Rapportage voorzieningenonderzoek

Monitor Open Standaarden 2024

PBLQ

Eindversie

14-10-2024

PBLQ
verbinders in de informatiesamenleving

Inhoudsopgave

1. Inleiding

1.1 Aanleiding

De Monitor Open Standaarden is een onderzoek naar de uitvoering en naleving van het pas-toe-of-leg-uit-beleid door overheidsorganisaties. De Monitor wordt gecoördineerd en uitgevoerd door ICTU in opdracht van het Bureau Forum Standaardisatie. ICTU heeft PBLQ gevraagd om als onderdeel van de Monitor het voorzieningenonderzoek uit te voeren. In het voorzieningenonderzoek wordt gekeken in hoeverre overheidsvoorzieningen voldoen aan de open standaarden van de pas-toe-of-leg-uit-lijst. De resultaten van het voorzieningenonderzoek 2024 worden in deze rapportage beschreven.

1.2 Doelstelling en scope

Doel van het voorzieningenonderzoek is het creëren van een beeld van de toepassing en naleving van open standaarden bij overheidsvoorzieningen.

De overheidsvoorzieningen die worden onderzocht komen grotendeels overeen met de voorzieningen van de Gemeenschappelijke Digitale Infrastructuur (GDI). Daarnaast zijn er enkele voorzieningen door de jaren heen op verzoek van het Ministerie van BZK – in de rol van stelselverantwoordelijke voor de digitale overheid – aan de scope toegevoegd.

Het voorzieningenonderzoek is voor het laatst uitgevoerd in 2021 en 2022. De positieve resultaten uit deze onderzoeken gaven voor de opdrachtgever aanleiding om het onderzoek in 2023 niet opnieuw te laten uitvoeren. In 2021 en 2022 is telkens een deel van de lijst met overheidsvoorzieningen onderzocht. Er werd destijds een onderscheid gemaakt tussen

(1) een set voorzieningen die direct raakt aan de communicatie en gegevensuitwisseling met burgers en bedrijven. Deze is in 2022 onderzocht.
(2) een set voorzieningen die gericht is op de communicatie en gegevensuitwisseling tussen overheden en op de onderliggende infrastructuur. Deze is in 2021 onderzocht.

Voor het onderzoek in 2024, waar deze rapportage de resultaten van beschrijft, is dit onderscheid losgelaten. Dat betekent dat in het huidige onderzoek alle overheidsvoorzieningen zijn meegenomen. De volledige lijst met onderzochte overheidsvoorzieningen is terug te vinden in bijlage A.

Om functionele en/of technische overlap tussen voorzieningen binnen het onderzoek te voorkomen zijn enkele voorzieningen dit jaar samengevoegd. Het gaat dan om voorzieningen die in 2021 of in 2022 onderzocht zijn, met een bijna overlappende scope. Dit is het geval voor:

- Het KvK Handelsregister is samengevoegd met het Nieuw HandelsRegister (NHR)
- RDW.nl is samengevoegd met de Basisregistratie Voertuigen (BRV)

Verder maakt DigiInkoop niet langer deel uit van de scope van het onderzoek, omdat deze voorziening in 2023 uit de lucht is gehaald. Dit brengt het totaal aantal voorzieningen dat dit jaar is onderzocht op 27.

1.3 Werkwijze

Er is een gestructureerde werkwijze gevolgd die bestond uit drie fasen:

1. **Voorbereidingsfase**

- Per voorziening is bepaald welk gedeelte van de voorziening wordt getoetst. Dit kan bijvoorbeeld gaan om een webdomein of een maildomein.

- Per voorziening is bepaald welke standaarden van de pas-toe-of-leg-uit-lijst van Forum Standaardisatie van toepassing zijn. Het vertrekpunt daarbij waren de rapportages van 2021 en 2022.
- Daarna is de publiek beschikbare compliance-test van internet.nl gebruikt om na te gaan of de voorziening aan de relevante standaarden voldoet. De manier waarop internet.nl in dit onderzoek is gebruikt om standaarden te toetsen, staat verder toegelicht onder paragraaf 1.4.4.
- Op basis van de bevindingen uit de compliance-testen en de professionele inschatting van de onderzoekers is per voorziening een tabel voorbereid. De tabel beschrijft de van toepassing zijnde open standaarden, de status die aangeeft of de voorziening aan deze standaarden voldoet en bevat een kolom waarin de beheerder van de voorziening een toelichting op de compliance-status kan geven.

2. Onderzoeksfase

- De tabellen zijn toegestuurd aan de beheerders of contactpersonen per voorziening. Aan hen is gevraagd om zowel de beschrijving van de scope (het gedeelte dat getoetst wordt) van de voorziening als de inschattingen ten aanzien van het gebruik van de juiste standaarden langs te lopen, te valideren en waar nodig aan te vullen als het gaat om standaarden die de onderzoekers zelf niet kunnen testen. Dat heeft er in de praktijk toe geleid dat een aantal domeinen aan het onderzoek is toegevoegd.
- De beheerders zijn gevraagd om een verklaring of toelichting op te nemen als de voorziening gedeeltelijk of niet aan een specifieke standaard voldoet. Dit is in lijn met het pas-toe-of-leg-uit-beleid van de overheid: als een voorziening niet aan een standaard van de verplichte lijst met open standaarden voldoet, moet zij kunnen uitleggen waarom dat niet het geval is.
  In aanvulling op deze toelichtingen hebben sommige beheerders ervoor gekozen om ook een toelichting op te nemen bij standaarden waar de voorziening reeds aan voldoet. Dit verklaart waarom sommige tabellen in deze rapportage uitgebreider zijn beschreven dan anderen.
- De reacties van de beheerders zijn gebruikt om de informatie uit de tabellen aan te vullen. Waar van toepassing is de compliance-status op basis van de nieuwe informatie door de onderzoekers aangepast.
- Daar waar verschillen van mening bestonden over het wel of niet voldoen aan de standaarden, zijn deze verschillen tussen de onderzoekers en de beheerders besproken. In de gevallen waar de verschillen ook na de gesprekken bleven bestaan, is dit duidelijk opgenomen in de rapportage.
- De volledige tabel is ten slotte aan de beheerder ter validatie voorgelegd.

3. Rapportagefase

- De geaccordeerde tabellen zijn in de rapportage opgenomen. Onderaan iedere tabel staat beschreven aan welke standaarden de voorziening nog niet voldoet en welke verschillen er in compliance bestaan tussen 2021 of 2022 en 2024.
- Er is eerst een conceptrapportage opgeleverd. Deze is met de opdrachtgever en kwaliteitsbewaker gedeeld. Op basis van hun feedback is vervolgens een eindrapportage opgesteld.

1.4 Aandachtspunten voor de lezer

1.4.1 Voorzieningen en standaarden geordend op basis van functionaliteit

De voorzieningen in deze rapportage zijn op basis van functionaliteit gegroepeerd, vergelijkbaar met hoe dit bij de Monitor Digitale Overheid gebeurt. De volgende functionele groepen worden onderscheiden:

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

De standaarden in de tabellen zijn gecategoriseerd op basis van domeinen waarin ze worden gebruikt. Hiervoor is gebruik gemaakt van de domeinen die het Forum Standaardisatie voor de standaarden van de pas-toe-of-leg-uit-lijst onderscheidt. Dit zijn:

- Bestuur en recht
- Bouwen en wonen
- Economie en werk
- Onderwijs en cultuur
- Openbaar en toegankelijk
- Schoon water en beschermde bodem
- Uitwisselingsfundament
- Veilig internet

1.4.2 Compliance-status

De onderzoekers hebben voor iedere voorziening bepaald in hoeverre de voorziening aan de van toepassing zijnde open standaarden voldoet. De tabellen beschrijven hiervoor de compliance-status. De status kan de volgende waarden hebben:

- **Ja** De voorziening is conform de standaard. Hiermee wordt bedoeld dat de standaard door de eindgebruiker te gebruiken is.
- **Nee** De voorziening is niet conform de standaard.
- **Deels** Onderdelen van de voorziening zijn conform aan de standaard, maar niet alle onderdelen. Hiermee wordt bedoeld dat een onderdeel van de voorziening helemaal aan de standaard voldoet. Dit kan bijvoorbeeld gebeuren als het webdomein wél aan de standaard voldoet, maar het maildomein niet.
- **Gepland** Er zijn concrete plannen om op korte termijn de voorziening conform aan de standaard te maken.
- **Onbekend** Er is onvoldoende informatie voor de onderzoekers om te bepalen of de voorziening aan de standaard voldoet.

Waar het gaat om de Digitoegankelijkheidsstandaard hebben we de status opgenomen zoals die is opgenomen in het register van toegankelijkheidsverklaringen. Meer informatie hierover staat onder paragraaf 1.4.5

1.4.3 Veranderingen op de pas-toe-of-leg-uit-lijst

Voor dit onderzoek is gebruik gemaakt van de pas-toe-of-leg-uit-lijst van 1 april 2024. Een overzicht van alle standaarden die op dat moment op de lijst stonden is opgenomen onder bijlage B.

Ten opzichte van 2022, het laatste jaar waarin dit onderzoek is uitgevoerd, is er één nieuwe standaard op de pas-toe-of-leg-uit-lijst gekomen: security.txt. Deze standaard maakt het mogelijk dat een organisatie security-contactinformatie op haar webserver kan publiceren. Daarnaast is de SAML-standaard veranderd in authenticatie-standaarden. Hieronder vallen zowel SAML als OpenID.NLGov. De standaarden COINS en OWMS, die bij de vorige meetmomenten (in 2021 en/of 2022) nog zijn meegenomen, maken geen deel meer uit van de lijst en zijn daarom in het onderzoek van dit jaar weggelaten.

1.4.4 Wijze van toetsen van een standaard

Het toetsen van de compliance gebeurt op twee manieren:

1. **Gebruik van de website internet.nl**

De website internet.nl is een initiatief van het Platform Internetstandaarden. De website maakt het mogelijk om te toetsen in hoeverre domeinen (zowel web als e-mail) aan bepaalde (beveiligings)standaarden voldoen. Dit gaat om:

- IPv4 en IPv6
- HTTPS & HSTS
- DMARC
- DKIM
- DNSSEC
- SPF
- STARTTLS & DANE
- TLS
- Security.txt
- RPKI

Internet.nl is bruikbaar voor alle voorzieningen die voor internetgebruikers te bereiken en gebruiken zijn. Als een voorziening gesloten is, en niet voor het algemene publiek te gebruiken is, kunnen deze testen niet worden uitgevoerd. Als een web- of maildomein bij een voorziening vooraf via internet.nl is getoetst wordt bij de introductie van de voorziening aangegeven welke domeinen zijn getoetst. Bij de voorzieningen waar deze toelichting ontbreekt, betekent dit dat de onderzoekers vooraf geen mogelijkheid hadden om de voorziening via internet.nl te testen.

Internet.nl toetst meer dan alleen het gebruik van de bovenstaande standaarden. Er wordt bijvoorbeeld ook gekeken naar hoe de standaarden geconfigureerd zijn, en welke optionele extra beveiligingsmaatregelen getroffen zijn. Daar waar dat leidt tot aandachtspunten, hebben we dit ook bij de beheerders aangegeven. Dat is echter niet altijd een reden om een standaard in de tabel af te keuren. Daarvoor hanteren we strikt de eisen die het Forum Standaardisatie hanteert in haar PTOLU-lijst. Daarmee kan het voorkomen dat bepaalde standaarden een status ‘ja’ ontvangen en tegelijkertijd nog aandachtspunten hebben in de toelichting.

2. **Bevragen van de beheerders**

In het onderzoek is de uitslag van de internet.nl-toets 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. Het gebruik van internet.nl is echter niet volledig dekkend voor alle standaarden die worden onderzocht. Voor de overige standaarden worden beheerders gevraagd naar de nalevingsstatus en een toelichting daarbij. De onderzoekers valideren de antwoorden van de beheerders. Waar nodig worden vervolgvragen gesteld. Zodoende ontstaat een volledig beeld van de mate waarin een voorziening aan de van toepassing zijnde standaarden voldoet.

1.4.5 Bijzondere standaarden van de pas-toe-of-leg-uit-lijst

Digitoegankelijk

Digitoegankelijk is de Nederlandse naam voor de Europese Norm EN 301 549. Die stelt dat overheidsorganisaties zich aan de WCAG-regels moeten houden voor websites en mobiele applicaties. De toegankelijkheidsregels zorgen dat zoveel mogelijk mensen zorgeloos gebruik kunnen maken van hun werk, ook als zij een permanente of tijdelijke beperking hebben.

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. 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.

Voor dit onderzoek is per voorziening gekeken of er een toegankelijkheidsverklaring in het openbare register is gepubliceerd. De toegankelijkheidsverklaring kent een van de volgende statussen:

- Status A: Voldoet volledig
- Status B: Voldoet gedeeltelijk
- Status C: Eerste maatregelen genomen
- Status D: Voldoet niet
- Status E: Geen toegankelijkheidsverklaring gepubliceerd

ISO 27001/2 en de BIO
De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen (Rijk, gemeenten, provincies en waterschappen). De BIO is gebaseerd op de NEN-ISO/IEC 27001:2017 en de NEN-ISO/IEC 27002:2017, die beiden op de pas-toe-of-leg-uit-lijst staan. Indien een organisatie voldoet aan de BIO, dan voldoen zij binnen de context van dit rapport ook aan de verplichting om de ISO 27001 en ISO 27002 standaard te gebruiken.

Streefbeeldafspraak en wettelijke verplichting
Open standaarden kunnen een extra verplichting krijgen aan de hand van een streefbeeldafspraak. Daarbij moet de standaard voor een bepaalde datum ingevoerd zijn en is er geen mogelijkheid meer om van die verplichting af te wijken. Streefbeeldafspraken gaan dus verder dan de 'pas toe of leg uit'-verplichting. Bij een streefbeeldafspraak moet de open standaard op alle ICT-systemen/-diensten geïmplementeerd worden, dus ook op bestaande. Er zijn op dit moment streefbeeldafspraken voor de volgende open standaarden: DKIM, DMARC, DNSSEC, IPv6 en IPv4, RPKI, STARTTLS en DANE, SPF en TLS.

Er geldt bovendien een wettelijke verplichting voor een tweetal standaarden: Digitale toegankelijkheid en HTTPS en HSTS.

1.4.6 Vergelijking met voorgaande jaren

In de rapportage is onder elke tabel een samenvatting opgenomen van de compliance van de voorziening aan de van toepassing zijnde open standaarden en hoe dit verschilt ten opzichte van de meting in voorgaande jaren. In de samenvatting komen de volgende zaken aan bod:

- Nieuw geteste standaarden voor deze voorziening – dit kan gaan om nieuwe standaarden op de pas-toe-of-leg-uit-lijst of om reeds bestaande standaarden die nu binnen de scope van de voorziening worden meegenomen waar dat eerder nog niet het geval was.
- Niet langer van toepassing zijnde standaarden voor deze voorziening – dit kan gaan om standaarden die niet langer op de pas-toe-of-leg-uit-lijst staan of om standaarden waarvan in samenspraak met de beheerder is bepaald dat deze niet (meer) relevant zijn voor de voorziening zijn.
- Verbeteringen – hier worden standaarden genoemd waar de voorziening ten opzichte van de vorige meting wel (deels) aan voldoet. Dit zijn dus verbeteringen in compliance.
- Verslechteringen – hier worden standaarden genoemd waar de voorziening ten opzichte van de vorige meting (deels) niet meer aan voldoet. Dit zijn dus verslechteringen in compliance.

Aan het einde van iedere samenvatting wordt voor de voorziening opgesomd (*concluderend …)* welke standaarden nog volledig geïmplementeerd moeten worden om een 100% compliance-score te halen.

2. Identificeren en authentiseren

2.1 BSN en BRP-V

Beheerorganisatie: RvIG

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

Standaard	Status	Toelichting beheerder
		Veilig internet
DNSSEC	Ja	De Beheervoorziening BSN en de BRP-V zijn DNSSEC-compliant.
HTTPS en HSTS	Ja	De Beheervoorziening BSN en BRP-V voldoet aan de HTTPS- en HSTS-standaarden.
IPv4 en IPv6	Nee	IPv6 gebruiken wordt niet gebruikt, maar het is wel mogelijk om dit toe te passen. Momenteel wordt gebruik gemaakt van IPv4.
NEN-ISO/IEC27001 en NEN-ISO/IEC27002	Ja	
NL GOV Assurance profile for OAuth 2.0	Deels	Deze standaard wordt gehanteerd in het BRP API traject onder het experimenteerbesluit. Deze standaard is niet van toepassing bij BV-BSN.
RPKI	Ja	De Beheervoorziening BSN en BRP-V zijn RPKI-compliant.
security.txt	Nee	Security.txt is nog niet toegepast, maar dit staat wel op de planning van de beheerder.
TLS	Ja	Intern wordt dit nog niet gebruikt. Dat is wel de ontwikkelrichting. (zero trust). Naar buiten toe wordt dit wel toegepast en op aanvraag van een afnemer kan dit ook tweezijdig worden toegepast.
		Uitwisselingsfundament
Digikoppeling	Deels	De BRP voldoet niet aan de Digikoppeling standaard. De BVBSN voldoet wel aan de Digikoppeling standaard.
OpenAPI Specification	Ja	De Beheervoorziening BSN en BRP-V voldoen aan de OpenAPI Specification
REST-API Design Rules	Deels	De BRP voldoet niet aan de REST-API Design Rules standaard. De BVBSN voldoet wel aan de REST-API Design Rules standaard.

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:
- DNSSEC
- Security.txt
- OpenAPI Specification

Niet langer van toepassing zijnde standaarden voor deze voorziening:
- StUF

Verbeteringen; de voorziening voldoet nu (deels) wel aan:
- RPKI
- NL GOV Assurance profile for OAuth 2.0
- REST-API Design Rules

Verslechteringen; de voorziening voldoet nu (deels) niet meer aan:
- IPv6

Concluderend moeten voor BSN en BRP-V de volgende standaarden (volledig) worden geïmplementeerd: IPv6, NL GOV Assurance profile for OAuth 2.0, security.txt, Digikoppeling en REST-API Design Rules.

2.2 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 registreren van donorschap, het aanvragen of inzien van pensioen- en zorgverzekeringen en diverse gemeentelijke aanvragen en belastingen.

Geteste web- en maildomeinen:
- www.digid.nl
  - Bron: https://internet.nl/site/www.digid.nl/2879137/
  - Bron: https://internet.nl/site/digid.nl/2879107/
- login.digid.nl
  - Bron: https://internet.nl/site/login.digid.nl/2879141/
- mijn.digid.nl
  - Bron: https://internet.nl/site/mijn.digid.nl/2879111/
- @digid.nl
  - Bron: https://internet.nl/mail/digid.nl/1290758/

Standaard	Status	Toelichting beheerder
		Veilig internet
DKIM	Ja	DigiD mail wordt verstuurd met een DKIM signature.
DMARC	Ja	DMARC is voor DigiD geconfigureerd als een van de anti-phishing maatregelen
DNSSEC	Ja	DNSSEC is doorgevoerd in de domeinen (DNS-zone) van DigiD en operationeel. Ook de mailservers voldoen aan de standaard
HTTPS en HSTS	Ja	HTTP-compressie staat alleen aan op het (sub)domein www.digid.nl, dat is de website van DigiD met alleen statistische content. Omdat deze content ook omvangrijke bestanden bevat, zoals instructievideo's, is besloten om HTTP-compressie aan te laten staan. Het risico hiervan op statistische content is beperkt.
IPv4 en IPv6	Ja	Het domein DigiD.nl is via IPv4 en IPv6 toegankelijk. Ook het mailverkeer verloopt via IPv4 en IPv6.
NEN-ISO/IEC27001 en NEN-ISO/IEC27002	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Overheid (BIO) van toepassing die is gebaseerd op NEN-ISO27001/2. Logius verantwoordt zich over deze norm aan het kerndepartement (BZK).
RPKI	Ja	De Logius voorziening DigiD is aangesloten op IP-reeksen die ontsloten worden via leveranciers uit het raamcontract ON2013. Deze IP-reeksen voldoen aan RPKI.
Authenticatie-standaarden	Ja	DigiD biedt aan afnemers een SAML-koppelvlak om authenticaties uit te kunnen voeren. Wanneer de afnemer "single sign on" wil

(OpenID.NLGov en SAML)		gebruiken is dit alleen mogelijk via het SAML-koppelvlak. De SAML koppelvlak-specificaties van DigiD zijn gepubliceerd op de website van Logius (zie: https://logius.nl/diensten/digid/documentatie/koppelvlakspecificatie-digid-saml-authenticatie)
security.txt	Ja	Voor alle (sub)domeinen van DigiD wordt doorverwezen naar de security.txt van het NCSC, zoals afgesproken binnen de Rijksoverheid.
SPF	Ja	SPF is relevant voor DigiD bij het verzenden van mails vanuit DigiD, en DigiD voldoet ook aan deze standaard.
STARTTLS en DANE	Ja	De mailservers van DigiD passen STARTTLS/DANE toe. Vanwege ondersteuning van oudere e-mailservers is een risicoafweging gemaakt om de TLS-versies 1.0 en 1.1 inclusief bepaalde ciphersuites te blijven aanbieden, zolang dit niet direct onveilig is voor de mailservers van DigiD. De bereikbaarheid van DigiD via e-mail en het aankomen van e-mail-notificaties is belangrijker dan de versleuteling van de berichten. Bij het versturen van berichten wordt rekening gehouden met de gevoeligheid van informatie. Bij de migratie naar het nieuwe Logius Platform wordt bekeken of dit op een andere manier ingevuld kan worden.
TLS	Ja	DigiD ondersteunt voor de publieke domeinen alleen TLS v1.3 en TLS v1.2.
		Openbaar en toegankelijk
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status B	DigiD heeft onderzoek gedaan naar de toegankelijkheid van de websites en mobiele apps. De DigiD app heeft status A bereikt maar niet alle websites voldoen aan alle toegankelijkheidseisen uit de norm (status B). Er zijn verbetermaatregelen benoemd en er is een planning hiervoor gemaakt. DigiD is daarom in control over de toegankelijkheid van de websites en mobiele apps. (zie de diverse verklaringen van DigiD op https://www.toegankelijkheidsverklaring.nl/register?w=digid)

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:

- Security.txt
- Authenticatie-standaarden (OpenID.NLGov en SAML)

Concluderend moet voor DigiD de volgende standaard (volledig) geïmplementeerd worden: Digitoegankelijk (EN 301 549 met WCAG 2.1).

2.3 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.

Geteste web- en maildomeinen:

- Machtigen.digid.nl
    - Bron: https://internet.nl/site/machtigen.digid.nl/2879109/#

Toelichting vanuit PBLQ: Ten tijde van het testen van de compliance van DigiD Machtigen voldeed de voorziening aan alle relevante standaarden. De onderstaande tabel is toentertijd opgesteld. Tijdens een laatste verificatietest voldeed DigiD Machtigen niet aan het doorverwijzen van HTTP naar HTTPS. De beheerder gaf aan dat dit te maken heeft met de nasleep van een recente infrastructuur-wijziging van DigiD Machtigen. Er is besloten om de tabel zoals die is opgesteld ten tijde van het testen op te nemen in de rapportage.

Standaard	Status	Toelichting beheerder
		Veilig internet
DMARC	Ja	Er is een DMARC-record geconfigureerd als een van de anti-phishing maatregelen. Verder wordt er geen email verstuurd onder de domeinnaam @machtigen.digid.nl. E-mails worden verstuurd onder het @digid.nl domein. Het DMARC-record en andere email gerelateerde standaarden worden door DigiD voorzien.
DNSSEC	Ja	Het domein machtigen.digid.nl voldoet aan DNSSEC.
HTTPS en HSTS	Ja	DigiD Machtigen maakt gebruik van HTTPS voor de communicatie tussen clients (zoals browsers) en servers. De DigiD Machtigen website heeft ook een HSTS-policy.
IPv6 en IPv4	Ja	De website van DigiD Machtigen is via IPv4 en IPv6 toegankelijk en ondersteund.
NEN-ISO/IEC27001 en NEN-ISO/IEC27002	Ja	Op de Rijksoverheid is de Baseline Informatiebeveiliging Overheid (BIO) van toepassing die is gebaseerd op NEN-ISO27001/2. Logius verantwoord zich over de BIO aan het kerndepartement (BZK).
RPKI	Ja	De Logius voorziening DigiD Machtigen is aangesloten op IP-reeksen die ontsloten worden via leveranciers uit het raamcontract ON2013. Deze IP-reeksen voldoen aan RPKI.
Authenticatie-standaarden (OpenID.NLGov en SAML)	Ja	Het authenticatiekoppelvlak met DigiD (voor burgers) en met eHerkenning (voor dienstverleners) voldoet aan de SAML-standard.
security.txt	Ja	Voor het subdomein machtigen.digid.nl wordt doorverwezen naar de security.txt van het NCSC, zoals afgesproken binnen de Rijksoverheid.
SPF	Ja	DigiD Machtigen verstuurt geen email vanaf het @machtigen.digid.nl domein. Er is wel een SPF-record aangemaakt, die aangeeft dat er vanaf dit domein geen email wordt verstuurd. E-mails worden verstuurd onder het @digid.nl domein. Het bijbehorende SPF-record en andere email gerelateerde standaarden vallen onder de verantwoordelijkheid van DigiD.
TLS	Ja	TLS is geïmplementeerd. DigiD Machtigen ondersteunt TLS v1.2. Hieraan is een beperkte set van cipher-suites toegekend, welke voldoen aan norm ‘voldoende’ en ‘goed’. Door een wijziging in de infrastructuur zal het binnenkort mogelijk worden om ook TLS v1.3 te ondersteunen.
		Uitwisselingsfundament
Digikoppeling	Deels	Recent ontwikkelde koppelvlakken en/of nieuwe versies van bestaande koppelvlakken zijn Digikoppeling compliant (bijvoorbeeld BOP). Er zijn echter nog koppelvlakken waarvan

		geen Digikoppeling compliant versie is gemaakt en/of 'legacy' koppelvlakken waar nog diensten en afnemers op aangesloten zitten. Deze koppelvlakken bestaan uit de tijd dat de Digikoppeling standaard in ontwikkeling was en voldoen deels aan de uiteindelijk ontstane Digikoppeling standaard. Er wordt gewerkt aan de herbouw van de diverse koppelvlakken, waarbij de Digikoppeling standaard wordt meegenomen.
		Openbaar en toegankelijk
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status A	DigiD Machtigen heeft onderzoek gedaan naar de toegankelijkheid van de website. Er wordt voldaan aan alle toegankelijkheidseisen uit de norm (Status A). DigiD Machtigen is daarom in control over de toegankelijkheid van de website en voldoet volledig aan de WCAG. (zie de officiële verklaring van DigiD Machtigen op https://www.toegankelijkheidsverklaring.nl/register/1203).
PDF (NEN-ISO)	Ja	De voorziening voldoet aan deze standaard. Er is de mogelijkheid gebruik te maken van het downloaden en opslaan in een PDF-document.

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:

- Security.txt
- Authenticatie-standaarden (OpenID.NLGov en SAML)

Verbeteringen; de voorziening voldoet nu (deels) wel aan:

- Digitoegankelijk (EN 301 549 met WCAG 2.1)

Concluderend moet voor DigiD Machtigen de volgende standaard (volledig) geïmplementeerd worden: Digikoppeling.

2.4 Afsprakenstelsel elektronische toegangsdiensten

Beheerorganisatie: Logius

Werking en inhoud van ETD:
eHerkenning is een veilig en betrouwbaar inlogmiddel waarmee men bij ruim 500 verschillende dienstverleners, zoals UWV, gemeenten, Belastingdienst en verzekeraars kan inloggen. 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. 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. Meer informatie is te vinden op de website https://eherkenning.nl/nl/wat-is-eherkenning.

Geteste web- en maildomeinen:

- www.eherkenning.nl
  - Bron: https://internet.nl/site/eherkenning.nl/2797617/
  - Bron: https://internet.nl/site/www.eherkenning.nl/2797618/
- @eherkenning.nl:
  - Bron: https://internet.nl/mail/eherkenning.nl/1246652/

Tijdens de looptijd van dit onderzoek is het niet gelukt een reactie te krijgen van de beheerder van ETD. Onderstaande tabel geeft de inschatting van de onderzoekers weer, en is dus niet gevalideerd door de beheerder. De gemaakte inschatting is gebaseerd op de toetsing van de domeinen via internet.nl, en de documentatie van het afsprakenstelsel.

Standaard	Status	Toelichting beheerder
		Veilig internet
DKIM	Ja	
DMARC	Ja	
DNSSEC	Ja	
HTTPS en HSTS	Ja	De webservers bieden een Referrer-Policy aan met een policy-waarde die met terughoudendheid moet worden gebruikt vanwege de mogelijke impact op beveiliging en privacy. Daarnaast bieden de webservers geen Content-Security-Policy (CSP) aan.
IPv4 en IPv6	Ja	
NEN-ISO/IEC27001 en NEN-ISO/IEC27002	Ja	In het afsprakenstelsel (v2 mei 2024) wordt certificering tegen ISO27001 geëist voor de deelnemers.
RPKI	Ja	
Authenticatie-standaarden (OpenID.NLGov en SAML)	Ja	SAML is een verplichte eis vanuit het stelsel.
security.txt	Ja	
SPF	Ja	
STARTTLS en DANE	Ja	De domeinen voldoen. Een aandachtspunt is het ontbreken van een TLSA-record voor DANE.
TLS	Ja	
		Openbaar en toegankelijk
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status B	
PDF (NEN-ISO)	Ja	In 2022 heeft de beheerder hierna volgende toelichting gegeven: *Toelichting 2022* *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.* Voor zover de onderzoekers konden achterhalen is deze toelichting nog steeds relevant en voldoet ETD waar van toepassing aan het gebruik van de standaard.

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:

- Authenticatie-standaarden (OpenID.NLGov en SAML)
- Security.txt

Concluderend moet voor het afsprakenstelsel elektronische toegangsdiensten de volgende standaard (volledig) geïmplementeerd worden: Digitoegankelijk (EN 301 549 met WCAG 2.1).

2.5 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 zeven toegetreden vertrouwensdienstverleners (TSP's) die PKIoverheidscertificaten verstrekken. Dit zijn: KPN, QuoVadis, Digidentity, Cleverbase, CIBG, het Ministerie van Infrastructuur en Waterstaat en het Ministerie van Defensie.

Geteste web- en maildomeinen:
- cert.pkioverheid.nl
  - Bron: https://internet.nl/site/cert.pkioverheid.nl/2797699/
- crl.pkioverheid.nl
  - Bron: https://internet.nl/site/crl.pkioverheid.nl/2797698/
- oid.pkioverheid.nl
  - Bron: https://internet.nl/site/oid.pkioverheid.nl/2823668/
- cps.pkioverheid.nl
  - Bron: https://internet.nl/site/cps.pkioverheid.nl/2823669/
- cp.pkioverheid.nl
  - Bron: https://internet.nl/site/cp.pkioverheid.nl/2823670/
- por.pkioverheid.nl
  - Bron: https://internet.nl/site/por.pkioverheid.nl/2823672/

Standaard	Status	Toelichting beheerder
		Veilig internet
DMARC	Ja	De beheerder geeft aan dat voor alle bovengenoemde domeinen DMARC van toepassing is.
DNSSEC	Ja	PKIoverheid maakt gebruik van DNSSEC.
HTTPS en HSTS	Deels	Een correctie voor het niet automatisch doorverwijzen van bezoekers van HTTP naar HTTPS is aangevraagd bij de leverancier. Daarnaast is het aanbieden van een CSP is aangevraagd bij de leverancier.
IPv4 en IPv6	Deels	Alle domeinen met uitzondering van crl.pkiverheid.nl zijn met een IPv6-adres toegankelijk. Vanwege beperkingen in de log stack is er momenteel nog geen mogelijkheid om IPv6 te implementeren op crl.pkioverheid.nl. Vanuit audit eisen geldt dat alle requests richting CRL moeten worden gelogd en dit is momenteel technisch niet mogelijk met de huidige inrichting om deze events aan elkaar te kunnen relateren (IPv4 en IPv6).
NEN-ISO/IEC27001 en NEN-ISO/IEC27002	Ja	PKIoverheid moet voldoen aan de zogenaamde Webtrust standaarden (zie www.webtrust.org voor meer informatie) die grotendeels overlappen met de BIO.
RPKI	Ja	RPKI is ingesteld.
security.txt	Ja	PKIoverheid maakt gebruik van security.txt.
TLS	Ja	TLS is van toepassing.
		Openbaar en toegankelijk
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status A	
PDF (NEN-ISO)	Ja	PDF/A wordt toegepast.

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:

- Security.txt

Niet langer van toepassing zijnde standaarden voor deze voorziening:

- SPF

Verbeteringen; de voorziening voldoet nu (deels) wel aan:

- Digitoegankelijk (EN 301 549 met WCAG 2.1)

Verslechteringen; de voorziening voldoet nu (deels) niet meer aan:

- HTTPS en HSTS

Concluderend moeten voor PKIoverheid de volgende standaarden volledig geïmplementeerd worden: HTTPS en HSTS en IPv6.

3. Dienstverlening en informatieverstrekken

3.1 Berichtenbox voor bedrijven

Beheerorganisatie: Rijksdienst voor Ondernemend Nederland (RvO)

Werking en inhoud van 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.

Geteste web- en maildomeinen:
- berichtenbox.antwoordvoorbedrijven.nl
    - Bron: https://internet.nl/site/berichtenbox.antwoordvoorbedrijven.nl/2797874/#
- @berichtenbox.antwoordvoorbedrijven.nl
    - Bron: https://internet.nl/mail/berichtenbox.antwoordvoorbedrijven.nl/1246868/
    - Bron: https://internet.nl/mail/antwoordvoorbedrijven.nl/1246869/

Standaard	Status	Toelichting beheerder
		Veilig internet
DKIM	Ja	Gevalideerd
DMARC	Ja	Gevalideerd
DNSSEC	Ja	Gevalideerd
HTTPS en HSTS	Ja	Gevalideerd
IPv4 en IPv6	Ja	Gevalideerd
RPKI	Ja	Gevalideerd
Authenticatie-standaarden (OpenID.NLGov en SAML)	Ja	De Berichtenbox maakt gebruik van TVS van DICTU. Hierin wordt gebruik gemaakt van SAML. De Berichtenbox voldoet aan alle eisen die TVS hieraan stelt.
security.txt	Nee	De beheerder geeft dan dat deze standaard nog niet toegepast is, maar dit zal in een volgende update worden toegevoegd.
SPF	Ja	Gevalideerd
STARTTLS en DANE	Ja	TLSA is een vereiste voor de mailservers, maar de voorziening Berichtenbox voor bedrijven maakt gebruik van de DICTU mailservers en hosten zelf geen mailservers. Vanuit dat oogpunt wordt er niet op getest/getoetst.
TLS	Ja	Gevalideerd
		Openbaar en Toegankelijk
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status D	Door de leeftijd van de applicatie voldoet de applicatie op dit moment niet aan de standaarden. Bij de ontwikkeling zal rekening gehouden worden met de WCAG en is het doel een zo hoog mogelijke score te behalen.
		Uitwisselingsfundament
Digikoppeling	Ja	De Berichtenbox voor bedrijven maakt gebruik van de Digikoppeling standaard. Hiermee kunnen instanties via een

		koppeling berichten versturen / ontvangen vanuit, bijvoorbeeld een eigen zaaksysteem.
StUF	Ja	De Digikoppeling van de Berichtenbox voor bedrijven maakt gebruik van het Standaard Uitwisselings Formaat (StUF), versie 3.01

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:
- Authenticatie-standaarden (OpenID.NLGov en SAML)
- security.txt
- STARTTLS en DANE

Niet langer van toepassing zijnde standaarden voor deze voorziening:
- PDF (NEN-ISO)

Verbeteringen; de voorziening voldoet nu (deels) wel aan:
- IPv4 en IPv6

Verslechteringen; de voorziening voldoet nu (deels) niet meer aan:
- Digitoegankelijk (EN 301 549 met WCAG 2.1)

Concluderend moeten voor Berichtenbox voor Bedrijven de volgende standaarden (volledig) geïmplementeerd worden: security.txt en Digitoegankelijk (EN 301 549 met WCAG 2.1).

3.2 Doc-Direkt / RvIHH

Beheerorganisatie: Rijksorganisatie voor Informatiehuishouding (RvIHH)

Werking en inhoud van Doc-Direkt / RvIHH:
Sinds 1 mei gaat Doc-Direkt verder onder de naam Rijksorganisatie voor Informatiehuishouding (RvIHH). De organisatie ondersteunt het Rijk bij het creëren van een toegankelijke, tijdige en transparante informatievoorziening die aansluit bij de huidige wet- en regelgeving. Naast het beheren en bewerken van papieren, digitale of hybride archieven, brengt de RvIHH structuur en ordening aan in alle informatieprocessen van de rijksoverheid.

RvIHH levert slimme tools en advies op maat op alle gebieden van de informatiehuishouding en archivering. Voorbeelden zijn generieke diensten als: het DMS Digidoc Online, Zoek&Vind applicatie, Woo-tooling, de officiële digitale handtekening en voorbereiding van parlementaire enquêtes. Voor meer informatie kijk op https://rvihh.nl.

Geteste web- en maildomeinen:
- www.doc-direkt.nl
  - Bron: https://internet.nl/site/doc-direkt.nl/2796639/
  - Bron: https://internet.nl/site/www.doc-direkt.nl/2796640/#
- Handelingenbank.info
  - Bron: https://internet.nl/site/handelingenbank.info/2796641/
  - Bron: https://internet.nl/mail/handelingenbank.info/1246254/#

Standaard	Status	Toelichting beheerder
		Veilig internet
DKIM	Ja	
DMARC	Ja	
DNSSEC	Ja	
HTTPS en HSTS	Ja	HTTP-compressie maakt het mogelijk om pagina's sneller te laden op mobiele devices. RvIHH heeft het adres handelingenbank.info extern gehost op een server die gedeeld wordt met anderen. Om HTTP-compressie uit te sluiten dient dat voor alle klanten gezamenlijk te gebeuren. Dit ligt nog niet in de planning van de hosting-partij (Zylon).

		De website handelingenbank.info is aan vervanging toe. Daartoe wordt een projectopdracht samengesteld. Het adequaat aanpassen van de headers op het voorkomen van bovengenoemde zaken (geen veilig ingestelde X-Frame-Options, X-Content-Type-Options, Content-Security-Policy) wordt opgenomen in de opdracht.
IPv4 en IPv6	Ja	
NEN-ISO/IEC27001 en NEN-ISO/IEC27002	Ja	RvIHH houdt rekening met de passende kaders bij inkoop en levering van diensten. RvIHH maakt over informatiebeveiliging en privacy afspraken met (sub)leveranciers en afnemers van dienstverlening. De beheersmaatregelen uit de Baseline Informatiebeveiliging Overheid (BIO) die direct betrekking hebben op de operationele dienstverlening van RvIHH zijn geïmplementeerd. RvIHH is een onderdeel van BZK. RvIHH werkt met het door de CISO BZK opgestelde Beleidskader Beveiliging en Privacy dat onder andere gebaseerd is op de BIO. RvIHH heeft besloten naar certificering 27001 toe te gaan werken. Het streven is om eind 2025 / begin 2026 over een certificering te beschikken.
RPKI	Ja	
Authenticatie-standaarden (OpenID.NLGov en SAML)	Ja	Voor verschillende diensten uit de PDC van RvIHH (Documentgenerator, Woo-hulptooling, Zoek&Vind, DMS) wordt gebruik gemaakt van SSOn Rijk. Na authenticatie wordt er een SAML-token uitgewisseld met betreffende toepassing voor veilige communicatie.
security.txt	Deels	De website handelingenbank.info is aan vervanging toe. Daartoe wordt een projectopdracht samengesteld. Het toevoegen van het security.txt bestand wordt opgenomen in de opdracht.
SPF	Ja	
STARTTLS en DANE	Ja	Voor de beide domeinen geldt dat er geen gebruik gemaakt wordt van mailfunctionaliteit. De website handelingenbank.info is aan vervanging toe. Daartoe wordt een projectopdracht samengesteld. In de opdracht wordt advies gevraagd over het plaatsen van een null-MX, aangezien er geen gebruik gemaakt wordt van mailfunctionaliteit. Het hebben van een actief DANE-schema is alleen nodig bij vervanging van certificaat-sleutels. Leverancier heeft bevestigd dat het rolloverschema wordt ingericht zodra er geüpdatet moet gaan worden omdat een certificaat verloopt.
TLS	Ja	Het domein https://doc-direkt.nl wordt uitgefaseerd. RvIHH heeft een nieuwe website als opvolger van https://doc-direkt.nl gerealiseerd. De bezoeker van het oude domein wordt doorgeleid naar het nieuwe domein https://rvihh.nl. Deze site is volledig compliant, zie https://internet.nl/site/rvihh.nl/2875934/ en https://internet.nl/mail/rvihh.nl/1289161/.
		Uitwisselingsfundament
Digikoppeling	Nee	RvIHH beschikt niet over een eigen systeem dat voorziet in Digikoppeling. In het verleden is wel getracht een Digikoppeling aansluiting te realiseren met samenwerkingspartner SSC-ICT, maar dat is niet gelukt. RvIHH maakt wel gebruik van Digikoppeling voor een dienst die ze levert aan BZK, maar die wordt extern gehost.
		Openbaar en toegankelijk

Ades Baseline Profiles	Ja	RvIHH biedt aan afnemers een tekenomgeving aan, waarin een certificaathouder documenten van een digitale handtekening kan voorzien. Het betreft persoonsgebonden certificaten, conform de standaard.
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Gepland	Met leverancier RedNose van Documentgenerator docGen wordt eraan gewerkt om alle sjablonen digitoegankelijk te laten zijn. Verdere instandhouding hiervan tijdens levenscyslus van document is aan afnemer om te organiseren.
PDF (NEN-ISO)	Ja	RvIHH ziet erop toe dat het scannen van documenten aan PDF/A norm voldoet.
SKOS	Nee	De standaard wordt nog niet toegepast. De website handelingenbank.info is aan vervanging toe. Daartoe wordt een projectopdracht samengesteld. Het toevoegen van de thesaurus in SKOS-formaat wordt mogelijk opgenomen in de opdracht.
ODF	Nee	Het ODF wordt niet gebruikt in de eigen bedrijfsvoering. Processen en systemen van zorgdragers die afnemer van dienstverlening van RvIHH zijn, zijn voornamelijk zo ingericht dat documenten gebaseerd op OOXML worden gecreëerd en als zodanig dienen verwerkt te worden.

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:
- Authenticatie-standaarden (OpenID.NLGov en SAML)
- Security.txt

Niet langer van toepassing zijnde standaarden voor deze voorziening:
- OWMS

Verbeteringen; de voorziening voldoet nu (deels) wel aan:
- HTTPS/HSTS

Verslechteringen; de voorziening voldoet nu (deels) niet meer aan:
- Digikoppeling
- Digitoegankelijk (EN 301 549 met WCAG 2.1)

Concluderend moeten voor Doc-Direkt / RvIHH de volgende standaarden (volledig) geïmplementeerd worden: security.txt, Digikoppeling, Digitoegankelijk (EN 301 549 met WCAG 2.1), SKOS en ODF.

3.3 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 diensten en informatie en is daarom met DigiD beveiligd. 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.

Geteste web- en maildomeinen:
- Mijn.overheid.nl
  - Bron: https://internet.nl/site/mijn.overheid.nl/2805189/
  - Bron: https://internet.nl/site/mijnoverheid.nl/2797656/
- @mijn.overheid.nl
  - Bron: https://internet.nl/mail/mijn.overheid.nl/1246682/

- Bron: https://internet.nl/mail/mijnoverheid.nl/1246685/

Standaard	Status	Toelichting beheerder
		Veilig internet
DKIM	Ja	MijnOverheid voldoet aan DKIM.
DMARC	Ja	Deze standaard wordt toegepast.
DNSSEC	Ja	MijnOverheid voldoet aan DNSSEC.
HTTPS en HSTS	Ja	HTTP-compressie is een bewuste, risico-overwogen keuze vanwege grote hoeveelheden data.
IPv4 en IPv6	Ja	De standaard wordt toegepast.
NEN-ISO/IEC27001 en NEN-ISO/IEC27002	Ja	Op MijnOverheid (een Rijksdienst) is de BIO van toepassing, deze is gebaseerd op de ISO27001. Logius verantwoord zich over de BIO aan het kerndepartement (BZK).
NL GOV Assurance profile for OAuth 2.0	Ja	MijnOverheid maakt gebruik van OpenID Connect (OIDC).
RPKI	Ja	Deze standaard wordt toegepast.
Authenticatie-standaarden (OpenID.NLGov en SAML)	Ja	MijnOverheid dienst voorziet in authenticatie middels DigiD. Voor deze koppeling wordt SAML2 gebruikt.
security.txt	Deels	
SPF	Ja	SPF is geïmplementeerd.
STARTTLS en DANE	Ja	MijnOverheid voldoet aan STARTTLS en DANE.
TLS	Ja	Het klopt dat client-initiated-renegotiation toe wordt gestaan. Dit is (nu nog) met reden, zodat ook nog oudere clients bediend kunnen worden. Er wordt overwogen of dit nog gewenst is en indien nodig aangepast. MijnOverheid hanteert TLS1.3
		Uitwisselingsfundament
Digikoppeling	Ja	MijnOverheid heeft meerdere koppelingen met (overheids-) ketenpartijen die allen de Digikoppeling standaarden gebruiken, zowel eBMS, WUS, of REST koppelingen.
OpenAPI Specification	Ja	Voor MijnOverheid worden de OpenAPI v3.0 specificaties in YAML-format gebruikt
REST-API Design Rules	Gepland	Er is een initiatief gestart (reeds lopend) om de bestaande en nieuwe API's van MijnOverheid te laten voldoen aan de benodigde specificaties/standaarden. Dit probleem wordt dus binnen een aanzienlijk korte termijn opgelost.
StUF	Ja	Voor een aantal koppelingen met Gemeentes wordt door MijnOverheid gebruik gemaakt van StUF. Dit is relevant voor de koppelingen van WOZ en Lopende Zaken.
		Openbaar en toegankelijk
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status A	Zie: https://dashboard.digitoegankelijk.nl/organisaties/27/websites-apps/14453
PDF (NEN-ISO)	Ja	De MijnOverheid-dienst, is een dienst die fungeert als een portaal naar de gegevens die ander overheidsinstanties hebben van een burger, en naar de Berichtenbox van een burger. Het kan beschouwd worden als een 'doorgeefluik'. Alle andere overheidsinstanties die documenten aanleveren, o.a. gegevens of in de Berichtenbox doen dit allemaal in PDF-standaard. MijnOverheid controleert of deze aangeleverde berichten aan de standaard voldoen. MijnOverheid produceert zelf ook enkel bestanden voor de burger en die zijn allemaal in PDF/A formaat.

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:
- NL GOV Assurance profile for OAuth 2.0
- Authenticatie-standaarden (OpenID.NLGov en SAML)
- Security.txt

Verbeteringen; de voorziening voldoet nu (deels) wel aan:
- STARTTLS en DANE

Verslechteringen; de voorziening voldoet nu (deels) niet meer aan:
- REST-API Design Rules

Concluderend moeten voor MijnOverheid de volgende standaarden (volledig) geïmplementeerd worden: security.txt en REST-API Design Rules.

3.4 Ondernemersplein

Beheerorganisatie: Kamer van Koophandel (KvK)

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.

Geteste web- en maildomeinen:
- Ondernemersplein.kvk.nl
  - Bron: https://internet.nl/site/ondernemersplein.kvk.nl/2797890/#
  - Bron: https://internet.nl/site/business.gov.nl/2797891/#
- @ondernemersplein.kvk.nl
  - Bron: https://internet.nl/mail/ondernemersplein.kvk.nl/1246887/
  - Bron: https://internet.nl/mail/business.gov.nl/1246889/#

Standaard	Status	Toelichting beheerder
		Veilig internet
DKIM	Ja	
DMARC	Ja	
DNSSEC	Gepland	Dat een mailserverdomein onveilig is, door het ontbreken van DNSSEC-ondertekening, is bekend en dit wordt naar verwachting in Q3 2024 opgepakt.
HTTPS en HSTS	Gepland	Dat een webserver een HSTS-policy aanbiedt met een geldigheidsduur voor caching (max-age) die niet voldoende lang (d.w.z. korter dan 1 jaar) is, is bekend en dit wordt naar verwachting in Q3 2024 opgepakt. Wat betreft het aanbieden van een Content-Security-Policy (CSP) met onveilige instellingen, deze kunnen niet weggehaald worden vanwege de werking van bepaalde functionaliteiten.
IPv4 en IPv6	Ja	
NEN-ISO/IEC27001 en NEN-ISO/IEC27002	Ja	
RPKI	Ja	
security.txt	Ja	De webserver biedt een security.txt-bestand op de juiste plaats aan en de inhoud ervan is syntactisch geldig. Echter, security.txt zou digitaal ondertekend moeten zijn. Dit wordt naar verwachting in Q3 2024 opgepakt.

SPF	Ja	
STARTTLS en DANE	Gepland	Het is bekend dat een mailserverdomein geen TLSA-record voor DANE bevat, dit wordt naar verwachting in Q3 2024 opgepakt.
TLS	Ja	
		Openbaar en Toegankelijk
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status A	
		Uitwisselingsfundament
REST-API Design Rules	Ja	Voor Ondernemersplein API´s zijn de REST-API Design Rules voor zover mogelijk toegepast.
		Bestuur en recht
BWB	Ja	

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:
- DKIM
- Security.txt
- STARTTLS en DANE

Verbeteringen; de voorziening voldoet nu (deels) wel aan:
- HTTPS en HSTS
- Digitoegankelijk (EN 301 549 met WCAG 2.1)

Verslechteringen; de voorziening voldoet nu (deels) niet meer aan:
- DNSSEC

Concluderend moeten voor Ondernemersplein de volgende standaarden (volledig) geïmplementeerd worden: DNSSEC, HTTPS en HSTS en STARTTLS en DANE.

3.5 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.

Geteste web- en maildomeinen:
- www.overheid.nl
  - Bron: https://internet.nl/site/overheid.nl/2797925/
  - Bron: https://internet.nl/site/www.overheid.nl/2797926/
- wetten.overheid.nl
  - Bron: https://internet.nl/site/wetten.overheid.nl/2797927/
- lokaleregelgeving.overheid.nl
  - Bron: https://internet.nl/site/lokaleregelgeving.overheid.nl/2797929/
- @overheid.nl
  - Bron: https://internet.nl/mail/overheid.nl/1246920/

Standaard	Status	Toelichting beheerder
		Veilig internet
DKIM	Ja	
DMARC	Ja	
DNSSEC	Ja	

HTTPS en HSTS	Ja	HTTP-compressie, CSP en Referrer policy worden in Q3 2024 (17-06-2024 t/m 06-09-2024) doorgevoerd.
IPv4 en IPv6	Ja	
NEN-ISO/IEC27001 en NEN-ISO/IEC27002	Nee	KOOP heeft deze standaard niet geïmplementeerd. Er wordt momenteel aan gewerkt om KOOP aan te sluiten bij de implementatie van deze standaard binnen Logius.
RPKI	Ja	
security.txt	Ja	
SPF	Ja	
STARTTLS en DANE	Ja	Geldigheid van de DANE-fingerprint op de domeinnaam in relatie tot het websitecertificaat wordt in het komende Q3 2024 doorgevoerd.
TLS	Ja	Het ondersteunen van meerdere TLS-versies is een bewuste keuze. In het verleden zijn deze TLS-versies uitgezet, maar dit leverde problemen op in de communicatie met sommige andere mailservers die de nieuwere versies nog niet ondersteunden. Daarom zijn deze weer aangezet.
	Uitwisselingsfundament	
REST-API Design Rules	Nee	Overheid.nl is niet de authentieke bron van de content/data die op het portaal wordt ontsloten en biedt daarom geen eigen API aan voor ontsluiting van deze content. Overheid.nl maakt derhalve gebruik van de API's van de achterliggende authentieke bronnen om content te publiceren op het portaal.
	Openbaar en toegankelijk	
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status A	

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:
- Security.txt
- SPF

Niet langer van toepassing zijnde standaarden voor deze voorziening:
- NL GOV Assurance profile for OAuth 2.0
- PDF (NEN-ISO)
- SKOS
- BWB
- JCDR

Verbeteringen; de voorziening voldoet nu (deels) wel aan:
- RPKI
- Digitoegankelijk (EN 301 549 met WCAG 2.1)

Verslechteringen; de voorziening voldoet nu (deels) niet meer aan:
- NEN-ISO/IEC27001 en NEN-ISO/IEC27002

Concluderend moeten voor Overheid.nl de volgende standaarden (volledig) geïmplementeerd worden: NEN-ISO/IEC27001 en NEN-ISO/IEC27002 en REST-API Design Rules.

3.6 Rijksoverheid.nl

Beheerorganisatie web: Dienst Publiek en Communicatie, ministerie van Algemene Zaken
Beheerorganisatie e-mail: SSC-ICT, ministerie van Binnenlandse Zaken

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 agentschap van het ministerie

van AZ en biedt shared servicediensten aan de Rijksoverheid op het gebied van communicatie. Het e-mailadres @rijksoverheid.nl wordt gebruikt door mensen van het ministerie van BZK en samenwerkingsverbanden tussen verschillende ministeries. Van het webdomein is DPC eigenaar en beheerder. DPC is tevens de beheerder van het hoofddomein voor de DNS. Het e-maildomein @rijksoverheid.nl wordt technisch beheerd door SSC-ICT.

Dit jaar zijn de web- en maildomeinen samengevoegd in de onderstaande tabel. De resultaten zijn door de beheerders van AZ en SSC-ICT afgestemd.

Geteste web- en maildomeinen:
- Rijksoverheid.nl
    - Bron: https://internet.nl/site/rijksoverheid.nl/2797716/
    - Bron: https://internet.nl/site/www.rijksoverheid.nl/2797717/
- @rijksoverheid.nl:
    - Bron: https://internet.nl/mail/rijksoverheid.nl/1246742/

Standaard	Status	Toelichting beheerder
		Veilig internet
DKIM	Ja	
DMARC	Ja	
DNSSEC	Ja	
HTTPS en HSTS	Ja	Het toepassen van HTTP-compressie is een bewuste afweging. Het restrisico is op andere manieren gemitigeerd. De desbetreffende instelling in de aanwezige CSP is bewust en op dit moment nodig voor de werking van de website. De bewust gebruikte waarde met betrekking tot de Referrer-Policy is op dit moment nodig voor de juiste werking van de website.
IPv4 en IPv6	Ja	
NEN-ISO/IEC27001 en NEN-ISO/IEC27002	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	Ja	
security.txt	Ja	
SPF	Ja	
STARTTLS en DANE	Ja	STARTLS en DANE is geregeld voor het maildomein.
TLS	Ja	
		Bestuur en recht
BWB	Ja	Binnen de website wordt verwezen naar wetgeving conform de BWB standaard. BWB wordt toegepast.
		Openbaar en toegankelijk
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status B	Zie: https://dashboard.digitoegankelijk.nl/organisaties/20/websites-apps/14046
PDF (NEN-ISO)	Ja	De centrale redactie van Rijksoverheid.nl stuurt op het aanbieden van de juiste typen PDF's. De redactie heeft geen zicht op, en is niet verantwoordelijk voor, het type PDF's dat door decentrale redacteuren van de ministeries zelfstandig via het platform open.overheid.nl op Rijksoverheid.nl worden geplaatst. PDF-documenten die de redactie zelf op Rijksoverheid.nl publiceert voldoen wel aan het juiste type PDF. Een aantal redacteuren is getraind in maken van digitaal toegankelijke Word- en PDF-documenten.
ODF	Ja	Het Platform Rijksoverheid Online en dus ook Rijksoverheid.nl accepteert alleen het gebruik van de volgende formaten: odt, ods, odp, pdf, rtf, zip, epub, csv, xml, sha2.

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:

- Security.txt

Verbeteringen; de voorziening voldoet nu (deels) wel aan:

- PDF (NEN-ISO)

Concluderend moet voor Rijksoverheid.nl de volgende standaard (volledig) geïmplementeerd worden: Digitoegankelijk (EN 301 549 met WCAG 2.1).

3.7 Rijksportaal

Beheerorganisatie: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Werking en inhoud van Rijksportaal:

Rijksportaal is het (Rijksbrede) raamwerk voor intranettoepassing voor alle (kern)departementen en verschillende uitvoeringsinstanties. Hiermee is het merendeel van de oorspronkelijke intranetten van de(kern)departementen vervangen. Rijksportaal geeft de rijksambtenaar toegang tot Rijksbrede en departementspecifieke informatie, bronnen en toepassingen. Ook is het vanuit het Rijksportaal mogelijk om nieuws van andere departementen te volgen en personeels- en facilitaire zaken te regelen.

Toelichting van de beheerder met betrekking tot het te onderzoeken webdomein:
De onderstaande url's zijn niet/of niet meer van het Rijksportaal. De eerste twee hebben betrekking op een domein welke niet van Rijksportaal is, maar ook niet door Rijksportaal is geregistreerd. De beheerder meent dat dit domein ooit is geclaimd door het ministerie Algemene Zaken. De laatste twee zijn url's van het oude Rijksportaal. Deze is in 2021 uitgezet en bestaat niet meer.

- *www.rijksportaal.nl*
- *rijksportaal.nl*
- *portal.rijksweb.nl*
- *portal.rp.rijksweb.nl*

Standaard	Status	Toelichting beheerder
		Veilig internet
DMARC	Ja	RFC7489 is toegepast.
DNSSEC	Ja	RFC4033, RFC4034 en RFC4035 zijn toegepast.
HTTPS en HSTS	Ja	HTTPS 1.2 en HSTS 1.2 zijn toegepast.
IPv4 en IPv6	Ja	IPv4 en IPv6 zijn toegepast.
RPKI	Ja	Rijksportaal is alleen toegankelijk op de overheidsomgeving (Haagse Ring) en VPN Diginetwerk deze omgevingen voldoen aan de standaard.
Authenticatie-standaarden (OpenID.NLGov en SAML)	Ja	SAML 2.0 is toegepast.
security.txt	Nee	Geen verdere toelichting vanuit de beheerder.
SPF	Ja	SPF 1 is toegepast.
TLS	Ja	TLS 1.2 en 1.3 zijn toegepast.
		Openbaar en toegankelijk
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status B	Zie voor meer informatie: https://www.rijksoverheid.nl/documenten/rapporten/2022/12/22/onderzoek-rijksportaal-overheid-i-nl-wcag-2-1-aa
PDF (NEN-ISO)	Ja	

ODF	Ja	ODF wordt ondersteund: ODF-bestanden kunnen geüpload en gedownload worden en de inhoud van ODF-bestanden kan door de zoekmachine worden geïndexeerd. Naast ODF worden op het Rijksportaal ook andere documentformaten gebruikt; het gebruik van ODF wordt niet afgedwongen.

Het nieuwe Rijksportaal bestaat sinds 2021 en heeft de volgende url: https://rijksportaal.overheid-i.nl/. Het Rijksportaal is het intranet van de Rijksoverheid en is alleen te benaderen via het interne netwerk de "Haagse Ring" of via een speciale VPN welke direct op Diginetwerk kan. Het Rijksportaal is niet te bereiken via het internet.

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:
- Authenticatie-standaarden (OpenID.NLGov en SAML)
- Security.txt

Niet langer van toepassing zijnde standaarden voor deze voorziening:
- DKIM

Verbeteringen; de voorziening voldoet nu (deels) wel aan:
- DMARC
- DNSSEC
- HTTPS en HSTS
- IPv4 en IPv6
- RPKI
- SPF
- Digitoegankelijk (EN 301 549 met WCAG 2.1)

Concluderend moeten voor Rijksportaal de volgende standaarden (volledig) geïmplementeerd worden: security.txt en Digitoegankelijk (EN 301 549 met WCAG 2.1).

3.8 Samenwerkende Catalogi

Beheerorganisatie: Logius

Werking en inhoud 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.

Geteste web- en maildomeinen:
- Zoekdienst.overheid.nl
    - Bronnen:
        - https://internet.nl/site/zoekdienst.overheid.nl/2869290/
        - https://internet.nl/mail/zoekdienst.overheid.nl/1248331/

Standaard	Status	Toelichting beheerder
		Veilig internet
DKIM	Gepland	De API van zoekdienst.overheid.nl zal dit jaar worden gemigreerd naar een nieuwe hosting partij. Als gevolg van deze migratie zal dit punt in 2024 opgelost worden.
DMARC	Ja	
DNSSEC	Ja	

HTTPS en HSTS	Ja	De API van zoekdienst.overheid.nl zal dit jaar worden gemigreerd naar een nieuwe hosting partij. Als gevolg van deze migratie zullen de restpunten in 2024 worden opgelost.
IPv4 en IPv6	Ja	
RPKI	Ja	
security.txt	Ja	
SPF	Gepland	De API van zoekdienst.overheid.nl zal dit jaar worden gemigreerd naar een nieuwe hosting partij. Als gevolg van deze migratie zal dit punt in 2024 opgelost worden.
TLS	Ja	
		Uitwisselingsfundament
OpenAPI Specification	Ja	Bronvermelding vanuit de beheerder: https://zoekdienst-sc.github.io/openapi.yaml
REST-API Design Rules	Nee	Er heeft tot nu toe geen vernieuwing op de API plaatsgevonden waarin dit kon worden meegenomen.
		Openbaar en Toegankelijk
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status B	De pagina's op Logius.nl zijn Digitoegankelijk.

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:

- DKIM
- DNSSEC
- Security.txt

Verbeteringen; de voorziening voldoet nu (deels) wel aan:

- HTTPS en HSTS
- TLS
- OpenAPI Specification
- Digitoegankelijk (EN 301 549 met WCAG 2.1)

Concluderend moeten voor Samenwerkende Catalogi de volgende standaarden (volledig) geïmplementeerd worden: DKIM, SPF, REST-API Design Rules en Digitoegankelijk (EN 301 549 met WCAG 2.1).

3.9 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. Sommige getoonde objectkenmerken, zoals bouwjaar en gebruiksoppervlakte, zijn afkomstig uit de Basisregistratie Adressen en Gebouwen. Ook voor deze gegevens is de gemeente verantwoordelijk. De getoonde grondoppervlakte is afkomstig uit de Basisregistratie Kadaster.

Geteste web- en maildomeinen:

- www.wozwaardeloket.nl
  - Bron: https://internet.nl/site/www.wozwaardeloket.nl/2787288/
- @wozwaardeloket.nl
  - Bron: https://internet.nl/mail/wozwaardeloket.nl/1257073/

Standaard	Status	Toelichting beheerder
		Veilig internet
DMARC	Ja	WOZ-Waardeloket is DMARC-compliant.
DNSSEC	Ja	WOZ-Waardeloket is DNSSEC-compliant.
HTTPS en HSTS	Ja	De beheerder zal overwegen om HTTP-compressie uit te schakelen. Het WOZ-waardeloket biedt overigens publieke informatie die alle gebruikers toch al onbelemmerd kunnen inzien, ook al wordt voor het transport TLS gebruikt. Daarnaast wordt onderzocht hoe de juiste content-security-policy ingesteld kan worden.
IPv4 en IPv6	Ja	WOZ-Waardeloket voldoet aan de IPv6 en IPv4 standaarden.
NEN-ISO/IEC27001 en NEN-ISO/IEC27002	Ja	Het Kadaster heeft het beleid dat de gehanteerde BIO (Baseline informatiebeveiliging Overheid) gebaseerd wordt op de laatste versie van marktconforme standaard ISO 27001, en de best practices uit ISO 27002 aangevuld met overheid specifieke maatregelen zoals beschreven in de BIO. Het Kadaster heeft dit jaar een nieuwe externe audit laten doen en werkt komende maanden aan verbeterpunten op basis van de gedane constateringen ten behoeve van nieuwe ISO 27001-certificering later in 2024.
RPKI	Ja	WOZ-Waardeloket is RPKI-compliant.
security.txt	Ja	WOZ-Waardeloket voldoet aan de security.txt standaard.
SPF	Ja	WOZ-Waardeloket is SPF-compliant.
TLS	Ja	WOZ-Waardeloket is TLS-compliant.
		Openbaar en toegankelijk
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status B	WOZ-Waardeloket heeft een toegankelijkheidsverklaring en voldoet daarmee aan de Digitoegankelijk standaard. Zie: https://www.toegankelijkheidsverklaring.nl/register/2678
PDF (NEN-ISO)	Ja	Het WOZ-waardeloket biedt de mogelijkheid een schermafdruk van de gegevens in PDF 1.7-formaat te downloaden. Zie: https://www.forumstandaardisatie.nl/open-standaarden/pdf-nen-iso

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:

- security.txt

Verbeteringen; de voorziening voldoet nu (deels) wel aan:

- DMARC
- TLS

Verslechteringen; de voorziening voldoet nu (deels) niet meer aan:

- Digitoegankelijk (EN 301 549 met WCAG 2.1)

Concluderend moet voor WOZ Waardeloket de volgende standaard (volledig) geïmplementeerd worden: Digitoegankelijk (EN 301 549 met WCAG 2.1).

4. Gegevens en registreren

4.1 BAG / BRK / BGT / WOZ / BRT

Beheerorganisatie: Kadaster

Werking en inhoud van BAG:
Gegevens van alle adressen en gebouwen in Nederland, zoals bouwjaar, oppervlakte, gebruiksdoel en locatie op de kaart.

Werking en inhoud van BRK:
De Basisregistratie Kadaster (BRK) bestaat uit de kadastrale registratie en de kadastrale kaart.

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

N.B.: De BGT heeft geen apart, toetsbaar website- of maildomein. Deze voorziening wordt daarom niet getoetst in het kader van het voorzieningenonderzoek van de Monitor Open Standaarden in 2024.

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

Werking en inhoud van BRT:
De BRT bestaat uit digitale topografische bestanden op verschillende schaalniveaus. Deze verzameling topografische bestanden is via dit portaal beschikbaar als open data.

Geteste web- en maildomeinen:
- Kadaster.nl
  - Bron: https://internet.nl/site/kadaster.nl/2789146/#
- www.kadaster.nl
  - Bron: https://internet.nl/site/www.kadaster.nl/2789148/#
- mijn.kadaster.nl
  - Bron: https://internet.nl/site/mijn.kadaster.nl/2789149/#
- bag.basisregistraties.overheid.nl
  - Bron: https://internet.nl/site/bag.basisregistraties.overheid.nl/2789151/#
- brk.basisregistraties.overheid.nl
  - Bron: https://internet.nl/site/brk.basisregistraties.overheid.nl/2789152/#
- brt.basisregistraties.overheid.nl
  - Bron: https://internet.nl/site/brt.basisregistraties.overheid.nl/2789153/#
- https://catalogus.kadaster.nl/nl/
  - Bron: https://internet.nl/site/catalogus.kadaster.nl/2843204/
- *@kadaster.nl – Dit maildomein is al getoetst in het kader van een andere voorziening en zal daarom niet meegenomen worden in het kader van de BAG, BRK, BGT, WOZ en BRT*.

Standaard	Status	Toelichting beheerder
		Veilig internet
DKIM	Ja	
DMARC	Ja	
DNSSEC	Ja	

HTTPS en HSTS	Deels	Het niet aanbieden van een HSTS-policy is bewust omdat op dit domein XSD's aangeboden worden op een onveilige URL. Het aanpassen van deze schema's heeft een behoorlijke impact op het ecosysteem van afnemers van deze API's en wordt daarom geleidelijk met andere aanpassingen op betreffende API's doorgevoerd. De beheerder zal daarnaast overwegen om HTTP-compressie uit te schakelen. De BAG, BRK, BGT, BRT en het WOZ-waardeloket biedt overigens publieke informatie die alle gebruikers toch al onbelemmerd kunnen inzien, ook al wordt voor het transport TLS gebruikt. Daarnaast wordt onderzocht hoe de juiste content-security-policy ingesteld kan worden.
IPv4 en IPv6	Ja	
NEN-ISO/IEC27001 en NEN-ISO/IEC27002	Ja	Het Kadaster heeft het beleid dat de gehanteerde BIO (Baseline informatiebeveiliging Overheid) gebaseerd wordt op de laatste versie van marktconforme standaard ISO 27001, en de best practices uit ISO 27002 aangevuld met overheid specifieke maatregelen zoals beschreven in de BIO. Het Kadaster heeft dit jaar een nieuwe externe audit laten doen en werkt komende maanden aan verbeterpunten op basis van de gedane constateringen ten behoeve van nieuwe ISO 27001-certificering later in 2024.
RPKI	Ja	
Authenticatie-standaarden (OpenID.NLGov en SAML)	Ja	In Mijn Kadaster wordt bij gebruik van de WDO-middelen gebruik gemaakt van SAML, Voor de informatie van de genoemde diensten is de WDO niet van toepassing. De informatie is beschikbaar als open data.
security.txt	Deels	De webserver biedt geen security.txt-bestand op de juiste plaats aan, het kon niet worden opgehaald, of de inhoud ervan is syntactisch niet geldig. De beheerder pakt dit op.
SPF	Ja	
TLS	Ja	
		Uitwisselingsfundament
Geo-standaarden	Ja	
OpenAPI Specification	Ja	
REST-API Design Rules	Ja	
StUF	Ja	
		Economie en werk
NLCIUS	Ja	Voor zover onderzochte diensten gefactureerd worden, in de meeste gevallen is het open data.
		Openbaar en toegankelijk
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status B	Zie: https://dashboard.digitoegankelijk.nl/organisaties/292
PDF (NEN-ISO)	Ja	Voor zover van toepassing zoals uittreksel Kadastrale kaart
SKOS	Ja	De catalogus voor de onderzochte diensten is te vinden op https://catalogus.kadaster.nl/nl/.

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:

- Authenticatie-standaarden (OpenID.NLGov en SAML)
- Security.txt

Niet langer van toepassing zijnde standaarden voor deze voorziening:
- NL GOV Assurance profile for OAuth 2.0
- STARTTLS en DANE
- OWMS
- Digikoppeling

Verbeteringen; de voorziening voldoet nu (deels) wel aan:
- Authenticatie-standaarden (OpenID.NLGov en SAML)
- TLS
- Digitoegankelijk (EN 301 549 met WCAG 2.1)
- PDF (NEN-ISO)
- SKOS
- NLCIUS

Concluderend moeten voor BAG, BRK, BGT, WOZ en BRT de volgende standaarden (volledig) geïmplementeerd worden: HTTPS en HSTS, security.txt en Digitoegankelijk (EN 301 549 met WCAG 2.1).

4.2 BRI

Beheerorganisatie: Belastingdienst

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

Tijdens de looptijd van dit onderzoek is het niet gelukt om de mate van compliance van de relevante standaarden voor de BRI te krijgen voor 2024. In overleg met de beheerder is besloten om de tabel van het laatste meetmoment (2021) te gebruiken en zodoende de voorziening wel mee te nemen in de rapportage.

Standaard	Status	Toelichting beheerder
		Veilig Internet
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 het VIR (Voorschrift Informatiebeveiliging Rijksdienst) 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.
RPKI (Beveiligen van de routing infrastructuur)	Ja	Eigen IP-adressen zijn ondertekend met RPKI. De BD valideert niet zelf RPKI ondertekende adressen, dat doet de internetprovider.
TLS (Beveiligde, versleutelde verbindingen)	Ja	Versie 1.2 van TLS maakt deel uit van de standaard beveiligingsrichtlijnen van de Belastingdienst.
		Uitwisselingsfundament
Digikoppeling 2.0 (Veilige berichtenuitwisselingen)	Nee	Digikoppeling wordt toegepast in de rol van afnemer van berichten van basisregistraties(Handelsregister). De ebMS-koppeling met Digilevering is operationeel in de productie-omgeving. De aansluiting op Digilevering wordt nu alleen gebruikt in de rol van afnemer van het stelsel van basisregistraties. Het aansluiten van de BRI als Basisregistratie/leverancier op Digilevering is niet gepland.

Toelichting PBLQ: Er zijn geen wijzigingen in de tabel, aangezien de tabel uit 2021 is opgenomen in de rapportage.

4.3 BRO

Beheerorganisatie: Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

Werking en inhoud van BRO:
De Basisregistratie Ondergrond (BRO) brengt alle informatie over de Nederlandse ondergrond op één plek bij elkaar en stelt deze via één loket digitaal beschikbaar. Per 1 januari 2018 is de wet BRO in werking getreden voor de eerste tranche van registratieobjecten (Geotechnisch sondeeronderzoek, Booronderzoek, Grondwatermonitoringput). De ketenprocessen van de BRO zijn ingericht en de bronhouders zijn in staat om aan te (laten) leveren via het Bronhouderportaal aan de Landelijke Voorziening (LV). Er is een gebruiksplicht inwerking getreden voor overheidsorganisaties en iedereen die in opdracht van hen werkzaamheden verricht. Voor meer informatie over de BRO kunt u terecht op de webpagina https://basisregistratieondergrond.nl.

Vanuit de BRO onderzoeken we de volgende webdomeinen: bronhouderportaal-bro.nl en broloket.nl. Het beheer van de Basisregistratie Ondergrond (BRO) wordt gecoördineerd door het Ministerie van Binnenlandse Zaken. Het technisch beheer is uitbesteed aan ICTU, Rijkswaterstaat (RWS) en TNO. Voor de voorziening onderzoeken we de volgende webdomeinen:

- bronhouderportaal-bro.nl (TNO)
- broloket.nl (TNO)
- bro-productomgeving.nl (TNO)
- basisregistratieondergrond.nl (RWS)
- bromonitor.nl (ICTU)

Toelichting vanuit PBLQ: Voor het onderzoek 2024 hebben we alleen antwoorden ontvangen voor de domeinen die door TNO worden beheerd, met uitzondering van bro-productomgeving.nl. Dit webdomein zit in de nasleep van een cloud-migratie. Deze en de overige domeinen zijn daarom buiten beschouwing gelaten.

Geteste web- en maildomeinen:
- www.bronhouderportaal-bro.nl
  - Bron: https://internet.nl/site/bronhouderportaal-bro.nl/2817814/
- https://www.broloket.nl
  - Bron: https://internet.nl/site/www.broloket.nl/2817816/

Standaard	Status	Toelichting beheerder
		Veilig internet
DNSSEC	Ja	
HTTPS en HSTS	Deels	Het klopt dat het domein https://www.bronhouderportaal-bro.nl en https://www.broloket.nl niet automatisch worden doorverwezen van HTTP naar HTTPS. Dit gebeurt overigens wel op domeinen https://bronhouderportaal-bro.nl en https://broloket.nl. Het issue wordt opgenomen op de planning. Het klopt het dat https://www.bronhouderportaal-bro.nl HTTP-compressie ondersteund. Dit gebeurt echter op de applicatieserver. Deze issues worden opgenomen op de planning.
IPv4 en IPv6	Ja	
NEN-ISO/IEC27001 en NEN-ISO/IEC27002	Ja	Zowel TNO als de leverancier/beheerder van de infrastructuur beschikken over de genoemde certificeringen. Er wordt voldaan aan de BIO. Zie ook de jaarlijkse ‘in control verklaring BIO’.
NL GOV Assurance profile for OAuth 2.0	Gepland	Oauth wordt toegepast toe bij notificaties en het is de ambitie om het BRO Bronhouderportaal ook te laten voldoen. Het groeipad voor dat laatste is als volgt: er wordt momenteel een BASIC AUTH

		mechanisme geïmplementeerd. De tokens worden verkregen via inloggen op het bronhouderportaal (via de geauthentiseerde webtoegang). Stap 1 (afgelopen 1.5 jaar transitie): het aantal tokens in het werkveld is drastisch teruggebracht. Dit komt door de "ontwarring" autorisatie / authenticatie. Het token wordt nu slechts gebruikt voor authenticatie. Autorisatie wordt middels een nieuwe REST service (v2) geregeld. Alle aangesloten partijen zijn inmiddels over. De tokens hebben ook een eindige levensduur gekregen. Stap 2: gepland vanaf Q4: parallelle introductie oAuth2 met als doel, uit-faseren BASIC AUTH eind 2025., maar dat is nog een groeipad
RPKI	Ja	
Authenticatie-standaarden (OpenID.NLGov en SAML)	Ja	Er wordt gebruik gemaakt van E-Herkenning, gebaseerd op SAML.
security.txt	Nee	Het klopt dat geen van de webservers het security.txt bestand aanbieden. Een onderzoek wordt op de backlog geplaatst en dit wordt, indien nodig/relevant, geïmplementeerd.
STARTTLS & DANE	Nee	Het klopt dat geen van de websitedomeinen TLSA-records bevatten voor DANE. Dit is al eerder onderzocht. De externe e-mailprovider (Solarwinds / Mail Assure) biedt hiervoor geen ondersteuning.
TLS	Ja	
		Uitwisselingsfundament
Digikoppeling	Ja	De BRO voldoet aan digikoppeling (WUS).
Geo-standaarden	Ja	De Geo-standaarden hebben heel recent een update gekregen. De BRO werkt aan implementatie van de laatste standaard, als één van de vroege implementators van OGC API features. De standaarden die golden toen gestart werd met bouw (WFS) voldoen wel. Daarnaast voldoet de BRO aan Geopackage.
OpenAPI Specification	Ja	De BRO voldoet. Dit wordt gevalideerd op de Developer Overheid website (zoek op BRO / BZK)
REST-API Design Rules	Deels	De BRO is compliant aan deze standaard. Dit geldt overigens voor alle API's behalve de REST-API op het bronhouderportaal. Hier is een update gepland.
		Bestuur en recht
BWB	Gepland	Versies van GAS (globale architectuur schets) en PSA (project start architectuur) en aanvullende architectuurdocumenten zullen evenals relevante onderdelen van website en documentatie gebruik maken van deze standaard voor verwijzingen naar wet- en regelgeving. (zie voorbeeld https://www.overheid.nl/help/wet-en-regelgeving/verwijzen-naar-wet-en-regelgeving). In de planning is opgenomen dat er eind 2024/begin 2025 een 'Project eind-architectuur' zal worden opgeleverd, gelijk oplopend met het in beheer nemen van Fase 2 van het project.
		Openbaar en toegankelijk
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status B en Status E	Enkele van de webdomeinen hebben een zelfverklaring met verschillende statussen (B en E). Zie hieronder de specificaties. - Voor website https://www.broloket.nl: status B (TNO). Zie https://dashboard.digitoegankelijk.nl/organisaties/658/websites-apps/3565 - Voor website: https://www.bronhouderportaal-bro.nl/login: status E. Zie

		https://dashboard.digitoegankelijk.nl/organisaties/53/websites-apps/d6235764
PDF (NEN-ISO)	Ja	In de lijst met open standaarden, welke refereert aan de PDF (NEN-ISO), wordt voor een PDF/UA document minimaal de 1.7 versie gevraagd. De in de BRO DMS aangeboden opslag documenten in pdf-formaat voldoen hieraan.
SKOS	Ja	Begrippen uit de BRO worden in SKOS (en NL-SBB) gepubliceerd op https://definities.geostandaarden.nl/nl/ Daarnaast staat ook een subset van begrippen van de BRO in SKOS (en in de nabije toekomst NL-SBB) op www.stelselcatalogus.nl. We werken met Logius aan volledige vulling.
		Schoon water en beschermde bodem
SIKB0101	Ja	De SIKB0101 standaard wordt volledig gevolgd bij het milieukwaliteit domein (registratieobjecten SLD/SAD).

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:
- NL GOV Assurance profile for OAuth 2.0
- Authenticatie-standaarden (OpenID.NLGov en SAML)
- Security.txt
- STARTTLS & DANE
- SKOS
- SIKB0101

Niet langer van toepassing zijnde standaarden voor deze voorziening:
- DKIM
- DMARC
- SPF
- Aquo-standaard

Verbeteringen; de voorziening voldoet nu (deels) wel aan:
- DNSSEC
- IPv4 en IPv6
- RPKI

Verslechteringen; de voorziening voldoet nu (deels) niet meer aan:
- REST-API Design Rules
- BWB

Concluderend moeten voor BRO de volgende standaarden (volledig) geïmplementeerd worden: HTTPS en HSTS, NL GOV Assurance profile for OAuth 2.0, security.txt, STARTTLS en DANE, REST-API Design Rules, BWB en Digitoegankelijk (EN 301 549 met WCAG 2.1).

4.4 BRV

Beheerorganisatie: Dienst Wegverkeer (RDW)

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

Geteste web- en maildomeinen:
- www.rdw.nl
  - Bron: https://internet.nl/site/www.rdw.nl/2891852/
  - https://internet.nl/site/rdw.nl/2891854/
- @rdw.nl

- https://internet.nl/mail/rdw.nl/1297741/

Standaard	Status	Toelichting beheerder
		Veilig internet
DKIM	Ja	
DMARC	Ja	
DNSSEC	Ja	
HTTPS en HSTS	Ja	De BRV is in afstemming met de leverancier van ons CMS, van waaruit de site wordt gegenereerd, of de gepaste maatregelen kunnen worden genomen.
IPv4 en IPv6	Gepland	Met de migratie naar Exchange-online in het derde kwartaal van 2024, waarin IPv6 een speerpunt is, moet dit opgelost zijn.
NEN-ISO/IEC27001 en NEN-ISO/IEC27002	Ja	
NL GOV Assurance profile for OAuth 2.0	Ja	
RPKI	Ja	
Authenticatie-standaarden (OpenID.NLGov en SAML)	Ja	
security.txt	Ja	
SPF	Ja	
STARTTLS en DANE	Gepland	Voor een volledige implementatie bestond een afhankelijkheid met Microsoft. Deze wordt op korte termijn opgelost en de planning is om in september 2024 hieraan volledig te voldoen.
TLS	Gepland	Voor een volledige implementatie bestond een afhankelijkheid met Microsoft. Deze wordt op korte termijn opgelost en de planning is om in september 2024 hieraan volledig te voldoen.
		Uitwisselingsfundament
OpenAPI Specification	Ja	Voor nieuwe REST-API ontsluitingen wordt deze standaard toegepast.
REST-API Design Rules	Ja	Voor nieuwe REST-API ontsluitingen wordt deze standaard toegepast.
Digikoppeling	Deels	RDW maakt voor alle nieuwe uitwisselingen gebruik van Digikoppeling. Dat is onder meer het geval in de uitwisseling met MijnOverheid (Berichtenbox), CJIB, Politie, ILT, CBR, de Belastingdienst, etc. De intentie is uitgesproken om ook bestaande koppelingen proactief te migreren om de voordelen van het Diginetwerk te benutten. Een planning hiervoor is nog niet vastgesteld.
		Economie en werk
NLCIUS	Ja	Met de implementatie van AFAS eind 2022 beschikt RDW over deze standaard.
		Openbaar en toegankelijk
Ades Baseline Profiles	Deels	Niet alle elektronische documenten worden gewaarmerkt. De documenten die worden gewaarmerkt voldoen aan de Ades Baseline Profiles.
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status B	RDW heeft een toegankelijkheidsverklaring “B – Voldoet gedeeltelijk (onderbouwing toereikend). Er wordt verwezen naar: https://www.toegankelijkheidsverklaring.nl/register/18530
PDF (NEN-ISO)	Ja	

SKOS	Ja

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:
- Authenticatie-standaarden (OpenID.NLGov en SAML)
- Security.txt
- NLCIUS
- Ades Baseline Profiles

Niet langer van toepassing zijnde standaarden voor deze voorziening:
- OWMS

Verbeteringen; de voorziening voldoet nu (deels) wel aan:
- DNSSEC
- HTTPS en HSTS
- NL GOV Assurance profile for OAuth 2.0
- REST-API Design Rules

Verslechteringen; de voorziening voldoet nu (deels) niet meer aan:
- IPv4 en IPv6
- TLS

Concluderend moeten voor BRV de volgende standaarden (volledig) geïmplementeerd worden: IPv6, STARTTLS en DANE, TLS, Digikoppeling, Ades Baseline Profiles en Digitoegankelijk (EN 301 549 met WCAG 2.1).

4.5 Digilevering

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting beheerder
		Veilig internet
DKIM	Ja	
DMARC	Ja	
DNSSEC	Ja	
HTTPS en HSTS	Ja	De webserver biedt geen Content-Security-Policy (CSP) aan, of biedt CSP aan met bepaalde onveilige instellingen.
Authenticatie-standaarden (OpenID.NLGov en SAML)	Ja	Authenticatie voor de applicatie worden geïmplementeerd middels Spring Security. Het portaal maakt gebruik van eHerkenning voor authenticatie van gebruikers. eHerkenning maakt gebruik van SAML2.
IPv4 en IPv6	Nee	De website is bereikbaar via IPv4 en IPv6, maar de beschikbare poorten of aangeboden headers over IPv4 zijn niet hetzelfde over IPv6.
RPKI	Ja	
security.txt	Ja	
SPF	Ja	
STARTTLS en DANE	Ja	
		Uitwisselingsfundament

Digikoppeling	Ja	Digilevering maakt gebruik van de Digikoppeling standaard voor het uitwisselen van berichten.
Geo-standaarden	Ja	Het Kadaster maakt gebruik van Geo-standaarden in het Digilevering-berichtenverkeer.
		Openbaar en toegankelijk
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status C	

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:
- Authenticatie-standaarden (OpenID.NLGov en SAML)
- Security.txt
- Geo-standaarden

Verslechteringen; de voorziening voldoet nu (deels) niet meer aan:
- Digitoegankelijk (EN 301 549 met WCAG 2.1)

Concluderend moeten voor Digilevering de volgende standaarden (volledig) geïmplementeerd worden: IPv6 en Digitoegankelijk (EN 301 549 met WCAG 2.1).

4.6 Digimelding

Beheerorganisatie: Logius

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

Standaard	Status	Toelichting beheerder
		Veilig internet
DKIM	Ja	Voldoet
DMARC	Ja	Voldoet
DNSSEC	Ja	Voldoet
HTTPS en HSTS	Ja	Voldoet
IPv4 en IPv6	Ja	Voldoet
RPKI	Ja	Voldoet
security.txt	Ja	Voldoet
SPF	Ja	Voldoet
STARTTLS en DANE	Gepland	De inhoud van het DANE record moet aangepast i.v.m. nieuw websitecertificaat. De aanvraag om de nieuwe string in DNS te zetten is al via ketenbeheer ingediend.
		Uitwisselingsfundament
Digikoppeling	Ja	Voldoet
		Openbaar en toegankelijk
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status D	Er zijn al veel stories opgepakt om dit te verbeteren op de huidige DGM. Met de nieuwe frontend is by design al met de digitoegankelijkheid rekening gehouden. Zodra deze op productie staat zal er een nieuwe scan gedaan moeten worden om dat te kunnen beoordelen.

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:
- Security.txt

Verbeteringen; de voorziening voldoet nu (deels) wel aan:
- IPv4 en IPv6

Verslechteringen; de voorziening voldoet nu (deels) niet meer aan:
- STARTTLS en DANE
- Digitoegankelijk (EN 301 549 met WCAG 2.1)

Concluderend moeten voor Digimelding de volgende standaarden (volledig) geïmplementeerd worden: STARTTLS en DANE en Digitoegankelijk (EN 301 549 met WCAG 2.1).

4.7 Nieuw Handelsregister (NHR)

Beheerorganisatie: Kamer van Koophandel

Werking en inhoud van 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.

Geteste web- en maildomeinen:
- www.kvk.nl
  - Bron: https://internet.nl/site/www.kvk.nl/2742629/
- @kvk.nl
  - Bron: https://internet.nl/mail/kvk.nl/1217169/

Standaard	Status	Toelichting beheerder
		Veilig internet
DKIM	Ja	NHR is DKIM-compliant.
DMARC	Ja	NHR is DMARC-compliant.
DNSSEC	Gepland	Het feit dat één mailserverdomein onveilig is, omdat deze niet ondertekend is met DNSSEC, wordt veroorzaakt door dat dit een Microsoft mailserver betreft. Microsoft ondersteunt DNSSEC al wel voor outbound emailverkeer maar nog niet voor inbound. Deze functionaliteit komt wel binnenkort beschikbaar maar de uitrol is vertraagd. Zie update van Microsoft van april 2024: *We regretfully must delay the public preview for Inbound SMTP DANE with DNSSEC from March to May 2024 due to necessary security investments that were identified as part of a Private Preview. This extension allows us the opportunity to further enhance our service's security measures, ensuring we meet the highest standards for our users. We appreciate your understanding and patience as we make these improvements.*
HTTPS en HSTS	Ja	NHR voldoet aan de HTTPS- en HSTS-standaarden.
IPv4 en IPv6	Ja	NHR voldoet aan de IPv6 en IPv4 standaarden.
NEN-ISO/IEC27001 en NEN-ISO/IEC27002	Ja	KVK is sinds 2016 gecertificeerd en verlengd, en de risicoanalyse en maatregelen zijn geactualiseerd.
NL GOV Assurance profile for OAuth 2.0	Ja	NHR voldoet volgens de beheerder aan de NL GOV Assurance profile for OAuth 2.0 standaard.
RPKI	Ja	NHR is RPKI-compliant.

Authenticatie-standaarden (OpenID.NLGov en SAML)	Ja	eHerkenning is SAML-based en wordt toegepast voor het aanleveren van jaarrekeningen en informatieverstrekking. In de notarisapplicatie kan de notaris van achter zijn computer rechtstreeks opgave doen. Ook hier wordt gebruik gemaakt van SAML als authenticatieprocedure. Omdat gebruik wordt gemaakt van een generiek identificatie- en authenticatiesysteem voor alle diensten van KvK kan SAML voor elke dienst ingezet worden voor authenticatie.
security.txt	Ja	NHR voldoet aan de security.txt standaard.
SPF	Ja	NHR is SPF-compliant.
STARTTLS en DANE	Gepland	KVK: Dit heeft dezelfde oorzaak als hiervoor bij DNSSEC genoemd, zie ook de update van Microsoft daar genoemd.
TLS	Ja	NHR ondersteunt TLS.
		Uitwisselingsfundament
Digikoppeling	Ja	Digikoppeling wordt door KVK actief gebruikt voor de HR Dataservice.
OpenAPI Specification	Ja	De OpenAPI Specification wordt door KVK gebruikt bij het (door)ontwikkelen van API's ten behoeve van ontsluiten van HR-informatie.
REST-API Design Rules	Ja	KVK hanteert de REST-API Design rules al geruime tijd, inmiddels zijn ook "oudere" API's in het kader van doorontwikkeling aangepast aan deze regels.
StUF	Ja	StUF wordt gebruikt in de HR Dataservice met Digikoppeling.
		Bestuur en recht
BWB	Gepland	Ja, in geval van wat binnen de KVK de Data-atlas heet, hierin zitten verwijzingen naar wet- en regelgeving, dit wordt in 2025 opgepakt.
		Economie en werk
NLCIUS	Ja	Elektronisch factureren conform de NLCIUS standaard is eind 2022 beschikbaar gemaakt.
		Openbaar en toegankelijk
Ades Baseline Profiles	Ja	NHR voldoet volgens de beheerder aan de Ades Baseline Profiles standaard.
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status B	De website van KVK heeft een toegankelijkheidsverklaring. De status is conform het Toegankelijkheidsregister, status B. Er wordt voldaan aan 36 van de 50 succescriteria. Er wordt met name gewerkt aan het beter toegankelijk krijgen van pdf's via de site. Dit is tevens een vereiste in het kader van Actieve Openbaarmaking. Een nieuwe versie van de Toegankelijkheidsverklaring is in de maak.
PDF (NEN-ISO)	Ja	Voor de duurzaam toegankelijke documenten hanteert KVK de PDF/A-2 norm.
SKOS	Gepland	KVK is bezig met een zogenaamde Data-atlas voor zowel intern als extern gebruik. Dit vervangt de Gegevenscatalogus voor afnemers en is op SKOS en DCAT v2 gebaseerd.

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:

- Authenticatie-standaarden (OpenID.NLGov en SAML)
- Security.txt
- BWB

Verbeteringen; de voorziening voldoet nu (deels) wel aan:

- NL GOV Assurance profile for OAuth 2.0

- RPKI
- STARTTLS en DANE
- Digitoegankelijk (EN 301 549 met WCAG 2.1)
- OpenAPI Specification
- NLCIUS

Verslechteringen; de voorziening voldoet nu (deels) niet meer aan:

- DNSSEC

Concluderend moeten voor NHR de volgende standaarden (volledig) geïmplementeerd worden: DNSSEC, STARTTLS en DANE, BWB, Digitoegankelijk (EN 301 549 met WCAG 2.1) en SKOS.

4.8 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 geo-data voor hergebruik beschikbaar wil stellen, kan zich tot PDOK wenden. Het dataportaal PDOK wordt gehost door het Kadaster.

Geteste web- en maildomeinen:

- pdok.nl
  - Bron: https://internet.nl/site/pdok.nl/2742556/
- www.pdok.nl
  - Bron: https://internet.nl/site/www.pdok.nl/2815680/
- @pdok.nl
  - Bron: https://internet.nl/mail/pdok.nl/1217196/

Standaard	Status	Toelichting beheerder
		Veilig internet
DKIM	Ja	PDOK is DKIM-compliant.
DMARC	Ja	PDOK is DMARC-compliant.
DNSSEC	Ja	PDOK is DNSSEC-compliant.
HTTPS en HSTS	Deels	HSTS lijkt wel aan te staan in de configuratie van de beheerder, maar uit de test lijkt dit uit te staan. De beheerder gaat dit intern uitzoeken.
IPv4 en IPv6	Ja	PDOK voldoet aan de IPv6- en IPv4-standaarden.
NEN-ISO/IEC27001 en NEN-ISO/IEC27002	Nee	Uit een interne audit is gebleken dat PDOK niet voldoet aan de NEN-ISO/IEC27001 en NEN-ISO/IEC27002. Hier wordt aan gewerkt vanuit het Kadaster.
RPKI	Ja	PDOK is RPKI-compliant.
security.txt	Ja	PDOK voldoet aan de security.txt standaard.
SPF	Ja	PDOK is SPF-compliant.
STARTTLS en DANE	Ja	Het ontbreken van actieve DANE-schema's en TLSA-records wordt intern uitgezocht door de beheerder.
TLS	Ja	Het feit dat mailservers client-initiated-renegotiation toestaan wordt intern uitgezocht door de beheerder.
		Uitwisselingsfundament
Geo-standaarden	Ja	PDOK voldoet aan de relevante geo-standaarden.
OpenAPI Specification	Ja	Zowel de OGC API's als overige restAPI's voldoen aan de OpenAPI Specification. Voorbeelden:

		- https://api.pdok.nl/lv/bgt/ogc/v1_0/api - https://api.pdok.nl/bzk/locatieserver/search/v3_1/ui/.
REST-API Design Rules	Deels	De vernieuwde OGC-API's voldoen op één paar kleine issues aan deze regels: https://api.pdok.nl/lv/bgt/ogc/v1_0 Eén issue wordt binnenkort opgelost (versie 1_0 wordt v1). Ander issue wordt teruggekoppeld (i.v.m. twijfels over de regel). PDOK wil in de toekomst zo veel mogelijk datasets via de OGC API's beschikbaar gaan stellen.
StUF	Ja	De BGT-dataset is via StUF beschikbaar: https://api.pdok.nl/lv/bgt/download/v1_0/ui/
		Openbaar en toegankelijk
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status D	PDOK heeft een toegankelijkheidsverklaring en voldoet daarmee aan de Digitoegankelijk standaard. Zie: https://www.pdok.nl/toegankelijkheid
PDF (NEN-ISO)	Gepland	Deze standaard is onder de aandacht. Een aantal PDF's worden momenteel omgezet naar WCAG-compliant HTML's.

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:
- Security.txt
- PDF (NEN-ISO)

Verbeteringen; de voorziening voldoet nu (deels) wel aan:
- HTTPS en HSTS
- REST-API Design Rules

Verslechteringen; de voorziening voldoet nu (deels) niet meer aan:
- NEN-ISO/IEC27001 en NEN-ISO/IEC27002
- Digitoegankelijk (EN 301 549 met WCAG 2.1)

Concluderend moeten voor PDOK de volgende standaarden (volledig) geïmplementeerd worden: HTTPS en HSTS, NEN-ISO/IEC27001 en NEN-ISO/IEC27002, REST-API Design Rules, Digitoegankelijk (EN 301 549 met WCAG 2.1) en PDF (NEN-ISO).

4.9 Stelselcatalogus

Beheerorganisatie: Logius

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

Geteste web- en maildomeinen:
- www.stelselcatalogus.nl
  - Bron: https://internet.nl/site/stelselcatalogus.nl/2796720/
  - Bron: https://internet.nl/site/www.stelselcatalogus.nl/2796721/
- @stelselcatalogus.nl
  - Bron: https://internet.nl/mail/stelselcatalogus.nl/1246287/

Standaard	Status	Toelichting beheerder
		Veilig internet
DMARC	Ja	
DNSSEC	Ja	

HTTPS en HSTS	Ja	Het aanbieden van een Content-Security-Policy (CSP) staat voor 2024 op de planning.
IPv4 en IPv6	Ja	
RPKI	Ja	
security.txt	Gepland	Oplossing voor dit is 'in progress'. Redirects naar het security.txt bestand (van NCSC) zijn nu opgenomen in de proxy. De productie proxy's worden bijgewerkt.
SPF	Ja	
TLS	Ja	
		Uitwisselingsfundament
REST-API Design Rules	Ja	De Stelselcatalogus voldoet aan de RESTAPI design rules. Hier staat hij conform deze standaard beschreven: https://stelselcatalogus.nl/api/v2
		Openbaar en toegankelijk
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status D	Uit het laatste onderzoek (08-apr-2022) is gebleken dat de website helaas nog niet volledig voldoet aan alle succescriteria. Op dat moment voldoet de website aan 36 van de 50 succescriteria. Deze PI wordt er een proces opgesteld om deze hertoetsing op tijd te doen en de bevindingen te bewerken.
PDF (NEN-ISO)	Ja	www.stelselcatalogus.nl biedt 1 PDF aan: de stelselplaat gegevens 2020. Dit is een PDF1.7 geannoteerde PDF, die in 2021 door een gespecialiseerd bureau is aangeleverd. Voor zover dit gecontroleerd kan worden, voldoet dit bestand aan de Digitoegankelijk. De foutmeldingen van de tooling op het forum lijken niet van toepassing aangezien dit document geen doorlopende tekst bevat. Alle beschikbare labels zijn leesbaar.
SKOS	Ja	Onderdelen van registratie worden in begrippen dan wel in gegevenselementen uitgedrukt. Begrippen zijn met behulp de SKOS-standaard gedefinieerd.

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:

- Security.txt
- SPF
- TLS

Niet langer van toepassing zijnde standaarden voor deze voorziening:

- BWB

Verbeteringen; de voorziening voldoet nu (deels) wel aan:

- IPv4 en IPv6

Verslechteringen; de voorziening voldoet nu (deels) niet meer aan:

- Digitoegankelijk (EN 301 549 met WCAG 2.1)

Concluderend moeten voor Stelselcatalogus de volgende standaarden (volledig) geïmplementeerd worden: security.txt en Digitoegankelijk (EN 301 549 met WCAG 2.1).

5. Dienstverlening en verbinden

5.1 Diginetwerk

Beheerorganisatie: Logius

Werking en inhoud van Diginetwerk:
Diginetwerk is een afsprakenstelsel en bestaat uit een beschreven samenwerking, normenkaders, handhavingsmechanismen, toetredingseisen en een set van standaarden. Diginetwerk is opgebouwd uit een aantal aan elkaar gekoppelde besloten *(overheids)netwerken, waarover overheidsorganisaties en organisaties met een publieke taak gegevens veiliger (vertrouwelijkheid en beschikbaarheid) met elkaar* kunnen uitwisselen dan via het internet. Een belangrijk onderdeel van Diginetwerk is de Koppelnet Publieke Sector (KPS) voorziening, die de fysieke koppeling tussen de diverse (overheids)netwerken faciliteert.

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

Standaard	Status	Toelichting beheerder
		Veilig internet
DNSSEC	Ja	De RijksDNS ondersteunt DNSSEC. De (Rijks)overheid organisaties die gebruikmaken van Diginetwerk zijn zelf verantwoordelijk voor de inrichting en gebruik van DNSSEC.
IPv4 en IPv6	Ja	Diginetwerk (infrastructuur) is compliant en biedt actief IPv6 aan, maar het gebruik van IPv6 wordt niet afgedwongen, dit ligt bij de aangesloten (Rijks)overheid organisaties zelf.
NEN-ISO/IEC27001 en NEN-ISO/IEC27002	Ja	BIO compliance of ISO27001/02 certificering is contractueel onderdeel van de samenwerkingsovereenkomsten met de leveranciers van Diginetwerkaansluitingen. De (Rijks)overheid organisaties die gebruikmaken van Diginetwerk zijn zelf verantwoordelijk voor BIO-compliance.

Veranderingen ten opzichte van de vorige meting:
Verbeteringen; de voorziening voldoet nu (deels) wel aan:
- IPv4 en IPv6

Concluderend zijn alle standaarden volledig geïmplementeerd voor Diginetwerk.

5.2 DigiPoort

Beheerorganisatie: Logius

Werking en inhoud van DigiPoort:
DigiPoort is een ICT-centrale waar berichtenverkeer voor de overheid afgehandeld wordt. Overheden kunnen DigiPoort inzetten om bedrijfs- en ketenprocessen te automatiseren. Omdat DigiPoort slechts machine-naar-machine-koppelingen levert en niet toegankelijk is vanaf het openbare internet, is gekozen voor de website aansluiten.procesinfrastructuur.nl, wat de voornaamste publieke website is van DigiPoort, voor onderstaande verantwoording.

Geteste web- en maildomeinen:
- aansluiten.procesinfrastructuur.nl
    - Bron: https://internet.nl/site/aansluiten.procesinfrastructuur.nl/2785266/

Standaard	Status	Toelichting beheerder
		Veilig internet
DMARC	Ja	DigiPoort is DMARC-compliant, zie bron.
DNSSEC	Ja	DigiPoort is DNSSEC-compliant, zie bron.
HTTPS en HSTS	Ja	DigiPoort voldoet aan de HTTPS en HSTS-standaarden, zie bron.
IPv4 en IPv6	Ja	DigiPoort voldoet aan de IPv6 en IPv4 standaarden, zie bron.
NEN-ISO/IEC27001 en NEN-ISO/IEC27002	Ja	DigiPoort voldoet aan de BIO.
RPKI	Ja	DigiPoort is RPKI-compliant, zie bron.
security.txt	Ja	DigiPoort voldoet aan de security.txt standaard, zie bron.
SPF	Ja	DigiPoort is SPF-compliant, zie bron.
TLS	Ja	DigiPoort ondersteunt TLS, zie bron.

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:
- Security.txt

Niet langer van toepassing zijnde standaarden voor deze voorziening:
- Digikoppeling
- SETU
- XBLR

Verbeteringen; de voorziening voldoet nu (deels) wel aan:
- IPv4 en IPv6

Concluderend zijn alle standaarden volledig geïmplementeerd voor DigiPoort.

5.3 Digitale Werkomgeving Rijk (DWR)

Beheerorganisatie: Ministerie van Binnenlandse Zaken en Overheidsrelaties

Werking en inhoud van DWR
De Digitale Werkomgeving Rijksdienst (DWR) is de ICT-werkomgeving voor rijksambtenaren. Deze werkomgeving is een onderdeel van de dienstverlening van het Shared Service Center-ICT (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 belangrijkste zijn voorzieningen voor kantoorautomatisering (bijvoorbeeld tekstverwerking), mail, veilige toegang tot internet (browsers) en opslag van ongestructureerde data. Verder biedt de digitale werkomgeving voorzieningen om beter en sneller samen te werken.

Standaard	Status	Toelichting beheerder
		Veilig internet
DKIM	Ja	DKIM is onderdeel van de maildomeinen die SSC-ICT faciliteert voor de klanten. Alle klanten zijn eigenaar van de maildomeinen en daarmee eindverantwoordelijk.
DMARC	Ja	DMARC is onderdeel van de maildomeinen die SSC-ICT faciliteert voor de klanten. Alle klanten zijn eigenaar van de maildomeinen en daarmee eindverantwoordelijk.
DNSSEC	Deels	DNSSEC is geïmplementeerd en alle domeinnamen die bij SSC-ICT in het ODC gehost worden voldoen aan DNSSEC. DNSSEC is echter nog niet beschikbaar bij al de cloudleveranciers; hier kan DNSSEC dus

		nog niet geïmplementeerd worden.
HTTPS en HSTS	Ja	De browsers van de DWR-client ondersteunen dit protocol. Overigens, maar geen onderdeel van DWR, is HTTPS/HSTS geïmplementeerd voor ongeveer 99%, resp. 90% van de websites die SSC-ICT host voor klanten.
IPv4 en IPv6	Ja	IPv4 is generiek in gebruik. IPv6 is voor de internet facing web, name en mailservices geïmplementeerd conform de Pas-toe-of-leg-uit-standaard. De gebruikte technische componenten van de DWR-client ondersteunen IPv6 en dual stack en zullen na afronding van het lopende onderzoek van het Forum Standaardisatie over het aanpassen van het functioneel toepassingsgebied van de standaard ook cf. de aangepaste standaard ingepland worden om van IPv6/dual stack gebruik te gaan maken.
NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002	Ja	SSC-ICT werkt via deze standaard en wordt hier ook op geaudit.
NL GOV Assurance profile for OAuth 2.0	Ja	DWR ondersteunt dit protocol.
RPKI	Ja	RPKI is ingeregeld voor DWR.
Authenticatie Standaarden (OpenID.NLGov en SAML)	Ja	DWR ondersteunt dit protocol.
SPF	Ja	Is onderdeel van de maildomeinen die SSC-ICT faciliteert voor de klanten. Alle klanten zijn eigenaar van de maildomeinen en daarmee eindverantwoordelijk.
STARTTLS en DANE	Ja	Is onderdeel van de maildomeinen die SSC-ICT faciliteert voor de klanten. Alle klanten zijn eigenaar van de maildomeinen en daarmee eindverantwoordelijk.
TLS	Ja	De gebruikte technische componenten van de DWR-client ondersteunen dit protocol t/m v1.3. Wordt standaard toegepast door SSC-ICT voor de domeinen die SSC-ICT host voor de klanten.
WPA2 Enterprise	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). WPA2- Enterprise is in 2021 ook aangezet op de gastnetwerken.
		Uitwisselingsfundament
Digikoppeling	Ja	Binnen JenV vindt elektronisch berichtenverkeer interdepartementaal plaats via de Justitie Berichten Service (JUBES). JUBES is vanuit JenV het koppelvlak voor de Digikoppelingdienst van Logius. De open standaarden eBMS en WUS zijn de daarbij gebruikte protocollen om de berichten veilig te versturen. Binnen BZ wordt deze standaard gebruikt voor de Mule koppeling. Verder nemen alle departementen uit het verzorgingsgebied van SSC-ICT deel aan eFacturatie. Op deze standaard wordt waar van toepassing aangesloten bij nieuwe koppelingen.
		Openbaar en toegankelijk
ODF	Ja	De DWR Next client wordt geleverd met zowel Libreoffice als Office365. Beide softwaresuites ondersteunen het lezen en schrijven van ODF-bestanden.

PDF (NEN-ISO)	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.

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:

- Authenticatie Standaarden (OpenID.NLGov en SAML)

Verbeteringen; de voorziening voldoet nu (deels) wel aan:

- DMARC
- HTTPS en HSTS
- IPv4 en IPv6
- NL GOV Assurance profile for OAuth 2.0
- RPKI

Concluderend moet voor DWR de volgende standaard (volledig) geïmplementeerd worden: DNSSEC.

5.4 TenderNed

Beheerorganisatie: RVO/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.

Geteste web- en maildomeinen:

- Tenderned.nl
  - Bron: https://internet.nl/site/tenderned.nl/2797986/#
  - Bron: https://internet.nl/site/www.tenderned.nl/2797988/#
- @tenderned.nl
  - Bron: https://internet.nl/mail/tenderned.nl/1246965/

Standaard	Status	Toelichting beheerder
		Veilig internet
DKIM	Ja	
DMARC	Ja	
DNSSEC	Ja	
HTTPS en HSTS	Ja	
IPv4 en IPv6	Ja	
NEN-ISO/IEC27001en NEN-ISO/IEC27002	Ja	TenderNed is ISO27001/2 gecertificeerd. Dit wordt jaarlijks geaudit.
RPKI	Ja	
Authenticatie-standaarden (OpenID.NLGov en SAML)	Ja	TenderNed voldoet aan OpenID.NLGov wat samen met SAML valt onder de ‘Authenticatie Standaarden’: https://www.forumstandaardisatie.nl/open-standaarden/authenticatie-standaarden
security.txt	Ja	
SPF	Ja	

STARTTLS en DANE	Ja	
TLS	Ja	
		Uitwisselingsfundament
OpenAPI Specification	Ja	De publieke API's worden beschreven door middel van OAS3.0.
REST-API Design Rules	Ja	De REST-API's die worden gebruikt, voldoen aan de design rules.
		Openbaar en toegankelijk
Digitoegankelijk (EN 301 549 met WCAG 2.1)	Status B	
PDF (NEN-ISO)	Nee	De automatisch gegenereerde PDF's (bij de aankondigingen) hebben versie 1.4. We zijn bezig met de tooling voor PDF generatie te upgraden.

Veranderingen ten opzichte van de vorige meting:
Nieuwe geteste standaarden voor deze voorziening:
- Authenticatie-standaarden (OpenID.NLGov en SAML)
- Security.txt

Verbeteringen; de voorziening voldoet nu (deels) wel aan:
- OpenAPI Specification
- REST-API Design Rules

Verslechteringen; de voorziening voldoet nu (deels) niet meer aan:
- PDF (NEN-ISO)

Concluderend moeten voor TenderNed de volgende standaarden (volledig) geïmplementeerd worden: Digitoegankelijk (EN 301 549 met WCAG 2.1) en PDF (NEN-ISO).

Bijlage A Voorzieningen en contactpersonen

Naam voorziening	Contactpersoon
BAG / BRK / BGT / WOZ / BRT	Koen Huisstede
Berichtenbox voor bedrijven	Ferdi Bouwman
BRI	Luc Boss
BRO	Jasper Snippe
BRV	Walter Huberts
BSN en GBA-V	Hans van Laar
DigiD	Evert-Jan van der Marck
DigiD Machtigen	Evert-Jan van der Marck
Digilevering	Perry Meezen
Digimelding	Perry Meezen
Diginetwerk	Arjen de Lange
DigiPoort	Jeroen Lambregts
Doc-Direkt	Olaf Holtrop
DWR	Rein Hennen
ETD	Stijn Horsten
MijnOverheid	Marcel Hoogteijling
NHR	Rob Spoelstra
Ondernemersplein	Rogier Smith
Overheid.nl	Mathijs Kleijnen
PDOK	Jeroen Hogeboom
PKIoverheid	Jochem van den Berge
Rijksoverheid.nl (webdomein)	Gerrit Berkouwer
Rijksportaal	Alain Boonzaier
Samenwerkende Catalogi	Kristian Mul
Stelselcatalogus	Kees-Jan Westmaas
Tenderned	Rudi van Eijk
WOZ-Waardeloket	Rijk van Haaften

Bijlage B Lijst verplichte open standaarden

Standaard
Ades Baseline Profiles
Aquo-standaard
Authenticatie-standaarden (OpenID.NLGov en SAML)
BWB
Digikoppeling
Digitoegankelijk (EN 301 549 met WCAG 2.1)
DKIM
DMARC
DNSSEC
E-Portfolio NL*
ECLI*
EML_NL*
Geo-Standaarden
GWSW
HTTPS en HSTS
IFC*
IPv4 en IPv6
JCDR
NEN-ISO/IEC 27001
NEN-ISO/IEC 27002
NL GOV Assurance profile for OAuth 2.0
NL LOM*
NLCIUS
NLCS*
ODF
OpenAPI Specification
PDF (NEN-ISO)
REST-API Design Rules
RPKI
security.txt
SETU
SIKB0101
SIKB0102
SKOS
SPF
STARTTLS en DANE
STIX en TAXII
StUF
TLS
VISI*
WDO Datamodel*
WPA2 Enterprise
XBRL

Toelichting PBLQ: Standaarden die niet uitgevraagd zijn, maar wel op de pas-toe-of-leg-uit lijst staan zijn gemarkeerd met een sterretje (*).