FS-20191211.05A2

PBLQ

Monitor Open Standaarden Voorzieningen 2019

Versie 1.00
26-11-2019

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 onderzoek uit in opdracht van Bureau Forum Standaardisatie en heeft PBLQ gevraagd een scan te maken van een aantal overheidsvoorzieningen.

1.2 Opdrachtformulering

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

1.3 Werkwijze

Voor dit onderzoek is gebruik gemaakt van de 'pas toe of leg uit'-lijst van 1 mei 2019. Per voorziening is gekeken of de standaarden op deze lijst relevant zijn.
Daarbij is telkens uitgegaan van de eindgebruiker. Dat is diegene die in de keten baat zou moet hebben bij het gebruik van open standaarden. Dit is expliciet zo gekozen, omdat het beleid ten aanzien van standaardisatie vooral gericht is op het stimuleren van interoperabiliteit. In eerdere onderzoeken is gebleken dat beheerders van voorzieningen soms terminologie gebruiken zoals 'voorbereid' zijn op een standaard, het ‘deels geïmplementeerd’ hebben of 'standaard xyz-ready zijn’. Hiermee bedoelen zij dat ze zelf voldoen aan de standaard of bezig zijn de standaard te implementeren, maar dat de andere partijen in hun keten nog geen gebruik kunnen maken van de standaard. Er is bijgevolg dan ook geen sprake van interoperabiliteit op basis van gebruik van de standaard. Wanneer er geen sprake is van interoperabiliteit hebben we dat in deze rapportage aangegeven.

In dit onderzoek wordt per voorziening een overzicht opgesteld van relevante standaarden en de mate waarin daarvan gebruik wordt gemaakt. Het vertrekpunt daarbij is telkens het overzicht van vorig jaar. Waar mogelijk zijn de standaarden opnieuw getoetst. Daarbij maken we onder meer gebruik van de testen die beschikbaar zijn via https://internet.nl. Hiermee kan voor een groot deel van de standaarden getoetst worden of eraan voldaan wordt[1]. Daarnaast kijken we – voor zover mogelijk – of de geplande activiteiten inmiddels uitgevoerd zijn. Voor nieuwe voorzieningen maken we een inschatting welke standaarden relevant zijn. Voor nieuwe standaarden op de lijst maken we een inschatting of ze relevant zijn voor de voorzieningen.

Op basis van bovenstaande inschattingen en toetsen maken we een eerste overzicht per voorziening. Dat overzicht wordt met een aantal expliciete vragen toegestuurd aan de vertegenwoordigers van de voorzieningen. Op basis van hun reactie wordt de verzamelde informatie aangescherpt. Het resultaat daarvan wordt voorgelegd aan de opdrachtgever, vervolgens in een definitieve versie toegestuurd aan de vertegenwoordigers van de voorzieningen en na akkoord opgenomen in de rapportage. Meestal heeft dit

[1] Deze toetst in bruikbaar voor een groot deel van de voorzieningen. Er zijn enkele uitzonderingen. Vaak betreft het ‘besloten’ voorzieningen die niet publiek via internet toegankelijk zijn.

proces meerdere iteraties nodig. Daar waar verschillen van mening zijn over het al dan niet voldoen aan de standaarden, zijn deze verschillen nader met elkaar besproken. In de gevallen waar de verschillen ook na de gesprekken bleven bestaan, is dit duidelijk opgenomen in de rapportage.

1.4 Aandachtspunten voor de lezer

1.4.1 Voorzieningen en standaarden geordend op basis van functionaliteit

De voorzieningen in deze monitor zijn op verzoek van de opdrachtgever op basis van functionaliteit gegroepeerd. De volgende functionele groepen worden in deze monitor onderscheiden:

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

Voor de volgorde van het overzicht van standaarden is de volgorde van de flyer[2] met standaarden van het Forum Standaardisatie aangehouden.

1.4.2 Status

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

- Ja: De voorziening is conform[3] de standaard,
- Nee: De voorziening is niet conform de standaard,
- Deels: Onderdelen van de voorziening zijn conform aan, maar niet alle onderdelen[4],
- Gepland: Er zijn concrete plannen (gekoppeld aan een datum) om de voorziening op korte termijn conform te maken aan de standaard.

1.4.3 Relevantie standaard

Voor de relevantiebepalingen zijn per standaard de beschrijvingen van het functioneel toepassingsgebied en van het organisatorisch toepassingsgebied, zoals vermeld op de pas-toe-of-leg-uit lijst van het Forum Standaardisatie gehanteerd.[5] 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.

---

[2] https://www.forumstandaardisatie.nl/sites/default/files/FS/2019/1211/Lijst-verplichte-open-standaarden-sept-2018-0.pdf

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

[4] 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.

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

1.4.4 Wijze van toetsen standaard

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

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

Gebruik van internet.nl
Voor een groot aantal standaarden hebben we gebruik gemaakt van de website internet.nl. De website is een initiatief van het Platform Internetstandaarden[6] en maakt het mogelijk om het gebruik van standaarden te toetsen op basis van een specifiek domein. Het betreft de volgende standaarden:

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

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

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

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

Er geldt een gefaseerde toepassing. Nieuwe websites gepubliceerd vanaf 23 september 2018 moesten uiterlijk op 23 september 2019 voldoen. Bestaande website gepubliceerd vóór 23 september 2018 moeten een jaar later voldoen. Mobiele applicaties moeten uiterlijk 23 juni 2021 voldoen.

Ten tijde van dit onderzoek wordt een nul-meting uitgevoerd naar het gebruik van de standaard Digitoegankelijk door overheden op basis van een Europees vastgestelde methodiek. Deze resultaten worden in de loop van 2019 verwacht en worden toegezonden aan de Tweede Kamer. In dat licht is in overleg met het Forum Standaardisatie en het Centrum voor Standaarden besloten de standaard niet nogmaals apart te onderzoeken voor deze monitor en wordt volstaan om hier te verwijzen naar de conclusies van dit rapport.

ISO 27001/2, BIR en BIO
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.
Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines informatieveiligheid voor Gemeenten, Rijk, Waterschappen en Provincies. Veel partijen zijn momenteel al bezig met de transitie naar de BIO. Hier is in de beoordeling rekening mee gehouden.

2. Identificeren en authenticeren

2.1 DigiD

Beheerorganisatie: Logius

Werking en inhoud van DigiD
Met hun persoonlijke DigiD kunnen burgers inloggen op websites van de overheid en van private organisaties met een publieke taak (zoals pensioenfondsen en zorgverzekeraars). Diensten die met DigiD geregeld kunnen worden zijn o.a. het doen van belastingaangifte, het regelen van toeslagen, het aanvragen van uitkeringen, het aanvragen van studiefinanciering, het inzien van het landelijk diplomaregister, het aanvragen van een omgevingsvergunning, het registreren van donorschap, het inzien van pensioenoverzichten en zorgverzekeringen en het aanvragen van het rijexamen.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	DigiD mail wordt verstuurd met een DKIM signature (zie: https://internet.nl/mail/digid.nl/).
DMARC (Anti-phishing)	Ja	DMARC is voor DigiD geconfigureerd als een van de Anti-phishing maatregelen. (zie https://internet.nl/mail/digid.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC is doorgevoerd in de domeinen (DNS-zones) van DigiD en operationeel. Ook de mailservers voldoen aan de standaard (zie: https://internet.nl/site/digid.nl/ en https://internet.nl/mail/digid.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	DigiD maakt gebruik van HTTPS voor de communicatie tussen clients (zoals browsers) en servers. Verder ondersteunt de DigiD website HSTS-policy met een geldigheidsduur van 1 jaar (zie: https://internet.nl/site/digid.nl/).
IPv4 en IPv6 (Internetnummers)	Ja	De website DigiD.nl is via IPv6 toegankelijk. Inmiddels verlopen ook de mailstromen via IPv6 (zie https://internet.nl/mail/digid.nl/ en https://internet.nl/site/digid.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Overheid (BIO) van toepassing die is gebaseerd op NEN-ISO27001/2. Logius heeft zich over toepassing van deze norm verantwoord door het afgeven van In Control Verklaringen (ICV's) aan de eigenaar (BZK/DGOBR).
SAML (Inloggegevens)	Ja	DigiD biedt aan afnemers een SAML-koppelvlak om authenticaties uit te kunnen voeren. Wanneer de afnemer “single sign on” wil gebruiken is dit alleen mogelijk via het SAML koppelvlak. De SAML koppelvlak specificaties van DigiD zijn gepubliceerd op de website van Logius, zie https://www.logius.nl/sites/default/files/public/bestanden/diensten/DigiD/Koppelvlakspecificatie-SAML-DigiD.pdf)

SPF (Preventie van mailspoofing/phishing)	Ja	SPF is relevant voor DigiD bij alle mails vanuit de DigiD applicatie, en DigiD voldoet ook aan deze standaard (zie https://internet.nl/mail/digid.nl/).
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Gepland	De mailserver van DigiD past STARTTLS/DANE toe (zie https://internet.nl/mail/digid.nl/). Er is nog een aandachtspunt voor de gebruikte ciphersuites, hiervoor is een wijziging onderweg die in Q3/4 2019 wordt doorgevoerd.
TLS (Beveiligde, versleutelde verbindingen)	Ja	DigiD ondersteunt voor de gebruikersdomeinen alleen TLS v1.2. Voor de afnemersdomeinen is een wijziging onderweg (Q3/4 2019) om TLS v1.0 ook uit te faseren, zodat ook alleen TLS v1.2 overblijft. De mailserver ondersteunt nog TLS v1.0 en v1.1; omdat deze ook voor andere voorzieningen gebruikt wordt, is de impact nog in onderzoek.

Ten opzichte van 2018 zijn er geen wijzingen in de statussen. Wel is de planning voor implementatie van STARTTLS/DANE verschoven.

Concluderend, moet DigiD nog enkele aandachtspunten oplossen om de volgende standaard (volledig) te implementeren: STARTTLS/DANE.

2.2 DigiD Machtigen

Beheerorganisatie: Logius

Werking en inhoud van DigiD Machtigen
DigiD Machtigen stelt burgers in staat anderen namens hen te machtigen om DigiD te gebruiken.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	Digid Machtigen ontvangt en verstuurd geen email op het domein machtigen.digid.nl. Er is een DMARC record (zie: https://internet.nl/mail/machtigen.digid.nl/)
DNSSEC (Beveiligde domeinnamen)	Ja	Het domein https://machtigen.digid.nl voldoet aan DNSSEC (zie: https://internet.nl/site/machtigen.digid.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	Deze standaarden zijn geïmplementeerd (zie: https://internet.nl/site/machtigen.digid.nl/).
IPv4 en IPV6 (Internetnummers)	Ja	Zowel IPv6 als IPv4 worden ondersteund (zie: https://internet.nl/site/machtigen.digid.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging)	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Rijk (BIR) van toepassing die is gebaseerd op NEN-ISO27001. Logius heeft zich over toepassing van de BIR norm verantwoord door het afgeven van In Control Verklaringen (ICV's) aan de eigenaar (BZK/DGOBR).

(Richtlijnen en principes informatiebeveiliging)		
SAML v2.0 (Inloggegevens)	Deels	Het authenticatie koppelvlak met eHerkenning voldoet aan de SAML standaard. Het authenticatie koppelvlak met DigiD maakt geen gebruik van SAML. Dit koppelvlak is door DigiD Machtigen gerealiseerd toen DigiD nog geen SAML koppelvlak bood. Overgang naar een SAML koppelvlak is voorzien bij de realisatie van de nieuwe website voor het DigiD Machtigen (publieke machtigingenregister), mogelijk al in het 4e kwartaal 2019. Naast authenticatie gebruikt DigiD Machtigen de SAML standaard ook om een getekend machtigingsbewijs af te geven, namelijk als een SAML assertion.
SPF (Preventie van mailspoofing/ phishing)	Ja	DigiD Machtigen verstuurd geen email aan gebruikers. Er is wel een SPF record aangemaakt voor het domein: machtigen.digid.nl welke aangeeft dat er vanaf dit domein geen email wordt verstuurd.
TLS (Beveiligde, versleutelde verbindingen)	Ja	TLS is geïmplementeerd. DigiD Machtigen ondersteunt TLS v1.0, TLS v1.1 en TLS v1.2. Voor brede comptabiliteit worden TLS 1.0 en 1.1 nog ondersteund.
		Document en (web/app)content
PDF/A en PDF 1.7 (Document-publicatie/ archivering)	Ja	De voorziening voldoet aan deze standaard.
		Overig
Digikoppeling 2.0	Deels	Recent ontwikkelde koppelvlakken en/of nieuwe versies van bestaande koppelvlakken zijn Digikoppeling compliant (bijvoorbeeld DVS 2017). Er zijn echter nog koppelvlakken waarvan geen Digikoppeling compliant versie is gemaakt en/of koppelvlakken waar nog diensten afnemers op aangesloten zitten (bijvoorbeeld PBS). Deze koppelvlakken bestaan uit de tijd dat de Digikoppeling standaard in ontwikkeling was en voldoen deels aan de uiteindelijk ontstane Digikoppeling standaard. Het is de bedoeling dat bestaande dienst afnemers overgaan naar de nieuwe koppelvlakken. Hier wordt niet actief op gestuurd. Door ontwikkelingen rondom eID, eIDAS en DigiD Machtigen moeten afnemers in de toekomst gebruik maken van andere koppelvlakken, waardoor gebruik van de niet compliant koppelvlakken zal afnemen. Bij nieuwe koppelvlakontwikkelingen zal meer naar de REST-API standaard worden gekeken dan naar Digikoppeling 2.0.

Ten opzichte van 2018 zijn er geen veranderingen.

Concluderend, moet DigiD Machtigen nog de volgende standaarden (volledig) implementeren: SAML en Digikoppeling 2.0.

2.3 PKIoverheid

Beheerorganisatie: Logius

Werking en inhoud van PKIoverheid
Met PKIoverheid wordt de betrouwbaarheid van informatie-uitwisseling via e-mail en websites op basis van Nederlandse (en Europese) wetgeving geborgd. Er zijn acht TSP's die PKIoverheidscertificaten verstrek- ken. Dit zijn: KPN, ESG, QuoVadis, Digidentity, Cleverbase, CIBG, het Ministerie van Infrastructuur en Waterstaat en het Ministerie van Defensie.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	Pkioverheid.nl voldoet aan DMARC.
DNSSEC (Beveiligde domeinnamen)	Ja	Het PKIoverheid-deel van de website van Logius en de website van PKIoverheid maken gebruik van DNSSEC (zie: https://internet.nl/domain/crl.pkioverheid.nl/ en https://internet.nl/domain/www.logius.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels	Deze standaard wordt toegepast door de voorziening (zie: https://internet.nl/domain/crl.pkioverheid.nl/ en https://internet.nl/domain/www.logius.nl/). Voor logius.nl, crl.pkioverheid.nl en cert.pkioverheid.nl is HTTPS goed geconfigureerd. pkioverheid.nl en www.pkioverheid.nl verwijzen door (oftewel 'redirecten') naar cert.overheid.nl. Alleen voor deze domeinen faalt de test op het punt "HTTPS-doorverwijzing".
IPv4 en IPV6 (Internetnummers)	Gepland	IPv6 is geïmplementeerd voor de informatiepagina's van PKIoverheid op de Logius website (zie: https://internet.nl/domain/www.logius.nl/). De PKIoverheid specifieke applicatiepagina's zijn op dit moment nog niet geschikt voor IPv6 (zie: https://internet.nl/domain/crl.pkioverheid.nl/). Dit was gepland voor Q4 2019. De implementatiedatum is gekoppeld aan gunning van een nieuw contract aan applicatieleverancier. Dit is uitgesteld naar Q1 2020.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Primair is het Webtrust normenkader van toepassing op PKIoverheid. Dit kader kent strengere eisen dan deze ISO standaarden vereisen. Implementatie van de BIR is daarnaast uitgevoerd op basis van best effort.
TLS	Ja	Het PKIoverheid deel van de website van Logius maakt gebruik van TLS 1.1 en 1.2 en de website van PKIoverheid zelf maakt gebruik van TLS 1.2 (zie: https://internet.nl/domain/crl.pkioverheid.nl/ en https://internet.nl/domain/www.logius.nl/).

		Document en (web/app)content
OWMS (Metadata overheidsinformatie)	Ja	Het PKIoverheid deel van de website van Logius voldoet aan de standaard, maar niet op de website van PKIoverheid (deze informatie is niet bedoeld voor hergebruik van overheidsinformatie).
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie /archivering)	Ja	Documenten die via de websites beschikbaar worden gesteld worden volgens PDF/A opgesteld.

Ten opzichte van 2018 gaat de status van HTTPS/HSTS van ja naar deels.

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

2.4 Beheervoorziening BSN en GBA-V

Beheerorganisatie: Rijksdienst voor Identiteitsgegevens (RvIG), Ministerie BZK

Werking en inhoud van BSN Beheervoorziening en GBA-V
De Beheervoorziening BSN (BV-BSN) is het geheel van voorzieningen dat zorgt voor het genereren, distribueren, beheren en raadplegen van het BSN. De GBA Verstrekkingsvoorziening (GBA-V) is de centrale component in het BRP-stelstel. Alle gegevens uit de gemeentelijke basisregistraties zijn ondergebracht in één 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 beheerder
		Internet en beveiliging
HTTPS/HSTS (Beveiligd, Versleuteld Webverkeer)	Ja	Alle aangeboden webservices draaien HTTPS en HSTS.
IPv4 en IPV6 (Bereikbaarheid nieuwe Internetnummers)	Nee	Het publiceren van de diensten op IPv6 wordt in 2020 op de backlog van infrastructuur wijzigingen gezet. Wanneer de diensten beschikbaar zijn op IPv6 is nog niet bekend. Er wordt al wel met de ODC leverancier gekeken hoe IPv6 publicatie van diensten zou moeten plaatsvinden.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De Rijksdienst voor Identiteitsgegevens heeft een beveiligingsplan op basis van de BIR. Hier worden externe audits op gedaan. Er is een In Control Verklaring (ICV) aanwezig.
TLS (Beveiligd Versleuteld emailverkeer)	Ja	De voorziening ondersteunt zowel TLS 1.2, 1.1 als 1.0.
		Stelstelstandaarden
Digikoppeling 2.0 (Veilige berichtuitwisseling)	Nee	Er zijn plannen om voor de BRP (basisregistratie personen) gebruik te gaan maken van Digikoppeling. Gezien het lopende

		BRP bezinningsproces is de planning onduidelijk. Ontsluiting van BV-BSN middels Digikoppeling zal niet plaatsvinden.
StUF (Uitwisseling administratieve overheidsgegevens)	Nee	De voorziening spreekt de WSI standaard XML/SOAP met haar gebruikers. Er is geen concrete planning voor de invoering van StUF.

Ten opzichte van 2018 zijn er geen veranderingen.

Concluderend moeten voor de beheervoorziening BSN en GBA-V nog de volgende standaarden (volledig) worden geïmplementeerd: IPv4 en IPV6, Digikoppeling 2.0, StUF.

2.5 Rijkspas

Beheerorganisatie: Ministerie van BZK

Werking en inhoud van Rijkspas
Rijkspas is de voorziening waarmee (een groot deel van) de rijksambtenaren toegang krijgt tot de gebouwen van de rijksoverheid. Het is een multifunctionele smartcard en onderdeel van een veilig en flexibel toegangsconcept voor fysieke toegang tot 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.

Het strategisch opdrachtgever- en eigenaarschap voor de Rijkspas is belegd bij DGOO/CIO Rijk/ICT Voorzieningen en Infrastructuur Rijk, die meer van dergelijke rijksbrede voorzieningen in het portfolio heeft. De tactische en operationele regie is in 2018 ondergebracht bij P-Direkt. SSC-ICT is in opdracht van CIO Rijk verantwoordelijk voor de housing en hosting van de Rijkspas Verkeershub en het Generiek Cardmanagement 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 beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Gepland	Voor Rijkspas worden mails verstuurd vanaf de applicatie voor Interdepartementale Toegang (IDT). In de huidige infrastructuur is dit niet toegepast. De eerdere planningen van Q3 2018 en Q4 2018 voor verhuizing van de Rijkspassystemen naar een nieuw datacenter waar DKIM wel toegepast zal worden zijn door SSC-ICT uitgesteld naar Q3 2019. De email server die gebruikt wordt is inmiddels wel verhuisd naar het ODC. Onderdeel van de totale applicatiemigratie (inclusief nieuwe email verzendadressen) is het mogelijk maken van DKIM.
DMARC (Anti-phishing)	Nee	P-direkt is afhankelijk van SSC-ICT voor implementatie van de standaard. De status hiervan is onbekend.
DNSSEC (Beveiligde domeinnamen)	Gepland	Rijkspas communiceert momenteel nog niet via het publieke internet. De verbinding die daarvoor voorzien is, maakt wel gebruik van DNSSEC. Voor communicatie binnen de Rijksoverheid wordt

		momenteel gebruik gemaakt van de Haagse Ring. Deze ondersteunt nog geen DNSSEC. De planning van 2017 is niet gehaald en is afhankelijk van de verhuizing naar het nieuwe data center. De verhuizing stond gepland voor Q1 2019 en staat nu gepland voor Q3 2019.
IPv4 en IPV6 (Internetnummers)	Nee	IPv4 wordt toegepast. De Haagse ring, waarover eigenlijk al het verkeer naar de Rijkspas voorzieningen loopt, ondersteunt geen IPv6. Deze dienst wordt door Logius geleverd, en is onderdeel van de 'connectiviteitsdiensten' waarvan I&I gebruik maakt.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De Rijkspas heeft een eigen normen- en beveiligingskader gebaseerd op ISO-9001 en 27001/2. Jaarlijks worden hier ook audits op gedaan, onder andere door de Audit Dienst Rijk.
SAML (Inloggegevens)	Ja	De Interdepartementale Toegang applicatie (IDT) is per 2015 aangesloten op de Single Sign On voorziening via SAML.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd.
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Nee	Rijkspas neemt email dienstverlening af van SSC-ICT, en vanuit deze leverancier is aangegeven dat nog niet alle randvoorwaarden in plaats zijn voor deze standaard. Eén van deze randvoorwaarden is DNSSEC, waarvan de implementatie afhankelijk is van de verhuizing naar het nieuwe data center. Na deze implementatie zal SSC-ICT opnieuw de mogelijkheden van STARTTLS en DANE analyseren.
TLS (Beveiligde, versleutelde verbindingen)	Ja	TLS wordt gebruikt voor het veilig ontsluiten van de website voor IdT.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Rijkspas maakt gebruik van het WUS-gedeelte van de Digikoppeling. De deelnemers kunnen zelf de keuze maken welk protocol ze hanteren, de standaard koppeling Rijkspas of de Digikoppeling.

Ten opzichte van 2018 is de planning voor implementatie van DKIM verplaatst van Q4 2018 naar Q3 2019 en de implementatie van DNSSEC is verplaatst van Q1 naar Q3 2019.

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

2.6 Stelsel elektronische toegangsdiensten

Beheerorganisatie: Logius

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

Het Afsprakenstelsel Elektronische Toegangsdiensten is een set van technische, functionele, juridische en organisatorische afspraken op basis waarvan het netwerk van 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 beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	Bij verstuurde email wordt DKIM toegepast, bij ontvangst gebeurd dit door de centrale email voorzieningen van Logius (SSC-ICT).
DMARC (Anti-phishing)	Gepland	Stelsel Elektronische toegangsdiensten voldoet aan DMARC, maar de policy is niet voor Q1 2019 aangescherpt. Er zijn nog enkele problemen waardoor het nog te vroeg is om van volledige implementatie te spreken. De planning is uiterlijk Q4 2019 volledig compliant te zijn. (Zie: https://internet.nl/mail/eherkenning.nl/ en https://internet.nl/mail/idensys.nl/)
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC werd in 2015 in de productieomgeving opgenomen.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	HTTPS en HSTS wordt toegepast op alle websites en webapplicaties onder beheer van de beheerorganisatie.
IPv4 en IPv6 (Internetnummers)	Deels	Niet alle voorzieningen voldoen aan IPv4 en IPv6. (Zie: https://internet.nl/mail/eherkenning.nl/ en https://internet.nl/mail/idensys.nl/). De webservers voldoen wel aan IPv6, maar niet alle mailservers voldoen. Voor onze inkomende mail zijn we als kleine voorziening van Logius afhankelijk van de dienstverlening van het Shared Service Centrum van het Rijk (SSC-ICT). We zijn als Logius wel in gesprek met SSC-ICT.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De BIR is van toepassing op Logius, in het stelsel wordt certificering tegen ISO27001 geëist voor de deelnemers. De beheerorganisatie zelf is als stelselbeheerder ook gecertificeerd volgens ISO 27001. Daarvoor is ook een in control statement beschikbaar.
SAML (Inloggegevens)	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.

(Preventie van mailspoofing/phishing)		
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	STARTTLS is geïmplementeerd voor eherkenning.nl en idensys.nl. DANE voor SMTP is voor de maildomeinen geïmplementeerd bij de KA-leverancier SSC-ICT.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Het afsprakenstelsel stelt het gebruik van TLS1.x verplicht.
		Document en (web/app)content
PDF 1.7, PDF/A-1 of PDF/A-2 (Documentpublicatie/ archivering)	Ja	Primair wordt de stelseldocumentatie via HTML op eherkenning.nl gepubliceerd. Stelseldocumentatie wordt met behulp van office software gepubliceerd in PDF/A-formaat. Overige documenten worden met een aparte tool in PDF/A formaat geconverteerd omdat het gehanteerde DMS dit niet ondersteunt.

Ten opzichte van 2018 is de geplande datum voor (volledige) implementatie van DMARC verschoven van Q1 2019 naar Q4 2019. Inmiddels voldoet de voorziening aan DANE, waardoor de status van STARTTLS en DANE van nee naar ja gaat. De status van IPv4 en IPv6 is veranderd van ja naar deels.

Concluderend moet stelsel elektronische toegangsdiensten nog de volgende standaarden (volledig) implementeren: DMARC, IPv4 en IPv6.

3. Dienstverlening en informatieverstrekken

3.1 MijnOverheid

Beheerorganisatie: Logius

Werking en inhoud van MijnOverheid
MijnOverheid is een persoonlijk toegangsportaal waarin verschillende diensten van de overheid ontsloten worden. MijnOverheid gaat over persoonlijke, en om die reden met DigiD beveiligde, diensten en informatie. Binnen MijnOverheid heeft de burger toegang tot de Berichtenbox, Lopende Zaken en Persoonlijke Gegevens. De Berichtenbox is de persoonlijke brievenbus waarin burgers post van onder meer de Belastingdienst, RDW, SVB, UWV, gemeenten en pensioenfondsen kunnen ontvangen. Lopende Zaken geeft weer wat de stand is van bijvoorbeeld aanvragen of vergunningen. Inzage Persoonlijke gegevens maakt het mogelijk om te controleren of de eigen gegevens correct zijn opgeslagen bij de overheid. Logius is verantwoordelijk voor het portaal, de aangesloten partijen zijn verantwoordelijk voor hun eigen dienstverlening die via MijnOverheid benaderd kan worden.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/ phishing)	Ja	MijnOverheid voldoet aan DKIM (zie: https://internet.nl/mail/mijnoverheid.nl/ En https://internet.nl/mail/mijn.overheid.nl/)
DMARC (Anti-phishing)	Ja	Deze standaard wordt toegepast.
DNSSEC (Beveiligde domeinnamen)	Ja	MijnOverheid voldoet aan DNSSEC (zie: https://internet.nl/site/mijnoverheid.nl/ en https://internet.nl/site/mijn.overheid.nl/)
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	Deze standaard wordt toegepast (zie: https://internet.nl/mail/mijnoverheid.nl/ en https://internet.nl/mail/mijn.overheid.nl/). HTTPS wordt toegepast voor zowel het domein mijn.overheid.nl, als mijnoverheid.nl. HSTS wordt toegepast voor het domein mijn.overheid.nl. HSTS voor mijnoverheid.nl is niet van toepassing, omdat die enkel redirect naar mijn.overheid.nl.
IPv4 en IPV6 (Internetnummers)	Deels	MijnOverheid gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik. MijnOverheid ondersteunt op dit moment IPv4 en IPv6. Mijn.overheid.nl voldoet aan de standaard. IPv6 staat niet op de inkomende mailservers er bestaat ook geen planning voor om dit wel te doen. Dit is ook minder urgent dan IPv6 op de website, waar we dit wel op ingeschakeld hebben.
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

(Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)		door het afgeven van In Control Verklaringen (ICV'en) aan de eigenaar (BZK/DGOBR). De ICV's zijn nog up-to-date.
SAML (Inloggegevens)	Ja	Authenticatie loopt via SAML.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is relevant en geïmplementeerd.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	Deze standaard wordt toegepast.
TLS (Beveiligde, versleutelde verbindingen)	Ja	In de dienstverlening aan burgers maakt MijnOverheid gebruik van een TLS 1.2-verbinding (Zie: https://internet.nl/site/mijn.overheid.nl). De koppelingen met afnemers (overheidsorganisaties) lopen ook via TLS op basis van PKIoverheid-certificaten.
		Document en (web/app)content
Open API Specification (Beschrijven van REST API's)	Ja	Deze standaard wordt gebruikt voor de REST-api's van MijnOverheid.
PDF 1.7, PDF/A-1 of PDF/A-2 (Documentpublicatie/ archivering)	Ja	MijnOverheid genereert zelf PDF-bestanden welke voldoen aan de PDF/A-1a standaard. MijnOverheid neemt concrete stappen om te gaan controleren op de toegankelijkheid en veiligheid van PDF-bestanden die aangeleverd worden door afnemers via de Berichtenbox.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Zowel nieuwe als oude koppelingen worden conform Digikoppeling 2.0 ingericht.
StUF (Uitwisseling administratieve overheidsgegevens)	Ja	MijnOverheid heeft waar relevant de koppeling op basis van StUF. Dit is alleen relevant voor WOZ en Lopende Zaken.

Ten opzichte van 2018 is de status van IPv4 en IPv6 van nee naar deels gegaan.

Concluderend, moet mijnOverheid nog de volgende standaarden (volledig) implementeren: IPv6.

3.2 Berichtenbox voor bedrijven

Beheerorganisatie: Rijksdienst voor Ondernemend Nederland (RVO).

Inhoud en werking Berichtenbox voor bedrijven
De Berichtenbox voor bedrijven is het beveiligde e-mailsysteem tussen ondernemers en de overheid. De Berichtenbox voor bedrijven is vergelijkbaar met de Berichtenbox voor burgers (zie MijnOverheid.nl), met als belangrijkste verschil dat de Berichtenbox voor bedrijven tweerichtingsverkeer tussen ondernemers en de overheid mogelijk maakt. Via de Berichtenbox wordt (bedrijfs)gevoelige informatie veilig uitgewisseld met overheden, bijvoorbeeld voor vergunningaanvragen aan gemeente of provincie, meldingen, inschrijvingen en registraties.

De Berichtenbox is speciaal gemaakt voor de Dienstenwet. Voor alle procedures die onder de Dienstenwet vallen, hebben ondernemers het recht om de Berichtenbox te gebruiken. Overheidsorganisaties zijn verplicht berichten via de Berichtenbox te beantwoorden.

BZK heeft het voornemen uitgesproken om de Berichtenbox voor bedrijven op termijn uit te faseren. Er dient dan wel een vervangend systeem te zijn voor berichtenverkeer naar ondernemingen én voor de loketfunctie in het kader van de Dienstenwet. Naar het zich nu laat aanzien, zal uitfasering eind 2022 zijn.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Nee	DKIM is niet geïmplementeerd (zie: https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/).
DMARC (Anti-phishing)	Nee	De BerichtenBox voor Bedrijven voldoet niet aan DMARC. Deze standaard is mede afhankelijk van SPF en DKIM, welke niet ondersteund worden door de BerichtenBox voor Bedrijven.
DNSSEC (Beveiligde domeinnamen)	Ja	Volgens internet.nl voldoet het domein berichtenbox.antwoordvoorbedrijven.nl (zie: https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	HTTPS en HSTS zijn geïmplementeerd (zie: https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/).
IPv4 en IPv6 (Internetnummers)	Nee	De website van de Berichtenbox ondersteunt IPv4 maar is volgens internet.nl niet toegankelijk via IPv6 (zie https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/). De Berichtenbox is wel IPv6 ready, maar nog niet de hele keten. E-ovb (beheerder van de Berichtenbox) is daarbij ook afhankelijk van leveranciers die hun IPv6 implementatie nog niet op orde hebben. De implementatie moet DICTU-breed gebeuren voordat dit voor de Berichtenbox gedaan zal worden. Een datum voor de implementatie is zowel in 2018 als in 2019 niet bekend.
SAML (Inloggegevens)	Ja	eHerkenning is SAML-based en wordt toegepast voor het inloggen op de Berichtenbox.
SPF	Nee	SPF is niet geïmplementeerd (zie https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/).

(Preventie van mailspoofing/phishing)		
TLS (Beveiligde, versleutelde verbindingen)	Nee	De Berichtenbox maakt gebruik van TLS 1.2 (zie: https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/). Maar de webserver staat client-initiated renegotiation toe, wat niet veilig is.
		Document en (web/app)content
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/ archivering)	Ja	Alle berichten kunnen worden gedownload (vanaf de Berichtenbox website) in PDF/A formaat. PDF-documenten worden gegenereerd in PDF A/1.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Overheden kunnen via Digikoppeling geautomatiseerd berichten verzenden en ontvangen. Ondernemers kunnen alleen handmatig (via de website) hun Berichtenbox gegevens opvragen.
STuF (Uitwisseling administratieve overheidsgegevens)	Ja	STuF wordt in combinatie met Digikoppeling gebruikt voor de uitwisseling met alle partijen die via digikoppeling op de berichtenbox zijn aangesloten.

Ten opzichte van 2018 voldoet de voorziening niet meer aan TLS, de status gaat van ja naar nee.

Concluderend moeten voor Berichtenbox voor bedrijven nog de volgende standaarden (volledig) worden geïmplementeerd: DKIM, DMARC, IPv4 en IPv6, SPF, TLS.

3.3 Overheid.nl

Beheerorganisatie: Kennis- en Exploitatiecentrum Officiële Overheidspublicaties (KOOP)

Werking en inhoud van Overheid.nl

De website Overheid.nl biedt centrale internettoegang voor informatie en diensten van de Nederlandse overheid. Overheid.nl is bestemd voor burgers, bedrijven en ondernemers en andere overheden. Overheid.nl bevat naast informatie en diensten ook de contactgegevens van Nederlandse overheidsorganisaties. Ook het domein wetten.overheid.nl valt onder deze voorziening.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	DKIM is geïmplementeerd (zie https://internet.nl/mail/overheid.nl/).
DMARC (Anti-phishing)	Ja	DMARC wordt toegepast op overheid.nl (Zie: https://internet.nl/mail/overheid.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	Overheid.nl voldoet sinds Q2 2015 aan DNSSEC (zie: https://internet.nl/site/www.overheid.nl/).

HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Gepland	HTTPS en HSTS zijn doorgevoerd op overheid.nl (zie https://internet.nl/site/www.overheid.nl/). Op een aantal sub-domeinen is HTTPS wel ingesteld, maar de configuratie voor HSTS-policy nog niet helemaal correct. Dit wordt in de zomer van 2019 hersteld.
IPv4 en IPV6 (Internetnummers)	Ja	Er wordt voldaan aan IPv4 en IPv6 (zie: https://internet.nl/domain/www.overheid.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Vanaf 2015 staat overheid.nl niet meer op de risicokaart van BZK en hoeft hiervoor geen ICV (In Control Verklaring) meer te worden afgegeven. Voor OEB, de applicatie die centraal staat in het publiceren van overheidsinformatie en richtinggevend is voor alle KOOP-dienstverlening, wordt wel jaarlijks een ICV afgegeven; deze is gebaseerd op de BIR die weer is gebaseerd op NEN-ISO/IEC 27001/27002. Alle dienstverlening van KOOP is ondergebracht bij een hostingpartij die jaarlijks een ISAE3402 Type II verklaring laat opstellen; deze verklaring baseert zich mede op de certificering met NEN-ISO/IEC 27001/27002.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	STARTTLS en DANE zijn geheel geïmplementeerd (zie: https://internet.nl/mail/overheid.nl/).
TLS (Beveiligde, versleutelde verbindingen)	Gepland	Deze standaard is doorgevoerd op overheid.nl (zie: https://internet.nl/site/www.overheid.nl/). Op een aantal sub-domeinen is TLS wel ingesteld, maar de configuratie voor client initiated renegotiation nog niet helemaal correct. Dit wordt in de zomer van 2019 hersteld.
		Document en (web/app)content
OWMS (Metadata overheidsinformatie)	Ja	Overheid.nl is gemetadateerd conform OWMS.
PDF 1.7 PDF/A-1 PDF/A-2 (Documentpublicatie/ archivering)	Ja	Alle PDF's van officiële bekendmakingen zijn PDF/A-1a zoals wettelijk bepaald is.
SKOS (Thesauri en begrippenwoordenboeken)	Ja	SKOS is geïmplementeerd voor de waardelijsten van OWMS.
		Juridische identificatie en verwijzing
BWB (Wet- en regelgeving)	Ja	Overheid.nl is zelfs de bron van de BWB identificatie. Zie wetten.overheid.nl.
JCDR (Decentrale regelgeving)	Ja	Overheid.nl is zelfs de bron van de JCDR identifiers (zie: https://zoek.overheid.nl/lokale_wet_en_regelgeving).

Ten opzichte van 2018 zijn er geen veranderingen in de statussen van de relevante standaarden. De planningen voor implementatie van HSTS en TLS zijn verschoven.

Concluderend, moet overheid.nl op een aantal subdomeinen nog de volgende standaarden (volledig) implementeren: HSTS en TLS.

3.4 Ondernemersplein

Beheerorganisatie: Kamer van Koophandel

Werking en inhoud van Ondernemersplein
Het Ondernemersplein is de centrale plek (website) waar overheden gezamenlijke informatie en hulpmiddelen aanbieden voor ondernemers, variërend van praktische stappenplannen en webinars tot informatie over regelgeving en geldzaken. Daarnaast bestaat de mogelijkheid voor overheden de content van Ondernemersplein via hun eigen kanalen te ontsluiten. Sinds dit jaar is ondernemersplein.kvk.nl nieuw, ondernemersplein.nl verwijst vanaf dit jaar door naar ondernemersplein.kvk.nl.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Deels	DKIM is geïmplementeerd voor de domeinen kvk.nl en ondernemersplein.nl (zie: https://internet.nl/mail/kvk.nl/249076/, https://internet.nl/mail/ondernemersplein.nl/) maar niet voor het domein ondernemersplein.kvk.nl (zie: https://internet.nl/mail/ondernemersplein.kvk.nl/246411/).
DMARC (Anti-phishing)	Ja	Ondernemersplein voldoet aan DMARC (zie: https://internet.nl/mail/ondernemersplein.nl/, https://internet.nl/mail/kvk.nl/249076/, https://internet.nl/mail/ondernemersplein.kvk.nl/246411/).
DNSSEC (Beveiligde domeinnamen)	Deels	De standaard is geïmplementeerd op de nieuwe DNS omgeving voor de webdomeinen en voor het maildomein ondernemersplein.kvk.nl. Voor de mailserverdomeinen kvk.nl en ondernemersplein.nl geldt dat DNSSEC niet is geïmplementeerd (zie: https://internet.nl/mail/kvk.nl/249076/# en https://internet.nl/mail/ondernemersplein.nl/249075/#). Ondernemersplein maakt geen gebruik van ondernemersplein.kvk.nl als mail adres. Alle mailadressen die worden gebruikt zijn @ondernemersplein.nl of @kvk.nl, waar DMARC, DKIM, SPF en STARTTTLS wel geïmplementeerd zijn. Desondanks is het verzoek wel neergelegd bij IT beheer om dit op te lossen. Naar verwachting gebeurt dit niet op korte termijn.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels	Aan deze standaard wordt voldaan voor het domein ondernemersplein.nl (zie: https://internet.nl/site/www.ondernemersplein.nl/), maar voor het domein ondernemersplein.kvk.nl geldt dat HSTS niet is geïmplementeerd (zie: https://internet.nl/site/ondernemersplein.kvk.nl/577753/#). – De HSTS Policy komt naar verwachting eind november 2019 live.
IPv4 en IPV6 (Internetnummers)	Deels	De website ondersteunt IPv4 en is toegankelijk via IPv6 (zie: https://internet.nl/site/www.ondernemersplein.nl/ en

		https://internet.nl/site/ondernemersplein.kvk.nl/577753/#). Voor het maildomein ondernemersplein.nl en kvk.nl is IPv6 niet geïmplementeerd (zie: https://internet.nl/mail/ondernemersplein.nl/249075/# en https://internet.nl/mail/kvk.nl/249076/). Implementatie van IPv6 voor de mailservers is niet mogelijk.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Ondernemersplein is gehost bij de Kamer van Koophandel. Daar liep een ISO 27001 certificeringstraject en Ondernemersplein heeft dit inmiddels toegepast en is door een audit in april 2016 gecertificeerd hierop. Toetsing vond plaats in februari 2019 met goed resultaat.
SPF (Preventie van mailspoofing/phishing)	Deels	Er wordt aan deze standaard voldaan op de domeinen kvk.nl en ondernemersplein.nl (zie: https://internet.nl/mail/kvk.nl/249076/# en https://internet.nl/mail/ondernemersplein.nl/). SPF is niet geïmplementeerd voor het domein ondernemersplein.kvk.nl (zie: https://internet.nl/mail/ondernemersplein.kvk.nl/246411/#)
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Nee	Aan STARTTLS wordt voldaan, maar aan DANE wordt nog niet voldaan. De KvK geeft zowel in 2018 als in 2019 aan nog te moeten onderzoeken of hieraan voldaan zal worden. Er is nog geen concreet onderzoekstraject gedefinieerd.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Er is een migratie uitgevoerd naar TLS 1.2 en op verzoek van de product owner wordt TLS 1.0 nog ondersteund.
		Document en (web/app)content
CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)	Nee	De tooling (CMS/ESB) ondersteunt de standaard wel, maar deze wordt niet actief gebruikt. Er zijn geen content leveranciers die hun CMS in CMIS vorm aan het Ondernemersplein.nl beschikbaar stellen. Concreet is er dus nog geen toepassing op dit moment en er zijn ook nog geen plannen om dit te doen.
OWMS (Metadata overheidsinformatie)	Nee	De informatie op de website is gemetadateerd volgens een eigen model die past bij de metadatering van de partners.
		Juridische identificatie en verwijzing
BWB (Wet- en regelgeving)	Ja	Binnen de website, de content van AvB, wordt verwezen naar wetgeving conform de BWB standaard.

Ten opzichte van 2018 is naast ondernemersplein.kvk.nl gekeken naar de domeinen ondernemersplein.nl en kvk.nl, omdat daarvandaan wordt gemaild. De status van de standaarden DKIM, HTTPS/HSTS en SPF is daarmee van ja naar deels gegaan, omdat niet alle domeinen voldoen. De status van de standaarden DNSSEC en IPv4 en IPv6 is van ja naar deels gegaan.

Concluderend moeten voor de voorziening ondernemersplein nog de volgende standaarden (volledig) worden geïmplementeerd: DKIM, DNSSEC, HTTPS/HSTS, IPv4 en IPV6, SPF, STARTTLS/DANE, CMIS, OWMS.

3.5 Samenwerkende catalogi

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DMARC (Anti-phishing)	Gepland	Samenwerkende Catalogi wordt beheerd door Logius waarmee DMARC valt onder het organisatorisch werkingsgebied. De validator is benaderbaar via een subdomein van Logius (scvalidator.logius.nl) waarvoor geldt dat dit een overheidsdomein is waarvandaan niet wordt gemaild. Daarmee valt dit onder het functioneel toepassingsgebied. Het DMARC-compliant maken van de validator stond gepland voor 2018. De validator van Samenwerkende Catalogi is in de tweede helft van juli 2019 gemigreerd naar een ander platform. Op dit moment worden alle relevante standaarden geïmplementeerd: HTTPS en HSTS, SPF, DMARC, TLS. Verwachting is dat dit Q3 2019 gereed is.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Gepland	De validator van Samenwerkende Catalogi is in de tweede helft van juli 2019 gemigreerd naar een ander platform. Op dit moment worden alle relevante standaarden geïmplementeerd: HTTPS en HSTS, SPF, DMARC, TLS. Verwachting is dat dit Q3 2019 gereed is.
IPv4 en IPv6 (Adressering van ICT-systemen binnen een netwerk)	Ja	Zowel de informatieve pagina's op logius.nl als de validator zelf zijn voorzien van IPV4 en IPV6 adressen. Dit na een migratie van beide omgevingen.
SPF (Preventie van mailspoofing/phishing)	Gepland	De validator van Samenwerkende Catalogi is in de tweede helft van juli 2019 gemigreerd naar een ander platform. Op dit moment worden alle relevante standaarden geïmplementeerd: HTTPS en HSTS, SPF, DMARC, TLS. Verwachting is dat dit Q3 2019 gereed is.
TLS (Beveiligde, versleutelde verbindingen)	Gepland	De validator van Samenwerkende Catalogi is in de tweede helft van juli 2019 gemigreerd naar een ander platform. Op dit moment worden alle relevante standaarden geïmplementeerd: HTTPS en HSTS, SPF, DMARC, TLS. Verwachting is dat dit Q3 2019 gereed is.
		Document en (web/app)content
Open Api Specification	Ja	Samenwerkende catalogi voldoet aan deze standaard.

(Beschrijven van REST API's)		
OWMS (Metadata overheidsinformatie)	Ja	Samenwerkende catalogi is volledig gebaseerd op OWMS.

Ten opzichte van 2018 voldoet Samenwerkende catalogi aan de standaard Open Api Specification en is het (volledig) implementeren van DMARC uitgesteld van 2018 naar Q3 2019. Ten opzichte van vorig jaar zijn verder de standaarden HTTPS en HSTS, IPv4 en IPv6, SPF en TLS toegevoegd.

Concluderend moet Samenwerkende catalogi nog de volgende standaarden (volledig) implementeren: DMARC, HTTPS en HSTS, SPF en TLS.

3.6 Rijksportaal

Beheer organisatie: SSC-ICT

Werking en inhoud van Rijksportaal
Het Rijksportaal is het (Rijksbrede) raamwerk voor intranettoepassing voor alle (kern)departementen en verschillende uitvoeringsinstanties. Hiermee is het merendeel van de oorspronkelijke intranetten van de(kern)departementen vervangen. Het Rijksportaal geeft de rijksambtenaar toegang tot Rijksbrede en departementspecifieke 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 beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/ phishing)	Nee	Onderbouwing beheerder ontbreekt.
DMARC (Anti-phishing)	Ja	Er wordt in enkele situaties gebruik gemaakt van email. Bijvoorbeeld om te reageren naar een redactie. Hierbij wordt gebruik gemaakt van de generieke e-mailvoorziening van SSC-ICT, die de DMARC standaard ondersteunt.
DNSSEC (Beveiligde domeinnamen)	Nee	Bij transitie Rijksportaal wordt deze bouwsteen opnieuw ingebracht.
IPv6 en IPv4 (Internet-nummers)	Nee	Het huidige Rijksportaal (versie 1.6.5) is alleen ingericht voor IPv4. Om performanceredenen wordt IPv6 momenteel nog niet toegepast. Als gevolg van de transitie naar het overheidsdatacenter (ODC), het beëindigen van de realisatie van release 1.7 en een lopende verkenning op een nieuwe omgeving is er zowel in 2018 als in 2019 geen doorontwikkeling t.a.v. nieuwe functionaliteit voor het Rijksportaal.

SAML (Inloggegevens)	Ja	Eind februari 2019 is de dienst SAML SSO voor Rijksportaal officieel door SSC-ICT opgeleverd en in beheer genomen. Begin december 2018 is de SAML-acceptatie omgeving opgeleverd. In december 2018 en begin januari 2019 is er getest door de kerndepartementen. Daarnaast is een pilot gedraaid met EZK/LNV. Inmiddels gebruiken EZK, LNV, Tweede Kamer, AZ en de belastingdienst deze manier van authenticatie voor het Rijksportaal.
SPF (Preventie van mailspoofing/phishing)	Nee	SPF is minder relevant voor deze oplossing. Echter, het gebruik van DKIM/DMARC (want maillinks) en het gebruik van mailservers laat onverlet dat SPF ook een (mogelijk) te gebruiken standaard dient te zijn.
		Document en (web/app)content
ODF (Document-bewerkingen)	Ja	ODF wordt ondersteund: ODF-bestanden kunnen geüpload en gedownload worden en de inhoud van ODF-bestanden kan door de zoekmachine worden geïndexeerd. Naast ODF worden op het Rijksportaal ook andere documentformaten gebruikt; het gebruik van ODF wordt niet afgedwongen.
PDF 1.7 PDF/A-1, PDF/A-2 (Documentpublicatie/ archivering)	Ja	PDF wordt ondersteund: PDF-bestanden kunnen geüpload en gedownload worden en de inhoud van PDF-bestanden kan door de zoekmachine worden geïndexeerd. Naast PDF 1.7, PDF/A-1 en PDF/A-2 worden op het Rijksportaal ook andere PDF-versies gebruikt; het gebruik van PDF 1.7, PDF/A-1 en PDF/A-2 wordt niet afgedwongen.

Ten opzichte van vorig jaar voldoet Rijksportaal aan SAML, waarmee de status van nee naar ja is gegaan. Ten opzichte van vorig jaar zijn verder de standaarden DKIM, DNSSEC en SPF opgenomen als relevant.

Concluderend moet voor Rijksportaal nog de volgende standaard (volledig) worden geïmplementeerd: DKIM, DNSSEC, IPv6, SPF.

3.7 ODC Noord

Beheerorganisatie: Dienst Uitvoering Onderwijs (DUO)

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

ODC-Noord maakt enerzijds gebruik van de DUO mailomgeving (odc-noord.nl en sso-noord.nl) en anderzijds van een eigen mailomgeving (rijkscloud.nl)

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM	Ja	DKIM is voor odc-noord.nl, sso-noord.nl en rijkscloud.nl geïmplementeerd voor ODC-Noord.

(Preventie van mailspoofing/phishing)		
DMARC (Anti-phishing)	Ja	DMARC is voor de betreffende domeinen geïmplementeerd. https://internet.nl/mail/odc-noord.nl/247561/#; https://internet.nl/mail/sso-noord.nl/247564/#control-panel-9
DNSSEC (Beveiligde domeinnamen)	Ja	ODC-Noord heeft sinds het onderzoek uit 2015 een eigen DNS ingericht, die DNSSEC gebruikt.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels	De cloud dashboards zijn allemaal uitsluitend via HTTPS benaderbaar, een aantal websites draaien op HSTS. Alle sites, met uitzondering van sso-noord.nl zijn voorzien van een SSL-certificaat. Het domein sso-noord.nl wordt voor 1 januari 2020 opgeheven. https://internet.nl/site/odc-noord.nl/574389/#control-panel-21; https://internet.nl/site/sso-noord.nl/574393/#control-panel-11 https://internet.nl/site/rijkscloud.nl/574696/#sitetls.
IPv6 en IPv4 (Internetnummers)	Gepland	Intern wordt IPv6 gebruikt op een specifiek netwerk. Nog niet alle benodigde producten worden met IPv6 aangeboden. Zodra de markt alles op het juiste niveau kan aanbieden zal dit geïmplementeerd worden en zullen de systemen die vanaf het internet benaderbaar zijn, ook worden ontsloten via IPv6. Planning is eind 2019 geïmplementeerd. https://internet.nl/site/odc-noord.nl/574389/#control-panel-21; https://internet.nl/site/rijkscloud.nl/574392/#control-panel-21; https://internet.nl/site/sso-noord.nl/574393/#control-panel-11; Nb. De mailomgeving van DUO waarop odc-noord.nl en sso-noord wordt gehost is daarentegen wel via IPv6 bereikbaar. https://internet.nl/mail/rijkscloud.nl/247562/#control-panel-16 Zodra ipv6 beschikbaar komt in Openstack kan rijkscloud.nl domein via ipv6 mail ontvangen en versturen.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Op 15 februari 2019 is door ODC-Noord een BIR in Control Verklaring voor 2018 afgegeven, ondersteund door een Assurance verklaring van de ADR. De onderliggende leveranciers voldoen aan de ISO. ODC-Noord voldoet aan de BIR.
SAML (Inloggegevens)	Gepland	ODC-Noord maakt voor het interne systeem geen gebruik van SAML. Bij het ontwikkelen van diensten ten bate van klanten (SaaS) wordt SAML onderzocht en waar mogelijk toegepast. Eerder stond SAML federatie, wat onderdeel uitmaakt van de multifactor implementatie voor de SAAS dienstverlening van ODC-Noord, op de roadmap voor eind 2018. SAML is doorgeschoven naar 2019 en wordt na de zomervakantie opgepakt. De PoC welke eerder dit jaar heeft plaatsgevonden, heeft uitgewezen dat de oplossing gaat werken.
SPF (Bescherming tegen e-mailphishing)	Ja	SPF is geïmplementeerd voor alle drie de domeinen.
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Nee	STARTTLS/DANE is voor de mailomgeving rijkscloud.nl onvoldoende veilig geïmplementeerd (niet conform de NCSC richtlijnen). De mailomgeving van DUO, waarop odc-noord.nl

		en sso-noord.nl worden gehost, is STARTTLS ingericht, maar DANE niet. https://internet.nl/mail/odc-noord.nl/247561/#; https://internet.nl/mail/rijkscloud.nl/247562/#control-panel-16; https://internet.nl/mail/sso-noord.nl/247564/#control-panel-9
TLS (Beveiligde, versleutelde verbindingen)	Deels	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. https://internet.nl/site/sso-noord.nl/574393/#control-panel-11; sso-noord.nl voldoet niet aan de standaard. Het domein sso-noord.nl wordt voor 1 januari 2020 opgeheven.
WPA2 Enterprise (Toegang tot een WiFi-netwerk met account)	Ja	Deze standaard is toegepast waar ODC-Noord wifi gebruikt.
		Document en (web/app)content
OWMS (Metadata overheidsinformatie)	Gepland	Oorspronkelijk stond de implementatie van OWMS gepland voor Q4 2018. De website van ODC-Noord is in een eerste fase herbouwd, maar nog niet op het gewenste platform. Begin september start hiervoor de tweede fase waarbij naast de webrichtlijnen ook aan OWMS standaard zal worden voldaan. Volledige implementatie is gepland voor Q4 2019.
PDF 1.7, PDF A/1, PDF A/2 (Document-publicatie/ archivering)	Deels	V.w.b. uitwisseling van (definitieve) documenten met externe partijen wordt gebruik gemaakt van PDF. PDFCreator van Windows wordt als printoptie in de kantoorautomatiseringsomgeving aangeboden. De standaardinstelling is PDF versie 1.4, optioneel is 1.5. Vooralsnog wordt er bij DUO nog voor gekozen om de gratis variant van PDF-creator beschikbaar te stellen. Deze biedt maximaal PDF 1.5. Gebruikers van LibreOffice (dat is het meest gebruikte Office-pakket binnen de operationele omgeving van ODC-Noord) kunnen documenten exporteren naar PDF/A-1. Op dit moment is dat nog geen standaard werkwijze. PDF/A is beschikbaar en wordt gebruikt voor formele documenten

Ten opzichte van 2018 voldoet ODC Noord aan DMARC en SPF. In 2018 voldeed ODC Noord aan HTTPS/HSTS, in 2019 voldoet de voorziening nog deels. De status van STARTTLS/DANE gaat van gepland naar nee. IPv4 en IPv6 was deels wordt gepland. TLS was gepland en wordt deels. ODF is niet meer relevant. De planningen voor implementatie van SAML en OWMS zijn verschoven.

Concluderend, moet ODC Noord nog de volgende standaarden (volledig) implementeren: HTTPS en HSTS, IPv6 en IPv4, SAML, STARTTLS/DANE, OWMS, PDF 1.7, PDF A/1, PDF A/2 en TLS.

3.8 Doc-Direkt

Beheerorganisatie: Doc-Direkt

Werking en inhoud van 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 beheerder

		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	Volgens SSC-ICT maakt Doc-Direkt gebruik van de mailservers van SSC-ICT, deze zijn onderdeel van het BZK domein, waarvoor DKIM actief is.
DMARC (Anti-phishing)	Ja	Doc-Direkt voldoet aan DMARC.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels	De standaard wordt toegepast. De laatste open realisatie is de website www.handelingenbank.nl. De certificaat aanvraag loopt en realisatie in 4e kwartaal 2018 is niet gehaald. Nieuwe planning voor implementatie is 4e kwartaal 2019.
IPv4 en IPv6 (Internetnummers)	Ja	Doc-Direkt voldoet aan IPv4 en IPv6.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Voor de informatiesystemen waarvan Doc-Direkt eigenaar is, is in 2016 een 'in controle verklaring' opgesteld. Op de punten waar Doc-Direkt afwijkt is een uitleg gegeven (explains) en er is een verbeterplan opgesteld. Verbeteringen worden inmiddels uitgevoerd.
SAML (Inloggegevens)	Ja	Via de werkplek DWR kunnen medewerkers via SSO inloggen op de door Doc-Direkt beheerde DMS applicatie.
SPF (Preventie van mailspoofing/phishing)	Ja	Ook SPF wordt inmiddels toegepast.
TLS (Beveiligde, versleutelde verbindingen)	Nee	TLS v 1.2 is van toepassing en behoort tot de dienstverlening van SSC-ICT. Er wordt gewerkt aan TLS 1.3.
		Document en (web/app)content
Ades Baseline Profiles (Digitaal ondertekenen van documenten)	Nee	Er wordt op dit moment een productiepilot gedraaid. Het is een gezamenlijk dienst van Doc-Direkt en SSC-ICT. De verwachting is dat we in 2020 deze dienst in onze PDC kunnen opnemen.
CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)	Nee	De mogelijkheid en noodzakelijkheid van het toepassen van deze standaard werd in 2016 nader onderzocht, maar dit heeft nog niet tot een besluit geleid. Er zijn in 2018 proof of concepts uitgevoerd.
ODF (Documentbewerkingen)	Nee	Voor bewerkbare documenten wordt alleen .doc-formaat gebruikt. Er zijn geen plannen ODF te gebruiken.
PDF 1.7 – PDF A/1 of PDF A/2 (Documentpublicatie/ archivering)	Ja	Doc-Direkt ondersteunt in haar archieven vooral PDF/A. Alles wat gescand wordt gaat naar PDF/A. Daarnaast wordt ook 1.7 veel gebruikt.
SKOS (Thesauri en begrippen-woordenboeken)	Nee	SKOS wordt op dit moment niet toegepast. Er waren in 2018 en er zijn in 2019 nog geen plannen bekend of en wanneer SKOS geïmplementeerd zal worden.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Nee	Sinds 2018 wordt door SSC-ICT gewerkt aan operationalisering van Digikoppeling voor het gebruik binnen de dienstverlening van Doc-Direkt.

Ten opzichte van 2018 is de planning voor implementatie van HTTPS en HSTS verschoven van 4e kwartaal 2018 naar 4e kwartaal 2019. Voor TLS is geen concrete planning afgegeven.

Concluderend moeten voor Doc-Direkt nog de volgende standaarden (volledig) worden geïmplementeerd: HTTPS/HSTS, TLS, Ades Baseline Profiles, CMIS, ODF, SKOS, Digikoppeling 2.0.

3.9 Rijksoverheid.nl

Beheerorganisatie: Ministerie van AZ (DPC)

Werking en inhoud van rijksoverheid.nl
De website Rijksoverheid.nl is de publiekswebsite met informatie van en over alle ministeries. De website wordt verzorgd door de Dienst Publiek en Communicatie (DPC). DPC is een baten-lastendienst van het ministerie van AZ en biedt shared servicediensten aan de rijksoverheid op het gebied van Communicatie. Het e-mail domein @rijksoverheid.nl is in beheer bij SSC-ICT van het ministerie van BZK. Het is niet helder wie zich verantwoordelijk voelt voor het emaildomein. Van het webdomein is AZ eigenaar en beheerder.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/ phishing)	Ja	DKIM is geïmplementeerd.
DMARC (Anti-phishing)	Nee	DMARC is geïmplementeerd maar de policy is onvoldoende strikt (zie: https://internet.nl/mail/rijksoverheid.nl/249091/#). SSC-ICT beheert technisch het maildomein en het aanzetten van de dmarc policy op quarantaine of reject is voor de SSC-ICT geen probleem. Het gevolg van het aanzetten van de stricte dmarc policy is dat partijen die mail mogen versturen als rijksoverheid.nl worden aangemerkt als SPAM. Dit komt omdat de echtheidskenmerken die de partijen toepassen niet overeenkomen met de echtheidskenmerken die SSC-ICT toepast op rijksoverheid.nl. Om er voor te zorgen dat de partijen mail kunnen versturen als rijksoverheid.nl zijn er meerdere oplossingen. In overleg met de eigenaar van het maildomein moet dan bepaald worden welke partijen gebruikt mogen maken van rijksoverheid.nl en welke niet.
DNSSEC (Beveiligde domeinnamen)	Ja	Rijksoverheid.nl is ondertekend met DNSSEC (zie: https://internet.nl/site/www.rijksoverheid.nl/). DPC biedt DNSSEC ook aan al haar klanten die domeinen via haar registrar-functie afnemen.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening voldoet aan deze standaard (zie: https://internet.nl/site/www.rijksoverheid.nl/).
IPv4 en IPV6 (Internetnummers)	Deels	De website rijksoverheid.nl ondersteunt zowel IPv6 als IPv4 (zie: https://internet.nl/site/www.rijksoverheid.nl/). IPv6 is niet voor (alle) mailservers geïmplementeerd (zie: https://internet.nl/mail/rijksoverheid.nl/249091/#). Het technisch beheer van een aantal maildomeinen wordt uitgevoerd door SSC-ICT. De internet facing kant van de DMZ gaat IPv6 eind 2019 ondersteunen.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De leveranciers hebben een NEN 27001/2 implementatie waarin de beveiliging van rijksoverheid.nl meegaat. DPC zelf valt onder de VIR/BIO-implementatie van het moederdepartement AZ. SSC-ICT werkt via deze standaard en wordt hier ook op geaudit. De laatste audit heeft plaatsgevonden in 2019.

SPF (Preventie van mailspoofing/phishing)	Ja	Het e-maildomein @rijksoverheid.nl is integraal van SPF voorzien (zie: https://internet.nl/mail/rijksoverheid.nl/). Vanwege ontbreken van een aanspreekpunt van het maildomein, heeft geen verdere afstemming plaats gevonden met een beheerder na toetsing van de standaard. Deze statustoekenning is van PBLQ en is niet gevalideerd.
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Ja	Verzendende mailservers die STARTTLS ondersteunen, kunnen met ontvangende mailserver(s) een beveiligde verbinding opzetten. Rijksoverheid.nl voldoet aan DANE (zie: https://internet.nl/mail/rijksoverheid.nl/). Vanwege ontbreken van een aanspreekpunt van het maildomein, heeft geen verdere afstemming plaats gevonden met een beheerder na toetsing van de standaard. Deze statustoekenning is van PBLQ en is niet gevalideerd.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Rijksoverheid.nl is onderdeel van het Platform Rijksoverheid Online en geheel voorzien van https door middel van QWAC PKIo EV certificaten (zie: https://internet.nl/site/www.rijksoverheid.nl/).
		Document en (web/app)content
ODF 1.2 (Documentbewerkingen)	Ja	Het CMS van het Platform Rijksoverheid Online accepteert slechts ODF (open standaard) formaten. Er zijn wel 'legacy'-bestanden in alleen .doc of .xls formaat.
OWMS (Metadata overheidsinformatie)	Ja	De beleidskeuzes (contentmodellen) zijn in te zien in het Informatie Publicatie Model (IPM) bij het OWMS (zie: http://standaarden.overheid.nl/rijksoverheid).
PDF 1.7 / PDF A/1 en PDF A/2 (Documentpublicatie/ archivering)	Deels	De centrale redactie van Rijksoverheid.nl stuurt op het aanbieden van de juiste typen pdf's. De centrale redactie heeft beperkt zicht op soort en type pdf's die door decentrale redacteuren van de ministeries zelfstandig op rijksoverheid.nl worden geplaatst. Er zijn veel verschillende organisaties die PDFs op rijksoverheid.nl kunnen plaatsen. Het is daardoor simpelweg niet helemaal onder controle welke soorten PDF worden toegepast.
		Juridische identificatie en verwijzing
BWB (Wet- en regelgeving)	Ja	Binnen de website wordt verwezen naar wetgeving conform de BWB standaard. BWB wordt toegepast.

Ten opzichte van 2018 is STARTTLS/DANE geïmplementeerd. De standaard DMARC is sinds 2018 onvoldoende geïmplementeerd. De status gaat van ja naar nee. Voor het maildomein geldt dat rijksoverheid.nl niet voldoet aan IPv6, waardoor de status van ja naar deels is gegaan. De status van de standaard PDF 1.7 / PDF A/1 en PDF A/2 is van nee naar deels gegaan. Verder is de applicatie die gebruik maakte van de standaard SAML komen te vervallen. Deze standaard is daardoor niet meer van toepassing. De statussen ten aanzien van de standaarden STARTTLS-DANE en SPF, gebruikt voor het emaildomein, zijn toegekend door PBLQ en niet gevalideerd. Ondanks herhaalde pogingen de verantwoordelijke te vinden, is dit niet gelukt.

Concluderend moeten voor de voorziening rijksoverheid.nl nog de volgende standaarden (volledig) worden geïmplementeerd: DMARC, IPv4 en IPV6, PDF1.7 / PDF A/1 en PDF A/2.

4. Gegevens en registreren

4.1 Basisregistraties

4.1.1 NHR (Handelsregister)

Beheerorganisatie: Kamer van Koophandel

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	Het domein kvk.nl voldoet aan DKIM (zie: https://internet.nl/mail/kvk.nl/).
DMARC (Anti-phishing)	Ja	NHR voldoet op mailservers aan DMARC (zie: https://internet.nl/mail/kvk.nl/).
DNSSEC (Beveiligde domeinnamen)	Nee	De ondertekening in de emailomgeving van kvk.nl vindt momenteel niet goed plaats. Dit wordt z.s.m. hersteld, in ieder geval in 2019. Er is samenhang met de HSTS melding hierna vanwege afspraken met de provider van kvk.nl.zie: https://en.internet.nl/site/kvk.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening gebruikt zowel HTTPS als HSTS. Alleen voor kvk.nl werkt hsts niet, dit wordt in 2019 hersteld. Was nog niet gebeurd om kvk.nl alleen redirect naar www.kvk.nl en deze werkt wel onder hsts. Er was en is dus geen security risico.
IPv4 en IPv6 (Internetnummers)	Deels	Mailservers e.d. zijn bereikbaar via zowel IPv4 als IPv6 maar de website van KvK nog niet, De website kvk.nl ondersteunt IPv4, maar is niet toegankelijk via IPv6 (zie: https://internet.nl/site/www.kvk.nl/). Het project om over te stappen naar IPv6 voor de website hangt samen met de wisseling van provider die KvK wil gaan doen, die wisseling gaat niet voor 2020 plaatsvinden.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De KvK is sinds 2016 ISO 27001 gecertificeerd en hanteert ISO27002.
SAML (Inloggegevens)	Ja	eHerkenning is SAML-based en wordt toegepast voor het aanleveren van jaarrekeningen en informatieverstrekking. In de notarisapplicatie kan de notaris van achter zijn computer rechtstreeks opgave doen. Ook hier wordt

		gebruik gemaakt van SAML als authenticatieprocedure. Omdat gebruik wordt gemaakt van een generiek identificatie- en authenticatiesysteem voor alle diensten van KvK kan SAML voor elke dienst ingezet worden voor authenticatie.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd voor NHR.
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Deels	De voorziening past STARTTLS toe, DANE nog niet (zie: https://internet.nl/mail/kvk.nl/). Op DNS-servers is dit uitgerold maar op de emailservers onder Microsoft niet omdat Microsoft DANE niet ondersteunt.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De KvK gebruikt TLS op de verbindingen waar voorheen SSL werd gebruikt. De KvK gebruikt versie TLS1.2 (zie: https://internet.nl/site/www.kvk.nl/).
		Document en (web/app)content
Ades Baseline Profiles (Digitaal ondertekenen van documenten)	Ja	De NHR voldoet aan de Ades Baseline Profiles standaard.
CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)	Deels	De bij de KvK in gebruik zijnde content management systemen, Sharepoint en Documentum zijn compliant aan de CMIS standaard, maar het webcontent platform Tridion (nog) niet vanwege een verouderde versie van de software. De upgrade van Tridion vindt in 2019 plaats, daarna worden de koppelingen daarmee aangepakt (2020 e.v.). Koppelingen met Sharepoint worden CMIS compliant uitgevoerd.
Open API Specification (Beschrijven van REST API's)	Deels	KvK gebruikt deze specificatie actief. Reeds operationele API's worden geleidelijk aangepast.
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/ archivering)	Ja	Alle uittreksels en informatie uit het NHR wordt in PDF/A-vorm verstrekt. Het betreft al grotendeels PDF A/2. Er zijn nog documenten in PDF A/1 die nog in 2019 worden omgezet.
SKOS (Thesauri en begrippen-woordenboeken)	Nee	SKOS is nog niet geïmplementeerd in Gegevenscatalogus NHR. De standaard wordt wel voorzien door diverse ondersteunende software pakketten in gebruik bij de KVK rondom het NHR. Implementatie van SKOS in de Gegevenscatalogus HR is nog niet ingepland vanwege andere prioriteiten.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Ongeveer 10% van het verkeer van het NHR gaat naar medeoverheden. Die uitwisselingen vinden allemaal plaats via Digikoppeling en StUF.
STuF (Uitwisseling administratieve overheids-gegevens)	Ja	Ongeveer 10% van het verkeer van het NHR gaat naar medeoverheden. Die uitwisselingen vinden allemaal plaats via Digikoppeling en StuF.
		E-facturatie en administratie

NLCIUS (Elektronisch factureren)	Nee	KvK heeft haar financiële systeem in 2018 naar AFAS gemigreerd. UBL 2.1 en SMeF 2.0 worden wel ondersteund maar de modelfactuur nog niet.

Ten opzichte van 2018 is de status van STARTTLS/DANE en Open API Specification van gepland naar deels gegaan. De status van DNSSEC is gegaan van ja naar nee. De status van HSTS is van deels naar ja gegaan. Daarnaast is de planning van IPv4 en IPv6 verschoven.

Concluderend moeten voor het NHR nog de volgende standaarden (volledig) worden geïmplementeerd: DNSSEC, IPv4 en IPv6, STARTTLS/DANE, CMIS, Open API Specification, SKOS, NLCIUS.

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

Beheerorganisatie: Kadaster

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

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

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

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

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

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

Standaard	Status	Toelichting beheerder
Internet en beveiliging		

DKIM (Preventie van mailspoofing/ phishing)	Ja	Het Kadaster voldoet aan DKIM.
DMARC (Anti-phishing)	Ja	Deze standaard is geïmplementeerd.
DNSSEC (Beveiligde domeinnamen)	Ja	De website www.kadaster.nl ondersteunt DNSSEC (zie: https://internet.nl/domain/www.kadaster.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels	HTTPS en HSTS zijn deels geïmplementeerd. (zie: https://internet.nl/domain/www.kadaster.nl/) Eerdere planningen voor volledige implementatie in Q1 en Q4 2018 zijn niet gehaald. HSTS is inmiddels op de meeste Kadaster endpoints geïmplementeerd. Er is een beperkte set aan Digikoppeling gerelateerde content (schema's) die nog niet over kunnen naar HTTPS en HSTS. Er is nog geen duidelijke planning voor.
IPv4 en IPv6 (Internetnummers)	Ja	Zowel IPv4 als IPv6 worden ondersteund door het Kadaster (zie: https://internet.nl/domain/www.kadaster.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Het Kadaster is gecertificeerd voor NEN-ISO/IEC 27001 en hanteert 27002. Het Handboek Beveiliging Kadaster is volledig op de BIR gebaseerd. In het jaarverslag is een in control statement opgenomen.
SPF (Preventie van mailspoofing/ phishing)	Ja	SPF is geïmplementeerd (zie: https://internet.nl/mail/kadaster.nl/).
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Nee	STARTTLS is geïmplementeerd (zie: https://internet.nl/domain/www.kadaster.nl/). Eerdere planningen voor implementatie van DANE per Q1 2018 en later Q1 2019 zijn niet gehaald. De verhuizing van het mail domein is vertraagd, waarbij opgemerkt moet worden dat de bestemming, in dit geval Microsoft, geen planning heeft voor de implementatie van DANE.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Deze standaard wordt volledig door het Kadaster ondersteund (zie: https://internet.nl/domain/www.kadaster.nl/).
		Document en (web/app)content
Open API Specification (Beschrijven van REST API's)	Ja	Deze standaard is geïmplementeerd.
PDF 1.7, PDF/A-1 en PDF/A-2 (Documentpublicatie/ archivering)	Ja	Uittreksels worden verstrekt in PDF 1.4-formaat. Databestanden worden vooral in GML uitgewisseld. GML is een standaard XML-formaat voor Geo-data, gebaseerd op de Geo-standaarden. Afnemers melden geen problemen met het huidige PDF formaat. Daarom geeft het Kadaster

		geen prioriteit aan het vervangen van PDF 1.4. Voor het archiveren van kennisgevingen wordt gebruik gemaakt van PDF/A-1.
SKOS (Thesauri en begrippen-woordenboeken)	Deels	Het Kadaster hanteert SKOS voor de beschikbaarstelling van begrippenkaders van basisregistraties. De begrippenkaders voor de BRK zoals gepubliceerd op brk.basisregistraties.nl, de BAG zoals gepubliceerd op bag.basisregistraties.nl en de BGT (IMgeo) en BRT op definities.geostandaarden.nl zijn allemaal conform SKOS. Voor de WOZ moet deze slag nog worden gemaakt. (4 van de 5 BR's). Hiervoor is nog geen planning. Het Kadaster is alleen verantwoordelijk voor de hosting en het technisch beheer van de LV-WOZ de verantwoordelijkheid voor de implementatie van SKOS ligt bij de Waarderingskamer. Voor zover bij het Kadaster bekend is er geen planning voor de implementatie van SKOS voor de LV-WOZ.
		E-facturatie en administratie
NLCIUS (Elektronisch factureren)	Nee	Invoering van elektronisch factureren is zowel 2018 als in 2019 onderhanden en daarop zal gebruik gemaakt gaan worden van de NLCIUS standaard.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichten-uitwisselingen)	Deels	Vrijwel alle koppelingen met afnemers, andere basisregistraties en evt. front-office systemen worden gelegd op basis van Digikoppeling: - de koppelingen voor het aanleveren van gegevens aan LV-BAG, LV-WOZ en LV-BGT zijn gebaseerd op Digikoppeling standaarden; - het aanleveren door bronhouders (o.a. notariaat) van gegevens aan de BRK is niet gebaseerd op Digikoppeling; - de koppelingen voor het verkrijgen van informatie van gegevens uit LV BAG en LV WOZ en BRK zijn gebaseerd op Digikoppeling. Daarnaast kan informatie uit LV's worden verkregen via PDOK (Publieke Dienstverlening op de Kaart) die gebruik maakt van de Open GEO-standaarden. Ook de informatie uit de BRT wordt op deze wijze geleverd. Gegevens uit de BGT zijn beschikbaar via PDOK.
Geo-Standaarden (Geografische informatie)	Ja	Naast de INSPIRE richtlijnen, maakt het Kadaster gebruik van NEN3610 en de meest gangbare Geo standaarden voor de betreffende basisregistraties.
StUF (Uitwisseling administratieve overheidsgegevens)	Ja	Het Kadaster maakt deels gebruik van StUF en is deels volgens de Geo-standaarden (GML) opgemaakt. StUF wordt gebruikt voor aanlevering van bronhouder naar LV-BAG, LV-WOZ en LV-BGT. WOZ en BGT worden ook geleverd in StUF.

Ten opzichte van 2018 is de status van HTTPS/HSTS veranderd van gepland naar deels. Er is een beperkte set aan Digikoppeling gerelateerde content (schema's) die nog niet over kunnen naar HTTPS en HSTS. Er is nog geen duidelijke planning voor. De status van STARTTLS/DANE is veranderd van gepland naar nee. De verhuizing van het mail domein is vertraagd.

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

4.1.3 BRT (Basisregistratie Topografie)

Beheerorganisatie: Kadaster

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	DMARC is geïmplementeerd.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels	HTTPS en HSTS zijn deels geïmplementeerd (zie: https://internet.nl/domain/www.kadaster.nl/). Eerdere planningen voor (volledige) implementatie in Q1 en in Q4 2018 zijn niet gehaald. HSTS is inmiddels op de meeste Kadaster endpoints geïmplementeerd. Er is een beperkte set aan Digikoppeling gerelateerde content (schema's) die nog niet over kunnen naar HTTPS en HSTS. Er is hier nog geen duidelijke planning voor.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Het Kadaster is gecertificeerd voor NEN-ISO/IEC 27001 en hanteert 27002. Het Handboek Beveiliging Kadaster is volledig op de BIR gebaseerd. In het jaarverslag is een in control statement opgenomen.
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Nee	STARTTLS is geïmplementeerd (zie: https://internet.nl/domain/www.kadaster.nl/). Eerdere planningen voor implementatie van DANE per Q1 2018 en later Q1 2019 zijn niet gehaald. De verhuizing van het mail domein is vertraagd, waarbij opgemerkt moet worden dat de bestemming, in dit geval Microsoft, geen planning heeft voor de implementatie van DANE.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Deze standaard wordt volledig door het Kadaster ondersteund (zie: https://internet.nl/domain/www.kadaster.nl/).
		Document en (web/app)content
OWMS (Metadata overheidsinformatie)	Nee	OWMS is wel van toepassing, maar PDOK hanteert via het Nationaal GEO Register de wettelijk vastgelegde standaarden, gebaseerd op Inspire en ISO volgens het zogenaamde NL profiel. Data.overheid.nl harvest het NGR met behulp van de CSW standaard (Catalogue Services for the Web' een OGC-Geostandaard (Open Geospatial Consortium), ook onderdeel van INSPIRE). De BRT voldoet dus niet aan de standaard maar voldoet

		wel aan alternatieve internationale standaarden. Er zijn geen interoperabiliteitsproblemen hierdoor.
SKOS (Thesauri en begrippen-woordenboeken)	Ja	Het Kadaster hanteert SKOS voor de beschikbaarstelling van begrippenkaders van basisregistraties. De begrippenkaders voor de BRK zoals gepubliceerd op brk.kadaster.nl, de BAG zoals gepubliceerd op bag.kadaster.nl en de BGT (IMgeo) en BRT op definities.geostandaarden.nl zijn allemaal conform SKOS.
		Stelselstandaarden
Geo-Standaarden (Geografische informatie)	Ja	De BRT wordt zowel geleverd via PDOK (Wat biedt Publieke Dienstverlening Op de Kaart) in GML (Objectdata), als via internationale Geo-standaarden. Daarnaast wordt de BRT geleverd via PDOK in rasterformaat in GEO, tiff formaat en WMTS (Web Map Tile Service).

Ten opzichte van 2018 is de status van HTTPS/HSTS veranderd van gepland naar deels. Er is een beperkte set aan Digikoppeling gerelateerde content (schema's) die nog niet over kunnen naar HTTPS en HSTS. Er is nog geen duidelijke planning voor. De status van STARTTLS/DANE is veranderd van gepland naar nee. De verhuizing van het mail domein is vertraagd.

Concluderend moeten voor de BRT nog de volgende standaarden (volledig) worden geïmplementeerd: HTTPS/HSTS, STARTTLS/DANE, OWMS.

4.1.4 BRO (Basisregistratie Ondergrond)

Beheer organisatie: Programmabureau BRO van het Ministerie BZK (afdeling DG BRW – RO)

Werking en inhoud BRO
De Basisregistratie Ondergrond (BRO) brengt alle informatie over de Nederlandse ondergrond op één plek bij elkaar en stelt deze via één loket digitaal beschikbaar. Per 1 januari 2018 is de wet BRO in werking getreden voor de eerste tranche van registratieobjecten (Geotechnisch sondeeronderzoek, Booronderzoek, Grondwatermonitoringput). De ketenprocessen van de BRO zijn ingericht en de bronhouders zijn in staat om aan te (laten) leveren via het Bronhouderportaal aan de Landelijke Voorziening (LV). Er is een gebruiksplicht inwerking getreden voor overheidsorganisaties en iedereen die in opdracht van hen werkzaamheden verricht. Op 1 februari 2018 waren er bijna 50 bronhouders aangesloten op het Bronhouderportaal. Het gaat om 28 gemeenten, acht provincies, negen waterschappen en vier overige overheidsorganisaties.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DNSSEC (Beveiligde domeinnamen)	Ja	Toegepast door alle hostingpartijen die BRO systemen hosten.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	BRO website (https://www.basisregistratieondergrond.nl), BRO web applicaties (DINO|BRO Loket https://www.dinoloket.nl) en APIs ondersteunen HTTPS en HSTS.
IPv4 en IPv6 (Internetnummers)	Deels	Hosting Landelijke Voorziening BRO door TNO bij Solvinity > Hoewel alle gebruikte componenten IPv6 capabel zijn, wordt het interne netwerk ingericht op basis van IPv4. Initieel is de internetverbinding

		ook alleen op basis van IPv4 ingericht. In een later stadium zal de internetverbinding doormiddel van een IPv4/IPv6 proxy ook via IPv6 beschikbaar worden gesteld. Hosting Bronhouderportaal BRO bij Standaard Platform (ODC Noord) > Zie status (d.d. maart 2018) in de monitor open standaardenbeleid https://www.noraonline.nl/wiki/Monitor_Open_Standaardenbeleid_2016/ODC-Noord-IPv6_en_IPv4 basisregistratieondergrond.nl is via IPv4 en IPv6 bereikbaar, voor dinoloket.nl geldt dat het domein nog alleen via IPv4 bereikbaar is.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	TNO (en hosting partij Solvinity) zijn ISO 27001/27002 compliant ICTU (en hosting partij SP|ODC-Noord) zijn ISO 27001/27002 compliant PDOK (en hosting partij CapGemini) zijn ISO 27001/27002 compliant
SAML (Inloggegevens)	Ja	Het Bronhouderportaal BRO maakt gebruik van eHerkenning voor authenticatie van gebruikers. eHerkenning ondersteunt SAML. Zie ook evaluatierapport SAML 2.0 Forum Standaardisatie https://www.forumstandaardisatie.nl/sites/default/files/FS/2018/0314/FS-20180314.03C-Evaluatie-SAML-2.0.pdf
TLS (Beveiligde, versleutelde verbindingen)	Ja	De BRO gebruikt SSL (TLS) certificaten voor inname en uitgifte APIs en voor beveiligde gegevensuitwisseling met PDOK.
		Document en (web/app)content
CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)	Ja	DIGIDOC2 > Interne opslag van formele documenten programma BRO vindt plaats in het DMS systeem van het Ministerie BZK Digidoc2 v7.0.1. Zie voor CMIS compliancy van Digidoc2 het onderzoek Forum uit 2014 (https://www.forumstandaardisatie.nl/sites/default/files/FS/2014/1028/FS-20141028.04A2-Aanvullend-onderzoek-CMIS.pdf). Inmiddels zijn de compliancy issues waarover in het 2014 rapport wordt gesproken mogelijk opgelost
	Ja	SAMENWERKINGSRUIMTEN RIJK (https://sts.dwr.rijksdienst.nl) > Samenwerkingsruimte BRO (externe uitwisseling o.a. met BIT) gebaseerd op Sharepoint.. Sharepoint ondersteunt CMIS development/content-management-interoperability-services-cmis-in-sharepoint
	Ja	CONFLUENCE > Confluence omgeving BRO is een WIKI omgeving voor alle operationele content management BRO programma. Confluence ondersteunt CMIS, zie https://community.atlassian.com/t5/Answers-Developer-

		Questions/How-do-I-set-up-a-CMIS-Repository-within-Confluence/qaq-p/518301 ALFRESCO DMS > Alfresco wordt door LV BRO en Bronhouderportaal BRO gebruikt voor opslag van IMBRO XML documenten registratie authentieke brondocumenten). Alfresco ondersteunt CMIS https://docs.alfresco.com/5.0/pra/1/topics/cmis-welcome.html
Open API Specification (Beschrijven van REST API's)	Ja	Het Bronhouderportaal BRO (voorportaal voor validatie van BRO gegevens voordat deze worden door geleverd naar de Landelijke Voorziening BRO) voldoet aan de open API specificatie https://www.bronhouderportaal-bro.nl/bpbro-frontend/documentation/api.html. De Landelijke Voorziening BRO voldoet aan de PTOLU Digikoppeling standaard (SOAP-XML).
Stelselstandaarden		
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Landelijke Voorziening BRO inname en uitgifte APIs zijn gebaseerd op Digikoppeling 2.0.
Geo-standaarden	Ja	BRO is een geo-basisregistratie. Geografische BRO gegevens worden o.a. beschikbaar gesteld via het GDI geo-knooppunt PDOK (www.pdok.nl). De PDOK APIs zijn gebaseerd op Open Geospatial Consortium standaarden (www.opengeospatial.org), waaronder OGC:WMS, OGC:WFS, OGC:WCS. Geografische gegevens worden uitgeleverd in open bestandsformaten (OGC:GML, OGC:Geopackage, OGC:GeoTIFF). BRO metadata wordt via het Nationaal Georegister (www.nationaalgeoregister.nl) ontsloten. Het Nationaal Georegister is gekoppeld met (wordt geharvest door) data.overheid.nl Het NGR is gebaseerd op de geo-standaarden CS-W 2.0 (discovery service), ISO 19115 NL profiel (metadata voor geografische datasets), en ISO 19119 NL profiel (metadata voor geografische web services)
Water en bodem		
Aquo-standaard	Ja	Relevante onderdelen worden meegenomen in de BRO standaardisatie van het grondwaterdomein (de aquo standaard omvat ook oppervlaktewater hetgeen buiten scope is voor de BRO).
Juridische verwijzingen		
BWB (Identificatie van en verwijzing naar wet- en regelgeving)	Gepland	Zou gebruikt kunnen (en moeten) worden voor verwijzingen naar BRO gerelateerde wetsartikelen vanuit de BRO website en in overige BRO documenten zoals programmaplan, GAS, PSA, etc. (zie voorbeeld https://www.overheid.nl/help/wet-en-regelgeving/verwijzen-naar-wet-en-regelgeving). De standaard wordt 3e kwartaal 2019 geïmplementeerd.

De BRO is dit jaar voor eerst opgenomen in het onderzoek. Voor SKOS, SIKB0101, SIKB0102 geldt dat deze standaarden (mogelijk) in de toekomst relevant zijn. I.v.m. SKOS: De BRO begrippen (o.a. registratieobjecten) worden binnenkort opgenomen in de Stelselcatalogus (gebaseerd op SKOS, zie

https://www.noraonline.nl/wiki/Stelselcatalogus ondersteunde standaarden Stelselcatalogus). Het BRO standaardisatieteam o.l.v. Geonovum heeft hierover reeds contact met Logius. I.v.m. SIKB0101: Mogelijk op termijn van belang voor BRO (opname van onderzoeksgegevens over de milieu-hygiënische kwaliteit van de bodem in de BRO wordt op dit moment onderzocht). I.v.m. SIKB0102: Archeologische informatie is geen onderdeel van de BRO > In een mogelijk vervolgprogramma “BRO II” zullen archeologische gegevens mogelijk onderdeel gaan uitmaken van de BRO.

Concluderend moeten voor de BRO nog de volgende standaarden (volledig) worden geïmplementeerd: IPv4 en IPv6 en BWB.

4.1.5 BRV (Basisregistratie Voertuigen)

Beheerorganisatie: RDW (Rijksdienst Wegverkeer)

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	De BRV voldoet aan DKIM.
DMARC (Anti-phishing)	Deels	De BRV voldoet aan DMARC. Rdw.nl voldoet niet aan de standaard, zie: https://internet.nl/mail/rdw.nl/253063/. De RDW is in 2017 gestart met een nieuwe leverancier die ook maatregelen voor het aanscherpen van DANE, DKIM, SPF, etc. zou meenemen. Doordat de implementatie van de digitale werkomgeving langer heeft geduurd dan beoogd, is dit tot op heden nog niet uitgevoerd. Augustus 2019 is RDW gestart om privacy en security verder te gaan verbeteren. De onderwerpen zoals DANE, DKIM, SPF, etc. zijn ook onderdeel van deze verbeteringen en de verwachting is dat RDW dit komende jaar de verbeteringen heeft doorgevoerd.
DNSSEC (Beveiligde domeinnamen)	Deels	De niet-gevoelige (technische) gegevens uit de BRV zijn te bevragen via www.rdw.nl. Alle .nl rdw domeinen zijn gesigned met DNSSEC. De diensten op (voertuig)gegevens draaien als microservices in de Azure cloud en het is bekend dat hierop geen DNSSEC en daarmee ook DANE mogelijk is. RDW en andere overheidspartijen hebben bij Microsoft gevraagd om dit op te lossen.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Deels	Implementatie zou medio 2018 gerealiseerd worden. Rdw.nl voldoet niet aan de standaard, zie: https://internet.nl/mail/rdw.nl/253063/. De RDW is in 2017 gestart met een nieuwe leverancier die ook maatregelen voor het aanscherpen van DANE, DKIM, SPF, etc. zou meenemen. Doordat de implementatie van de digitale werkomgeving langer heeft geduurd dan beoogd, is dit tot op heden nog niet uitgevoerd. Augustus 2019 is RDW gestart om privacy en security verder te gaan verbeteren. De

		onderwerpen zoals DANE, DKIM, SPF, etc. zijn ook onderdeel van deze verbeteringen en de verwachting is dat RDW dit komende jaar de verbeteringen heeft doorgevoerd. De diensten op (voertuig)gegevens, die als microservices in de Azure cloud draaien, voldoen wel aan HTTPS/HSTS.
IPv4 en IPv6 (Internetnummers)	Nee	IPv4 wordt ondersteund, IPv6 wordt nog niet ingezet. De BRV is te bevragen via www.rdw.nl. Op dit moment ziet de RDW voor de BRV nog geen noodzaak om op IPv6 over te gaan.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De BRV voldoet aan deze standaard.
SAML (Inloggegevens)	Ja	De BRV voldoet aan SAML.
SPF (Preventie van mailspoofing/phishing)	Ja	RDW ondersteunt en gebruikt de SPF standaard voor email verkeer.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	De BRV voldoet aan STARTTLS, DANE, DKIM en SPF
TLS (Beveiligde, versleutelde verbindingen)	Ja	RDW ondersteunt en gebruikt de TLS protocollen op de e-mail servers en Digikoppeling.
		Document en (web/app)content
CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)	Nee	In de loop van 2019/2020 zal het document management systeem voor de primaire processen geschikt worden gemaakt voor aansluiting door geautomatiseerde processen. CMIS zal als standaard voor de ontsluiting worden gehanteerd.
Open API Specification (Beschrijven van REST API's)	Ja	De BRV voldoet aan Open API Specification.
OWMS (Metadata overheidsinformatie)	Ja	De toegang tot BRV-data is op data.overheid.nl in overeenstemming met OWMS gemetadateerd beschikbaar.
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/archivering)	Ja	Bij digitale dienstverlening worden uittreksels en informatie uit de BRV in PDF/A vorm verstrekt.
SKOS (Thesauri en begrippenwoordenboeken)	Ja	De BRV voldoet aan SKOS.
		Stelselstandaarden

Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	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. De intentie is uitgesproken om ook bestaande koppelingen pro-actief te migreren om de voordelen van het diginetwerk te benutten. Een planning hiervoor is nog niet vastgesteld.

Ten opzichte van 2018 voldoet de voorziening nog deels aan DMARC. De status is van ja naar deels gegaan. De status van HTTPS/HSTS ging van gepland naar deels.. De status van DNSSEC is van ja naar deels gegaan.

Concluderend moeten voor de BRV nog de volgende standaarden (volledig) worden geïmplementeerd: DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, CMIS, Digikoppeling 2.0.

4.1.6 BRI (Basisregistratie Inkomen)

Ondanks herhaalde verzoeken en gesprekken met verschillende contactpersonen om dit jaar informatie aan te leveren ten aanzien van gebruik van standaarden bij de BRI, is het dit jaar niet gelukt een reactie te krijgen van de belastingdienst.

Beheerorganisatie: Belastingdienst

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	De voorziening voldoet aan de DMARC standaard.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De BRI voldoet aan de standaard beveiligingseisen van de Belastingdienst. Deze eisen zijn conform VIR met classificatie departementaal vertrouwelijk. Voor opsporingsgegevens (FIOD) geldt een strakker regime. Aangezien het beveiligingskader voor de gehele Belastingdienst geldt, is er geen apart in control statement voor de BRI.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De actuele versies van TLS maken deel uit van de standaard beveiligingsrichtlijnen van de Belastingdienst.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Digikoppeling wordt toegepast in de rol van afnemer van berichten van basisregistraties(HR). De ebMS-koppeling met Digilevering is operationeel in de productie-omgeving. De aansluiting op Digilevering wordt nu alleen gebruikt in de rol van afnemer van het stelsel van basisregistraties. Het aansluiten van

	de BRI als Basisregistratie/leverancier op Digilevering was niet eerder dan 2017-2018 gepland.

Ten opzichte van 2018 zijn er geen wijzigingen opgenomen in de tekst.

4.2 Digilevering

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM[7] (Preventie van mailspoofing/phishing)	Ja	Digilevering draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. DKIM is geïmplementeerd op de centrale voorziening mail relay.
DMARC (Anti-phishing)	Ja	DMARC is inmiddels geïmplementeerd en doorgevoerd in de DNS instellingen.
DNSSEC[8] (Beveiligde domeinnamen)	Ja	DNSSEC is geïmplementeerd op de centrale voorziening DNS.
HTTPS/HSTS[9] (Beveiligd, versleuteld webverkeer)	Ja	Digilevering voldoet aan de HTTPS standaard. Voor Digilevering is een PKIO certificaat verplicht om te kunnen aanloggen op de applicatie. Zonder dit certificaat kan de https doorverwijzing niet slagen en biedt www.internet.nl geen toetsing. HSTS wordt aangeboden.

[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

IPv4 en IPv6 (Internetnummers)	Nee	IPv6 kan niet worden aangeboden, omdat de infrastructuur van Logius dit nog niet voldoende ondersteunt. Dit is een Logius breed vraagstuk. De vraag hoe IPv6 geïmplementeerd dient te worden is wederom bij onze architecten ingediend.
SPF[10] (Preventie van mailspoofing/phishing)	Ja	Digilevering draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. SPF is geïmplementeerd op de centrale voorziening mail relay.
STARTTLS/DANE[11] (Beveiligd, versleuteld mailverkeer)	Ja	Digilevering draait op het Logius Managed Services platform. Vanuit de clouddienst is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Digilevering maakt gebruik van Digikoppeling.

Ten opzichte van 2018 is DMARC volgens planning geïmplementeerd. De status van IPv4 en IPv6 ging van gepland naar nee.

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

4.3 Digimelding

Beheerorganisatie: Logius

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

[10] idem

[11] idem

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Gepland	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. Gepland Q3 2019.
DMARC (Anti-phishing)	Ja	DMARC is geïmplementeerd.
DNSSEC[12] (Beveiligde domeinnamen)	Ja	DNSSEC is geïmplementeerd.
HTTPS/HSTS[13] (Beveiligd, versleuteld webverkeer)	Ja	De url portaal.digimelding.nl voldoet aan HTTPS en HSTS.
IPv4 en IPv6 (Internetnummers)	Nee	Digimelding gebruikt het Logius infrastructuurplatform. IPv6 kan niet worden aangeboden, omdat de infrastructuur van Logius dit nog niet voldoende ondersteunt. Dit is een Logius breed vraagstuk. De vraag hoe IPv6 geïmplementeerd dient te worden is wederom bij onze architecten ingediend. Digimelding ondersteunt op dit moment alleen IPv4.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd.
STARTTLS/DANE[14] (Beveiligd, versleuteld mailverkeer)	Nee	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.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Digimelding maakt gebruik van Digikoppeling.

[12] [12] 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.

[13] Digimelding portaal is alleen benaderbaar via de url portaal.digimelding.nl

[14] 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.

Ten opzichte van 2018 voldoet Digimelding niet meer aan de standaard DKIM, de status is veranderd van ja naar gepland. Verder voldoet de voorziening inmiddels aan de standaarden DMARC en HTTPS en HSTS.

Concluderend moet Digimelding de volgende standaarden nog (volledig) implementeren: DKIM, IPv4 en IPv6 en STARTTLS/DANE.

4.4 Stelselcatalogus

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	De Stelselcatalogus voldoet aan DMARC (zie: https://internet.nl/mail/stelselcatalogus.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC is geïmplementeerd op de centrale voorziening DNS (zie: https://internet.nl/site/www.stelselcatalogus.nl/).
HTTPS/ HSTS (Beveiligd, versleuteld webverkeer)	Gepland	De voorziening voldoet niet meer aan HTTPS (zie: https://internet.nl/site/www.stelselcatalogus.nl/). De website www.stelselcatalogus.nl zal voor eind 2019 worden voorzien van een certificaat.
IPv4 en IPv6 (Internetnummers)	Nee	De Stelselcatalogus gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt niet de open standaard IPv4 en IPv6 voor internet gebruik. Stelselcatalogus ondersteunt geen IPv6 (zie: https://internet.nl/site/www.stelselcatalogus.nl/).
		Document en (web/app)content
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/ archivering)	Ja	Documenten worden als PDF-A/1 aangeboden via de website.
SKOS (Thesauri en begrippen-woordenboeken)	Ja	SKOS wordt toegepast door de voorziening.
		Juridische identificatie en verwijzing

BWB (Wet- en regelgeving)	Ja	De Stelselcatalogus gebruikt het Basis Wetten Bestand (BWB) via Juriconnect als open standaard voor de link naar de wetgeving als bron. De Juriconnect Id's worden gebruikt om per gegeven of begrip in de Stelselcatalogus de link te leggen naar de wet en het artikel in het Basis Wetten Bestand.

Ten opzichte van 2018 is een planning afgegeven voor implementatie van HTTPS/HSTS (status van nee naar gepland) en voldoet de stelselcatalogus niet langer aan IPv4 en IPv6 (status van ja naar nee).

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

4.5 P-Direkt

Beheerorganisatie: P-Direkt

Werking en inhoud van 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 beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	P-Direkt maakt gebruik van de mailservers van SSC-ICT, onder andere voor het versturen van de loonstroken aan de medewerkers. Het initiatief voor de adoptie van dit soort standaarden ligt dan ook bij SSC-ICT. Navraag bij SSC-ICT leert dat DKIM actief gemaakt is voor deze mailservice van P-Direkt.
DMARC (Anti-phishing)	Ja	De Rijksbrede mail voorziening waarvan P-Direkt gebruik maakt, ondersteunt DMARC.
DNSSEC (Beveiligde domeinnamen	Nee	Op de Haagse ring maakt het netwerk van SSC-ICT, waar P-Direkt gebruik van maakt, geen gebruik van DNSSEC. Ook hier geldt dat P-Direkt een afnemer is van een Rijksbrede dienstverlening en het initiatief voor het implementeren van DNSSEC bij de SSC-ICT ligt. DNSSEC is nog niet geïmplementeerd binnen SSC-ICT en dus ook niet op het P-Direkt Self Service portaal. Op de externe website www.p-direkt.nl is DNSSEC wel geïmplementeerd.

HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	HTTPS is 100% doorgevoerd voor alle communicatie met klanten. HSTS is volledig geïmplementeerd op de interne en externe site van P-Direkt.
IPv4 en IPv6 (Internetnummers)	Nee	De P-Direkt omgeving, draaiend in de ODC Rijswijk omgeving en beheert door SSC-ICT, is gebaseerd op IPv4. ODC Rijswijk en Haagse Ring (het koppelnetwerk waar P-Direkt gebruik van maakt) ondersteunt geen IPv6.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De hosting van de dienstverleningssystemen van P-Direkt voldoet aan de BIR (BIR compliancy is integraal onderdeel van de inrichting van het Overheids Data Center, en als zodanig daarmee ook voor P-Direkt). Daarmee wordt indirect voldaan aan NEN-ISO/IEC 27001/27002, de BIR is immers gebaseerd op NEN-ISO/IEC 27001/27002, aangevuld met overheidsspecifieke maatregelen. In Q2 2019 is in samenwerking met het Ministerie van Infrastructuur en Waterstaat een project gestart om volledig Baseline Informatiebeveiliging Overheid (BIO), en daarmee NEN-ISO/IEC 27001/27002 compliant te zijn. Verwachtte afronding is eind 2019, begin 2020. Een aantal P-Direkt systemen, inclusief beheerorganisatie voldoet inmiddels aan de BIO.
SAML (Inloggegevens)	Ja	P-Direkt gebruikt SAML om Single Sign-On in te vullen. Verbinding naar de kerndepartementen is gelegd, maar een gedeelte van de rijksambtenaren van onderliggende organisatieonderdelen, moeten nog handmatig inloggen. P-Direkt heeft met de kerndepartementen de afspraak gemaakt dat de kerndepartementen verantwoordelijk zijn voor het implementeren van de Single Sign-on functie bij de onderliggende organisatieonderdelen.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd door de beheerder van de maildienst (in het geval van P-Direkt is dat SSC-ICT).
STARTTLS/DANE	Nee	STARTTLS en DANE zijn van toepassing. STARTTLS is wel geïmplementeerd op de Rijks Mail Relay, DANE niet.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Alle diensten van P-Direkt die door middel van HTTP worden ontsloten, worden aangeboden via TLS v1.0, v1.1 en v1.2.
		Document en (web/app)content
Ades Baseline Profiles (Digitaal ondertekenen van documenten)	Nee	De implementatie van deze standaard is nog niet gestart en hiervoor is nog geen concrete planning.
ODF (Document-bewerkingen)	Nee	Veel brieven die automatisch gegenereerd worden, worden in Word gemaakt en naar managers verstuurd, die deze dan zelf nog aanpassen. P-Direkt gebruikt .doc(x), omdat dit voor de doelgroep het meest gangbaar is. De ontvanger van de brieven zou dit zelf moeten omzetten met de aanwezige KA software die ODF ondersteunt. In het proces dat brieven genereert is het niet mogelijk ODF bestanden te genereren.
PDF 1.7 – PDF A/1 of PDF A/2 (Documentpublicatie/ archivering)	Ja	De meeste zaken die het digitale personeelsdossier ingaan zijn PFDA/1. Sinds de ingebruikname van de nieuwe versie van het Document/Record Management Systeem worden ook de loonstroken opgeslagen in PDF A/1 formaat.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	P-Direkt heeft vele interfaces met partijen binnen de overheid, Identity management, hr-data, arbo-diensten, ziekmeldingen, koppelingen met BD. Het salarisverwerkingssysteem werkt op basis van Digikoppeling. Alle nieuwe koppelingen die P-Direkt ontwikkelt,

		worden gebouwd op basis van Digikoppeling. Richting 2018 migreert de voorziening naar de rijksdatacenters, Digikoppeling krijgt dan een nog belangrijkere rol. Nieuwe interfaces zoals TEM2W, IDM2 en de ARBO interface zijn conform Digikoppeling 2.0.
		Juridische identificatie en verwijzing
BWB (Wet- en regelgeving)	Ja	Alle verwijzingen naar wetten worden conform de BWB-standaard gemaakt. De redactie heeft de richtlijn dat ze altijd op deze manier handelt bij verwijzingen naar wetsteksten of andere regels en richtlijnen die op wetten.overheid.nl te vinden zijn.

Ten opzichte van 2018 is HTTPS/HSTS van gepland naar ja gegaan. Implementatie van NEN-ISO/IEC 27001/27002 en PDF is van deels naar ja gegaan. STARTTLS/DANE is nieuw opgenomen.

Concluderend moeten voor P-direkt nog de volgende standaarden (volledig) worden geïmplementeerd: DNSSEC, IPv6, Ades Baseline Profiles, ODF en STARTTLS/DANE.

5. Dienstverlening en verbinden

5.1 eFactureren

Beheerorganisatie: Logius

Werking en inhoud van eFactureren
Voor de uitwisseling van digitale bestanden sluiten verzenders en ontvangers van de facturen aan op een centrale infrastructuur. Bedrijven leveren hun facturen voor de overheid elektronisch aan bij Digipoort. Digipoort controleert of de e-factuur betrouwbaar, leesbaar en verwerkbaar is. Dit overlapt buiten Digikoppeling verder volledig met de andere 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 beheerder
		E-facturatie en administratie
NLCIUS (Elektronisch factureren)	Nee	De SMEF 2.0 standaard was nog niet geïmplementeerd maar wordt opgevolgd door de NLCIUS. Per 19 april 2019 is de NLCIUS verplicht voor overheden, volgens Europese richtlijn 2014/55. Implementatie van NLCIUS stond gepland voor Q2 2019. Implementatie staat niet meer concreet gepland. De verwachting is dat implementatie Q2 2020 gereed is.

Ten opzichte van 2018 is de implementatiedatum van de standaard NLCIUS verplaatst van Q2 2019 naar Q2 2020 (naar verwachting).

Concluderend moet voor de voorziening eFactureren nog de volgende standaard (volledig) worden geïmplementeerd: NLCIUS.

5.2 SBR

Beheerorganisatie: Logius

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

Koophandel (KvK), het Centraal Bureau voor de Statistiek (CBS) en de Dienst Uitvoering Onderwijs (DUO)[15]. De voorziening voor de e-dienstverlening is Digipoort. SBR heeft een eigen website.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/ phishing)	Nee	De website van SBR (http://www.sbr-nl.nl) heeft ook een mailserver die niet voldoet aan DKIM. Zie: https://internet.nl/mail/sbr-nl.nl/249059/De website is overgezet naar het Ministerie van AZ.
DMARC (Anti-phishing)	Nee	SBR voldoet niet aan DMARC. Dit stond gepland voor Q1 2019 en nieuwe planning volgt in Q4 2019.
DNSSEC (Beveiligde domeinnamen)	Ja	De website van SBR (http://www.sbr-nl.nl) Voldoet zowel op het web als het maildomein aan DNSSEC.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening voldoet aan HTTPS en HSTS. Zie: https://internet.nl/site/sbr-nl.nl/563965/
IPv4 en IPv6 (Internetnummers)	Deels	De website van SBR wordt bij een derde partij gehost en is bereikbaar met IPv6. Er zijn mailservers die niet voldoen aan IPv6. IPv6 kan niet worden aangeboden, omdat de infrastructuur van Logius dit nog niet voldoende ondersteunt. Dit is een Logius breed vraagstuk. De vraag hoe IPv6 geïmplementeerd dient te worden is wederom bij onze architecten ingediend.
SPF (Preventie van mailspoofing/phishing)	Ja	De website van SBR (http://www.sbr-nl.nl) heeft ook een mailserver. Deze voldoet aan SPF (zie: https://internet.nl/mail/sbr-nl.nl/).
STARTTLS/ DANE (Beveiligd, versleuteld mailverkeer)	Nee	Aan STARTTLS en DANE wordt nog niet voldaan. Dit stond gepland voor Q1 2019 en nieuwe planning volgt in Q4 2019.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De verbinding alleen mogelijk voor voldoende veilige TLS-versies (zie: https://internet.nl/site/www.sbr-nl.nl/#). In geval van Digipoort geldt voor de markt bij koppelvlak WUS en ebMS dat TLS 1.2 de standaard is. TLS 1.0 (en mogelijk ook 1.1) is uitgefaseerd. SSL v3 en v3.1 zijn in 2015 uitgefaseerd. Het koppelvlak Grote Berichten 3.0 worden op TLS 1.0 en TLS 1.1 aangeboden. TLS 1.0 en TLS 1.1 worden nog uitgefaseerd.

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

		Document en (web/app)content
Ades Baseline Profiles (Digitaal ondertekenen van documenten)	Ja	Binnen SBR (Assurance) waarbij bijvoorbeeld jaarverslagen worden ondertekend door een accountant, wordt binnen DigiPoort gebruik gemaakt van XAdES als EU standaard.
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/archivering)	Ja	Bij het publiceren van documenten houdt Logius voor SBR PDF/A aan bij publicatie.
		E-facturatie en administratie
XBRL (Bedrijfs-rapportages)	Ja	SBR maakt gebruik van XBRL.

Ten opzichte van 2018 is de status van DKIM, DMARC en STARTTLS/DANEvan gepland naar nee gegaan. De status van IPv4 en IPv6 ging van ja naar deels. De voorziening voldoet aan HTTPS en HSTS. Deze standaard is nieuw opgenomen.

Concluderend moet SBR de volgende standaarden nog (volledig) implementeren: DKIM, DMARC, IPv4 en IPv6, STARTTLS/DANE.

5.3 Digipoort

Beheerorganisatie: Logius

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

Omdat Digipoort slechts machine-naar-machine koppelingen levert en niet toegankelijk is vanaf het openbare internet, is deze voorziening niet getoetst met de toetsen van internet.nl.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	Digipoort maakt gebruik van de e-mailserver uit de centrale voorziening EASI. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. DKIM is geïmplementeerd op de centrale voorziening mail relay.
DMARC (Anti-phishing)	Gepland	Planning voor de implementatie van DMARC was Q1 2019, als onderdeel van een Logius breed project voor Domein verhuizing. Deze planning is niet gehaald, nu is deze wijziging ingepland voor Q3 2019.
DNSSEC	Gepland	Implementatie van DNSSEC zou plaatsvinden in Q1 2019 en is nu deels aanwezig en wordt deels ingepland voor Q3 2019.

(Beveiligde domeinnamen)		
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	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 (Internetnummers)	Nee	Digipoort gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik niet. IPv6 kan niet worden aangeboden, omdat de infrastructuur van Logius dit nog niet voldoende ondersteund. Dit is een Logius breed vraagstuk. De vraag hoe IPv6 geïmplementeerd dient te worden is wederom bij onze architecten ingediend. Digipoort ondersteunt IPv4. Implementatie van IPv6 stond gepland voor Q1 2019 maar dient opnieuw te worden ingepland.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	DigiPoort voldoet aan de BIR. Leveranciers voldoen aan ISO 27001 of een vergelijkbare standaard.
SPF (Preventie van mailspoofing/phishing)	Gepland	DigiPoort heeft geen SPF-records. Er wordt niet gemaild vanuit dit domein, maar SPF zou wel ingericht moeten worden. De planning van Q1 2019 is niet gehaald en de standaard wordt ingericht in Q3/Q4 2019.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Digipoort ondersteunt TLS v1.2, maar niet meer de verouderde versies.
		Stelselstandaarden
Digikoppeling (Veilige berichten-uitwisselingen)	Ja	Digipoort voldoet aan deze standaard. Zie de koppelvlakspecificaties op http://www.logius.nl/producten/gegevensuitwisseling/digitpoort/koppelvlakken.
		E-facturatie en administratie
SETU (Informatie flexibele arbeidskrachten)	Ja	DigiPoort ondersteunt de uitwisseling van SETU-hr-XML berichten.
XBRL en Dimensions (Bedrijfsrapportages)	Ja	De standaard wordt ondersteund door Digipoort.

De situatie ten opzichte van 2018 is gewijzigd, vanwege een belangrijke migratie is er sprake van een ‘Freeze’ periode geweest. Hierdoor zijn de noodzakelijke wijzigingen na deze migratie opnieuw gepland en delen hiervan recent opgeleverd dit betreft DMARC, DNSSEC en SPF. Wijzigingen worden momenteel op de verschillende domeinen uitgevoerd. Verder ging IPv4 en IPV6 ging van gepland naar nee.

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

5.4 Diginetwerk

Beheerorganisatie: Logius

Werking en inhoud van Diginetwerk
Diginetwerk is een afsprakenstelsel en bestaat uit een beschreven samenwerking, normenkaders, handhavingsmechanismen, toetredingseisen en een set van standaarden. Diginetwerk is opgebouwd uit een aantal aan elkaar gekoppelde besloten overheidsnetwerken, waarover overheden gegevens veiliger (vertrouwelijkheid en beschikbaarheid) met andere overheden kunnen uitwisselen dan via het internet. Een belangrijk onderdeel van Diginetwerk is de Koppelnet Publieke Sector (KPS) voorziening, welke de fysieke koppeling tussen de diverse deelnemers verzorgt.

De binnen Diginetwerk toegepaste set standaarden heeft betrekking op het transport van data (netwerk standaarden), standaarden op applicatie- of gegevensniveau maken geen onderdeel uit van het afsprakenstelsel. Logius is als regievoerder/beheerder van het afsprakenstelsel in gesprek met het Forum Standaardisatie en deelnemers om de relevante standaarden van de PTOLU-lijst binnen Diginetwerk toe te passen. Standaarden worden toegepast als die een toegevoegde waarde hebben binnen het besloten netwerkstelsel en door de deelnemers geïmplementeerd kunnen worden zonder afbreuk te doen aan het besloten karakter.

Bij deze toetsing is voorlopig niet gekeken naar de standaarden in de hoger gelegen lagen van het OSI-model.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DNSSEC (Beveiligde domeinnamen)	Gepland	DNSSEC valt voor het besloten netwerk buiten het afsprakenstelsel. Een aantal deelnemers maakt echter gebruik van de diginetwerk domeinnamen om ook op het openbare internet hun dienst ter beschikking te stellen. Hiervoor is besloten wel gebruik te maken van DNSSEC. Gepland voor 2020.
IPv4 en IPV6 (Internetnummers)	Gepland	IPv4 is geïmplementeerd door de deelnemers aan Diginetwerk. De implementatie van IPv6 stond gepland voor Q4 2018 en wordt 2020. Vanwege aanbesteding KPS (koppelpunt van Diginetwerk) is ondersteuning van IPv6 gepland als onderdeel van de migratie naar de nieuwe KPS leverancier.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Deze standaard is onderdeel van het algemene beveiligingsbeleid van Logius. Logius voldoet aan deze standaard en Diginetwerk is ook gebaseerd op deze standaard.

Ten opzichte van 2018 is de standaard DMARC afgevoerd i.v.m. relevantie. Diginetwerkdomein gebruik op internet voldeed in 2018 aan DNSSEC, maar voldoet in 2019 niet aan DNSSEC. De dns leverancier is verzocht dit verder te onderzoeken en op te lossen. Gepland voor 2020. De planning van IPv4 en IPv6 is verschoven.

Concluderend, moeten voor het besloten Diginetwerk nog de volgende standaarden (volledig) worden geïmplementeerd: IPv6. Voor het gebruik van diginetwerk domeinnamen op internet moeten de volgende standaarden (volledig) worden geïmplementeerd: DNSSEC.

5.5 Tenderned

Beheerorganisatie: PIANOo/DICTU

Werking en inhoud van Tenderned
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 beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	E-mails verzonden vanuit TenderNed zijn beveiligd met DKIM (zie: https://internet.nl/mail/tenderned.nl/).
DMARC (Anti-phishing)	Nee	Tenderned voldoet niet aan DMARC.
DNSSEC (Beveiligde domeinnamen)	Ja	Het domein is gesigned met DNSSEC (zie: https://internet.nl/site/www.tenderned.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Nee	De client-server communicatie van TenderNed is beveiligd met HTTPS, maar niet met HSTS (zie: https://internet.nl/site/www.tenderned.nl/).
IPv4 en IPV6 (Internetnummers)	Nee	Tenderned.nl is zowel in 2018 als in 2019 niet voorbereid op IPv6 (zie: https://internet.nl/site/www.tenderned.nl/). TenderNed is afhankelijk van de hostingpartij. Wanneer deze een transitie door maakt naar IPv6 zal TenderNed daarin mee gaan.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	TenderNed is ISO27001/2 gecertificeerd. Dit wordt jaarlijks geaudit.
SAML (Inloggegevens)	Ja	Per 1 juli 2014 is het mogelijk voor gebruikers om, naast de huidige registreer- en inlogmogelijkheden, gebruik te maken van inloggen via eHerkenning. (Bron: http://www.tenderned.nl/eherkenning-en-tenderned-0)
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is inmiddels aangezet door de technisch dienstverlener DICTU. (Zie: https://internet.nl/mail/tenderned.nl/140321/#mailauth).
STARTTLS en DANE	Ja	STARTTLS en DANE worden ondersteund.

(Beveiligd, versleuteld mailverkeer)		
TLS (Beveiligde, versleutelde verbindingen)	Ja	TenderNed past TLS 1.2 toe (zie: https://internet.nl/site/www.tenderned.nl/). Voor een aantal koppelingen wordt nog TLS 1.0 gebruikt voor compatibiliteit.
		Document en (web/app)content
Open API Specification (Beschrijven van REST API's)	Nee	De publieke API's worden beschreven door middel van Swagger. Swagger kan je zien als OAS versie 2.0. Swagger als API Specificatie bestaat niet meer en is opgegaan in OAS. Tenderned voldoet daarmee niet aan OAS 3.0. Deze versie is belangrijk omdat deze samenhang aanbrengt in de verschillende manieren om API specificaties op te stellen.
PDF 1.7, PDF/A-1, PDF/A-2 (Documentpublicatie/ archivering)	Ja	Geautomatiseerd gecreëerde PDF's (bij de aankondigingen) zijn gemaakt in versie 1.7.

Ten opzichte van vorig jaar voldoet Tenderned aan DKIM en STARTTLS/DANE. De statussen zijn gegaan van nee naar ja. Verder voldoet de voorziening niet meer aan HSTS waardoor de status van de standaard HTTPS/HSTS van ja naar nee gaat.

Concluderend moeten voor Tenderned nog de volgende standaarden (volledig) worden geïmplementeerd: DMARC, HTTPS en HSTS, IPv4 en IPV6, Open API Specification.

5.6 DWR

Beheerorganisatie: Ministerie BZK

Werking en inhoud van DWR
De Digitale Werkomgeving Rijksdienst (DWR) is de ICT-werkomgeving voor rijksambtenaren. Deze werkomgeving is een onderdeel van de dienstverlening van SSC-ICT. SSC-ICT ontwikkelt en beheert DWR voor een groot aantal ministeries. De digitale werkomgeving bestaat uit verschillende onderdelen voor infrastructuur en connectiviteit. De drie belangrijkste zijn de uniforme digitale werkomgeving voor ambtenaren (DWR Next client), één website voor overheidsinformatie en diensten (rijksoverheid.nl), en gebruik van web 2.0 toepassingen om beter en sneller samen te werken. Komende jaren wordt de technologie verder geïntegreerd en zullen in afstemming met de afnemers van de dienstverlening de standaarden verder worden ingevuld; in 2019 worden onder meer de afnemers uit het domein van het Ministerie van Justitie en Veiligheid voorzien van de DWR Next Client.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	De implementatie van DKIM is voor SSC-ICT zelf geheel afgerond.
DMARC (Anti-phishing)	Nee	De technische implementatie van DMARC is afgerond. Het doorvoeren van de DMARC *reject policy* moet nog worden uitgevoerd, maar dit kan nog niet voor (een aantal) externe applicaties die mailen of klanten die gebruik maken van externe mailingdiensten. Open staat derhalve nog het

		aanbieden van een dienst hiervoor. SSC-ICT is voor realisatie van deze dienst afhankelijk van de betreffende klanten. De inrichting van deze dienst wordt projectmatig opgepakt; dit project bevindt zich op dit moment in de initiatiefase.
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC is geïmplementeerd en alle domeinnamen die bij SSC-ICT gehost worden voldoen aan DNSSEC.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Gepland	HTTPS wordt gebruikt, maar HSTS wordt nog niet standaard aangezet voor websites die SSC-ICT host voor klanten. Andere webgebaseerde voorzieningen maken wel gebruik van HSTS. Implementatie van deze standaarden is voor eind 2019 voorzien.
IPv4 en IPV6 (Internetnummers)	Gepland	IPv4 is in gebruik. De gebruikte technische componenten van DWR ondersteunen wel IPv6. IPv6 is een onderdeel van de infrastructuur en IPv6 reeksen worden uitgedeeld door Logius. De internet facing kant van de DMZ gaat IPv6 eind 2019 ondersteunen.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	SSC-ICT werkt via deze standaard en wordt hier ook op geaudit. De laatste audit heeft plaatsgevonden in 2019.
SAML (Inloggegevens)	Ja	Single Sign-on (SSO) op basis van SAML 2.0 wordt aangeboden als dienst in de Servicecatalogus van SSC-ICT. Het SSO-koppelvlak is een generieke dienst. Het project DOorontwikkeling Single Sign-On (DOrSSOn) voorziet internet facing aanvulling van de huidige oplossing met open source componenten gebaseerd op de standaarden SAML 2.0 en OAuth 2.0 in opdracht van de CIO Rijk.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF wordt op alle domeinen toegepast.
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Ja	STARTTLS en DANE zijn geïmplementeerd.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De op de werkplek aangeboden browsers ondersteunen TLS. De internet mailvoorziening werkt met STARTTLS. Voor webservers met applicaties van klanten wordt dit toegepast voor de klanten die dit hebben aangevraagd.
WPA2 Enterprise (Toegang tot een WiFi-netwerk met account)	Ja	Op de wifivoorziening wordt deze standaard toegepast. Wifi wordt door SSC-ICT als voorziening geleverd in de kantoorpanden waar SSC-ICT IT-dienstverlener voor het pand is (IDV-P).
		Document en (web/app)content
ODF 1.2 (Documentbewerkingen)	Ja	De DWR Next client wordt geleverd met zowel Libreoffice als Office 2016. Beide softwaresuites ondersteunen het lezen en schrijven van ODF-bestanden.
PDF 1.7 / PDF A/1 en PDF A/2 (Documentpublicatie/ archivering)	Ja	De DWR Next client kan alle types PDF lezen. Schrijven van PDF kan op meerdere manieren. Alle types worden ondersteund, al is daarvoor soms wel het installeren van Adobe Acrobat Professional benodigd. PDF A/2 is mogelijk

		voor klanten die Adobe Acrobat Pro afnemen. De regulier verstrekte Adobe Acrobat Standard ondersteunt PDF A/2 niet, maar wel PDF 1.7 en PDF A/1. De scanfunctionaliteit in het reguliere multifunctional printplatform voor de werkomgeving ondersteunt PDF 1.7 en PDF A/1.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Binnen JenV vindt elektronisch berichtenverkeer interdepartementaal plaats via de Justitie Berichten Service (JUBES). JUBES is vanuit JenV het koppelvlak voor de Digikoppelingdienst van Logius. De open standaarden eBMS en WUS zijn de daarbij gebruikte protocollen om de berichten veilig te versturen. Binnen BZ wordt deze standaard gebruikt voor de Mule koppeling. Verder nemen alle departementen uit het verzorgingsgebied van SSC-ICT deel aan eFacturatie. Op deze standaard wordt waar van toepassing aangesloten bij nieuwe koppelingen.

Ten opzichte van 2018 is de status van DMARC van deels naar nee gegaan en is de status van DKIM, DNSSEC en Digikoppeling 2.0 van deels naar ja gegaan. Verder is de status van STARTTLS/DANE van gepland naar ja gegaan. De planning van HTTPS/HSTS en IPv4 en IPv6 is verschoven.

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

5.7 DigiInkoop

Beheerorganisatie: Logius

Werking en inhoud van DigiInkoop
DigiInkoop is een rijksbreed geautomatiseerd inkoopsysteem dat het inkoopproces vereenvoudigt. DigiInkoop is er voor de inkoop van alle producten en diensten, van kantoorartikelen tot inhuur van personeel. Daarnaast biedt de voorziening DigiInkoop een Leverancierssportaal voor Leveranciers van de Rijksoverheid. Hiermee kunnen deze leverancier Offertes, Orders en Facturatie afhandelen, met één inlog voor de hele Rijksoverheid.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	De standaard DKIM is geïmplementeerd. (zie: https://internet.nl/mail/digiinkoop.nl/).
DMARC (Anti-phishing)	Ja	De standaard DMARC is geïmplementeerd (zie: https://internet.nl/mail/digiinkoop.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	DigiInkoop voldoet aan DNSSEC (zie: https://internet.nl/mail/digiinkoop.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening voldoet aan HTTPS/HSTS. Zie https://internet.nl/site/digiinkoop.nl/)
IPv4 en IPV6 (Internet-nummers)	Nee	IPv6 werd in 2016, 2017 en 2018 niet ondersteund door de hoster van DigiInkoop. Er zijn geen plannen dit te realiseren, en er is geen opdracht om dit aan te passen. (zie: https://internet.nl/mail/digiinkoop.nl/).

NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	DigiInkoop voldoet aan de BIR. Er is een in control statement afgegeven. Leveranciers voldoen aan ISO 27001.
SPF (Preventie van mailspoofing/phishing)	Ja	DigiInkoop voldoet aan deze standaard. (zie: https://internet.nl/mail/digiinkoop.nl/).
TLS (Beveiligde, versleutelde verbindingen)	Ja	DigiInkoop is TLS 1.2 compliant (zie: https://internet.nl/mail/digiinkoop.nl/).
		Document en (web/app)content
PDF/A en PDF 1.7 (Documentpublicatie/archivering)	Ja	De DigiInkoop 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 DigiInkoop gebruik van maakt: https://www.logius.nl/ondersteuning/gegevensuitwisseling/ubl-ohnl en https://www.logius.nl/ondersteuning/gegevensuitwisseling/setu-hr-xml-ohnl).
		E-facturatie en administratie
NLCIUS (Elektronisch factureren)	Nee	Per 19 april 2019 is de NLCIUS verplicht voor overheden, volgens Europese richtlijn 2014/55/EU. De SMEF 2.0 standaard wordt opgevolgd door de NLCIUS. Implementatie stond gepland voor Q2 2019. Er is gekozen voor een tijdelijke tussenoplossing om aan de Europese richtlijn te voldoen, er zijn geen concrete plannen voor implementatie, de verwachting is dat het Q2 2020 gereed is.
SETU (Informatie flexibele arbeidskrachten)	Ja	DigiInkoop ondersteunt de uitwisseling van SETU-hr-XML berichten.

Ten opzichte van 2018 zijn de DKIM, DMARC en SPF standaard geïmplementeerd, de status is van gepland naar ja gegaan. De status van de standaard NLCIUS is van gepland naar de status nee gegaan.

Concluderend, moet DigiInkoop nog de volgende standaarden (volledig) implementeren: IPv4 en IPV6 , NLCIUS.

Bijlage A Geïnterviewde personen

Naam voorziening	Contactpersoon
BAG, WOZ, BGT, BRK	Koen Huisstede
Berichtenbox voor bedrijven	Dick Bruinsma, Laura Ouwehand
BRI	Henk Heerink, Harry Roumen
BRO	Erik van der Zee, Marjan Bevelander
BRT	Koen Huisstede
BRV	Gert Stel, Walter Huberts
BSN en GBA-V	Bob te Riele, Hans van laar
DigiInkoop	Güldeniz Özdemir Isik, Erwin Kaats
DigiD	Evert-Jan van der Marck
DigiD Machtigen	Güldeniz Özdemir Isik, Erwin Kaats
Digilevering	Güldeniz Özdemir Isik, Erwin Kaats
Digimelding	Güldeniz Özdemir Isik, Erwin Kaats
Diginetwerk	Glenn Lutke Schipholt
DigiPoort	Güldeniz Özdemir Isik, Erwin Kaats
Doc-Direkt	Ali Amin Shahidi
DWR	Rein Hennen, Cees Vaes, Paul Slats, Jan Pothof
eFactureren	Güldeniz Özdemir Isik, Erwin Kaats
Stelsel elektronische toegangsdiensten	Güldeniz Özdemir Isik, Erwin Kaats
MijnOverheid	Güldeniz Özdemir Isik, Erwin Kaats
NHR	Rob Spoelstra
ODC Noord	Jaap Jansma
Ondernemersplein	Elie Mokheiber
Overheid.nl	Lucien de Moor, Hans Overbeek
P-Direkt	Richard Schop, Eric van der Ende
PKI Overheid	Güldeniz Özdemir Isik, Erwin Kaats
Rijksoverheid.nl	Cees den Heijer, Gerrit Berkouwer, Cees Vaes
Rijkspas	Jacqueline Vlietland
Rijksportaal	Marvin Kramer, Marc van Hilvoorde
Samenwerkende Catalogi	Güldeniz Özdemir Isik, Erwin Kaats
SBR	Güldeniz Özdemir Isik, Erwin Kaats
Stelselcatalogus	Gerben Stevens
Tenderned	Rudi van Eijk

Bijlage B Lijst verplichte open standaarden

Standaard
Ades Baseline Profiles
Aquo-standaard
BWB
CMIS
COINS
Digikoppeling
DKIM
DMARC
DNSSEC
E-Portfolio NL
ECLI
EML_NL
Geo-Standaarden
HTTPS en HSTS
IFC
IPv6 en IPv4
JCDR
NEN-ISO/IEC 27001
NEN-ISO/IEC 27002
NL LOM
NLCIUS
NLCS
ODF
OpenAPI Specification
OWMS
PDF (NEN-ISO)
SAML
SETU
SIKB0101
SIKB0102
SKOS
SPF
STARTTLS en DANE
STIX en TAXII
StUF
TLS
VISI
WDO Datamodel
WPA2 Enterprise
XBRL