen. Het is momenteel onduidelijk wanneer de invoering gepland is.

Ten opzichte van het onderzoek uit 2015 zijn er enkele ontwikkelingen te benoemen. De geplande migratie van Digipoort OTP naar het KIS|MS platform is inmiddels in gang en als einddatum van deze migratie staat 2017 vast. Bij TLS is de status gewijzigd van Gepland naar Nee, omdat er op dit moment geen concrete plannen meer bekend zijn.

Van die sinds het vorige onderzoek nieuw aan de lijst toegevoegde standaarden (SKOS, SPF, SIKB0102 en WPA2 Enterprise) is alleen SPF relevant voor de voorziening. Echter, Digipoort OTP voldoet hier niet aan en er zijn nog geen plannen gemaakt om dat wel te doen.

4.16.2 Digipoort / PI

Standaard	Status	Toelichting
DNSSEC	Nee	Hoewel Digipoort werkt met PKI certificaten ter authenticatie, zou DNSSEC ook ingericht moeten zijn. Dit is niet zo.
Digikoppeling	Ja	Zie de koppelvlakspecificaties op http://www.logius.nl/producten/gegevensuitwisseling/digitpoort/koppelvlakken
DKIM	Ja	Digipoort/PI voldoet aan DKIM. Dit is ook relevant omdat de voorziening een SMTP koppelvlak heeft.
IPv4 en IPV6	Ja	Digipoort PI is een applicatie die draait op het platform Managed Services. Voor dit onderdeel wordt de dienstverlening van Managed Services betrokken.
NEN-ISO/IEC 27001/27002	Ja	DigiPoort / OTP voldoet aan de BIR. Leveranciers voldoen aan ISO 27001 of vergelijkbare standaard.
SETU	Ja	Digipoort/PI ondersteunt de uitwisseling van SETU-hr-XML berichten
SPF	Nee	Digipoort heeft geen SPF-records. Er wordt niet gemaild vanuit dit domein, maar SPF zou wel ingericht moeten worden.
XBRL en Dimensions	Ja	Wordt ondersteund door Digipoort/PI
TLS v1.2, v1.1 en v1.0	Ja	Digipoort / PI ondersteunt alle versies.

Ten opzichte van het onderzoek van vorig jaar is ondertussen DKIM als relevante standaard voor deze voorziening meegenomen. Hier wordt ook aan voldaan. Ook DNSSEC is dit jaar als relevante standaard meegenomen voor deze voorziening, maar hier wordt nog niet aan voldaan.

Hiernaast is een verandering bij deze voorziening ten opzichte van het onderzoek van vorig jaar dat van de nieuw op de lijst toegevoegde standaarden (SKOS, SPF, SIKB0102 en WPA2 Enterprise) SPF als relevante standaard voor deze voorzieningen bij komt. Echter, Digipoort/PI voldoet hier nog niet aan en er bestaan nog geen concrete plannen.

4.17 Doc-Direkt

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

Standaard	Status	Toelichting
Digikoppeling	Nee	De informatie-uitwisseling tussen het Nationaal Archief en Doc-Direkt wordt binnen de context van de programma's DWR – archief en E-depot gerealiseerd en doorontwikkeld. De planning wordt buiten Doc-Direkt om bepaald en deze is bij Doc-Direkt niet bekend. De planning wordt bepaald door BZK (DWR-Archief) en het Nationaal Archief (E-depot). Doc-Direkt heeft geen invloed op deze planningen.
DKIM	Ja	Volgens SSC-ICT maakt Doc-Direkt gebruik van de mailservers van SSC-ICT, deze zijn onderdeel van het BZK domein, waarvoor DKIM actief is.
IPv4 en IPv6	Nee	De Haagse ring, waarover praktisch al het verkeer naar de Doc-Direkt voorzieningen loopt, ondersteunt geen IPv6. Het is bij Doc-Direkt niet bekend wanneer IPv6 gebruikt gaat worden. De beheerder van de Haagse Ring is Logius. De Haagse Ring is onderdeel van Diginetwerk. Binnen Diginetwerk wordt alleen IPv4 gebruikt, binnen het nummerplan is nu nog voldoende IPv4 ruimte beschikbaar.
NEN-ISO/IEC 27001/27002	Ja	Voor de informatiesystemen waarvan Doc-Direkt eigenaar is, is in 2015 een 'in controle verklaring' opgesteld. Op de punten waar Doc-Direkt afwijkt is een uitleg gegeven (explains) en er is een verbeterplan opgesteld.
ODF	Nee	Voor bewerkbare documenten wordt alleen .doc-formaat gebruikt. Er zijn geen plannen ODF te gebruiken.
PDF 1.7 – PDF A/1 of PDF A/2	Ja	Doc-Direkt ondersteunt in haar archieven vooral PDF/A. Alles wat gescand wordt gaat naar PDF/A. Daarnaast wordt ook 1.7 veel gebruikt.
SAML	Ja	Via de werkplek DWR kunnen medewerkers via SSO inloggen op de door Doc-Direkt beheerde DMS applicatie.
SKOS	Nee	SKOS wordt op dit moment niet toegepast. Er zijn nog geen plannen bekend of en wanneer SKOS geïmplementeerd zal worden.
SPF	Nee	Ook SPF wordt op dit moment niet toegepast, en het is nog niet bekend of en wanneer SPF geïmplementeerd zal worden.
TLS v1.2, v1.1 en v1.0	Nee	Het is bij Doc-Direkt niet bekend of TLS van toepassing is en daarmee ook niet wanneer dit geïmplementeerd is.
CMIS v1.0	Nee	De mogelijkheid en noodzakelijkheid van het toepassen van deze standaard wordt nader onderzocht.

Ten opzichte van het onderzoek uit 2015 zijn met betrekking tot de toen onderzochte standaarden geen veranderingen gemaakt bij Doc-Direkt.

Van de sinds het vorige onderzoek nieuwe op de lijst opgenomen standaarden (SKOS, SPF, SIKB0102 en WPA2 Enterprise) zijn alleen de eerste twee relevant voor Doc-Direkt. Echter, geen van deze wordt op dit moment toegepast en er zijn ook nog geen plannen bekend of en wanneer ze geïmplementeerd zullen worden.

4.18 Digitale Werkomgeving Rijksdienst (DWR)

De Digitale Werkomgeving Rijksdienst (DWR) is de ICT-werkplek voor rijksambtenaren. Deze werkplek is een onderdeel van de dienstverlening van SSC-ICT Haaglanden. SSC-ICT Haaglanden ontwikkeld en beheert de DWR-werkplek. De nieuwe digitale werkomgeving bestaat uit verschillende onderdelen voor infrastructuur en connectiviteit. De 3 belangrijkste zijn uniforme digitale werkomgeving voor alle ambtenaren (DWR-Client), 1 website voor alle overheidsinformatie en diensten (rijksoverheid.nl), en gebruik van web 2.0 toepassingen om beter en sneller samen te werken. Komende jaren wordt de technologie verder geïntegreerd en zal in afstemming met de afnemers van de dienstverlening de standaarden verder worden ingevuld.

Standaard	Status	Toelichting
Digikoppeling	Deels	Binnen VenJ vindt elektronisch berichtenverkeer interdepartementaal plaats via de Justitie Berichten Service (JUBES). JUBES is vanuit VenJ het koppelvlak voor de Digikoppeling dienst van Logius. De open standaarden eBMS en WUS zijn de daarbij gebruikte protocollen om de berichten veilig te versturen.
DKIM	Deels	DKIM is geïmplementeerd voor 72 van de 90 domeinen die SSC-ICT in beheer heeft. Het is geïmplementeerd in combinatie met SPF en DMARC (DMARC is begin 2015 aangemeld voor opname op de pas-toe-of-leg-uit-lijst).
DNSSEC	Deels	De domeinen van de klanten van SSC-ICT die via de DNS van AZ lopen voldoen. De domeinen van de klanten van SSC-ICT die via de DNS van SSC-ICT lopen voldoen eind 2017. SSC-ICT geeft aan dat de cliënt DNSSEC-validatie ondersteunt, en dat RijksDNS DNSSEC-validatie ondersteunt.
IPv4 en IPV6	Nee	IPv4 is in gebruik. De gebruikte technische componenten van DWR ondersteunen wel IPv6. IPv6 is een onderdeel van de infrastructuur en IPv6 reeksen worden uitgedeeld door Logius. Het is de bedoeling dat de internet facing kant van de DMZ IPv6 gaat ondersteunen, maar een concrete tijdlijn staat nog niet vast.
NEN-ISO/IEC 27001/27002	Ja	DWR voldoet aan de BIR en wordt hier ook op ge-audit. De laatste audit heeft plaatsgevonden in de zomer van 2014. De locatie Zoetermeer is ISO 2700x gecertificeerd.
ODF 1.2 JPEG / PNG	Ja	De DWR cliënt wordt geleverd met zowel Libreoffice als Office 2007 als Office 2010. Beide suites ondersteunen het lezen en schrijven van ODF bestanden.
PDF 1.7 / PDF A/1 en PDF A/2	Ja	De DWR cliënt kan alle types PDF lezen. Schrijven van PDF kan op meerdere manieren. Alle types worden ondersteund al is daarvoor soms wel het installeren van Adobe Acrobat Professional benodigd. PDF A/2 is nog niet mogelijk, omdat Adobe Acrobat het niet ondersteund.
SAML	Ja	Single Sign On (SSO) op basis van SAML wordt aangeboden binnen de DWR producten en diensten catalogus. Het SSO koppelvlak is een generieke dienst.
SPF	Deels	SPF wordt op 72 van de 90 domeinen toegepast.
Webrichtlijnen	Ja	Op de DWR cliënt kan de Firefox browser omgaan met de technische eisen uit de Webrichtlijnen. Internet Explorer doet dat in mindere mate, maar is wel nodig omdat de webinterfaces van verschillende bedrijfsvoeringsystemen nog geen modernere browsers ondersteunen. Op dit moment is Internet Explorer 11 de standaard browser. Frontmotion Firefox (24.7) is de 2e browser.
TLS v1.2, v1.1 en v1.0	Ja	De op de werkplek aangeboden browser ondersteunen deze versies van TLS. De internet mailvoorziening werkt met starttls. Voor webservers met applicaties van klanten wordt dit toegepast voor de klanten die dit hebben aangevraagd.
WPA2 Enterprise	Ja	Op de wifivoorziening van DWR wordt deze standaard toegepast. Dit is een kantoorvoorziening.

Ten opzichte van het onderzoek uit 2015 zijn er volgende ontwikkelingen: Rondom IPv6 zijn er plannen om hieraan te voldoen, maar er zit nog steeds geen concrete tijdslijn aan vast. DKIM staat dit jaar op Deels hoewel dit vorig jaar op Ja stond. Gezien de toelichting in 2105 en 2016 hetzelfde is (geïmplementeerd voor 72 van de 90 domeinen) had dit ook in 2015 op Deels moeten staan.

Ten opzichte van vorig jaar staan er de volgende nieuwe standaarden op de lijst: SKOS, SPF, SIKB0102 en WPA2 Enterprise. Alleen SPF en WPA2 Enterprise zijn relevant en worden ook (bij SPF deels) toegepast.

4.19 Semantisch model eFactureren

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

Standaard	Status	Toelichting
DNSSEC	Nee	eFactureren heeft een website als portaal voor gebruikers (dit e-factuurportaal wat door Logius wordt aangeboden is een variant van Digiinkoop.nl en de domein is dus https://digiinkoop.nl. Er zijn daarnaast ook diverse e-factuur portalen, die in de markt worden aangeboden zoals papierloosfactureren.nl en Simplerinvoicing, maar deze worden niet door Logius geleverd). Deze website wordt zeer beperkt gebruik. Logius heeft gepland in 2015 DNSSEC in te voeren en dan per voorziening te kijken hoe DNSSEC geïmplementeerd wordt. Echter, DNSSEC is nog niet geïmplementeerd bij eFactureren.
IPv4 en IPV6	Nee	IPv6 wordt niet toegepast. Logius is afhankelijk van de hoster van eFactureren.
NEN-ISO/IEC 27001/27002	Ja	Deze standaard is onderdeel van het algemene beveiligingsbeleid van Logius (BIR). Logius voldoet aan deze standaard, daarmee voldoet ook eFactureren aan deze standaard.
Semantisch model e-factureren	Ja	De e-facturen moeten voldoen aan de SMEF specificaties.
SPF	Nee	Het van Logius aangeboden e-factuurportaal Digiinkoop.nl gebruikt Digipoort. Voor dit portaal zou een "v=spf1 -all"-record moeten worden aangemaakt.
Webrichtlijnen	Nee	eFactureren heeft een website als portaal voor gebruikers. Deze website wordt zeer beperkt gebruik. eFactureren heeft een analyse gemaakt van de kosten om aan de Webrichtlijnen te voldoen. Voor het beperkte aantal gebruikers acht eFactureren de kosten te hoog om de website conform de Webrichtlijnen op te zetten.
PDF/A en PDF 1.7	Ja	Documenten die op logius.nl beschikbaar worden gesteld zijn in PDF/A formaat. De documenten die worden bedoelt zijn de e-factuur standaarden documentatie. (Net zoals bij Digi-Inkoop zijn dit de documenten m.b.t. berichtenverkeer standaarden waar Digi-inkoop gebruik van maakt: https://www.logius.nl/ondersteuning/gegevensuitwisseling/ubl-ohnl en https://www.logius.nl/ondersteuning/gegevensuitwisseling/setu-hr-xml-ohnl).

Ten opzichte van het onderzoek uit 2015 is een van de ontwikkelingen geweest dat PDF dit jaar als relevante standaard in de tabel is meegenomen.

Wel zijn er een aantal nieuwe standaarden nieuw op de lijst gekomen (SKOS, SPF, SIKB0102 en WPA2 Enterprise). Van deze standaarden is alleen SPF relevant voor eFactureren (ook al wordt niet gemaild van deze domein en worden e-facturen via Digipoort verstuurd), om te voorkomen dat fraudeurs (phishing) e-mails in naam van eFactureren kunnen sturen. De gebruiker weet niet altijd dat er vanaf een bepaald domein nooit gemaild wordt, en kan denken dat de e-mail echt van eFactureren komt.

4.20 MijnOverheid

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

Standaard	Status	Toelichting
Digikoppeling	Deels	Nieuwe koppelingen worden conform Digikoppeling ingericht. Er is nog een beperkt aantal , dat niet voldoen.
DKIM	Ja	Volgens https://internet.nl/mail/mijn.overheid.nl/results# voldoet MijnOverheid aan DKIM.
DNSSEC	Ja	Volgens https://internet.nl/site/www.mijn.overheid.nl/ voldoet MijnOverheid aan DNSSEC.
IPv4 en IPV6	Nee	IPv6 wordt niet ondersteund, er zijn geen plannen hiervoor.
OWMS	Deels	Een deel van de content is conform OWMS gemetadateerd. Er is geen plan om dit voor de gehele inhoud te doen. Voor metadatering zijn geen gegevenswoordenboeken gemaakt, omdat de metadatering beperkt is.
PDF 1.7, PDF/A-1 of PDF/A-2	Deels	De koppelvlakspecificaties voor de Berichtenbox bevatten eisen waaraan afnemers moeten voldoen. Die eisen beschrijven een voorkeur voor PDF/A-1a (ISO 19005-1). PDF/X (ISO 15930) is ook toegestaan. MijnOverheid controleert het bijlageformaat niet. MijnOverheid wijst bijlages die niet aan de normen voldoen ook niet af. Daardoor kunnen afnemers berichtbijlages conform PDF 1.7 / A-1a / A-2 plaatsen. MijnOverheid genereert geen PDF-berichten. Op dit moment voert men een impact-analyse uit om te onderzoeken wat het betekent wanneer men wel gaat scannen van PDF-bijlages en daar eventueel acties aan verbinden.
NEN-ISO/IEC 27001/27002	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Rijk (BIR) van toepassing die is gebaseerd op NEN-ISO27001. Logius heeft zich over toepassing van deze norm verantwoord door het afgeven van In Control Verklaringen (ICV's) aan de eigenaar (BZK/DGOBR).
SAML	Ja	Authenticatie loopt via SAML
SPF	Ja	SPF is relevant en inmiddels geïmplementeerd.
StUF	Ja	MijnOverheid heeft waar relevant de koppeling op basis van StUF.
Webrichtlijnen	Deels	De laatste Webrichtlijnen toets is door Stichting Accessibility uitgevoerd (niet meer door Centric zoals voorheen) en hieruit zijn een aantal issues naar voren gekomen. Deze issues worden (en zijn deels al) opgelost in diverse releases voor eind 2016, zodat MijnOverheid dan volledig aan de standaard voldoet.
TLS v1.2, v1.1 en v1.0	Ja	In de dienstverlening aan burgers maakt MijnOverheid gebruik van een TLS 1.2-verbinding (https://internet.nl/site/mijn.overheid.nl). De koppelingen met afnemers (overheidsorganisaties) lopen ook via TLS op basis van PKIoverheid-certificaten.

Ten opzichte van het onderzoek van vorig jaar zijn er enkele nieuwe ontwikkelingen. Zo is bij Webrichtlijnen de status van Gepland naar Deels veranderd. Eind 2016 zal volledig hieraan voldaan worden.

Ook zijn er een aantal nieuwe standaarden op de lijst (SKOS, SPF, SIKB0102, WPA2 Enterprise). Alleen SPF is hiervan relevant voor MijnOverheid, en inmiddels ook al geïmplementeerd.

4.21 NHR (Nieuw HandelsRegister)

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

Standaard	Status	Toelichting
Digikoppeling	Ja	Ongeveer 10% van het verkeer van het NHR gaat naar mede-overheden. Die uitwisselingen vinden allemaal plaats via Digikoppeling en StUF.
DNSSEC	Gepland	Er loopt nu (2016) een traject voor het vervangen van infracomponenten hierbij wordt ook DNSSEC mogelijk.
DKIM	Ja	Het domein kvk.nl voldoet aan DKIM (https://internet.nl/mail/kvk.nl/results).
IPv4 en IPv6	Nee	De website kvk.nl ondersteunt IPv4, maar is niet toegankelijk via IPv6 volgens https://internet.nl/site/kvk.nl/results#. Het project om over te stappen naar IPv6 project is door de KvK nog niet ingepland. De KvK heeft wel voorbereidingen getroffen, waaronder de overstap naar een andere ISP provider, zodat de KvK een migratie naar IPv6 uit kan gaan voeren.
NEN-ISO/IEC 27001/27002	Ja	De KvK is (zomer 2016) ISO 27001 gecertificeerd en hanteert ISO27002.
PDF 1.7, PDF A/1, PDF A/2	Ja	Alle uittreksels en informatie uit het NHR wordt in PDF/A-vorm verstrekt. Het betreft PDF A/1.
SAML	Ja	eHerkenning is SAML-based en wordt toegepast voor het aanleveren van jaarrekeningen en informatieverstrekking. In de notarisapplicatie kan de notaris van achter zijn computer rechtstreeks opgave doen. Ook hier wordt gebruik gemaakt van SAML als authenticatieprocedure. Er loopt nu (2016) een traject waarbij de authenticatieprocedures en infrastructuur worden vervangen. Hierdoor kan SAML straks voor elke dienst ingezet worden voor authenticatie
SKOS	Nee	SKOS is nog niet geïmplementeerd in Gegevenscatalogus NHR. De standaard wordt wel voorzien door diverse ondersteunende software pakketten in gebruik bij de KVK rondom het NHR. Voor deze standaard zal een impactscan uitgezet worden, maar wanneer dit gaat gebeuren kan op dit moment nog niet aangegeven worden.
SPF	Ja	SPF is ten opzichte van het vorige onderzoek nieuwe op de lijst en inmiddels geïmplementeerd door NHR.
STuF	Ja	Ongeveer 10% van het verkeer van het NHR gaat naar medeoverheden. Die uitwisselingen vinden allemaal plaats via Digikoppeling en StUF.
Webrichtlijnen	Deels	De KvK voldoet voor een groot deel aan de Webrichtlijnen. Voor 2017 staat een scan op de planning om de status te herijken en van daaruit noodzakelijke verbeteringen door te voeren.
TLS v1.2, v1.1 en v1.0	Ja	De KvK gebruikt TLS op de verbindingen waar voorheen SSL werd gebruikt. De kamer is nu in een migratie traject om volledig over te gaan op TLS1.2.

CMIS v1.0	Deels	De bij de KvK in gebruik zijn de content management systemen Tridion en Documentum zijn compliant aan de CMIS standaard. Nog niet alle interne koppelingen op deze systemen zijn al gemigreerd naar deze standaard, daar zijn op dit moment nog geen plannen voor.

Ten opzichte van het onderzoek uit 2015 zijn er een aantal nieuwe ontwikkelingen. Zo is de KvK sinds de zomer 2016 ISO 27001 gecertificeerd en hanteert ook ISO27002. DNSSEC stond vorig jaar nog op Nee, maar inmiddels liggen concrete plannen voor de implementatie voor. DKIM stond vorig jaar nog niet in de tabel, maar wordt dit jaar als relevante standaard meegenomen. Webrichtlijnen stond vorig jaar op Ja, maar in feite werd dit jaar van de voorziening teruggekoppeld dat de KvK maar voor "een groot deel" hieraan voldoet; vandaar dat de status naar Deels is gewijzigd.

Daarnaast zijn er ook een aantal nieuwe standaarden op de lijst bijgekomen (SKOS, SPF, SIKB0102 en WPA2 Enterprise). Van deze zijn SKOS en SPF relevant voor de voorziening. Echter, alleen SPF is inmiddels geïmplementeerd.

4.22 ODC Noord

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

Standaard	Status	Toelichting
DKIM	Gepland	Nog geen DKIM voor ODC-Noord. Voor e-mail maakt ODC-Noord vooralsnog gebruik van de mail-faciliteiten van DUO. Er zou een eigen e-mailinfrastructuur vanaf eind 2015 komen, maar dit is nog niet in gang gebracht. In het kader van de beweging van OCW naar één werkplekconcept is het mogelijk dat op termijn een multi-tenant mail-oplossing aangeboden wordt, maar dit is nog niet in gang.
DNSSEC	Ja	ODC-Noord heeft sinds het onderzoek uit 2015 een eigen DNS ingericht, die DNSSEC gebruikt.
IPv6 en IPv4	Deels	Intern wordt IPv6 gebruikt op een specifiek netwerk. Nog niet alle benodigde producten worden met IPv6 aangeboden. Zodra de markt alles op het juiste niveau kan aanbieden zal dit geïmplementeerd worden en de systemen die vanaf het internet benaderbaar zijn ook worden ontsloten via IPv6.
NEN-ISO/IEC 27001/27002	Gepland	ODC-Noord implementeert op dit moment de BIR. Er is nog geen in control statement. De leveranciers van de rekencentra voldoen beide aan ISO 27001. Een BIR-audit op housing is uitgevoerd eind 2014. Er is een ADR (Audit Dienst Rijk) onderzoek gepland per departement. Dit richt zich o.a. op de opvolging die de departementen hebben gegeven aan nog uit te voeren activiteiten genoemd o.a. in de bevindingen uit het BIR onderzoek van de ADR over 2015 (bijvoorbeeld in de vorm van verbeterplannen verankerd in jaarplannen), en op de onderbouwing (dossiervorming) bij de systemen voor het wel of niet voldoen aan de BIR. De planning voorziet dat het onderzoek in november 2016 afgerond is en de rapportage in januari 2017 gepubliceerd wordt.
ODF 1.2, JPEG en PNG	Ja	In de operatie van ODC-Noord wordt over het algemeen gebruik gemaakt van documenten in ODF-formaat. Vanwege opmaak- en interoperabiliteitsproblemen wordt dit voor communicatie met externen beperkt gebruikt.

OWMS	Nee	Hier is nog aandacht voor geweest in versie 1.0 van de ODC-Noord website. OWMS wordt meegenomen in volgende versie. Hiervoor zal in het najaar 2016 nog geen datum gepland worden.
PDF 1.7, PDF A/1, PDF A/2	Deels	V.w.b. uitwisseling van (definitieve) documenten met externe partijen wordt gebruik gemaakt van PDF. PDFCreator van Windows wordt als printoptie in de kantoorautomatiseringsomgeving aangeboden. De standaardinstelling is PDF versie 1.4, optioneel is 1.5. De vraag is uitgezet bij DUO/WPD of het mogelijk is naar een hogere versie af te drukken. Gebruikers van LibreOffice (dat is het meest gebruikte Office-pakket binnen de operationele omgeving van ODC-Noord) kunnen documenten exporteren naar PDF/A-1. Op dit moment is dat nog geen standaard werkwijze.
SAML	Nee	ODC-Noord maakt voor het interne systeem geen gebruik van SAML. Bij het ontwikkelen van diensten ten bate van klanten (SaaS) wordt SAML onderzocht en waar mogelijk toegepast.
TLS 1.2, 1.1 en 1.0	Ja	Beleid van ODC-Noord voor internet-gekoppelde systemen is dat TLS (in volgorde) van TLS1.2, TLS1.1 wordt aangeboden. TLS 1.0 wordt niet toegepast tenzij er een explain komt van de site-eigenaar.
Webrichtlijnen 2	Deels	Websites van ODC-Noord die aan het internet ontsloten zijn, voldoen in principe aan de Webrichtlijnen, dit is een inrichtingseis. ODC heeft de website niet laten toetsen. Het waarmerk drempelvrij is dan ook niet behaald. De WCAG checker op http://checkers.eiii.eu/ geeft bijvoorbeeld bij https://www.odc-noord.nl/over-odc-noord een hoge, maar onvolledige, score van 107/112.
WPA2 Enterprise	Ja	Deze standaard is toegepast waar ODC-Noord wifi gebruikt.

Ten opzichte van het onderzoek van 2015 zijn er enkele ontwikkelingen bij de bestaande standaarden geweest. DNSSEC was in 2015 nog niet geïmplementeerd, maar is dat inmiddels wel. Een aantal standaarden (DKIM, NEN-ISO/IEC 27001/27002) hebben nog wel de status "Gepland", maar er zijn inmiddels nieuwe planningen voor de implementatie gemaakt. Webrichtlijnen was de status vorig jaar Ja, maar bij de voorziening wordt aangegeven dat niet volledig hieraan voldaan wordt; vandaar dat de status naar Deels gewijzigd is.

Ten opzichte van vorig jaar staan er ook een aantal nieuwe standaarden op de lijst: SKOS, SPF, SIKB102 en WPA2 Enterprise. Echter, deze zijn niet relevant voor ODC-Noord. Wel is WPA2 Enterprise toegepast waar ODC wifi gebruikt.

4.23 Ondernemersplein

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

Standaard	Status	Toelichting
BWB	Ja	Binnen de website, de content van AvB, wordt verwezen naar wetgeving conform de BWB standaard
DKIM	Nee	DKIM is nog niet geïmplementeerd. Er zijn op dit moment nog geen plannen om dit te implementeren.

DNSSEC	Nee	DNSSEC is niet geïmplementeerd op www.ondernemersplein.nl.
IPv4 en IPV6	Ja	De website ondersteunt IPv4 en is toegankelijk via IPv6.
NEN-ISO/IEC 27001/27002	Ja	Ondernemersplein is gehost bij de Kamer van Koophandel. Daar liep een ISO 27001 certificeringstraject en Ondernemersplein heeft dit inmiddels toegepast en is door een audit in april 2016 ook gecertificeerd hierop.
OWMS	Nee	De informatie op de website is gemetadateerd volgens een eigen model die past bij de metadatering van de partners.
Webrichtlijnen	Gepland	Er is inmiddels een nieuw design van de website, en de Webrichtlijnen werden als uitgangspunt bij de ontwikkeling aangehouden. Wel is de website op dit moment nog niet gekeurd, maar vanuit het ontwikkelingsteam wordt dit al onderzocht (bijvoorbeeld werd in 2016 een quick scan door een externe partij gedaan) en er is gepland om nog voor eind 2016 aan de Webrichtlijnen te voldoen en dit ook te laten toetsen..
SKOS	Nee	Er wordt niet aan deze standaard voldaan. Het moet nog onderzocht worden of hieraan voldaan zal worden en plannen gemaakt worden.
SPF	Nee	Er wordt niet aan deze standaard voldaan. Het moet nog onderzocht worden of hieraan voldaan zal worden en plannen gemaakt worden.
TLS v1.2, v1.1 en v1.0	Gepland	Volgens het Collegebesluit is v1.2 de norm, maar Ondernemersplein biedt op dit moment alleen TLS v1.0 aan. Dit heeft te maken met de huidige domein/ISP. Er zijn wel plannen om voor eind 2016 hieraan te voldoen.
CMIS v1.0	Ja	Het CMS en ESB zijn CMIS voorbereid. Echter zijn er geen content leveranciers die hun CMS in CMIS vorm aan het Ondernemersplein.nl beschikbaar stellen. Concreet is er dus nog geen toepassing op dit moment en er zijn ook nog geen plannen om dit te doen.

Ten opzichte van het onderzoek uit 2015 zijn er een aantal veranderingen. Bij een aantal van de toen getoetste standaarden is de status van implementatie veranderd: IPv6 en NEN-ISO/IEC 27001/27002 zijn inmiddels geïmplementeerd. Bij Webrichtlijnen en TLS v1.2 was de status in 2015 nog Nee, maar inmiddels liggen er concrete plannen om dit in de toekomst te implementeren.

Ook staan een aantal nieuwe standaarden op de lijst (SKOS, SPF, SIKB0102, en WPA2 Enterprise). Alleen SKOS en SPF zijn hiervan relevant voor de voorziening. Echter, er wordt nog niet aan deze standaarden voldaan.

4.24 Overheid.nl

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

Standaard	Status	Toelichting
DKIM	Gepland	DKIM zou in Q3/Q4 2015 worden geïmplementeerd, maar is nog niet geïmplementeerd. Dit hangt samen met de implementatie van SPF. De inventarisatie hiervoor is inmiddels gestart en er wordt met de hosting partij aan gewerkt zodat dit naar verwachting uiterlijk per 1-1-2017 geïmplementeerd is.
DNSSEC	Ja	Overheid.nl voldoet sinds Q2 2015 aan DNSSEC.

IPv4 en IPV6	Gepland	De voorbereidingen voor de implementatie zijn gestart en is in onderzoek. Omdat achter overheid.nl verschillende applicaties zitten die gefaseerd over gaan kan de beheerorganisatie dat niet precies te voorspelen, maar geeft aan te verwachten dat overheid.nl IPv6 uiterlijk per 1-4-2017 volledig ondersteunt.
NEN-ISO/IEC 27001/27002	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Rijk (BIR) van toepassing die is gebaseerd op NEN-ISO27001. Logius heeft zich over toepassing van deze norm verantwoord door het afgeven van In Control Verklaringen (ICV's) aan de eigenaar (BZK/DGOBR). Vanaf 2015 staat overheid.nl niet meer op die risicokaart van BZK en hoeft geen ICV meer worden afgegeven.
OWMS	Ja	Overheid.nl is gemetadateerd conform OWMS
PDF 1.7 PDF/A-1 PDF/A-2	Ja	De onderdelen van Overheid.nl die in beheer zijn bij Logius kan alleen via het CMS van Overheid.nl een pdf worden geüpload. Logius plaatst alleen PDF's die PDF/A-1a zijn. Het plaatsen van PDF's komt zelden voor. De PDF's van Officiële bekendmakingen zijn in beheer bij KOOP (Uitvoerings-organisatie Bedrijfsvoering Rijk). Logius dwingt niet af dat deze PDF/A-1a zijn.
SKOS	Ja	SKOS is geïmplementeerd voor de waardelijsten van OWMS.
Webrichtlijnen	Gepland	Momenteel vindt herontwerp van de site plaats. Daarin worden webrichtlijnen als verplicht onderdeel meegenomen. Het redesign project heeft als einddatum 1-4-2017.
TLS v1.2, v1.1 en v1.0	Ja	Volgens internet.nl wordt aan deze standaard voldaan.

Ten opzichte van het onderzoek uit 2015 zijn er een aantal ontwikkelingen. De status van IPv4/6 en van de Webrichtlijnen is veranderd van Nee naar Gepland, en TLS is inmiddels geïmplementeerd. Er zijn een aantal nieuwe standaarden op de lijst gekomen (SKOS, SPF, SIKB0102 en WPA2 Enterprise). SKOS is relevant, maar is nog niet geïmplementeerd. Op dit moment wordt nog onderzocht of en wanneer dit zal gebeuren. SPF is mogelijk relevant, de inventarisatie hiervoor is gestart. De andere twee nieuwe standaarden zijn niet relevant voor Overheid.nl.

4.25 P-Direkt

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

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

Standaard	Status	Toelichting
BWB	Ja	Alle verwijzingen naar wetten worden conform de BWB-standaard gemaakt. De redactie heeft de richtlijn dat ze altijd op deze manier handelt bij verwijzingen naar wetsteksten of andere regels en richtlijnen die op wetten.overheid.nl te vinden zijn.
Digikoppeling	Ja	P-Direkt heeft vele interfaces met partijen binnen de overheid, Identity management, HR-data, Arbo-diensten, ziekmeldingen, koppelingen met BD. Salarisverwerkingssysteem werkt op basis van Digikoppeling. Alle nieuwe koppelingen die P-Direkt ontwikkelt, worden gebouwd op basis van Digikoppeling. Richting 2018 migreert de voorziening naar de

		rijksdatacenters, Digikoppeling krijgt dan een nog belangrijkere rol.
DKIM	Ja	P-Direkt maakt gebruik van de mailservers van SSC-ICT, onder andere voor het versturen van de loonstroken aan de medewerkers. P-Direkt heeft aangegeven dat het initiatief voor de adoptie van dit soort standaarden dan ook bij SSC-ICT ligt. Navraag bij SSC-ICT leert dat DKIM actief gemaakt is voor deze mailservice van P-Direkt.
DNSSEC	Nee	Op de Haagse ring maakt het netwerk van SSC-ICT, waar P-Direkt gebruik van maakt, geen gebruik van DNSSEC. Ook hier geldt dat P-Direkt een afnemer is van een Rijksbrede dienst en het initiatief voor het implementeren van DNSSEC bij de SSC-ICT ligt. SSC-ICT geeft in een reactie aan dat zij op hun beurt weer afhankelijk zijn van de leverancier van de Haagse ring, namelijk Logius.
IPv4 en IPv6	Nee	De Haagse ring, waarover eigenlijk al het verkeer naar de P-Direkt loopt, ondersteunt geen IPv6. De P-Direkt voorzieningen, zoals gehost bij Match, ondersteunen in theorie momenteel al IPv6. In de praktijk is nog geen enkele afnemer op IPv6 aangesloten. Op het aanbieden van IPv6 door de Haagse Ring heeft P-Direkt geen invloed.
NEN-ISO/IEC 27001/27002	Ja	Eind 2014 voldeed P-Direkt aan de BIR. Daarover is een in control statement afgegeven. In 2015 werd dit proces herhaald. In 2016-2017 gaat P-Direkt de dienstverleningssystemen migreren naar het Overheids Datacenter onder beheer van SSC-ICT. BIR compliancy is integraal onderdeel van de inrichting van het ODC, en als zodanig daarmee ook voor P-Direkt.
ODF	Nee	Veel brieven die automatisch gegenereerd worden, worden in Word gemaakt en naar managers verstuurd, die deze dan zelf nog aanpassen. P-Direkt gebruikt .doc, omdat dit voor de doelgroep het meest gangbaar is. De ontvanger van de brieven zou dit zelf moeten omzetten met de aanwezige KA software die ODF ondersteunt. Het proces dat brieven genereert is het niet mogelijk ODF bestanden te genereren.
PDF 1.7 – PDF A/1 of PDF A/2	Deels	De meeste zaken die het digitale personeelsdossier ingaan zijn PFD/A. De grootste uitzondering/afwijking zijn de digitale loonstroken, die zijn nog altijd PDF 1.3. Reden/oorzaak is dat deze aangemaakt worden met een standaard SAP conversieroutine die niet anders dan PDF 1.3 kan genereren. Er is momenteel geen concreet plan de loonstroken in PDF A/x te genereren. PDF A/2 wordt nog niet gebruikt binnen P-Direkt.
SAML	Ja	P-Direkt gebruikt SAML om Single Sign-On in te vullen. Verbinding naar de kerndepartementen is gelegd, maar een gedeelte van de rijksambtenaren van onderliggende organisatieonderdelen, moeten nog handmatig inloggen. P-Direkt heeft met de kerndepartementen de afspraak gemaakt dat de kerndepartementen verantwoordelijk zijn voor het implementeren van de Single Sign-on functie bij de onderliggende organisatieonderdelen.
SPF	Gepland	SPF moet nog geïmplementeerd worden door de beheerder van de mail dienst (in het geval van P-Direkt is dat SSC-ICT).
TLS v1.2, v1.1 en v1.0	Ja	Alle diensten van P-Direkt die door middel van HTTP worden ontsloten, worden enkel aangeboden via TLS v1.0 of hoger.
Webrichtlijnen	Nee	Het Portal is nog altijd in ontwikkeling. Er is op dit portal nog geen Webrichtlijnen toets geweest. P-Direkt is zich ervan bewust dat er nog geen volledige compliancy is met de Webrichtlijnen.

Ten opzichte van vorig jaar staat een aantal nieuwe standaarden op de lijst: SKOS, SPF, SIKB0102 en WPA2 Enterprise. Alleen SPF is relevant voor P-Direkt. Voor de implementatie geldt echter hetzelfde als

bij DKIM, namelijk moet deze standaard nog geïmplementeerd worden door de beheerder van de mail dienst (SSC-ICT).

Een nieuwe ontwikkeling ten opzichte van 2015 is de migratie van de dienstverleningssystemen naar ODC in 2016-17. Dit betekent dat BIR compliancy gewaarborgd blijft. Gelet op de ontwikkeling van het portal zijn dit jaar de webrichtlijnen opgenomen in de tabel.

4.26 PKI overheid

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

Standaard	Status	Toelichting
DNSSEC	Ja	Het PKIoverheid-deel van de website van Logius en de website van PKIoverheid maken gebruik van DNSSEC.
IPv4 en IPV6	Deels	IPv6 is inmiddels deels geïmplementeerd voor de websites van de centrale hiërarchie (alleen voor www.pkioverheid.nl). De subdomeinen staan gehost bij een andere partij die (nog) geen ondersteuning biedt voor IPv6.
NEN-ISO/IEC 27001/27002	Ja	Primair is het Webtrust normenkader van toepassing op PKIoverheid. Dit kader kent strengere eisen dan deze ISO standaarden vereisen. Implementatie van de BIR is daarnaast uitgevoerd op basis van best effort.
PDF 1.7, PDF A/1, PDF A/2	Ja	Documenten die via de websites beschikbaar worden gesteld worden volgens PDF/A opgesteld.
Webrichtlijnen	Ja	De website van Logius als de website van PKIoverheid zelf voldoen aan de Webrichtlijnen. Een Waarmerk Drempelvrij is verkregen.
TSL 1.2 en 1.1	Ja	Het PKIoverheid deel van de website van Logius en de website van PKIoverheid maken gebruik van TLS 1.1 en 1.2.
OWMS	Ja	Op website van Logius ja, maar niet op de website van PKIoverheid (info is niet bedoeld voor hergebruik van overheidsinformatie).

Met betrekking tot de standaarden die vorig jaar tijdens het onderzoek op de lijst stonden is bij PKIoverheid een ontwikkeling geweest bij IPv6. De implementatie van deze standaard was in 2015 nog gepland. Inmiddels is de standaard deels geïmplementeerd (voor de website www.pkioverheid.nl). Ook is OWMS dit jaar opgenomen als relevante standaard in de tabel.

Sinds het vorige onderzoek zijn er een aantal nieuwe standaarden op de lijst (SKOS, SPF, SIKB0102, en WPA2 Enterprise). Geen van deze standaarden is relevant voor de voorziening, en ze zijn dus ook niet geïmplementeerd.

4.27 Rijksoverheid.nl

De website Rijksoverheid.nl is de publiekswebsite met informatie van en over alle ministeries. De website wordt verzorgd door de Dienst Publiek en Communicatie (DPC). DPC is een baten-lastendienst van het

ministerie van AZ en biedt shared servicediensten aan de rijksoverheid op het gebied van Communicatie.

Standaard	Status	Toelichting
BWB	Ja	Binnen de website wordt verwezen naar wetgeving conform de BWB standaard. Er worden geen wetsteksten op de website als content geplaatst. Dit is een richtlijn voor de redactie.
DKIM	Ja	DKIM is geïmplementeerd voor de bulk van het mailverkeer. Dit heeft betrekking op de nieuwsbrieven die DPC namens de diverse departementale opdrachtgevers verstuurt. Het gaat om de nieuwsbrieven- en persberichten-service voor de Rijksoverheid en het DPC-mailverkeer. Deze zijn met SPF-DKIM-DMARC uitgerust. DKIM is niet ingericht voor andere DPC-mailstromen, zoals de persoonlijke mailboxen van de medewerkers van DPC, omdat deze lopen via de SSC-ICT mailservers. Dat betekent dat e-mailverkeer gebruikmakend van @rijksoverheid.nl niet onder beheer van DPC valt.
DNSSEC	Ja	Rijksoverheid.nl is ondertekend met DNSSEC. DPC biedt DNSSEC ook aan al haar klanten die domeinen via haar registrar-functie afnemen.
IPv4 en IPV6	Ja	Rijksoverheid.nl ondersteunt zowel IPv6 als IPv4.
NEN-ISO/IEC 27001/27002	Ja	Hosting leverancier Ordina heeft een NEN 27001/2 implementatie waarin de beveiliging van rijksoverheid.nl meegaat. DPC zelf valt onder de VIR/BIR-implementatie van het moederdepartement AZ. Na, onder andere, een analyse van het CMS heeft AZ in december 2014 een Control Verklaring (ICV) afgegeven voor haar ICT omgeving.
OWMS	Ja	De beleidskeuzes (contentmodellen) zijn in te zien in het Informatie Publicatie Model (IPM) bij het OWMS. Zie: http://standaarden.overheid.nl/rijksoverheid.
ODF 1.2 JPEG / PNG	Ja	Het CMS van het Platform Rijksoverheid Online accepteert slechts PDF en ODF formaten. Er zijn wel 'legacy'-bestanden in alleen .doc of .xls formaat. Nieuwe documenten zijn echter altijd tenminste in PDF- of indien bewerkbaar, in ODF-formaat beschikbaar. De PDF-generator die men gebruikt is goed voor het leeuwendeel van de PDF's op de website en genereert PDF-bestanden in PDF/A-1a. Voor afbeeldingen wordt gebruik gemaakt van JPG (foto's) en van 8-bits PNG (logo's).
PDF 1.7 / PDF A/1 en PDF A/2	Deels	De hierboven genoemde lijn is bij de redactie ingezet, maar veel recente stukken worden aangeboden in PDF 1.4. Het gebruik van PDF 1.4 wordt door DPC ontmoedigd. De PDF-generator die men gebruikt is goed voor het leeuwendeel van de PDF's op de website en genereert PDF-bestanden in PDF/A-1a.
SAML	Ja	Er is een soort WeTransfer app binnen het Rijksoverheid online platform. Deze maakt gebruik van SAML voor het authentiseren van gebruikers. Er zijn geen andere diensten die via Rijksoverheid worden aangeboden en inloggen vereisen (met SAML).
Webrichtlijnen	Ja	De website voldoet aan de Webrichtlijnen (versie 2). Zie ook de verantwoording daarover op: http://www.rijksoverheid.nl/toegankelijkheid.
TLS v1.2, v1.1 en v1.0	Ja	Rijksoverheid.nl maakt gebruik van het Platform Rijksoverheid Online en daardoor geheel voorzien van https door middel van PKIoverheid-certificaten.
SPF	Ja	Het e-maildomein @rijksoverheid.nl is integraal van SPF voorzien.

Daarnaast staan ten opzichte van vorig jaar een aantal nieuwe standaarden op de lijst. SKOS, SIKB0102 en WPA2 Enterprise zijn niet relevant voor de voorziening. SPF is dat wel en is ook geïmplementeerd.

4.28 Rijkspas

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

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

Standaard	Status	Toelichting
DKIM	Nee	Voor Rijkspas worden mails verstuurd vanaf de applicatie voor Interdepartementale Toegang (IdT). Daar is nog geen DKIM voor voorzien.
DNSSEC	Nee	Rijkspas communiceert momenteel nog niet via het publieke internet. De verbinding die daarvoor voorzien is, maakt wel gebruik van DNSSEC. Voor communicatie binnen de Rijksoverheid wordt momenteel gebruik gemaakt van de Haagse Ring. Deze ondersteunt geen DNSSEC.
IPv4 en IPV6	Nee	De Haagse ring, waarover eigenlijk al het verkeer naar de Rijkspas voorzieningen loopt, ondersteunt geen IPv6. Deze dienst wordt door Logius geleverd, en is onderdeel van de 'connectiviteitsdiensten' waarvan I&I gebruik maakt.
NEN-ISO/IEC 27001/27002	Ja	De Rijkspas heeft een eigen normen- en beveiligingskader gebaseerd op ISO-9001 en 27001/2. Jaarlijks worden hier ook audits op gedaan, onder andere door de Audit Dienst Rijk.
SAML	Ja	De Interdepartementale Toegang applicatie is per 2015 aangesloten op de Single Sign On voorziening via SAML.
SPF	Nee	Hiervoor moet de impact en de mogelijkheid voor implementatie nog bepaald worden.
TLS v1.2, v1.1 en v1.0	Ja	TLS wordt gebruikt voor het veilig ontsluiten van de website voor IdT.
Digikoppeling	Ja	Rijkspas maakt gebruik van het WUS-gedeelte van de Digikoppeling. De Deelnemers kunnen zelf de keuze maken welk protocol ze hanteren, de standaard koppeling Rijkspas of de Digikoppeling.

Een ontwikkeling sinds 2015 is dat bij het vorige onderzoek Digikoppeling nog niet als relevante standaard voor de Rijkspas beschouwd werd, maar inmiddels wel. Digikoppeling wordt door de Rijkspas toegepast. Daarnaast is ook SAML inmiddels geïmplementeerd door de Rijkspas.

Ten opzichte van vorig jaar staat een aantal nieuwe standaarden op de lijst: SKOS, SPF, SIKB0102 en WPA2 Enterprise. De nieuwe standaarden op de lijst SKOS, WPA2 Enterprise en SIKB0102 zijn niet relevant voor de voorziening, op basis van het op de lijst aangegeven functioneel toepassingsgebied en organisatorisch werkingsgebied. SPF is wel relevant voor de voorziening. Hiervoor zal de impact en de mogelijkheid voor implementatie nog bepaald worden.

4.29 Rijksportaal

Het Rijksportaal is het (rijksbrede) raamwerk voor intranettoepassing voor alle (kern)departementen en verschillende uitvoeringsinstanties. Hiermee is het merendeel van de oorspronkelijke intranetten van de(kern)departementen vervangen. Rijksportaal geeft de rijksambtenaar toegang tot rijksbrede en departementsspecifieke informatie, bronnen en toepassingen. Ook is het vanuit Rijksportaal mogelijk om nieuws van andere departementen te volgen en personeels- en facilitaire zaken te regelen. SSC-ICT voert het technisch beheer over het Rijksportaal in opdracht van BZK/TBGI (de rijksbrede regie organisatie voor generieke ICT).

Standaard	Status	Toelichting
IPv4 & IPv6	Gepland	Het Rijksportaal is nu alleen ingericht voor IPv4. Het door SSC-ICT geleverde netwerk ondersteunt geen IPv6, en IP6 staat niet op de roadmap Rijksportaal. In 2015 was SSC-ICT bezig met het voorbereiden van het netwerk op IPv6 zo dat vervolgens een impactanalyse gedaan kan worden voor het gebruik van IPv6 door het Rijksportaal. Echter, er heeft nog geen impact analyse plaatsgevonden. Navraag in 2016 leerde dat eerst de transitie naar ODC Rijswijk en de release 1.7 afgerond wordt. Verwachte oplevering van IPv6 is januari 2017, tot deze tijd is er een freeze.
OWMS	Nee	OWMS wordt op dit moment niet gebruikt. Er zijn geen plannen om OWMS te gaan gebruiken. Daarnaast is SSC-ICT geen eigenaar van de content. Toen het Rijksportaal in 2007 werd ontwikkeld bestond deze standaard nog niet. Dit onderwerp kan mogelijk worden meegenomen in de doorontwikkeling naar Rijksportaal 2, indien meer bekend is over de impact daarvan op de content en de meerwaarde die dit oplevert ten aanzien van gebruik.
SAML	Ja	De implementatie van SAML is juli 2016 opgeleverd. Het Ministerie V&J zal de eerste klant zijn die gaat aansluiten gebruikers acceptatietesten hebben medio augustus 2016 plaatsgevonden.
ODF (png, jpeg)	Ja	ODF wordt ondersteund. Het kan geüpload en gedownload worden. Ook kan op .odf-bestanden gezocht worden. Rijksportaal (document 'Richtlijnen PDF Rijksoverheid' op het Rijksportaal) bevat wel aanbevelingen ten aanzien van document formaten, maar dwingt dit niet af.
PDF 1.7 PDF/A-1, PDF/A-2	Ja	PDF wordt ondersteund. Het kan geüpload en gedownload worden. Ook kan op .pdf-bestanden gezocht worden. Er wordt alleen gecontroleerd op de bestandsextensie, niet op PDF-versie. Rijksportaal (document 'Richtlijnen PDF Rijksoverheid' op het Rijksportaal) bevat wel aanbevelingen ten aanzien van document formaten, maar dwingt dit niet af.

Het 'pas toe of leg uit'-principe rond Webrichtlijnen geldt strikt genomen niet voor intranet-websites die alleen intern binnen de overheid worden gebruikt. De doorontwikkeling en content inrichting van Rijksportaal richt zich echter wel zoveel mogelijk op toegankelijkheid, zoek- en vindbaarheid en toekomstvastheid, omdat dit als belangrijk wordt gezien voor de verschillende groepen gebruikers die toegang hebben tot Rijksportaal. Rijksportaal voldoet dan ook gemiddeld tot goed aan de kwaliteitseisen uit de Webrichtlijnen.

Ten opzichte van het onderzoek uit 2015 zijn er een aantal nieuwe ontwikkelingen. Zo is de implementatie van de SAML standaard (in 2015 nog gepland) inmiddels opgeleverd. Ten behoeve van de implementatie van IPv6 bestaat inmiddels een concrete planning met verwachte oplevering in januari 2017.

Er zijn ook een aantal nieuwe standaarden op de lijst (SKOS, SPF, SIKB0102 en WPA2 Enterprise). Echter, geen van deze standaarden is relevant voor de voorziening.

4.30 Stelsel Elektronische Toegangsdiensten

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

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

Standaard	Status	Toelichting
DNSSEC	Ja	DNSSEC werd in 2015 in de productieomgeving opgenomen.
NEN-ISO/IEC 27001/27002	Ja	De BIR is van toepassing op Logius, in het stelsel wordt certificering tegen ISO27001 geëist voor de deelnemers. De beheerorganisatie zelf is als stelselbeheerder ook gecertificeerd. Daarvoor is ook een in controlstatement beschikbaar.
PDF 1.7, PDF/A-1 of PDF/A-2	Ja	Stelseldocumentatie wordt met behulp van office software gepubliceerd in PDF/A-formaat. Overige documenten worden met een aparte tool in PDF/A formaat geconverteerd omdat het gehanteerde DMS dit niet ondersteunt.
SAML	Ja	SAML is een verplichte eis vanuit het stelsel.
Webrichtlijnen	Ja	De Webrichtlijnen zijn een eis vanuit het stelsel aan de deelnemers. Bij vermoeden van non-conformiteit kan een toets worden opgestart.
SPF	Ja	SPF wordt toegepast bij de voorziening, maar wordt vooralsnog niet vereist als toe te passen techniek voor deelnemers.
TLS v1.2, v1.1 en v1.0	Ja	Het afsprakenstelsel stelt het gebruik van TLS1.x verplicht.

Ten opzichte van het onderzoek uit 2015 zijn er geen wijzigingen met betrekking tot de toepassing van de open standaarden zoals toen opgenomen in de pas toe of leg uit lijst.

Daarnaast zijn er enkele nieuwe standaarden op de lijst (SKOS, SPF, SIKB0102, WPA2 Enterprise), waarvan alleen SPF relevant is voor de voorziening. SPF wordt dan ook toegepast.

4.31 Samenwerkende Catalogi

Samenwerkende Catalogi koppelt de productcatalogi van verschillende overheidsorganisaties. De koppeling van productcatalogi door Samenwerkende Catalogi maakt het 'no wrong door'- principe mogelijk. Dit bekent dat over organisatiegrenzen heen gezocht kan worden naar producten en diensten. Het is de standaard (specificatie) voor het publiceren en uitwisselen van metadata over producten en diensten binnen de overheid, zoals bijvoorbeeld het aanvragen van een vergunning of het aanvragen van een reisdocument. Deze data is doorzoekbaar door middel van de Zoekdienst van KOOP. De eindgebruiker ziet de zoekdienst niet, maar gebruikt de portalen overheid.nl en ondernemersplein.nl. Overheid.nl gebruikt de Zoekdienst, ondernemersplein.nl heeft een eigen ontsluitingsmechanisme. Daarnaast kan de eindgebruiker via de desbetreffende overheden informatie via samenwerkende catalogi opvragen.

Standaard	Status	Toelichting
OWMS	Ja	Samenwerkende catalogi is volledig gebaseerd op OWMS.
Webrichtlijnen	Ja	Publicatie standaard op www.logius.nl zie aldaar voor Webrichtlijnen compliance. Overheid.nl ontsluit decentrale content op basis van Samenwerkende Catalogi, zie voor Webrichtlijnen compliance aldaar; Publicatie op basis van Samenwerkende Catalogi door overheden op eigen website Webrichtlijnen compliance eigen verantwoordelijkheid deelnemers (Rijk/gemeenten/provincies/waterschappen)

Ten opzichte van het onderzoek uit 2015 zijn de volgende ontwikkelingen te vermelden. Met betrekking tot de in 2015 getoetste standaarden zijn er geen veranderingen. Ook zijn dit jaar Webrichtlijnen als relevante standaard meegenomen.

Geen van de sinds het vorige onderzoek nieuw in de lijst opgenomen standaarden (SKOS, SPF, SIKB0102, WPA2 Enterprise) is relevant voor Samenwerkende Catalogi. Alleen SKOS heeft (indirecte) relevantie: de Samenwerkende Catalogi standaard zelf maakt hier géén gebruik van, want die beschrijft immers geen taxonomie, maar gebruikt wel de OWMS standaard die SKOS toepast. OWMS wordt ook gebruikt voor de voor Samenwerkende Catalogi relevante metadata zoals indeling van organisaties, thema's en productnamen.

4.32 SBR (Standard Business Reporting)

SBR is de nationale standaard voor de digitale uitwisseling van alle bedrijfsmatige rapportages. Sinds 1 januari 2013 is SBR de exclusieve aanlevermethode voor de aangiften van de inkomensbelasting en de vennootschapsbelasting. Vanaf 2014 geldt dit voor de omzetbelasting-aangiften. Ook de statistiek-opgaven en het deponeren van de jaarrekeningen (januari 2015) zal op termijn verplicht via SBR lopen. SBR is gebaseerd op XBRL. De voorziening voor de e-dienstverlening is Digipoort. Daarnaast heeft SBR een website.

Standaard	Status	Toelichting
Digikoppeling	Ja	DK ebMS standaard voor meldingen tussen informatiesystemen wordt ingezet in het kader van SBR voor communicatie tussen Overheid en Digipoort. DK WUS standaard voor de bevraging van informatiesystemen wordt in kader van SBR gebruikt voor o.a. aanleveringen, bijhouden status van aanleveringen, machtigingsregistratie, ophalen mededelingen. WUS voor SBR ingezet voor communicatie tussen Bedrijven en Digipoort.
DKIM	Ja	De website van SBR (http://www.sbr-nl.nl) heeft ook een mailserver. Deze voldoet aan DKIM (volgens internet.nl).
DNSSEC	Nee	De website van SBR (http://www.sbr-nl.nl) is ondergebracht bij een derde partij. Ook het technisch DNS-beheer is daar ondergebracht, maar nog niet alle domeinen maken gebruik van DNSSEC. De Digipoort wordt gedraaid op het platform van EASI Managed Services (EASI MS). EASI MS is het generieke verwerkingsplatform. DNSSEC wordt nog niet gebruikt voor de Digipoort / EASI MS. Er is wel het voornemen om DNSSEC in te voeren, en naar de impact en tijdlijn wordt op dit moment gekeken.
IPv4 en IPv6	Deels	De website van SBR wordt bij een derde partij gehost en is bereikbaar met IPv6. Digipoort / EASI MS is niet bereikbaar via IPv6.
PDF 1.7, PDF A/1, PDF A/2	Ja	Bij het publiceren van documenten houdt Logius voor SBR PDF/A aan bij publicatie.
SPF	Nee	De website van SBR (http://www.sbr-nl.nl) heeft ook een mailserver. Deze voldoet niet aan SPF (zie https://internet.nl/mail/sbr-nl.nl/results).

TLS 1.0, 1.1 en 1.2	Ja	Op het domein sbr-nl.nl, die hoort bij de voorziening) wordt TLS niet afgedwongen (https://internet.nl/site/www.sbr-nl.nl/#). Voor WUS en ebMS geldt dat TLS 1.2 de standaard is. SSL v3 en v3.1 zijn in 2015 uitgefaseerd. TLS 1.0 (en mogelijk ook 1.1) wordt uitgefaseerd (planning 2017). Het koppelvlak Grote Berichten 3.0 en FTPS v1.6.1 worden op TLS 1.1 en 1.2 aangeboden (https://internet.nl/site/www.sbr-nl.nl/#). Voor WUS en ebMS geldt dat TLS 1.2 de standaard is. SSL v3 en v3.1 zijn in 2015 uitgefaseerd. TLS 1.0 (en mogelijk ook 1.1) wordt uitgefaseerd (planning 2017). Het koppelvlak Grote Berichten 3.0 en FTPS v1.6.1 worden op TLS 1.1 en 1.2 aangeboden.
Webrichtlijnen	Nee	SBR-NL.nl voldoet aan de Webrichtlijnen en is hier op getoetst
XBRL	Ja	SBR maakt gebruik van XBRL.

Ten opzichte van vorig jaar staat een aantal nieuwe standaarden op de lijst: SKOS, SPF, SIKB0102 en WPA2 Enterprise. Alleen SPF is van deze standaarden relevant voor de voorziening, omdat de website van SBR (http://www.sbr-nl.nl) ook een mailserver heeft. Echter, deze voldoet niet aan SPF. Ook is de status van IPv4/IPv6 van Nee naar Deels gewijzigd. Bij Webrichtlijnen is dit jaar de status Nee toegepast omdat niet kan worden aangegeven of dit getoetst wordt.

Een andere ontwikkeling ten opzichte van het vorige onderzoek is dat er inmiddels plannen zijn om DNSSEC te implementeren. Een tijdslijn is nog niet bekend.

4.33 Stelselcatalogus

De Stelselcatalogus is een online catalogus die inzicht geeft in welke gegevens het Stelsel van Basisregistraties bevat, wat ze betekenen en hoe ze met elkaar verbonden zijn. Met die informatie kunnen overheden bepalen of de gegevens uit de basisregistratie(s) makkelijk zijn in te passen in hun eigen werkprocessen. De Stelselcatalogus wordt beheerd door Logius.

Standaard	Status	Toelichting
BWB	Ja	De Stelselcatalogus gebruikt het Basis Wetten Bestand (BWB) via Juriconnect als open standaard voor de link naar de wetgeving als bron. De Juriconnect Id's worden gebruikt om per gegeven of begrip in de Stelselcatalogus de link te leggen naar de wet en het artikel in het Basis Wetten Bestand.
OWMS	Ja	OWMS is als standaard gebruikt binnen digitaleoverheid.nl. De webpagina's van Stelselcatalogus vallen binnen deze website.
PDF 1.7, PDF A/1, PDF A/2	Ja	Documenten worden als PDF-A/1 aangeboden via de website.
Webrichtlijnen	Ja	De webpagina's van de Stelselcatalogus vallen binnen de website van digitaleoverheid.nl. Zie certificaat van toegankelijkheid van Accessibility.nl
SKOS	Ja	SKOS wordt toegepast door de voorziening.
DKIM	Gepland	Digilevering draait op het platform van Logius Managed Services. Aanpassingen op dit platform ter ondersteuning van de standaard worden Logius breed aangepakt. Het voldoen aan beveiligingsstandaarden, waaronder DKIM, wordt opgenomen in het jaarplan 2017. Dit wordt echter per dienst geïmplementeerd.
DNSSEC	Gepland	Digilevering draait op het platform van Logius Managed Services. Aanpassingen op dit platform ter ondersteuning van de standaard worden Logius breed aangepakt. Voor DNSSEC geldt dat een aantal diensten gebruik van maakt van DNSSEC en een aantal nog niet. Er loopt een traject om alle diensten van Logius te voorzien van DNSSEC. De planning hiervan is Q4 2016, Q1 2017.

IPv4 en IPv6	Gepland	Digilevering draait op het platform van Logius Managed Services. Aanpassingen op dit platform ter ondersteuning van de standaard worden Logius breed aangepakt. IPv6 wordt door de meeste diensten gebruikt. Enkele (legacy) implementaties gebruiken dit nog niet. De platformen ondersteunen dit en er is een IPv6 adresplan beschikbaar. Het omzetten wordt in het jaarplan 2017 meegenomen.

Ten opzichte van het onderzoek uit 2015 zijn DKIM, DNSSEC en IPv4/IPv6 als relevante standaarden voor deze voorziening toegevoegd. Ook is OWMS inmiddels geen relevante standaard meer. De reden hiervoor is dat de website van de Stelselcatalogus sinds 2015 gehost wordt op de Logius website. Stelselcatalogus verstrekt geen metadata op de website. Als er pagina's aan toegevoegd worden met bijvoorbeeld overzichten van basisregistraties en hun bronhouders, dan wordt gekeken of de weergave daarvan strookt met de weergave zoals gestandaardiseerd door OWMS. In principe wordt OWMS dus toegepast, alleen is er voor de website in zijn huidige vorm geen content waarvoor OWMS relevant is.

Ook staan er een aantal nieuwe standaarden op de lijst, waarvan alleen SKOS relevant is.

4.34 TenderNed

TenderNed is het online marktplein voor aanbestedingen van de Nederlandse overheid. Het is een volledig digitaal aanbestedingssysteem voor aanbestedende diensten en ondernemingen in Nederland.

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

Standaard	Status	Toelichting
DKIM	Nee	E-mails verzonden vanuit TenderNed zijn niet beveiligd met DKIM.
DNSSEC	Nee	Het domein is niet gesigned met DNSSEC. TenderNed is afhankelijk van de registrar. Dat is Dienst Publiek en Communicatie van het Ministerie van Algemene Zaken. Wanneer deze een transitie door maakt naar DNSSEC zal TenderNed daar in mee gaan. TenderNed zal DNSSEC alleen eerder invoeren als dat vanuit strategisch niveau door EZ wordt besloten. TenderNed gaat DNSSEC het niet proactief implementeren.
IPv4 en IPV6	Nee	Tenderned.nl is niet voorbereid op IPv6 (https://internet.nl/site/tenderned.nl/results#). TenderNed is afhankelijk van de hostingpartij. Wanneer deze een transitie door maakt naar IPv6 zal TenderNed daar in mee gaan.
NEN-ISO/IEC 27001/27002	Ja	TenderNed is ISO27001/2 gecertificeerd. (Bron http://www.tenderned.nl/sites/default/files/Gebruiksvoorwaarden_TenderNed_juni_2014_0.pdf)
PDF 1.7, PDF/A-1, PDF/A-2	Ja	Geautomatiseerd gecreëerde PDF's (bij de aankondigingen) zijn gemaakt in versie 1.7.
SAML	Ja	Per 1 juli 2014 is het mogelijk voor gebruikers om, naast de huidige registreer- en inlogmogelijkheden, gebruik te maken van inloggen via eHerkenning. De huidige mogelijkheden worden vanaf deze datum uitgefaseerd. (http://www.tenderned.nl/eherkenning-en-tenderned-0)
SPF	Ja	TenderNed past de SPF standaard toe.
Webrichtlijnen	Ja	Voldoet, zie de eigen uitleg op http://www.tenderned.nl/tenderned-voldoet-aan-Webrichtlijnen
TLS v1.2, v1.1 en v1.0	Ja	TenderNed past TLS 1.2 toe.

Ten opzichte van het vorige onderzoek zijn er twee ontwikkelingen. Ten eerste is inmiddels een upgrade doorgevoerd van TLS v1.0 naar v1.2, dus TenderNed voldoet hier aan de norm. Ten tweede is sinds 2015 een aantal nieuwe standaarden aan de lijst toegevoegd (SKOS, SPF, SIKB0102 en WPA2 Enterprise), waarvan alleen SPF relevant is. TenderNed voldoet ook aan deze standaard.

5 Essay #2: De rol van maatwerk-leveranciers

Verken de speelvelden, en speel met de relevante spelers

Op ons verzoek hebben de onderzoekers van PBLQ - Piet Hein Minnecré en Florian Henning - nog een tweede essay geschreven. Ook dit tweede essay heeft, hoewel het onderdeel is van de Monitor Open Standaardenbeleid, een ander karakter. De Monitor richt zich op de kwantitatieve kenmerken van de adoptie van open standaarden, dit essay heeft een kwalitatief en explorerend karakter.

Vorig jaar is als onderdeel van de Monitor Open Standaardenbeleid 2015 onderzoek gedaan naar de invloed van gemeentelijke softwareleveranciers op het gebruik van standaarden bij de overheid. De conclusie was toen dat gemeentelijke leveranciers een grote invloed hebben op de adoptie van open standaarden, maar dat zij in beperkte mate in staat zijn om als individuele leverancier de snelheid van adoptie te beïnvloeden. Op basis daarvan zijn toen een aantal aanbevelingen voor het Forum geformuleerd, onder meer over het zoeken naar aansluiting bij zogenaamde 'burning platforms' en daarbij te kiezen voor een brede aanpak gericht op het oplossen van het interoperabiliteitsvraagstuk.

Ook dit jaar is ons gevraagd om – wederom in het kader van de Monitor – een aantal gesprekken met leveranciers te voeren om op die manier meer begrip te krijgen voor de factoren en partijen die van invloed zijn op de adoptie van standaarden. Deze keer waren het niet de leveranciers van gemeentelijke software, maar is ervoor gekozen een aantal gesprekken te voeren met marktpartijen die zowel system integrator zijn als leverancier van maatwerksoftware. De reden voor deze onderzoeksopzet was om te kijken hoe zich de bevindingen van het leveranciersonderzoek uit 2015 verhouden tot deze groep van leveranciers. Gelden dezelfde conclusies en aanbevelingen voor alle soorten leveranciers, of kunnen er duidelijke verschillen benoemd worden? En wat kan je doen om deze leveranciers te betrekken, op welke issues en stakeholders moet je dan focussen?

Dit essay is gebaseerd op die gesprekken, de gesprekken met de beheerders van de GDI-voorzieningen, maar ook aangevuld met onze eigen kennis en meningen.

Dat gezegd zijnde, vallen we graag met de deur in huis. Naar aanleiding van deze ronde concluderen we dat de bevindingen van vorig jaar prima overeind blijven, maar dat de rol van grote marktpartijen die zich positioneren als system integrator en als maatwerkleveranciers heel anders is dan die van de leveranciers in het gemeentelijke veld. De rol van de leveranciers die wij dit jaar spraken is veel kleiner wanneer het gaat om de adoptie van standaarden van de lijst van het Forum. Samengevat: het spel dat gespeeld moet worden veranderd niet, het speelveld verandert wel. En daarmee wisselen per domein en soms per standaard de partijen waarmee je het moet spelen.

5.1 Een ander speelveld

Het bleek dit jaar niet makkelijk om grote marktpartijen zover te krijgen mee te werken aan een interview over het gebruik van standaarden van de lijst van het Forum. In dit soort gevallen is het altijd een beetje raden waarom het zo lastig blijkt. Ongetwijfeld is een deel van het antwoord dat dit zeer grote wereldwijde bedrijven betreft, waarbinnen het lastig is de juiste gesprekspartners te vinden die zichzelf ook nog capabel en gemandateerd voelen om namens het bedrijf uitspraken te doen. Maar op basis van de informatie en gesprekken die we wel hadden, wordt duidelijk dat er ook nog wat anders speelt.

5.1.1 De PTOLU-standaarden lijken geen issue voor deze partijen

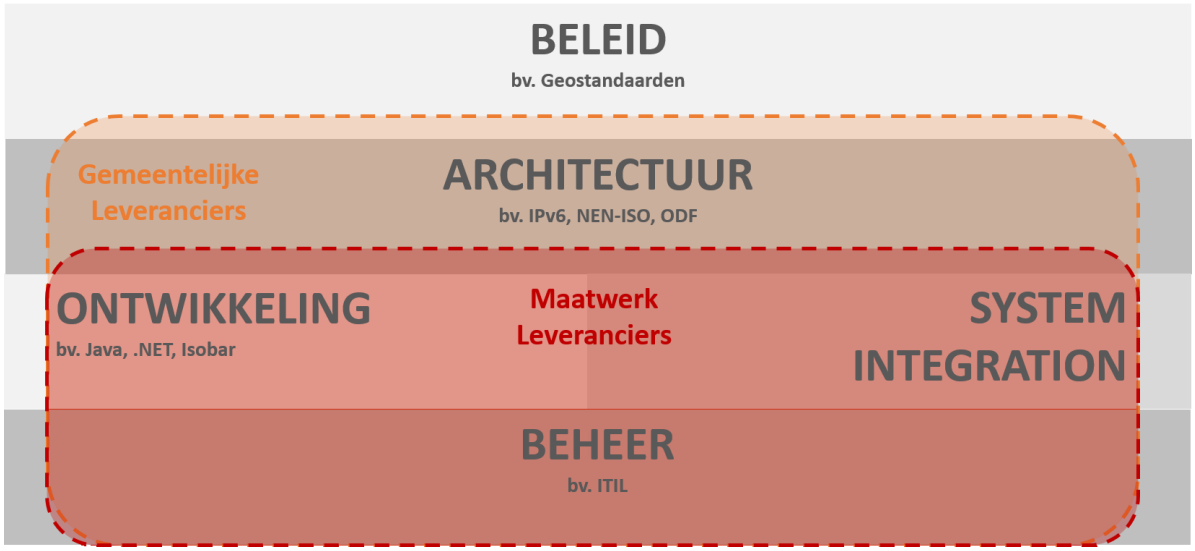
Deze leveranciers lijken zich weinig bezig te houden met de standaarden op de PTOLU-lijst. Niet alleen is de lijst niet goed bekend, maar ook de standaarden van de lijst worden niet genoemd en zijn nauwelijks bekend. Dat wil vast niet zeggen dat niemand binnen dergelijke grote bedrijven bekend is met de standaarden, maar het blijkt zeker geen onderdeel van hun beleid te vormen. Uitzondering

daarop waren de beveiligingsstandaarden zoals ISO27001 en ISO27002, en de meer technische standaarden. Voor de beveiligingsstandaarden geldt dat leveranciers intern beleid hebben om aan deze breed gedragen internationale standaarden te voldoen. Dat beleid voeren ze vanuit hun eigen verantwoordelijkheid, maar ook omdat klanten (overheid en bedrijfsleven) hier om vragen. Deze categorie standaarden vallen onder de noemer 'grote bekende technische standaarden die ingebakken zitten in producten' die de leveranciers leveren, denk aan IPv6. De PTOLU lijst is voor hen dus geen punt van aandacht.

Dat was vorig jaar wel degelijk anders. Toen gaven alle betrokken leveranciers uit het gemeentelijke domein aan de lijst te kennen en hadden ze er een mening over. Zo werd toen aangegeven dat de PTOLU lijst handig is bij het plannen van de lange termijn doorontwikkeling van hun software, en dat het een nuttig instrument is in het gesprek met hun klanten. Maar ze konden ook expliciet kritiekpunten benoemen, bijvoorbeeld de grote diversiteit van standaarden op de lijst en over het gebrek aan uitleg over de implementatie. Ook voelden leveranciers zich te weinig betrokken bij de PTOLU lijst.

5.1.2 Andere rol, en ook andere standaarden

De onbekendheid met de lijst van standaarden is voor een groot deel te verklaren door het verschil in rol tussen deze partijen en de partijen die we vorig jaar spraken. We illustreren dit met onderstaande figuur. Deze geeft een sterk vereenvoudigd beeld van het proces van de ontwikkeling weer: van beleid, naar de inrichting van architectuur, naar ontwikkeling en/of system integration, tot het beheer van software. In elk van deze lagen worden in de praktijk keuzes voor het gebruik van standaarden gemaakt. In de figuur hebben we ter illustratie een aantal relevante standaarden geplot.



Als we de standaarden van de PTOLU lijst volledig zouden plotten op de figuur, dan zou duidelijk worden dat de meeste keuzes hierover gemaakt worden in het ontwerp van de architectuur. In tegenstelling tot gemeentelijke leveranciers zijn de maatwerk softwareontwikkelaars hier veel minder mee bezig. Zij komen aan bod als de belangrijkste keuzes gemaakt zijn en werken bijvoorbeeld een PSA verder uit in meer gedetailleerde ontwerpen op basis waarvan ze software bouwen. Hun impact op de keuze van de standaarden is daarmee ook veel kleiner. Vanzelfsprekend worden de standaarden van het Forum wel gebruikt in en door de software die ontwikkeld wordt, maar de keuze voor de standaard wordt er niet bij deze partijen gemaakt.

Daarnaast hanteren de maatwerkleveranciers wel degelijk standaarden. Maar met uitzondering van de eerder genoemde beveiligingsstandaarden gaat het dan meestal om standaarden voor 'good coding', zoals ISOBAR Code standards en Best Practices of om gestandaardiseerde ontwikkel- en beheermethodieken. Dergelijke standaarden liggen (tot nu toe) buiten de scope van de lijsten van het Forum.

Bij de leveranciers van gemeentelijke software lag dat anders. Ook zij (zeker de grotere partijen) zijn actief in de ontwikkeling en het beheer van software, maar daarnaast hebben zij ook een rol in de

hoger gelegen lagen. Vaak zijn zij het die doorvertaling van (nieuwe) wet- en regelgeving naar de software maken. Daarbij maken ze keuzes voor bepaalde standaarden en ontwikkelen ze zelf standaarden voor gegevensuitwisseling. Dat is ook precies het terrein waar de samenwerking (en soms frictie) met KING en gemeenten ontstaat. De leveranciers die we voor dit onderzoek spraken spelen veel minder een rol in die laag. Architectuur wordt veelal bepaald door de architecten die bij de overheid zelf actief zijn en werken aan de ontwikkeling van bijvoorbeeld de generieke voorzieningen.

5.2 Elk domein, subdomein en elke standaard is weer anders

5.2.1 'De leverancier' bestaat niet

Natuurlijk is bovenstaande een sterke generalisering van leveranciers. Niet alle gemeentelijke leveranciers vertalen beleid naar software, en vanzelfsprekend werken er architecten bij de leveranciers van maatwerk en beheer. Veel leveranciers zijn dusdanig groot dat ze actief zijn in meerdere domeinen en daarbij ook telkens verschillende rollen op zich nemen. Wat die rol precies is, en wat hun invloed is op het gebruik van standaarden, wisselt daarmee. Dat wisselt overigens ook per domein, per thema en standaard. Juist door die diversiteit wordt het uiterst moeilijk voor het Forum om een "algemeen" leveranciersbeleid te bepalen dat voor alle groepen leveranciers effectief is.

5.2.2 Een paar voorbeelden

Om bovenstaande te illustreren geven we een paar voorbeelden van de verschillen per domein.

- Veel van de **GDI-voorzieningen** worden ontworpen en/of doorontwikkeld door ICTU en/of Logius. Deze partijen ontwikkelen daarbij een architectuur en maken daarbij de keuze voor de relevante standaarden, voor zover deze nog niet in de opdracht meegegeven zijn. Maatwerkleveranciers werken deze architectuur verder uit in ontwerpen, maar zijn nauwelijks meer van invloed op de keuze voor standaarden. Wie in dit vlak invloed uit wil oefenen, moet zich richten op de opdrachtgever (beleid), de architecten van ICTU en/of Logius.
- Uit de interviews met de grote leveranciers van maatwerk en system integratie kwam naar voren dat zij geregeld spreken met de CIO's van het Rijk. Die gesprekken gaan dan vaak over de ICT voor de eigen **bedrijfsvoering** van de overheid en in mindere mate over de hulp bij de ontwikkeling van specifieke voorzieningen of de ontwikkelingen ten aanzien van bepaalde beleidsthema's.
- Bij de **technische infrastructuur** (waar standaarden als IPv6 etc. relevant zijn) ligt dat vaak weer net anders. Deze standaarden worden meestal niet opgenomen in de architectuur van de voorzieningen omdat het beschouwd wordt als basisinfrastructuur. De onderliggende laag wordt vaak weer geleverd door andere partijen, zoals DICTU en SSC-ICT die weer afhankelijk zijn van hun eigen opdrachtgevers, van de vraag van de voorzieningen en hun opdrachtgevers, maar ook van hun eigen leveranciers.
- Bij **gemeenten** geldt dat zij zelf veel invloed uitoefenen op hun ICT, maar ook KING werkt sterk aan het gebruik van standaarden. Daarnaast spelen de leveranciers zoals ook eerder beschreven in het gemeentelijke domein een stevige rol.
- Uit eerder onderzoek voor het Ministerie van Economische Zaken blijkt dat in het primair **onderwijs** de rol van uitgevers heel belangrijk is [59]. Zij ontwikkelen de lesmethode en leveren vaak ook software die daarbij gebruikt wordt. Daarnaast werkt Kennisnet aan de standaardisatie in het onderwijs. Voor het HBO's en Universiteiten werkt het weer heel anders.
- In de wereld van het **watermanagement** (AQUO standaard) wordt een belangrijke rol vervuld door bijvoorbeeld het Informatiehuis Water, maar zie je ook dat die wereld zeer gefragmenteerd is door grote veelheid aan partijen en belangen (kennisinstituten, decentrale overheden, ondernemers etc.) en het gebrek aan punten waar centraal gestuurd wordt. Sturing is dan lastig, terwijl standaardisatie wel erg noodzakelijk is.

Bovenstaande voorbeelden zijn een sterk vereenvoudigde weergave van de vaak complexe dynamiek waar de keuze voor de adoptie van standaarden tot stand komt. Ze geven echter goed

[59] https://www.rijksoverheid.nl/binaries/rijksoverheid/documenten/rapporten/2009/05/07/het-actieplan-noiv-en-het-onderwijs-een-verkenning-van-mogelijke-stimuleringsmaatregelen/08et21.pdf

weer dat er geen one-size-fits-all-aanpak te hanteren valt. Waar het beste invloed aangewend kan worden, is per domein en per type standaard sterk wisselend.

5.3 Conclusie en aanbevelingen

5.3.1 Deze groep leverancier heeft een beperkt invloed op de adoptie

Leveranciers van maatwerksoftware hebben een beperkte rol bij de keuzes voor het gebruik van standaarden van de PTOLU lijst. Het lijkt dan ook weinig zin te hebben voor het Bureau Forum Standaardisatie om veel inspanning op deze groep te richten. In de rol van system integrator lijkt hun invloed wat groter, al lijkt die zich dan vooral te beperken tot de ICT ter ondersteuning van de bedrijfsvoering van de overheid. De leveranciers geven zelf aan dat de CIO daar een belangrijke gesprekspartner is, en dat lijkt dan ook een logisch aanknopingspunt voor het Forum om te kijken of de gezamenlijke belangen verder versterkt kunnen worden.

5.3.2 Niet alleen hoe je speelt, maar ook waar en met wie je speelt

De aanbevelingen uit het essay van vorig jaar waren sterk gericht op hoe je het spel kan spelen om effectief invloed uit te oefenen. Dat wordt dit jaar aangevuld met de notie dat ook de spelers in het spel elke keer anders zijn, afhankelijk van het spelveld waar het om draait.

Bij de gemeentelijke leveranciers werd in het essay van vorig jaar geconstateerd dat ze wel degelijk invloed hebben op de toepassing van standaarden in hun producten en dienste. Gezien die invloed is het mogelijk om die leveranciers te activeren en te hanteren als drijvende kracht achter de adoptie van standaarden. Bijvoorbeeld door de leveranciers mee te nemen in de ontwikkeling van het standaardisatiebeleid, door duidelijkere roadmaps aan te geven om hun waarneming van onvoorspelbaarheid in het standaardisatiebeleid weg te nemen, door gebruik te maken van impactanalyses voor leveranciers zoals die van KING, of door het certificeren van leveranciers die aantoonbaar voldoen aan de standaarden van de lijst.

Echter, bij de leveranciers van maatwerk en system integrators zijn deze bevindingen en aanbevelingen niet per se van toepassing. Deze partijen blijken in de praktijk veel minder van invloed op de keuzes voor de PTOLU-standaarden van het Forum. Deels om dat ze niet over de keuze gaan (die wordt vaak door de architecten van de opdrachtgever gemaakt) maar ook omdat de ze gezien de aard van hun producten en diensten veel minder bezig zijn met de PTOLU-standaarden. Onder de noemer “standaardisatie” vallen bij hun meestal een heel andere type standaarden. De verwachting is dat rol van leveranciers en de wijze waarop ze te beïnvloeden telkens net anders zal zijn.

Het is lastig om in algemene zin vast te stellen waar de keuzes voor standaarden bepaald worden. Eigenlijk is dat sterk afhankelijk van het domein, de partijen, hun rollen, maar ook van de standaard en dus ook van individuele personen. Wie invloed uit wil oefenen moet goed weten waar deze het beste aangewend kan worden[60].

Dat beeld wordt versterkt door het onderzoek dat Marthe Fuld eerder dit jaar voor het Forum Standaardisatie deed[61], waaruit bleek dat de inkopers van organisaties een beperkte rol hebben bij keuze voor standaarden (terwijl het PTOLU-beleid juist erg aan het inkoopproces is opgehangen). Daarnaast zijn er nog de bevindingen uit het eerste (‘Van toetsen naar verleiden’), zie paragraaf 4.2. Daarin komt de rol van zogenaamde ‘innovatoren’ sterk naar voren. Bij deze ‘innovatoren’ (met name architecten, technisch en proces specialisten) bepalen keuzes ten aanzien van standaarden op basis van meritocratie. Deze ‘innovatoren’ zijn vaak de mensen in de uitvoeringsteams die een goed zicht hebben op wat er speelt en relevant is in de context van een organisatie. Zij spelen het spel op basis

[60] Technieken zoals stakeholderanalyses en het opstellen van beïnvloedingsdiagrammen (of causale relatiediagrammen) zijn uitstekende hulpmiddelen om te kijken waar keuzes gemaakt worden, welke invloeden daarop werken, en waar gedrukt kan worden om verandering te bewerkstelligen. Nog krachtiger werken deze middelen als ze samen met de betrokken actoren worden opgesteld waarbij dan gelijk het gesprek gevoerd kan worden over de eigen rol in de adoptie van standaarden.

[61] https://www.forumstandaardisatie.nl/sites/bfs/files/atoms/files/FS_160608.5A_Eindrapportage_open_standaarden_bij_aanbestedingen.pdf

van hun eigen kennis en kunnen hiermee juist wel of juist niet bijdragen aan het succes van open standaarden. Voor het Forum kunnen deze 'innovatoren' dus een belangrijke ingangs- of beïnvloedingspunt zijn. Deze groep actoren kan door een partij als het Forum het meest effectief bereikt worden door de relevante expertise te bezitten en bovendien hun specifieke domein goed te kennen.

Het is echter voor het Forum in zijn huidige vorm en omvang niet mogelijk om voor alle 38 standaarden de omgeving en relevante stakeholders voldoende te kennen om die rol overal te spelen. Focus is daarom noodzakelijk. Alleen dan kan het Forum zijn invloedsfeer verhogen.

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

Een belangrijk beleidsinstrument binnen 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.

Dr. mr. M.H. (Mathieu) Paapst (RU Groningen) heeft enkele jaren geleden onderzoek gedaan naar de Europese aanbestedingen door de publieke sector in de eerste helft van 2010[62]. Daarbij is per aanbesteding 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'). Uit dit onderzoek kwam naar voren dat de overheid het beleid dat vanuit de Rijksoverheid is geformuleerd ten aanzien van het gebruik van open standaarden slechts in beperkte mate uitvoert.

In het kader van het onderzoek Monitor Open standaardenbeleid 2016 is nu voor het vijfde achtereenvolgende jaar een soortgelijk onderzoek gedaan. De aanpak en de resultaten daarvan komen aan bod in paragrafen 6.1, 6.2 en 6.3. Vanaf 2014 is daar een element aan toegevoegd, door een deel van de onderzochte aanbestedingen bij wijze van second opinion door een tweede expert te laten beoordelen. Een dergelijke tweede beoordeling is ook dit jaar weer uitgevoerd, inmiddels voor de derde keer. De opbrengst staat beschreven in paragraaf 6.4.

6.1 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) en de decentrale overheden (voor de periode Q3 en Q4 2015 en Q1 en Q2 2016). Dit jaar is dat, net als vorig jaar, uitgevoerd door eerdergenoemde dr. mr. M.H. Paapst (RUG). 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[63]). 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 van de aanbestedingen moeten de aanbestedingsdocumenten bestudeerd kunnen worden. In de praktijk van het onderzoek hebben zich in dat verband enkele knelpunten voorgedaan. Een opvallend punt bij deze monitor 2016 is dat bij 'Rijksoverheid' sprake is van beduidend minder aanbestedingen dan in voorgaande jaren terwijl de omvang van de populatie voor de andere overheden qua omvang wel goed vergelijkbaar is met eerdere jaren. Een sluitende verklaring hiervoor valt niet te geven; daar is geen onderzoek naar gedaan. Wat deze keer wel is

[62] Onderdeel van zijn promotieonderzoek naar de aanbestedingspraktijk. De betreffende resultaten zijn gepubliceerd als *ICT beleid en aanbestedingspraktijk - 1e tussenrapportage,* 15 november 2010.
[63] Voor de periode 2014/2015 lagen deze bedragen marginaal lager: € 134.000 voor het Rijk en voor decentrale overheden € 207.000.

opgevallen, is dat er duidelijke signalen zijn dat er meer dan voorheen gebruik wordt gemaakt van raamovereenkomsten. Daarbij zijn deze raamovereenkomsten vaak zodanig ingericht (ofwel in algemene - soms vage - termen geformuleerd, ofwel heel breed met een bundeling van een groot aantal te onderscheiden opdrachten) dat het niet goed mogelijk is om met voldoende zekerheid te bepalen welke standaarden van de ptolu lijst op die specifieke raamovereenkomst van toepassing zijn; het toepassingsgebied is niet voldoende scherp vast te stellen. Ook al ligt het voor de hand dat in een later stadium - als sprake is van een daadwerkelijke gerichte en duidelijk afgebakende aanbesteding - wel standaarden van de ptolu lijst relevant zijn, dan zijn deze raamovereenkomsten toch in dit vroege stadium gekwalificeerd als '(nog) niet beoordeelbaar'. Geredeneerd vanuit de beleidsdoelstelling om de toepassing van deze standaarden van de ptolu lijst in te voeren, is met deze praktijk sprake van een onwenselijke situatie. Sturing op de uitvoering van dit beleid wordt zo minder eenvoudig. Vanuit de aanbestedingspraktijk: als de uitvraag dan ook nog wordt begeleid met de zinsnede "wij willen als organisatie vooral ontzorgd worden", dan kan het beeld ontstaan dat de inkopende organisatie afscheid neemt van haar rol als richtinggevende marktspeler waar het gaat om software-ontwikkeling met inbegrip van het gebruik van open standaarden.

Andere knelpunten waarmee de beoordelaars te maken hebben gehad:

- van een deel van de aanbestedingen bleken de documenten bij nader onderzoek niet (meer) beschikbaar via Negometrix;
- in een enkel geval was bij nadere beschouwing sprake van een niet-openbare aanbesteding;
- een aantal aanbestedingen was voor dit onderzoek minder geschikt omdat sprake was van een aanbesteding op bijvoorbeeld onderhoud en licentiebeheer of van aanschaf van hardware. De competitie blijft in die gevallen beperkt tot een strijd om de laagste winstmarge in plaats van om een 'battle' tussen elkaar beconcurrerende pakketten.

De beoordeling van aanbestedingen heeft plaatsgevonden in drie opeenvolgende tranches: juli tot en met december 2015, januari tot en met maart 2016 en april tot en met juni 2016. Het streven is erop gericht geweest om 50 aanbestedingen te beoordelen: 34 van de Rijksoverheid en 16 van mede-overheden, zoveel als mogelijk gespreid over de tranches. Mede als gevolg van bovenstaande knelpunten is daarvan noodgedwongen afgeweken. Deze knelpunten deden zich –zoals eerder al opgemerkt- voornamelijk voor bij aanbestedingen Rijksoverheid waardoor de spoeling daar uiteindelijk dun werd. Uiteindelijk zijn 44 aanbestedingen beoordeeld en van een kwalificatie voorzien: 21 bij het Rijk (departementen en uitvoeringsorganisaties) en 23 bij mede-overheden. Het aandeel aanbestedingen Rijksoverheid (48%) ligt daarmee lager dan vorig jaar (in 2015 52%) maar hoger dan in de jaren daarvoor (35% in 2014 en 33% in 2013). De 44 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 relatief veel 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 vorig jaar groot. Enkele willekeurige voorbeelden van aanbestedingen die zijn beoordeeld:

- virtuele assistent ten behoeve van vragen bij eindgebruikers (Rijk);
- ontwikkeling, implementatie en beheer van een online onderzoeksplatform (uitvoeringsorganisatie / Rijk);
- beheer en onderhoud en verdere ontwikkeling van tij-poortadviseringssysteem (uitvoeringsorganisatie / Rijk);
- levering van werkplekapparatuur en gerelateerde diensten (politie);
- realiseren en implementeren van een e-HRM systeem (provincie);
- realisatie en onderhoud van een web presence (gemeente);
- werkprocesapplicatie met zaakgerichte, objectgerichte en DMS-functionaliteit (veiligheidsregio);
- aanschaf en onderhoud van een applicatie Basisregistratie Adressen Gebouwen (gemeente);
- onderhoud en levering van Microsoft-licenties (waterschap).

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 de Nota van Inlichtingen ook niet heeft meegewogen bij het opmaken van de beoordeling. Bij de vorige monitor (2015) zou het al dan niet in de beschouwing meenemen van de informatie uit de Nota van Inlichtingen in een enkel geval van invloed zijn geweest op de beoordeling. Dit jaar was daarvan geen sprake. Daarnaast is onderzocht op welke wijze de verantwoording ('leg uit') over 2015 heeft plaatsgevonden[64].

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.

[64] Dit jaar is voor twee sets van beoordeelde aanbestedingen nagegaan in hoeverre 'leg uit' heeft plaatsgevonden: de set aanbestedingen uit Q3 en Q4 2015 die in deze Monitor 2016 zijn beoordeeld èn de set aanbestedingen uit Q1 en Q2 2015 die vorig jaar zijn beoordeeld (in het kader van de Monitor 2015).

6.2 'Pas toe of leg uit' bij feitelijke aanbestedingen in 2015/2016

Pas toe

In totaal had in de eerdergenoemde 44 aanbestedingen om 257 open standaarden gevraagd moeten worden, feitelijk werd er echter 113 keer om een open standaard gevraagd - dat is dus 44% daarvan (zie tabel 16), vergelijkbaar met het percentage van vorig jaar (2014/2015: 43%). Over de jaren 2012 en 2013 lag dit percentage beduidend lager, op respectievelijk 30% en 25%.

Bij 8 van de 44 aanbestedingen (18%; vorig jaar 21%) werd om alle relevante open standaarden gevraagd, dat is 'pas toe' in strikte zin: 2 aanbestedingen door een ministerie, 1 door een uitvoeringsorganisatie, 3 door gemeenten, 1 door de politie en 1 door een veiligheidsregio.

Daarnaast werd bij 24 aanbestedingen (55%; vorig jaar 50%) gevraagd om een deel van de voor die aanbesteding relevante standaarden.

Bij de resterende 12 aanbestedingen (27%; vorig jaar 29%) - 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 (18%),
- er is om een deel van de relevante open standaarden gevraagd, onderverdeeld in:
    - er is om de (lees: alle) cruciale open standaarden gevraagd maar om één of meer andere niet (9%),
    - er is om open standaarden gevraagd, maar om minimaal een cruciale niet (45%),
- er zijn geen relevante open standaarden gevraagd, onder te verdelen in:
    - er wordt alleen verwezen naar architectuur-kaders (2%),
    - er wordt in algemene zin aandacht besteed aan open standaardenbeleid (2%),
    - er is geen aandacht voor open standaardenbeleid (23%),
    - de aanbesteding is strijdig met het open standaardenbeleid (0%)[65].

[65] Bij de vorige monitor kregen nog twee aanbestedingen het predicaat 'strijdig met open standaarden beleid'. Dit jaar niet waarbij moet worden opgemerkt dat bij enkele raamovereenkomsten een kwalificatie 'strijdig met open standaarden beleid' dicht bij was. Uiteindelijk zijn deze aanbestedingen niet in de beoordeling meegenomen. Daarover is het nodige opgemerkt in paragraaf 6.1.

Tabel 16: 'Pas toe' en 'leg uit' bij feitelijke aanbestedingen 2015/2016
(Bron: onderzoek feitelijke aanbestedingen juli 2015 t/m juni 2016, uitgevoerd zomer 2016)

	Ministeries + Uitvoerings-organisaties		Gemeenten + Provincies + Waterschappen		**Totaal 2015 / 2016**		Totaal 2014 / 2015	
	totaal	in %	totaal	in %	**totaal**	in %	totaal	in %
aanbestedingen waarbij OS relevant	*21*	*100 %*	*23*	*100 %*	***44***	*100 %*	*48*	*100 %*
alle relevante OSn gevraagd	**4**	**(19 %)**	**4**	**(17 %)**	**8**	**(18 %)**	**10**	**(21 %)**
deel van relevante OSn gevraagd	**11**	**52 %**	**13**	**57 %**	**24**	**55 %**	**24**	**50 %**
* cruciale OSn gevraagd	0	(0 %)	4	(17 %)	**4**	(9 %)	11	23 %
* OSn gevraagd, maar cruciale niet	11	(52 %)	9	(39 %)	**20**	(45 %)	13	27 %
geen relevante OSn gevraagd	**6**	**29 %**	**6**	**26 %**	**12**	**27 %**	**14**	**29 %**
* alleen architectuur-kaders	0	(0 %)	1	(4 %)	**1**	(2 %)	0	0 %
* algemene aandacht aan OSn-beleid	0	(0 %)	1	(4 %)	**1**	(2 %)	3	6 %
* geen aandacht voor OSn-beleid	6	(29 %)	4	(17 %)	**10**	(23 %)	9	19 %
* strijdig met OSn-beleid	0	(0 %)	0	(0 %)	**0**	(0 %)	2	4 %
totaal aantal relevante OSn	103	100 %	154	100 %	**257**	100 %	210	100 %
* aantal cruciale relevante OSn	79	77 %	123	81 %	**202**	79 %		
totaal aantal gevraagde relevante OSn	45	44 %	68	44 %	**113**	44 %	90	43 %
* niet alle OSn gevraagd => Leg Uit vereist	17	(81 %)	19	(83 %)	**36**	(82 %)	38	(79 %)
cruciale OSn wel gevraagd	0		4		**4**		11	
Leg Uit in jaarverslag beslist vereist	17		15		**32**		27	100 %
- idem, maar beperkt tot Q3+Q4 2015 [66]	*8*	*(100 %)*	*7*	*(100 %)*	***15***	*(100 %)*	*11*	*(100 %)*
- concrete verantwoording in jaarverslag	*0*	*(0 %)*	*0*	*(0 %)*	***0***	*(0 %)*	*0*	*(0 %)*
- beperkte verantwoording in jaarverslag	*3*	*(38 %)*	*0*	*(0 %)*	***3***	*(20 %)*	*4*	*(36 %)*
- geen Leg Uit in jaarverslag	*5*	*(62 %)*	*7*	*(100 %)*	***12***	*(80 %)*	*7*	*(64 %)*
Totaal	21	100 %	23	100 %	**44**	100 %	48	100 %

NB: het groen gemarkeerde blok betreft aantallen standaarden, de rest van de tabel betreft aantallen aanbestedingen

De verschillen in scores in tabel 16 tussen Rijk en decentrale overheden zijn klein. Het aandeel aanbestedingen waarbij om alle relevante standaarden werd gevraagd ligt bij het Rijk op 19% en bij decentrale overheden op 17%. Ook bij de twee andere hoofdcategorieën zijn de verschillen klein: 52% tegen 57% bij de categorie 'deel van de relevante open standaarden gevraagd' en 29% tegen 26% bij de categorie waarin de varianten zijn ondergebracht op 'geen enkele relevante standaard gevraagd'.

Uit het horizontaal met groen gemarkeerde blok in de tabel valt op dat ongeveer 4 op de 5 relevante standaarden door de beoordelaars als cruciaal worden aangemerkt. Daarmee wordt bedoeld dat de

[66] Een controle op toepassing van het leg-uit principe heeft alleen kunnen plaatsvinden over de aanbestedingen uit 2015, waarover verantwoording had moeten worden afgelegd in het Jaarverslag 2015.

kern van de applicatie raakvlakken heeft met de betreffende standaard. Tot slot is opvallend dat het aandeel bevraagde standaarden zowel voor het Rijk als voor de overige overheden op 44% ligt. Dat percentage is min of meer gelijk aan dat van vorige jaar (43%).

Vorig jaar is bij de uitvoering van de monitor vastgesteld dat de mate waarin de onderzochte aanbestedingen voldeden aan het open standaardenbeleid beduidend was verbeterd. Ter herinnering: het aandeel van de hoogst gewaarde categorie (alle relevante standaarden gevraagd) was opgelopen (21% tegen 14% in het jaar daarvoor) en het aandeel van de vier laagst gewaardeerde categorieën (in de tabel samengebracht in de hoofdcategorie 'geen relevante open standaarden gevraagd') was toen teruggelopen van 59% naar 29%. Die terugloop deed zich toen bij elke daaronder vallende subcategorie voor, met als uitzondering de laatste (strijdigheid met open standaardenbeleid). Naar aanleiding van die bevindingen is –toen al- de vraag gesteld welk vervolg deze verbetering zou krijgen, met als mogelijke opties een terugval naar eerdere waarden, een consolidering van de verbetering of mogelijk zelfs een doortrekken van de positieve lijn. Op basis van tabel 16 kan worden geconcludeerd dat sprake is van een genuanceerd beeld waar het gaat om de consolidering van de eerder geboekte winst:

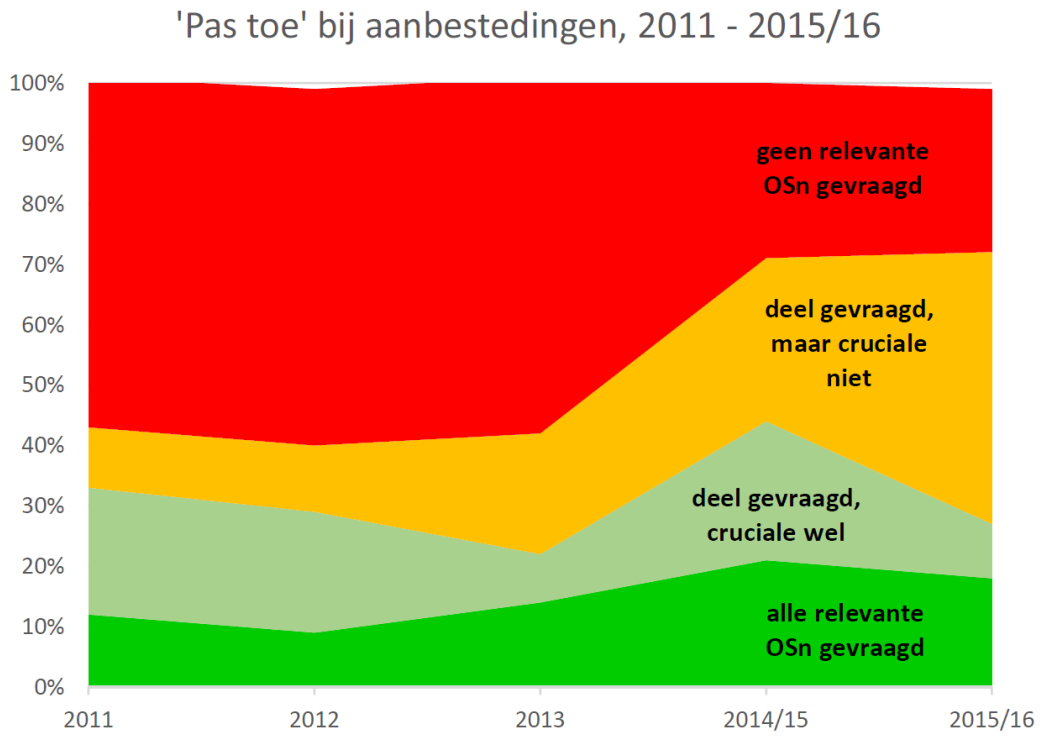
- in de hoogst gewaardeerde categorie is sprake van een lichte teruggang, van 21% naar 18%;
- in het cluster van de vier laagst gewaardeerde categorieën is sprake van een lichte verbetering, van 29% naar 27%.
- in de middencategorie is –per saldo- sprake een oplopend percentage: een stijging van 50% naar 55%.

Al met al lijkt sprake van een consolidering van het beeld van vorig jaar maar binnen de hierboven genoemde middencategorie is sprake van een verschuiving die het beeld wat minder gunstig maakt:

- wel gevraagd om alle cruciale open standaarden maar om één of meer andere niet: van 23% vorig jaar naar 9% nu;
- gevraagd om open standaarden, maar om minimaal één cruciale niet: van 27% vorig jaar naar 45% nu.

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

Figuur 17: 'Pas toe' bij feitelijke aanbestedingen 2011 - 2015/2016



De verbetering die vorig jaar zichtbaar werd, blijkt voor een deel bestendig te zijn. Het groene vlak blijft ongeveer even groot als vorig jaar. 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) tot dit jaar 18%.

Hetzelfde geldt voor het rode vlak; ook dat is ongeveer even groot als vorig jaar. Het aantal aanbestedingen waarbij niet om relevante open standaarden is gevraagd terwijl dat wel had gemoeten daalde van 29% vorig jaar naar 27% dit jaar. Met name in die categorie werd vorig jaar een forse verbetering bereikt. In de periode daarvóór (2011-2013) heeft dit percentage altijd stabiel net onder de 60% gelegen.

In het midden-gedeelte van de figuur is de verschuiving waar te nemen zoals hierbij al is verwoord: het gele gedeelte is duidelijke groter geworden en dat is ten koste gegaan van het lichtgroene deel. Als het lichtgroene en het groene deel worden samengenomen –alle cruciale open standaarden zijn gevraagd- ligt de score in deze monitor weer op het niveau van de monitor van twee jaar terug.

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.

Veiligheidsregio Utrecht: de opdracht betreft de realisatie van een werkprocesapplicatie met een zaakgerichte, een objectgerichte en een DMS-functionaliteit (document management systeem). Van de aangeboden oplossing wordt verwacht dat zowel opslag als ontsluiting van documenten uit alle gangbare formats wordt ondersteund. De relevant geachte standaarden (PDF, ODF, StUF, CMIS, Webrichtlijnen, ISO 27001/02, SAML en Digikoppeling en –minder cruciaal- PNG en JPEG) worden alle uitgevraagd.

Belastingdienst: de opdrachtgever beoogt met deze raamovereenkomst te voorzien in de toekomstige behoefte aan mid-volume scan-oplossingen en aanverwante dienstverlening. Onder dat laatste wordt verstaan: implementatie, derde-lijns support, opleiding, onderhoud en beheer. Als relevante en tevens cruciale standaarden zijn aangemerkt: ISO 27001/02 en PDF/A. Het bestek bevat een uitgebreide verwijzing naar de BIR en er is expliciet opgenomen dat gescand moet kunnen worden in onder andere PDF-formaat.

Gemeente Breda: de gemeente is op zoek naar een Nederlandstalige standaardapplicatie passend in de gemeentelijke architectuur, ten behoeve van de verplichte bijhouding van de Basisregistratie Adressen en Gebouwen (BAG). Alle standaarden die relevant en cruciaal worden geacht (StUF, PDF, ODF, IPv4/6, GEO-standaarden en TLS) worden in de bevraging door de opdrachtgever meegenomen. SAML –door de beoordelaars ook relevant geacht, zij het niet cruciaal- wordt echter niet uitgevraagd.

Ministerie van V&J: in deze aanbesteding gaat het om levering van standaardprogrammatuur en daaraan gerelateerde dienstverlening ten behoeve van de Belastingdienst en de Kamer van Koophandel. De volgende standaarden worden aangemerkt als relevant en tevens cruciaal: PDF, ODF, ISO27001/02, JPEG, PNG, SMeF, TLS en SETU. Naast het feit dat de benodigde standaarden gericht worden uitgevraagd, noemt de opdrachtgever in de stukken ook expliciet het open standaarden beleid.

6.3 'Pas toe' per open standaard

Voor de mate waarin om een open standaard wordt gevraagd (wanneer die voor de aanbesteding relevant is) biedt tabel 16 al een eerste indicatie. Van de relevant geachte standaarden (257 standaarden op een totaal van 44 aanbestedingen) is om 44% in het traject van de aanbesteding daadwerkelijk gevraagd. Om deze cijfers in het juiste perspectief te plaatsen het volgende:

- het aantal relevant geachte standaarden per aanbesteding ligt gemiddeld duidelijk hoger dan vorig jaar (5,8 versus 4,3 standaarden per aanbesteding[67]);
- het percentage uitgevraagd 44% ligt fractioneel hoger dan vorig jaar (2015: 43%[68]);
- combinatie van bovenstaande twee punten duidt erop dat er dit jaar per aanbesteding meer standaarden zijn uitgevraagd dan vorig jaar (2,6 versus 1,9).

De consolidatie van het percentage uitgevraagd laat zich ook vertalen naar de scores voor 'Pas toe' per afzonderlijke standaard.

Het aantal standaarden waarop procentueel gezien 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 18.

[67] De omvang van de ptolu-lijst is min of meer vergelijkbaar met die van vorig jaar.
[68] Deze 43% van vorig jaar was een flinke verbetering ten opzichte van het jaar daarvoor (toen 25%).

Tabel 18: 'Pas toe' bij feitelijke aanbestedingen in 2015 / 2016, per standaard

(Bron: onderzoek feitelijke aanbestedingen juli 2015 t/m juni 2016, uitgevoerd zomer 2016)

0 x ≥ 75 % 16 x 25-75 % 9 x < 25 %	Ministeries + Uitvoerings-Organisaties		Gemeenten + Provincies + Waterschappen		**Totaal 2015/2016**		*Totaal 2014/2015*
aantal aanbestedingen: n =	*21*		*23*		*44*		*48*
	relevant	comply: gevraagd in % van relevant	relevant	comply: gevraagd in % van relevant	relevant	comply: gevraagd in % van relevant	comply: gevraagd in % van relevant
Sinds 2008 op de lijst:							
NEN-ISO\IEC 27001:2005nl	15	73 %	15	47 %	30	60 %	70 %
NEN-ISO\IEC 27002:2007nl	15	60 %	14	36 %	29	48 %	72 %
PNG	2	50 %	3	33 %	5	40 %	0 %
JPEG	2	50 %	6	67 %	8	63 %	0 %
PDF **)	11	73 %	15	60 %	26	65 %	62 %
StUF	3	33 %	8	88 %	11	73 %	67 %
Sinds 2009 op de lijst:							
SETU	1	100 %	2	0 %	3	33 %	0 %
SAML	4	50 %	13	23 %	17	29 %	39 %
Sinds 2010 op de lijst:							
XBRL v2.1	1	0 %	1	0 %	2	0 %	100 %
E−portfolio			5	0 %	5	0 %	0 %
Aquo Standaard							
IPv6 en IPv4	6	17 %	7	0 %	13	8 %	32%
OAI−PMH			2	0 %	2	0 %	100%
Sinds 2011 op de lijst:							
NL LOM							
Webrichtlijnen *)	7	29 %	9	78 %	16	56 %	63 %
OWMS	2	0 %	1	0 %	3	0 %	
IFC	1	0 %			1	0 %	
STOSAG			1	0%	1	0 %	
Sinds 2012 op de lijst:							
DNSSEC	1	0 %	1	0 %	2	0 %	0 %
DKIM	1	0 %	1	100 %	2	50 %	
ODF 1.2	15	24 %	15	33 %	30	30 %	19 %
Sinds 2013 op de lijst:							
Digikoppeling	2	50 %	4	25 %	6	33 %	50 %
BWB							0 %
ECLI							0 %
EMN_NL							
JCDR	1	0 %			1	0 %	
Sem. Model e-Factureren	1	0 %	1	100 %	2	50 %	
Sinds 2014 op de lijst:							
WDO Datamodel							
TLS	11	36 %	17	65 %	28	54 %	23 %
Geo−standaarden			3	33 %	3	33 %	100 %
SIKB 0101							
Visi							
Cmis	1	0 %	10	50 %	11	45 %	
Sinds 2015 op de lijst: ***)							
SKOS							
SPF							
Totaal	**103**	**44 %**	**154**	**44 %**	**257**	**44 %**	**43 %**

**) Webrichtlijnen zijn dit jaar, net als vorig jaar, alleen relevant beoordeeld voor externe webapplicaties.*
***) Bij de beoordelingen is geen onderscheid gemaakt tussen de verschillende PDF-varianten.*
****) SIKB0102 en WPA2 Enterprise zijn pas in februari 2016 op de lijst geplaatst, en daarom buiten de beoordelingen gelaten.*

Aan de hand van tabel 18 kan worden afgelezen welke standaarden vaker dan gemiddeld worden bevraagd bij de onderzochte aanbestedingen. Dit zijn de volgende standaarden: de ISO 27001/02, JPEG, PDF, StUF, Webrichtlijnen, TLS en CMIS, en met wat een minder gewicht DKIM en E-factureren. Deze beide laatste standaarden scoren in de tabel weliswaar een uitvraag-percentage van 50% maar voor beide standaarden geldt dat deze slechts twee maal als relevant zijn aangemerkt.

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 als relevant zijn aangemerkt, vallen enkele verschillen ten opzichte van vorig jaar op:

- met name de uitvraag bij TLS is sterk verbeterd (vooral toe te schrijven aan een forse stijging bij de andere overheden dan het Rijk) en in wat mindere mate geldt dit ook voor ODF;
- een drietal standaarden laat een tegenovergesteld beeld zien met een relatief flinke daling: hiervan is met name sprake bij IPv4/6 en ISO 27002 en in wat minder mate ook bij SAML. Wat opvalt is dat het aandeel uitgevraagd bij de ISO 27002 geen gelijke tred meer houdt met de uitvraag van de ISO 27001. Een deel van de verklaring zit hem in een uitvraag die als volgt is geformuleerd: "…..informatiebeveiliging op basis van ISO 27001 of gelijkwaardig". In dergelijke gevallen is alleen ISO 27001 is uitgevraagd aangemerkt.

6.4 'Leg uit' bij feitelijke aanbestedingen

Bij 8 aanbestedingen die in het kader van deze monitor 2016 zijn beoordeeld , is om alle relevante standaarden gevraagd. Bij de andere 36 aanbestedingen had dus in het jaarverslag verantwoording afgelegd moeten worden ('Leg uit') voor het niet toepassen van de betreffende relevante standaard(en). Bij 4 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 32 aanbestedingen (door 28 verschillende overheidsorganisaties) is 'Leg uit' zonder twijfel vereist, omdat hierbij niet gevraagd werd om één of meer van de relevante open standaarden (20 aanbestedingen) of om geen enkele relevante standaard gevraagd is (12 aanbestedingen).

Van deze 32 aanbestedingen is het voor 15 aanbestedingen (door 14 overheidsorganisaties, waarvan 6 ministeries) op dit moment mogelijk om in het Jaarverslag 2015 te controleren of 'leg-uit' is toegepast; deze 15 aanbestedingen dateren uit Q3 – Q4 12015. Voor de resterende 17 aanbestedingen kan dat pas na het verschijnen van de jaarverslagen over 2016. Van 'Leg uit' was in de jaarverslagen van de 14 overheidsorganisaties echter geen sprake, in die zin dat in geen van de jaarverslagen een concrete aanbesteding wordt genoemd uit het voorliggende onderzoek waarbij van de lijst voor 'pas toe of leg uit' werd afgeweken.

Bij de decentrale overheden is in de jaarverslagen geen enkele verwijzing naar het onderliggende beleid teruggevonden. Bij de departementen ligt dat iets 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: de Belastingdienst), Defensie, Infrastructuur en Milieu, VWS, OCW en Economische Zaken. Van deze zes departementen zijn namelijk aanbestedingen beoordeeld uit Q3+Q4 2015, met een beoordeling die noodzaakt tot 'leg uit'. In onderstaand schema zijn deze zes ministeries aangegeven met oranje.

Het overall-beeld is als volgt:

- vier ministeries (vorig jaar zes) hebben een verantwoording opgenomen in het jaarverslag 2015;
- 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';
- zeven ministeries (en W&R) vermelden niets over open standaarden.

In een enkel geval is 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	[Geen] Het Ministerie van Algemene Zaken heeft geen grote ICT-projecten uitgevoerd in 2015. *(Bron: B Beleidsverslag onder 3: bedrijfsvoeringsparagraaf)*
BZK	*Afwijkingen instructie rijksdienst bij aanschaf ICT diensten of ICT producten* Het Ministerie van BZK heeft in 2015 gehandeld conform artikel 3, eerste lid van de «Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten». Er zijn in de regel geen ICT-diensten of -producten aangeschaft waarbij is afgeweken van de open standaarden op de «pas toe of leg uit»-lijst van College Standaardisatie. Van afwijkingen is sprake bij de aanschaf van licenties en tooling voor de dienstverleningssystemen SAP en Oracle van bijvoorbeeld P-Direkt en Rijksvastgoedbedrijf (RVB). Doordat de dienstverlening draait op gesloten systemen, kan de tooling niet op basis van open standaarden worden geselecteerd. 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 binnen de Logius-producten met eventuele afwijkingen en toelichting. *(Bron: 4 Bedrijfsvoeringsparagraaf, onder 3)*
BUZA	[Geen]
DEF	[Geen]
EZ	[Geen]
FIN	*ICT-voorwaarden voor open standaarden* Voldaan is aan de verplichting van artikel 3, eerste lid van de Instructie rijksdienst bij aanschaf van ICT-diensten of ICT-producten. *(Bron: 6 Bedrijsvoeringsparagraaf, onder 5)*
IM	*Instructie Rijksdienst* 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. In het verslagjaar is geen sprake geweest van een afwijking van de Instructie Rijksdienst. *(Bron: 6 Bedrijfsvoeringsparagraaf, onder 2D)*
OCW	[Geen. NB: vorig jaar nog wel]
SZW	*Open standaarden* ICT-producten en -diensten van boven de € 50.000 dienen in het inkoop- en aanbestedingsproces te voldoen aan de open standaardennorm. In 2015 heeft SZW voldaan aan de open standaardennorm. *(Bron: 6 Bedrijfsvoeringsparagraaf, onder 3)*
V&J	[Geen]
VWS	[Geen. NB: vorig jaar nog wel]
WR	[Geen]

Leg uit in Q1 + Q2 2015

In de vorig jaar verschenen Monitor 2015 zijn onder andere aanbestedingen beoordeeld uit Q1+Q2 2015. Voor deze 16 aanbestedingen kon op dat moment 'leg-uit' nog niet onderzocht worden. Dat onderzoek heeft nu plaatsgevonden, omdat de Jaarverslagen 2015 nu wèl beschikbaar zijn.

Deze 16 aanbestedingen (door 15 overheidsorganisaties, waarvan 4 ministeries) zijn gelijk verdeeld over 'Rijk' en 'mede-overheden'. Van 'Leg uit' was in de jaarverslagen van deze 15 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 dus nog niet toe hebben geleid, dat de verplichting wijd verspreid wordt toegepast om in jaarverslagen over specifieke aanbestedingen (en daarvoor relevante open standaarden) te verantwoorden waarom daar niet om is gevraagd. In vergelijking met de verslaglegging over 2014 valt op dat bij twee departementen de verwijzing naar het beleid rond de toepassing van open standaarden is komen te vervallen (dit betreft de miniseries van OCW en VWS).

De bevindingen rond het toepassen van het 'Leg uit' principe in 2015 zijn min of meer gelijk aan de voorgaande jaren (2011 tot en met 2014), met de nuancering zoals hierboven beschreven. En overigens ook aan 2010. Door de RUG is destijds nagegaan in hoeverre door overheden verantwoording is afgelegd voor het niet toepassen van open standaarden bij de onderzochte aanbestedingen uit de eerste helft van 2010. In dat onderzoek werd in geen enkel jaarverslag een verantwoording voor het niet toepassen van relevante standaarden gevonden.

6.5 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 19 is weergegeven hoe vaak elk van de standaarden van de lijst relevant is gebleken bij een aanbesteding. Van de 37 standaarden op de lijst voor 'pas toe of leg uit' waren er 25 standaarden minimaal bij een aanbesteding relevant (in 2015: 21 van de 35), de andere 12 waren dus voor geen van de 44 onderzochte aanbestedingen in 2015 relevant.

Een vijftal standaarden steekt er met kop en schouders bovenuit als het gaat om de mate waarin zij relevant worden geacht, getuige tabel 19: de ISO 27001/02, PDF, ODF en TLS, met scores van ongeveer 60% of hoger. Deze standaarden zijn bij 26 tot 30 (van de 44) aanbestedingen als relevant aangemerkt. Daarna volgt een groep van eveneens vijf standaarden die bij meer dan 10 aanbestedingen als relevant zijn aangemerkt: StUF, SAML, IPv4/6, Webrichtlijnen en CMIS. Opvallend in die laatste opsomming is de positie van IPv4/6. Deze was vorig jaar nog bij 77% van de aanbestedingen relevant, en dit jaar bij 30%. Een soortgelijke constatering is al eerder gedaan, bij tabel 18.

Aan de andere kant: van de 25 standaarden die in het kader van de beoordeling van aanbestedingen relevant werden geacht, zijn er dit jaar 8 slechts incidenteel als relevant aangemerkt (vorig jaar waren dat er nog 11):

- XBRL v2.1, OAI-PMH, DNSSEC, DKIM en E-factureren twee keer, en
- IFC, STOSAG en JCDR één keer.

Eerder in dit hoofdstuk - bij tabel 16 - is al opgemerkt dat het aantal relevant geachte standaarden per aanbesteding duidelijk hoger ligt dan vorig jaar. Mede naar aanleiding van tabel 19 kan daar nog aan worden toegevoegd dat de afzonderlijke standaarden van de lijst gemiddeld genomen hoger scoren als het gaat om de vraag of deze standaarden relevant zijn voor de betreffende aanbesteding.

In vergelijking met de vorige monitor is een drietal standaarden bij geen enkele aanbesteding relevant gebleken. Dit betreft twee juridische standaarden (BWB en ECLI) en NTA 9040 maar daar moet bij worden aangetekend dat de relevantie van deze standaarden vorig jaar al marginaal 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 (OWMS, IFC, STOSAG, DKIM, JCDR en E-factureren) met één uitzondering: CMIS. Deze standaard werd vorig jaar nog niet in de beoordeling meegenomen omdat deze standaard pas halverwege de periode waarover werd beoordeeld op de lijst is geplaatst (december 2014).

In vergelijking met de vorige monitor valt op dat sprake is van een verschuiving in de mate waarin standaarden als relevant zijn aangemerkt voor de onderzochte aanbestedingen. Als we als criterium een verschuiving van minimaal 10% aanhouden valt het volgende op:

- vaker benoemd als relevant: ISO27001 (+ 26%), ISO 27002 (+28%), JPEG (+ 16%), Webrichtlijnen (+19%), ODF (+24%) en CMIS (+25%);
- minder vaak benoemd als relevant: IPv4/6 (-47%). Vorig jaar stond IPv4/6 juist als bijna grootste stijger genoemd met een plus van 26%.

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: 44% dit jaar tegen 43% vorig jaar. In tabel 19 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: PDF (39%), NEN-ISO\IEC 27001/27002 (41% respectievelijk 32%) en TLS (34%). IPv4/6 stond vorig jaar nog in dit rijtje met een score van 23% maar dit jaar is het percentage veel lager (2%).

Na dit rijtje koplopers volgen nog enkele standaarden met een score van boven de 10%: Webrichtlijnen en ODF met beide 20%, StUF met 18% en een drietal standaarden met een score van 11% : JPEG, SAML en CMIS. Om de andere standaarden is slechts bij enkele aanbestedingen gevraagd of - ten onrechte - zelfs in het geheel niet. Dit laatste is het geval bij XBRL v2.1, E-portfolio, OAI-PMH, OWMS, IFC, STOSAG, DNSSEC en JCDR. Deze 0-scores doen zich overigens alleen voor bij standaarden die slechts incidenteel (meestal 1 of 2 keer, in een enkel geval 3 en 4 keer) als relevant zijn aangemerkt.

Tabel 19: Open standaarden relevant / gevraagd bij feitelijke aanbestedingen in 2015/2016
(Bron: onderzoek feitelijke aanbestedingen juli 2015 t/m juni 2016, uitgevoerd zomer 2016)

	Ministeries + Uitvoerings-organisaties		Gemeenten + Provincies + Waterschappen		**Totaal 2015/2016**	
aantal aanbestedingen: n =	*21*		*23*		***44***	
	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**
Sinds 2008 op de lijst:						
NEN-ISO\IEC 27001:2005nl	71 %	52 %	65 %	30 %	**68 %**	**41 %**
NEN-ISO\IEC 27002:2007nl	71 %	43 %	61 %	22 %	**66 %**	**32 %**
PNG	10 %	5 %	13 %	4 %	**11 %**	**5 %**
JPEG	10 %	5 %	26 %	17 %	**18 %**	**11 %**
PDF **)	52 %	38 %	65 %	39 %	**59 %**	**39 %**
StUF	14 %	5 %	35 %	30 %	**25 %**	**18 %**
Sinds 2009 op de lijst:						
SETU	5 %	5 %	9 %	0 %	**7 %**	**2 %**
SAML	19 %	10 %	57 %	13 %	**39 %**	**11 %**
Sinds 2010 op de lijst:						
XBRL v2.1	5 %	0 %	4 %	0 %	**5 %**	**0 %**
E−portfolio			22 %	0 %	**11 %**	**0 %**
Aquo Standaard						
IPv6 en IPv4	29 %	5 %	30 %	0 %	**30 %**	**2 %**
OAI−PMH			9 %	0 %	**5 %**	**0 %**
Sinds 2011 op de lijst:						
NL LOM						
Webrichtlijnen *)	33 %	10 %	39 %	30 %	**36 %**	**20 %**
OWMS	10 %	0 %	4 %	0 %	**7 %**	**0 %**
IFC	5 %	0 %			**2 %**	**0 %**
STOSAG			4 %	0 %	**2 %**	**0 %**
Sinds 2012 op de lijst:						
DNSSEC	5 %	0 %	4 %	0 %	**5 %**	**0 %**
DKIM	5 %	0 %	4 %	4 %	**5 %**	**2 %**
ODF 1.2	71 %	19 %	65 %	22 %	**68 %**	**20 %**
Sinds 2013 op de lijst:						
ebMS/WUS/Digikoppeling	10 %	5 %	17 %	4 %	**14 %**	**5 %**
BWB						
ECLI						
EMN_NL						
JCDR	5 %	0 %			**2 %**	**0 %**
Sem. Model e-factureren	5 %	0 %	4 %	4 %	**5 %**	**2 %**
EML_NL						
Sinds 2014 op de lijst:						
TLS	52 %	19 %	74 %	48 %	**64 %**	**34 %**
WDO Datamodel						
Geo−standaarden			13 %	4 %	**7 %**	**2 %**
SIKB 0101						
Visi						
Cmis	5 %	0 %	43 %	22 %	**25 %**	**11 %**
Sinds 2015 op de lijst:						
SKOS						
SPF						
Totaal	**103**	**44**	**154**	**44**	**257**	**44**

**) Webrichtlijnen zijn dit jaar, net als vorig jaar, alleen relevant beoordeeld voor externe webapplicaties.*
***) Bij de beoordelingen is geen onderscheid gemaakt tussen de verschillende PDF-varianten.*

6.6 Tweede beoordeling

In de onderzoeksopzet is net als vorig jaar plaats ingeruimd voor een tweede beoordeling voor een deel van de door dhr. Paapst beoordeelde aanbestedingen. Deze is verricht door dhr. Krukkert en dhr. Van den Berg (beiden TNO). Het doel van deze tweede beoordeling was drieledig:

- een toets op de beoordeling van de 'eerste beoordelaar';
- eventuele aanscherping van een aanvankelijk oordeel op basis van onderlinge discussie tussen beide beoordelaars:
    - aanvullende standaarden benoemen of juist standaarden die aanvankelijk relevant werden beoordeeld laten vallen;
    - eventueel een andere blik op het uitvragen;
    - een aanpassing van het eindoordeel;
- het krijgen van zicht 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 25 aanbestedingen Rijk bestudeerd, 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 is een bijeenkomst gearrangeerd –met daarbij ook Bureau Forum Standaardisatie aanwezig- om de gezamenlijke uitgangspunten die aan de basis liggen van het beoordelingswerk met elkaar te bespreken een waar nodig aan te scherpen.

Na de beoordeling in eerste aanleg zijn beide zienswijzen vervolgens onderling uitgewisseld en hebben gediend als input om met elkaar het gesprek te voeren over deze beide beoordelingen. Die gesprekken hebben plaatsgevonden in augustus en september. De focus in die gesprekken lag logischerwijze op de punten waar de afzonderlijke beoordelingen een verschil lieten zien.

Als eerste valt op dat de beide beoordelaars aanvankelijk voor 16 van de 25 aanbestedingen een ander oordeel hadden, in de categorisering zoals opgenomen in tabel 16. Ter vergelijking: vorig jaar bestond bij aanvang verschil van mening over 21 van de 25 aanbestedingen. Daaraan liggen vier delen van een oorzaak ten grondslag:

- een andere kijk op de vraag of de aanbesteding als zodanig voor beoordeling geschikt is;
- een andere kijk op de relevantie van een standaard voor een specifieke aanbesteding;
- een uiteenlopende interpretatie van de wijze waarop door de aanbestedende partij is uitgevraagd;
- nuance-verschillen bij het toekennen van een waarde-oordeel.

Een dergelijk vertrekpunt lijkt een indicatie om vraagtekens te plaatsen bij de eenduidigheid waarmee de lijst voor 'pas toe of leg uit' toegepast kan worden op aanbestedingen, als experts (in eerste instantie) al tot een uiteenlopende inschatting komen. Voor bij aanbestedingen betrokken functionarissen die slechts incidenteel van doen hebben met de lijst voor 'pas toe of leg uit', zou het moeilijk kunnen zijn om deze lijst goed in praktijk te brengen.

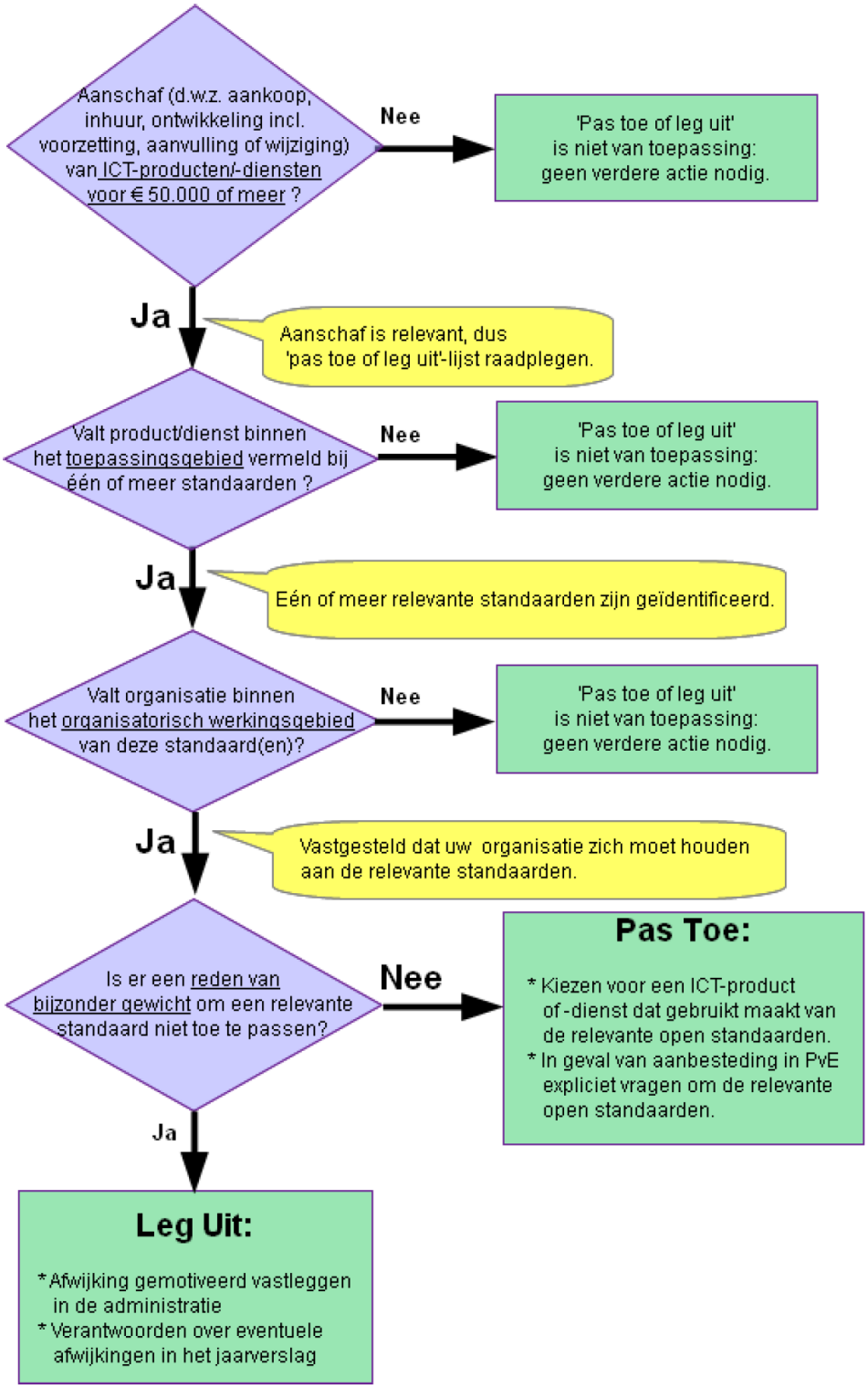
Op basis van de discussie die is gevoerd met de beide beoordelaars is overigens op vrijwel alle aanbestedingen consensus bereikt als het gaat om de uiteindelijke beoordeling, met nog vier lichte twijfelgevallen. Daar waar uiteindelijk (kleine) verschillen van inzicht bleven bestaan, is in dit hoofdstuk uitgegaan van het oordeel van de hoofdbeoordelaar. De meerwaarde van een second-opinion sessie zou eraan kunnen worden afgelezen dat de hoofdbeoordelaar voor 9 aanbestedingen zijn aanvankelijke oordeel heeft bijgesteld op basis van de onderlinge discussies die zijn gevoerd. Deels zijn deze aanpassingen terug te voeren tot de heroverweging om enkele raamovereenkomsten met de kwalificatie 'in deze vorm niet beoordeelbaar' terzijde te schuiven en daar dus ook geen kwalificatie aan te geven. Verder werden, redenerend vanuit de optiek van de hoofdbeoordelaar, sommige aanbestedingen 'hoger' beoordeeld (4) en een enkele lager (1). Bovendien waren de verschuivingen op de schaal van beoordelings-waarden op één enkele uitzondering na (van: alleen in algemene zin aandacht voor open standaarden naar: alle relevante open standaarden bevraagd) marginaal.

Gezien het bovenstaande heeft de tweede beoordeling zijn waarde bewezen. Uitwisseling van inzichten en ervaringen heeft ertoe geleid dat er consensus ontstaat. Tijdens dat proces heeft de second opinion tot een aantal inhoudelijke discussies tussen de experts geleid die ook relevant kunnen zijn om beter zicht te krijgen op mogelijke onduidelijkheden in de aanbestedingspraktijk bij – in dit geval – een overheidsinstelling[69].

[69] 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.

Bijlagen

A. 'Pas toe of leg uit' in het kort



B. Functioneel toepassingsgebied en organisatorisch werkingsgebied [70]

Standaard[71] *(op lijst sinds)*	**Functioneel toepassingsgebied**	**Organisatorisch werkingsgebied**
Internet & beveiliging		
DKIM *(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 *(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.
IPv6 en IPv4 *(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 *(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 *(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 *(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 *(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.
TLS *(4 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 *(2 februari 2016)*	Veilige, met behulp van een account geauthenticeerde toegang tot een wifi-netwerk van een (semi-)overheidsorganisatie. Toegang tot publieke wifi-netwerken van overheden voor gasten zonder account is uitgesloten van de verplichting	Nederlandse overheden (Rijk, provincies, gemeenten en waterschappen) en instellingen uit de (semi-) publieke sector.
Document en (web)Content		
CMIS *(9 december 2014)*	Het toegankelijk maken van ongestructureerde gegevens in content repositories van Content Management Systemen (CMS'en) en Document Management Systemen (DMS'en) 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.
ODF 1.2 *(15 juni 2012)*	Voor de uitwisseling van reviseerbare documenten.	Overheden en instellingen uit de publieke sector.

[70] Dit overzicht is gebaseerd op de stand van zaken in de zomer van 2016. Daarom is de standaard STARTTLS & DANE nog niet in dit overzicht meegenomen.
[71] Bij het overzicht is de indeling naar domeinen aangehouden zoals opgesteld door Bureau Forum Standaardisatie. Twee standaarden (de Aquo-standaard en SIKB0101) zijn bij twee domeinen ingedeeld (bij Stelselstandaarden en bij Water & bodem) en in die zin is in dit overzicht derhalve sprake van een beperkte overlap.

OWMS *(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 *(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 *(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 *(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 *(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.
Webrichtlijnen 2.0 *(v 2.0: 23 juni 2011)*	Webgebaseerde informatie-, interactie-, transactie- en participatiediensten.	Overheden en instellingen uit de publieke sector.
Stelselstandaarden		
Aquo-standaard *(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.
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 aanbevelenswaardig 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.
SIKB0101 *(9 december 2014)*	Uitwisselen van onderzoeksgegevens over de milieuhygiënische kwaliteit van de bodem en de specifieke gegevens die direct voortkomen uit (of vooruitlopen op) de besluiten die het bevoegd gezag naar aanleiding daarvan heeft genomen.	Overheden (Rijk, provincies, gemeenten en waterschappen), semi-overheden en instellingen uit de publieke sector.
StUF *(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 *(17 juni 2013)*[72]	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 *(20 mei 2009)*	De elektronische berichtenuitwisseling rondom de bemiddeling/inhuur van flexibele arbeidskrachten	Overheden en instellingen uit de (semi-)publieke sector

[72] Inmiddels staat op de lijst een nieuwe datum van een geactualiseerd besluit: 15 november 2016.

WDO Datamodel *(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 *(17 april 2010)*	* XBRL: Elektronisch verkeer dat te kenmerken is als verantwoordingsverkeer 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 *(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 *(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 *(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 *(15 november 2011)*	Uitwisseling in het kader van bouwwerkinformatiemodellen	Overheden, semi-overheden en instellingen binnen de publieke sector.
Visi *(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 *(17 mei 2016 2010)*	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 *(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 *(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 *(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 *(28 november 2013)*	Identificatie van rechterlijke uitspraken, onder meer ter citatie.	Overheden (Rijk, provincies, gemeenten, waterschappen) en instellingen uit de (semi-) publieke sector.
JCDR *(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 *(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 *(15 november 2011)*	De standaard moet ingezet worden voor: digitaal container- en pasmanagement voor afval en grondstoffen	Gemeenten en gemeentelijke afvalinzamelaars.

C. Halfjaarlijkse meting Informatieveiligheidsstandaarden BFS – medio 2016

Achtergrond

Sinds 2015 biedt het Platform Internet Standaarden[73] de mogelijkheid om via de website internet.nl 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[74]. 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[75]. Voorliggende notitie bevat de resultaten van de meest recente meting van augustus 2016.

Om welke standaarden gaat het

Het Nationaal Beraad heeft bovengenoemde afspraken gemaakt met betrekking tot de volgende standaarden[76]:

- DNSSEC: Domeinnaambeveiliging
- TLS[77] : Beveiligde verbinding
- DKIM: Anti-Phishing
- SPF: Anti-Phishing
- DMARC[78]: Anti-Phishing (rapportages)

De kosten en inspanning die een organisatie moet investeren om aan deze standaarden te voldoen zijn overzichtelijk[79].

Om welke domeinen gaat het

Het gaat om de volgende groepen met domeinen: (152 niet-gemeenten)

- 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)
    - Provincies en Waterschappen
    - Partijen die behorend tot Klein LEF

---

[73] 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/

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

[75] 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.

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

[77] Voor TLS geldt dat het Nationaal Beraad de ambitie uitsprak deze 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.

[78] 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'.

[79] In het geval van DNSSEC en TLS gaat het om enkele honderden euro's per jaar. De volledige inzet van SPF, DKIM en DMARC kan jaarlijks tot vijfduizend Euro kosten. Voor TLS, DNSSEC, SPF en DKIM blijkt dit onder andere uit de impactanalyse en factsheets die IBD voor deze standaarden heeft gepubliceerd. Uw organisatie kan ook DMARC met beperkte kosten direct inzetten, al vergt de volledige analyse en configuratie van e-mail stromen van de organisatie enige aandacht en tijd. Overheidsorganisaties verzamelen daarom herbruikbare ervaring met DMARC configuratie en tooling die met uw organisatie kan worden gedeeld.

Gemeenten

Omdat VNG/KING ten tijde van de afspraak in het Nationaal Beraad een impactanalyse uitvoerde op de standaarden, is er niet eerder gerapporteerd over de gemeentedomeinen. Het gaat om 398 unieke gemeentedomeinen. In deze rapportage worden de scores van de gemeentedomeinen wel meegenomen. Om de rapportage makkelijk vergelijkbaar te houden met de eerdere halfjaarlijkse rapportages, zijn de gemeentescores afzonderlijk weergegeven.

Hoe wordt gemeten

De meting geeft de stand van zaken weer op de peildatum in augustus 2016[80]. De meting laat zien of een domein de gemeten standaarden ondersteunt. 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 maten 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[81]. Wij nodigen u uit om ons te melden als een bepaald domein geen 'transactiesite' herbergt, en daarom geen TLS ondersteunt.
- Tevens verzoeken wij organisaties die om weloverwogen *andere redenen* niet aan deze IV standaard voldoen, deze overwegingen aan ons te melden[82].
- 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 (met name SPF) ook op domeinen waarvan een organisatie geen e-mail verstuurt. Dit is relevant omdat ook die domeinen worden misbruikt (burgers weten vaak niet dat ze niet meer worden gebruikt), en juist domeinen waarvandaan niet gemaild wordt, makkelijk kunnen worden geblokkeerd met SPF.

Resultaten

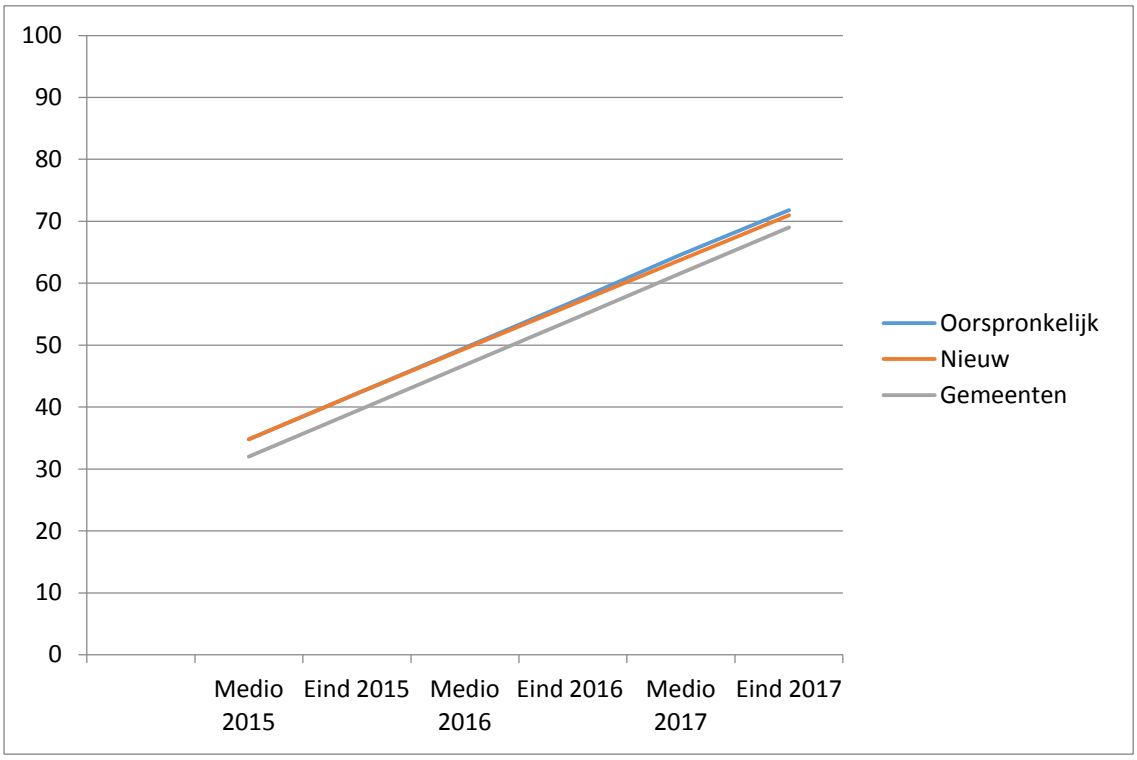
Bij de eerste meting medio 2015 was de gemiddelde adoptiegraad van de vijf standaarden op de toen getoetste set van grofweg 150 Nationaal Beraad domeinen **34,8 %.** Aan het einde van het jaar stond dit percentage op **42,2 %** en medio 2016 op **49,4 %** . Dit betekent dat ondanks de uitgesproken ambitie van het Nationaal Beraad de groei het afgelopen halve jaar niet is toegenomen.

Als we dit groeipercentage wordt extrapoleren naar het einde van 2017 (einde mandaatperiode van Forum Standaardisatie), dan blijkt dat zonder aanvullende acties, de adoptiegraad op dat moment zal blijven steken op **71%** en daarmee achterblijft op het afgesproken streefbeeld om de standaarden eind 2017 – daar waar van toepassing – te hebben geïmplementeerd.

De groei bij gemeenten ligt in de lijn van de groei bij partijen in het Nationaal Beraad. Door de iets lagere adoptiegraad bij de eerste meting (**32%**) zal de adoptiegraad van gemeenten eind 2017 bij extrapolatie uitkomen op **69%**.

[80] Het is mogelijk dat organisaties of gemeenten sindsdien adoptiemaatregelen genomen hebben, die (nog) niet in deze meting te zien zijn.
[81] In de overzichtslijsten is het ontbreken van TLS daarom geel gekleurd (in plaats van rood).
[82] In de praktijk maken organisaties zelden gebruik van het 'leg-uit' instrument in het 'pas-toe-of-leg-uit' beleid. Hierdoor missen wij mogelijk informatie over goede redenen om een standaard in een gegeven organisatie niet of gedeeltelijk toe te passen.

Gemiddeld adoptieniveau IV-standaarden geëxtrapoleerd naar eind 2017

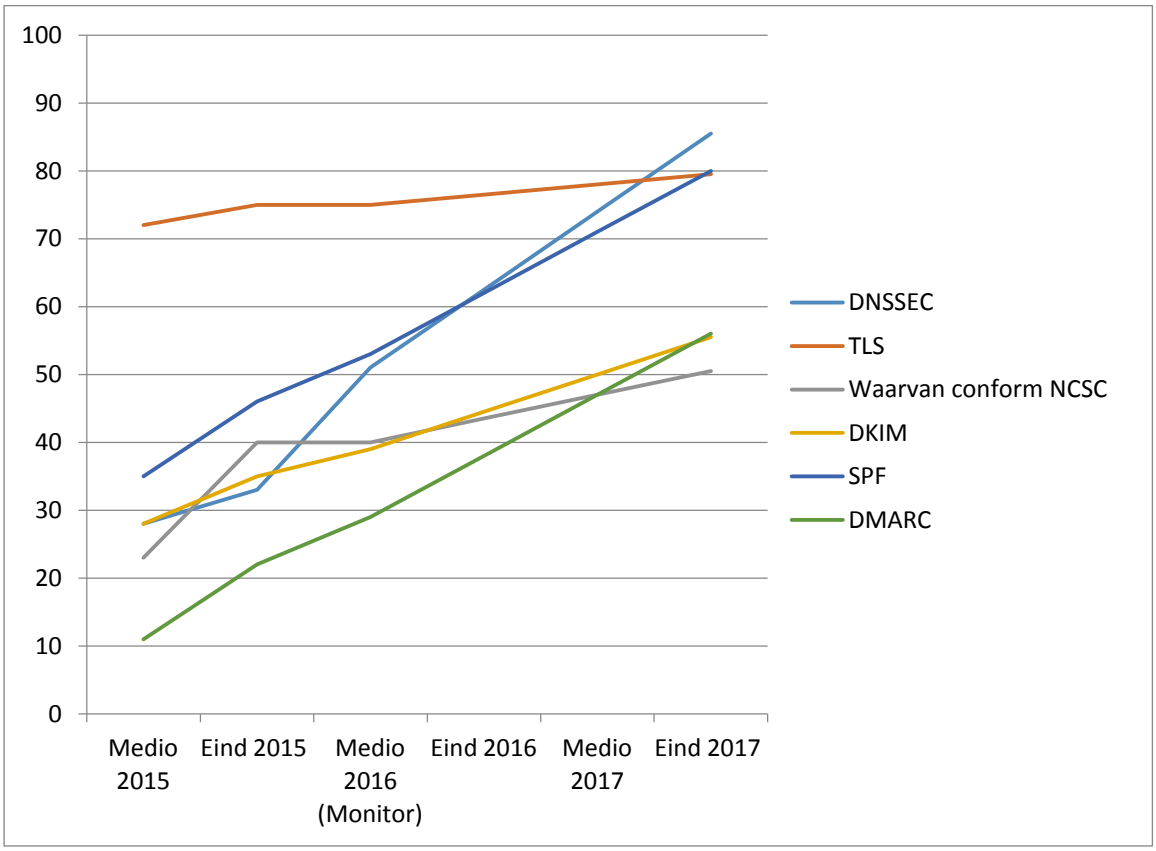


Figuur 1. Gemiddeld adoptieniveau IV-standaarden geëxtrapoleerd naar eind 2017.

Betekenis van de lijnen:

- 'Oorspronkelijk': verwachte groei adoptiegraad tot eind 2017 op basis van groei 2e helft 2015 (zonder gemeenten).
- 'Nieuw': verwachte groei adoptiegraad tot eind 2017 op basis van groei 1e helft 2016 (zonder gemeenten).
- 'Gemeenten': verwachte groei adoptiegraad op basis van groei afgelopen jaar (alleen gemeenten).

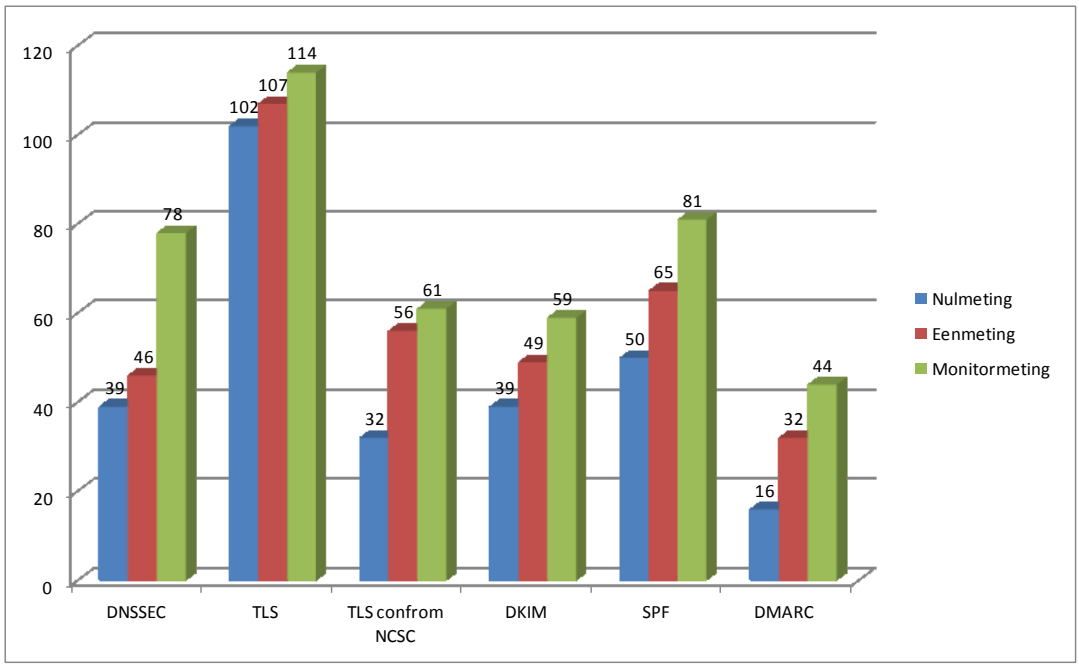
Per standaard ziet de verwachte groei bij organisaties van het Nationaal Beraad er als volgt uit:



Figuur 2: Gemiddelde groei per standaard geëxtrapoleerd naar eind 2017 (zonder gemeenten)

De resultaten per standaard

Figuur 3 geeft het absoluut aantal ondersteunde standaarden aan voor de 152 getoetste niet-gemeentelijke domeinen.



Figuur 3: Nationaal Beraad: het absoluut aantal ondersteunde standaarden, per standaard.

Betekenis van de staven:

- 'Nulmeting': medio 2015 (140 domeinen)
- 'Eenmeting': eind 2015 (140 domeinen)
- 'Deze meting': medio 2016 (152 domeinen)

De volgende tabel geeft de relatieve adoptiegraad weer per standaard, gebaseerd op de aantallen in figuur 3:

Nationaal Beraad	Nulmeting	Eenmeting	Deze meting	Verschil
DNSSEC	28%	33%	51%	23%
TLS	73%	76%	75%	2%
Waarvan conform NCSC	23%	40%	40%	17%
DKIM	28%	35%	39%	11%
SPF	35%	46%	53%	18%
DMARC	11%	22%	29%	18%

TLS was en is met afstand de meest toegepaste standaard (75%). Hierdoor is de relatieve groei van TLS beperkt. Daarentegen is het aantal sites dat TLS op de door het NCSC voorgeschreven veilige manier is geconfigureerd[83] over het afgelopen jaar flink gestegen (23% naar 40%). De groei van DNSSEC was in de tweede helft van 2015 beperkt, maar is met name in de eerste helft van 2016 flink toegenomen. DMARC is een relatief nieuwe standaard die met name in 2015 nog niet veel werd toegepast (11%). DMARC laat over het afgelopen jaar wel de grootste relatieve groei zien.

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

Best scorende domeinen en grootste stijgers

Onderstaande niet-gemeentelijke domeinen behalen een maximale score op de 5 getoetste standaarden en hebben TLS bovendien geconfigureerd volgens de aanbevelingen van het NCSC.

Best scorende domeinen

Domein	Organisatie
www.cbpweb.nl	Autoriteit persoonsgegevens
www.cjib.nl	Centraal Justitieel Incasso Bureau
www.ibdgemeenten.nl	Informatiebeveiligingsdienst voor gemeenten
www.logius.nl	Logius (Min. BZK)
www.rechtspraak.nl	Min. V&J
www.rijksoverheid.nl	Rijksoverheid
www.werkenbijdefensie.nl	Min. Defensie
www.forumstandaardisatie.nl	Forum Standaardisatie
lijsten.forumstandaardisatie.nl	Forum Standaardisatie

Daarnaast zijn er bij veel domeinen aanzienlijke verbeteringen te melden. Twee domeinen hebben vier standaarden meer toegepast dan bij de eerste meting een jaar eerder. En nog eens vijftien domeinen laten een nog steeds indrukwekkende verbetering zien van drie standaarden t.o.v. de eerste meting.

Gestegen met 4 standaarden

Domein	Organisatie
www.stelselcatalogus.nl	Logius (Min. BZK)
www.derbg.nl	Website van de Regionale Belastinggroep

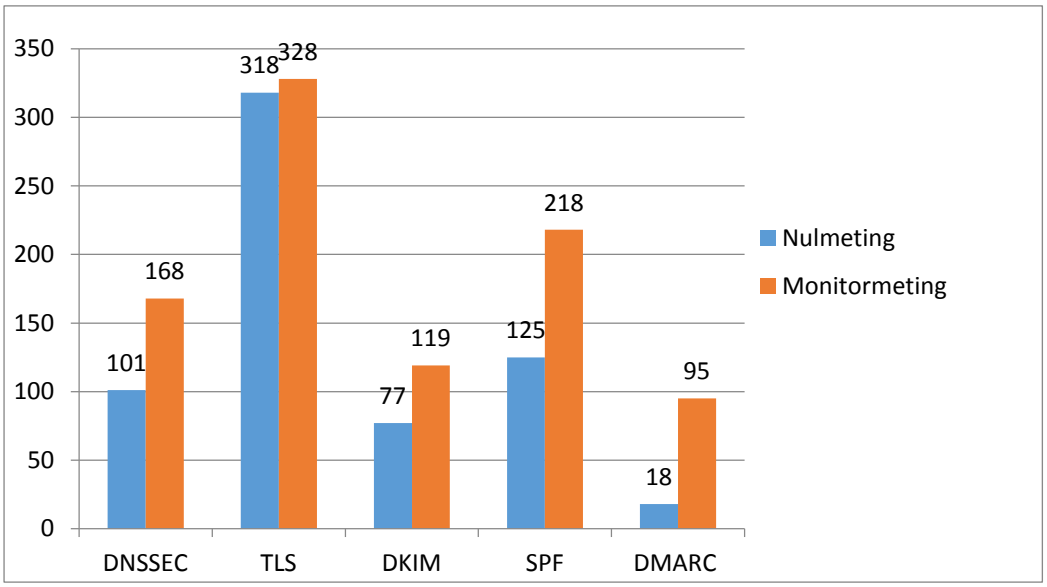
Gestegen met 3 standaarden

Domein	Organisatie
www.eidstelsel.nl	Logius (Min. BZK)
www.idensys.nl	Logius (Min. BZK)
register.digikoppeling.nl	Logius (Min. BZK)
www.rijksdienstvooridentiteitsgegevens.nl	Rijksdienst voor identiteitsgegevens (Min. BZK)
www.werk.nl	UWV (Min. SZW)
mijn.toeslagen.nl	Belastingdienst (Min. Fin)
www.duo.nl	DUO (Min OC&W)
siam.duo.nl	DUO (Min OC&W)
www.rijkswaterstaat.nl	Rijkswaterstaat (Min I&M)
www.cbs.nl	Centraal Bureau voor de Statistiek
www.crisis.nl	Nationaal Coördinator Terrorisme Bestrijding (MinV&J)
www.toeslagen.nl	Belastingdienst
www.provinciegroningen.nl	Provincie Groningen
www.prvlimburg.nl	Provincie Limburg
www.bsgw.nl	Belastingsamenwerking gem. en waterschappen Limburg

Gemeenten

In juni 2015 en in augustus 2016 hebben wij 398 unieke gemeentedomeinen getoetst met internet.nl. Dit betreft de hoofddomeinen van de gemeenten.

Veel gemeenten gebruiken naast het hoofddomein verschillende (sub)domeinen voor uiteenlopende doeleinden. Gemeente Den Haag hanteert bijvoorbeeld het domein mijn.denhaag.nl voor het deel van de website dat bedoeld is om als burger of bedrijf gegevens door te geven en diensten aan te vragen. De tooling die wij gebruiken voor de meting kan niet bepalen welke domeinen een gemeente gebruikt naast het hoofddomein, en waarvoor deze precies gebruikt worden. Om die reden is gekozen alleen de hoofddomeinen te toetsen[84].



Figuur 4: Gemeenten: absoluut aantal ondersteunde standaarden, per standaard

Betekenis van de staven:

- Nulmeting: medio 2015 (398 domeinen)
- Deze meting: medio 2016 (398 domeinen)

De volgende tabel geeft de relatieve adoptiegraad voor gemeenten weer per standaard, gebaseerd op de aantallen in figuur 4:

Gemeenten	Nulmeting	Deze meting	Verschil
DNSSEC	25%	42%	17%
TLS	80%	82%	2%
Waarvan conform NCSC	nb	21%	nvt
DKIM	19%	30%	11%
SPF	31%	55%	24%
DMARC	5%	25%	20%

[84] Forum Standaardisatie roept gemeenten en overige overheden op om aanvullende domeinen aan te melden waarvan zij vinden dat die onderdeel moeten zijn van de toetsing.

De adoptie van IV-standaarden groeit bij gemeenten in een tempo dat vergelijkbaar is met andere overheden. Het gebruik van DNSSEC en met name SPF is bovengemiddeld toegenomen bij gemeenten.

Wat opvalt is dat de initiële adoptiegraad van TLS bij gemeenten al hoog lag in 2015 (80%) en in 2016 is doorgegroeid naar 82%. Daarbij tekenen we aan dat, vergeleken met de niet-gemeentelijke domeinen, het aantal domeinen waarop gemeenten TLS configureren volgens de aanbevelingen van het NCSC[85] nog relatief laag is (21%).

In 2015 pasten gemeenten net als andere overheden DMARC nog op beperkte schaal toe, maar de laatste meting laat zien dat de adoptie van DMARC bij gemeenten flink groeit.

De scores van de individuele domeinen worden vanaf december 2016 gepubliceerd op de website van het Forum: https://www.forumstandaardisatie.nl/thema/internet-en-beveiliging

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

D. FAQ Monitor Open standaardenbeleid

In deze bijlage staat een aantal veelgestelde vragen (en het antwoord daarop) met betrekking tot de monitor en het open standaardenbeleid.

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 Vorig jaar 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.*

Over het beleid

Q Moet mijn organisatie voldoen aan 34 standaarden?
A *Nee. Elke overheidsorganisatie moet bij ICT-aanbestedingen vragen om de voor die aanbesteding relevante open standaarden van de lijst voor 'pas toe of leg uit'. 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. Bij de lijst voor 'pas toe of leg uit' (zie https://lijsten.forumstandaardisatie.nl) is het functionele toepassingsgebied en het organisatorische werkingsgebied van elke standaard vermeld. In de achterliggende toelichting wordt dit nader toegelicht. Voor één aanbesteding kunnen uiteraard meerdere open standaarden relevant zijn.*

Q Op welk moment moet ik voldoen aan een standaard?
A *Bij elke aanbesteding moet om de relevante standaarden gevraagd worden die op het moment van uitvragen op de lijst voor 'pas toe of leg uit' staan. Dit geldt zowel voor de aanschaf van ICT-producten of -diensten als voor inhuur en voor ontwikkeling. Het geldt voor nieuwe producten of diensten, maar ook voor voorzetting van reeds eerder verleende diensten en voor aanvulling op of wijziging van bestaande producten of diensten.*

Q Volgens mij is deze standaard voor mijn aanbesteding niet relevant?
A *Als het betreffende ICT-product of -dienst valt binnen het functionele toepassingsgebied van de standaard, en als de aanbestedende organisatie bovendien valt binnen het organisatorische werkingsgebied van de standaard, dan vereist de Rijksinstructie dat voor die standaard gekozen wordt. De Rijksinstructie laat geen ruimte om zelf te besluiten of een standaard 'in dit geval niet relevant' is. Het is wel mogelijk om hier gemotiveerd van af te wijken, op enkele gronden: onvoldoende aanbod, onvoldoende veiligheid of onvoldoende zekerheid bij het functioneren. Dan is het verplicht ('Leg uit') om deze afwijking in het jaarverslag te vermelden en te motiveren (zie https://www.forumstandaardisatie.nl/open-standaarden/voor-overheden/pas-toe-of-leg-uit-regime/leg-uit-in-de-praktijk).*

Q Ik ken een beter of goedkoper alternatief voor de standaard op de lijst, mag ik deze dan uitvragen?
A *Nee, het is verplicht om te vragen om de open standaard (die van toepassing is) van de lijst voor 'pas toe of leg uit'. Als het alternatief interessant is om op te nemen op deze lijst, kan je deze wel aanmelden bij Bureau Forum Standaardisatie.*

Q Wie kan ons helpen bij de inschatting of een standaard gevraagd dient te worden?
A *Bij twijfel kan altijd contact opgenomen worden met Bureau Forum Standaardisatie via: forumstandaardisatie@logius.nl of 070: 888 7776.*