PBLQ

Monitor Open Standaarden Voorzieningen 2018

Versie 1.1
30-11-2018

PBLQ
verbinders in de informatiesamenleving

Inhoudsopgave

1. Inleiding 1

1.1 Aanleiding 1
1.2 Opdrachtformulering 1
1.3 Werkwijze 1
1.4 Aandachtspunten voor de lezer 2
1.4.1 Voorzieningen en standaarden geordend op basis van functionaliteit 2
1.4.2 Status 2
1.4.3 Relevantie standaard 2
1.4.4 Wijze van toetsen standaard 3

2. Identificeren en authenticeren 5

2.1 DigiD 5
2.2 DigiD Machtigen 6
2.3 PKIoverheid 8
2.4 Beheervoorziening BSN en GBA-V 10
2.5 Rijkspas 11
2.6 Stelsel elektronische toegangsdiensten 13

3. Dienstverlening en informatieverstrekken 14

3.1 MijnOverheid 14
3.2 Berichtenbox voor bedrijven 17
3.3 Overheid.nl 18
3.4 Ondernemersplein 20
3.5 Samenwerkende catalogi 22
3.6 Rijksportaal 23
3.7 ODC Noord 24
3.8 Doc-Direkt 26
3.9 Rijksoverheid.nl 28

4. Gegevens en registreren 30

4.1 Basisregistraties 30
4.1.1 NHR (Handelsregister) 30
4.1.2 BAG (Basisregistraties Adressen en Gebouwen), BRK (Basisregistratie Kadaster), BGT (Basisregistratie Grootschalige Topografie), WOZ (Basisregistratie Waarde Onroerende Zaken) 32
4.1.3 BRT (Basisregistratie Topografie) 35
4.1.4 BRV (Basisregistratie Voertuigen) 37
4.1.5 BRI (Basisregistratie Inkomen) 39

4.2 Digilevering 40
4.3 Digimelding 41
4.4 Stelselcatalogus 43
4.5 P-Direkt 44

5. Dienstverlening en verbinden 47

5.1 eFactureren 47
5.2 SBR 47
5.3 Digipoort 49
5.4 Diginetwerk 50
5.5 Tenderned 51
5.6 DWR 53
5.7 Digi-Inkoop 55

Bijlage A Geïnterviewde personen 58

PBLQ
verbinders in de informatiesamenleving

1. Inleiding

1.1 Aanleiding

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

1.2 Opdrachtformulering

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

1.3 Werkwijze

Voor dit onderzoek is gebruik gemaakt van de 'pas toe of leg uit'-lijst van 1 mei 2018. 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. 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. 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

In tegenstelling tot vorig jaar zijn de voorzieningen in deze monitor op basis van functionaliteit gegroepeerd conform de indeling die eerder in de Monitor Generieke Digitale Infrastructuur 2018 is gehanteerd. De volgende functionele groepen worden in deze monitor onderscheiden:

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

Omdat niet alle voorzieningen die in dit onderzoek worden getoetst zijn opgenomen in de Monitor Generieke Digitale Infrastructuur 2018 zijn de overige voorzieningen ingedeeld in bovenstaande categorieën in overleg met de opdrachtgever.

Ook de ordening van de standaarden in de tabellen is dit jaar anders dan voorheen. Op verzoek van de opdrachtgever is de volgorde van de flyer[1] met het overzicht van 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[2] de standaard,
- Nee: De voorziening is niet conform de standaard,
- Deels: Onderdelen van de voorziening zijn conform aan, maar niet alle onderdelen[3],
- 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.[4] 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

[1] https://www.forumstandaardisatie.nl/sites/bfs/files/Lijst_verplichte_open_standaarden_juli_2018_1.pdf

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

[3] 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.

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

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.

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 een volledig en accuraat beeld op te leveren.

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[5] 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
- HSTS
- HTTPS
- DMARC
- DKIM
- SPF
- STARTTLS
- TLS
- DANE

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 naar waar dit aan kan liggen.

Webrichtlijnen en Digitoegankelijk
Op 24 mei is het Tijdelijk besluit digitale toegankelijkheid overheid gepubliceerd in het Staatsblad. Het besluit, dat de Europese toegankelijkheidsrichtlijn (2016/2102) omzet in bindende nationale regelgeving, treedt per 1 juli 2018 in werking. Het doel is om de toegankelijkheid van websites en mobiele applicaties (apps) van overheidsinstanties te waarborgen.

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

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.
Er geldt een gefaseerde toepassing. Nieuwe websites gepubliceerd vanaf 23 september 2018 moeten 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.

In deze monitor zijn we, gelet op de invoeringsdatum van 1 juli 2018 en de gafaseerde invoeringssystematiek zijn we voor dit onderzoek nog uitgegaan van de systematiek voor Webrichtlijnen. Concreet: is er een toets uitgevoerd en is er een onderbouwing in de vorm van een toetsingsrapport, een beschrijving van de toets, of een verwijzing naar een certificaat van een inspectie-instelling zoals Accessibility of Waarmerk drempelvrij.nl.

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

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

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

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

2. Identificeren en authenticeren

2.1 DigiD

Beheerorganisatie: Logius

Werking en inhoud van DigiD (bron: Monitor GDI 2018)
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 al 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
		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 release 4.5 van DigiD en inmiddels 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 Rijk (BIR) van toepassing die is gebaseerd op NEN-ISO27001. Logius heeft zich over toepassing van deze norm verantwoord door het afgeven van In Control Verklaringen (ICV's) aan de eigenaar (BZK/DGOBR).
SAML (Inloggegevens)	Ja	DigiD biedt aan afnemers een SAML-koppelvlak. De meeste afnemers zitten nog op het A-select koppelvlak. SAML-berichtuitwisseling in het eID stelsel (http://www.eid-stelsel.nl) zal anders zijn dan die van DigiD. Om partijen niet tot meerdere migraties te dwingen houdt DigiD het A-select koppelvlak nog in stand.

SPF (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 toe (zie https://internet.nl/mail/digid.nl/). Planning voor de implementatie van DANE is Q4 2018
TLS (Beveiligde, versleutelde verbindingen)	Ja	DigiD ondersteunt TLS v1.0 en TLS v1.2. TLS 1.1 wordt niet ondersteund, omdat Logius een sterke voorkeur heeft voor TLS 1.2. Om brede comptabiliteit mogelijk te maken wordt TLS 1.0 nog steeds ondersteund.
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Ja	DigiD voldoet aan de WR2-AA richtlijnen van het Waarmerk drempelvrij.nl (zie https://www.digid.nl/toegankelijkheid/). Het certificaat is een jaar geldig. Inspectiedatum is 22 december 2017.

Ten opzichte van 2017 voldoet Digid aan de WR2-AA richtlijnen van het Waarmerk drempelvrij.nl. De STARTTLS/DANE standaard is van de status ‘ja’ naar de status ‘gepland’ gegaan, omdat er een aanstaande implementatie van DANE gepland is voor Q4 2018.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Digid voldoet aan de nieuw opgenomen standaard DMARC. DMARC is voor DigiD geconfigureerd als een van de Anti-phishing maatregelen.

Concluderend, moet voor DigiD de volgende standaard nog (volledig) worden geïmplementeerd: 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. DigiD Machtigen wordt beheerd door Logius. Onderstaande antwoorden zijn grotendeels gebaseerd op de Verantwoording Open Standaarden die jaarlijks door Logius zelf opgesteld wordt.

Standaard	Status	Toelichting
		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) (Richtlijnen en principes 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).
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 aansluiting op het eID stelsel. 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 v1.2, v1.1 en v1.0 (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
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Gepland	Wijzigingen ten behoeve van Digitoegankelijk compliance zijn in Q2 2018 geïmplementeerd. In Q3 wordt dit getoetst door betrokken partijen.

(Toegankelijkheid web content)		
PDF/A en PDF 1.7 (Documentpublicatie/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.

Ten opzichte van 2017 zijn wijzigingen ten behoeve van Digitoegankelijk in Q2 2018 geïmplementeerd. In Q3 2018 wordt dit getoetst door betrokken partijen. De status is verhoogd van nee naar gepland.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Deze standaard is geïmplementeerd.

Concluderend, moeten voor Digid Machtigen nog de volgende standaarden (volledig) worden geïmplementeerd: Digikoppeling 2.0, Digitoegankelijk (EN 301 549 met WCAG 2.0), SAML v2.0.

2.3 PKIoverheid

Beheerorganisatie: Logius

Werking en inhoud van PKIoverheid (bron: Monitor GDI 2018)
Wat DigiD en eHerkenning zijn voor respectievelijk burgers en bedrijven, is PKIoverheid voor de overheid, PKIoverheid bevat de digitale certificaten die door zogenaamde Trust Service Providers (TSP's) beschikbaar worden gesteld aan overheidsorganisaties, opdat zij veilig met elkaar kunnen communiceren.
Met PKIoverheid wordt de betrouwbaarheid van informatie-uitwisseling via e-mail en websites op basis van Nederlandse (en Europese) wetgeving geborgd. Er zijn zeven TSP's die PKIoverheidscertificaten verstrek- ken. Dit zijn: KPN, ESG, QuoVadis, Digidentity, CIBG, het Ministerie van Infrastructuur en Waterstaat en het Ministerie van Defensie.

Standaard	Status	Toelichting
		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)	Ja	Deze standaard wordt toegepast door de voorziening (zie: https://internet.nl/domain/crl.pkioverheid.nl/ en https://internet.nl/domain/www.logius.nl/).
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 is gepland voor Q4 2019.
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.
TSL 1.2 en 1.1	Ja	Het PKIoverheid deel van de website van Logius maakt gebruik van TLS 1.1 en 1.2 en de website van PKIoverheid zelf maakt gebruik van TLS 1.2 (zie: https://internet.nl/domain/crl.pkioverheid.nl/ 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 2017 is er een concrete planning voor de implementatie van IPv6 in Q4 2019.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. PKIoverheid voldoet aan de standaard DMARC.

Concluderend, moet voor PKIoverheid nog de volgende standaarden (volledig) worden geïmplementeerd: 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 centsrale, 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
		Internet en beveiliging
HTTPS/HSTS (Beveiligd, Versleuteld Webverkeer)	Ja	Alle aangeboden webservices draaien HTTPS en HSTS.
IPv4 en IPV6 (Bereikbaarheid nieuwe Internetnummers)	Nee	De voorzieningen zijn IPv6-ready in datacentrum, maar er wordt momenteel gebruik gemaakt van IPv4 adressen via Gemnet/Diginetwerk. Het is nog niet bekend wanneer er met het ontsluiten op IPv6 zal worden begonnen. Wel is inmiddels de ontsluiting via DigiNetwerk begonnen.
NEN-ISO/IEC 27001/27002 (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 v1.2, v1.1 en v1.0 (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 BRP bezinningsproces is de planning onduidelijk. Ontsluiting van BV-BSN middels Digikoppeling zal niet plaatsvinden. Gebruik van beide voorzieningen verloopt via besloten netwerken, meer specifiek en voornamelijk Gemnet/Diginetwerk. Aansluitingen op Diginetwerk zijn inmiddels gerealiseerd en zijn richting gemeenten en afnemers gecommuniceerd.

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 2017 zijn er geen wijzigingen anders dan dat over de aansluitingen met het diginetwerk inmiddels is gecommuniceerd met gemeenten en afnemers.

Van de standaarden die in 2018 nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) zijn er geen relevant voor BSN Beheervoorziening en GBA-V.

Concluderend moet voor de BSN Beheervoorziening en GBA-V nog (volledig) worden geïmplementeerd: Digikoppeling 2.0, IPv4 en IPV6, StUF.

2.5 Rijkspas

Beheerorganisatie: Ministerie van BZK

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

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

Standaard	Status	Toelichting
		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 planning van Q3 2018 voor verhuizing van de Rijkspassystemen naar een nieuw datacenter waar DKIM wel toegepast zal worden is door de leverancier uitgesteld naar Q4 2018.
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 staat gepland voor Q1 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 de 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 v1.2, v1.1 en v1.0 (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 2017 is de implementatie van DKIM, STARTTLS/DANE, DNSSEC vertraagd vanwege de afhankelijkheid met de verhuizing naar een nieuw datacenter.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. P-direkt is afhankelijk van SSC-ICT voor implementatie van de standaard. De status hiervan is onbekend.

Concluderend, moeten voor de Rijkspas nog de volgende standaarden (volledig) worden geïmplementeerd: DKIM, DNSSEC, DMARC, 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 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
		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 wordt voor Q1 2019 aangescherpt.
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)	Ja	Beide voorzieningen voldoen aan IPv4 en IPv6.
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 controlstatement beschikbaar.
SAML (Inloggegevens)	Ja	SAML is een verplichte eis vanuit het stelsel.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF wordt toegepast bij de voorziening, maar wordt vooralsnog niet vereist als toe te passen techniek voor deelnemers.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Nee	STARTTLS is geïmplementeerd voor eherkenning.nl en idensys.nl. De implementatie van DANE is in zowel 2017 als 2018 nog onderwerp van onderzoek. Hier is nog geen concrete planning voor.

TLS v1.2, v1.1 en v1. (Beveiligde, versleutelde verbindingen)	Ja	Het afsprakenstelsel stelt het gebruik van TLS1.x verplicht.
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Ja	Digitoegankelijk (EN 301 549 met WCAG 2.0) is een eis vanuit het stelsel aan de deelnemers. Bij vermoeden van non-conformiteit kan een toets worden opgestart. De website voor eHerkenning.nl, onder beheer van de beheersorganisatie zelf, voldoet en is getoetst conform WCAG 2.0 (AA): https://www.accessibility.nl/ondersteuning/inspectie/site-1497. Voor Idensys staat dit gepland (mede afhankelijk van besluitvorming).
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 2017 zijn IPv4 en IPv6 geïmplementeerd.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Implementatie van DMARC staat gepland voor Q1 2019.

Concluderend, moeten voor het Stelsel Elektronische toegangsdiensten nog de volgende standaarden (volledig) worden geïmplementeerd: DMARC, STARTTLS en DANE.

3. Dienstverlening en informatieverstrekken

3.1 MijnOverheid

Beheerorganisatie: Logius

Werking en inhoud van MijnOverheid (bron: Monitor GDI 2018)
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
		Internet en beveiliging
DKIM (Preventie van mailspoofing/ phishing)	Ja	MijnOverheid voldoet aan DKIM (zie: https://internet.nl/mail/mijnoverheid.nl/).
DMARC (Anti-phishing)	Ja	Deze standaard wordt toegepast.
DNSSEC (Beveiligde domeinnamen)	Ja	MijnOverheid voldoet aan DNSSEC (zie: https://internet.nl/site/mijnoverheid.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	Deze standaard wordt toegepast (zie: https://internet.nl/mail/mijnoverheid.nl/).
IPv4 en IPV6 (Internetnummers)	Nee	Mijnoverheid gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik. Mijnoverheid ondersteunt op dit moment alleen IPv4. De verwachting is dat implementatie van IPv6 in Q4 2018 kan worden opgepakt maar deze plannen zijn nog niet concreet.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes 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 deze norm verantwoord 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 v1.2, v1.1 en v1.0 (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
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Ja	De laatste Webrichtlijnentoets is door Stichting Accessibility uitgevoerd (niet meer door Centric zoals voorheen). De toegankelijkheidsverklaring moet nog geplaatst worden.
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 ondersteunt het genoemde PDF formaat, maar controleert hier niet op. MijnOverheid genereert zelf geen PDF files. In 2016 is een impact-analyse uitgevoerd om te onderzoeken wat het betekent wanneer men PDF-bijlages wel gaat controleren en wat eventuele vervolgacties zijn. Er is toen besloten om niet op formaat te gaan controleren.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisseling en)	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 2017 voldoet MijnOverheid geheel aan Digikoppeling 2.0. De status is verhoogd van deels naar ja. MijnOverheid voldoet aan de Digitoegankelijk (EN 301 549 met WCAG 2.0) standaard. Er is een webrichtlijnen toets uitgevoerd. De status is verhoogd van gepland naar ja. Ten opzichte van 2017 is de relevantie van de OWMS standaard door de beheerder getoetst. De standaard is niet van toepassing bevonden.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) zijn DMARC en Open API Specification relevant. DMARC en Open API Specification zijn geïmplementeerd.

Concluderend, moet MijnOverheid nog de volgende standaard (volledig) implementeren: IPv4 en IPV6.

3.2 Berichtenbox voor bedrijven

Beheerorganisatie: Rijksdienst voor Ondernemend Nederland (RVO).

Inhoud en werking Berichtenbox voor bedrijven (Bron: Monitor GDI 2018)
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.

Standaard	Status	Toelichting
		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 niet bekend.
SAML (Inloggegevens)	Ja	eHerkenning is SAML-based en wordt toegepast voor het inloggen op de Berichtenbox.
SPF (Preventie van mailspoofing/phishing)	Nee	SPF is niet geïmplementeerd (zie https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/).
TLS v1.2, v1.1 en v1.	Ja	De Berichtenbox maakt gebruik van TLS 1.2 (zie: https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/).

(Beveiligde, versleutelde verbindingen)		
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Nee	Dictu heeft een webrichtlijnen toets gedaan. Een concrete planning voor implementatie van de standaard is nog niet bekend.
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 2017 is HSTS nu afgedwongen door de frontend servers. De status van HTTPS/HSTS is verhoogd van nee naar ja. Voor de standaarden die sinds vorig jaar nog geïmplementeerd moeten worden zijn geen data bekend.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Echter voldoet de BerichtenBox voor Bedrijven niet aan DMARC. Deze standaard is mede afhankelijk van SPF en DKIM, welke niet ondersteund worden door de BerichtenBox voor Bedrijven.

Concluderend, moet BerichtenBox voor Bedrijven nog de volgende standaarden (volledig) implementeren: Digitoegankelijk (EN 301 549 met WCAG 2.0), DKIM, DMARC, IPv4 en IPv6, SPF.

3.3 Overheid.nl

Beheerorganisatie: Kennis- en Exploitatiecentrum Officiële Overheidspublicaties (KOOP)

Werking en inhoud van overheid.nl (bron: Monitor GDI 2018)
Overheid.nl biedt centrale internettoegang (website) 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.

Standaard	Status	Toelichting
		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 behoudens DMARC policy gepland medio 2018.
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	Het portaal-gedeelte (www.overheid.nl) voldoet aan de standaard (zie https://internet.nl/site/www.overheid.nl/), behoudens HTTP-compressie, gepland medio 2018. Een restant sub-domeinen zal uiterlijk eind 2018 aan deze standaarden voldoen. Alleen wetten.overheid.nl voldoet nog niet. Dit wordt met de laatste toegankelijkheidsupdate in de zomer van 2018 uitgevoerd.
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 v1.2, v1.1 en v1.0 (Beveiligde, versleutelde verbindingen)	Gepland	Deze standaard is doorgevoerd, behoudens Client-initiated renegotiation, dit staat gepland voor medio 2018 (zie: https://internet.nl/site/www.overheid.nl/).
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Gepland	Er is een toegankelijkheidsverklaring conform EN 301459. De nieuwe eisen van deze nieuwe richtlijn zijn meegenomen in de vernieuwing van Overheid.nl. Deze is maart 2018 als beta live gegaan. M.b.t. toegankelijkheid is een onafhankelijk onderzoek uitgevoerd. Toegankelijkheidsverklaring zal geplaats worden na afronding beta-fase medio 2018.
OWMS	Ja	Overheid.nl is gemetadateerd conform OWMS.

(Metadata overheidsinformatie)		
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 2017 vindt volledige implementatie van HTTPS en HSTS plaats in 2018 i.p.v. 2017. De status blijft vooralsnog gehandhaafd op gepland. Daarnaast zijn ten op zichte van 2017 de standaarden BWB en JCDR opgenomen. Overheid.nl is de bron van de JCDR identifiers en is de bron van de BWB identificatie.

Van de standaarden die in 2018 nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Overheid.nl voldoet aan DMARC.

Concluderend moeten voor overheid.nl nog (volledig) worden geïmplementeerd: Digitoegankelijk (EN 301 549 met WCAG 2.0), HTTPS en HSTS, TLS v1.2, v1.1 en v1.0.

3.4 Ondernemersplein

Beheerorganisatie: Kamer van Koophandel

Werking en inhoud van Ondernemersplein (bron: Monitor GDI 2018)
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.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	DKIM is geïmplementeerd (zie: https://internet.nl/mail/ondernemersplein.nl/).
DMARC (Anti-phishing)	Ja	Ondernemersplein.nl voldoet aan DMARC (zie: https://internet.nl/mail/ondernemersplein.nl/).

DNSSEC (Beveiligde domeinnamen)	Ja	De standaard is geïmplementeerd op de nieuwe DNS omgeving.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	Aan deze standaard wordt voldaan (zie: https://internet.nl/site/www.ondernemersplein.nl/).
IPv4 en IPV6 (Internetnummers)	Ja	De website ondersteunt IPv4 en is toegankelijk via IPv6 (zie: https://internet.nl/site/www.ondernemersplein.nl/).
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. Nieuwe toetsing vindt plaats in februari 2019.
SPF (Preventie van mailspoofing/phishing)	Ja	Er wordt aan deze standaard voldaan (zie: https://internet.nl/mail/ondernemersplein.nl/).
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Nee	Aan STARTTLS wordt voldaan, maar aan DANE wordt nog niet voldaan. De KvK geeft aan nog te moeten onderzoeken of hieraan voldaan zal worden. Er is nog geen concreet onderzoekstraject gedefinieerd.
TLS v1.2, v1.1 en v1. (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.
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Ja	Verklaring is beschikbaar. Meer informatie beschikbaar op: https://www.ondernemersplein.nl/toegankelijkheid/. De laatste toets is uitgevoerd in mei 2018.
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 2017 voldoet ondernemersplein aan DNSSEC en TLS. De status van DNSSEC is verhoogd van gepland naar ja. De status van TLS is verhoogd van nee naar ja. De SKOS standaard is ten opzichte van 2017 verwijderd. Het ondernemersplein zou nog onderzoeken of de standaard

relevant was, en heeft inmiddels aangegeven geen begrippenlijsten, axonomieën en/of linked data op de website aan te bieden. Daarmee is de standaard niet relevant.

Van de standaarden die in 2018 nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Ondernemersplein voldoet aan DMARC.

Concluderend moeten voor ondernemersplein nog (volledig) geïmplementeerd: CMIS, OWMS, STARTTLS/DANE.

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
		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 staat gepland voor 2018.
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Deels	Publicatie standaard op www.logius.nl zie aldaar voor Digitoegankelijk compliance. Overheid.nl ontsluit decentrale content op basis van Samenwerkende Catalogi, zie voor Digitoegankelijk compliance aldaar; Publicatie op basis van Samenwerkende Catalogi door overheden op eigen website Digitoegankelijk compliance eigen verantwoordelijkheid deelnemers (Rijk/gemeenten/provincies/waterschappen). De validator (scvalidator.logius.nl) is tot op heden niet getest op toegankelijkheid. Deze verplichting zal ingaan op 23 september 2020. Voor die tijd zal de validator zijn getest en eventuele tekortkomingen verholpen.

Open Api Specification (Beschrijven van REST API's)	Nee	Samenwerkende catalogi voldoet niet aan deze standaard. Momenteel wordt de relevantie van deze standaard nader bepaald.
OWMS (Metadata overheidsinformatie)	Ja	Samenwerkende catalogi is volledig gebaseerd op OWMS.

Ten opzichte van 2017 is Digitoegankelijk (EN 301 549 met WCAG 2.0) van 'ja' naar de status 'deels' gegaan. De validator (scvalidator.logius.nl) is tot op heden niet getest op toegankelijkheid. Deze verplichting zal ingaan op 23 september 2020. Voor die tijd zal de validator zijn getest en eventuele tekortkomingen verholpen.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) zijn Open API en DMARC relevant. Samenwerkende Catalogi voldoet nog niet aan deze standaarden. DMARC staat gepland voor 2018 en voor Open API wordt momenteel de relevantie nader bepaald.

Voor Samenwerkende Catalogi moeten dus nog de volgende standaarden (volledig) worden geïmplementeerd: Digitoegankelijk (EN 301 549 met WCAG 2.0), DMARC, Open API.

3.6 Rijksportaal

Beheer organisatie: SSC-ICT

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

Standaard	Status	Toelichting
		Internet en beveiliging
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 email-voorziening van SSC-ICT, die de DMARC standaard ondersteunt.
IPv6 en IPv4 (Internet-nummers)	Nee	Het huidige Rijksportaal (versie 1.6.5) is alleen ingericht voor IPv4. Om performance redenen 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 geen doorontwikkeling t.a.v. nieuwe functionaliteit voor het Rijksportaal.

SAML (Inloggegevens)	Gepland	De implementatie van SAML is in juli 2016 opgeleverd. Het Ministerie van Veiligheid en Justitie is de eerste klant die kan worden aangesloten op de huidige versie 1.6.5 van het Rijksportaal. De acceptatie van SAML is door het Ministerie Justitie en Veiligheid niet volledig afgerond vóór de transitie naar het ODC. Als gevolg hiervan dient deze functionaliteit opnieuw getest te worden. De functionaliteit is overigens wel beschikbaar en wordt nog zonder formele support gebruikt.
		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 2017 is de status van de SAML standaard op gepland gezet in plaats van ‘ja’, omdat de functionaliteit opnieuw getest wordt en hoewel het beschikbaar is, nog zonder formele support wordt gebruikt.

Van de standaarden die in 2018 nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Rijksportaal voldoet aan deze standaard.

Concluderend moet voor Rijksportaal nog IPv6 en IPv4 en SAML (volledig) worden geïmplementeerd.

3.7 ODC Noord

Beheerorganisatie: Dienst Uitvoering Onderwijs (DUO)

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

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	DKIM is geïmplementeerd voor ODC-Noord.

DMARC (Anti-phishing)	Nee	DNSSEC, SPF, DKIM en delivery over TLS zijn geïmplementeerd. Voor odc-noord.nl en sso-noord.nl zijn er DMARC records.
DNSSEC (Beveiligde domeinnamen)	Ja	ODC-Noord heeft sinds het onderzoek uit 2015 een eigen DNS ingericht, die DNSSEC gebruikt.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De cloud dashboards zijn allemaal uitsluitend via HTTPS benaderbaar een aantal websites draaien op HSTS. De overige websites zijn in de loop van 2017 aangepast. Alle sites zijn voorzien van een SSL-certificaat.
IPv6 en IPv4 (Internetnummers)	Deels	Intern wordt IPv6 gebruikt op een specifiek netwerk. Nog niet alle benodigde producten worden met IPv6 aangeboden. Zodra de markt alles op het juiste niveau kan aanbieden zal dit geïmplementeerd worden en zullen de systemen die vanaf het internet benaderbaar zijn, ook worden ontsloten via IPv6.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	In december 2017 is door ODC-Noord een BIR in Control Verklaring 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. SAML federatie staat op de roadmap voor eind 2018
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Gepland	De implementatie van DANE is voor eind 2018 gepland. STARTTLS is geïmplementeerd.
TLS 1.2, 1.1 en 1.0 (Beveiligde, versleutelde verbindingen)	Ja	Het beleid van ODC-Noord voor internet-gekoppelde systemen is dat TLS (in volgorde) van TLS1.2, TLS1.1 wordt aangeboden. TLS 1.0 wordt niet toegepast tenzij er een explain komt van de site-eigenaar.
WPA2 Enterprise (Toegang tot een WiFi-netwerk met account)	Ja	Deze standaard is toegepast waar ODC-Noord wifi gebruikt.
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Gepland	De websites van ODC-Noord worden op dit moment herbouwd. Digi-toegankelijk is een inrichtingseis. Verwachte oplevering is Q3 2018.
ODF (Document-bewerkingen)	Ja	In de operatie van ODC-Noord wordt over het algemeen gebruik gemaakt van documenten in ODF-formaat. Vanwege opmaak- en interoperabiliteitsproblemen wordt dit voor communicatie met externen beperkt gebruikt.
OWMS (Metadata overheidsinformatie)	Gepland	De websites van ODC-Noord worden op dit moment herbouwd. De vraag of hierbij ook de OWMS worden toegepast staat uit. Implementatie van OWMS staat gepland voor Q4 2018.

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 2017 is implementatie van Digitoegankelijk (EN 301 549 met WCAG 2.0) gepland. De status is verhoogd van nee naar gepland. De websites van ODC-Noord worden op dit moment herbouwd. Digi-toegankelijk is een inrichtingseis. Verwachte oplevering is Q3 2018. DKIM is geïmplementeerd. ODC Noord voldoet sinds 2018 aan DKIM, NEN-ISO/IEC 27001/27002 en HTTPS/HSTS. De status van DKIM is verhoogd van gepland naar ja. De status van NEN/ISO/27001/27002 is verhoogd van nee naar ja. De status van HTTPS/HSTS is verhoogd van deels naar ja. Implementatie van SAML en START/TLS staat gepland voor eind 2018.

Van de standaarden die in 2018 nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. ODC Noord voldoet nog niet aan deze standaard.

Concluderend moeten voor ODC Noord nog (volledig) worden geïmplementeerd: Digitoegankelijk (EN 301 549 met WCAG 2.0), DMARC, IPv6 en IPv4, OWMS, PDF 1.7, PDF A/1, PDF A/2, SAML, STARTTLS/DANE.

3.8 Doc-Direkt

Beheerorganisatie: Doc-Direkt

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

Standaard	Status	Toelichting
		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 vindt plaats in het 4e kwartaal 2018.
IPv4 en IPv6 (Internetnummers)	Ja	Doc-Direkt voldeed al aan IPv4 en voldoet inmiddels ook aan 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 v1.2, v1.1 en v1.0 (Beveiligde, versleutelde verbindingen)	Nee	Het is bij Doc-Direkt niet bekend of TLS van toepassing is en daarmee ook niet wanneer dit geïmplementeerd is.
		Document en (web/app)content
Ades Baseline Profiles (Digitaal ondertekenen van documenten)	Nee	Bij Doc-Direct loopt momenteel een onderzoek over de mogelijke toepassing van deze standaard in de toekomst. De uitkomsten daarvan zijn naar verwachting in het eerste kwartaal van 2019 bekend i.p.v. het eerste kwartaal van 2018.
CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)	Nee	De mogelijkheid en noodzakelijkheid van het toepassen van deze standaard werden in 2016 nader onderzocht, maar dit heeft nog niet tot een besluit geleid. Inmiddels zijn er 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 zijn nog geen plannen bekend of en wanneer SKOS geïmplementeerd zal worden.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Nee	Op dit moment wordt door SSC-ICT gewerkt aan operationalisering van Digikoppeling voor het gebruik binnen de dienstverlening van Doc-Direkt.

Ten opzichte van 2017 is er uitloop op het onderzoek dat Doc-Direct uitvoert over de mogelijke toepassing van Ades Baseline Profiles in de toekomst. De uitkomsten daarvan zijn naar verwachting in het eerste kwartaal van 2019 bekend i.p.v. het eerste kwartaal van 2018. Verder wordt door SSC-ICT gewerkt aan operationalisering van Digikoppeling voor het gebruik binnen de dienstverlening van Doc-Direkt. Verder wordt HTTPS/HSTS deels toegepast en is volledige implementatie gepland voor het vierde kwartaal van 2018. De status van HTTPS/HSTS is verhoogd van nee naar deels. Verder voldoet Doc-Direkt inmiddels aan IPv4 en IPv6 en SPF. De status van IPv4 en IPv6 en SPF is verhoogd van nee naar ja.

Van de standaarden die in 2018 nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant.

Concluderend moeten voor Doc-Direkt nog (volledig) worden geïmplementeerd: Ades Baseline Profiles, CMIS, Digikoppeling 2.0, HTTPS/HSTS, ODF, SKOS, TLS v1.2, v1.1 en v1.0.

3.9 Rijksoverheid.nl

Beheerorganisatie: Ministerie van AZ (DPC)

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

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/ phishing)	Ja	DKIM is geïmplementeerd. Dit heeft onder meer betrekking op de nieuwsbrieven die DPC namens de diverse departementale opdrachtgevers verstuurt. Het gaat om de nieuwsbrieven- en persberichten-service voor de Rijksoverheid en het DPC-mailverkeer. Deze zijn met SPF-DKIM-DMARC uitgerust.
DMARC (Anti-phishing)	Ja	DMARC is geïmplementeerd.
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)	Ja	Rijksoverheid.nl ondersteunt zowel IPv6 als IPv4 (zie: https://internet.nl/site/www.rijksoverheid.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Hosting leverancier Ordina heeft een NEN 27001/2 implementatie waarin de beveiliging van rijksoverheid.nl meegaat. DPC zelf valt onder de VIR/BIR-implementatie van het moederdepartement AZ.
SAML (Inloggegevens)	Ja	Er is een soort WeTransfer app binnen het Rijksoverheid online platform. Deze maakt gebruik van SAML voor het authentiseren van gebruikers. Er zijn geen andere diensten die via Rijksoverheid worden aangeboden en inloggen vereisen (met SAML).
SPF (Preventie van mailspoofing/phishing)	Ja	Het e-maildomein @rijksoverheid.nl is integraal van SPF voorzien (zie: https://internet.nl/mail/rijksoverheid.nl/).
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Gepland	Verzendende mailservers die STARTTLS ondersteunen, kunnen met ontvangende mailserver(s) een beveiligde verbinding opzetten. Tenminste één van de mailserverdomeinen bevat geen TLSA-record voor DANE (zie:

		https://internet.nl/mail/rijksoverheid.nl/). SSC-ICT geeft aan dat de planning voor implementatie van DANE Q4 2018 is.
TLS v1.2, v1.1 en v1.0 (Beveiligde, versleutelde verbindingen)	Ja	Rijksoverheid.nl maakt gebruik van het Platform Rijksoverheid Online en daardoor geheel voorzien van https door middel van PKIo EV certificaten (zie: https://internet.nl/site/www.rijksoverheid.nl/).
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Ja	De website voldoet aan Digitoegankelijk (WCAG 2.0). Zie ook de verantwoording daarover op: http://www.rijksoverheid.nl/toegankelijkheid.
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)	Nee	DPC publiceert zelf geen PDF's, maar departementen kunnen PDF's op Rijksoverheid plaatsen. Vooralsnog kan de Rijksoverheid praktisch niet aan deze richtlijn voldoen. DPC is daarover met BZK in gesprek.
		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 2017 is de PDF standaard op nee gezet. En is de STARTTLS/DANE standaard opgenomen en op gepland gezet. SSC-ICT is voornemens DANE te implementeren in Q4 2018.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Rijksoverheid.nl voldoet aan DMARC.

Concluderend, moeten voor rijksoverheid.nl nog de volgende standaarden (volledig) worden geïmplementeerd: PDF 1.7 / PDF A/1 en PDF A/2, STARTTLS/DANE.

4. Gegevens en registreren

4.1 Basisregistraties

4.1.1 NHR (Handelsregister)

Beheerorganisatie: Kamer van Koophandel

Werking en inhoud NHR (bron: Monitor GDI 2018)
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
		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 zowel website als mailservers aan DMARC (zie: https://internet.nl/mail/kvk.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC wordt volledig toegepast (zie: https://en.internet.nl/site/kvk.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels	De voorziening gebruikt zowel HTTPS als HSTS. Eén subdomein (kvk.nl zonder www) gebruikt nog geen HSTS, dit wordt hersteld.
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 is in 2017 uitgesteld tot 2018 maar nog niet ingepland.
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)	Gepland	De voorziening past alleen STARTTLS toe, DANE nog niet (zie: https://internet.nl/mail/kvk.nl/). KvK heeft inmiddels de middelen in huis om DANE op DNS-servers te gaan ondersteunen. De beheerder geeft echter aan dat dit een lastige, risicovolle operatie is. De start ervan is voorzien in 2018.
TLS v1.2, v1.1 en v1. (Beveiligde, versleutelde verbindingen)	Ja	De KvK gebruikt TLS op de verbindingen waar voorheen SSL werd gebruikt. De kamer is inmiddels overgegaan op TLS1.2 (zie: https://internet.nl/site/www.kvk.nl/).
		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 Tridion, Sharepoint en Documentum zijn compliant aan de CMIS standaard. Nog niet alle interne koppelingen op deze systemen zijn gemigreerd naar deze standaard, daar zijn ook nog geen plannen voor. Koppelingen met Sharepoint worden CMIS compliant uitgevoerd.
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Deels	De KvK voldoet volledig aan de eisen van Digitoegankelijk voor alle nieuwe onderdelen. Voor oudere onderdelen van de website wordt getracht compliant te zijn in 2019. Voor nieuwe app's geldt inmiddels standaard de Digitoegankelijk eis.
Open API Specification (Beschrijven van REST API's)	Gepland	KvK zal in 2018 een start maken om aan deze standaard te voldoen. Reeds operationele API's worden echter hierop niet 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 PDF A/1.
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.
		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 overheidsgegevens)	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 migreert haar financiële systeem in 2018 naar ProFiT van AFAS, UBL 2.1 en SMeF 2.0 worden wel ondersteund maar de modelfactuur nog niet.

Ten opzichte van 2017 zijn er een aantal ontwikkelingen. Alle nieuwe onderdelen van NHR voldoen aan Digitoegankelijk (EN 301 549 met WCAG 2.0). Voor oudere onderdelen van de website wordt getracht compliant te zijn in 2019. DNSSEC wordt volledig toegepast. HTTPS/HSTS is van de status gepland naar de status deels gegaan. Mailservers e.d. zijn bereikbaar via zowel IPv4 als IPv6. De website kvk.nl ondersteunt IPv4, maar is niet toegankelijk via IPv6. Dit was gepland voor 2017, maar is verzet naar 2018. De voorziening past alleen STARTTLS toe, DANE nog niet (zie https://internet.nl/mail/kvk.nl/). KvK heeft inmiddels de middelen in huis om DANE op DNS-servers te gaan ondersteunen, de start ervan is vertraagd (Q4 2017) en voorzien in 2018.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) zijn DMARC, NLCIUS en Open API relevant. Volgens KVK voldoen zowel website als mailservers aan DMARC. Implementatie van Open API staat gepland voor 2018. NHR voldoet nog niet aan NLCIUS.

Concluderend, moeten voor NHR nog de volgende standaarden (volledig) worden geïmplementeerd: CMIS, Digitoegankelijk (EN 301 549 met WCAG 2.0), HTTPS/HSTS, IPv4 en IPv6, SKOS, STARTTLS/DANE, NLCIUS, Open API.

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 (bron: Monitor GDI 2018)
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 (bron: Monitor GDI 2018)

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 (bron: Monitor GDI 2018)
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 (bron: Monitor GDI 2018)
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
		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)	Gepland	HTTPS is correct geconfigureerd (en wordt afgedwongen). HSTS is deels geïmplementeerd en is gepland in Q3 en 4 verder geïmplementeerd te worden (zie: https://internet.nl/domain/www.kadaster.nl/)De verwachte implementatie per Q1 2018 is niet gehaald.
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)	Gepland	STARTTLS is geïmplementeerd, maar de verwachte implementatie van DANE is gepland per Q1 2019 te zijn geïmplementeerd (zie: https://internet.nl/domain/www.kadaster.nl/).De verwachte implementatie van DANE per Q1 2018 is niet behaald.
TLS v1.2, v1.1 en v1.0. (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
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Ja	Het Kadaster voldoet aan de Webrichtlijnen en heeft een toegankelijkheidsverklaring gepubliceerd op kadaster.nl.
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.
		E-facturatie en administratie
NLCIUS (Elektronisch factureren)	Nee	Invoering van elektronisch factureren is 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 2017 is de Digikoppeling 2.0 standaard van status 'ja' op status 'deels' gezet, omdat een aantal koppelingen niet op Digikoppeling gebaseerd zijn. De PDF 1.7, PDF/A-1 en PDF/A-2 standaard is volledig geïmplementeerd.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) zijn DMARC, NLCIUS en Open API relevant. DMARC en Open API zijn geïmplementeerd. Invoering van elektronisch factureren is onderhanden en daarop zal gebruik gemaakt gaan worden van de NLCIUS standaard.

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

4.1.3 BRT (Basisregistratie Topografie)

Beheerorganisatie: Kadaster

Werking en inhoud BRT (bron: Monitor GDI 2018)
De Basisregistratie Topografie (BRT) bestaat uit digitale topografische bestanden, veelal kaarten, op verschillende schaal niveaus.

Standaard	Status	Toelichting
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	DMARC is geïmplementeerd.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Gepland	HTTPS wordt al toegepast, HSTS is deels geïmplementeerd (zie: https://internet.nl/domain/www.kadaster.nl/). Verdere implementatie is gepland in Q3 en Q4 2018. Implementatie per Q1 2018 is niet gehaald.

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)	Gepland	STARTTLS is geïmplementeerd (zie: https://internet.nl/domain/www.kadaster.nl/). DANE is gepland per Q1 2019 te zijn geïmplementeerd. Verwachte implementatie van DANE per Q1 2018 is niet gehaald.
TLS v1.2, v1.1 en v1. (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
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Nee	Het Kadaster voldoet aan de Webrichtlijnen en heeft een toegankelijkheidsverklaring gepubliceerd op kadaster.nl. Naar verwachting voldoet het Kadaster in Q4 2018 volledig aan de toegankelijkheidsrichtlijn.
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 2017 is de status van de standaard Digitoegankelijk (EN 301 549 met WCAG 2.0) van de status 'ja' naar 'nee' gegaan. De verwachting van de beheerder is dat het kadaster wat Digitoegankelijk (EN 301 549 met WCAG 2.0) betreft in Q4 2018 volledig aan de toegankelijkheidsrichtlijn voldoet.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. DMARC is reeds geïmplementeerd.

Concluderend moet de BRT nog de volgende standaarden (volledig) implementeren: Digitoegankelijk (EN 301 549 met WCAG 2.0), HTTPS/HSTS, OWMS, STARTTLS/DANE. Ten aanzien van OWMS moet opgemerkt worden dat wel wordt voldaan aan overige en verplichte internationale standaarden. Daarmee wordt bewust afgeweken van de OWMS standaard.

4.1.4 BRV (Basisregistratie Voertuigen)

Beheerorganisatie: RDW (Rijksdienst Wegverkeer)

Werking en inhoud van BRV (Bron: Monitor GDI 2018)
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
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	De BRV voldoet aan DKIM.
DMARC (Anti-phishing)	Ja	De BRV voldoet aan DMARC.
DNSSEC (Beveiligde domeinnamen)	Ja	De BRV voldoet aan DNSSEC. De niet-gevoelige (technische) gegevens uit de BRV zijn te bevragen via www.rdw.nl. Die site is volgens internet.nl gesigned met DNSSEC. Alle .nl rdw domeinen zijn gesigned met DNSSEC.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Gepland	Implementatie wordt medio 2018 gerealiseerd.
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)	Ja	De BRV voldoet aan deze standaard.

(Richtlijnen en principes informatiebeveiliging)		
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 v1.2, v1.1 en v1. (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	Het bij RDW gebruikte platform voor document management ondersteunt CMIS maar er is voor RDW op dit moment geen aanleiding, zowel intern als extern, om CMIS toe te passen.
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Deels	De website van de RDW voldoet nog niet volledig aan de Webrichtlijnen (versie 2, niveau AA). Voor de status wordt verwezen naar: https://www.rdw.nl/over-rdw/dienstverlening/kwaliteits--en-servicenormen/toegankelijkheidsverklaring.
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	Deels	RDW maakt voor alle nieuwe uitwisselingen gebruik van Digikoppeling. Dat is onder meer het geval in de uitwisseling met

(Veilige berichtenuitwisseling en)	MijnOverheid (Berichtenbox), CJIB, Politie, ILT, CBR, de Belastingdienst, etc. Bestaande koppelingen blijven via bestaande middelen lopen, tenzij onderhoud of wijzigingen de mogelijkheid bieden om de digikoppeling mee te nemen.

Ten opzichte van 2017 voldoet de BRV aan STARTTLS/DANE. Verder is DKIM toegevoegd, de BRV voldoet aan deze standaard.

Van de standaarden die in 2018 nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) zijn DMARC en Open API Specification relevant. BRV voldoet aan beide standaarden.

Concluderend moeten voor de BRV nog (volledig) worden geïmplementeerd: CMIS, Digikoppeling 2.0, Digitoegankelijk (EN 301 549 met WCAG 2.0), HTTPS en HSTS en IPv4 en IPv6.

4.1.5 BRI (Basisregistratie Inkomen)

Beheerorganisatie: Belastingdienst

Werking en inhoud BRI (bron: Monitor GDI 2018)
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
		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 v1.2, v1.1 en v1. (Beveiligde, versleutelde verbindingen)	Ja	De actuele versies van TLS maken deel uit van de standaard beveiligingsrichtlijnen van de Belastingdienst.
WPA2 Enterprise (Toegang tot een WiFi-netwerk met account)	Ja	WPA2 wordt toegepast door de Belastingdienst.
		Stelselstandaarden
Digikoppeling 2.0	Ja	Digikoppeling wordt toegepast in de rol van afnemer van berichten van basisregistraties(HR). De ebMS-koppeling met

(Veilige berichtenuitwisselingen)	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 2017 zijn er ten aanzien van reeds opgenomen standaarden geen wijzigingen.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. BRI voldoet aan DMARC.

Concluderend voldoet BRI (volledig) aan de verplichte standaarden.

4.2 Digilevering

Beheerorganisatie: Logius

Inhoud en werking van Digilevering (Bron: Monitor GDI 2018)
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
		Internet en beveiliging
DKIM[6] (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)	Gepland	Implementatie van DMARC staat gepland voor Q1 2019.
DNSSEC[7] (Beveiligde domeinnamen)	Ja	DNSSEC is geïmplementeerd op de centrale voorziening DNS.

[6] 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.

[7] idem

HTTPS/HSTS[8] (Beveiligd, versleuteld webverkeer)	Nee	Digilevering voldoet aan de HTTPS standaard. Aan HSTS wordt niet voldaan.
IPv4 en IPv6 (Internetnummers)	Gepland	Implementatie van IPv6 staat gepland voor Q1 2019. Digilevering gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik.
SPF[9] (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[10] (Beveiligd, versleuteld mailverkeer)	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.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Digilevering maakt gebruik van Digikoppeling.

Ten opzichte van 2017 staat de implementatie van IPv6 gepland voor Q1 2019. De status van HTTPS/HSTS is van ‘ja’ naar ‘nee’ gegaan, omdat niet voldaan wordt aan HSTS.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Implementatie van de standaard staat gepland voor Q1 2019.

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

4.3 Digimelding

Beheerorganisatie: Logius

Inhoud en werking van Digimelding (bron: Monitor GDI 2018)

[8] idem

[9] idem

[10] idem

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.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	DKIM draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. DKIM is geïmplementeerd op de centrale voorziening mail relay.
DMARC (Anti-phishing)	Gepland	Implementatie van DMARC staat gepland voor Q1 2019.
DNSSEC[11] (Beveiligde domeinnamen)	Ja	DNSSEC is geïmplementeerd op de centrale voorziening DNS.
HTTPS/HSTS[12] (Beveiligd, versleuteld webverkeer)	Nee	Digilevering voldoet aan de HTTPS standaard. HSTS wordt niet toegepast.
IPv4 en IPv6 (Internetnummers)	Nee	Digimelding gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik. Digimelding ondersteunt op dit moment alleen IPv4.
SPF[13] (Preventie van mailspoofing/phishing)	Ja	Digimelding draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar buiten te sturen om te voorkomen dat de applicatiebeheerder of een van haar systemen als spam/malware verstuurder wordt aangemerkt. Alle mail-versturende systemen moeten gebruik maken van de centrale voorziening mail relay als zij mail willen versturen. SPF is geïmplementeerd op de centrale voorziening mail relay.
STARTTLS/DANE[14]	Ja	Digimelding draait op het Logius Managed Services platform. Vanuit de VPC is het niet mogelijk mail direct naar

[11] [11] 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.

[12] idem

[13] idem

[14] idem

(Beveiligd, versleuteld mailverkeer)		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.

Ten opzichte van 2017 is de status van HTTPS/HSTS van ‘ja’ naar ‘nee’ gegaan, omdat niet voldaan wordt aan HSTS.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Implementatie van DMARC staat gepland voor Q1 2019.

Concluderend, moeten voor Digimelding nog de volgende standaarden (volledig) worden geïmplementeerd: DMARC, HTTPS/HSTS, IPv4 en IPv6.

4.4 Stelselcatalogus

Beheerorganisatie: Logius

Inhoud en werking van stelselcatalogus (bron: Monitor GDI 2018)
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
		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)	Nee	HTTPS is in 2017 geïmplementeerd. HSTS wordt nog niet ondersteund (zie: https://internet.nl/site/www.stelselcatalogus.nl/).

IPv4 en IPv6 (Internetnummers)	Ja	De Stelselcatalogus gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik. Stelselcatalogus ondersteunt IPv4 en IPv6 (zie: https://internet.nl/site/www.stelselcatalogus.nl/92837).
		Document en (web/app)content
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Ja	De webpagina's van de Stelselcatalogus vallen binnen de website van digitaleoverheid.nl. Zie certificaat van toegankelijkheid van Accessibility.nl. Zie: https://www.digitaleoverheid.nl/toegankelijkheidsverklaring.
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 2017 is HTTPS geïmplementeerd. HSTS wordt nog niet ondersteund.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. De Stelselcatalogus voldoet aan DMARC.

Concluderend, moet de Stelselcatalogus nog de volgende standaard (volledig) implementeren: HTTPS/ HSTS.

4.5 P-Direkt

Beheerorganisatie: P-Direkt

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

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

Standaard	Status	Toelichting

		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. P-Direkt heeft aangegeven dat het initiatief voor de adoptie van dit soort standaarden dan ook bij SSC-ICT ligt. Navraag bij SSC-ICT leert dat DKIM actief gemaakt is voor deze mailservice van P-Direkt.
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 dienst en het initiatief voor het implementeren van DNSSEC bij de SSC-ICT ligt. SSC-ICT gaf in 2016 aan dat zij op hun beurt weer afhankelijk zijn van de leverancier van de Haagse ring, namelijk Logius. Inmiddels is DNSSEC nog niet geïmplementeerd en is er geen verdere informatie voorhanden.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Gepland	HTTPS is 100% doorgevoerd voor alle communicatie met klanten. HSTS is nog niet geïmplementeerd. De externe sites P-Direkt.nl en sciorijk.nl voldoen beide aan HSTS. Eén interne site voldoet hier niet aan. Planning voor implementatie is Q1 2019.
IPv4 en IPv6 (Internetnummers)	Nee	De Haagse ring, waarover eigenlijk al het verkeer naar P-Direkt loopt, ondersteunt geen IPv6. De P-Direkt voorzieningen, zoals gehost bij Match, ondersteunen in theorie momenteel al IPv6.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Deels	De hosting van de dienstverleningssystemen van P-Direkt voldoet aan de BIR (BIR compliancy is integraal onderdeel van de inrichting van het ODC, en als zodanig daarmee ook voor P-Direkt). Echter, de beheersorganisatie voldoet niet volledig aan de BIR en zit in een proces/project om aan de BIR te voldoen.
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).
TLS v1.2, v1.1 en v1.0 (Beveiligde, versleutelde verbindingen)	Ja	Alle diensten van P-Direkt die door middel van HTTP worden ontsloten, worden enkel aangeboden via TLS v1.0 of hoger.
		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. P-Direkt doet onderzoek naar geavanceerde en gekwalificeerde digitale handtekeningen.

Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Gepland	Het Portal is nog altijd in ontwikkeling. Er is op dit portal nog geen Webrichtlijnen toets geweest. P-Direkt is zich ervan bewust dat er nog geen volledige compliancy is met de Webrichtlijnen. P-Direkt is in het proces van de impactanalyse van het (tijdelijke) besluit Digitoegankelijk. Hieruit vloeit voor P-Direkt de eis voort om te voldoen aan WCAG 2.x. Voor nieuwe websites streeft P-direkt naar implementatie voor 23 september 2019. Bestaande websites hoopt P-direkt voor 23 september 2020 te hebben omgebouwd. De 2 mobiele apps zijn aangepast voor 23 juni 2021.
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)	Deels	De meeste zaken die het digitale personeelsdossier ingaan zijn PFD/A. De grootste uitzondering/afwijking zijn de digitale loonstroken, die zijn nog altijd PDF 1.3. Reden/oorzaak is dat deze aangemaakt worden met een standaard SAP conversieroutine die niet anders dan PDF 1.3 kan genereren. Er is momenteel geen concreet plan de loonstroken in PDF A/x te genereren. PDF A/2 wordt nog niet gebruikt binnen P-Direkt.
		Stelselstandaarde
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 2017 is de SPF standaard geïmplementeerd. Bovendien zijn er concrete planningen afgegeven voor de implementatie van Digitoegankelijk (EN 301 549 met WCAG 2.0) en HTTPS/HSTS.

Van de standaarden die in 2018 nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. P-direkt voldoet aan deze standaard.

Concluderend moet voor P-direkt nog (volledig) worden geïmplementeerd: Ades Baseline Profiles, Digitoegankelijk (EN 301 549 met WCAG 2.0), DNSSEC, HTTPS/HSTS, IPv4 en IPv6, NEN-ISO/IEC 27001/27002, ODF, PDF 1.7 – PDF A/1 of PDF A/2.

5. Dienstverlening en verbinden

5.1 eFactureren

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting
		E-facturatie en administratie
NLCIUS (Elektronisch factureren)	Gepland	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 staat gepland voor Q2 2019.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen NLCIUS relevant. NLCIUS vervangt standaard SMEF 2.0. Implementatie van deze standaard staat gepland voor Q2 2019.

Concluderend, moet voor eFactureren nog de volgende standaarden (volledig) worden geïmplementeerd: NLCIUS.

5.2 SBR

Beheerorganisatie: Logius

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

Dienst Uitvoering Onderwijs (DUO)[15]. De voorziening voor de e-dienstverlening is Digipoort. SBR heeft een eigen website.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/ phishing)	Gepland	De website van SBR (http://www.sbr-nl.nl) heeft ook een mailserver. Omdat de website overgezet wordt naar het Ministerie van AZ, moet DKIM (naast DMARC en SPF) nog ingesteld worden. Daardoor voldoet de website momenteel niet aan DKIM. Planning voor implementatie is Q1, 2019.
DMARC (Anti-phishing)	Gepland	SBR voldoet niet aan DMARC. Dit staat gepland voor Q1 2019.
DNSSEC (Beveiligde domeinnamen)	Ja	De website van SBR (http://www.sbr-nl.nl) Voldoet zowel op het web als het maildomein aan DNSSEC.
IPv4 en IPv6 (Internetnummers)	Ja	De website van SBR wordt bij een derde partij gehost en is bereikbaar met IPv6.
SPF (Preventie van mailspoofing/phis hing)	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)	Gepland	Aan STARTTLS wordt voldaan, door de voorziening. Aan DANE wordt nog niet voldaan. Dit is opgenomen in de planning voor Q1 2019.
TLS 1.0, 1.1 en 1.2 (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.
		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.

[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.

Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Gepland	Voor SBR-NL.nl is op Digitoegankelijk getoetst en op zes punten na voldoet deze, er is nog geen verklaring. Per oktober 2018 wordt een nieuw CMS geïmplementeerd.
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 2017 is de implementatie van Digitoegankelijk (EN 301 549 met WCAG 2.0), DKIM en STARTTLS/DANE gepland voor Q1 2019. Verder wordt voldaan aan DNSSEC en SPF.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Implementatie van DMARC staat gepland voor Q1 2019.

Concluderend, moeten voor de SBR nog de volgende standaarden (volledig) worden geïmplementeerd: Digitoegankelijk (EN 301 549 met WCAG 2.0), DKIM, DMARC, STARTTLS/DANE.

5.3 Digipoort

Beheerorganisatie: Logius

DigiPoort is een ICT-centrale waar berichtenverkeer voor de overheid afgehandeld wordt. Overheden kunnen DigiPoort inzetten om bedrijfs- en ketenprocessen te automatiseren. Omdat Digipoort slechts machine-naar-machine koppelingen levert en niet toegankelijk is vanaf het openbare internet, is deze voorziening niet getoetst met de toetsen van internet.nl.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	DigiPoort voldoet aan DKIM. Dit is ook relevant omdat de voorziening een SMTP koppelvlak heeft.
DMARC (Anti-phishing)	Gepland	Planning voor de implementatie van DMARC is Q1 2019, als onderdeel van een Logius breed project voor Domein verhuizing.
DNSSEC (Beveiligde domeinnamen)	Gepland	Implementatie van DNSSEC vindt plaats in Q1 2019.
HTTPS/HSTS	Ja	De voorziening voldoet aan HTTPS. Formeel wordt niet aan HSTS voldaan, maar de standaard HTTP (poort 80) is bij de voorziening helemaal niet

(Beveiligd, versleuteld webverkeer)		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)	Gepland	Digipoort gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internet gebruik. Digipoort ondersteunt IPv4. Implementatie van IPv6 staat gepland voor Q1 2019.
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. Dit is opgenomen in de planning voor Q1 2019.
TLS v1.2, v1.1 en v1. (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.

Ten opzichte van 2017 is een concrete planning afgegeven voor de implementatie voor DNSSEC, IPv6 en SPF. Verder is de standaard STARTTLS/DANE afgevoerd, omdat de voorziening niet over een eigen emailvoorziening beschikt.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Planning voor de implementatie van DMARC is Q1 2019.

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

5.4 Diginetwerk

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	Diginetwerk.nl voldoet aan DMARC
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC validatie wordt toegepast op Rijks-DNS.
IPv4 en IPV6 (Internetnummers)	Gepland	IPv4 is geïmplementeerd voor Diginetwerk. De implementatie van IPv6 staat gepland voor Q4 2018.
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 2017 is er een concrete planning voor de implementatie van IPv6, namelijk Q4 2018. Verder is de standaard STARTTLS/DANE afgevoerd, omdat de voorziening niet over een eigen emailvoorziening beschikt.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. Diginetwerk voldoet aan DMARC.

Concluderend, moet Diginetwerk nog de volgende standaard (volledig) implementeren: IPv4 en IPV6.

5.5 Tenderned

Beheerorganisatie: PIANOo/DICTU

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

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

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM	Nee	E-mails verzonden vanuit TenderNed zijn niet beveiligd met DKIM (zie: https://internet.nl/mail/tenderned.nl/).

(Preventie van mailspoofing/phishing)		
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)	Ja	De client-server communicatie van TenderNed is beveiligd met HTTPS en HSTS (zie: https://internet.nl/site/www.tenderned.nl/).
IPv4 en IPV6 (Internetnummers)	Nee	Tenderned.nl is 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 (Beveiligd, versleuteld mailverkeer)	Nee	STARTTLS wordt ondersteund. DANE nog niet.
TLS v1.2, v1.1 en v1.0 (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
Digitoegankelijk (EN 301 549 met WCAG 2.0) (Toegankelijkheid web content)	Nee	TenderNed wordt vanaf 2017 gerenoveerd. Daarbij worden de schermen deels vernieuwd. De beheerder heeft aangegeven nog tot in 2019 te renoveren. Bij de implementatie van nieuwe schermen worden de richtlijnen uit EN 301 539 toegepast.
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 2017 is inmiddels SPF geïmplementeerd door de technische dienstverlener. De renovatie van Tenderned is nog gaande en gaat nog tot in 2019 door.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) zijn DMARC en Open API relevant. Echter voldoet Tenderned aan beide standaarden niet.

Concluderend, moet Tenderned nog de volgende standaarden (volledig) implementeren: Digitoegankelijk (EN 301 549 met WCAG 2.0), DKIM, DMARC, IPv4 en IPV6, Open API Specification, STARTTLS en DANE.

5.6 DWR

Beheerorganisatie: Ministerie BZK

De Digitale Werkomgeving Rijksdienst (DWR) is de ICT-werkomgeving voor rijksambtenaren. Deze werkomgeving is een onderdeel van de dienstverlening van SSC-ICT. SSC-ICT ontwikkelt en beheert 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.

Binnen SSC-ICT loopt momenteel een project om relevante, voor DWR van toepassing zijnde Open Standaarden te implementeren zover deze nog niet geïmplementeerd waren.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Deels	De implementatie van DKIM en DMARC is voor SSC-ICT zelf voor 90% afgerond. Open staat nog het aanbieden van een dienst voor externe applicaties die mailen of klanten die gebruik maken van externe mailingdiensten. SSC-ICT is voor realisatie van deze dienst afhankelijk van de betreffende klanten.
DMARC (Anti-phishing)	Deels	De implementatie van DKIM en DMARC is voor SSC-ICT zelf voor 90% afgerond. Open staat nog het aanbieden van een dienst voor externe applicaties die mailen of klanten die gebruik maken van externe mailingdiensten. SSC-ICT is voor realisatie van deze dienst afhankelijk van de betreffende klanten.

DNSSEC (Beveiligde domeinnamen)	Deels	De domeinen van de klanten van SSC-ICT die via de DNS van AZ lopen voldoen reeds. De domeinen van de klanten van SSC-ICT die via de DNS van SSC-ICT lopen voldoen eind 2018 i.p.v. eind 2017. SSC-ICT geeft aan dat de cliënt zelf DNSSEC-validatie ondersteunt, er is alleen nog een issue met de Proxy die niet om kan gaan met de validatie. Dit issue is belegd bij de leverancier. RijksDNS tenslotte ondersteunt DNSSEC-validatie.
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 2018 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 2018 ondersteunen.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	SSC-ICT werkt via deze standaard en wordt hier ook op ge-audit. De laatste audit heeft plaatsgevonden in 2017.
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)	Gepland	De internet mailvoorziening werkt met STARTTLS. Implementatie van DANE in Q4 2018 is in voorbereiding in het verlengde van het initiatief ‘Veilige E-mail Coalitie’. De implementatie van DANE is afhankelijk van DNSSEC, welke ook in Q4 2018 voorzien is (zie hierboven onder “DNSSEC”).
TLS v1.2, v1.1 en v1.0 (Beveiligde, versleutelde verbindingen)	Ja	De op de werkplek aangeboden browsers ondersteunen deze versies van TLS. De internet mailvoorziening werkt met STARTTLS. Voor webservers met applicaties van klanten wordt dit toegepast voor de klanten die dit hebben aangevraagd.
WPA2 Enterprise (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
Digitoegankelijk (EN 301 549 met WCAG 2.0)	Deels	Niet alle websites waar SSC-ICT zelf eigenaar is, voldoen op dit moment aan Digitoegankelijk. SSC-ICT is niet de eigenaar van alle websites van haar klanten, bij deze websites ligt de verantwoordelijkheid derhalve bij de klant zelf.

(Toegankelijkheid web content)		
ODF 1.2 (Documentbewerkingen)	Ja	De DWR Next client wordt geleverd met zowel Libreoffice 5.x 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)	Deels	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 2017 is een concrete planning afgegeven voor implementatie van HTTPS/HSTS, IPv6 en DANE. Inmiddels wordt SPF voor alle domeinen toegepast. Ten opzichte van vorig jaar is de standaard Ades Baseline Profiles verwijderd als relevante standaard. De reden daarvoor is dat dit jaar de beheerder van de voorziening heeft aangegeven dat het onderdeel waarop de standaard van toepassing is niet onder de scope van de DWR voorziening valt. PBLQ kan zich hierin vinden. Overigens is SSC-ICT wel in staat de standaard te leveren en voldoen zij in die zin dus wel.

Van de standaarden die in 2018 nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) is alleen DMARC relevant. DWR voldoet deels aan deze standaard.

Concluderend moeten voor DWR nog (volledig) worden geïmplementeerd: Digitoegankelijk (EN 301 549 met WCAG 2.0), DKIM, DMARC, DNSSEC, HTTPS/HSTS, IPv4 en IPV6, STARTTLS/DANE. De beheerder geeft aan dat SSC-ICT voor de implementatie van sommige standaarden afhankelijk is van haar klanten en zich derhalve niet verantwoordelijk voelt voor het gebruik van de standaard door de klant.

5.7 Digi-Inkoop

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting

		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Gepland	Implementatie is opgenomen in de planning (Q1, 2019).
DMARC (Anti-phishing)	Gepland	Implementatie is opgenomen in de planning (Q1, 2019).
DNSSEC (Beveiligde domeinnamen)	Ja	Digi-Inkoop voldoet aan DNSSEC (zie: https://internet.nl/mail/digiinkoop.nl/).
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening voldoet aan HTTPS/HSTS.
IPv4 en IPV6 (Internet-nummers)	Nee	IPv6 werd in 2016 en 2017 niet ondersteunt door de hoster van Digi-Inkoop. Er zijn geen plannen dit te realiseren, en er is geen opdracht om dit aan te passen (zie: https://internet.nl/mail/digiinkoop.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Digi-Inkoop voldoet aan de BIR. Er is een in control statement afgegeven. Leveranciers voldoen aan ISO 27001.
SPF (Preventie van mailspoofing/phishing)	Gepland	Digi-Inkoop voldoet nog niet aan deze standaard, implementatie is opgenomen in de planning voor Q2 2019.
TLS v1.2, v1.1 en v1.0 (Beveiligde, versleutelde verbindingen)	Ja	Digi-Inkoop 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 Digi-Inkoop applicatie produceert inkooporders en facturen in PDF formaat. Documenten die op logius.nl beschikbaar worden gesteld zijn in PDF/A formaat (dit zijn de documenten over de berichtenverkeerstandaarden waar Digi-Inkoop gebruik van maakt: https://www.logius.nl/ondersteuning/gegevensuitwisseling/ubl-ohnl en https://www.logius.nl/ondersteuning/gegevensuitwisseling/setu-hr-xml-ohnl).
		E-facturatie en administratie
NLCIUS (Elektronisch factureren)	Gepland	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 staat gepland voor Q2 2019.
SETU (Informatie flexibele arbeidskrachten)	Ja	Digi-Inkoop ondersteunt de uitwisseling van SETU-hr-XML berichten.

Ten opzichte van 2017 zijn implementatie van DKIM en SPF opgenomen in de planning. DKIM is nieuw opgenomen ten opzichte van vorig jaar. Digi-Inkoop voldoet aan HTTPS/HSTS. De status van HTTPS/HSTS is verhoogd van nee naar ja.

Van de standaarden die nieuw op de lijst staan (COINS, DMARC, NLCIUS, NLCS, Open API) zijn DMARC en NLCIUS relevant. Implementatie van beiden worden opgenomen in de planning.

Concluderend, moeten voor Digi-Inkoop nog de volgende standaarden (volledig) worden geïmplementeerd: DKIM, DMARC, IPv4 en IPV6, NLCIUS, SPF.

Bijlage A Geïnterviewde personen

Naam voorziening	Contactpersoon
BAG, WOZ, BGT, BRK	Harrie van Leeuwen / Piet van der Krieke
Berichtenbox voor bedrijven	Dick Bruinsma, Laura Ouwehand
BRI	Harry Roumen
BRT	Harrie van Leeuwen / Piet van der Krieke
BRV	Walter Huberts, Gert Stel
BSN en GBA-V	Bob te Riele, Hans van Laar
Digi-Inkoop	Peter Haasnoot, Erwin Kaats
DigiD	Peter Haasnoot, Erwin Kaats
DigiD Machtigen	Peter Haasnoot, Erwin Kaats
Digilevering	Peter Haasnoot, Erwin Kaats
Digimelding	Peter Haasnoot, Erwin Kaats
Diginetwerk	Peter Haasnoot, Erwin Kaats
DigiPoort	Peter Haasnoot, Erwin Kaats
Doc-Direkt	Ali Amin Shahidi
DWR	Rein Hennen
eFactureren	Peter Haasnoot, Erwin Kaats
Stelsel elektronische toegangsdiensten	Peter Haasnoot, Erwin Kaats
MijnOverheid	Peter Haasnoot, Erwin Kaats
NHR	Rob Spoelstra
ODC Noord	Jaap Jansma
Ondernemersplein	Milla van der Have, Wouter Nieuwenhuis
Overheid.nl	Lucien de Moor, Hans Overbeek
P-Direkt	Jos van Vlimmeren
PKI Overheid	Peter Haasnoot, Erwin Kaats
Rijksoverheid.nl	Marc van de Graaf, Cees den Heijer
Rijkspas	Stefano Sacceddu
Rijksportaal	Leon Boender
Samenwerkende Catalogi	Peter Haasnoot, Erwin Kaats
SBR	Peter Haasnoot, Erwin Kaats
Stelselcatalogus	Peter Haasnoot, Erwin Kaats
Tenderned	Rudi van Eijck