



Bijlage Invulformulier Relevante open standaarden Geïntegreerd Financieel en Inkoop Systeem

INVULFORMULIER LEVERANCIER

Vraag	Relevantie Provincie Zeeland	Oplossing voldoet hieraan (J/N)	Opmerkingen
De oplossing kan voldoen aan hieronder genoemde open standaarden .	Hoog	J/N	

De lijst met open standaarden is samengesteld via de [Beslisboom Forum Standaardisatie voor de 'pas toe of leg uit'-lijst](#).

De volgende standaarden zijn vermoedelijk relevant:

Digikoppeling

Digikoppeling realiseert geautomatiseerde, veilige gegevensuitwisseling tussen informatiesystemen voor sectoroverstijgende gegevensuitwisseling, op basis van vier koppelvakstandaarden (DK ebMS standaard voor meldingen tussen informatiesystemen, DK WUS standaard voor de bevraging van informatiesystemen, DK GB standaard voor de uitwisseling van grote berichten, of REST API om gegevens veilig uit te wisselen volgens het [REST principe](#)).

<https://www.forumstandaardisatie.nl/open-standaarden/digikoppeling>

Digitoegankelijk (EN 301 549 met WCAG 2.1)

Door toepassing van Digitoegankelijk worden websites, webapplicaties en documenten voor iedereen toegankelijk, ook voor mensen met permanente, tijdelijke of situationele functiebeperkingen. Zo krijgt iedereen dezelfde toegang tot overheidsinformatie.

Let op: per 1 juli 2018 zijn overheidsorganisaties wettelijk verplicht om Digitoegankelijk (EN 301 549 en WCAG 2.1) te gebruiken voor de toegankelijkheid van websites en mobiele applicaties. Kijk voor [meer informatie](#).

<https://www.forumstandaardisatie.nl/open-standaarden/digitoegankelijk-en-301-549-met-wcag-21>

DKIM

DKIM faciliteert van het vaststellen van organisatorische herkomst voor e-mail afkomstig van overheidsdomeinen, als deze over een onbeveiligde, publieke internetverbinding wordt verstuurd wanneer verdere authenticatie ontbreekt.

<https://www.forumstandaardisatie.nl/open-standaarden/dkim>

DMARC

DMARC is een standaard die het voor organisaties mogelijk maakt om te bepalen hoe e-mailproviders, die DMARC ondersteunen, omgaan met e-mail waarvan niet kan worden vastgesteld dat deze afkomstig is van het eigen domein. Hierdoor kunnen organisaties voorkomen dat anderen e-mails versturen namens het e-maildomein van de organisatie.

<https://www.forumstandaardisatie.nl/open-standaarden/dmarc>

DNSSEC

DNSSEC zorgt voor de beveiliging van DNS door aan het DNS-record een digitale handtekening toe te voegen en deze bij uitwisseling te verifiëren.

<https://www.forumstandaardisatie.nl/open-standaarden/dnssec>

HTTPS en HSTS

HTTPS en HSTS zorgen samen voor beveiligde verbindingen met websites, met als doel de veilige uitwisseling van gegevens tussen een webserver en client (vaak een webbrowswer).

Let op: per 1 juli 2023 zijn overheidsorganisaties wettelijk verplicht om HTTPS en HSTS te gebruiken voor beveiligen van publiek toegankelijke websites en webapplicaties. Kijk voor [meer informatie](#).

<https://www.forumstandaardisatie.nl/open-standaarden/https-en-hsts>

IPv6 en IPv4

IPv6 en IPv4 standaardiseren communicatie op netwerkniveau over organisatiegrenzen heen tussen organisaties, individuele eindgebruikers, apparaten, diensten en sensoren.

<https://www.forumstandaardisatie.nl/open-standaarden/ipv6-en-ipv4>

NEN-ISO/IEC 27001

NEN-ISO/IEC 27001 specificeert de eisen voor het vaststellen, implementeren, uitvoeren, controleren, beoordelen, bijhouden en verbeteren van een gedocumenteerd Information Security Management System (ISMS) in het kader van de algemene bedrijfsrisico's voor de organisatie.

<https://www.forumstandaardisatie.nl/open-standaarden/nen-isoiec-27001>

NEN-ISO/IEC 27002

NEN-ISO/IEC 27002 omvat "best practices" op het gebied van het organiseren van informatiebeveiliging voor een organisatie, bestaande uit het beheer van bedrijfsmiddelen, veilig personeel, toegangsbeveiliging, cryptografie, fysieke beveiliging en beveiliging van de omgeving, beveiliging in de bedrijfsvoering, communicatiebeveiliging, leveranciersrelaties, beheer van informatiebeveiligingsincidenten, informatiebeveiligingsaspecten van bedrijfscontinuïteitsbeheer, naleving en de acquisitie, ontwikkeling en het onderhoud van informatiesystemen.

ICO Wizard

<https://www.forumstandaardisatie.nl/open-standaarden/nen-isoiec-27002>

NL GOV Assurance profile for OAuth 2.0

NL GOV Assurance profile for OAuth 2.0 zorgt ervoor dat de autorisatie van gebruikers van REST APIs van de overheid op een uniforme en eenduidige plaats vindt.

<https://www.forumstandaardisatie.nl/open-standaarden/nl-gov-assurance-profile-oauth-20>

NLCIUS

NLCIUS beschrijft welke gegevenselementen er opgenomen dienen te worden op een elektronische factuur naar overheidsorganisaties in Nederland.

<https://www.forumstandaardisatie.nl/open-standaarden/nlcius>

ODF

<https://www.forumstandaardisatie.nl/open-standaarden/odf>

OpenAPI Specification

Een OpenAPI Specification (OAS) beschrijft de eigenschappen van de data die een API als input accepteert en als output teruggeeft. Met OAS 3.0 kunnen zowel mensen als machines de dataset attributen van een REST API vinden, bekijken en verwerken zonder toegang tot de programmatuur en zonder aanvullende documentatie.

<https://www.forumstandaardisatie.nl/open-standaarden/openapi-specification>

PDF (NEN-ISO)

<https://www.forumstandaardisatie.nl/open-standaarden/pdf-nen-iso>

REST-API Design Rules

De standaard REST-API Design Rules geeft een verzameling basisregels voor structuur en naamgeving waarmee de overheid op een uniforme en eenduidige manier REST-API's aanbiedt ten behoeve van het ontsluiten van overheidsinformatie en/of functionaliteit.

<https://www.forumstandaardisatie.nl/open-standaarden/rest-api-design-rules>

RPKI

Met Resource Public Key Infrastructure (RPKI) kan de rechtmatige houder van een blok IP-adressen een autoritatieve, digitaal getekende verklaring publiceren met betrekking tot de intenties van de routing vanaf haar netwerk. Deze verklaringen kunnen andere netwerkbeheerders cryptografisch valideren en vervolgens gebruiken om filters in te stellen die onrechtmatige routing negeren.

<https://www.forumstandaardisatie.nl/open-standaarden/rpki>

security.txt

security.txt moet worden toegepast op alle systemen die via HTTPS publiek benaderbaar zijn, zodat securitycontactinformatie duidelijk is.

<https://www.forumstandaardisatie.nl/open-standaarden/securitytxt>

SETU

De SETU-standaard is de elektronische berichtenuitwisseling rondom de bemiddeling/inhuur van flexibele arbeidskrachten.

<https://www.forumstandaardisatie.nl/open-standaarden/setu>

SPF

Met SPF kan worden gecontroleerd of een e-mailserver gerechtigd is om namens een domeinnaam e-mail te mogen verzenden.

<https://www.forumstandaardisatie.nl/open-standaarden/spf>

STARTTLS en DANE

STARTTLS in combinatie met DANE gaan af luisteren of manipuleren van mailverkeer door internetcriminelen tegen.

<https://www.forumstandaardisatie.nl/open-standaarden/starttls-en-dane>

StUF

StUF regelt uitwisseling en bevraging van basisgegevens die behoren tot een aantal wettelijk vastgestelde basisregistraties, zoals Personen (GBA), Adressen (BRA), Gebouwen (BGA), Kadaster (BRK), Nieuw Handelsregister (NHR) en Waarde Onroerende Zaken (WOZ); uitwisseling en bevraging van zaakgegevens die behoren tot het producten- en dienstenportfolio van gemeenten; uitwisseling van domein- of sectorspecifieke gegevens waarin ook basis- en/of zaakgegevens voorkomen en waarvoor geen andere (inter)nationale (XML-gebaseerde) berichtenstandaard is vastgesteld.

<https://www.forumstandaardisatie.nl/open-standaarden/stuf>

TLS

TLS beveiligt met behulp van certificaten de verbinding (op de transportlaag) tussen client- en serversystemen of tussen serversystemen onderling, voor zover deze gerealiseerd wordt met internettechnologie.

<https://www.forumstandaardisatie.nl/open-standaarden/tls>

XBRL

XBRL moet worden toegepast om (financiële)rapportage gegevens uit te wisselen via het internet. Doordat XBRL-bestanden direct leesbaar zijn voor softwareapplicaties, betekent dit een enorme kostenbesparing op het vlak van verzamelen en verwerken van bedrijfsinformatie.

<https://www.forumstandaardisatie.nl/open-standaarden/xbrl>