



gemeenschappelijke regeling
DE BEVELANDEN

Bijlage 2B
Standaarden Forum Standaardisatie voor
Financieel pakket
Kenmerk: siw008440- Z20.049547

1.	<u>VERPLICHTE STANDAARDEN</u>	3
1.1	<u>ADES BASELINE PROFILES</u>	3
1.2	<u>CMIS</u>	3
1.3	<u>DKIM</u>	3
1.4	<u>DMARC</u>	3
1.5	<u>DNSSEC</u>	3
1.6	<u>HTTPS EN HSTS</u>	4
1.7	<u>IPv6 EN IPv4</u>	4
1.8	<u>NEN-ISO/IEC 27001 & 27002</u>	4
1.9	<u>NL GOV ASSURANCE PROFILE FOR OAUTH 2.0</u>	4
1.10	<u>NLCIUS</u>	4
1.11	<u>ODF</u>	4
1.12	<u>OPENAPI SPECIFICATION</u>	5
1.13	<u>PDF (NEN-ISO)</u>	5
1.14	<u>REST-API DESIGN RULES</u>	5
1.15	<u>RPKI</u>	5
1.16	<u>SAML</u>	5
1.17	<u>SPF</u>	5
1.18	<u>STARTTLS EN DANE</u>	6
1.19	<u>StUF</u>	6
1.20	<u>TLS</u>	6
1.21	<u>XBRL</u>	6
2.	<u>TOTSTANDKOMING STANDAARDEN</u>	8

1. Verplichte standaarden

Onderstaande standaarden worden door Forum standaardisatie aangemerkt als verplicht indien de standaard ook relevant is voor het Financieel pakket. Een en ander hangt af van de type oplossing. In kwaliteitscriterium 1 kunt u aangeven aan welke eisen u voldoet. Indien u niet aan de standaard voldoet moet u aangeven waarom deze niet relevant is.

De volgende standaarden kunnen van toepassing kunnen zijn:

1.1 Ades Baseline Profiles

De Advanced Electronic Signature (AdES) standaard voorziet in het digitaal tekenen van documenten met een geavanceerde of gekwalificeerde digitale handtekening.

<https://www.forumstandaardisatie.nl/standaard/ades-baseline-profiles> [1]

1.2 CMIS

CMIS maakt ongestructureerde gegevens in content repositories van Content Management Systemen (CMS'en) en Document Management Systemen (DMS'en) toegankelijk met als doel deze gegevens uit te wisselen met andere CMS en DMS systemen.

<https://forumstandaardisatie.nl/standaard/cmisis> [2]

1.3 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://forumstandaardisatie.nl/standaard/dkim> [3]

1.4 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://forumstandaardisatie.nl/standaard/dmarc> [4]

1.5 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://forumstandaardisatie.nl/standaard/dnssec> [5]

1.6 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 webbrowser).

<https://www.forumstandaardisatie.nl/standaard/https-en-hsts> [6]

1.7 IPv6 en IPv4

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

<https://forumstandaardisatie.nl/standaard/ipv6-en-ipv4> [7]

1.8 NEN-ISO/IEC 27001 & 27002

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. 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.

<https://www.forumstandaardisatie.nl/standaard/nen-isoiec-27001> [8]

1.9 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>

[9]

1.10 NLCIUS

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

<https://www.forumstandaardisatie.nl/standaard/nlcious> [10]

1.11 ODF

ODF is een standaard voor uitwisseling van reviseerbare documenten. ODF bestanden hebben een structuur waardoor ze gemakkelijk te exporteren zijn naar PDF documenten die voldoen aan duurzaamheids- en toegankelijkheidsrichtlijnen. Dankzij deze structuur kunnen zoekmachines ODF bestanden goed indexeren en vinden.

<https://forumstandaardisatie.nl/standaard/odf> [11]

1.12 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/standaard/openapi-specification> [12]

1.13 PDF (NEN-ISO)

PDF is een formaat voor de uitwisseling van documenten waarvan de pagina opmaak vastligt. Het uitgangspunt van PDF is dat gebruikers documenten kunnen uitwisselen, bekijken en afdrukken, onafhankelijk van de omgeving waarin ze worden aangemaakt, bekeken of afgedrukt.

<https://www.forumstandaardisatie.nl/standaard/pdf-nen-iso> [13]

1.14 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>
[14]

1.15 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/standaard/rpki> [15]

1.16 SAML

SAML standaardiseert federatieve (web)browser-gebaseerde single-sign-on (SSO). Dat wil zeggen dat een gebruiker na eenmalig inloggen via zijn browser toegang krijgt tot verschillende diensten van verschillende partijen.

<https://forumstandaardisatie.nl/standaard/saml> [16]

1.17 SPF

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

<https://forumstandaardisatie.nl/standaard/spf> [17]

1.18 STARTTLS en DANE

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

<https://www.forumstandaardisatie.nl/standaard/starttls-en-dane> [18]

1.19 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://forumstandaardisatie.nl/standaard/stuf> [19]

1.20 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://forumstandaardisatie.nl/standaard/tls> [20]

1.21 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://forumstandaardisatie.nl/standaard/xbrl-en-dimensions> [21]

- [1] <https://www.forumstandaardisatie.nl/standaard/ades-baseline-profiles>
- [2] <https://forumstandaardisatie.nl/standaard/cmisis>
- [3] <https://forumstandaardisatie.nl/standaard/dkim>
- [4] <https://forumstandaardisatie.nl/standaard/dmarc>
- [5] <https://forumstandaardisatie.nl/standaard/dnssec>
- [6] <https://www.forumstandaardisatie.nl/standaard/https-en-hsts>
- [7] <https://forumstandaardisatie.nl/standaard/ipv6-en-ipv4>
- [8] <https://www.forumstandaardisatie.nl/standaard/nen-isoiec-27001>
- [9] <https://www.forumstandaardisatie.nl/open-standaarden/nl-gov-assurance-profile-oauth-20>
- [10] <https://www.forumstandaardisatie.nl/standaard/nlcuis>
- [11] <https://forumstandaardisatie.nl/standaard/odf>
- [12] <https://www.forumstandaardisatie.nl/standaard/openapi-specification>
- [13] <https://www.forumstandaardisatie.nl/standaard/pdf-nen-iso>
- [14] <https://www.forumstandaardisatie.nl/open-standaarden/rest-api-design-rules>
- [15] <https://www.forumstandaardisatie.nl/standaard/rpki>
- [16] <https://forumstandaardisatie.nl/standaard/saml>
- [17] <https://forumstandaardisatie.nl/standaard/spf>
- [18] <https://www.forumstandaardisatie.nl/standaard/starttls-en-dane>
- [19] <https://forumstandaardisatie.nl/standaard/stuf>
- [20] <https://forumstandaardisatie.nl/standaard/tls>
- [21] <https://forumstandaardisatie.nl/standaard/xbrl-en-dimensions>

2. Totstandkoming standaarden

De hierboven genoemde standaarden zijn geleverd door Forum Standaardisatie door invulling van de beslisboom op 3-11-2020 met onderstaande antwoorden.

Uw organisatie in de publieke sector

Er is een bepaalde vorm van ICT of er wordt ICT beoogd om in te kopen, aan te besteden of op een ander manier aan te schaffen. Wie is de eigenaar of de opdrachtgever?

- * Gemeente of gemeenschappelijke regeling

Gegevens soort

Welk soort gegevens worden er door de ICT-voorziening uitgewisseld met bedrijven of instanties?

- * Basisregistraties / overheidsgegevens
- * Financieel / rapportages
- * Statistieken / verkiezingen

Gegevens type

Welk type gegevens wordt verwerkt door de ICT-voorziening?

- * Gestructureerde berichten om geautomatiseerde verwerking mogelijk te maken
- * Documenten (zoals tekstbestanden, spreadsheets, e-mail, etc.)
- * Metadata: aanvullende informatie over of voor berichten, documenten en multimedia content

Communicatie kanalen

Middels welk communicatiekanaal wisselt de ICT-voorziening gegevens uit?

- * Via een website of webapplicatie
- * Via e-mail
- * Tussen systemen (machine-to-machine)

Beveiliging & privacy

Welk van de volgende beveiliging- en/of privacyaspecten spelen een rol bij de ICT-voorziening?

- * Beveiliging en privacy speelt een rol bij de nieuwe voorziening

Specifieke vragen

Is het van belang dat de voorziening voorziet in het elektronisch ondertekenen van digitale documenten?

* Ik weet het niet

Wisselt het Content of Document Management Systeem niet-gestructureerde informatie (documenten, afbeeldingen, etc.), inclusief metadata, uit met Content of Document Management Systemen buiten de organisatie?

* Ja

Wordt de voorziening gebruikt om informatie uit te wisselen met de opdrachtgevers en de opdrachtnemers tijdens het bouwproject?

* Nee

Wordt de voorziening gebruikt voor de elektronische uitwisseling van gegevens tussen overheden?

* Nee

Moet de voorziening toegankelijk zijn voor mensen met een functiebeperking?

* Nee

Verstuurt of ontvangt de voorziening e-mails?

* Ja

Verstuurt of ontvangt de voorziening e-mails?

* Ja

Beschikt de voorziening over een domeinnaam (het adres van een website op het internet)?

* Ja

Wordt de voorziening gebruikt voor het verwerken en uitwisselen van verkiezingsgegevens?

* Nee

Is er sprake van een website of webapplicatie?

* Ja

Beschikt de voorziening over een IP-adres (internetnummer)?

* Ja

Is informatiebeveiliging relevant voor de voorziening?

* Ja

Ontsluit de voorziening gegevens of applicaties met REST-API's?

* Ik weet het niet

Wordt de voorziening gebruikt voor het ontvangen en verwerken van elektronische facturen?

* Ja

Verwerkt de voorziening bewerkbare documenten (bestaande uit tekst, spreadsheets, tabellen, grafische elementen en dus ook websites?)

* Ja

Maakt de voorziening gebruik van een of meerdere API (Application Programming Interface)?

* Ik weet het niet

Is er sprake van een website of webapplicatie waarbij overheidsinformatie wordt verwerkt of gegenereerd?

* Nee

Biedt de voorziening informatie aan in de vorm van een document waarvan de pagina opmaak vastligt (PDF-document)?

* Ja

Ontsluit de voorziening gegevens of applicaties met REST-API's?

* Ik weet het niet

Is beveiliging van het internetverkeer relevant voor de voorziening?

* Ja

Is het de bedoeling om eenmalig inloggen voor de voorziening mogelijk te maken?

* Ja

Wordt de voorziening gebruikt voor de verwerking of uitwisseling van informatie over de inzet van flexibele arbeidskrachten?

* Nee

Wordt de voorziening gebruikt voor het uitwisselen van bodeminformatie (kwaliteit en milieuhygiëne)?

* Nee

Wisselt de voorziening archeologische informatie uit tussen opgravende instanties, vondstendepots en/of archeologische registers?

* Nee

Wordt de voorziening gebruikt voor het publiceren van begrippenlijsten of digitale gegevenswoordenboeken?

* Nee

Verstuurt of ontvangt de voorziening e-mails?

* Ja

Verstuurt of ontvangt de voorziening e-mails?

* Ja

Wordt de voorziening gebruikt voor het uitwisselen van administratieve overheidsgegevens (zoals gegevens uit basisregistraties) met gemeenten?

* Ja

Verstuurt of ontvangt de voorziening gegevens over een openbaar netwerk (zoals internet)?

* Ja

Betreft de voorziening een wifi-netwerk?

* Nee

Wordt de voorziening gebruikt voor het uitwisselen/verwerken van (financiële) bedrijfsrapportages?

* Ja