PBLQ

Monitor Open Standaarden Voorzieningen 2020

Versie 0.99
3-12-2020

PBLQ
verbinders in de informatiesamenleving

Inhoudsopgave

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

1.2 Opdrachtformulering

Doel van deze opdracht is het creëren van een beeld van de toepassing van open standaarden bij de verschillende voorzieningen van de overheid. Oorspronkelijk bestond de te onderzoeken lijst uit voorzieningen in de Gemeenschappelijke Digitale Infrastructuur (GDI), maar op verzoek van BZK zijn daar andere voorzieningen aan toegevoegd. Dit maakt dat de voorzieningen die de laatste jaren zijn onderzocht een divers karakter hebben. In overleg met het Forum Standaardisatie wordt dit jaar een aangepaste lijst van voorzieningen onderzocht.

De oorspronkelijke lijst is opgedeeld in een set voorzieningen die direct raakt aan de communicatie en gegevensuitwisseling met burgers en bedrijven en een set voorzieningen die vooral gericht is op de communicatie en gegevensuitwisseling tussen overheden dan wel op de onderliggende infrastructuur.

Door een beperkte set van voorzieningen te onderzoeken:
- Reduceren we de administratieve lasten voor de beheerders van voorzieningen;
- Vergroten we de tijd tussen de onderzoeken zodat meer ruimte ontstaat voor de implementatie van de standaarden;
- Vergroten we de leesbaarheid van de rapportage. Door de logische tweedeling is het rapport minder lijvig.

Dit jaar zijn de voorzieningen onderzocht die direct raken aan de communicatie en gegevensuitwisseling met burgers en bedrijven.

1.3 Werkwijze

Voor dit onderzoek is gebruik gemaakt van de 'pas toe of leg uit'-lijst van 1 april 2020. Voor elke voorziening is gekeken of de standaarden op deze lijst relevant zijn. Daarbij is telkens uitgegaan van de eindgebruiker. Dat is degene die in de keten baat zou moeten hebben bij het gebruik van open standaarden. Dit is expliciet zo gekozen, omdat het beleid ten aanzien van standaardisatie vooral gericht is op het stimuleren van interoperabiliteit. In eerdere onderzoeken is gebleken dat beheerders van voorzieningen soms terminologie gebruiken zoals 'voorbereid' zijn op een standaard, het ‘deels geïmplementeerd’ hebben of 'standaard xyz-ready zijn’. Hiermee bedoelen zij dat ze zelf voldoen aan de standaard of bezig zijn de standaard te implementeren, maar dat de andere partijen in hun keten nog geen gebruik kunnen maken van de standaard. Er is bijgevolg dan ook geen sprake van interoperabiliteit op basis van gebruik van de standaard. Wanneer er geen sprake is van interoperabiliteit hebben we dat in deze rapportage aangegeven.

In dit onderzoek wordt per voorziening een overzicht opgesteld van relevante standaarden en de mate waarin daarvan gebruik wordt gemaakt. Het vertrekpunt daarbij is telkens het overzicht van vorig jaar. Waar

mogelijk zijn de standaarden opnieuw getoetst. Daarbij maken we onder meer gebruik van de testen die beschikbaar zijn via https://internet.nl. Hiermee kan voor een groot deel van de standaarden getoetst worden of eraan voldaan wordt[1]. Daarnaast kijken we – voor zover mogelijk – of de geplande activiteiten inmiddels uitgevoerd zijn. Voor nieuwe voorzieningen maken we een inschatting welke standaarden relevant zijn. Voor nieuwe standaarden op de lijst maken we een inschatting of ze relevant zijn voor de voorzieningen.

Op basis van bovenstaande inschattingen en toetsen maken we een eerste overzicht per voorziening. Dat overzicht wordt met een aantal expliciete vragen toegestuurd aan de vertegenwoordigers van de voorzieningen. Op basis van hun reactie wordt de verzamelde informatie aangescherpt. Het resultaat daarvan wordt voorgelegd aan de opdrachtgever, vervolgens in een definitieve versie toegestuurd aan de vertegenwoordigers van de voorzieningen en na akkoord opgenomen in de rapportage. Meestal heeft dit proces meerdere iteraties nodig. Daar waar verschillen van mening zijn over het al dan niet voldoen aan de standaarden, zijn deze verschillen nader met elkaar besproken. In de gevallen waar de verschillen ook na de gesprekken bleven bestaan, is dit duidelijk opgenomen in de rapportage.

1.4 Aandachtspunten voor de lezer

1.4.1 Voorzieningen en standaarden geordend op basis van functionaliteit

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

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

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

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

[2] https://www.forumstandaardisatie.nl/sites/bfs/files/Lijst_verplichte_open_standaarden_sept-2018_0.pdf

1.4.2 Status

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

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

1.4.3 Relevantie standaard

Voor de relevantiebepalingen zijn per standaard de beschrijvingen van het functioneel toepassingsgebied en van het organisatorisch toepassingsgebied, zoals vermeld op de pas-toe-of-leg-uit lijst van het Forum Standaardisatie gehanteerd.[5] Standaarden die niet relevant zijn voor een voorziening, zijn niet in de tabel opgenomen. In een beperkt aantal gevallen is onder de tabel nog een toevoeging opgenomen over standaarden die in de eerste inschatting wel relevant leken, maar dat bij nadere inspectie (nog) niet zijn. Ook in gevallen waar verwarring zou kunnen ontstaan over de relevantie is een nadere toelichting onder de tabel opgenomen. Daarnaast is voor de standaarden die dit jaar nieuw zijn op de lijst, opgenomen of ze relevant zijn. Deze inschatting is samen met de beheerders van de voorzieningen gemaakt.

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 de mate waarin de voorziening voldoet aan de standaarden. Waar de antwoorden van de beheerder en PBLQ afwijken van elkaar geven we dit helder aan in de rapportage. Per voorziening wordt het relevante onderdeel van de rapportage nog ter instemming voorgelegd aan de beheerder. Bovenstaande werkwijze maakt het mogelijk om ondanks de uitdagingen bij het toetsen van standaarden toch tot een volledig en accuraat beeld te komen.

Gebruik van internet.nl

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

[4] De bedoeling hiervan is dus niet dat een voorziening gedeeltelijk aan een standaard voldoet, maar dat *een onderdeel van* de voorziening helemaal aan de standaard voldoet. Voor dit onderdeel is dan in feite de status “Ja” van toepassing, maar niet voor de overige onderdelen. Idealiter zouden op termijn alle onderdelen van een voorziening aan de relevante standaard moeten voldoen.

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

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

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

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

Webrichtlijnen en Digitoegankelijk

Op 24 mei 2018 is het Tijdelijk besluit digitale toegankelijkheid overheid gepubliceerd in het Staatsblad. Het besluit, dat de Europese toegankelijkheidsrichtlijn (2016/2102) omzet in bindende nationale regelgeving, is per 1 juli 2018 in werking getreden. Het doel is om de toegankelijkheid van websites en mobiele applicaties (apps) van overheidsinstanties te waarborgen.
Het besluit maakt deel uit van een breder pakket aan maatregelen dat een inclusieve benadering van digitale overheidsdienstverlening moet realiseren. Uitgangspunt daarbij is dat mensen met en zonder beperking op gelijke basis moeten kunnen deelnemen aan de maatschappij. Als websites goed in elkaar zitten kunnen ze door iedereen worden gebruikt, ook door bezoekers met een beperking.
Concreet moeten overheden vanaf 23 september 2020 voldoen aan het besluit. Vanaf deze datum moeten overheidsinstanties de toegankelijkheidsnorm toepassen op al hun websites. Als een website nog niet volledig toegankelijk is, dan moet de organisatie op basis van een gestructureerde aanpak en binnen een redelijk haalbare termijn, toewerken naar volledig voldoen aan alle toegankelijkheidseisen. In een toegankelijkheidsverklaring, die is ondertekend door een bestuurder of een verantwoordelijk functionaris, wordt verklaard hoever de overheidsinstantie is gevorderd met de toegankelijkheid van de website.
Momenteel is de wijze waarop overheden omspringen met de verplichting nog zeer divers. Gelet daarop en gelet op het feit dat 23 september 2020 bij de start van dit onderzoek nog een half jaar verder lag, is in overleg met de opdrachtgever besloten pas volgend jaar te toetsen op het al dan niet hebben van een toegankelijkheidsverklaring. We zullen dan ook (in overleg met de beheerder van de standaard) kijken of er een verdere objectivering van de beoordeling van het al dan niet voldoen aan de standaard mogelijk en wenselijk is.

ISO 27001/2, en de BIO

Vanaf 1 januari 2020 is de Baseline Informatiebeveiliging Overheid (BIO) van kracht. De BIO vervangt de bestaande baselines informatieveiligheid voor Gemeenten, Rijk, Waterschappen en Provincies. Binnen de Rijksoverheid dient elke organisatie een eigen implementatie van de BIO te hebben. De BIO is gestructureerd op de ISO 27001 en ISO 27001/2 standaard. Indien een organisatie voldoet aan de BIO, 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.

RPKI

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

De standaard RPKI staat sinds eind november 2019 op de pas-toe-of-leg-uit lijst van het Forum Standaardisatie. De standaard moet voorkomen dat internetverkeer wordt omgeleid naar systemen van niet-geautoriseerde netwerken en is instrumenteel in het voorkomen van een 'hijack' van het verkeer. De standaard draagt daarmee bij aan het voorkomen van het afhandig maken van gegevens van gebruikers en/of het (on)bewust bereikbaar maken van bepaalde websites.
In het onderzoek is gebleken dat er onduidelijkheid was bij een groot aantal beheerders van voorzieningen over de vraag of de standaard voor hen van toepassing is.

- RPKI is een standaard die sterk 'onder de motorkap' zit, en daarmee ver afstaat van het werk van de gemiddelde beheerder van een voorziening. In veel gevallen gaat men ervan uit dat de netwerkleverancier dit regelt.
- Daarnaast wekt het functioneel toepassingsgebied in de lijst met standaarden verwarring. In schijnbare tegenstelling tot de tekst bij het organisatorisch functioneringsgebied ("van toepassing op overheden en instellingen uit de publieke sector") geeft het functioneel toepassingsgebied aan dat RPKI moet worden toegepast door netwerkaanbieders en houders van blokken IP-adressen bij het aanbieden van netwerkconnectiviteit.

Vanwege de verwarring is in overleg met Bureau Forum Standaardisatie besloten de standaard dit jaar nog niet in de tabel op te nemen. We hebben in het kader van dit onderzoek wel getoetst[7] of de standaard wordt toegepast en naar aanleiding van het onderzoek hebben ook een aantal voorzieningen de standaard alsnog geadopteerd. Uit het onderzoek blijkt dat 3 voorzieningen inmiddels wel voldoen aan de standaard, en dat nog 13 voorzieningen de standaard moeten adopteren. Alle voorzieningen die niet voldoen hebben daarnaast een mail ontvangen met deze boodschap. In een volgende monitor wordt de standaard wel in de tabel opgenomen.

2. Identificeren en authenticeren

2.1 DigiD

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	DigiD mail wordt verstuurd met een DKIM signature (zie: https://internet.nl/mail/digid.nl/).

[7] De toetsing van RPKI is in samenwerking met het Bureau Forum Standaardisatie uitgevoerd. Voor de toetsing zijn de relevantie ip-adressen van de voorzieningen gecontroleerd via https://stat.ripe.net/46.22.185.32#tabId=routing

DMARC (Anti-phishing)	Ja	DMARC is voor DigiD geconfigureerd als een van de anti-phishing maatregelen (zie: https://internet.nl/mail/digid.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC is doorgevoerd in de domeinen (DNS-zones) van DigiD en operationeel. Ook de mailservers voldoen aan de standaard (zie: https://internet.nl/site/digid.nl/ en https://internet.nl/mail/digid.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	DigiD maakt gebruik van HTTPS voor de communicatie tussen clients (zoals browsers) en servers. Verder ondersteunt de DigiD website HSTS-policy met een geldigheidsduur van 1 jaar (zie: https://internet.nl/site/digid.nl/).
IPv4 en IPv6 (Internetnummers)	Ja	De website DigiD.nl is via IPv6 toegankelijk. Inmiddels verlopen ook de mailstromen via IPv6 (zie https://internet.nl/mail/digid.nl/ en https://internet.nl/site/digid.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Overheid (BIO) van toepassing die is gebaseerd op NEN-ISO27001/2. Logius heeft zich over toepassing van deze norm verantwoord door het afgeven van In Control Verklaringen (ICV's) aan de eigenaar (BZK/DGOBR).
SAML (Inloggegevens)	Ja	DigiD biedt aan afnemers een SAML-koppelvlak om authenticaties uit te kunnen voeren. Wanneer de afnemer “single sign on” wil gebruiken is dit alleen mogelijk via het SAML koppelvlak. De SAML koppelvlak-specificaties van DigiD zijn gepubliceerd op de website van Logius (zie: https://www.logius.nl/sites/default/files/public/bestanden/diensten/DigiD/Koppelvlakspecificatie-SAML-DigiD.pdf)
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is relevant voor DigiD bij alle mails vanuit de DigiD applicatie, en DigiD voldoet ook aan deze standaard (zie: https://internet.nl/mail/digid.nl/).
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Ja	De mailservers van DigiD passen STARTTLS/DANE toe (zie: https://internet.nl/mail/digid.nl/). Vanwege ondersteuning van oudere e-mailservers is een risicoafweging gemaakt om de TLS-versies 1.0 en 1.1 te blijven aanbieden.
TLS (Beveiligde, versleutelde verbindingen)	Ja	DigiD ondersteunt voor de website-domeinen alleen TLS v1.2. Voor het backend-domein digid.nl is vanwege ondersteuning van afnemers met oudere backend-systemen een risicoafweging gemaakt om nog een aantal “uit te faseren” ciphersuites te handhaven.

Ten opzichte van 2019 voldoet de voorziening aan STARTTLS/DANE.

Concluderend zijn er geen standaarden die DigiD nog (volledig) dient te implementeren.

2.2 DigiD Machtigen

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	DigiD Machtigen ontvangt en verstuurt 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 BIO 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)	Ja	Het authenticatiekoppelvlak met eHerkenning voldoet aan de SAML standaard. Het authenticatiekoppelvlak met DigiD maakt gebruik van SAML. Overgang naar een SAML koppelvlak is gerealiseerd met de livegang van de nieuwe website voor het DigiD Machtigen (publieke machtigingenregister), 10 juni 2020. 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 verstuurt geen email aan gebruikers. Er is wel een SPF record aangemaakt voor het domein: machtigen.digid.nl welke aangeeft dat er vanaf dit domein geen email wordt verstuurd.
TLS (Beveiligde, versleutelde verbindingen)	Gepland	TLS is geïmplementeerd. DigiD Machtigen ondersteunt TLS v1.2. TLS 1.0 en 1.1 worden niet meer ondersteund. We hebben nog een waarschuwing voor cypher volgorde en we ondersteunen onvoldoende veilige parameters voor Diffie-Hellman-sleuteluitwisseling. Dit staat op de planning voor de patchronde van juli 2020.
		Document en (web/app)content
PDF/A en PDF 1.7	Ja	De voorziening voldoet aan deze standaard.

(Document-publicatie/ archivering)		
		Stelselstandaarden
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 (Een koppelvlak waarover een aangesloten dienstaanbieder kan controleren of iemand daadwerkelijk gemachtigd is om te handelen namens een vertegenwoordigde)). Deze koppelvlakken bestaan uit de tijd dat de Digikoppeling standaard in ontwikkeling was en voldoen deels aan de uiteindelijk ontstane Digikoppeling standaard. Het is de bedoeling dat bestaande dienst afnemers overgaan naar de nieuwe koppelvlakken. Hier wordt niet actief op gestuurd. Door ontwikkelingen rondom eID, eIDAS en DigiD Machtigen moeten afnemers in de toekomst gebruik maken van andere koppelvlakken, waardoor gebruik van de niet compliant koppelvlakken zal afnemen. Bij nieuwe koppelvlakontwikkelingen zal meer naar de REST-API standaard worden gekeken dan naar Digikoppeling 2.0.

Ten opzichte van 2019 voldoet DigiD Machtigen aan SAML. De voorziening voldoet niet aan TLS, waardoor de status van ja naar gepland gaat.

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

2.3 PKIoverheid

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	Pkioverheid.nl voldoet aan DMARC (zie: https://internet.nl/mail/pkioverheid.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	Het PKIoverheid-deel van de website van Logius en de website van PKIoverheid maken gebruik van DNSSEC (zie: https://internet.nl/domain/crl.pkioverheid.nl/ en https://internet.nl/domain/www.logius.nl/).

HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Deels	Deze standaard wordt toegepast door de voorziening (zie: https://internet.nl/domain/crl.pkioverheid.nl/ en https://internet.nl/domain/www.logius.nl/). Voor logius.nl, crl.pkioverheid.nl en cert.pkioverheid.nl is HTTPS goed geconfigureerd. pkioverheid.nl en www.pkioverheid.nl verwijzen door (oftewel 'redirecten') naar cert.overheid.nl. Alleen voor deze domeinen faalt de test op het punt "HTTPS-doorverwijzing". Met het ingaan van het nieuwe contract is het compliant maken aan de open standaarden van de website pkioverheid.nl een van de projecten die hierin is opgenomen.
IPv4 en IPV6 (Internetnummers)	Nee	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/). De implementatiedatum is gekoppeld aan gunning van een nieuw contract aan applicatieleverancier. Gunning heeft inmiddels plaatsgevonden. Implementatie van IPV6 is een van de projecten die in dit contract is opgenomen. Planning hiervan heeft nog niet plaatsgevonden.
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 BIO is daarnaast uitgevoerd op basis van best effort.
TLS	Ja	Het PKIoverheid deel van de website van Logius maakt gebruik van TLS 1.1 en 1.2 en de website van PKIoverheid zelf maakt gebruik van TLS 1.2 (zie: https://internet.nl/domain/crl.pkioverheid.nl/ en https://internet.nl/domain/www.logius.nl/). Uit te faseren ciphers voor pkioverheid.nl worden opgepakt bij vernieuwing van website.
		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 2019 is de planning voor implementatie van IPv4 en IPv6 niet gehaald. Er is geen nieuwe planning afgegeven. De status gaat van gepland naar nee.

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

2.4 Afsprakenstelsel elektronische toegangsdiensten

Beheerorganisatie: Logius

Werking en inhoud van het Afsprakenstelsel Elektronische Toegangsdiensten
Het Afsprakenstelsel Elektronische Toegangsdiensten is een set van technische, functionele, juridische en organisatorische afspraken op basis waarvan het netwerk van eHerkenning wordt geleverd in een publiek-private samenwerking. Dat betekent dat het netwerk wordt geleverd door private dienstverleners, waarbij er publieke ondersteunende diensten zijn (in beheer bij de 'Beheerorganisatie eHerkenning'). 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.

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 eHerkenning en is in beheer bij de 'Beheerorganisatie eHerkenning', die is ondergebracht bij Logius. Het afsprakenstelsel is sterk aan veranderingen onderhevig. Zo was Idensys tot voor kort nog onderdeel van het stelsel, wordt het inloggen vanuit Europa bij overheidsinstellingen in Nederland sinds begin 2019 ondersteund (eIDAS) en kan men vanaf eind 2020 via het stelsel inloggen in Europa met een Nederlands inlogmiddel (eIDAS).

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	Bij verstuurde e-mail wordt DKIM toegepast, bij ontvangst gebeurt dit door de centrale e-mailvoorziening, die Logius als dienst afneemt van het Shared Service Centrum van het Rijk (SSC-ICT).
DMARC (Anti-phishing)	Gepland	Het Afsprakenstelsel Elektronische Toegangsdiensten maakt geen gebruik van e-mailfunctionaliteit, maar de policy voor ondersteunende e-maildiensten is niet voor Q1 2020 aangescherpt. Door een scopewijziging bij een aanbesteding wordt een oude component later dan voorzien uit productie genomen, waardoor de policy nog niet aangescherpt kon worden. De nieuwe planning is uiterlijk Q4 2020 volledig compliant te zijn. (Zie: https://internet.nl/mail/eherkenning.nl/)
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC werd in 2015 in de productieomgeving opgenomen.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	HTTPS en HSTS wordt toegepast op alle websites en webapplicaties onder beheer van de beheerorganisatie en deelnemers in het stelsel.
IPv4 en IPv6 (Internetnummers)	Deels	Het Afsprakenstelsel Elektronische Toegangsdiensten voldoet aan IPv4 en IPv6. Ondersteunende e-mailservers, die geen onderdeel uitmaken van het netwerk, voldoen niet volledig. (Zie: https://internet.nl/mail/eherkenning.nl/). Voor inkomende e-mail wordt door Logius gebruik gemaakt van de dienstverlening van het Shared Service Centrum van het Rijk (SSC-ICT).
NEN-ISO/IEC 27001/27002	Ja	In het afsprakenstelsel wordt certificering tegen ISO27001 geëist voor de deelnemers. De beheerorganisatie eHerkenning is als

(Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)		stelselbeheerder ook gecertificeerd volgens ISO 27001. Daarvoor is ook een in control statement beschikbaar.
SAML (Inloggegevens)	Ja	SAML is een verplichte eis vanuit het stelsel.
SPF (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)	Ja	STARTTLS is geïmplementeerd voor eherkenning.nl en idensys.nl. DANE voor SMTP is voor de maildomeinen geïmplementeerd bij de centrale e-mailvoorziening, die Logius als dienst afneemt van het Shared Service Centrum van het Rijk (SSC-ICT).
TLS (Beveiligde, versleutelde verbindingen)	Deels	Het Afsprakenstelsel Elektronische Toegangsdiensten stelt het gebruik van TLS volgens de richtlijnen van het NCSC verplicht. Ondersteunde e-mailservers, die geen onderdeel uitmaken van het netwerk, voldoen niet volledig (zie: https://internet.nl/mail/eherkenning.nl/). Voor inkomende e-mail wordt door Logius gebruik gemaakt van de dienstverlening van het Shared Service Centrum van het Rijk (SSC-ICT).
		Document en (web/app)content
PDF 1.7, PDF/A-1 of PDF/A-2 (Documentpublicatie/ archivering)	Ja	Primair wordt de stelseldocumentatie via HTML op eherkenning.nl gepubliceerd. Stelseldocumentatie wordt met behulp van officesoftware 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 2019 voldoet de voorziening nog deels aan TLS. De status van deze standaard is van ja naar deels gegaan. De planning voor het implementeren van DMARC is niet gehaald, de status blijft gelijk.

Concluderend moeten voor Afsprakenstelsel Elektronische Toegangsdiensten nog de volgende standaarden (volledig) worden geïmplementeerd: DMARC, IPv4 en IPv6, TLS.

3. Dienstverlening en informatieverstrekken

3.1 MijnOverheid

Beheerorganisatie: Logius

Werking en inhoud van MijnOverheid
MijnOverheid is een persoonlijk toegangsportaal waarin verschillende diensten van de overheid ontsloten worden. MijnOverheid gaat over persoonlijke, en om die reden met DigiD beveiligde, diensten en informatie. Binnen MijnOverheid heeft de burger toegang tot de Berichtenbox, Lopende Zaken en Persoonlijke Gegevens. De Berichtenbox is de persoonlijke brievenbus waarin burgers post van onder meer de

Belastingdienst, RDW, SVB, UWV, gemeenten en pensioenfondsen kunnen ontvangen. Lopende Zaken geeft weer wat de stand is van bijvoorbeeld aanvragen of vergunningen. Inzage Persoonlijke Gegevens maakt het mogelijk om te controleren of de eigen gegevens correct zijn opgeslagen bij de overheid. Logius is verantwoordelijk voor het portaal, de aangesloten partijen zijn verantwoordelijk voor hun eigen dienstverlening die via MijnOverheid benaderd kan worden.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/ phishing)	Ja	MijnOverheid voldoet aan DKIM (zie: https://internet.nl/mail/mijnoverheid.nl/ en https://internet.nl/mail/mijn.overheid.nl/).
DMARC (Anti-phishing)	Ja	Deze standaard wordt toegepast.
DNSSEC (Beveiligde domeinnamen)	Ja	MijnOverheid voldoet aan DNSSEC (zie: https://internet.nl/site/mijnoverheid.nl/ en https://internet.nl/site/mijn.overheid.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	HTTPS wordt toegepast voor zowel het domein mijn.overheid.nl, als mijnoverheid.nl. HSTS wordt toegepast voor het domein mijn.overheid.nl. HSTS voor mijnoverheid.nl is niet van toepassing, omdat die enkel redirect naar mijn.overheid.nl.
IPv4 en IPV6 (Internetnummers)	Ja	MijnOverheid gebruikt het Logius infrastructuurplatform. Dit platform ondersteunt de open standaard IPv4 en IPv6 voor internetgebruik. MijnOverheid ondersteunt op dit moment IPv4 en IPv6. Mijn.overheid.nl voldoet aan de standaard. IPv6 staat niet op de inkomende mailservers er bestaat ook geen planning voor om dit wel te doen.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Op de Rijksoverheid is de BIO 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 (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. MijnOverheid gebruikt TLS 1.2 en veilige

		cipher suites. Een aantal oude ciphers wordt nog ondersteund omdat er anders problemen ontstaan bij afnemers, burgers e.d. TLS 1.3 moet nog geïmplementeerd worden. Oudere versies worden niet meer geaccepteerd.
		Document en (web/app)content
Open API Specification (Beschrijven van REST API's)	Ja	Deze standaard wordt gebruikt voor de REST-API's van MijnOverheid.
PDF 1.7, PDF/A-1 of PDF/A-2 (Documentpublicatie/archivering)	Ja	MijnOverheid genereert zelf PDF-bestanden welke voldoen aan de PDF/A-1a standaard. MijnOverheid neemt concrete stappen om te gaan controleren op de toegankelijkheid en veiligheid van PDF-bestanden die aangeleverd worden door afnemers via de Berichtenbox.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Zowel nieuwe als oude koppelingen worden conform Digikoppeling 2.0 ingericht.
StUF (Uitwisseling administratieve overheidsgegevens)	Ja	MijnOverheid heeft waar relevant de koppeling op basis van StUF. Dit is alleen relevant voor WOZ en Lopende Zaken.

Ten opzichte van 2019 is de status van IPv4 en IPv6 van deels naar ja gegaan. HTTPS/HSTS is – ondanks negatieve score op internet.nl - goedgekeurd naar aanleiding van handmatige analyse door onderzoekers van het Bureau Forum Standaardisatie.

Concluderend zijn er geen standaarden die mijnOverheid nog (volledig) moet implementeren.

3.2 Berichtenbox voor bedrijven

Beheerorganisatie: Rijksdienst voor Ondernemend Nederland (RVO).

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

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

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	@antwoordvoorbedrijven.nl en @berichtenbox.antwoordvoorbedrijven.nl voldoen hieraan. Dit kan gecontroleerd worden op https://internet.nl/mail/antwoordvoorbedrijven.nl en https://internet.nl/mail/berichtenbox.antwoordvoorbedrijven.nl N.B. De notificaties de we sturen hebben als afzender noreply-berichtenbox@antwoordvoorbedrijven.nl
DMARC (Anti-phishing)	Ja	@antwoordvoorbedrijven.nl en @berichtenbox.antwoordvoorbedrijven.nl voldoen hieraan. Dit kan gecontroleerd worden op https://internet.nl/mail/antwoordvoorbedrijven.nl en https://internet.nl/mail/berichtenbox.antwoordvoorbedrijven.nl N.B. De notificaties de we sturen hebben als afzender noreply-berichtenbox@antwoordvoorbedrijven.nl
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)	Gepland	HTTPS/HSTS is al operationeel op de Berichtenbox maar is nog niet volledig geïmplementeerd. HTTPS/HSTS wordt RvO breed gerealiseerd (overgang naar nieuwe SOAP versie; zogenaamde cloud migratie), staat gepland voor realisatie uiterlijk medio 2021.
IPv4 en IPv6 (Internetnummers)	Gepland	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 implementatie moet DICTU-breed gebeuren voordat dit voor de Berichtenbox gedaan zal worden. IPv6 wordt RvO breed gerealiseerd en is onderdeel van de toegangsverleningsservice (TVS) voorziening en moet ultimo 2021 zijn gerealiseerd.
SAML (Inloggegevens)	Ja	eHerkenning is SAML-based en wordt toegepast voor het inloggen op de Berichtenbox.
SPF (Preventie van mailspoofing/phishing)	Ja	@antwoordvoorbedrijven.nl en @berichtenbox.antwoordvoorbedrijven.nl voldoen hieraan. Dit kan gecontroleerd worden op https://internet.nl/mail/antwoordvoorbedrijven.nl en https://internet.nl/mail/berichtenbox.antwoordvoorbedrijven.nl N.B. De notificaties de we sturen hebben als afzender noreply-berichtenbox@antwoordvoorbedrijven.nl
TLS (Beveiligde, versleutelde verbindingen)	Nee	De Berichtenbox maakt gebruik van TLS 1.2 (zie: https://internet.nl/site/www.berichtenbox.antwoordvoorbedrijven.nl/). Client-initiated renegotiation komt niet door de test. Client-initiated renegotiation (CIR) heeft impact op de beschikbaarheid en niet op de vertrouwelijkheid. Kort samengevat: wij zien CIR niet als een

		beveiligingsissue en is ook niet als zodanig in de Pentest naar voren gekomen.
		Document en (web/app)content
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/ archivering)	Ja	Alle berichten kunnen worden gedownload (vanaf de Berichtenbox website) in PDF/A formaat. PDF-documenten worden gegenereerd in PDF A/1.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Overheden kunnen via Digikoppeling geautomatiseerd berichten verzenden en ontvangen. Ondernemers kunnen alleen handmatig (via de website) hun Berichtenbox gegevens opvragen.
StUF (Uitwisseling administratieve overheidsgegevens)	Ja	StUF wordt in combinatie met Digikoppeling gebruikt voor de uitwisseling met alle partijen die via digikoppeling op de Berichtenbox zijn aangesloten.

Ten opzichte van 2019 voldoet de voorziening aan DMARC, DKIM en SPF, de status van HTTPS/HSTS is van ‘ja’ naar ‘gepland’ gegaan en de status van IPv4 en IPv6 is van ‘nee’ naar ‘gepland’ gegaan.

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

3.3 Overheid.nl

Beheerorganisatie: Kennis- en Exploitatiecentrum Officiële Overheidspublicaties (KOOP)

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	DKIM is geïmplementeerd (zie: https://internet.nl/mail/overheid.nl/).
DMARC (Anti-phishing)	Ja	DMARC is volledig doorgevoerd.
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)	Ja	Overheid.nl voldoet aan HTTPS en HSTS (zie: https://internet.nl/site/overheid.nl/).

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 BIO 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	Overheid.nl voldoet hieraan (zie: https://internet.nl/mail/overheid.nl/).
TLS (Beveiligde, versleutelde verbindingen)	Gepland	Op de website is het volledig doorgevoerd. De mailomgeving geeft een melding. Deze wordt opgelost in oktober 2020.
		Document en (web/app)content
OWMS (Metadata overheidsinformatie)	Ja	Overheid.nl is gemetadateerd conform OWMS.
PDF 1.7 PDF/A-1 PDF/A-2 (Documentpublicatie/ archivering)	Ja	Alle PDF's van officiële bekendmakingen zijn PDF/A-1a zoals wettelijk bepaald is.
SKOS (Thesauri en begrippenwoordenboeken)	Ja	SKOS is geïmplementeerd voor de waardelijsten van OWMS.
		Juridische identificatie en verwijzing
BWB (Wet- en regelgeving)	Ja	Overheid.nl is zelfs de bron van de BWB identificatie (zie: wetten.overheid.nl).
JCDR (Decentrale regelgeving)	Ja	Overheid.nl is zelfs de bron van de JCDR identifiers (zie: https://zoek.overheid.nl/lokale_wet_en_regelgeving).

Ten opzichte van 2019 voldoet de voorziening aan HTTPS en HSTS, maar niet langer (volledig) aan TLS.

Concluderend moeten voor Overheid.nl nog de volgende standaarden (volledig) worden geïmplementeerd: TLS.

3.4 Ondernemersplein

Beheerorganisatie: Kamer van Koophandel

Ondernemersplein is een onderdeel van de website van de Kamer van Koophandel. Dat heeft geleid tot een effect ten aanzien van het gebruik van standaarden en de wijze van rapporteren daarvan namelijk in het jaarverslag (miv 2020). KVK heeft op kwartaalbasis een interne WDO scan ingericht waarmee haar business owners kunnen sturen op compliancy aan de WDO. WDO is een superset van de standaarden die via de Monitor gedekt worden.

Werking en inhoud van Ondernemersplein

Het Ondernemersplein is de centrale plek (website) waar overheden gezamenlijke informatie en hulpmiddelen aanbieden voor ondernemers, variërend van praktische stappenplannen en webinars tot informatie over regelgeving en geldzaken. Daarnaast bestaat de mogelijkheid voor overheden de content van Ondernemersplein via hun eigen kanalen te ontsluiten. Ondernemersplein.kvk.nl is de vervanger van ondernemersplein.nl, die sinds 2019 slechts doorverwijst.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Deels	DKIM is geïmplementeerd voor domein kvk.nl maar niet specifiek voor het subdomein ondernemersplein.kvk.nl.
DMARC (Anti-phishing)	Ja	Ondernemersplein als onderdeel van kvk.nl voldoet aan DMARC.
DNSSEC (Beveiligde domeinnamen)	Ja	Ondernemersplein voldoet aan DNSSEC voor de website. Er wordt niet gemaild vanuit mail subdomein maar van kvk.nl.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	Aan deze standaard wordt voldaan voor het domein kvk.nl
IPv4 en IPV6 (Internetnummers)	Nee	IPv4 klaar, IPv6 target : eind 2021 conform overheidsbrede afspraken
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	Ondernemersplein is onderdeel van de website van de Kamer van Koophandel. KVK is ISO 27001 gecertificeerd vanaf 2016. KVK is in 2019 opnieuw succesvol gecertificeerd.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd voor kvk.nl.
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Nee	Aan STARTTLS wordt voldaan, maar aan DANE wordt nog niet voldaan. De KvK vindt de relevantie van DANE voor mail laag: er zijn geen mailservers die DANE geïmplementeerd hebben.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De websites ondernemersplein.kvk.nl en www.kvk.nl zijn TLS 1.2 of beter beveiligd.
		Document en (web/app)content
CMIS	Nee	De tooling (CMS/ESB) ondersteunt de standaard, maar deze wordt niet actief gebruikt. Er zijn geen content leveranciers die hun

(Content-uitwisseling tussen CMS-/DMS-systemen)		CMS in CMIS vorm aan het Ondernemersplein beschikbaar stellen. Concreet is er dus nog geen toepassing op dit moment en er zijn ook nog geen plannen om dit te doen.
OWMS (Metadata overheidsinformatie)	Nee	De informatie op de website is gemetadateerd volgens een eigen model die past bij de metadatering van de partners.
		Juridische identificatie en verwijzing
BWB (Wet- en regelgeving)	Ja	Binnen de website, de content van AvB, wordt verwezen naar wetgeving conform de BWB standaard.

Ten opzichte van 2019 voldoet Ondernemersplein aan DNSSEC, HTTP/HTTPS en SPF.

Concluderend, moet Ondernemersplein nog de volgende standaarden (volledig) implementeren: DKIM, IPv6, DANE, CMIS en OWMS.

3.5 Samenwerkende catalogi

Beheerorganisatie: Logius

Inhoud en werking van Samenwerkende Catalogi
Samenwerkende Catalogi koppelt de productcatalogi van verschillende overheidsorganisaties. De koppeling van productcatalogi door Samenwerkende Catalogi maakt het ‘no wrong door’- principe mogelijk. Dit bekent dat over organisatiegrenzen heen gezocht kan worden naar producten en diensten. Het is de standaard (specificatie) voor het publiceren en uitwisselen van metadata over producten en diensten binnen de overheid, zoals bijvoorbeeld het aanvragen van een vergunning of het aanvragen van een reisdocument. Deze productinformatie is voor iedereen doorzoekbaar door middel van een API. De eindgebruiker gebruikt de portalen Overheid.nl en Ondernemersplein.nl. Zowel Overheid.nl als het Digitaal Ondernemersplein haalt de productinformatie uit de SC API.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DMARC (Anti-phishing)	Ja	De online validatieservice controleert of Samenwerkende Catalogi XML-bestanden op de juiste wijze zijn opgemaakt en de metadata voldoen aan de technische specificaties van Samenwerkende Catalogi en de Overheid.nl Web Metadata Standaard OWMS. De validator is benaderbaar via een subdomein van Logius (scvalidator.logius.nl). De validator voldoet aan deze standaard.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	nee	De validator van Samenwerkende Catalogi voldoet niet meer aan HTTPS. Gepland is om dit mee te nemen in de migratie naar een andere provider. De verwachting is dat dit in 2020 gaat plaatsvinden.
IPv4 en IPv6 (Adressering van ICT-systemen binnen een netwerk)	Ja	Zowel de informatieve pagina’s op logius.nl als de validator zelf zijn voorzien van IPv4 en IPv6 adressen. Dit na een migratie van beide omgevingen.
SPF	Ja	De validator van Samenwerkende Catalogi voldoet aan deze standaard.

(Preventie van mailspoofing/phishing)		
TLS (Beveiligde, versleutelde verbindingen)	Nee	De validator van Samenwerkende Catalogi voldoet niet meer aan deze standaard. Gepland is om dit mee te nemen in de migratie naar een andere provider. De verwachting is dat dit in 2020 gaat plaatsvinden.
		Document en (web/app)content
Open API Specification (Beschrijven van REST API's)	Ja	Samenwerkende catalogi voldoet aan deze standaard.
OWMS (Metadata overheidsinformatie)	Ja	Samenwerkende catalogi is volledig gebaseerd op OWMS.

Ten opzichte van 2019 voldoet de voorziening aan DMARC en SPF. De statussen van deze standaarden gaan van gepland naar ja. De status van HTTPS en HSTS en TLS gaat van gepland naar nee.

Concluderend moeten voor samenwerkende catalogi nog de volgende standaarden (volledig) worden geïmplementeerd: HTTPS/HSTS, TLS.

3.6 RDW.nl

Beheerorganisatie: RDW (Rijksdienst Wegverkeer)

Werking en inhoud van RDW.nl
De website RDW.nl biedt informatie over de dienst wegverkeer (RDW). De RDW beheert onder andere het kentekenregister. De website kent specifieke functies voor particulier- en zakelijk gebruik. Particulieren kunnen via RDW.nl bijvoorbeeld digitaal een keuringsafspraak voor hun auto maken of een kentekenbewijs voor de brommer of scooter aanvragen. Bedrijven kunnen via RDW.nl bijvoorbeeld kentekenbewijzen voor bedrijfsvoertuigen aanvragen en ontheffingen voor transporteurs regelen. Voor digitale diensten en producten verwijst RDW.nl naar onderliggende domeinen. Het is daarnaast voor particulieren mogelijk om via DigiD in te loggen op RDW.nl om eigen gegevens te raadplegen.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	De BRV (basisregistratie voertuigen) voldoet aan DKIM.
DMARC (Anti-phishing)	Gepland	De BRV voldoet aan DMARC. Rdw.nl voldoet niet aan de standaard, zie: https://internet.nl/mail/rdw.nl/. De RDW is in 2017 gestart met een nieuwe leverancier. Doordat de implementatie van de digitale werkomgeving langer heeft geduurd dan beoogd, is dit tot op heden nog niet uitgevoerd. Augustus 2019 is RDW gestart om privacy en security verder te gaan verbeteren. Medio 2020 is deze verbetering doorgevoerd.

DNSSEC (Beveiligde domeinnamen)	Deels	De niet-gevoelige (technische) gegevens uit de BRV zijn te bevragen via www.rdw.nl. Alle .nl rdw domeinen zijn gesigned met DNSSEC. De diensten op (voertuig)gegevens draaien als microservices in de Azure cloud en het is bekend dat hierop geen DNSSEC en daarmee ook DANE mogelijk is. RDW en andere overheidspartijen hebben bij Microsoft gevraagd om dit op te lossen.
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Gepland	Implementatie zou medio 2018 gerealiseerd worden. Rdw.nl voldoet niet aan de standaard, zie: https://internet.nl/site/rdw.nl/. De RDW is in 2017 gestart met een nieuwe leverancier. Doordat de implementatie van de digitale werkomgeving langer heeft geduurd dan beoogd, is dit tot op heden nog niet uitgevoerd. Augustus 2019 is RDW gestart om privacy en security verder te gaan verbeteren. Medio 2020 is deze verbetering doorgevoerd. De diensten op (voertuig)gegevens, die als microservices in de Azure cloud draaien, voldoen wel aan HTTPS/HSTS.
IPv4 en IPv6 (Internetnummers)	Nee	IPv4 wordt ondersteund, IPv6 wordt nog niet ingezet. De BRV is te bevragen via www.rdw.nl. Op dit moment ziet de RDW voor de BRV nog geen noodzaak om op IPv6 over te gaan.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De BRV voldoet aan deze standaard.
SAML (Inloggegevens)	Ja	De BRV voldoet aan SAML.
SPF (Preventie van mailspoofing/phishing)	Ja	RDW ondersteunt en gebruikt de SPF standaard voor email verkeer.
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Gepland	Deze zullen uiterlijk Q3 2020 geconfigureerd zijn overeenkomstig de overheidsstandaarden (zie: https://internet.nl/mail/rdw.nl/).
TLS (Beveiligde, versleutelde verbindingen)	Nee	RDW ondersteunt en gebruikt de TLS protocollen op de e-mail servers en Digikoppeling. Er wordt nog gekeken naar verbetering van instellingen, zodat TLS voldoende veilig wordt geïmplementeerd (zie: https://internet.nl/mail/rdw.nl/).
		Document en (web/app)content
CMIS (Content-uitwisseling tussen CMS-/DMS-systemen)	Nee	Inmiddels relevant doordat de RDW bezig is met de ontwikkeling van een centraal Document Management Systeem voor de geautomatiseerde processen. Dit systeem wordt ontsloten via CMIS. In de loop van 2019/2020 zal het document management systeem voor de primaire processen geschikt worden gemaakt voor aansluiting door geautomatiseerde processen. CMIS zal als standaard voor de ontsluiting worden gehanteerd.
Open API Specification	Ja	De BRV voldoet aan Open API Specification.

(Beschrijven van REST API's)		
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.
		E-facturatie en administratie
NLCIUS (Elektronisch factureren)	Nee	De huidige SAP implementatie voldoet hier niet aan. Er zal in de komende periode een aanbesteding plaatsvinden voor het Finance domein waarin deze standaard zal worden meegenomen.
Ades Baseline Profiles	Nee	De RDW voldoet niet aan deze standaard. De RDW heeft een aantal PDF-documenten die op een andere manier worden ondertekend. Er liggen op dit moment geen plannen om deze Ades compatible te maken.

Dit jaar worden alleen de set voorzieningen onderzocht die direct raken aan de communicatie en gegevensuitwisseling met burgers en bedrijven. RDW.nl staat "nieuw" op de lijst. Voor de monitor open standaarden 2021 wordt de set voorzieningen onderzocht die vooral gericht is op de communicatie en gegevensuitwisseling tussen overheden dan wel op de onderliggende infrastructuur. Hieronder valt de BRV. Die wordt volgend jaar separaat onderzocht. Zoals is te zien zijn deze voorzieningen met elkaar verweven.

Concluderend moeten voor RDW.nl nog de volgende standaarden (volledig) worden geïmplementeerd: DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, STARTTLS en DANE, TLS, CMIS, NLCIUS, Ades Baseline Profiles.

3.7 Rijksoverheid.nl

Beheerorganisatie webdomein: Ministerie van AZ (DPC)
Beheerorganisatie maildomein: Onbekend

Werking en inhoud van rijksoverheid.nl
De website Rijksoverheid.nl is de publiekswebsite met informatie van en over alle ministeries. De website wordt verzorgd door de Dienst Publiek en Communicatie (DPC). DPC is een baten-lastendienst van het ministerie van AZ en biedt shared servicediensten aan de rijksoverheid op het gebied van Communicatie. Het e-mail domein @rijksoverheid.nl is in technisch beheer bij SSC-ICT van het ministerie van BZK. Het is niet helder wie zich verantwoordelijk voelt voor het emaildomein. Van het webdomein is AZ eigenaar en beheerder. Voor het maildomein is SSC-ICT de technisch beheerder. Kantekening hierbij is dat AZ/DPC de beheerder is voor de DNS. Vanuit het Bureau Forum Standaardisatie zijn gesprekken gevoerd met betrokken partijen. Daarbij is aangegeven dat er gezocht wordt naar een verantwoordelijke voor het emaildomein.

3.7.1 Maildomein

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/ phishing)	Ja	DKIM is geïmplementeerd (zie: https://internet.nl/mail/rijksoverheid.nl/).
DMARC (Anti-phishing)	Ja	DMARC policy staat op reject, de meest strikte policy (zie: https://internet.nl/mail/rijksoverheid.nl/).
DNSSEC (Beveiligde domeinnamen)	Ja	Rijksoverheid.nl is ondertekend met DNSSEC (zie: https://internet.nl/mail/www.rijksoverheid.nl/). DPC biedt DNSSEC ook aan al haar klanten die domeinen via haar registrar-functie afnemen (zie: https://internet.nl/mail/rijksoverheid.nl/).
IPv4 en IPV6 (Internetnummers)	Gepland	IPv6 is niet voor (alle) mailservers geïmplementeerd (zie: https://internet.nl/mail/rijksoverheid.nl/249091/#). Het technisch beheer van een aantal maildomeinen wordt uitgevoerd door SSC-ICT. De internet facing kant van de DMZ gaat IPv6 in 2020/2021.
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	De leveranciers hebben een NEN 27001/2 implementatie waarin de beveiliging van rijksoverheid.nl meegaat. DPC zelf valt onder de VIR/BIO-implementatie van het moederdepartement AZ. SSC-ICT werkt via deze standaard en wordt hier ook op geaudit. De laatste audits hebben plaatsgevonden in 2019 en 2020.
SPF (Preventie van mailspoofing/phishing)	Ja	Het e-maildomein @rijksoverheid.nl is integraal van SPF voorzien (zie: https://internet.nl/mail/rijksoverheid.nl/). Deze wordt door SSC-ICT beheerd in samenwerking met AZ. Technisch gezien is SSC-ICT het aanspreekpunt.
STARTTLS/DANE (Beveiligd, versleuteld mailverkeer)	Ja	Verzendende mailservers die STARTTLS ondersteunen, kunnen met ontvangende mailserver(s) een beveiligde verbinding opzetten. Rijksoverheid.nl voldoet aan DANE (zie: https://internet.nl/mail/rijksoverheid.nl/). Deze wordt door SSC-ICT beheerd in samenwerking met AZ. Technisch gezien is SSC-ICT het aanspreekpunt.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De nieuwe versies en oude worden ondersteund. Best practice is de oude TLS versies aan laten staan op de mailservers i.v.m. interoperabiliteit. Het uitzetten kan tot gevolg hebben dat er onvercijferd wordt gecommuniceerd.

3.7.2 Webdomein

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
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	De website 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	De leveranciers hebben een NEN 27001/2 implementatie waarin de beveiliging van rijksoverheid.nl meegaat. DPC zelf valt onder de VIR/BIO-implementatie van het moederdepartement AZ.
RPKI (Beveiligen van de routing infrastructuur)	Nee	Het publiceren van ROA's doet Rijksoverheid.nl al langer. Het valideren en het 'droppen' van invalide routes doet Rijksoverheid.nl niet. We denken na over mogelijke toepassing.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Het webdomein van rijksoverheid.nl voldoet aan TLS (zie: https://internet.nl/site/www.rijksoverheid.nl/).
		Document en (web/app)content
ODF 1.2 (Documentbewerkingen)	Ja	Het CMS van het Platform Rijksoverheid Online accepteert slechts ODF (open standaard) formaten. Er zijn wel 'legacy'-bestanden in alleen .doc of .xls formaat.
OWMS (Metadata overheidsinformatie)	Ja	De beleidskeuzes (contentmodellen) zijn in te zien in het Informatie Publicatie Model (IPM) bij het OWMS (zie: http://standaarden.overheid.nl/rijksoverheid).
PDF 1.7 / PDF A/1 en PDF A/2 (Documentpublicatie/ archivering)	Deels	De centrale redactie van Rijksoverheid.nl stuurt op het aanbieden van de juiste typen PDF's. De centrale redactie heeft beperkt zicht op soort en type PDF's die door decentrale redacteuren van de ministeries zelfstandig op rijksoverheid.nl worden geplaatst. Er zijn veel verschillende organisaties die PDF's op rijksoverheid.nl kunnen plaatsen. Het is daardoor simpelweg niet helemaal onder controle welke soorten PDF worden toegepast. Sinds eind 2019 gebruikt Rijksoverheid.nl een nieuwe module voor invoer van een deel van de documenten. PDF-documenten uit deze module voldoen aan alle richtlijnen. Naar aanleiding van de verplichte toegankelijkheid van overheidswebsites gaat in 2020 de centrale redactie in gesprek met de ministeries over het voldoen aan de toegankelijkheidseisen bij alle documenten die externe redacties op Rijksoverheid.nl plaatsen of laten plaatsen.
		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 2019 is voor het maildomein DMARC geïmplementeerd. De status gaat van nee naar ja. Voor het maildomein geldt dat rijksoverheid.nl niet voldoet aan IPv6, de planning van 2019 is niet gehaald en doorgeschoven naar eind 2020. De status gaat naar gepland. Het webdomein voldoet net als vorig jaar aan IPv4 en IPv6. Nieuw op de lijst en relevant voor het webdomein is RPKI. De voorziening voldoet niet aan deze standaard.

Concluderend moeten voor de voorziening rijksoverheid.nl nog de volgende standaarden (volledig) worden geïmplementeerd voor het maildomein: IPv4 en IPV6.

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

3.8 WOZ Waardeloket

Beheerorganisatie: Kadaster

Werking en inhoud van WOZ Waardeloket
Het WOZ Waardeloket biedt de mogelijkheid de WOZ-waarde van woningen te raadplegen. Het WOZ Waardeloket is bedoeld voor het individueel raadplegen van afzonderlijke woningen. De getoonde WOZ-waarden zijn formeel door de desbetreffende gemeente vastgestelde WOZ-waarden. De gemeente is dan ook verantwoordelijk voor deze WOZ-waarde. De getoonde objectkenmerken, zoals bouwjaar en gebruiksoppervlakte, zijn afkomstig uit de Basisregistraties adressen en gebouwen. Ook voor deze gegevens is de gemeente verantwoordelijk.

Standaard	Status	Toelichting
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	Centraal geregeld: Het Kadaster voldoet aan DKIM. Er is geen mailserver voor het domein wozwaardeloket.nl en DKIM records worden op dit domein niet ondersteund (zie: https://internet.nl/mail/wozwaardeloket.nl).
DMARC (Anti-phishing)	Nee	Centraal geregeld: Deze standaard is geïmplementeerd. Er is geen mail server voor het domein wozwaardeloket.nl en er is geen DMARC policy quarantine of reject actief (zie: https://internet.nl/mail/wozwaardeloket.nl).
DNSSEC (Beveiligde domeinnamen)	Ja	DNSSEC wordt ondersteund (zie: https://internet.nl/site/www.wozwaardeloket.nl).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Ja	HTTPS en HSTS zijn geïmplementeerd (zie: https://internet.nl/site/www.wozwaardeloket.nl).
IPv4 en IPv6 (Internetnummers)	Ja	Exact dezelfde website is zowel over IPv4 als IPv6 bereikbaar (zie: https://internet.nl/site/www.wozwaardeloket.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/wozwaardeloket.nl).
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Nee	STARTTLS is beschikbaar. Er is geen mailserver voor het domein wozwaardeloket.nl en DANE is daarom niet actief. Er is geen Null MX record (RFC 7505) ingesteld voor dit domein (zie: https://internet.nl/mail/wozwaardeloket.nl).
TLS (Beveiligde, versleutelde verbindingen)	Ja	Minimaal TLS 1.2 (zie: https://internet.nl/site/www.wozwaardeloket.nl).
		Document en (web/app)content

PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/ archivering)	Nee	Het WOZ-waardeloket biedt de mogelijkheid een schermafdruk van de gegevens in PDF-formaat te downloaden. Dit is momenteel geen PDF 1.7, PDF A/1 of PDF A/2.

Het WOZ Waardeloket is een dit jaar nieuw onderzochte voorziening. Digikoppeling is niet van toepassing, doordat de WOZ voorziening en het WOZ Waardeloket beide in uitvoering zijn bij het Kadaster. WOZ is een portal op voorzieningen waar Geo-standaarden worden toegepast (bijv. PDOK).

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

4. Gegevens en registreren

4.1 NHR (Handelsregister)

Beheerorganisatie: Kamer van Koophandel

Werking en inhoud NHR
Het Handelsregister is de basisregistratie waarin alle rechtspersonen en ondernemingen in Nederland zijn opgenomen. Aansluiten op de Basisregistratie Handelsregister gaat om het tot stand brengen van een elektronische verbinding tussen het Handelsregister en de afnemer. Actuele gegevens uit het Handelsregister kunnen worden overgebracht via de informatieproducten van het Handelsregister. Bij de toetsing van NHR is dit jaar naar de website kvk.nl en de onderliggende systemen en koppelingen gekeken.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	Het domein kvk.nl voldoet aan DKIM (zie: https://internet.nl/mail/kvk.nl/).
DMARC (Anti-phishing)	Ja	NHR voldoet op mailservers aan DMARC (zie: https://internet.nl/mail/kvk.nl/).
DNSSEC (Beveiligde domeinnamen)	Gepland	Kvk,nl is DNSSEC beveiligd. De Microsoft Exchange 365 cloud omgeving niet. Volgens planning van Microsoft wordt DNSSEC eind 2021 ondersteund.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening gebruikt zowel HTTPS als HSTS. Alleen voor kvk.nl werkt HSTS niet, dit is in 2019 hersteld. Was nog niet gebeurd omdat kvk.nl alleen redirect naar www.kvk.nl en deze werkt wel onder HSTS. Er was en is dus geen security risico.
IPv4 en IPv6 (Internetnummers)	Nee	Netwerkprovider KPN ondersteunt geen IPv6. KvK kan in principe IPv6 verkeer aan. Intern wordt IPv4 gebruikt.
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 STARTTLS toe, DANE nog niet (zie: https://internet.nl/mail/kvk.nl/). Volgens planning van Microsoft wordt STARTTLS/DANE eind 2021 ondersteund.
TLS (Beveiligde, versleutelde verbindingen)	Ja	De mailserver kvk-nl.mail.protection.outlook.com ondersteunt nog TLS 1.1. Dit is een externe mailserver. De leverancier (Microsoft) dient de TLS versies uit te faseren. De KVK zal dit opnemen met de leverancier. Op deze mailserver wordt ook TLS 1.2 ondersteunt. KVK is actief bezig om alle TLS implementaties op versie 1.3 te krijgen, daarbij is ook de Wet Digitale Overheid een belangrijke aanleiding. Dat verloopt voorspoedig. Een uitzondering geldt voor een stuk legacy-programmatuur (AS/400 software) waar TLS 1.0 nog wordt gebruikt. Hiervoor zal een exceptie met risicoanalyse worden opgesteld ter nadere bespreking. In afwachting van de uitfasering van deze legacy willen wij zo min mogelijk aanpassingen daarin doen. Het uitfaseren van deze legacy heeft nogal wat vertraging bij ons opgelopen en niet zeker is of dit in 2020 kan worden afgerond.
		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)	Gepland	De bij de KvK in gebruik zijnde contentmanagement systemen, Sharepoint en Documentum zijn compliant aan de CMIS standaard, maar het webcontent platform Tridion (nog) niet vanwege een verouderde versie van de software. De KVK is bezig om Tridion uit te faseren door een nieuw CMS systeem aan te besteden. CMIS is hierin een knock out criterium. Aanbesteding en implementatie vindt in 2020/21 plaats. Koppelingen met Sharepoint worden CMIS compliant uitgevoerd.
Open API Specification (Beschrijven van REST API's)	Deels	KvK gebruikt deze specificatie actief. Reeds operationele API's worden geleidelijk aangepast.
PDF 1.7, PDF A/1, PDF A/2 (Documentpublicatie/ archivering)	Ja	Alle uittreksels en informatie uit het NHR wordt in PDF/A-vorm verstrekt. Het betreft al grotendeels PDF A/2.
SKOS (Thesauri en begrippen-woordenboeken)	Gepland	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. Eerste evaluatie van SKOS voor NHR heeft plaatsgevonden. De KVK wil dit in 2020/2021 verwezenlijken.
		Stelselstandaarden
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Ja	Ongeveer 10% van het verkeer van het NHR gaat naar medeoverheden. Die uitwisselingen vinden allemaal plaats via Digikoppeling en StUF.
StUF (Uitwisseling administratieve overheids-gegevens)	Ja	Ongeveer 10% van het verkeer van het NHR gaat naar medeoverheden. Die uitwisselingen vinden allemaal plaats via Digikoppeling en StUF.
		E-facturatie en administratie
NLCIUS (Elektronisch factureren)	Nee	KvK heeft haar financiële systeem in 2018 naar AFAS gemigreerd. UBL 2.1 en SMeF 2.0 worden wel ondersteund, maar de modelfactuur nog niet.

Ten opzichte van 2019 zijn de volgende standaarden van ‘nee’ en/of ‘deels’ naar ‘gepland’ gegaan: DNSSEC, STARTTLS/DANE, CMIS en SKOS. Daarnaast voldoet de voorziening niet langer meer aan de standaard IPv4 en IPv6. Voor de Open API Specification en NLCIUS zijn er geen veranderingen opgetreden.

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

4.2 PDOK

Beheer organisatie: Kadaster

Werking en inhoud van PDOK
Bij PDOK vind je open datasets van de overheid met actuele geo-informatie. Deze datasets zijn benaderbaar via geo webservices, RESTful API's en beschikbaar als downloads en linked data. PDOK is tot stand gekomen door een samenwerking tussen het Kadaster, de ministeries van Infrastructuur en Waterstaat, Binnenlandse Zaken en Koninkrijksrelaties en Economische Zaken en Klimaat, Rijkswaterstaat en Geonovum. PDOK is een open initiatief. Elke overheidsorganisatie die zijn geodata voor hergebruik beschikbaar wil stellen, kan zich tot PDOK wenden. Het dataportaal PDOK wordt gehost door het Kadaster.

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.pdok.nl ondersteunt DNSSEC (zie: https://internet.nl/domain/www.pdok.nl/).

HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Gepland	Er is een probleem met HSTS-policy via pdok.nl (zie: https://internet.nl/site/pdok.nl). Melding gemaakt om opgelost te worden. Verwachting is dat dit in juli 2020 opgelost wordt.
IPv4 en IPv6 (Internetnummers)	Ja	Zowel IPv4 als IPv6 worden ondersteund door het Kadaster (zie: https://internet.nl/domain/www.pdok.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 en is deels door standaarden op basis van de BIO vervangen. In het jaarverslag is een in control statement opgenomen.
SPF (Preventie van mailspoofing/phishing)	Ja	SPF is geïmplementeerd (zie: https://internet.nl/mail/pdok.nl/).
STARTTLS en DANE (Beveiligd, versleuteld mailverkeer)	Ja	STARTTLS en DANE zijn geïmplementeerd (zie: https://internet.nl/mail/pdok.nl/).
TLS (Beveiligde, versleutelde verbindingen)	Ja	Deze standaard wordt volledig door het Kadaster ondersteund (zie: https://internet.nl/domain/www.pdok.nl/). PDOK volgt de richtlijnen van het NCSC voor TLS. Hieruit blijkt dat mogelijke problemen met cipher-volgorde wat betreft vertrouwelijkheid geen risico vormen, omdat de data openbaar is volgens de BIV classificatie.
Document en (web/app)content		
Open API Specification (Beschrijven van REST API's)	Ja	Deze standaard is geïmplementeerd en wordt toegepast.
OWMS (Metadata overheidsinformatie)	Ja	PDOK ontsluit metadata via het NGR (www.nationaalgeoregister.nl), deze gaat in ieder geval uit van ISO en INSPIRE (en NL profielen). Data.overheid.nl harvest het NGR. v.w.b. OWMS: https://data.overheid.nl/nationaal-georegister.
Stelselstandaarden		
Geo-standaarden	Ja	PDOK maakt gebruik van OGC en INSPIRE standaarden voor haar webservices. Webservices kennen verschillende formaten qua uitlevering. Downloads worden via formaten GeoPackages en GML aangeleverd en uitgeserveerd.
StUF	Ja	Voor het uitserveren van de BGT.

PDOK.nl is een nieuw onderzochte voorziening die vanaf 2020 voor het eerst wordt getest in de Monitor. Geconcludeerd kan worden dat de voorziening nog niet (volledig) voldoet aan HTTPS/HSTS.

5. Dienstverlening en verbinden

5.1 TenderNed

Beheerorganisatie: PIANOo/DICTU

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

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

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	E-mails verzonden vanuit TenderNed zijn beveiligd met DKIM (zie: https://internet.nl/mail/tenderned.nl/).
DMARC (Anti-phishing)	Ja	Dienstverlener DICTU heeft DMARC aangezet.
DNSSEC (Beveiligde domeinnamen)	Ja	Het domein is gesigned met DNSSEC (zie: https://internet.nl/site/www.tenderned.nl/).
HTTPS en HSTS (Beveiligd, versleuteld webverkeer)	Nee	De client-server communicatie van TenderNed is beveiligd met HTTPS en niet met HSTS (zie: https://internet.nl/site/www.tenderned.nl/).
IPv4 en IPV6 (Internetnummers)	Nee	TenderNed.nl is zowel in 2018 en 2019 als in 2020 niet voorbereid op IPv6 (zie: https://internet.nl/site/www.tenderned.nl/). TenderNed is afhankelijk van de hostingpartij. Wanneer deze een transitie doormaakt naar IPv6 zal TenderNed daarin mee gaan. Er is geen planning om dat wel te doen op dit moment.
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.
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)	Ja	STARTTLS en DANE worden ondersteund.

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

Ten opzichte van 2019 is DMARC geïmplementeerd. De status gaat van nee naar ja.

Concluderend moeten voor TenderNed nog de volgende standaarden (volledig) worden geïmplementeerd: HTTPS/ HSTS, IPv4 en IPv6, Open API Specification.

5.2 DigiInkoop

Beheerorganisatie: Logius

Werking en inhoud van DigiInkoop
DigiInkoop is een rijksbreed geautomatiseerd inkoopsysteem dat het inkoopproces vereenvoudigt. DigiInkoop is er voor de inkoop van alle producten en diensten, van kantoorartikelen tot inhuur van personeel. Daarnaast biedt de voorziening DigiInkoop een leveranciersportaal voor leveranciers van de Rijksoverheid. Hiermee kunnen deze leveranciers offertes, orders en facturatie afhandelen, met één inlog voor de hele Rijksoverheid.

Standaard	Status	Toelichting beheerder
		Internet en beveiliging
DKIM (Preventie van mailspoofing/phishing)	Ja	De standaard DKIM is geïmplementeerd. (zie: https://internet.nl/mail/digiinkoop.nl/). Digiinkoop.nl ontvangt geen mail. Het DNS mx record mta.dc.ordina.nl is ook niet meer van toepassing. Dus alle verwijzingen hiernaar (die internet.nl gebruikt) kunnen buiten beschouwing worden gelaten. De DNS record zal verwijderd worden. Vanuit noreply@digiinkoop.nl wordt wel mail verstuurd. SPF/DKIM/DMARC zijn dus wel van toepassing.
DMARC (Anti-phishing)	Nee	De standaard is geïmplementeerd, maar de policy is onvoldoende strikt. Onderzoek loopt naar striktere policy implementatie, de verwachting is Q3 2020 hieraan te kunnen voldoen (zie: https://internet.nl/mail/digiinkoop.nl/).
DNSSEC	Ja	DigiInkoop voldoet aan DNSSEC (zie: https://internet.nl/mail/digiinkoop.nl/). DigiInkoop.nl ontvangt

(Beveiligde domeinnamen)		geen mail. Het DNS mx record mta.dc.ordina.nl is ook niet meer van toepassing. Dus alle verwijzingen hiernaar (die internet.nl gebruikt) kunnen buiten beschouwing worden gelaten. De DNS record zal verwijderd worden.
HTTPS/HSTS (Beveiligd, versleuteld webverkeer)	Ja	De voorziening voldoet aan HTTPS/HSTS. Opvallend is dat internet.nl dat niet goed vast kan stellen (zie https://internet.nl/site/digiinkoop.nl/). Hier wordt nog verder onderzoek naar gedaan.
IPv4 en IPV6 (Internet-nummers)	Gepland	Er loopt een migratie naar een cloudplatform. Verwachting is dat hier IPv6 beschikbaar komt Q4 2020 (zie: https://internet.nl/site/digiinkoop.nl/).
NEN-ISO/IEC 27001/27002 (Managementsysteem informatiebeveiliging) (Richtlijnen en principes informatiebeveiliging)	Ja	DigiInkoop voldoet aan de BIR. Er is een in control statement afgegeven. Leveranciers voldoen aan ISO 27001.
SPF (Preventie van mailspoofing/phishing)	Ja	DigiInkoop voldoet aan deze standaard (zie: https://internet.nl/mail/digiinkoop.nl/).
TLS (Beveiligde, versleutelde verbindingen)	Ja	DigiInkoop is TLS 1.2 compliant (zie: https://internet.nl/mail/digiinkoop.nl/). mta.dc.ordina.nl is uitgefaseerd.
		Document en (web/app)content
PDF/A en PDF 1.7 (Documentpublicatie/archivering)	Ja	De DigiInkoop applicatie produceert inkooporders en facturen in PDF-formaat. Documenten die op logius.nl beschikbaar worden gesteld zijn in PDF/A-formaat (dit zijn de documenten over de berichtenverkeerstandaarden waar DigiInkoop gebruik van maakt: https://www.logius.nl/ondersteuning/gegevensuitwisseling/ubl-ohnl en https://www.logius.nl/ondersteuning/gegevensuitwisseling/setu-hr-xml-ohnl).
		E-facturatie en administratie
NLCIUS (Elektronisch factureren)	Ja	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 is conform planning in Q2 2019 gerealiseerd.
SETU (Informatie flexibele arbeidskrachten)	Ja	DigiInkoop ondersteunt de uitwisseling van SETU-hr-XML berichten.

Ten opzichte van 2019 voldoet de voorziening niet meer aan DMARC. Verder is de status van de IPv4 en IPv6 standaarden van nee naar gepland gegaan. De voorziening voldoet aan NLCIUS.

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

Bijlage A Geïnterviewde personen

Naam voorziening	Contactpersoon
Berichtenbox voor bedrijven	Erwin Sakkers
DigiInkoop	Güldeniz Özdemir Isik
DigiD	Güldeniz Özdemir Isik
DigiD Machtigen	Güldeniz Özdemir Isik
Stelsel elektronische toegangsdiensten	Güldeniz Özdemir Isik
MijnOverheid	Güldeniz Özdemir Isik
NHR	Rob Spoelstra
Ondernemersplein	Elie Mokheiber, Rienco Ligtenbarg, Gaico Aertssen
Overheid.nl	Erna Wisselaar
PDOK	Jeroen Hogeboom
PKI Overheid	Güldeniz Özdemir Isik
Rijksoverheid.nl	Gerrit Berkouwer, Cees Vaes
RDW.nl	Gert Stel,
Samenwerkende Catalogi	Güldeniz Özdemir Isik
Tenderned	Rudi van Eijk
WOZ Waardeloket	Rijk van Haaften

Bijlage B Lijst onderzochte verplichte open standaarden

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