FS-20171213.04A1

PBLQ

Monitor Open Standaarden Voorzieningen

Versie 1.0
1-12-2017

PBLQ
verbinders in de informatiesamenleving

Inhoudsopgave

1. Inleiding

1.1 Aanleiding

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

1.2 Opdrachtformulering

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

1.3 Werkwijze

Voor dit onderzoek is gebruik gemaakt van de 'pas toe of leg uit'-lijst van 16 juni 2017. Per voorziening is gekeken of de standaarden op deze lijst relevant zijn. Daarbij is telkens uitgegaan van de eindgebruiker. Dat is diegene die in de keten baat zou moet hebben bij het gebruik van open standaarden. Dit is expliciet zo gekozen, omdat het beleid ten aanzien van standaardisatie vooral gericht is op het stimuleren van interoperabiliteit. In eerdere onderzoeken is gebleken dat beheerders van voorzieningen soms terminologie gebruiken zoals 'voorbereid' zijn op een standaard, het ‘deels geïmplementeerd’ hebben of 'standaard xyz-ready' zijn. Hiermee bedoelen zij dat ze zelf voldoen aan de standaard of bezig zijn de standaard te implementeren, maar dat de andere partijen in hun keten nog geen gebruik kunnen maken van de standaard. Er is bijgevolg dan ook geen sprake van interoperabiliteit op basis van gebruik van de standaard. Wanneer er geen sprake is van interoperabiliteit hebben we dat in deze rapportage duidelijk aangegeven.

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

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

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

1.4 Aandachtspunten voor de lezer

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

- Ja: De voorziening is conform[1] met de standaard,
- Nee: De voorziening is niet conform met de standaard,
- Deels: Onderdelen van de voorziening zijn conform maar niet alle onderdelen[2],
- Gepland: Er zijn concrete plannen (gekoppeld aan een datum) om de voorziening op korte termijn conform te maken met de standaard.

Relevant of niet relevant
Voor de relevantiebepalingen zijn per standaard de beschrijvingen van het functioneel toepassingsgebied en van het organisatorisch toepassingsgebied, zoals vermeld op de pas-toe-of-leg-uit lijst van het Forum Standaardisatie gehanteerd.[3] Standaarden die niet relevant zijn voor een voorziening, zijn niet in de tabel opgenomen. In een beperkt aantal gevallen is onder de tabel nog een toevoeging opgenomen over standaarden die in de eerste inschatting wel relevant leken, maar dat bij nadere inspectie (nog) niet zijn. Ook in gevallen waar verwarring zou kunnen ontstaan over de relevantie is een nadere toelichting onder de tabel opgenomen. Daarnaast is voor de standaarden die dit jaar nieuw zijn op de lijst, opgenomen of ze relevant zijn. Deze inschatting is samen met de beheerders van de voorzieningen gemaakt.

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

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

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

---

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

[2] 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.

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

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

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

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

2. Gebruik standaarden per voorziening

2.1 BAG, BRK, WOZ en BGT

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

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

Standaard	Status	Toelichting
Ades Baseline Profiles	Nee	Deze standaard is nog niet geïmplementeerd. De mate van relevantie zal worden nagegaan.
Digikoppeling 2.0	Ja	Vrijwel alle koppelingen met afnemers, andere basisregistraties en evtl. front-office systemen worden gelegd op basis van Digikoppeling: - de koppelingen voor het aanleveren van gegevens aan LV-BAG, LV-WOZ en LV-BGT zijn gebaseerd op Digikoppeling standaarden; - het aanleveren door bronhouders (o.a. notariaat) van gegevens aan de BRK is niet gebaseerd op Digikoppeling; - de koppelingen voor het verkrijgen van informatie van gegevens uit LV BAG en LV WOZ en BRK zijn gebaseerd op Digikoppeling. Daarnaast kan informatie uit LV's worden verkregen via PDOK (Publieke Dienstverlening op de Kaart) die gebruik maakt van de Open GEO-standaarden. Ook de informatie uit de BRT wordt op deze wijze geleverd. Gegevens uit de BGT zijn beschikbaar via PDOK.
Digitoegankelijk	Ja	Het Kadaster voldeed vorig jaar al aan de Webrichtlijnen en heeft

(EN 301 549 met WCAG 2.0)		een toegankelijkheidsverklaring gepubliceerd op kadaster.nl.
DKIM	Ja	De implementatie van DKIM wordt is 8 september 2017 afgerond.
DNSSEC	Ja	De website www.kadaster.nl ondersteunt DNSSEC (zie https://internet.nl/domain/www.kadaster.nl/87074)
Geo-Standaarden	Ja	Naast de INSPIRE richtlijnen, maakt het Kadaster gebruik van NEN3610 en de meest gangbare Geo standaarden voor de betreffende basisregistraties.
HTTPS/HSTS	Gepland	HTTPS is correct geconfigureerd (en wordt afgedwongen) en alleen HSTS ontbreekt nog (zie https://internet.nl/domain/www.kadaster.nl/87074). Dit wordt na 8 september opgepakt, met verwachte implementatie per Q1 2018.
IPv4 en IPv6	Ja	Zowel IPv4 als IPv6 worden ondersteund door het Kadaster. (zie https://internet.nl/domain/www.kadaster.nl/87074)
NEN-ISO/IEC 27001/27002	Ja	Het Kadaster is gecertificeerd voor NEN-ISO/IEC 27001 en hanteert 27002. Het Handboek Beveiliging Kadaster is volledig op de BIR gebaseerd. In het jaarverslag is een in control statement opgenomen.
PDF 1.7, PDF/A-1 en PDF/A-2	Deels	Uittreksels worden verstrekt in PDF 1.4-formaat. Databestanden worden vooral in GML uitgewisseld. GML is een standaard XML-formaat voor Geo-data, gebaseerd op de Geo-standaarden. Afnemers melden geen problemen met het huidige PDF formaat. Daarom geeft het Kadaster geen prioriteit aan het vervangen van PDF 1.4. Voor het archiveren van kennisgevingen wordt gebruik gemaakt van PDF/A-1.
SKOS	Deels	Het Kadaster hanteert SKOS voor de beschikbaarstelling van begrippenkaders van basisregistraties. De begrippenkaders voor de BRK zoals gepubliceerd op brk.kadaster.nl, de BAG zoals gepubliceerd op bag.kadaster.nl en de BGT (IMgeo) en BRT op definities.geostandaarden.nl zijn allemaal conform SKOS. Voor de WOZ moet deze slag nog worden gemaakt. (4 van de 5 BR's)
SPF	Ja	Is geïmplementeerd per 8 september. (zie https://internet.nl/mail/kadaster.nl/36502)
STARTTLS/DANE	Gepland	STARTTLS is geïmplementeerd, maar DANE wordt na 8 september opgepakt, met verwachte implementatie per Q1 2018. (zie https://internet.nl/domain/www.kadaster.nl/87074)
StUF	Ja	Het Kadaster maakt deels gebruik van StUF en is deels volgens de Geo-standaarden (GML) opgemaakt. StUF wordt gebruikt voor aanlevering van bronhouder naar LV-BAG, LV-WOZ en LV-BGT. WOZ en BGT worden ook geleverd in StUF.
TLS v1.2, v1.1 en v1.0.	Ja	Deze standaard wordt volledig door het Kadaster ondersteund. (zie https://internet.nl/domain/www.kadaster.nl/87074)

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

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

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

2.2 Berichtenbox voor bedrijven

Beheerorganisatie: Rijksdienst voor Ondernemend Nederland (RVO).

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

Standaard	Status	Toelichting
Digikoppeling 2.0	Ja	Overheden kunnen via Digikoppeling geautomatiseerd berichten verzenden en ontvangen. Ondernemers kunnen alleen handmatig (via de website) hun Berichtenbox gegevens opvragen.
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Nee	Dictu heeft een webrichtlijnen toets gedaan, zie meegezonden stuk. Een concrete planning is nog niet bekend.
DKIM	Nee	DKIM is niet geïmplementeerd (zie https://internet.nl/mail/berichtenbox.antwoordvoorbedrijven.nl/34865).[4]
DNSSEC	Ja	Volgens internet.nl voldoet het domein berichtenbox.antwoordvoorbedrijven.nl (zie https://internet.nl/mail/berichtenbox.antwoordvoorbedrijven.nl/34865).
HTTPS/HSTS	Nee	HTTPS is geïmplementeerd, maar HSTS wordt niet afgedwongen (zie https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/91865).
IPv4 en IPv6	Nee	De website van de Berichtenbox ondersteunt IPv4 maar is volgens internet.nl niet toegankelijk via IPv6 (zie https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/91865). De Berichtenbox is wel IPv6 ready, maar nog niet de hele keten. E-ovb (beheerder van de Berichtenbox) is daarbij ook afhankelijk van leveranciers die hun IPv6 implementatie nog niet op orde hebben. De implementatie moet DICTU-breed gebeuren voordat dit voor de Berichtenbox gedaan zal worden. Een datum voor de implementatie is niet bekend.
PDF 1.7, PDF A/1, PDF A/2	Ja	Alle berichten kunnen worden gedownload (vanaf de Berichtenbox website) in PDF/A formaat. PDF-documenten worden gegenereerd in PDF A/1.
SAML	Ja	eHerkenning is SAML-based en wordt toegepast voor het inloggen op de

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

		Berichtenbox.
SPF	Nee	SPF is niet geïmplementeerd (zie https://internet.nl/mail/berichtenbox.antwoordvoorbedrijven.nl/34865).[5]
STuF	Ja	Wordt in combinatie met Digikoppeling gebruikt voor de uitwisseling met alle partijen die via digikoppeling op de berichtenbox zijn aangesloten.
TLS v1.2, v1.1 en v1.	Ja	De Berichtenbox maakt gebruik van TLS (1.2, 1.1 en 1.0). Zie https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/87107.

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

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

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

2.3 BRI

Beheerorganisatie: Belastingdienst

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

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

Standaard	Status	Toelichting
Digikoppeling 2.0	Ja	Digikoppeling wordt toegepast in de rol van afnemer van berichten van basisregistraties(HR). De ebms-koppeling met Digilevering is operationeel in de produktie-omgeving. De aansluiting op Digilevering wordt nu alleen gebruikt in de rol van afnemer van het stelsel van basisregistraties. Het aansluiten van de BRI als Basisregistratie/leverancier op Digilevering was vorig jaar niet eerder dan 2017-2018 gepland.
NEN-	Ja	De BRI voldoet aan de standaard beveiligingseisen van de

[5] Idem.

ISO/IEC 27001/27002		Belastingdienst. Deze eisen zijn conform VIR met classificatie departementaal vertrouwelijk. Voor opsporingsgegevens (FIOD) geldt een strakker regime. Aangezien het beveiligingskader voor de gehele Belastingdienst geldt, is er geen apart in control statement voor de BRI.
TLS v1.2, v1.1 en v1.	Ja	De actuele versies van TLS maken deel uit van de standaard beveiligingsrichtlijnen van de Belastingdienst.
WPA2 Enterprise	Ja	WPA2 wordt toegepast door de Belastingdienst.

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

2.4 BRT

Beheerorganisatie: Kadaster

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

Standaard	Status	Toelichting
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Ja	Het Kadaster voldeed al aan de Webrichtlijnen en heeft daarnaast een toegankelijkheidsverklaring gepubliceerd op kadaster.nl, waarin zij verklaart z.s.m. te willen voldoen aan Digitoegankelijk.
Geo-Standaarden	Ja	De BRT wordt zowel geleverd via PDOK (Wat biedt Publieke Dienstverlening Op de Kaart) in GML (Objectdata), als via internationale Geo-standaarden. Daarnaast wordt de BRT geleverd via PDOK in rasterformaat in GEO, tiff formaat en WMTS (Web Map Tile Service).
HTTPS/HSTS	Gepland	HTTPS wordt al toegepast, HSTS nog niet (zie https://internet.nl/domain/www.kadaster.nl/87074). Dit wordt na 8 september 2017 opgepakt, met verwachte implementatie per Q1 2018.
NEN-ISO/IEC 27001/27002	Ja	Het Kadaster is gecertificeerd voor NEN-ISO/IEC 27001 en hanteert 27002. Het Handboek Beveiliging Kadaster is volledig op de BIR gebaseerd. In het jaarverslag is een in control statement opgenomen.
OWMS	Nee	OWMS is wel van toepassing, maar PDOK hanteert via het Nationaal GEO Register de wettelijk vastgelegde standaarden, gebaseerd op Inspire en ISO volgens het zogenaamde NL

		profiel. Data.overheid.nl harvest het NGR met behulp van de CSW standaard (Catalogue Services for the Web' een OGC-Geostandaard (Open Geospatial Consortium), ook onderdeel van INSPIRE). De BRT voldoet dus niet aan de standaard maar voldoet wel aan alternatieve internationale standaarden. Er zijn geen interoperabiliteitsproblemen hierdoor.
SKOS	Ja	Het Kadaster hanteert SKOS voor de beschikbaarstelling van begrippenkaders van basisregistraties. De begrippenkaders voor de BRK zoals gepubliceerd op brk.kadaster.nl, de BAG zoals gepubliceerd op bag.kadaster.nl en de BGT (IMgeo) en BRT op definities.geostandaarden.nl zijn allemaal conform SKOS.
STARTTLS/DANE	Gepland	STARTTLS is al geïmplementeerd (zie https://internet.nl/domain/www.kadaster.nl/87074). DANE zal na 8 september opgepakt worden, met verwachte implementatie per Q1 2018.
TLS v1.2, v1.1 en v1.	Ja	Deze standaard wordt volledig door het Kadaster ondersteund (zie https://internet.nl/domain/www.kadaster.nl/87074)

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

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

2.5 BRV

Beheerorganisatie: RDW (Rijksdienst Wegverkeer)

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

Standaard	Status	Toelichting
CMIS	Nee	RDW doet aan verschillende vormen van document management. De RDW consolideert daarvoor op het Sharepoint platform. Dat platform kan CMIS ondersteunen, maar het staat per default uit. Er is op dit moment geen aanleiding, zowel intern als extern, om CMIS toe te passen.
Digikoppeling 2.0	Deels	RDW maakt voor alle nieuwe uitwisselingen gebruik van Digikoppeling. Dat is onder meer het geval in de uitwisseling met MijnOverheid (Berichtenbox), CJIB, Politie, ILT, CBR, de Belastingdienst, etc.
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Deels	De RDW heeft de toegankelijkheidsverklaring op de site geplaatst. Zie: https://www.rdw.nl/overrdw/Paginas/Toegankelijkheidsverklaring.aspx?path=Portal/Over RDW/Kwaliteit. De website van de RDW voldoet nog niet volledig aan Digitoegankelijk. Wel loopt een project voor volledige herbouw van RDW.nl. Hierin is aandacht voor Digitoegankelijk. Wanneer de site wordt opgeleverd zal een audit hierop worden gedaan.

DNSSEC	Ja	De niet-gevoelige (technische) gegevens uit de BRV zijn te bevragen via www.rdw.nl. Die site is volgens internet.nl gesigned met DNSSEC. Alle .nl rdw domeinen zijn gesigned met DNSSEC. Alle overige domeinen (.eu, .info, .com) staan binnen het programma RIT op de planning voor eind 2017, maar maken geen deel uit van de BRV.
HTTPS en HSTS	Gepland	HSTS gaat Fujitsu activeren voor de HTTPS ingangen die onderdeel zijn van de nieuwe werkplek omgeving. Voor de RDW diensten omgeving wordt HSTS geactiveerd bij de overgang van TMG naar F5. Dit wordt voor 1 juli 2018 gerealiseerd.
IPv4 en IPv6	Nee	IPv4 wordt gesupport, IPv6 wordt nog niet ingezet. De BRV is te bevragen via www.rdw.nl. Op dit moment ziet de RDW voor de BRV nog geen noodzaak om op IPv6 over te gaan.
NEN-ISO/IEC 27001/27002	Ja	RDW is ISO 27001/2 gecertificeerd. RDW voldoet niet aan alle extra voorschriften van de BIR, dat hoeft ook niet want RDW is gehouden aan de VIR (en met auditor is afgesproken dat voldoen aan de 27001/27002 norm gelijk staat aan voldoen aan de VIR). Er is een in control statement van de 27001/27002 en de BKR-audit.
OWMS	Ja	De toegang tot BRV-data is op data.overheid.nl in overeenstemming met OWMS gemetadateerd beschikbaar.
PDF 1.7, PDF A/1, PDF A/2	Ja	Bij digitale dienstverlening worden uittreksels en informatie uit de BRV in PDF/A vorm verstrekt.
SAML	Ja	Op 4 juli 2017 is de SAML2.0 koppeling actief geworden.
SKOS	Ja	Socrata verzorgt de open data omgeving van de RDW (https://opendata.rdw.nl/browse). Het RDF-XML formaat wordt ondersteund en de beheerder geeft aan dat zeer waarschijnlijk ook de SKOS standaard wordt ondersteund.
SPF	Ja	RDW ondersteunt en gebruikt de SPF standaard voor email verkeer.
STARTTLS en DANE	Gepland	STARTTLS, DANE, DKIM en SPF wordt bij de overgang naar Fujitsu voor alle DNS domeinen geïmplementeerd. Dit wordt voor 1 juli 2018 gerealiseerd.
TLS v1.2, v1.1 en v1.	Ja	RDW ondersteunt en gebruikt de TLS protocollen op de e-mail servers en Digikoppeling.

Ten opzichte van het onderzoek uit 2016 zijn er enkele ontwikkelingen. SAML was vorig jaar nog alleen in SAML 1.1 geïmplementeerd, maar sinds juli 2017 is versie 2.0 geïmplementeerd. Digitoegankelijk (vorig jaar nog Webrichtlijnen) staat nog steeds op status “Deels”, maar er loopt inmiddels een project voor de herbouw van rdw.nl, waarin ook aandacht voor Digitoegankelijk besteed zal worden. De SKOS standaard is dit jaar geïmplementeerd door het RDF-XML formaat te ondersteunen. Inmiddels is ook de TLS standaard toegepast op rdw.nl.

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

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

2.6 BSN Beheervoorziening en GBA-V

Beheerorganisatie: Rijksdienst voor Identiteitsgegevens (RvIG), Ministerie BZK

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

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

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

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

2.7 Digi-Inkoop

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting
DNSSEC	Ja	Digi-Inkoop voldoet aan DNSSEC (zie https://internet.nl/mail/digiinkoop.nl/36515).
HTTPS/HSTS	Nee	De voorziening voldoet aan HTTPS, maar niet aan HSTS[6]. Hiervoor bestaat nog geen planning.
IPv4 en IPV6	Nee	IPv6 werd vorig jaar niet ondersteunt door de hoster van Digi-Inkoop. Er zijn geen plannen dit te realiseren, en er is geen opdracht om dit aan te passen. (zie ook https://internet.nl/mail/digiinkoop.nl/36515)
NEN-ISO/IEC 27001/27002	Ja	Digi-Inkoop voldoet aan de BIR. Er is een in control statement afgegeven. Leveranciers voldoen aan ISO 27001.
PDF/A en PDF 1.7	Ja	De Digi-Inkoop applicatie produceert inkooporders en facturen in PDF formaat. Documenten die op logius.nl beschikbaar worden gesteld zijn in PDF/A formaat (dit zijn de documenten over de 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).
SETU	Ja	Digi-Inkoop ondersteunt de uitwisseling van SETU-hr-XML berichten
SMeF 2.0	Nee	Digi-Inkoop gebruikt de OHNL standaard voor berichtenuitwisseling en voldoet daarmee aan SMeF 1.3. Digi-Inkoop maakt gebruik van de specificaties van het semantisch model. Echter, er is geen opdracht om een upgrade naar 2.0 uit te voeren.
SPF	Nee	Digi-Inkoop voldoet nog niet aan deze standaard, en er bestaan op dit moment ook nog geen plannen om dit in de toekomst te implementeren. Digiinkoop.nl is alleen een applicatie domein, er wordt niet gemaild vanaf dit domein.
TLS v1.2, v1.1 en v1.0	Ja	Digi-Inkoop is 1.2 compliant (zie https://internet.nl/mail/digiinkoop.nl/36515).

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

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

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

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

2.8 DigiD

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Ja	Als overgangsperiode voldoet DigiD nu nog aan de Webrichtlijnen, een externe toets ten behoeve hiervan heeft plaatsgevonden (https://www.accessibility.nl/ondersteuning/inspectie/site-981 en https://www.digid.nl/help). Echter, tijdens dit onderzoek vond er een toets plaats WCAG2.0 AA t.b.v. de nog op te stellen Digitoegankelijk verklaring.
DKIM	Ja	DigiD mail wordt verstuurd met een DKIM signature (zie https://internet.nl/mail/digid.nl/34847).
DNSSEC	Ja	DNSSEC is doorgevoerd in release 4.5 van DigiD en inmiddels operationeel. Ook de mailservers voldoen aan de standaard (zie https://internet.nl/domain/digid.nl/87081).
HTTPS en HSTS	Ja	DigiD maakt gebruik van HTTPS voor de communicatie tussen clients (zoals browsers) en servers. Verder ondersteunt de DigiD website HSTS-policy met een geldigheidsduur van 1 jaar (zie https://internet.nl/domain/digid.nl/87081).
IPv4 en IPv6	Ja	De website DigiD.nl is via IPv6 toegankelijk. Inmiddels verlopen ook de mailstromen via IPv6 (zie https://www.internet.nl/mail/digid.nl/17054).
NEN-ISO/IEC 27001/27002	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Rijk (BIR) van toepassing die is gebaseerd op NEN-ISO27001. Logius heeft zich over toepassing van deze norm verantwoord door het afgeven van In Control Verklaringen (ICV's) aan de eigenaar (BZK/DGOBR).
SAML	Ja	DigiD biedt aan afnemers een SAML-koppelvlak. De meeste afnemers zitten nog op het A-select koppelvlak. SAML berichtuitwisseling in het eID stelsel (http://www.eid-stelsel.nl) zal anders zijn dan die van DigiD. Om partijen niet tot meerdere migraties te dwingen houdt DigiD het A-select koppelvlak nog in stand.
SPF	Ja	SPF is relevant voor DigiD bij alle mails vanuit de DigiD applicatie, en DigiD voldoet ook aan deze standaard (zie https://internet.nl/mail/digid.nl/34847)
STARTTLS/DANE	Ja	De mailserver van DigiD passen STARTTLS en DANE toe (zie https://www.internet.nl/mail/digid.nl/41975).
TLS	Ja	DigiD ondersteunt TLS v1.0 en TLS v1.2. TLS 1.1 wordt niet ondersteund, omdat Logius een sterke voorkeur heeft voor TLS 1.2. Om brede comptabiliteit mogelijk te maken wordt TLS 1.0 nog steeds ondersteund.

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

HTTPS/HSTS en STARTTLS/DANE relevant voor DigiD. Aan HTTPS/HSTS zowel als aan STARTTLS/DANE wordt voldaan.

Concluderend, worden bij deze voorziening alle relevanten standaarden toegepast.

2.9 DigiD Machtigen

Beheerorganisatie: Logius

DigiD Machtigen stelt burgers in staat anderen namens hen te machtigen. DigiD Machtigen wordt beheerd door Logius. Onderstaande antwoorden zijn grotendeels gebaseerd op de Verantwoording Open Standaarden die jaarlijks door Logius zelf opgesteld wordt. De huidige versie van DigiD Machtigen is 4.10

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

		gaan. Naast authenticatie gebruikt DigiD Machtigen de SAML standaard ook om een getekend machtigingsbewijs af te geven, namelijk als een SAML assertion.
SPF	Ja	De voorziening voldoet aan deze standaard, zie ook de toelichting bij DigiD.
TLS v1.2, v1.1 en v1.0	Ja	TLS is geïmplementeerd. DigiD Machtigen ondersteunt TLS v1.0, TLS v1.1 en TLS v1.2. Voor brede comptabiliteit worden TLS 1.0 en 1.1 nog ondersteund. Tijdens dit onderzoek is DDM aangepast zodat de site ook compliant is met de alle eisen die door de toets via internet.nl gehanteerd worden.

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

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

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

2.10 Digilevering

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting
Digikoppeling 2.0	Ja	Digilevering maakt gebruik van Digikoppeling
DKIM[7]	Ja	Digilevering draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. DKIM is geïmplementeerd op de centrale voorziening mail relay.
DNSSEC[8]	Ja	DNSSEC is geïmplementeerd op de centrale voorziening DNS.
HTTPS/HSTS[9]	Ja	Digilevering voldoet aan de HTTPS standaard. Aan HSTS wordt niet

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

[8] idem

[9] idem

		voldaan.
IPv4 en IPv6	Nee	Digilevering gebruikt het Logius infrastructuur platform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik. Digilevering ondersteunt op dit moment alleen IPv4.
SPF[10]	Ja	Digilevering draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. SPF is geïmplementeerd op de centrale voorziening mail relay.
STARTTLS/DANE[11]	Ja	Digilevering draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen.

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

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

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

2.11 Digimelding

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting
Digikoppeling 2.0	Ja	Digimelding maakt gebruik van Digikoppeling
DKIM[12]	Ja	DKIM draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. DKIM is geïmplementeerd op de centrale voorziening mail relay.

[10] idem

[11] idem

[12] idem

DNSSEC[13]	Ja	DNSSEC is geïmplementeerd op de centrale voorziening DNS.
HTTPS/HSTS[14]	Ja	Digilevering voldoet aan de HTTPS standaard. HSTS wordt niet toegepast.
IPv4 en IPv6	Nee	Digimelding gebruikt het Logius infrastructuur platform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik. Digimelding ondersteunt op dit moment alleen IPv4.
SPF[15]	Ja	Digilevering draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. SPF is geïmplementeerd op de centrale voorziening mail relay.
STARTTLS/DANE[16]	Ja	Digimelding draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen.

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

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

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

2.12 Diginetwerk

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting
DNSSEC	Ja	DNSSEC validatie wordt toegepast op Rijks-DNS.
IPv4 en IPV6	Nee	Binnen Diginetwerk wordt alleen IPv4 gebruikt, binnen het

[13] idem
[14] idem
[15] idem
[16] idem

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

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

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

2.13 DigiPoort

Beheerorganisatie: Logius

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

Omdat Digipoort slechts machine-naar-machine koppelingen levert zijn is deze voorziening niet getoetst met de toetsen van internet.nl.

Standaard	Status	Toelichting
Digikoppeling	Ja	Zie de koppelvlakspecificaties op http://www.logius.nl/producten/gegevensuitwisseling/digitpoort/koppelvlakken
DKIM	Ja	DigiPoort voldoet aan DKIM. Dit is ook relevant omdat de voorziening een SMTP koppelvlak heeft.
DNSSEC	Nee	Hoewel DigiPoort werkt met PKI certificaten ter authenticatie, zou DNSSEC ook ingericht moeten zijn. Er zijn geen plannen om dit in te richten, omdat de voorziening geen businesscase hiervoor ziet omdat het risico nihil is.
HTTPS/HSTS	Ja	De voorziening voldoet aan HTTPS. Formeel wordt niet aan HSTS voldaan, maar de standaard HTTP (poort 80) is bij de voorziening helemaal niet ontsloten, zodat feitelijk alleen via HTTPS een verbinding gemaakt kan worden. In de geest voldoet de voorziening dus impliciet wel aan HSTS.
IPv4 en IPV6	Nee	Digipoort gebruikt het Logius infrastructuur platform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik. Digipoort ondersteunt IPv4
NEN-ISO/IEC 27001/27002	Ja	DigiPoort voldoet aan de BIR. Leveranciers voldoen aan ISO 27001 of vergelijkbare standaard.

SETU	Ja	DigiPoort ondersteunt de uitwisseling van SETU-hr-XML berichten
SPF	Nee	DigiPoort heeft geen SPF-records. Er wordt niet gemaild vanuit dit domein, maar SPF zou wel ingericht moeten worden. Er wordt op dit moment naar gekeken, maar er liggen nog geen formele plannen deze stap te maken.
STARTTLS/DANE	Ja	Zowel STARTTLS als DANE zijn beide ingericht.
TLS v1.2, v1.1 en v1.	Ja	Digipoort ondersteunt v1.2, maar niet meer de verouderde versies.
XBRL en Dimensions	Ja	Wordt ondersteund door Digipoort.

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

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

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

2.14 Digitale Werkomgeving Rijksdienst (DWR)

Beheerorganisatie: Ministerie BZK

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

Standaard	Status	Toelichting
Ades Baseline Profiles	Deels	SSC-ICT is in staat om dit te leveren waar het door een afnemer gevraagd wordt. Voor een aantal klanten wordt dit geleverd.
Digikoppeling 2.0	Deels	Binnen VenJ vindt elektronisch berichtenverkeer interdepartementaal plaats via de Justitie Berichten Service (JUBES). JUBES is vanuit VenJ het koppelvlak voor de Digikoppeling dienst van Logius. De open standaarden eBMS en WUS zijn de daarbij gebruikte protocollen om de berichten veilig te versturen. Verder nemen alle departementen uit het verzorgingsgebied van SSC-ICT deel aan

		eFacturatie.
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Deels	Niet alle websites waar SSC-ICT zelf eigenaar is, voldoen op dit moment aan Digitoegankelijk. SSC-ICT is niet eigenaar van alle websites van haar klanten, bij deze websites ligt de verantwoordelijkheid bij de klant zelf.
DKIM	Deels	DKIM is geïmplementeerd voor 72 van de 90 domeinen die SSC-ICT in beheer heeft. Het is geïmplementeerd in combinatie met SPF en DMARC (DMARC is begin 2015 aangemeld voor opname op de pas-toe-of-leg-uit-lijst).
DNSSEC	Deels	De domeinen van de klanten van SSC-ICT die via de DNS van AZ lopen, voldoen. De domeinen van de klanten van SSC-ICT die via de DNS van SSC-ICT lopen, voldoen eind 2017. SSC-ICT geeft aan dat de cliënt DNSSEC-validatie ondersteunt, en dat RijksDNS DNSSEC-validatie ondersteunt.
HTTPS/HSTS	Deels	HTTPS wordt gebruikt, maar HSTS wordt niet standaard aangezet voor websites die SSC-ICT host voor klanten. Andere webgebaseerde voorzieningen maken wel gebruik van HSTS.
IPv4 en IPV6	Deels	IPv4 is in gebruik. De gebruikte technische componenten van DWR ondersteunen wel IPv6. IPv6 is een onderdeel van de infrastructuur en IPv6 reeksen worden uitgedeeld door Logius. Het is de bedoeling dat de internet facing kant van de DMZ IPv6 gaat ondersteunen, maar een concrete tijdlijn staat nog niet vast.
NEN-ISO/IEC 27001/27002	Ja	DWR voldoet aan de BIR en wordt hier ook op ge-audit. De laatste audit heeft plaatsgevonden in de periode 2015/2016.
ODF 1.2	Ja	De DWR Next client wordt geleverd met zowel Libreoffice 5.0 als Office 2016. Beide softwaresuites ondersteunen het lezen en schrijven van ODF bestanden.
PDF 1.7 / PDF A/1 en PDF A/2	Ja	De DWR Next client kan alle types PDF lezen. Schrijven van PDF kan op meerdere manieren. Alle types worden ondersteund, al is daarvoor soms wel het installeren van Adobe Acrobat Professional benodigd. PDF A/2 is mogelijk voor klanten die Adobe Acrobat Pro afnemen. De regulier verstrekte Adobe Acrobat Standard ondersteunt PDF A/2 niet, maar wel PDF 1.7 en PDF A/1.
SAML	Ja	Single Sign-on (SSO) op basis van SAML 2.0 wordt aangeboden als dienst in de Servicecatalogus van SSC-ICT. Het SSO-koppelvlak is een generieke dienst. Het project DOorontwikkeling Single Sign-On (DOrSSOn) voorziet internet facing aanvulling van de huidige oplossing met open source componenten gebaseerd op de standaarden SAML 2.0 en OAuth 2.0 in opdracht van de CIO Rijk.
SPF	Deels	SPF wordt op 72 van de 90 domeinen toegepast.
STARTTLS/DANE	Nee	De internet mailvoorziening werkt met STARTTLS. Implementatie van onder meer DANE is in onderzoek in het verlengde van het initiatief 'Veilige E-mail Coalitie'. DANE wordt niet meer in 2017 geimplementeerd, maar waarschijnlijk pas in 2018.
TLS v1.2, v1.1 en v1.0	Ja	De op de werkplek aangeboden browsers ondersteunen deze versies van TLS. De internet mailvoorziening werkt met STARTTLS. Voor webservers met applicaties van klanten wordt dit toegepast voor de klanten die dit hebben aangevraagd.
WPA2 Enterprise	Ja	Op de wifivoorziening van DWR wordt deze standaard toegepast. Dit is een kantoorvoorziening.

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

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

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

2.15 Doc-Direkt

Beheerorganisatie: Doc-Direkt

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

Standaard	Status	Toelichting
Ades Baseline Profiles	Nee	Bij Doc-Direct loopt momenteel een onderzoek over de mogelijke toepassing van deze standaard in de toekomst. De uitkomsten daarvan zijn naar verwachting in het eerste kwartaal van 2018 bekend.
CMIS	Nee	De mogelijkheid en noodzakelijkheid van het toepassen van deze standaard werden in 2016 nader onderzocht, maar dit heeft nog niet tot een besluit geleid.
Digikoppeling 2.0	Nee	Op dit moment wordt geen gebruik gemaakt van Digikoppeling
DKIM	Ja	Volgens SSC-ICT maakt Doc-Direkt gebruik van de mailservers van SSC-ICT, deze zijn onderdeel van het BZK domein, waarvoor DKIM actief is.
HTTPS/HSTS	Nee	Ook hierover loopt een onderzoek over de mogelijke toepassing van deze standaard in de toekomst. De uitkomsten daarvan zijn naar verwachting in het eerste kwartaal van 2018 bekend.
IPv4 en IPv6	Nee	De Haagse ring, waarover praktisch al het verkeer naar de Doc-Direkt voorzieningen loopt, ondersteunt geen IPv6. Het is bij Doc-Direkt niet bekend wanneer IPv6 gebruikt gaat worden. De beheerder van de Haagse Ring is Logius. De Haagse Ring is onderdeel van Diginetwerk. Binnen Diginetwerk wordt alleen IPv4 gebruikt, binnen het nummerplan is nu nog voldoende IPv4 ruimte beschikbaar.
NEN-ISO/IEC 27001/27002	Ja	Voor de informatiesystemen waarvan Doc-Direkt eigenaar is, is in 2016 een 'in controle verklaring' opgesteld. Op de punten waar Doc-Direkt afwijkt is een uitleg gegeven (explains) en er is een verbeterplan opgesteld.
ODF	Nee	Voor bewerkbare documenten wordt alleen .doc-formaat gebruikt. Er zijn geen plannen ODF te gebruiken.
PDF 1.7 – PDF A/1 of PDF A/2	Ja	Doc-Direkt ondersteunt in haar archieven vooral PDF/A. Alles wat gescand wordt gaat naar PDF/A. Daarnaast wordt ook 1.7 veel gebruikt.

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

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

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

2.16 eFactureren

Beheerorganisatie: Logius

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

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

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

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

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

2.17 MijnOverheid

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting
Digikoppeling 2.0	Deels	Nieuwe koppelingen worden conform Digikoppeling 2.0 ingericht. Nagenoeg alle koppelingen voldoen aan de standaard, alleen in het uitzonderlijke geval dat een afnemer dit niet ondersteunt, dan niet.
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Gepland	De laatste Webrichtlijnen toets is door Stichting Accessibility uitgevoerd (niet meer door Centric zoals voorheen) en hieruit zijn een aantal issues naar voren gekomen. Deze issues zijn opgelost en er is een nieuwe toets aangevraagd. Pas daarna kan worden vastgesteld of MijnOverheid volledig voldoet aan deze standaard.
DKIM	Ja	MijnOverheid voldoet aan DKIM (conform https://internet.nl)
DNSSEC	Ja	MijnOverheid voldoet aan DNSSEC (conform https://internet.nl)
HTTPS en HSTS	Ja	Deze standaard wordt toegepast.
IPv4 en IPV6	Nee	Mijnoverheid gebruikt het Logius infrastructuur platform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik. Mijnoverheid ondersteunt op dit moment alleen IPv4. (Er zijn plannen om IPv6 te activeren, maar er is nog geen concrete datum aan deze plannen gekoppeld)
NEN-ISO/IEC 27001/27002	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Rijk (BIR) van toepassing die is gebaseerd op NEN-ISO27001. Logius heeft zich over toepassing van deze norm verantwoord door het afgeven van In Control Verklaringen (ICV's) aan de eigenaar (BZK/DGOBR). De ICV’s zijn nog up-to-date.
OWMS	Nee	OWMS wordt niet ondersteund, want de web content van MijnOverheid is specifiek voor MijnOverheid en wordt dus niet uitgewisseld met andere partijen.
PDF 1.7, PDF/A-1 of PDF/A-2	Ja	MijnOverheid ondersteunt het genoemde PDF formaat, maar controleert hier niet op. MijnOverheid genereert zelf geen PDF files. In 2016 is een impact-analyse uitgevoerd om te onderzoeken wat het betekent wanneer men PDF-bijlages wel gaat controleren en wat eventuele vervolgacties zijn. Er is besloten om niet op formaat te gaan controleren
SAML	Ja	Authenticatie loopt via SAML
SPF	Ja	SPF is relevant en inmiddels geïmplementeerd.

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

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

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

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

2.18 NHR

Beheerorganisatie: Kamer van Koophandel

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

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

		2017 nog te gaan ondersteunen.
IPv4 en IPv6	Nee	De website kvk.nl ondersteunt IPv4, maar is niet toegankelijk via IPv6 (zie https://internet.nl/site/www.kvk.nl/87180). Het project om over te stappen naar IPv6 project is door de KvK nog niet ingepland. De KvK had in 2016 wel voorbereidingen getroffen, waaronder de overstap naar een andere ISP provider, zodat de KvK een migratie naar IPv6 uit kan gaan voeren. Deze situatie was in augustus 2017 nog niet veranderd.
NEN-ISO/IEC 27001/27002	Ja	De KvK is sinds 2016 ISO 27001 gecertificeerd en hanteert ISO27002.
PDF 1.7, PDF A/1, PDF A/2	Ja	Alle uittreksels en informatie uit het NHR wordt in PDF/A-vorm verstrekt. Het betreft PDF A/1.
SAML	Ja	eHerkenning is SAML-based en wordt toegepast voor het aanleveren van jaarrekeningen en informatieverstrekking. In de notarisapplicatie kan de notaris van achter zijn computer rechtstreeks opgave doen. Ook hier wordt gebruik gemaakt van SAML als authenticatieprocedure. Er liep in 2016 een traject waarbij de authenticatieprocedures en infrastructuur werden vervangen. Hierdoor kan SAML inmiddels voor elke dienst ingezet worden voor authenticatie.
SKOS	Nee	SKOS is nog niet geïmplementeerd in Gegevenscatalogus NHR. De standaard wordt wel voorzien door diverse ondersteunende software pakketten in gebruik bij de KVK rondom het NHR. Voor deze standaard zou in 2016 een impactscan uitgezet worden, maar dit is nog niet gebeurd. Wanneer dit wel gaat gebeuren kan door de KvK nog niet aangegeven worden.
SPF	Ja	SPF is ten opzichte van het vorige onderzoek nieuw op de lijst en inmiddels geïmplementeerd door NHR.
STARTTLS/DANE	Nee	De voorziening past alleen STARTTLS toe, DANE nog niet (zie https://internet.nl/mail/kvk.nl/34914). De planning is om HSTS Q4 2017 te gaan ondersteunen.
STuF	Ja	Ongeveer 10% van het verkeer van het NHR gaat naar medeoverheden. Die uitwisselingen vinden allemaal plaats via Digikoppeling en StuF.
TLS v1.2, v1.1 en v1.	Ja	De KvK gebruikt TLS op de verbindingen waar voorheen SSL werd gebruikt. De kamer is inmiddels overgegaan op TLS1.2 (zie https://internet.nl/site/www.kvk.nl/87180).

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

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

2.19 ODC Noord

Beheerorganisatie: Dienst Uitvoering Onderwijs (DUO)

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

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

A/1, PDF A/2		wordt gebruik gemaakt van PDF. PDFCreator van Windows wordt als printoptie in de kantoorautomatiseringsomgeving aangeboden. De standaardinstelling is PDF versie 1.4, optioneel is 1.5. Vooralsnog wordt er bij DUO nog voor gekozen om de gratis variant van PDF-creator beschikbaar te stellen. Deze biedt maximaal PDF 1.5. Gebruikers van LibreOffice (dat is het meest gebruikte Office-pakket binnen de operationele omgeving van ODC-Noord) kunnen documenten exporteren naar PDF/A-1. Op dit moment is dat nog geen standaard werkwijze.
SAML	Nee	ODC-Noord maakt voor het interne systeem geen gebruik van SAML. Bij het ontwikkelen van diensten ten bate van klanten (SaaS) wordt SAML onderzocht en waar mogelijk toegepast.
STARTTLS/DANE	Gepland	De implementatie van STARTTLS en DANE loopt op dit moment. Afronding is voor eind 2018 gepland.
TLS 1.2, 1.1 en 1.0	Ja	Het beleid van ODC-Noord voor internet-gekoppelde systemen is dat TLS (in volgorde) van TLS1.2, TLS1.1 wordt aangeboden. TLS 1.0 wordt niet toegepast tenzij er een explain komt van de site-eigenaar.
WPA2 Enterprise	Ja	Deze standaard is toegepast waar ODC-Noord wifi gebruikt.

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

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

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

2.20 Ondernemersplein

Beheerorganisatie: Kamer van Koophandel

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

Standaard	Status	Toelichting
BWB	Ja	Binnen de website, de content van AvB, wordt verwezen naar wetgeving conform de BWB standaard
CMIS	Nee	De tooling (CMS/ESB) ondersteunt de standaard wel, maar deze wordt niet actief gebruikt. Er zijn er geen content leveranciers die hun CMS in CMIS vorm aan het Ondernemersplein.nl beschikbaar stellen. Concreet is er dus nog geen toepassing op dit moment en er zijn ook nog geen plannen om dit te doen.
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Ja	Verklaring is beschikbaar. Meer informatie beschikbaar op: https://www.ondernemersplein.nl/toegankelijkheid/
DKIM	Ja	DKIM is geïmplementeerd (zie https://internet.nl/mail/ondernemersplein.nl/34765)
DNSSEC	Gepland	Wordt geïmplementeerd dit jaar op de nieuwe DNS omgeving.
HTTPS/HSTS	Ja	Aan deze standaard wordt voldaan (zie https://internet.nl/site/www.ondernemersplein.nl/86899).
IPv4 en IPV6	Ja	De website ondersteunt IPv4 en is toegankelijk via IPv6 (zie https://internet.nl/site/www.ondernemersplein.nl/86899).
NEN-ISO/IEC 27001/27002	Ja	Ondernemersplein is gehost bij de Kamer van Koophandel. Daar liep een ISO 27001 certificeringstraject en Ondernemersplein heeft dit inmiddels toegepast en is door een audit in april 2016 ook gecertificeerd hierop.
OWMS	Nee	De informatie op de website is gemetadateerd volgens een eigen model die past bij de metadatering van de partners.
SKOS	Nee	Er wordt niet aan deze standaard voldaan. Het moet nog onderzocht worden of hieraan voldaan zal worden en plannen gemaakt worden.
SPF	Ja	Er wordt aan deze standaard voldaan (zie https://internet.nl/mail/ondernemersplein.nl/34765).
STARTTLS/DANE	Nee	Aan STARTTLS wordt voldaan, maar aan DANE wordt nog niet voldaan. De KvK geeft aan nog te moeten onderzoeken of hieraan voldaan zal worden.
TLS v1.2, v1.1 en v1.	Nee	Technisch kan er worden overgestapt naar alleen TLS 1.2 echter plannen zijn uitgesteld door slechte browser ondersteuning aan eindgebruiker.

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

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

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

2.21 Overheid.nl

Beheerorganisatie: Kennis- en Exploitatiecentrum Officiële Overheidspublicaties (KOOP)

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

Standaard	Status	Toelichting
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Gepland	Er is een toegankelijkheidsverklaring conform EN 301459. De nieuwe eisen van deze nieuwe richtlijn zijn meegenomen in de vernieuwing van Overheid.nl, die eind 2017 staat gepland.
DKIM	Ja	DKIM is geïmplementeerd (zie https://internet.nl/domain/www.overheid.nl/87086).
DNSSEC	Ja	Overheid.nl voldoet sinds Q2 2015 aan DNSSEC (zie https://internet.nl/domain/www.overheid.nl/87086).
HTTPS en HSTS	Gepland	Het portaal-gedeelte (www.overheid.nl) voldoet aan de standaard (zie https://internet.nl/domain/www.overheid.nl/87086). Een aantal sub-sites staat nog gepland om in 2017 aan deze standaarden te laten voldoen.
IPv4 en IPV6	Ja	Er wordt voldaan aan IPv4 en IPv6 (zie https://internet.nl/domain/www.overheid.nl/87086).
NEN-ISO/IEC 27001/27002	Ja	Vanaf 2015 staat overheid.nl niet meer op die risicokaart van BZK en hoeft geen ICV meer worden afgegeven.
OWMS	Ja	Overheid.nl is gemetadateerd conform OWMS.
PDF 1.7 PDF/A-1 PDF/A-2	Ja	Alle PDF's van Officiële bekendmakingen zijn PDF/A-1a zoals wettelijk bepaald is.
SKOS	Ja	SKOS is geïmplementeerd voor de waardelijsten van OWMS.
STARTTLS en DANE	Ja	STARTTLS en DANE zijn geheel geïmplementeerd (zie https://internet.nl/mail/overheid.nl/34850).
TLS v1.2, v1.1 en v1.0	Gepland	De aanpassingen in deze standaard staan ingepland voor tweede helft 2017.

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

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

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

2.22 P-Direkt

Beheerorganisatie: P-Direkt

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

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

Standaard	Status	Toelichting
Ades Baseline Profiles	Nee	De implementatie van deze standaard is nog niet gestart.
BWB	Ja	Alle verwijzingen naar wetten worden conform de BWB-standaard gemaakt. De redactie heeft de richtlijn dat ze altijd op deze manier handelt bij verwijzingen naar wetsteksten of andere regels en richtlijnen die op wetten.overheid.nl te vinden zijn.
Digikoppeling 2.0	Ja	P-Direkt heeft vele interfaces met partijen binnen de overheid, Identity management, hr-data, arbo-diensten, ziekmeldingen, koppelingen met BD. Salarisverwerkingssysteem werkt op basis van Digikoppeling. Alle nieuwe koppelingen die P-Direkt ontwikkelt, worden gebouwd op basis van Digikoppeling. Richting 2018 migreert de voorziening naar de rijksdatacenters, Digikoppeling krijgt dan een nog belangrijkere rol.
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Nee	Het Portal is nog altijd in ontwikkeling. Er is op dit portal nog geen Webrichtlijnen toets geweest. P-Direkt is zich ervan bewust dat er nog geen volledige compliancy is met de Webrichtlijnen.
DKIM	Ja	P-Direkt maakt gebruik van de mailservers van SSC-ICT, onder andere voor het versturen van de loonstroken aan de medewerkers. P-Direkt heeft aangegeven dat het initiatief voor de adoptie van dit soort standaarden dan ook bij SSC-ICT ligt. Navraag bij SSC-ICT leert dat DKIM actief gemaakt is voor deze mailservice van P-Direkt.
DNSSEC	Nee	Op de Haagse ring maakt het netwerk van SSC-ICT, waar P-Direkt gebruik van maakt, geen gebruik van DNSSEC. Ook hier geldt dat P-Direkt een afnemer is van een Rijksbrede dienst en het initiatief voor het implementeren van DNSSEC bij de SSC-ICT ligt. SSC-ICT gaf in 2016 aan dat zij op hun beurt weer afhankelijk zijn van de leverancier van de Haagse ring, namelijk Logius.
HTTPS/HSTS	Nee	HTTPS is 100% doorgevoerd voor alle communicatie met klanten. HSTS is nog niet geïmplementeerd.
IPv4 en IPv6	Nee	De Haagse ring, waarover eigenlijk al het verkeer naar de P-Direkt loopt, ondersteunt geen IPv6. De P-Direkt voorzieningen, zoals gehost bij Match, ondersteunen in theorie momenteel al IPv6. In de praktijk is nog geen enkele afnemer op IPv6 aangesloten. Op het aanbieden van IPv6 door de Haagse Ring heeft P-Direkt geen invloed.
NEN-ISO/IEC 27001/27002	Deels	De hosting van de dienstverleningssystemen van P-Direkt voldoet aan de BIR (BIR compliancy is integraal onderdeel van de inrichting van

		het ODC, en als zodanig daarmee ook voor P-Direkt). Echter, er bestaat bij de beheerorganisatie nog onduidelijkheid of de beheerorganisatie ook aan de BIR voldoet. Daarom staat de status hier op Deels.
ODF	Nee	Veel brieven die automatisch gegenereerd worden, worden in Word gemaakt en naar managers verstuurd, die deze dan zelf nog aanpassen. P-Direkt gebruikt .doc, omdat dit voor de doelgroep het meest gangbaar is. De ontvanger van de brieven zou dit zelf moeten omzetten met de aanwezige KA software die ODF ondersteunt. Het proces dat brieven genereert is het niet mogelijk ODF bestanden te genereren.
PDF 1.7 – PDF A/1 of PDF A/2	Deels	De meeste zaken die het digitale personeelsdossier ingaan zijn PFD/A. De grootste uitzondering/afwijking zijn de digitale loonstroken, die zijn nog altijd PDF 1.3. Reden/oorzaak is dat deze aangemaakt worden met een standaard SAP conversieroutine die niet anders dan PDF 1.3 kan genereren. Er is momenteel geen concreet plan de loonstroken in PDF A/x te genereren. PDF A/2 wordt nog niet gebruikt binnen P-Direkt.
SAML	Ja	P-Direkt gebruikt SAML om Single Sign-On in te vullen. Verbinding naar de kerndepartementen is gelegd, maar een gedeelte van de rijksambtenaren van onderliggende organisatieonderdelen, moeten nog handmatig inloggen. P-Direkt heeft met de kerndepartementen de afspraak gemaakt dat de kerndepartementen verantwoordelijk zijn voor het implementeren van de Single Sign-on functie bij de onderliggende organisatieonderdelen.
SPF	Nee	SPF moet nog geïmplementeerd worden door de beheerder van de mail dienst (in het geval van P-Direkt is dat SSC-ICT).
TLS v1.2, v1.1 en v1.0	Ja	Alle diensten van P-Direkt die door middel van HTTP worden ontsloten, worden enkel aangeboden via TLS v1.0 of hoger.

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

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

2.23 PKIoverheid

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting
DNSSEC	Ja	Het PKIoverheid-deel van de website van Logius en de website van PKIoverheid

		maken gebruik van DNSSEC (zie https://internet.nl/domain/crl.pkioverheid.nl/87088 en https://internet.nl/domain/www.logius.nl/87089).
HTTPS/HSTS	Ja	Deze standaard wordt toegepast door de voorziening (zie https://internet.nl/domain/crl.pkioverheid.nl/87088 en https://internet.nl/domain/www.logius.nl/87089).
IPv4 en IPV6	Gepland	IPv6 is geïmplementeerd voor de informatiepagina's van PKIoverheid op de Logius website (zie https://internet.nl/domain/www.logius.nl/87089). De PKIoverheid specifieke applicatiepagina's zijn op dit moment nog niet geschikt voor IPv6 (zie https://internet.nl/domain/crl.pkioverheid.nl/87088). Navraag bij de leverancier leert dat dit wel is opgenomen op de roadmap maar (nog) niet voor 2017.
NEN-ISO/IEC 27001/27002	Ja	Primair is het Webtrust normenkader van toepassing op PKIoverheid. Dit kader kent strengere eisen dan deze ISO standaarden vereisen. Implementatie van de BIR is daarnaast uitgevoerd op basis van best effort.
OWMS	Ja	Op website van Logius ja, maar niet op de website van PKIoverheid (info is niet bedoeld voor hergebruik van overheidsinformatie).
PDF 1.7, PDF A/1, PDF A/2	Ja	Documenten die via de websites beschikbaar worden gesteld worden volgens PDF/A opgesteld.
TSL 1.2 en 1.1	Ja	Het PKIoverheid deel van de website van Logius maakt gebruik van TLS 1.1 en 1.2 en de website van PKIoverheid zelf maakt gebruik van TLS 1.2 (zie https://internet.nl/domain/crl.pkioverheid.nl/87088 en https://internet.nl/domain/www.logius.nl/87089).

Sinds het onderzoek van 2016 zijn er de volgende ontwikkelingen. De status van IPv6 is gewijzigd naar Gepland. Digitoegankelijk wordt als niet relevant voor de voorziening geacht, omdat de PKIoverheid specifieke applicatiepagina's (cert.pkioverheid.nl, crl.pkioverheid.nl en cps.pkioverheid.nl) voornamelijk bedoeld zijn voor machinale verwerking en het dus ook niet nodig geacht wordt om deze toegankelijk te maken (conform Webrichtlijnen of opvolgers).

Een aantal standaarden zijn ten opzichte van het vorige onderzoek nieuw op de PTOLU lijst. Hiervan is alleen de HTTPS/HSTS standaard relevant voor de voorziening, en deze standaard wordt ook toegepast.

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

2.24 Rijksoverheid.nl

Beheerorganisatie: Ministerie van AZ (DPC)

De website Rijksoverheid.nl is de publiekswebsite met informatie van en over alle ministeries. De website wordt verzorgd door de Dienst Publiek en Communicatie (DPC). DPC is een baten-lastendienst van het ministerie van AZ en biedt shared servicediensten aan de rijksoverheid op het gebied van Communicatie.

Standaard	Status	Toelichting
BWB	Ja	Binnen de website wordt verwezen naar wetgeving conform de BWB standaard. BWB wordt dus toegepast.

Digitoegankelijk (EN 301 549 met WCAG 2.0)	Ja	De website voldoet aan Digitoegankelijk (WCAG 2.0). Zie ook de verantwoording daarover op: http://www.rijksoverheid.nl/toegankelijkheid.
DKIM	Ja	DKIM is geïmplementeerd voor de bulk van het mailverkeer. Dit heeft betrekking op de nieuwsbrieven die DPC namens de diverse departementale opdrachtgevers verstuurt. Het gaat om de nieuwsbrieven- en persberichten-service voor de Rijksoverheid en het DPC-mailverkeer. Deze zijn met SPF-DKIM-DMARC uitgerust. DKIM is niet ingericht voor andere DPC-mailstromen, zoals de persoonlijke @rijksoverheid.nl mailboxen (niet in gebruik bij DPC), omdat deze lopen via de SSC-ICT mailservers. Dat betekent dat e-mailverkeer gebruikmakend van @rijksoverheid.nl niet onder beheer van DPC valt. Ook de domain @rijksoverheid.nl voldoet aan DKIM (zie https://internet.nl/mail/rijksoverheid.nl/34858).
DNSSEC	Ja	Rijksoverheid.nl is ondertekend met DNSSEC (zie https://internet.nl/site/www.rijksoverheid.nl/86909). DPC biedt DNSSEC ook aan al haar klanten die domeinen via haar registrar-functie afnemen.
HTTPS/HSTS	Ja	De voorziening voldoet aan deze standaard (zie https://internet.nl/site/www.rijksoverheid.nl/86909).
IPv4 en IPV6	Ja	Rijksoverheid.nl ondersteunt zowel IPv6 als IPv4 (zie https://internet.nl/site/www.rijksoverheid.nl/86909).
NEN-ISO/IEC 27001/27002	Ja	Hosting leverancier Ordina heeft een NEN 27001/2 implementatie waarin de beveiliging van rijksoverheid.nl meegaat. DPC zelf valt onder de VIR/BIR-implementatie van het moederdepartement AZ. AZ is het enige departement dat zonder bevindingen door de ADR audits is gekomen.
ODF 1.2	Ja	Het CMS van het Platform Rijksoverheid Online accepteert slechts PDF en ODF (open standaard) formaten. Er zijn wel 'legacy'-bestanden in alleen .doc of .xls formaat. Nieuwe documenten zijn echter altijd tenminste in PDF- of indien bewerkbaar, in ODF-formaat beschikbaar. De PDF-generator die men gebruikt is goed voor het leeuwendeel van de PDF's op de website en genereert PDF-bestanden in PDF/A-1a.
OWMS	Ja	De beleidskeuzes (contentmodellen) zijn in te zien in het Informatie Publicatie Model (IPM) bij het OWMS (zie: http://standaarden.overheid.nl/rijksoverheid).
PDF 1.7 / PDF A/1 en PDF A/2	Ja	DPC publiceert zelf geen PDF's, maar departementen kunnen PDFs op Rijksoverheid plaatsen. Vooralsnog kan de Rijksoverheid praktisch niet aan deze richtlijn voldoen. DPC is daarover met BZK in gesprek.
SAML	Ja	Er is een soort WeTransfer app binnen het Rijksoverheid online platform. Deze maakt gebruik van SAML voor het authentiseren van gebruikers. Er zijn geen andere diensten die via Rijksoverheid worden aangeboden en inloggen vereisen (met SAML).
SPF	Ja	Het e-maildomein @rijksoverheid.nl is integraal van SPF voorzien (zie https://internet.nl/mail/rijksoverheid.nl/34768).
TLS v1.2, v1.1 en v1.0	Ja	Rijksoverheid.nl maakt gebruik van het Platform Rijksoverheid Online en daardoor geheel voorzien van https door middel van PKIo EV certificaten (zie https://internet.nl/site/www.rijksoverheid.nl/87100) .

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

Concluderend, zijn alle relevante standaarden bij deze voorziening geïmplementeerd.

2.25 Rijkspas

Beheerorganisatie: Ministerie van BZK

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

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

Standaard	Status	Toelichting
Digikoppeling 2.0	Ja	Rijkspas maakt gebruik van het WUS-gedeelte van de Digikoppeling. De deelnemers kunnen zelf de keuze maken welk protocol ze hanteren, de standaard koppeling Rijkspas of de Digikoppeling.
DKIM	Gepland	Voor Rijkspas worden mails verstuurd vanaf de applicatie voor Interdepartementale Toegang (IdT). In de huidige infrastructuur is dit niet toegepast. Uiterlijk Q3 2018 worden de Rijkspassystemen verhuisd naar een nieuw datacenter waar DKIM wel toegepast zal worden.
DNSSEC	Gepland	Rijkspas communiceert momenteel nog niet via het publieke internet. De verbinding die daarvoor voorzien is, maakt wel gebruik van DNSSEC. Voor communicatie binnen de Rijksoverheid wordt momenteel gebruik gemaakt van de Haagse Ring. Deze ondersteunt nog geen DNSSEC, maar de leverancier geeft aan dat de verwachting is DNSSEC eind 2017 wel geïmplementeerd gaat worden.
IPv4 en IPV6	Nee	IPv4 wordt toegepast. De Haagse ring, waarover eigenlijk al het verkeer naar de Rijkspas voorzieningen loopt, ondersteunt geen IPv6. Deze dienst wordt door Logius geleverd, en is onderdeel van de ‘connectiviteitsdiensten’ waarvan I&I gebruik maakt.
NEN-ISO/IEC 27001/27002	Ja	De Rijkspas heeft een eigen normen- en beveiligingskader gebaseerd op ISO-9001 en 27001/2. Jaarlijks worden hier ook audits op gedaan, onder andere door de Audit Dienst Rijk.
SAML	Ja	De Interdepartementale Toegang applicatie (IDT) is per 2015 aangesloten op de Single Sign On voorziening via SAML.
SPF	Ja	SPF is geïmplementeerd.
STARTTLS/DANE	Nee	Rijkspas neemt email dienstverlening af van SSC-ICT, en vanuit deze leverancier is aangegeven de nog niet alle randvoorwaarden in plaats zijn voor deze standaard. Eén van deze randvoorwaarden is DNSSEC, waarvan de implementatie einde 2017 verwacht wordt. Na deze implementatie zal SSC-ICT opnieuw de mogelijkheden van STARTTLS en DANE analyseren.
TLS v1.2, v1.1 en v1.0	Ja	TLS wordt gebruikt voor het veilig ontsluiten van de website voor IdT.

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

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

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

2.26 Rijksportaal

Beheer organisatie: Ministerie BZK

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

Standaard	Status	Toelichting
IPv4 & IPv6	Nee	Het huidige Rijksportaal (versie 1.6.5) is alleen ingericht voor IPv4. Om performance redenen wordt IPv6 momenteel nog niet toegepast. Oplossing van de oorzaken van de performance-issues is onderwerp van onderzoek.
ODF	Ja	ODF wordt ondersteund: ODF-bestanden kunnen geüpload en gedownload worden en de inhoud van ODF-bestanden kan door de zoekmachine worden geïndexeerd. Naast ODF worden op het Rijksportaal ook andere documentformaten gebruikt; het gebruik van ODF wordt niet afgedwongen.
PDF 1.7 PDF/A-1, PDF/A-2	Ja	PDF wordt ondersteund: PDF-bestanden kunnen geüpload en gedownload worden en de inhoud van PDF-bestanden kan door de zoekmachine worden geïndexeerd. Naast PDF 1.7, PDF/A-1 en PDF/A-2 worden op het Rijksportaal ook andere PDF-versies gebruikt; het gebruik van PDF 1.7, PDF/A-1 en PDF/A-2 wordt niet afgedwongen.
SAML	Ja	De implementatie van SAML is in juli 2016 opgeleverd. Het Ministerie van Veiligheid en Justitie is de eerste klant die kan worden aangesloten op de huidige versie 1.6.5 van het Rijksportaal.

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

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

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

Concluderend, moet het Rijksportaal alleen nog de IPv6implementeren.

2.27 Samenwerkende Catalogi

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Ja	Publicatie standaard op www.logius.nl zie aldaar voor Digitoegankelijk compliance. Overheid.nl ontsluit decentrale content op basis van Samenwerkende Catalogi, zie voor Digitoegankelijk compliance aldaar; Publicatie op basis van Samenwerkende Catalogi door overheden op eigen website Digitoegankelijk compliance eigen verantwoordelijkheid deelnemers (Rijk/gemeenten/provincies/waterschappen)
OWMS	Ja	Samenwerkende catalogi is volledig gebaseerd op OWMS.

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

2.28 SBR (Standard Business Reporting)

Beheerorganisatie: Logius

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

Dienst Uitvoering Onderwijs (DUO)[17]. De voorziening voor de e-dienstverlening is Digipoort. SBR heeft een eigen website.

Standaard	Status	Toelichting
Ades Baseline Profiles	Ja	Binnen SBR (Assurance) waarbij bijvoorbeeld jaarverslagen worden ondertekend door een accountant, wordt binnen DigiPoort gebruik gemaakt van XAdES als EU standaard.
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Nee	Voor SBR-NL.nl werd nog niet op Digitoegankelijk getoetst dus er is nog geen verklaring, vandaar voldoet de website nog niet aan het toetsingbeleid van deze standaard.
DKIM	Nee	De website van SBR (http://www.sbr-nl.nl) heeft ook een mailserver. In het verleden voldeed deze aan DKIM, maar omdat de website overgezet wordt naar het Ministerie van AZ, moet DKIM (naast DMARC en SPF) nog ingesteld worden. Daardoor voldoet de website momenteel niet aan DKIM).
DNSSEC	Nee	De website van SBR (http://www.sbr-nl.nl) is ondergebracht bij een derde partij. Ook het technisch DNS-beheer is daar ondergebracht, maar nog niet alle domeinen maken gebruik van DNSSEC.
IPv4 en IPv6	Ja	De website van SBR wordt bij een derde partij gehost en is bereikbaar met IPv6.
PDF 1.7, PDF A/1, PDF A/2	Ja	Bij het publiceren van documenten houdt Logius voor SBR PDF/A aan bij publicatie.
SPF	Nee	De website van SBR (http://www.sbr-nl.nl) heeft ook een mailserver. Deze voldoet niet aan SPF (zie https://internet.nl/mail/sbr-nl.nl/results). De SBR website is hierin afhankelijk van de 'moederwebsite' www.logius.nl.
STARTTLS/DANE	Nee	Aan STARTTLS wordt voldaan, door de voorziening. Aan DANE wordt nog niet voldaan, hiervoor is ook nog geen planning bekend omdat de SBR website hierbij afhankelijk is van de 'moederwebsite' www.logius.nl.
TLS 1.0, 1.1 en 1.2	Ja	De verbinding alleen mogelijk voor voldoende veilige TLS-versies. (zie https://internet.nl/site/www.sbr-nl.nl/#). In geval van Digipoort geldt voor de markt bij koppelvlak WUS en ebMS dat TLS 1.2 de standaard is. TLS 1.0 (en mogelijk ook 1.1) is uitgefaseerd. SSL v3 en v3.1 zijn in 2015 uitgefaseerd. Het koppelvlak Grote Berichten 3.0 worden op TLS 1.0 en TLS 1.1 aangeboden. TLS 1.0 en TLS 1.1 worden nog uitgefaseerd.
XBRL	Ja	SBR maakt gebruik van XBRL.

Ten opzichte van het onderzoek uit 2016 zijn er een aantal ontwikkelingen. Omdat SBR geen infrastructuur voorziening in de typische zin is maar veeleer een standaard die op de DigiPoort

[17] 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.

voorziening draait, staat Digikoppeling niet meer als relevante standaard in de tabel voor SBR maar bij DigiPoort. Omdat DigiPoort dit jaar geheel aan de IPv6 standaard voldoet, staat deze standaard nu ook bij SBR op “Ja”. Aan DKIM wordt in tegenstelling tot vorig jaar niet voldaan, omdat de website recent is overgezet naar een nieuwe beheerder.

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

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

2.29 Stelsel Elektronische Toegangsdiensten

Beheerorganisatie: Logius

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

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

Standaard	Status	Toelichting
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Ja	Digitoegankelijk (EN 301 549 met WCAG 2.0) is een eis vanuit het stelsel aan de deelnemers. Bij vermoeden van non-conformiteit kan een toets worden opgestart. De website voor eHerkenning.nl, onder beheer van de beheersorganisatie zelf, voldoet en is getoetst conform WCAG 2.0 (AA): https://www.accessibility.nl/ondersteuning/inspectie/site-1497. Voor Idensys staat dit gepland (mede afhankelijk van besluitvorming).
DKIM	Ja	Bij verstuurde email wordt DKIM toegepast, bij ontvangst gebeurd dit door de centrale email voorzieningen van Logius (SSC-ICT).
DNSSEC	Ja	DNSSEC werd in 2015 in de productieomgeving opgenomen.
HTTPS en HSTS	Ja	HTTPS en HSTS wordt toegepast op alle websites en webapplicaties onder beheer van de beheerorganisatie.
IPv4 en IPv6	Gepland	Aan de ondersteuning van IPv6 voor alle (publiek toegankelijke) systemen wordt gewerkt. De plandatum om IPv6 geheel geïmplementeerd te hebben is eind 2017.
NEN-ISO/IEC 27001/27002	Ja	De BIR is van toepassing op Logius, in het stelsel wordt certificering tegen ISO27001 geëist voor de deelnemers. De beheerorganisatie zelf is als stelselbeheerder ook gecertificeerd

		volgens ISO 27001. Daarvoor is ook een in controlstatement beschikbaar.
PDF 1.7, PDF/A-1 of PDF/A-2	Ja	Primair wordt de stelseldocumentatie via HTML op eherkenning.nl gepubliceerd. Stelseldocumentatie wordt met behulp van office software gepubliceerd in PDF/A-formaat. Overige documenten worden met een aparte tool in PDF/A formaat geconverteerd omdat het gehanteerde DMS dit niet ondersteunt.
SAML	Ja	SAML is een verplichte eis vanuit het stelsel.
SPF	Ja	SPF wordt toegepast bij de voorziening, maar wordt vooralsnog niet vereist als toe te passen techniek voor deelnemers.
STARTTLS en DANE	Nee	STARTTLS is geïmplementeerd voor eherkenning.nl en idensys.nl. De implementatie van DANE is nog onderwerp van onderzoek.
TLS v1.2, v1.1 en v1.	Ja	Het afsprakenstelsel stelt het gebruik van TLS1.x verplicht.

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

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

2.30 Stelselcatalogus

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting
BWB	Ja	De Stelselcatalogus gebruikt het Basis Wetten Bestand (BWB) via Juriconnect als open standaard voor de link naar de wetgeving als bron. De Juriconnect Id's worden gebruikt om per gegeven of begrip in de Stelselcatalogus de link te leggen naar de wet en het artikel in het Basis Wetten Bestand.
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Ja	De webpagina's van de Stelselcatalogus vallen binnen de website van digitaleoverheid.nl. Zie certificaat van toegankelijkheid van Accessibility.nl .Zie https://www.digitaleoverheid.nl/toegankelijkheidsverklaring
DNSSEC	Ja	DNSSEC is geïmplementeerd op de centrale voorziening DNS (zie https://internet.nl/site/www.stelselcatalogus.nl/92837).
HTTPS / HSTS	Nee	De HTTPS implementatie staat gepland voor medio Q4 2017. HSTS wordt nog niet geïmplementeerd.

IPv4 en IPv6	Ja	Stelselcatalogus gebruikt het Logius infrastructuur platform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik. Stelselcatalogus ondersteunt IPv4 en IPv6 (zie https://internet.nl/site/www.stelselcatalogus.nl/92837).
PDF 1.7, PDF A/1, PDF A/2	Ja	Documenten worden als PDF-A/1 aangeboden via de website.
SKOS	Ja	SKOS wordt toegepast door de voorziening.

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

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

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

2.31 TenderNed

Beheerorganisatie: PIANOo/DICTU

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

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

Standaard	Status	Toelichting
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Nee	TenderNed wordt momenteel gerenoveerd. Daarbij worden de schermen deels vernieuwd. Bij de implementatie van nieuwe schermen worden de richtlijnen uit EN 301 539 toegepast.
DKIM	Nee	E-mails verzonden vanuit TenderNed zijn niet beveiligd met DKIM (zie https://internet.nl/mail/tenderned.nl/34863).
DNSSEC	Ja	Het domein is gesigned met DNSSEC (zie https://internet.nl/site/www.tenderned.nl/86922).
HTTPS en HSTS	Ja	De client-server communicatie van TenderNed is beveiligd met HTTPS en HSTS (zie https://internet.nl/site/www.tenderned.nl/86922).
IPv4 en IPV6	Nee	Tenderned.nl is niet voorbereid op IPv6 (zie https://internet.nl/site/www.tenderned.nl/86922). TenderNed is afhankelijk van de hostingpartij. Wanneer deze een transitie door maakt naar IPv6 zal TenderNed daar in mee gaan.
NEN-ISO/IEC 27001/27002	Ja	TenderNed is ISO27001/2 gecertificeerd. Dit wordt jaarlijks geaudit.
PDF 1.7,	Ja	Geautomatiseerd gecreëerde PDF's (bij de aankondigingen) zijn

PDF/A-1, PDF/A-2		gemaakt in versie 1.7.
SAML	Ja	Per 1 juli 2014 is het mogelijk voor gebruikers om, naast de huidige registreer- en inlogmogelijkheden, gebruik te maken van inloggen via eHerkenning. De huidige mogelijkheden worden vanaf deze datum uitgefaseerd. (Bron: http://www.tenderned.nl/eherkenning-en-tenderned-0)
SPF	Nee	TenderNed past de SPF standaard niet toe (zie https://internet.nl/mail/tenderned.nl/34863). In het verleden is SPF wel actief geweest voor tenderned.nl. Dit leverde echter problemen op na een migratie van mailservers bij de DICTU. Daarom is deze functionaliteit uitgezet.
STARTTLS en DANE	Nee	STARTTLS wordt ondersteund. DANE nog niet.
TLS v1.2, v1.1 en v1.0	Ja	TenderNed past TLS 1.2 toe (zie https://internet.nl/site/www.tenderned.nl/86922). Voor een aantal koppelingen wordt nog TLS 1.0 gebruikt voor compatibiliteit.

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

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

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

Geïnterviewde personen

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