# Handreiking open standaarden bij aanschaf ICT

## Handreiking open standaarden bij aanschaf ICT

## Introductie

Voldoen aan het ‘pas toe of leg uit’- beleid is de verantwoordelijkheid van de opdrachtgever of budgethouder onder wiens mandaat een ICT-aanschaf plaatsvindt. Het ligt echter op de weg van de inkoopadviseur om de opdrachtgever zo nodig te wijzen op het bestaan van het ‘pas toe of leg uit’-beleid en het gesprek hierover te beginnen zodra sprake is van een ICT aanbesteding van € 50.000 of meer.

Deze handreiking heeft het doel om dit gesprek te stimuleren. Door het belang van de ‘pas toe of leg uit’-standaarden te benadrukken, het kiezen voor de juiste standaarden in een specifiek geval makkelijker te maken, voorbeelden te geven voor bestekteksten en uitleg te geven over hoe gemotiveerd uitgelegd moet worden bij het achterwege laten van standaarden.

Informatie

Deze handreiking is bedoeld voor opdrachtgevers en inkoopadviseurs. Vooral bij overheidsorganisaties, maar ook bij andere organisaties in de (semi) publieke sector.

Laatst bijgewerkt: 17 juli 2023

Download

## 1. Open standaarden

De openheid van standaarden zorgt voor leveranciersonafhankelijkheid, naast interoperabiliteit. Afhankelijk van de aard van de standaard, kunnen open standaarden zorgen voor veiligheid in het digitale verkeer, goede vindbaarheid, toegankelijkheid en (her)gebruik van data.

Kenmerken van open standaarden zijn:

1. dat er geen hindernissen zijn om de inhoud van de afspraken te kennen (laagdrempelig beschikbare documentatie);
2. dat de afspraken vervolgens vrij (her)bruikbaar zijn omdat geen intellectuele eigendomsrechten dit beperken;
3. dat een ieder inspraak kan hebben op de inrichting van de standaard;
4. en hiervoor terecht kan bij een onafhankelijke en duurzaam ingerichte non-profit beheerorganisatie van de standaard.

NB: Open standaarden worden vaak in één adem genoemd met open source. Hoewelopen standaarden en open source elkaar kunnen versterken als het gaat om goede ICT te gebruiken in de publieke ruimte, zijn het toch ook twee verschillende dingen. Open standaarden gaan over koppelvlakken die iedere ICT leverancier kan inbouwen. Open source software betreft software waarbij de broncode voor iedereen beschikbaar is. Open standaarden kunnen zowel in open source software als in gesloten software geïmplementeerd zijn.

Meer informatie hierover:

Open standaarden of open source software

Forum Standaardisatie toetst standaarden voor elektronische gegevensuitwisseling onder andere op bovengenoemde kenmerken voor openheid. Dit gebeurt in een openbare procedure. Komt een standaard met succes hierdoor, dan kan de standaard op de lijst gezet worden met open standaarden van het Forum Standaardisatie.

Standaarden op deze lijst hebben twee statussen: ‘pas toe of leg uit’ óf aanbevolen. Een open standaard komt op de ‘pas toe of leg uit’- lijst als de standaard nog een extra stimulans nodig heeft om gebruikt te worden. In deze handreiking bedoelen wij verder met open standaarden, de standaarden voor elektronische gegevensuitwisseling die op de ‘pas toe of leg uit’- lijst staan van het Forum Standaardisatie.

'Pas toe of leg uit'-standaarden

1.1 Voordelen van open standaarden

### 1.1 Voordelen van open standaarden

**Interoperabiliteit**

Standaardisatie van ICT zorgt ervoor dat systemen naadloos op elkaar aansluiten. Het digitale verkeer stroomt door. Organisaties kunnen doen waarvoor ze in het leven geroepen zijn, door onderling goed samen te werken en door goed in verbinding te staan met de burgers en bedrijven waar de meeste publieke dienstverlening uiteindelijk voor bedoeld is. Alle open standaarden op de ‘pas toe of leg uit’- lijst zorgen in beginsel voor interoperabiliteit en leveranciersonafhankelijkheid maar bij sommige standaarden is deze goede doorstroom van gegevens het het meest prominente doel.

**Veiligheid**

Veilig verkeer in de digitale wereld, zoals bijvoorbeeld betrouwbare websites en e-mails waar niet zomaar iedereen bij kan. Nalaten van het gebruik van de informatieveiligheidstandaarden kan tot grote schade leiden en tast het vertrouwen in overheidsorganisaties en andere publieke dienstverleners aan. De open standaarden niet gebruiken die hiervoor verplicht zijn of dringend aanbevolen valt bijna niet uit te leggen.

**Toegankelijkheid**

Iedereen moet mee kunnen doen, ook digitaal. Een functiebeperking mag geen drempel zijn voor deelname aan het digitale verkeer en informatie moet beschikbaar zijn in begrijpelijke taal voor iedereen. Inclusie dus, ook in de digitale wereld. Meer over toegankelijkheid: https://www.digitoegankelijk.nl.

**Openbaarheid**

Openbaarheid van bestuur en rechtspraak, openbare informatie, open data, en linked data. Zonder het gebruik van de juiste open standaarden is dit niet waar te maken. Openbare informatie dient toegankelijk, vindbaar en begrijpelijk en (her)bruikbaar te zijn.

1.2 ‘Pas toe of leg uit’ betekenis

### 1.2 ‘Pas toe of leg uit’-betekenis

Wat betekent de ‘pas toe of leg uit’- status van de open standaarden op de lijst van het Forum Standaardisatie nu precies?

**Pas toe**

Gebruik de relevante standaarden op de lijst van het Forum Standaardisatie, uiterlijk bij aanschaf van ICT, wanneer deze aanschaf € 50.000 of meer bedraagt. Een ICT-aanschaf kan gaan om een dienst, een product, een aanbesteding of inbesteding, verbouw of nieuwbouw. Een standaard is relevant als de ICT valt onder het toepassingsgebied zoals beschreven op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie.

NB: Vaak gaat een aanschaf gepaard met inkoop en aanbesteding, vandaar dat deze handreiking 'Vragen om open standaarden bij inkoop' heet. Maar eigenlijk moeten de relevante standaarden toegepast worden bij aanschaf, wat een ruimer begrip is.

**Leg uit**

Relevante standaarden toch niet gebruiken mag alleen met een geldige reden, die terug te vinden is in het jaarverslag. Een geldige redenen is wanneer een ICT-dienst of product naar verwachting in onvoldoende mate wordt aangeboden, onvoldoende veilig of zeker functioneert, of een andere reden van bijzonder gewicht.

1.3 Juridische verankering

## 1.3 Juridische verankering

'Pas toe of leg uit' is juridisch wat versnipperd geregeld. Misschien dat het beleid daarom vaak wat vrijblijvend geïnterpreteerd wordt (het hoeft niet echt) en niet als een verplichting.

Het is echter een misvatting om te denken dat verplichtingen alleen zouden kunnen voortvloeien op grond van een wet in formele zin. Verplichtingen kunnen ook volgen uit bestuursafspraken en richtlijnen, die nagekomen dienen te worden.

In tegenstelling tot wat vaak wordt gedacht, geldt 'pas toe of leg uit' als een verplichting voor de meeste overheidsorganisaties. Het gaat daarbij (nog) niet om een verplichting op grond van een wet in formele zin (maar de wet Digitale Overheid kan hier vanaf 2021 wellicht verandering in brengen), maar om een verplichting op grond van een ministeriële regeling, namelijk de Instructie Rijksdienst bij aanschaf van ICT-diensten of ICT-producten (BWBR0024717) én -in aansluiting hierop- de afspraken die bestuurders van gemeenten, provincies, waterschappen en uitvoeringsorganisaties hebben gemaakt die in de loop der tijd herhaaldelijk zijn bevestigd.

**Overheidsorganisaties**

Voor rijksoverheidsorganisaties geldt sinds 2008 de Instructie Rijksdienst bij aanschaf ICT-diensten of ICT-producten (BWBR0024717). Door het Overheidsbreed Beleidsoverleg Digitale Overheid is in 2018 uitdrukkelijk afgesproken dan ZBO's ook gehouden zijn aan deze instructie. In deze instructie wordt in artikel 3, lid 1 bepaald dat: Bij de aanschaf van een ICT-dienst of ICT-product voor een toepassingsgebied dat voorkomt op de lijst die op de website www.forumstandaardisatie.nl is gepubliceerd, wordt gekozen voor een ICT-dienst of een ICT-product dat gebruikt maakt van een bij het desbetreffende toepassingsgebied vermelde open standaard. Uit de toelichting blijkt dat deze verplichting geldt voor de aanbesteding, inkoop of ontwikkeling van ICT-producten en ICT-diensten ter waarde van € 50.000 en meer. Niet alleen voor nieuwe producten of diensten, maar ook als het gaat om aanpassing van bestaande producten of diensten.

Daarnaast staat in de Rijksbegrotingsvoorschriften (RBV) een bepaling m.b.t. de paragraaf 'Rijksbrede bedrijfsvoeringsonderwerpen':

Gebruik open standaarden en open source software. Dit onderwerp wordt in deze paragraaf alleen vermeld indien is afgeweken (het 'comply of explain'-beginsel) van artikel 3, eerste lid van de Instructie rijksdienst bij aanschaf ICT-diensten of ICT-producten). De Tweede Kamer wil dat de overheid meer gebruik maakt van open standaarden en open source software. De Instructie rijksdienst schrijft voor dat bij de aanschaf en ontwikkeling van ICT-diensten of ICT-producten in beginsel gebruik moet worden gemaakt van open standaarden van de lijst van het College Standaardisatie. Valide afwijkingsgronden zijn opgenomen in de Instructie Rijksdienst. Als er sprake is van afwijking van de Instructie Rijksdienst dan wordt dit gemotiveerd aangegeven.

NB: Het College Standaardisatie bestaat al een aantal jaren niet meer en het Overheidsbreed Beleidsoverleg Digitale Overheid (OBDO) is hiervoor sinds 2018 in de plaats gekomen. Een wijziging van de Rijksbegrotingsvoorschriften is eind 2020 nog niet doorgevoerd.

In 2008 is in de iNUP-bestuursakkoorden als Resultaatafspraak 20 opgenomen, voor zover het open standaarden betreft: gemeenten maken gebruik van de open standaarden zoals vastgesteld door het College standaardisatie en werken hierbij volgens het principe 'pas toe of leg uit'. Deze resultaatafspraak was van toepassing op gemeenten, provincies en waterschappen.

Deze afspraak is hierna herhaaldelijk herbevestigd in het College Standaardisatie en het Nationaal Beraad Digitale Overheid.

Op 18 april 2018 heeft het OBDO voor het laatst besloten dat ook mede-overheden bij aanschaf van ICT moeten kiezen voor de relevante open standaarden van de 'pas toe of leg uit'-lijst.

**Andere organisaties in de publieke sector**

Is een organisatie géén overheidsorganisatie zoals hierboven genoemd, dan is het gebruik van de 'pas toe of leg uit'- standaarden strikt genomen niet verplicht.'Pas toe of leg uit' mag dan worden opgevat als een dringend advies.

Er is geen toezicht of handhaving als 'pas toe of leg uit' niet wordt nageleefd of opgevolgd. Het onderscheid 'verplicht' of 'dringend aanbevolen' heeft wat dat betreft geen consequenties.

**Monitor Open Standaarden en IV-meting**

Er is dus geen toezicht en handhaving op 'pas toe of leg uit'. Wél vindt jaarlijks monitoring plaats en halfjaarlijks een meting van de internet- en beveiligingstandaarden om te zien hoe het staat met het gebruik van de standaarden op de 'pas toe of leg uit'- lijst. Om het gebruik van de 'pas toe of leg uit'-standaarden te meten en tegelijkertijd ook  om de adoptie een impuls te geven.

In de Monitor Open Standaarden worden aanbestedingsdocumenten en jaarverslagen onderzocht . De onderzoekers bekijken in de aanbestedingsdocumenten of organisaties om de relevante open standaarden vragen en of zij goed verantwoording afleggen in jaarverslagen als dit niet gebeurt. Zoals al eerder gezegd anno 2020 is er nog veel ruimte te zien voor verbetering op dit punt.

Daarnaast voert het Forum Standaardisatie twee keer per jaar een meting uit naar het gebruik van een aantal internet en beveiligheidstandaarden, met behulp van de webtool internet.nl. In dit onderzoek is overigens wél een stijgende lijn te zien.

1.4 Relevante standaarden bepalen

## 1.4 Relevante standaarden bepalen

Om met het oog op ICT-kwaliteit bij de overheid de relevante open standaarden te selecteren en op te nemen in een aanbesteding, zijn er online een aantal tools beschikbaar die elkaar aanvullen.

**Beslisboom Open Standaarden**

Het meest aangewezen instrument om de weg te vinden in de toepassingsgebieden bij de standaarden op de 'pas toe of leg uit'- lijst is deBeslisboom. Deze Beslisboom is bedoeld om tot een eerste inschatting te komen van de standaarden die met het oog op een ICT-aanschaf relevant zijn. De vragen van de Beslisboom dienen bij voorkeur zo veel mogelijk beantwoord te worden met de betrokkenen van een aanbesteding. De Beslisboom geeft een eerste ruwe selectie van relevante standaarden voor nadere overweging. Neem voor meer advies op maat contact op met het Bureau Forum Standaardisatie.

**De ICO-Wizard**

De ISO 27001 en ISO 27002 standaarden staan op de 'pas toe of leg uit'-lijst en zijn heel vaak van toepassing als het gaat om een nieuwe aanschaf van ICT. Voor overheidsorganisaties zijn de ISO 270001 en ISO 27002 vertaald naar de BIO (Baseline Informatiebeveiliging Overheid) en dus ook heel vaak van toepassing. Ten tijde van het actualiseren van deze handreiking in 2020, ontwikkelt het Centrum voor Informatie en Privacybescherming (CIP) de ICO-Wizard. Dat is net als de Beslisboom Open Standaarden ook een instrument om vroeg in het proces nadere afwegingen te maken, maar dan specifiek over beveiliging. Met de ICO-Wizard kunnen organisaties ervoor zorgen dat bij inkoop de juiste BIO veiligheidsnormen in beeld komen, zodat de organisatie ze ook kan opnemen in het programma van eisen van een aanbesteding. De ICO- Wizard vult de Beslisboom Open Standaarden nader aan en gaat dieper in op de veiligheidsnormen van de BIO. Veel veiligheidstandaarden van de 'pas toe of leg uit'- lijst komen ook in deze Wizard terug.

**Internet.nl**

Met internet.nl kunnen organisaties bepalen of hun websites en e-mailadressen voldoen aan een aantal van de internet en beveiligingstandaarden van de 'pas toe of leg uit'- lijst. Pagina 14 van 47 op internet.nl is sinds 2020 ook een Hall of Fame opgenomen van 'hosters' die een 100% score hebben.

## 2. Praktijkvoorbeelden

Voor iedere standaard op de ‘pas toe of leg uit’-lijst is een formeel toepassingsgebied gedefinieerd. Tegenover de abstracte toepassingsgebieden van de ‘pas toe of leg uit’-standaarden staat de werkelijkheid van een enorme variëteit in toepassingen. Dat maakt maatwerk van het bepalen van de relevante standaarden en het toepassen in de praktijk.

Bij het aanschaffen van nieuwe ICT moet telkens de toepasselijkheid van een ‘pas toe of leg uit’-standaard herkend worden.

Om dit te illustreren en om meer gevoel te krijgen bij de toegevoegde waarde van de standaarden in de praktijk, staan in dit hoofdstuk tien voorbeelden van aanbestedingen genoemd die onderzocht zijn in het kader van de Monitor Open Standaarden. De praktijkvoorbeelden illustreren de volgende 10 ICT-producten of -diensten:

Meer voorbeelden van onderzochte aanbestedingen zijn te vinden in de bijlage vande Monitor Open Standaarden.

2.1 Cloud computing

### 2.1 Cloud computing

**Integratieplatform routeren, transformeren en orkestreren berichten**

Aanbestedingsnummer: 229233

Opdrachtgever: Gemeente Stein

TenderNed: Integratieplatform voor routeren, transformeren en orkestreren berichten

In 2021 heeft de gemeente Stein een aanbesteding gedaan voor een integratieplatform ten behoeve van de distributie, routeren, transformeren, orkestreren van berichten tussen applicaties. De oplossing wordt als SAAS-oplossing geleverd, en de opdrachtnemer voert het volledige (technische) onderhoud uit.

Voor deze aanbesteding zijn waarschijnlijk de volgende standaarden relevant:

- Digikoppeling; voor gegevensuitwisseling tussen systemen waarbij er noodzaak is voor tweezijdige authenticatie.
- StUF; vanwege de uitwisseling van administratieve overheidsgegevens
- HTTPS en HSTS; voor een veilige uitwisseling van gegevens tussen een webserver en client
- TLS; voor een veilige uitwisseling van gegevens tussen clients en servers, inclusief machine-to-machine communicatie.
- SAML; vanwege single sign on.
- OpenAPI; vanwege de wens om gebruik te maken van gestandaardiseerde en gedocumenteerde koppelvlakken.
- ISO 27001/27002; vanwege de omgang met persoonsgegevens dient de leverancier aan te geven of hij in het bezit is van deze certificering danwel op een ander wijze kan voldoen aan de normen vanuit de Baseline Informatiebeveiliging Overheid.
- PDF en ODF; vanwege het kunnen maken van rapportages.

- IPv4 en IPv6; Gebruikers en andere ICT-systemen moeten het integratieplatform kunnen bereiken via zowel IPv4 als IPv6

In deze aanbesteding heeft de gemeente met betrekking tot de berichtenstandaard aangegeven dat zij daarbij de toepassing verwachten van de standaarden van het forum standaardisatie en zowel de berichtenstandaarden van eindproducten als halffabricaten benoemd binnen GEMMA.

**Integraal Systeem Sociaal Domein (Regie- en Backofficefunctionaliteit in één systeem)**

Aanbestedingsnummer: 247924

Opdrachtgever: Werkorganisatie BUCH

TenderNed: Integraal systeem sociaal domein

In 2022 doet werkorganisatie BUCH een aanbesteding voor de Implementatie, het hosten en onderhouden van een integraal SAAS systeem voor het sociaal domein. De werkorganisatie BUCH werkt voor de gemeenten Bergen, Uitgeest, Castricum en Heiloo. Bij deze aanbesteding zijn de volgende standaarden door de werkorganisatie geëist:

- TLS; voor versleuteling van het datatransport;
- StUF; vanwege de uitwisseling van administratieve overheidsgegevens
- SAML; vanwege single-sign-on mogelijkheid;
- IPv4 en IPv6; gebruikers en andere ICT-systemen moeten het systeem kunnen bereiken via zowel IPv4 als IPv6;
- DNSSEC; voor een geldige ondertekening van de domeinnaam van het ICT systeem;
- STARTTLS & DANE, SPF, DKIM en DMARC voor beveiliging e-mail;
- ISO 27001/27002; voor informatiebeveiliging;
- HTTPS en HSTS; voor beveiligde toegang tot o.a. email;
- PDF en ODF; vanwege het werken met reviseerbare en niet-reviseerbare documenten.
- Digitoegankelijk, voor toegankelijkheid van het systeem voor personen met een functiebeperking.

2.2 Websites of webapplicaties

## 2.2 Websites of webapplicaties

**Open Inwoner Platform**

- Aanbestedingsnummer: 232093
- Opdrachtgever: Coöperatie Dimpact UA
- TenderNed: Open inwoner Platform

Gemeentes voeren de WMO, Jeugdwet, Participatiewet, Inburgeringswet uit, hebben essentiële taken op het gebied van Schuldhulpverlening en specifiek beleid op het gebied van Armoede. Belangrijke doelen van deze wetten zijn zelfstandigheid, gebruik van het sociale netwerk, zonder dat er 'gaten' vallen. i4Sociaal is een initiatief van 6 gemeenten, samen met Dimpact, om betere invulling te geven aan de doelstellingen van deze wetten, middels een digitaal ondersteuningsplatform voor haar inwoners. Het Open Inwoner Platform moet op termijn gemeentebreed in te zetten zijn en kan daarmee op termijn de vervanging zijn van de "MijnOmgeving" van een gemeente: het is het platform met name voor de inwoner.

In deze aanbesteding uit 2021 heeft men de beslisboom Open Standaarden met de uitkomsten integraal opgenomen in het programma van eisen:

- Ades Baseline Profiles: De Advanced Electronic Signature (AdES) standaard voorziet in het digitaal tekenen van documenten met een geavanceerde of gekwalificeerde digitale handtekening
- Digikoppeling: realiseert geautomatiseerde gegevensuitwisseling tussen informatiesystemen voor sector overstijgend berichtenverkeer
- Digitoegankelijk: Door toepassing van Digitoegankelijk worden websites en webapplicaties toegankelijk voor mensen met een functiebeperking.
- 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 en HSTS; Voor de veilige uitwisseling van gegevens tussen een webserver en client.
- IPv4 en IPv6; Gebruikers en andere ICT-systemen moeten het ICT-systeem kunnen bereiken via zowel IPv4 als IPv6
  .
- ISO 27001/27002;
  vanwege de omgang met persoonsgegevens dient de leverancier aan te geven of hij in het bezit is van deze certificering danwel op een ander wijze kan voldoen aan de normen vanuit de Baseline Informatiebeveiliging Overheid
- 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 plaatsvindt.
- PDF; voor verwerking van niet-reviseerbare documenten
- ODF; voor de verwerking van bewerkbare documenten.

- OpenAPI; want er is sprake van te beschrijven koppelvlakken op basis van REST API's.

- OWMS; vanwege het metadateren van publieke overheidsinformatie op internet.
- RPKI; voor veilige routering vanaf het netwerk.
- 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.
- StUF; uitwisseling en bevraging van zaakgegevens die behoren tot het producten- en dienstenportfolio van gemeenten;
- 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.

Door de beslisboom met de uitkomsten integraal op te nemen laat men niet alleen zien welke standaarden relevant kunnen zijn, maar geeft het tevens inzicht voor leveranciers over de verwachtingen die er bij de aanbestedende dienst zijn.

**Portaal Schuldhulpverlening**

- Aanbestedingsnummer: 222775
- Opdrachtgever: Gemeente Breda
- TenderNed: Portaal Schuldhulpverlening

Dit betreft een aanbesteding om tot een overeenkomst te komen voor de levering, implementatie en het beheer van een website/portaal voor "Schuldhulpverlening". Met de aanschaf van een nieuw portaal wil Breda een belangrijke stap zetten. Enerzijds om voor burgers (en hulpverleners) het inzicht in hun schulden te verbeteren. En anderzijds om qua toegankelijkheid en security/privacy een oplossing in huis te hebben die aansluit op momenteel vigerende wetgeving.

Voor dit portaal wordt een contract aangegaan voor 3 jaar met de mogelijkheid om 3 keer met 1 jaar te verlengen. In het programma van eisen worden een aantal standaarden expliciet genoemd:

- PDF; vanwege de mogelijkheid om niet-reviseerbare rapportages te kunnen maken en exporteren.
- ODF; omdat de aanvrager de mogelijkheid moet hebben om bijlagen digitaal toe te voegen in een aantal formaten waaronder odt, ods en odp.
- Digitoegankelijk; voor toegankelijkheid van het systeem voor personen met een functiebeperking.

- StUF: uitwisseling en bevraging van zaakgegevens die behoren tot het producten- en dienstenportfolio van gemeenten;

- ISO 27001/27002; vanwege de informatiebeveiliging.

Naast deze specifiek genoemde standaarden stelt men in Breda als eis dat de levering dient te voldoen aan de "Bredase ICT-kwaliteitsnormen". In dat document is de architectuur en infrastructuur beschreven. Inzake beveiliging is daar opgenomen dat de leverancier zich gedurende de looptijd van het contract conformeert aan de meest recente

versie van de BIO of gelijkwaardig normenkader naast de geldende wet en regelgeving, en dat ze minimaal eens per drie jaar een Assurance verklaring zoals ISO 27001/27002 kunnen overleggen. Ook verwijst men naar de ICT-beveiligingsrichtlijnen voor webapplicaties.

Om aan de BIO te kunnen voldoen volgt de gemeente Breda in het geval van webapplicaties

de 'Beveiligingsrichtlijnen voor webapplicaties' van het National Cyber Security Center (NCSC). Deze beveiligingsrichtlijnen voor webapplicaties geven een leidraad voor veiliger ontwikkelen, beheren en aanbieden van webapplicaties en bijbehorende infrastructuur.

Deze richtlijnen zijn hier te vinden: https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties

Leveranciers die REST API's aanbieden, dienen API-documentatie op te leveren conform de OAS (OpenAPISpecification) 3.x standaard, inclusief de authenticatie mogelijkheden.

Andere standaarden die expliciet in het document worden genoemd zijn: TLS, HTTPS, HSTS, Digitoegankelijk, DNSSEC, SPF, DKIM en DMARC, STARTTLS en DANE: standaarden voor de beveiliging van mailverkeer middels encryptie

Bovendien verwijst het document naar het actieplan Nederland Open in Verbinding waarin door het kabinet is aangegeven dat het gebruik van open standaarden door overheidsorganisaties niet meer vrijblijvend is. De gemeente Breda conformeert zich dan ook aan de lijst met open standaarden van het Forum Standaardisatie volgens het 'pas toe of leg uit' beleid. Van leveranciers wordt verwacht dat zij voor de levering van de diensten aan de gemeente Breda dan ook gebruik maken van de relevante open standaarden uit deze lijst.

**Nederlandse publieke omroep**

De Nederlandse Publieke Omroep doet in 2018 een openbare aanbesteding voor het leveren van development en design voor de ontwikkeling van 9 nieuwe apps voor NPO Radio algemeen en de diverse radiomerken van de NPO, inclusief beheer, ondersteuning en onderhoud. De apps moeten d.m.v. gestandaardiseerde en gedocumenteerde koppelvlakken (bijv. API's) kunnen koppelen met andere systemen en databases in de keten.

Het gaat hier om webapplicaties en bij deze aanbesteding zijn waarschijnlijk de volgende standaarden relevant:

- SAML, want in het bestek is gevraagd om koppeling met NPO single sign-on en profielendata;
- Digitoegankelijk, want het gaat over applicaties voor burgers;
- HTTPS en HSTS en TLS, want het betreft een webapplicatie en voor beveiliging van netwerkverbindingen;
- OpenAPI Specification, vanwege de wens om gebruik te maken van gestandaardiseerde en gedocumenteerde koppelvlakken.

2.3 Werkplek en kantoorsoftware

## 2.3 Werkplek en kantoorsoftware

**Planningsapplicatie 'IB-MeT-PMB-V&OR'**

- Aanbestedingsnummer: 224643
- Opdrachtgever: Gemeente Amsterdam, afdeling ICT
- TenderNed: Planningsapplicatie

Levering en onderhoud van een Planningsapplicatie in de vorm van een SaaS-oplossing waarmee automatisch, dynamisch en flexibel van opzet planningen worden gegenereerd;

Bij deze aanbesteding van de gemeente Amsterdam zijn de volgende standaarden relevant:

- TLS; voor versleuteling van het datatransport;
- SAML; vanwege single-sign-on mogelijkheid;
- IPv4 en IPv6;  Gebruikers en andere ICT-systemen  moeten het ICT-systeem kunnen bereiken via zowel IPv4 als IPv6;
- DNSSC; voor een geldige ondertekening van de domeinnaam van het ICT systeem;
- STARTTLS & DANE, SPF en DKIM; voor beveiliging e-mail;
- ISO 27001/27002; voor informatiebeveiliging;
- HTTPS en HSTS beveiligde toegang tot o.a. email;
- PDF en ODF vanwege het werken met reviseerbare en niet-reviseerbare documenten.
- Digitoegankelijk, voor toegankelijkheid van de bijbehorende op te leveren website.
- SKOS en OWMS : Het ICT-systeem biedt ten behoeve van gegevensuitwisseling volledig werkende ondersteuning voor SKOS en OWMS.

Alle bovengenoemde standaarden worden in deze aanbesteding ook daadwerkelijk gevraagd. Er wordt bovendien in het bestek vaak verwezen naar het gebruik van open standaarden en men verwijst ook vaak naar de ‘pas toe of leg uit’-lijst van Forum Standaardisatie

**Huis voor Klokkenluiders**

Het Huis voor Klokkenluiders publiceert eind 2017 doet een aanbesteding voor een onafhankelijke ICT-dienstverlener om de kleine organisatie op ICT-gebied te ontzorgen en een digitale werkomgeving bij onder te brengen. De werkzaamheden van Het Huis zijn zeer vertrouwelijk en vragen om een beveiligde digitale werkomgeving. De scope van de aanbesteding bevat het leveren van een beveiligde digitale werkomgeving, ICT infrastructuurdiensten/hosting, hardware incl. software voor werkplekken (incl. onderhoud en beheer), en koppelingen met het SaaS-systeem en Citrix werkomgeving.

Bij deze aanbesteding zijn waarschijnlijk de volgende standaarden relevant:

- WPA2 Enterprise, voor beschikking kantoor over internettoegang;
- TLS, voor inrichting mailkoppeling naar zaaksysteem;
- SAML, vanwege single-sign-on mogelijkheid;
- IPv6 & IPv4, voor internetverbinding van de digitale werkomgeving;
- DNSSEC, voor domeinnaam van de digitale werkomgeving;
- STARTTLS & DANE, SPF en DKIM, voor beveiliging e-mail;
- ISO 27001 / ISO 27002, voor informatiebeveiliging;
- HTTPS en HSTS, voor beveiligde toegang tot o.a. email;
- PDF en ODF, vanwege het werken met reviseerbare en niet-reviseerbare documenten.

**Toelichting**

Alle bovengenoemde standaarden worden in deze aanbesteding ook daadwerkelijk gevraagd. Er wordt bovendien in het bestek vaak verwezen naar het gebruik van open standaarden en men verwijst ook vaak naar de ‘pas toe of leg uit’-lijst van Forum Standaardisatie. Bovendien spoort men aan het gebruik van niet algemeen geaccepteerde standaarden nadrukkelijk te vermijden.

2.4 E-mail

## 2.4 E-mail

**E-mail management tool**

- Aanbestedingsnummer: 227555
- Opdrachtgever : Gemeente Venlo
- TenderNed: E-mail management tool

Deze opdracht uit 2021 omvat het leveren, implementeren en onderhouden van een e-mail applicatie. Deze applicatie maakt het onder andere mogelijk om snel en eenvoudig vanuit diverse applicaties e-mails en andere data te verzenden, en ontvangen en verzonden e-mail berichten (en bijlagen) correct op te slaan ten behoeve van dossiervorming.

In deze aanbesteding zijn waarschijnlijk de volgende standaarden relevant:

- IPv6 & IPv4, voor internetverbinding van de e-mailvoorziening;
- HTTPS en HSTS, voor een beveiligde verbinding;
- TLS, voor versleuteling van de verbinding;
- DKIM, DMARC, SPF, want het betreft inkomend en uitgaand e-mailverkeer;
- STARTTLS & DANE, want het gaat hier om een ontvangende en verzendende e-mailserver;
- ISO 27001 / ISO 27002, voor informatiebeveiliging;

PDF en ODF vanwege het werken met reviseerbare en niet-reviseerbare documenten (zoals kunnen uitdraaien van managementrapportages);

**Algemene Zaken / DPC**

Het Ministerie van Algemene Zaken, Dienst Publiek en Communicatiedoet een openbare aanbesteding voor het leveren en beheren van een e-mailmanagementvoorziening voor het Platform Rijksoverheid Online (PRO), inclusief facultatieve dienstverlening rondom optimalisatie van het e-mailkanaal.

In deze aanbesteding zijn waarschijnlijk de volgende standaarden relevant:

- IPv6 & IPv4, voor internetverbinding van de e-mailvoorziening;
- HTTPS en HSTS, voor een beveiligde verbinding;
- TLS, voor versleuteling van de verbinding;
- DKIM, DMARC, SPF, want het betreft inkomend en uitgaand e-mailverkeer;
- STARTTLS & DANE, want het gaat hier om een ontvangende en verzendende e-mailserver;
- ISO 27001 / ISO 27002, voor informatiebeveiliging;
- PDF en ODF vanwege het werken met reviseerbare en niet-reviseerbare documenten (zoals kunnen uitdraaien van managementrapportages);
- OpenAPI Specification, vanwege de mogelijkheid dat gebruik zal worden gemaakt van een API.

**Toelichting**

Zoals hiervoor al aangegeven is de Baseline Informatiebeveiliging Overheid (BIO), dan wel zijn de standaarden ISO 27001/27002 relevant voor vrijwel alle aanbestedingen. In dit specifieke geval al helemaal omdat er door de nieuwe leverancier een groot aantal persoonsgegevens (immers e-mailadressen) gemigreerd moest gaan worden van het oude naar het nieuwe systeem.

In de BIO is opgenomen dat persoonsgegevens niet onversleuteld over onbeveiligde/onvertrouwde netwerken verzonden mogen worden. Informatie die is opgenomen in een elektronisch bericht behoord passend te worden beschermd. Deze baseline verplicht zodoende afgedwongen versleuteling van verbindingen zoals STARTTLS die in combinatie met DANE ondersteunt. Ook het gebruik van ODF is in deze aanbesteding terecht van de toekomstige leverancier geëist:

“Opdrachtnemer stelt ook verzendstatistieken beschikbaar in ODF-formaat.

Opdrachtnemer stelt tevens een gebruikershandleiding beschikbaar in ODF-formaat.”

En omdat er mogelijk gebruik moet worden gemaakt van een API, is er ook het volgende op voorhand al geëist:

“Voor het gebruik van een API is de open API-Specification vastgesteld als open standaard. Opdrachtgever volgt deze standaard gecombineerd met de standaarden voor web en e-mail”.

Zoals ook uit bovengenoemd praktijkvoorbeeld blijkt: let er op dat bij software ten behoeve van e-mail, dat meerdere standaarden relevant kunnen zijn uit de domeinen “Internet en beveiliging” en “Documenten en webcontent”.

Het gaat bij e-mail niet alleen om het aanschaffen of in gebruik nemen van een 'e-mail client', maar vaak ook om de inrichting van allerlei ICT-systemen van waaruit door middel van het e-mailprotocol een bericht of nieuwsbrief kan worden verzonden. Denk bijvoorbeeld aan de verderop nog te bespreken 'multifunctionals', waarbij het vaak mogelijk is om vanuit de 'multifunctional' gescande documenten te verzenden aan een mailadres.

2.5 Spraak en/of datacommunicatiediensten

## 2.5 Spraak en/of datacommunicatiediensten

**Berichtendienst voor UWV**

- Aanbestedingsnummer: 230127
- Opdrachtgever: UWV
- TenderNed: Berichtendienst voor UWV

Deze aanbesteding ziet op het door UWV versturen van berichten naar mobiele telefoons van de doelgroepen waarop de dienstverlening van UWV zich richt.

Voor deze aanbesteding zijn waarschijnlijk de volgende standaarden relevant:

- DNSSEC voor een geldige ondertekening van de domeinnaam van het ICT systeem;
- HTTPS en HSTS; voor een beveiligde verbinding voor het webportaal;
- TLS; voor versleuteling van verbindingen;
- PDF; omdat er niet-reviseerbare rapportages worden gevraagd;
- ISO 27007/27002; De leverancier is immers de spil in het communicatienetwerk van UWV.
- IPv4 en IPv6; want het gaat om internet gebaseerde koppelvlakken
- SAML, vanwege single-sign-on mogelijkheid
- DKIM, DMARC, SPF, want het betreft inkomend en uitgaand e-mailverkeer;
- STARTTLS & DANE, want het gaat hier om een ontvangende en verzendende e-mailserver;

###### Toelichting

Waar het gaat om (hardware bevattende) software ten behoeve van spraak en/of datacommunicatie, zijn meerdere standaarden relevant uit het cluster “Internet en beveiliging”. Daarbij kan gedacht worden aan de inkoop van Voice over IP diensten (internetbellen), maar ook aan smartphones of tablets waarmee verbinding kan worden gemaakt met het internet.

WPA2 Enterprise maakt het bijvoorbeeld mogelijk dat gebruikers automatisch en veilig toegang krijgen tot aangesloten WiFi-netwerken. Ook als deze WiFi-netwerken zich buiten de eigen organisatie bevinden. De authenticatie vindt plaats op basis van bestaande identiteitsgegevens van de gebruiker, hierdoor hoeven gebruikers niet opnieuw in te loggen. Met het gebruik van WPA2 Enterprise is ook de integriteit van de netwerkverbinding geborgd.

En omdat er bij dit soort diensten vrijwel altijd sprake is van (vertrouwelijke) gegevensverwerking door een leverancier, is de eis om ISO 27001/27002 hier ook absoluut noodzakelijk.

**Luchtverkeersleiding Nederland spraakdiensten**

Luchtverkeersleiding Nederland wil in 2019 een overeenkomst sluiten met een telecomprovider voor het leveren, onderhouden en verder evolueren van vaste spraakdiensten, gekoppeld aan telefonie platformen zoals deze in gebruik zijn binnen LVNL. Het betreft hier met name SIP-trunk dienstverlening op diverse LVNL locaties in Nederland. Er wordt ook een webportaal geëist waarmee LVNL zelf de configuratie kan instellen.

Voor deze aanbesteding zijn waarschijnlijk de volgende standaarden relevant:

- IPv6 & IPv4, want SIP is een VoIP technologie;
- HTTPS en HSTS, voor een beveiligde verbinding voor het webportaal;
- TLS, voor versleuteling van verbindingen;
- PDF, omdat er niet-reviseerbare rapportages worden gevraagd;
- ISO 27001 / ISO 27002. De leverancier is immers de spil in het communicatienetwerk van LVNL.

###### Toelichting

Waar het gaat om (hardware bevattende) software ten behoeve van spraak en/of datacommunicatie, zijn meerdere standaarden relevant uit het cluster “Internet en beveiliging”. Daarbij kan gedacht worden aan de inkoop van Voice over IP diensten (internetbellen), maar ook aan smartphones of tablets waarmee verbinding kan worden gemaakt met het internet.

WPA2 Enterprise maakt het bijvoorbeeld mogelijk dat gebruikers automatisch en veilig toegang krijgen tot aangesloten WiFi-netwerken. Ook als deze WiFi-netwerken zich buiten de eigen organisatie bevinden. De authenticatie vindt plaats op basis van bestaande identiteitsgegevens van de gebruiker, hierdoor hoeven gebruikers niet opnieuw in te loggen. Met het gebruik van WPA2 Enterprise is ook de integriteit van de netwerkverbinding geborgd.

En omdat er bij dit soort diensten vrijwel altijd sprake is van (vertrouwelijke) gegevensverwerking door een leverancier, is de eis om ISO 27001/27002 hier ook absoluut noodzakelijk.

2.6 Multifunctionals

## 2.6 Multifunctionals

Leveren, servicen en onderhouden multifunctionals en repromachine

- Aanbestedingsnummer: 240946
- TenderNed: Leveren, servicen en onderhoud multifunctional
- Opdrachtgever: Gemeente Den Helder

De Gemeente Den Helder vraagt in 2021 om het leveren, servicen en onderhouden van multifunctionals en repromachines. De gemeente wenst de apparatuur te huren. Deze opdracht bestaat uit diverse “fases” waarin door o.a. wijzigingen t.a.v. de huisvesting de behoefte wijzigt.

Niet limitatief zijn bij een dergelijke aanbesteding de volgende standaarden relevant:

- PDF;  omdat de printbestanden soms in een niet te reviseren formaat geleverd worden;
- TLS;  versleuteling van verbindingen tussen de printers en andere netwerkcomponenten;
- IPv4 en IPv6; vanwege het gebruik van IP-reeksen;
- HTTPS, omdat de software met behulp van een webbrowser benaderbaar moet zijn.
- ODF; want het betreft het afdrukken van reviseerbare documenten en rapportages;
- ISO 27001/27002; vanwege informatieveiligheid;

###### Toelichting

Waar het gaat om (hardware bevattende) software ten behoeve van, of om te gebruiken op werkplekken, zijn meerdere standaarden relevant uit de clusters “Internet en beveiliging” en “Documenten en webcontent”. Zo maakt een 'multifunctional' in veel gevallen verbinding via een (inter)netwerk waardoor bijvoorbeeld versleuteling via TLS en bereikbaarheid via IPv6 belangrijk is; Maar ook moet het in staat zijn om ODF-documenten te verwerken, en indien de 'multifunctional' ook gebruikt kan worden om mee te scannen dan moet er de mogelijkheid zijn voor een output in het pdf formaat. Indien het mogelijk is om vanuit de 'multifunctional' te e-mailen, dan dienen ook de beveiligingstandaarden uit de inkoopcategorie “email” hier geëist te worden. Indien de leverancier van de multifunctional ook dient te voorzien in onderhoud en beheer, dan is het noodzakelijk om de ISO 27001 / 27002 eis te stellen aan de organisatie van de leverancier.

**IUC-Noord fullcolour rolprint oplossing**

IUC-Noord vraagt in 2019 in een aanbesteding om het leveren, installeren en onderhouden van een 'fullcolour' hoog volume 'rolprint' oplossing en bijbehorende randapparatuur. Niet limitatief zijn de volgende standaarden relevant:

- ISO 27001 / ISO 27002, vanwege informatieveiligheid;
- PDF, omdat de printbestanden soms in een niet te reviseren formaat geleverd worden;
- TLS, voor versleuteling van verbindingen tussen de printers en andere netwerkcomponenten;
- OpenAPI Specification, vanwege de wens om documentatie waarin de koppelvlakken/interfaces tot in detail beschreven staan.

###### Toelichting

Waar het gaat om (hardware bevattende) software ten behoeve van, of om te gebruiken op werkplekken, zijn meerdere standaarden relevant uit de clusters “Internet en beveiliging” en “Documenten en webcontent”. Zo maakt een 'multifunctional' in veel gevallen verbinding via een (inter)netwerk waardoor bijvoorbeeld versleuteling via TLS en bereikbaarheid via IPv6 belangrijk is; Maar ook moet het in staat zijn om ODF-documenten te verwerken, en indien de 'multifunctional' ook gebruikt kan worden om mee te scannen dan moet er de mogelijkheid zijn voor een output in het pdf formaat. Indien het mogelijk is om vanuit de 'multifunctional' te e-mailen, dan dienen ook de beveiligingstandaarden uit de inkoopcategorie “email” hier geëist te worden.

2.7 Financieël/ administratieve systemen

## 2.7 Financieel/ administratieve systemen

**Financieel systeem gemeente 's-Hertogenbosch**

- Aanbestedingsnummer: 245083
- TenderNed: Financieel systeem 's Hertogenbosch
- Opdrachtgever: gemeente 's-Hertogenbosch

De gemeente 's-Hertogenbosch wil met haar financiële beleid ervoor zorgen dat er een financieel gezonde organisatie is die de dienstverlening aan haar burgers en bedrijven in stand kan houden. De gemeente 's-Hertogenbosch zoekt hiervoor een nieuw financieel systeem. Het nieuwe systeem moet de medewerkers, zowel de financiële medewerkers als de niet financiële medewerkers, ondersteunen in de rechtmatige, juist en volledige uitvoering van de werkzaamheden.
In het aanbestedingsdocument stelt de gemeente als eis dat gegevensuitwisseling en koppelingen met andere applicaties zijn ingericht overeenkomstig hetgeen is beschreven bij de technische architectuur / koppelingen in het aanbestedingsdocument. In dat document zijn diverse open standaarden opgenomen.

Standaarden die waarschijnlijk relevant zijn:

- SAML; want er is sprake van single sign on.
- OpenAPI: want er is sprake van te beschrijven koppelvlakken op basis van REST API's.
- PDF; want het betreft niet-reviseerbare documenten en archivering;
- HTTPS, HSTS en TLS want het betreft een webportaal;
- ISO 27001/27002 vanwege de beveiliging van persoonsgegevens;
- ODF; want het betreft het opstellen van documenten en rapportages;
- DMARC, SPF en DKIM; want het betreft inkomend en uitgaand e-mailverkeer.

##### Toelichting

Waar het gaat om software ten behoeve van, of om te gebruiken als financieel/administratieve systemen, zijn meerdere standaarden relevant uit de domeinen "Internet en beveiliging", "Documenten en webcontent" en "E-facturatie en administratie". De internet en beveiligingstandaarden zijn bijvoorbeeld relevant indien het financieel/administratieve systeem benaderbaar wordt via het internet. Ook dient het in geval van rapportages mogelijk te zijn om de output te krijgen in ODF.

NLCIUS geeft duidelijkheid aan overheden en bedrijven over de elementen en gegevens die op facturen naar overheidsorganisaties gebruikt dienen te worden in Nederland.

**Applicatie subsidieproces**

ZonMw financiert gezondheidsonderzoek. Het doel van de nieuwe applicatie die zij aanbesteden in 2017 is om het subsidieproces te faciliteren en te ondersteunen. Middels het portaal, kunnen organisaties, externen (beoordelaars) en individuele aanvragers het traject van aanvraag tot en met de vaststelling van de subsidie (inclusief de verantwoording) volledig digitaal afhandelen. Intern binnen ZonMw wordt de subsidieaanvraag verder verwerkt en beoordeeld in het te verwerven pakket.

Standaarden die waarschijnlijk relevant zijn:

- XBRL, want het betreft rapportages met een financiële component en gegevensuitwisseling met een financieel systeem;
- HTTPS en HSTS & TLS, want het betreft een webportaal;
- ISO 27001 / ISO 27002, vanwege de beveiliging van persoonsgegevens;
- ODF, want het betreft het opstellen van documenten en rapportages;
- PDF, want het betreft niet-reviseerbare documenten en archivering;
- SAML, want door middel van inloggen moet een indiener zijn aanvraag. kunnen opstellen, indienen, aanpassen en intrekken;
- Digitoegankelijk, want het een betreft een portaal voor burgers en bedrijven;
- DMARC, SPF en DKIM, want het betreft inkomend en uitgaand e-mailverkeer.

##### Toelichting

Waar het gaat om software ten behoeve van, of om te gebruiken als financieel/administratieve systemen, zijn meerdere standaarden relevant uit de domeinen "Internet en beveiliging", "Documenten en webcontent" en "E-facturatie en administratie". De internet en beveiligingstandaarden zijn bijvoorbeeld relevant indien het financieel/administratieve systeem benaderbaar wordt via het internet. Ook dient het in geval van rapportages mogelijk te zijn om de output te krijgen in ODF.

NLCIUS geeft duidelijkheid aan overheden en bedrijven over de elementen en gegevens die op facturen naar overheidsorganisaties gebruikt dienen te worden in Nederland.

2.8 E-HRM-systemen

### 2.8 Voorbeeld: E-HRM-systemen

e-HRM systeem t.b.v. gemeente Gorinchem

- Aanbestedingsnummer: 220465
- Opdrachtgever: Gemeente Gorinchem
- TenderNed: E-HRM-systemen

De gemeente Gorinchem doet een aanbesteding voor de levering, inrichting en beheren van een nieuw e-HRM systeem (SaaS-oplossing) . Daarbij wenst de gemeente de volledige ondersteuning bij de implementatie en de koppelingen met omringende applicaties.

De leverancier moet kunnen voldoen aan de volgende standaarden:

- ISO 27001/27002; voor informatie-veiligheid van o.a. persoonsgegevens;
- SAML; want er is sprake van uitwisseling van autorisatie en authenticatiegegevens;
- HTTPS, HSTS en TLS; voor beveiliging portals en websites;
- DNSSEC; voor beveiliging van webverkeer.
- IPv4 en IPv6; want het gaat om internet gebaseerde koppelvlakken
- DKIM, DMARC, SPF, want het betreft inkomend en uitgaand e-mailverkeer;
- STARTTLS & DANE, want het gaat hier om een ontvangende en verzendende e-mailserver;
- PDF, voor het genereren van rapporten.

Aanvullend geeft de gemeente ook nog aan dat de opdrachtnemer ervoor dient te zorgen dat zijn oplossing en de geleverde koppelingen voldoen aan de pas-toe-of-leg-uit lijst van Open Standaarden van het Forum Standaardisatie.

##### Toelichting

Waar het gaat om e-HRM systemen, zijn meerdere standaarden relevant uit de domeinen "Internet en beveiliging", "onderwijs en loopbaan" en "Documenten en webcontent". Zo zijn e-HRM systemen vaak benaderbaar via het internet, waardoor vrijwel alle standaarden die voorkomen bij de inkoopcategorie "website of webapplicatie" ook in dit geval relevant zijn. Denk daarbij niet alleen aan beveiliging, maar ook aan Digitoegankelijk en -voor het kunnen inloggen- aan SAML.

Binnen het domein "onderwijs en loopbaan" kan gedacht worden aan e-Portfolio. Met E-portfolio NL kunnen de competenties van een individu worden bijgehouden. Het voordeel van deze standaard is dat de student/lerende medewerker zijn profiel mee kan nemen naar verschillende organisaties.

Binnen "Documenten en webcontent" kan worden gedacht aan ODF of PDF, bijvoorbeeld omdat er vanuit de systemen rapportages uitgedraaid moeten kunnen worden.

**Nederlandse Zoregautoriteit SaaS oplossing**

De Nederlandse Zorgautoriteit zoekt in 2018 een partij voor het leveren van een integrale SaaS oplossing voor de HRM en F&C processen waarbij de salaris administratie/-verwerking als dienstverlening wordt aangeboden, waarmee de beschreven gebruikersproblemen worden verholpen en waardoor de opdrachtgever goede en efficiënte dienstverlening kan leveren aan haar medewerkers. Er moeten ook koppelingen komen met andere oplossingen van externe partijen en er moet data van de oude naar de nieuwe omgeving worden gemigreerd.

De volgende standaarden zijn hier waarschijnlijk relevant:

- e-Portfolio, want het gaat hier om een e-HRM systeem waarin ook het HRM proces "Talent management" is opgenomen;
- ISO 27001 / ISO 27002, voor informatie-veiligheid van o.a. persoonsgegevens;
- SAML, want single sign on functionaliteit gevraagd;
- HTTPS en HSTS en TLS, voor beveiliging portals en websites;
- DNSSEC, voor beveiliging van webverkeer.
- XBRL, voor uitwisseling van documenten met financiële informatie d.m.v. gelegde koppelingen;
- ODF en PDF, voor het genereren van rapporten.

##### Toelichting

Waar het gaat om e-HRM systemen, zijn meerdere standaarden relevant uit de domeinen "Internet en beveiliging", "onderwijs en loopbaan" en "Documenten en webcontent". Zo zijn e-HRM

systemen vaak benaderbaar via het internet, waardoor vrijwel alle standaarden die voorkomen bij de inkoopcategorie “website of webapplicatie” ook in dit geval relevant zijn. Denk daarbij niet alleen aan beveiliging, maar ook aan Digitoegankelijk en -voor het kunnen inloggen- aan SAML.

Binnen het domein “onderwijs en loopbaan” kan gedacht worden aan e-Portfolio. Met E-portfolio NL kunnen de competenties van een individu worden bijgehouden. Het voordeel van deze standaard is dat de student/lerende medewerker zijn profiel mee kan nemen naar verschillende organisaties.

Binnen “Documenten en webcontent” kan worden gedacht aan ODF of PDF, bijvoorbeeld omdat er vanuit de systemen rapportages uitgedraaid moeten kunnen worden.

2.9 Netwerken

## 2.9 Voorbeeld: netwerken

#### Netwerkinfrastructuur 2021

Aanbestedingsnummer: 230878

Opdrachtgever: Gemeente Zoetermeer

TenderNed: Netwerkinfrastructuur 2021

De gemeente Zoetermeer vraagt in 2021 het volgende uit:

- Een nieuwe LAN infrastructuur gecombineerd met een Wifi-oplossing.
- Integraal management en oplossing aangeboden als dienst.
- Een nieuwe firewall oplossing, aangeboden als beheerde dienst in combinatie met een microsegmentatie implementatie en een Zero Trust strategie.

Het geheel moet integreren met bestaande onderdelen van de huidige infrastructuur.

In deze aanbesteding zijn de volgende standaarden waarschijnlijk relevant:

- ISO 27001/27002; vanwege informatieveiligheid;

- DNSSEC; vanwege een beveiligde DNS;
- IPv4 en IPv6; vanwege het gebruik van IP-reeksen;
- HTTPS, HSTS en TLS; voor een beveiligde verbinding met internet.
- OpenAPI; e aangeboden oplossing moet voor integratie met andere tools of services open API’s ondersteunen.
- WPA2 Enterprise, vanwege de toegang tot het Wifi-netwerk.

##### Toelichting

Waar het gaat om software ten behoeve van, of om te gebruiken in netwerken zijn meerdere standaarden relevant uit het cluster “Internet en beveiliging”. Hier is de eis om ondersteuning van IPv6 in combinatie met IPv4 (duall stack) absoluut noodzakelijk. IPv6 is niet 'backwards compatible'. Dit wil zeggen dat een IPv4-systeem niet een IPv6-systeem kan bereiken, of andersom. Om die reden moet een organisatie bij de aanschaf van een ICT-product/-dienst beide versies uitvragen.

En aangezien via de netwerkdiensten vrijwel altijd persoonsgegevens verwerkt kunnen worden, ligt ook een ISO 27001/27002 eis voor de hand. Het is overigens niet nodig om deze ISO-standaarden bij alle inkopen van ICT-producten en diensten te vereisen. Inkopende organisaties dienen zelf, ten aanzien van een specifieke aanschaf, risico-gebaseerd te bepalen of zij de naleving van deze standaarden van hun leverancier vereisen, mede op basis van de eigen intern geldende baseline informatiebeveiliging. In de communicatie dient helder te zijn dat niet beoogd wordt om in alle gevallen van toepassing van deze standaarden certificering van de leverancier te eisen; in eerste instantie kan naleving van de standaarden vereist worden en daarna, voor zover opportuun voor de inkopende organisatie in het specifieke geval, kan certificering van de leverancier vereist worden.

#### RDW Wifi dienstverlening

De RDW heeft besloten de complete Wifi dienstverlening extern af te nemen zodanig dat Wifi op alle RDW-locaties in Nederland als een managed service wordt aangeboden. In 2018 publiceren zij hiervoor een aanbesteding. Onderdeel van deze aanbesteding is een volledige dienst die 'end-2-end' de gewenste functionaliteit levert, inclusief de complete installatie, implementatie en onderhoud & support. Ook gasten maken hier gebruik van. De opdracht bestaat uit levering van apparatuur t.b.v. wifi dienstverlening, implementatie en installatie van apparatuur en dienst, beheer & support van apparatuur en dienst, en internetconnectiviteit incl. DNS en DHCP.

In deze aanbesteding eist de RDW in ieder geval de volgende twee standaarden:

- ISO 27001 / ISO 27002, vanwege informatieveiligheid;
- WPA2 Enterprise, vanwege de toegang tot het Wifi-netwerk.

De volgende standaarden hadden echter ook gevraagd kunnen worden:

- DNSSEC, vanwege een beveiligde DNS;
- IPv6 & IPv4, vanwege het gebruik van IP-reeksen;
- HTTPS en HSTS en TLS, voor een beveiligde verbinding met internet.

##### Toelichting

Waar het gaat om software ten behoeve van, of om te gebruiken in netwerken zijn meerdere standaarden relevant uit het cluster “Internet en beveiliging”. Hier is de eis om ondersteuning van IPv6 in combinatie met IPv4 (duall stack) absoluut noodzakelijk. IPv6 is niet 'backwards compatible'. Dit wil zeggen dat een IPv4-systeem niet een IPv6-systeem kan bereiken, of andersom. Om die reden moet een organisatie bij de aanschaf van een ICT-product/-dienst beide versies uitvragen.

En aangezien via de netwerkdiensten vrijwel altijd persoonsgegevens verwerkt kunnen worden, ligt ook een ISO 27001/27002 eis voor de hand. Het is overigens niet nodig om deze ISO-standaarden bij alle inkopen van ICT-producten en diensten te vereisen. Inkopende organisaties dienen zelf, ten aanzien van een specifieke aanschaf, risico-gebaseerd te bepalen of zij de naleving van deze standaarden van hun leverancier vereisen, mede op basis van de eigen intern geldende baseline informatiebeveiliging. In de communicatie dient helder te zijn dat niet beoogd wordt om in alle gevallen van toepassing van deze standaarden certificering van de leverancier te eisen; in eerste instantie kan naleving van de standaarden vereist worden en daarna, voor zover opportuun voor de inkopende organisatie in het specifieke geval, kan certificering van de leverancier vereist worden.

2.10 Basisregistraties/ overheidsgegevens

## 2.10 Basisregistraties/ overheidsgegevens

#### Burgerzaken applicatie

- Aanbestedingsnummer: 223407
- TenderNed: Burgerzaken applicatie
- Opdrachtgever: gemeente Nijmegen

In 2021 doet de gemeente Nijmegen een aanbesteding voor de levering en implementatie van een burgerzakenapplicatie. In het Programma van Eisen zijn de volgende standaarden geëist:

- PDF; documenten die moeten worden omgezet naar een niet-reviseerbaar formaat; In dit specifiek geval moeten er managementrapportages geëxporteerd kunnen worden naar diverse formaten.
- DMARC, SPF, DKIM en DANE; vanwege een email mogelijkheid.
- StUF; voor uitwisseling gegevens uit de basisregistraties;
- ISO 27001/27002; relevant m.b.t. informatiebeveiliging;
- Digitoegankelijk; want het betreft o.a. een webapplicatie;

Waarschijnlijk zijn ook de volgende standaarden relevant:

- SAML; voor authenticatie bij inloggen.
- HTTPS, HSTS en TLS voor het tot stand komen van veilig webverkeer;
- DNSSEC; voor de domeinnaam van de webapplicatie;

In het bestek kiest deze organisatie ervoor om met betrekking tot beveiligingstandaarden de volgende eis te stellen: “
De software waarmee de dienst is geïmplementeerd, is volgens relevante standaarden beveiligd, conformeert zich telkens aan de laatst bekende beveiligingsinzichten en is blijvend van voldoende kwaliteit. Richtlijnen van de Autoriteit Persoonsgegevens (AP), Nationaal Cyber Security Centrum (NCSC), Informatiebeveiligingsdienst voor gemeenten (IBD), Forum Standaardisatie en Open Web Application Security Project (OWASP) zijn hierbij normstellend.”

#### Toelichting

Waar het gaat om software en informatiesystemen ten behoeve van basisregistraties en ten behoeve van het registreren en uitwisselen van informatie met een geografische component, zijn meerdere standaarden relevant uit de clusters “stelselstandaarden” en “Water en bodem”. StUF is bijvoorbeeld een universele berichtenstandaard voor het elektronisch uitwisselen van gegevens tussen applicaties. Het domein van de StUF-taal omvat informatieketens tussen overheidsorganisaties (basisregistraties en landelijke voorzieningen) en gemeentebrede informatieketens en -functionaliteit. StUF is beschreven in XML en gebaseerd op geaccepteerde internetstandaarden. Digikoppeling is van toepassing bij aanschaf of ontwikkeling van systemen bedoeld voor gestructureerde berichtenuitwisseling met voorzieningen zoals de basisregistraties en berichtverkeer dat sectoroverstijgend is. Indien het ICT-systeem een rapportagemogelijkheid moet hebben, dient ook gedacht te worden aan standaarden uit het cluster “ Documenten en webcontent” zoals ODF of PDF.

#### Zaakgericht werken systeem

Het Ministerie van Sociale Zaken en Werkgelegenheid doet in 2018 een aanbestedingvoor een zaakgericht werken systeem die de processen van de afdeling CAV kan ondersteunen. Om hun taken op het gebied van Cao-aanmelding, AVV en Pensioenen uit te kunnen voeren maakt de afdeling gebruik van applicaties die het eind van hun levensduur hebben bereikt en dienen te worden vervangen. De opdracht bestaat uit het beheren en (door)ontwikkelen van een website, de aanschaf van een licentie voor een zaakgericht werken systeem, en het beheren, onderhouden en doorontwikkelen van dat systeem. Het systeem bevat tevens een e-mailfunctionaliteit.

Waarschijnlijk zijn de volgende standaarden relevant:

- StUF, voor uitwisseling gegevens uit de basisregistraties;
- ISO 27001 / ISO 27002, m.b.t. informatiebeveiliging;
- DNSSEC, voor domeinnaam voor website/webportaal;
- SAML, voor authenticatie bij inloggen.
- Digitoegankelijk, want het betreft o.a. een webapplicatie;
- HTTPS en HSTS en TLS, voor het tot stand komen van veilig webverkeer;
- PDF, voor documenten die moeten worden omgezet naar een niet-reviseerbaar formaat;
- DMARC, SPF en DKIM, vanwege een email mogelijkheid.

#### Toelichting

Men spreekt in dit bestek bovendien de wens uit om maximaal gebruik te maken van open standaarden en daarbij wordt verwezen naar Forum Standaardisatie en de ‘pas toe of leg uit’-lijst.

Waar het gaat om software en informatiesystemen ten behoeve van basisregistraties en ten behoeve van het registreren en uitwisselen van informatie met een geografische component, zijn meerdere standaarden relevant uit de clusters “stelselstandaarden” en “Water en bodem”. StUF is bijvoorbeeld een universele berichtenstandaard voor het elektronisch uitwisselen van gegevens tussen applicaties. Het domein van de StUF-taal omvat informatieketens tussen overheidsorganisaties (basisregistraties en landelijke voorzieningen) en gemeentebrede informatieketens en -functionaliteit. StUF is beschreven in XML en gebaseerd op geaccepteerde internetstandaarden. Digikoppeling is van toepassing bij aanschaf of ontwikkeling van systemen bedoeld voor gestructureerde berichtenuitwisseling met voorzieningen zoals de basisregistraties en berichtverkeer dat sectoroverstijgend is. Indien het ICT-systeem een rapportagemogelijkheid moet hebben, dient ook gedacht te worden aan standaarden uit het cluster “ Documenten en webcontent” zoals ODF of PDF.

2.11 Inhuur

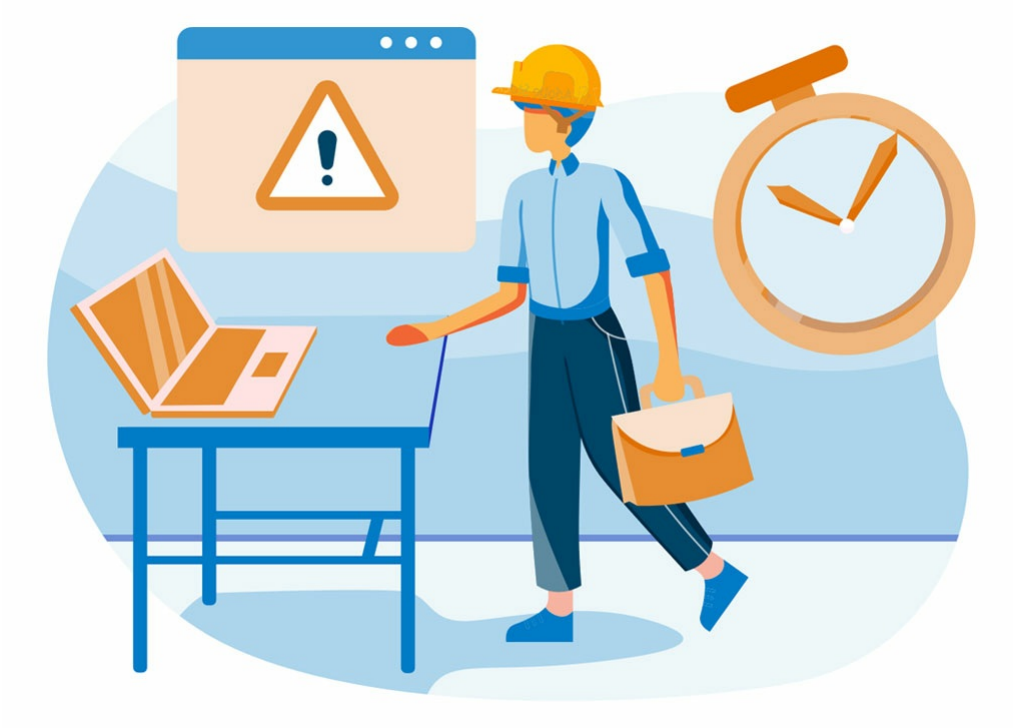
## 2.11 Inhuur

De Belastingdienst deed in 2017 een aanbesteding voor het leveren van een Rijksbrede HR werving & selectie oplossing ter ondersteuning van in-, door- en uitstroom van medewerkers van het Rijk en Defensie. De oplossing dient geleverd te worden als SaaS (Software as a Service).

SETU was hierbij expliciet als eis in het bestek opgenomen aangezien er sprake is van berichtenuitwisseling rondom flexibele arbeidskrachten.

In de aanbesteding waren waarschijnlijk meerdere standaarden uit het cluster “Internet en beveiliging” , “Documenten en webcontent”, en uit het cluster “onderwijs en loopbaan” van belang:

- HTTPS en HSTS & TLS, want de toegang tot het systeem gaat volledig via een web browser;
- ISO 27001 / ISO 27002, want het SaaS systeem bevat te beschermen persoonsgegevens;
- SAML, want er wordt in het bestek gesproken over single sign on;
- DNSSEC, want het SaaS systeem is bereikbaar via een domeinnaam;
- Digitoegankelijk, want er is ook sprake van interactie via een webportaal voor burgers;
- ODF en PDF, want het systeem moet kunnen omgaan met reviseerbare en niet-reviseerbare documenten;
- STARTTLS & DANE, SPF en DKIM, want het betreft inkomend en uitgaand e-mailverkeer;
- ePortfolio, want het betreft uitwisseling van gegevens over werkervaring en competenties.



## 3. Bestekteksten

Hieronder leest u voorbeeld-bestekteksten voor inkopers van overheidsorganisaties. De teksten dienen op maat gemaakt te worden voor de betreffende opdracht van de aanbestedende dienst. Hierbij moeten de algemene uitgangspunten van AW2012 (met name het beginsel van proportionaliteit) toegepast worden.

Om die reden zijn er geen bedragen, aantallen, jaartallen en dergelijke opgenomen in de teksten maar wel het in te vullen veld [x]. Ook andere velden die nog ingevuld moeten worden zijn op die wijze gemarkeerd, bijvoorbeeld [naam standaard]. Daarnaast is in de voorbeeld- bestekteksten rekening gehouden met twee mogelijke aanbestedingsprocedures: 'niet-openbaar' waarbij er sprake is van een gegadigde en 'openbaar' waarbij er sprake is van een inschrijver.

Om de eisen en wensen met betrekking tot standaarden in een kader te plaatsen kan de aanbestedende dienst onderstaande toelichtende teksten opnemen:

Algemene bestekteksten

| | **Bestektekst** |
|---|---|
| Open Standaarden | [Aanbestedende dienst] wil graag dat de dienst of product, conform het open- standaardenbeleid van de Nederlandse overheid, werkt op basis van open standaarden met als achterliggende doelen de bevordering van de interoperabiliteit en de vergroting van de leveranciersonafhankelijkheid. |
| Verwijzing naar verplichte Open Standaarden | [Aanbestedende dienst] verwijst in de specificatie van de dienst of product expliciet naar de relevante, verplichte open standaarden die op de pas toe of leg uit'-lijst van Forum Standaardisatie staan. |
| Beoordeling 'of gelijkwaardig' | Mocht de inschrijver/gegadigde een 'gelijkwaardige' standaard aanbieden, dan dient deze aan te tonen dat dit alternatief voldoet aan de door het Forum Standaardisatie gehanteerde en gepubliceerde criteria voor opname op de 'pas toe of leg uit'-lijst, zodat interoperabiliteit en leveranciersonafhankelijkheid in voldoende mate voor de [<br>aanbestedende dienst<br>] zijn gewaarborgd. |
| Garanties naar de toekomst | In het kader van Preventief en/of Innovatief Onderhoud garandeert inschrijver/gegadigde ten minste:<br>1. dat de dienst of het product steeds tijdig zal blijven voldoen aan de relevante Wet- en regelgeving;<br>2. dat de dienst of het product steeds tijdig geschikt zal blijven voor gegevensuitwisseling met de overige relevante onderdelen van het applicatielandschap (voor zover bekend bij inschrijver/gegadigde) en in dat kader aan de overeengekomen interoperabiliteitseisen zal blijven voldoen;<br>3. dat de dienst of het product door middel van het tijdig uitbrengen van updates en/of upgrades steeds tijdig zal blijven voldoen aan nieuwe versies van de relevante open standaarden die in de Overeenkomst als vereiste normen zijn gespecificeerd; |

### 3.1 Geschiktheidseisen

Onderstaande geschiktheidseisen kan een aanbestedende dienst hanteren om de geschiktheid en bekwaamheid van een leverancier met de desbetreffende relevante open standaard te kunnen beoordelen.

Kerncompetentie Ervaring

| | **Kerncompetentie Ervaring** |
|---|---|
| **Bestektekst** | De [gegadigde/inschrijver]dient aan te tonen dat hij in de afgelopen [<br>x<br>] jaar ervaring heeft opgedaan met het succesvol implementeren van ICT-systemen, die gegevens uitwisselen conform de open standaard [naam standaard] zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. Om aan te tonen dat [gegadigde/inschrijver] voldoet aan deze kerncompetentie dient u bij [het verzoek tot deelneming/de inschrijving] [x] relevante referentie[s] op te geven waaruit blijkt dat [gegadigde/inschrijver] voldoende ervaring heeft met betrekking tot deze kerncompetentie. |
| **Doel en toelichting** | Inzicht in de aantoonbare ervaring van de gegadigde/inschrijver met de gevraagde open standaard. De vraag kan verder worden gespecificeerd door in deze eis een specifiek ICT-systeem te noemen. Deze eis, de vraag naar referenties, kan eventueel worden ingepast in de andere referentie-eisen. |

Bekwaamheid

| | **Bekwaamheid** |
|---|---|
| **Bestektekst** | De [gegadigde/inschrijver] geeft een duidelijk inzicht in het kwaliteitsniveau en de beschikbaarheid van zijn personeel dat de [gegadigde/inschrijver] voornemens is in te zetten bij de implementatie van het ICT-systeem dat gegevens uitwisselt conform de open standaard [naam standaard] zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig.<br><br>De [gegadigde/inschrijver] overlegt daartoe een overzicht van minimaal [x] medewerkers en hun CV's en opleidingscertificaten waarover [gegadigde/inschrijver] kan beschikken waaruit hun ervaring met en kennis van [naam standaard] duidelijk blijkt. |
| **Doel en toelichting** | Inzicht in bekwaamheid van het in te zetten personeel. Voor diverse open standaarden bestaan er opleidingstrajecten. Deze kunnen worden aangeboden door leveranciers en door onafhankelijke onderwijsinstellingen. |

### 3.2 Selectiemethode

Doorgaans is de mate van ervaring (bijv. het meer of minder vaak een open standaard in een ICT-product of dienstverlening toegepast hebben) geen adequate geschiktheidseis, ook niet vanuit het oogpunt van proportionaliteit. Het is in veel gevallen beter om uit te gaan van de hiervoor beschreven knock-out geschiktheidseisen. Om die reden zijn er geen voorbeeld-bestekteksten voor selectiecriteria opgenomen. Dat laat onverlet dat het in specifieke gevallen toch passend kan zijn om een geschiktheidseis voor een open standaard op te nemen. Het is

aan de aanbestedende  dienst om dat te bepalen.

### 3.3 Open standaarden als technische specificatie

Het opnemen van een open standaard in een bestektekst kwalificeert in aanbestedingsrechtelijke termen als het verwijzen naar technische specificaties conform artikel 2.76 van de Aanbestedingswet 2012. Een dergelijke verwijzing is in principe toegestaan. Uiteraard mag deze niet strijdig zijn met de beginselen van de AW2012. Dat betekent onder andere dat deze specificatie objectief toepasbaar en niet discriminatoir mag zijn. De wet schrijft wel voor dat de aanbestedende partij de zinsnede “of gelijkwaardig” toevoegt aan de formulering van de technische specificatie. Het is daarbij van belang dat de aanbestedende dienst aangeeft hoe de gelijkwaardigheid aangetoond moet worden met passende middelen door de leverancier die hier een beroep op doet. De aanbestedende dienst kan hiervoor de toetsingscriteria voor opname op de ‘pas toe of leg uit’-lijst hanteren en daarbij verwijzen naar achterliggende doelen van interoperabiliteit en leveranciersonafhankelijkheid. Indien geen criteria opgenomen worden, is een gegadigde/inschrijver vrij in de methode om zelf aan te tonen of de alternatieve standaard ‘gelijkwaardig’ is. Omdat een open standaard door alle leveranciers te implementeren is, werkt deze in principe niet discriminerend. Toch kan er in gevallen sprake zijn van alternatieven die ook in de behoeften voorzien. Zo kan een nieuwere versie van een standaard uit de ‘pas toe of leg uit’-lijst interoperabel zijn met hetgeen wordt gevraagd. Zoals eerder beschreven, zijn open standaarden op zichzelf niet in strijd met deze algemene beginselen van mededinging. Gelet op het voorgaande is het bij verwijzing naar een open standaard aan te raden om:

1. De achterliggende ratio, namelijk vergroten van interoperabiliteit én bevorderen van leveranciersonafhankelijkheid, te vermelden.
2. Te vermelden dat de gevraagde standaard is opgenomen op de ‘pas toe of leg uit’-lijst en dat eventueel aangeboden ‘gelijkwaardige’ standaarden ook aan de toetsingscriteria van het Forum Standaardisatie moeten voldoen.

## 4. Bestekteksten, specifiek per standaard

De lijst hieronder toont voor een paar ‘pas toe of leg uit’-standaarden voorbeelden voor gunningseisen (Eis) en gunningscriteria (Wens). Een verkorte omschrijving van de toepassing op basis van het formele toepassingsgebied op de ‘pas toe of leg uit’-lijst. Indien er twee toepassingen zijn, is er een sjabloon per toepassing en wordt de nummering van Toepassing 1, Toepassing 2 etc. aangehouden.

Begrippen

| Begrip | Toelichting |
|---|---|
| Volledige naam | De volledige naam van de open standaard, inclusief eventuele actuele versie. |
| Standaardisatie-organisatie | De naam van de organisatie die de open standaard beheert. |
| Specificatie-document | De online vindplaats (URL) waar het specificatiedocument van de open standaard beschikbaar is. Omwille van de transparantie en de objectiviteit is het aan te raden om in een bestek deze vindplaats ook op te nemen. |
| ICT-diensten of producten | De categorie uit hoofdstuk 4 waarbij de standaard vaak relevant is. |

Onderdelen bestekteksten

| Onderdeel | Toelichting |
|---|---|
| Eis | De gunningseis die gesteld kan worden aan de te leveren dienst of product. |
| Verificatie van de eis | De wijze van verificatie van deze gunningseis. |
| Wens | De mogelijkheid om bovenop de eis een wens te formuleren die een onderdeel van de EMVI-gunning kan zijn; indien een wens op dat gebied doorgaans niet passend is, dan is in het sjabloon ‘Geen’ opgenomen. |
| Beoordeling wens | De wijze van beoordeling en verificatie van de reactie van de inschrijver op de wens. |
| Opmerkingen | Eventuele aanvullende opmerkingen ten behoeve van de voorbeeld-bestekteksten. |

### 4.1 Internet en beveiliging

IPv4 & IPv6 (Internetnummers) voor servers

Toepassing: bereikbaarheid van ICT-systemen, zoals websites, e-mailsystemen en DNS-systemen.

Volledige naam: Internet Protocol versie 6 en 4 (RFC2460 en RFC791) Standaardisatie-organisatie: IETF Specificatie-documenthttps://tools.ietf.org/html/rfc2460 https://tools.ietf.org/html/rfc791

Voorbeeld van relevante ICT-diensten of producten:

- Website of webapplicatie
- E-mail
- Spraak- en/of datacommunicatiediensten
- Netwerken

En alle overige aan internet te koppelen ICT-systemen, zoals 'multifunctional'.

| Bestekonderdeel | Voorbeeld-bestektekst |
|---|---|

| | |
|---|---|
| Eis | Het ICT-systeem biedt volledig werkende ondersteuning voor de open standaarden IPv4 én IPv6 (‘dual stack’) -zoals opgenomen op de ‘pas toe of leg uit’-lijst van Forum Standaardisatie of daaraan gelijkwaardig. Dit betekent in ieder geval dat:<br>1. Gebruikers en andere ICT-systemen het ICT-systeem kunnen bereiken via zowel IPv4 als IPv6 zonder dat er sprake is van functionele of non-functionele (bijv. qua prestatie) verschillen.<br>2. Configuratiefunctionaliteit voor IP-adressen (bijv. een IP-whitelist) in het ICT-systeem zowel voor IPv4 als IPv6 beschikbaar is. |
| Verificatie eis | Na opleveren: testresultaat in website- en e-mailtest ophttps://www.internet.nl |
| Wens | Beschrijf de wijze van het monitoren en de incidentoplossing die u toepast, zodat het opgeleverde ICT-systeem goed bereikbaar blijft via zowel IPv6 als IPv4. |
| Beoordeling wens | Hoe beter het monitoren en de incidentoplossing is gewaarborgd door de gegadigde/inschrijver, hoe hoger de score is. Criteria waaraan de invulling van de wens getoetst wordt, moeten objectief bepaalbaar en controleerbaar zijn. |

NB: Voor gedetailleerde eisen en wensen m.b.t. IPv6 zie RIPE554 “Requirements for IPv6 in ICT Equipment”, ook beschikbaar in het Nederlands via de website van Forum Standaardisatie. De beschreven wens is met name van belang voor kritieke ICT-systemen. Het is voor kritieke ICT-systemen aan te raden om aanvullend algemene eisen en wensen op te nemen ten aanzien van de beveiliging en de beschikbaarheid. IPv6 is niet 'backwards compatible' met IPv4. Daarom is het cruciaal om voorlopig beide te ondersteunen.

### IPv4 & IPv6 (Internetnummers) voor clients

| **Naam en versie** | **IP versie 6 en 4** |
|---|---|
| Toepassing | Internetverbinding van cliëntsystemen, zoals desktops, laptops en mobiele apparaten |
| Volledige naam | Internet Protocol versie 6 en 4 (RFC2460 en RFC791) |
| Standaardisatie-organisatie | IETF |
| Specificatie-document | https://tools.ietf.org/html/rfc2460 https://tools.ietf.org/html/rfc791 |
| ICT-diensten of producten | • Werkplek en kantoorsoftware<br>• Netwerken |
| Bestekonderdeel | Voorbeeld-bestektekst |
| Eis | De internetverbinding van het client-systeem biedt volledig werkende ondersteuning voor de Open Standaarden IPv4 én IPv6 (‘dual stack’) zoals opgenomen op de ‘pas toe of leg uit’-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. Dit betekent in ieder geval dat gebruikers websites kunnen bezoeken, e-mail kunnen verzenden en ontvangen en andere ICT-systemen kunnen bereiken zowel via IPv4 als via IPv6 zonder dat er sprake is van functionele of non-functionele (bijv. qua prestatie) verschillen. |
| Verificatie eis | Na opleveren: testresultaat voor IPv6 in internetverbindingtest ophttps://www.internet.nl |
| Wens | Beschrijf de wijze van monitoring en incidentoplossing die u toepast zodat cliëntsystemen goed bereikbaar blijven via zowel IPv6 als IPv4. |
| Beoordeling wens | Hoe beter de monitoring en incidentoplossing is gewaarborgd door de gegadigde/inschrijver, hoe hoger de score is. Criteria waaraan de invulling van de wens getoetst wordt, moeten objectief bepaalbaar en controleerbaar zijn. |
| Opmerkingen | De beschreven wens is met name van belang voor kritieke ICT-systemen. Het is voor kritieke ICT-systemen aan te raden om aanvullend algemene eisen en wensen op te nemen ten aanzien van de beveiliging en de beschikbaarheid. |

### DNSSEC (Domeinnaambeveiliging) voor ondertekening

Bij het doel: ondertekening

| **Naam en versie** | **DNSSEC** |
|---|---|
| Toepassing | Digitale ondertekening van eigen domeinnaaminformatie |
| Volledige naam | Domain Name System Security Extensions (RFC4033, RFC4034, RFC4035 en verder) |
| Standaardisatie-organisatie | IETF |
| Specificatie-document | https://datatracker.ietf.org/doc/rfc4033/ e.v. |
| ICT-diensten of producten | Website of webapplicatie E-mail Spraak- en/of datacommunicatiediensten. Alle overige aan internet te koppelen ICT-systemen. |
| Bestekonderdeel | Voorbeeld-bestektekst |
| Eis | De domeinnaam van het ICT-systeem biedt volledig werkende ondersteuning voor de Open Standaard DNSSEC - zoals opgenomen op de ‘pas toe of leg uit’-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. Dit betekent dat de domeinnaaminformatie, zoals bijbehorende IP-adressen, met een geldige DNSSEC-handtekening is ondertekend. |
| Verificatie eis | Na opleveren: testresultaat voor DNSSEC-ondertekening in website- en e-mailtest op https://www.internet.nl . |
| Wens | Beschrijf uw beheerprocedure om de betrouwbaarheid en beschikbaarheid van de ondertekening met de Open Standaard DNSSEC of gelijkwaardig te waarborgen. |
| Beoordeling wens | Het beoordelingskader voor dit criterium is RFC6781 "DNSSEC Operational Practices, Version 2” van IETF of vergelijkbaar. |
| Opmerkingen | De beschreven wens is met name van belang voor kritieke ICT-systemen. Het is voor kritieke ICT-systemen aan te raden om aanvullend algemene eisen en wensen op te nemen ten aanzien van de beveiliging en de beschikbaarheid. |

### DNSSEC (Domeinnaambeveiliging) voor validatie

Doel is validatie

| **Naam en versie** | **DNSSEC** |
|---|---|
| Toepassing | Validatie van digitale handtekening van opgevraagde domeinnamen |
| Volledige naam | Domain Name System Security Extensions (RFC4033, RFC4034, RFC4035 en verder) |
| Standaardisatie-organisatie | IETF |
| Specificatie-document | https://datatracker.ietf.org/doc/rfc4033/ e.v. |
| ICT-diensten of producten | Werkplek en kantoorsoftware Netwerken |
| Bestekonderdeel | Voorbeeld-bestektekst |
| Eis | De opvragende DNS-software (resolver) biedt volledig werkende ondersteuning voor validatie c.q. verificatie van handtekeningen conform de open standaard DNSSEC - zoals opgenomen op de ‘pas toe of leg uit’-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. Dit betekent dat de DNSSEC-handtekeningen van opgevraagde domeinnamen worden gevalideerd. |
| Verificatie eis | Na opleveren: testresultaat voor DNSSEC-validatie in internetverbinding-test ophttps://www.internet.nl. |
| Wens | Beschrijf uw procedure voor het omgaan met validatiefouten van met DNSSEC ondertekende domeinnamen (bijv. afhandeling vragen eindgebruikers en inzet zogenaamde 'Negative Trust Anchors'). |
| Beoordeling wens | Het beoordelingskader voor dit criterium is RFC7646 'Definition and Use of DNSSEC Negative Trust Anchors' van IETF. |
| Opmerkingen | Het is voor kritieke ICT-systemen aan te raden om algemene eisen en wensen op te nemen ten aanzien van de beveiliging en de beschikbaarheid. |

### TLS (Beveiligde verbinding)

| **Naam en versie** | **TLS versie 1.3 én 1.2** |
|---|---|
| Toepassing | TLS moet worden toegepast op de uitwisseling van gegevens tussen clients en servers, inclusief machine-to-machine communicatie. |
| Volledige naam | Transport Layer Security (RFC5246) |
| Standaardisatie-organisatie | IETF |
| Specificatie-document | http://datatracker.ietf.org/doc/rfc5246/ |
| ICT-diensten of producten | Website of webapplicatie E-mail Spraak- en/of datacommunicatiediensten |
| Bestekonderdeel | Voorbeeld-bestektekst |

| | |
|---|---|
| Eis | Het ICT-systeem (bijv. de website) biedt volledig werkende ondersteuning voor beveiligde verbindingen conform de Open Standaard TLS (versie 1.3 én 1.2) -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. Dit betekent dat:<br>1. er een geldig (PKIoverheid-)certificaat is geïnstalleerd op het ICT-systeem;<br>2. op basis waarvan andere systemen een TLS-verbinding kunnen opzetten met dit ICT-systeem;<br>3. waarvan de veiligheid van de TLS-configuratie voldoet aan de "ICT-beveiligingsrichtlijnen voor TLS" van NCSC;<br>4. en in geval van een website zowel het TLS protocol als het HTTPS protocol een veilige configuratie hebben. |
| Verificatie eis | Na opleveren: testresultaat voor TLS in website- of e-mailtest ophttps://www.internet.nl.<br>Beschrijf uw beheerprocedure om |
| Wens | 1. het PKI overheid-certificaat veilig te beheren tijdig te vernieuwen;<br>2. de correcte en veilige werking van de TLS-verbinding te monitoren en incidenten op te lossen. |
| Beoordeling wens | Ad 1: Het beoordelingskader hiervoor is de factsheet "Veilig beheer van digitale certificaten" van NCSC of vergelijkbaar. Ad 2: Hoe beter de monitoring en incidentoplossing is gewaarborgd door de gegadigde/inschrijver, hoe hoger de score is. Criteria waaraan de invulling van de wens getoetst wordt, moeten objectief bepaalbaar en controleerbaar zijn. |
| Opmerkingen | Controleer na het inkoopmoment regelmatig met behulp van beschikbare validatie-tools, zoals Internet.nl, of TLS 1.3 en TLS 1.2 nog worden toegepast en controleer ook de veilige configuratie daarvan aan de hand van de geactualiseerde TLS-richtlijnen van NCSC. |

DKIM (Anti-phishing)

| **Naam en versie** | **DKIM versie 1** |
|---|---|
| Toepassing | Digitale ondertekening van mails door verzender zodat ontvanger de authenticiteit en integriteit van de mail kan vaststellen. DKIM is complementair aan de Open Standaard SPF. |
| Volledige naam | DomainKeys Identified Mail (DKIM) Signatures (RFC6376) |
| Standaardisatie-organisatie | IETF |
| Specificatie-document | https://tools.ietf.org/html/rfc6376 |
| ICT-diensten of producten | E-mail |
| Bestekonderdeel | Voorbeeld-bestektekst |
| Eis | De e-mailvoorziening biedt volledig werkende ondersteuning voor DKIM versie 1-zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. Dit betekent dat:<br>1. op het systeem een publiek/privaat sleutelpaar is gegenereerd of kan worden gegenereerd;<br>2. de publieke DKIM-sleutel is gepubliceerd in de DNS van de e-maildomeinnaam;<br>3. alle uitgaand e-mailberichten worden ondertekend met de private DKIM-sleutel;<br>4. alle inkomende e-mailberichten worden gecontroleerd op de geldigheid van een eventuele DKIM-handtekening en het systeem hieraan mogelijke acties verbindt. |
| Verificatie eis | Na opleveren: testresultaat voor DKIM in e-mailtest ophttps://www.internet.nl, https://www.mail-tester.com of via de tools op https://dmarc.org/resources/deployment-tools/.<br>Beschrijf uw beheerprocedure om: |
| Wens | 1. de DKIM-sleutels veilig te genereren, te beheren en te vernieuwen; en<br>2. de correcte werking van DKIM te monitoren zowel voor inkomende als uitgaande e-mail. |
| Beoordeling wens | Het beoordelingskader hiervoor is de NCSC-factsheet "Factsheet Bescherm domeinnamen tegen phishing" en de relevante Best Practices van M3AAWG (m.n. "DKIM Key Rotation Best Common Practices" en "Best Practices for Implementing DKIM To Avoid Key Length Vulnerability"). |
| Opmerkingen | Het is voor kritieke ICT-systemen aan te raden om algemene eisen en wensen op te nemen ten aanzien van de beveiliging en de beschikbaarheid. |

SPF (Anti-phishing)

| **Naam en versie** | **SPF versie 1** |
|---|---|
| Toepassing | Het controleren of een e-mailserver gerechtigd is om namens een domeinnaam e-mail te mogen verzenden. SPF is complementair aan de Open Standaard DKIM. |
| Volledige naam | Sender Policy Framework (RFC7208) |
| Standaardisatie-organisatie | . |
| Specificatie-document | https://tools.ietf.org/html/rfc7208 |
| ICT-diensten of producten | • E-mail |
| Bestekonderdeel | Voorbeeld-bestektekst |
| Eis | De e-mailvoorziening biedt volledige ondersteuning voor de open standaard SPF versie 1 -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. Dit betekent dat:<br>1. de IP-adressen van de verzendende systemen als SPF-record worden geregistreerd in de DNS van de verzendende domeinnaam;<br>2. alle inkomende e-mailberichten worden gecontroleerd op de geldigheid van het verzendend IP-adres tegen het IP-adres dat in SPF-record staat van de verzendende domeinnaam. |
| Verificatie eis | Na opleveren: testresultaat voor SPF in e-mailtest ophttps://www.internet.nl, https://www.mail-tester.com of via de tools op https://dmarc.org/resources/deployment-tools/.<br>Beschrijf uw beheerprocedure om: |
| Wens | 1. de SPF-records te genereren en indien nodig aan te passen, en<br>2. de correcte werking van SPF te monitoren zowel voor inkomende als uitgaande e-mails. |
| Beoordeling wens | Het beoordelingskader hiervoor is de NCSC-factsheet "Factsheet Bescherm domeinnamen tegen phishing" . |
| Opmerkingen | Het is voor kritieke ICT-systemen aan te raden om algemene eisen en wensen op te nemen ten aanzien van de beveiliging en de beschikbaarheid. |

SAML (Inloggegevens)

| **Naam en versie** | **SAML versie 2.0** |
|---|---|
| Toepassing | Eenmalig inloggen (en uitloggen) waardoor een gebruiker via zijn/haar browser toegang heeft tot verschillende webdiensten. Onder andere DigiD en eHerkenning maken gebruik van SAML voor het koppelvlak met aangesloten organisaties. |
| Volledige naam | Security Assertion Markup Language |
| Standaardisatie-organisatie | OASIS |
| Specificatie-document | http://www.oasis-open.org/committees/security/ |
| ICT-diensten of producten | • Website of webapplicatie |
| Bestekonderdeel | Voorbeeld-bestektekst |
| Eis | Het ICT-systeem biedt volledig werkende ondersteuning van SAML versie 2.0 -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig, zodat gebruikers via eenmalig in- en uitloggen veilige toegang hebben tot verschillende gekoppelde webdiensten. |
| Verificatie eis | • Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem aan deze standaard voldoet;<br>• Succesvol doorlopen van Interoperability Certification Program van Kantara of vergelijkbaar Interoperability Program;<br>• Na oplevering:volledig werkende aansluiting op systeem zoals DigiD en eHerkenning indien dat het doel is. |
| Wens | Geen |
| Beoordeling wens | Geen |
| Opmerkingen | Het is voor kritieke ICT-systemen aan te raden om algemene eisen en wensen op te nemen ten aanzien van de beveiliging en de beschikbaarheid. |

ISO 27001 (Managementsysteem informatiebeveiliging)

| Naam en versie | ISO 27001 versie 2013 |
|---|---|
| Toepassing | Eisen voor een managementsysteem informatiebeveiliging. |
| Volledige naam | 27001: Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging (NEN-ISO/IEC 27001:2013 nl ) |
| Standaardisatie-organisatie | NEN-ISO/IEC |
| Specificatie-document | https://www.nen.nl/nen-iso-iec-27001-2013-nl-188752 |
| ICT-diensten of producten | Alle ICT-systemen/-diensten, met name die met privacy- en/of bedrijfs-gevoelige informatie. |
| Bestekonderdeel | Voorbeeld-bestektekst |
| Eis | De gegadigde/inschrijver heeft een managementsysteem informatiebeveiliging in werking voor te leveren ICT-systeem/-dienst conform de Open Standaard NEN-ISO/IEC 27001:2013-zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig, zoals de BIO (Baseline Informatiebeveiliging Overheid). |
| Verificatie eis | • Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem/-dienst aan deze standaard voldoet;<br>• Certificaat betreffende te leveren ICT-systeem/-dienst inzake conformiteit met NEN-ISO/IEC 27001:2013 dat is verstrekt door een RvA-geaccrediteerde organisatie, of een gelijkwaardig certificaat. |
| Wens | Geen |
| Beoordeling wens | Geen |
| Opmerkingen | Afhankelijk van het product dat wordt gevraagd kan het voldoen aan ISO/IEC 27001 worden aangetoond door een certificaat te overleggen. Het kan gezien de marktsituatie te zwaar zijn om van alle gegadigden/inschrijvers vooraf volledige certificatie te vragen. Een en ander is tevens afhankelijk van de risico-inschatting van de gegevensverwerking en de aard van de dienstverlening. |

ISO 27002 (Richtlijnen en principes informatiebeveiliging)

| Naam en versie | ISO 27002 versie 2013 |
|---|---|
| Toepassing | 'Best practices' voor het nemen van maatregelen op het gebied informatiebeveiliging. |
| Volledige naam | 27002: Praktijkrichtlijn met beheersmaatregelen op het gebied van informatiebeveiliging (NEN-ISO/IEC 27002:2013 nl) |
| Standaardisatie-organisatie | NEN-ISO/IEC |
| Specificatie-document | https://www.nen.nl/nen-iso-iec-27002-2013-nl-188742 |
| ICT-diensten of producten | Alle ICT-systemen/-diensten, met name die met privacy- en/of bedrijfs-gevoelige informatie. |
| Bestekonderdeel | Voorbeeld-bestektekst |
| Eis | De gegadigde/inschrijver heeft voor te leveren ICT-systeem/-dienst beheersmaatregelen op het gebied van informatiebeveiliging in werking die zijn gebaseerd op de Open Standaard NEN-ISO/IEC 27002:2013 -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig, zoals de Baseline informatiebeveiliging Overheid (BIO). |
| Verificatie eis | Akkoordverklaring eventueel met toelichtende beschrijving van getroffen beheersmaatregelen in relatie tot ISO 27002. |
| Wens | Geen |
| Beoordeling wens | Geen |
| Opmerkingen | Voldoen aan het gestelde in de BIO (Baseline Informatiebeveiliging Overheid) kan aanbestedingsrechtelijk als gelijkwaardig aan ISO 27002 worden beschouwd. Het is van belang dat een aanbestedende dienst zelf een scherp beeld heeft van mogelijke risico's en noodzakelijke maatregelen, en op basis daarvan meer specifieke eisen en wensen opneemt naast de algemene verwijzing naar ISO 27002 of naar de BIO. |

HTTPS en HSTS

| Begrip | HTTPS & HSTS |
|---|---|
| Toepassing | HTTPS en HSTS moeten worden toegepast op de communicatie tussen clients (zoals webbrowsers) en servers voor alle websites en webservices. HTTPS zorgt voor het gebruik van HTTP over een met TLS beveiligde verbinding. Dit betekent dat het webverkeer door middel een certificaat wordt versleuteld. HSTS zorgt ervoor dat een webbrowser, na het eerste contact over HTTPS, bij vervolgbezoek de website altijd direct over HTTPS opvraagt. |
| Volledige naam | HyperText Transfer Protocol Secure (HTTPS) en HTTP Strict Transport Security (HSTS) |
| Standaardisatie-organisatie | IETF |
| Specificatie-document | https://datatracker.ietf.org/doc/rfc2818/ https://tools.ietf.org/html/rfc6797 |
| ICT-diensten of producten | • Website of webapplicatie<br>• E-HRM systemen<br>• Netwerken |
| Bestekonderdeel | Voorbeeld-bestektekst |
| Eis | Het ICT Systeem biedt volledig werkende ondersteuning voor HTTPS en HSTS -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. |
| Verificatie van de eis | • Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem aan standaard voldoet.<br>• Testresultaten van validatietooling voor HTTPS en HSTS zoals www.internet.nl en https://www.ssllabs.com/ssltest/ |
| Wens | Geen |
| Beoordeling wens | Geen |
| Opmerkingen | |

DMARC

| Begrip | DMARC |
|---|---|
| Toepassing | DMARC maakt het mogelijk om beleid in te stellen over de manier waarop een e-mailprovider om moet gaan met e-mail waarvan niet kan worden vastgesteld dat deze afkomstig is van het vermelde afzenderdomein. Hierdoor kunnen organisaties voorkomen dat anderen e-mails versturen namens het e-maildomein van de organisatie. DMARC moet worden toegepast op alle overheidsdomeinnamen, ook op domeinen waarvan niet wordt gemaild, én op alle mailservers waarmee de overheid e-mail ontvangt. |
| Volledige naam | Domain-based Message Authentication, Reporting, and Conformance |
| Standaardisatie-organisatie | IETF |
| Specificatie-document | https://datatracker.ietf.org/doc/rfc7489/ |
| ICT-diensten of producten | • E-mail |
| Bestekonderdeel | Voorbeeld-bestektekst |
| Eis | De e-mailvoorziening biedt volledig werkende ondersteuning voor DMARC -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. |
| Verificatie van de eis | • Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem aan standaard voldoet;<br>• Testresultaten van validatie 'tooling' voor DMARC zoals www.internet.nl, https://www.mail-tester.com of via de tools op https://dmarc.org/resources/deployment-tools/. |
| Wens | Geen |
| Beoordeling wens | Geen |
| Opmerkingen | Geen |

Starttls/Dane

| Begrip | Starttls/Dane |
|---|---|
| Toepassing | Mailverkeer tussen mailservers verloopt via SMTP. STARTTLS in combinatie met DANE gaan, in aanvulling op SMTP, afluisteren of manipuleren van dit mailverkeer door internetcriminelen tegen. Beide standaarden moeten in combinatie worden toegepast op ontvangende en verzendende e-mailservers. |
| Volledige naam | STARTTLS en DANE |

| | |
|---|---|
| Standaardisatie-organisatie | IETF |
| Specificatie-document | https://tools.ietf.org/html/rfc3207 https://tools.ietf.org/html/rfc7672 |
| ICT-diensten of producten | • E-mail |
| Bestekonderdeel | Voorbeeld-bestektekst |
| Eis | De e-mailvoorziening biedt volledige ondersteuning voor de Open Standaard STARTTLS en DANE -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. |
| Verificatie van de eis | • Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem aan standaard voldoet.<br>• Testresultaten van validatietooling voor STARTTLS/DANE zoals www.internet.nl |
| Wens | Geen |
| Beoordeling wens | Geen |
| Opmerkingen | Organisaties die STARTTLS en DANE toepassen worden opgeroepen de standaarden te implementeren volgens de adviezen van het NCSC. |

RPKI

| Naam en versie | RPKI |
|---|---|
| Toepassing | Het ondertekenen van IP-adressen en IT-systemen. Dit dient ter beveiliging van het BGP (Border Gateway Protocol) (voorkomen van route hijacks). |
| Volledige naam | Resource Public Key Infrastructure |
| Standaardisatieorganisatie | IETF |
| Specificatiedocument | https://datatracker.ietf.org/doc/html/rfc6480 |
| Relevante inkoopcategorie | Netwerken |
| Bestekonderdeel | Voorbeeld-bestektekst |
| Eis | Voor de integriteit van de te leveren IT-systemen is vereist dat bij de routing van informatie op het internet RPKI wordt toegepast. Het IT-systeem biedt daarom volledig werkende ondersteuning voor de open standaard RPKI – zoals opgenomen op de 'pas toe of leg uit'-lijst van het Forum Standaardisatie – of daaraan gelijkwaardig. Dit betekent in ieder geval dat leverancier – die via BGP routes ontvangt – filtert op basis van alle wereldwijde gepubliceerde ROA's. |
| Verificatie eis | Akkoordverklaring, eventueel met toelichting hoe leverancier borgt dat het IT-systeem/-dienst aan deze standaard voldoet. |
| Wens | Geen |
| Beoordeling wens | Geen |
| Opmerkingen | Met het filteren op basis van de ROA's wordt in ieder geval bedoeld dat invalide routes nooit geaccepteerd of geadverteerd mogen worden. |

### 4.2 Documenten en (web)content

PDF/A (Formaat documentpublicatie / archivering)

| Naam en versie | PDF/A-1 en PDF/A-2 |
|---|---|
| Toepassing | Voor publicatie of archivering van documenten waarbij toegankelijkheid nu en in de toekomst van belang is. PDF/A is een gestandaardiseerde versie van PDF. Op de 'pas toe of leg uit'-lijst staat PDF als overkoepelende standaard genoemd. |
| Volledige naam | Portable Document Format Archivable (NEN-ISO 19005-1:2005 en NEN-ISO 19005-2:2011) |
| Standaardisatie-organisatie | NEN-ISO |
| Specificatie-document | https://www.nen.nl/nen-iso-19005-1-2005-c2-2012-en-167243, https://www.nen.nl/nen-iso-19005-2-2011-en-161167 |
| ICT-diensten of producten | • Website of webapplicatie<br>• Werkplek en kantoorsoftware<br>• Multi-functionals |
| Bestekonderdeel | Voorbeeld-bestektekst |
| Eis | 1. Het te leveren ICT-systeem (bijv. webapplicatie) kan documenten genereren/beheren/publiceren in een formaat conform de Open Standaard PDF/A -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig;<br>2. Met het te leveren kantoorsoftwarepakket kan de gebruiker documenten bekijken en/of creëren in een formaat conform de Open Standaard PDF/A -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig;<br>3. Met de te leveren multi-functional kan de gebruiker scans maken en vastleggen in een formaat conform de Open Standaard PDF/A -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. |
| Verificatie eis | • Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem aan standaard voldoet.<br>• Testresultaten van validatietooling voor PDF/A zoals VeraPDF (https://verapdf.org), Adobe Preflight en tooling op andere pagina van deze website. |
| Wens | Geen |
| Beoordeling wens | Geen |
| Opmerkingen | Voor meer achtergrond zie de informatie over open documentformaten op dewebsite van Forum Standaardisatie. |

PDF 1.7 (Formaat documentpublicatie)

| Naam en versie | PDF 1.7 |
|---|---|
| Toepassing | Voor publicatie van documenten met dynamische content waarbij (duurzame) toegankelijkheid minder van belang is. PDF1.7 gestandaardiseerde versie van PDF. Deze versie is rijker qua functionaliteit dan PDF/A. Dit kan echter ten koste gaan van de interoperabiliteit. Daarom dient PDF1.7 alleen ingezet te worden als de functionaliteit van PDF/A tekortschiet. Op de 'pas toe of leg uit'-lijst staat PDF als overkoepelende standaard genoemd. |
| Volledige naam | Portable document format -- Part 1: PDF 1.7 |
| Standaardisatie-organisatie | ISO |
| Specificatie-document | http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51502 |
| ICT-diensten of producten | • Website of webapplicatie<br>• Werkplek en kantoorsoftware<br>• Multi-functionals |
| Bestekonderdeel | Voorbeeld-bestektekst |
| Eis | 1. Het te leveren ICT-systeem (bijv. webapplicatie) kan documenten genereren/tonen/beheren/publiceren in een formaat conform de open standaard PDF1.7 -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig.<br>2. Met het te leveren kantoorsoftwarepakket kan de gebruiker documenten bekijken en/of creëren in in een formaat conform de open standaard PDF1.7 -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig.<br><br>1. Met de te leveren multi-functional kan de gebruiker scans maken en vastleggen in een formaat conform de open otandaard PDF1.7 -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. |
| Verificatie eis | • Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem aan deze standaard voldoet.<br>• Testresultaten van validatie 'tooling' voor PDF1.7 zoals Adobe Preflight. |
| Wens | Geen |
| Beoordeling wens | Geen |
| Opmerkingen | Voor meer achtergrond zie de informatie over open documentformaten op dewebsite van Forum Standaardisatie. |

ODF (Formaat documentbewerking)

| Naam en versie | ODF versie 1.2 |
|---|---|

| | |
|---|---|
| Toepassing | Voor het publiceren of uitwisselen van documenten (tekst, rekenbladen en presentatie) in bewerkbare vorm, zodat de ontvanger aanpassingen en toevoegingen kan doen. |
| Volledige naam | Open Document Formaat |
| Standaardisatie-organisatie | OASIS en ISO |
| Specificatie-document | https://www.oasis-open.org/committees/office/ http://standards.iso.org/ittf/PubliclyAvailableStandards/ |
| ICT-diensten of producten | • Website of webapplicatie<br>• Werkplek en kantoorsoftware<br>• Multi-functionals |
| Bestekonderdeel | Voorbeeld-bestektekst |
| Eis | 1. Het te leveren ICT-systeem (bijv. webapplicatie) kan documenten genereren/tonen/beheren/publiceren in ODF versie 1.2 -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig.<br>2. Met het te leveren kantoorsoftwarepakket kan de gebruiker documenten bekijken en/of creëren in een formaat conform de Open Standaard ODF versie 1.2 -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig.<br>3. Met de te leveren multi-functional kan de gebruiker scans maken en vastleggen in een formaat conform de Open Standaard ODF versie 1.2 -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. |
| Verificatie eis | • Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem aan deze standaard voldoet.<br>• Testresultaten van validatietooling voor ODF, zoals ODF Validator en ODFAutoTests . Zie ook: https://www.gov.uk/government/publications/open-document-format-odf-validators-and-compliance-testing. |
| Wens | Geen |
| Beoordeling wens | Geen |
| Opmerkingen | Voor meer achtergrond zie de informatie over open documentformaten op de website van Forum Standaardisatie. Een wijdverbreid misverstand is dat ODF alleen ondersteund wordt door alternatieve office-pakketten zoals LibreOffice en OpenOffice. Dat klopt niet. Microsoft Office en Google Docs bieden ook ODF-ondersteuning. Over het algemeen geldt dat recentere software-versies betere ondersteuning bieden ten behoeve van ODF. |

## Digitoegankelijk

| **Naam en versie** | **Digitoegankelijk (EN 301549 met WCAG 2.1)** |
|---|---|
| Toepassing | Inkoop, ontwerpen, bouwen en beheren van toegankelijke websites en webapplicaties. De richtlijnen zijn gebaseerd op Europese en internationale standaarden (met name EN 301 549 en WCAG2.1), en op in de praktijk beproefde oplossingen van professionals. Ze zijn van toepassing op alle webcontent dus bijvoorbeeld ook op gepubliceerde en nog te publiceren documenten. |
| Volledige naam | Digitoegankelijk |
| Standaardisatie-organisatie | ETSI |
| Specificatie-document | www.digitoegankelijk.nl |
| ICT-diensten of producten | • Website of webapplicatie |
| Bestekonderdeel | Voorbeeld-bestektekst |
| Eis | • Leverancier levert de resultaten in digitaal toegankelijke format op en toont aan dat deze voldoen aan de wettelijk verplichte digitale toegankelijkheidsstandaard WCAG 2.1, niveaus A en AA.<br>• Het meegeleverde bewijs bestaat uit een door een ter zake kundige expert opgesteld toegankelijkheidsrapport opgesteld volgens de WCAG-EM methode.<br>• Een automatisch gegenereerd toegankelijkheidsrapport of screenshot uit een kantoorapplicatie of validatietool volstaat niet. |
| Verificatie eis | • Akkoordverklaring eventueel met toelichtende beschrijving van specifieke situaties en uitzonderingen op basis van digitoegankelijk.nl/beleid/specifieke-situaties;<br>• Handmatig onderzoek en advies door een toegankelijkheidsexpert;<br>• Automatisch onderzoek is deels geschikt omdat niet alle aspecten van WCAG 2.1 automatisch getoetst kunnen worden maar wel geschikt voor indicatief beeld: http://checkers.eiii.eu/. |
| Wens | Geen |
| Beoordeling wens | Geen |
| Opmerkingen | • Digitoegankelijk (EN 301 549 met WCAG 2.1) vervangt Webrichtlijnen 2.0 op de 'pas toe of leg uit'-lijst sinds oktober 2016. Zowel Digitoegankelijk als Webrichtlijnen baseren zich op de technische toegankelijkheidsstandaard WCAG 2.1 van W3C, alleen gaat Digitoegankelijk uit van de Europese Norm EN 301 549 die ook instructies voor inkoop beschrijft.<br>• Zie aanvullend 'EN 301 549 - Accessibility requirements suitable for public procurement of ICT products and services in Europe' van CEN, CENELEC en ETSI (http://www.etsi.org/deliver/etsi_en/301500_301599/301549/01.01.01_60/en_301549v010101p.pdf).<br>• Digitoegankelijk is wettelijk verplicht op grond van de Wet digitale overheid.<br>• Zie voor het besluit Wet digitale overheid en Staatsblad 2018, 141. |

## SKOS (Thesauri en begrippenwoordenboeken)

| **Naam en versie** | **SKOS** |
|---|---|
| Toepassing | Ordenen en publiceren van kennissystemen (Knowledge Organization Systems), zoals thesauri, classificatieschema's en taxonomieën, binnen de context van het semantisch web en (linked) open data. |
| Volledige naam | Simple Knowledge Organization System (W3C Recommendation 18 August 2009) |
| Standaardisatie-organisatie | W3C |
| Specificatie-document | https://www.w3.org/TR/skos-reference/ |
| ICT-diensten of producten | • Website of webapplicatie<br>• Werkplek en kantoorsoftware |
| Bestekonderdeel | Voorbeeld-bestektekst |
| Eis | Het ICT-systeem biedt volledig werkende ondersteuning voor de Open Standaard SKOS -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. |
| Verificatie eis | • Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem aan deze standaard voldoet;<br>• Testresultaten van validatie 'tooling' zoals vindbaar op https://www.w3.org/2004/02/skos/validation. |
| Wens | Geen |
| Beoordeling wens | Geen |
| Opmerkingen | SKOS bouwt voort op de Linked Data Standaarden (RDF, RDFS, OWL). Naarmate de LD-standaarden breder toegepast worden en de hoeveelheid op LD-gebaseerde standaarden toeneemt, ontstaan er steeds meer toepassingsmogelijkheden voor SKOS-gebaseerde vocabulaires. SKOS-vocabulaires gaan in toenemende mate het hart vormen van semantische interoperabiliteit. |

## Open API specification (beschrijven van REST APIs)

| **Naam en versie** | **Open API Specification 3.0** |
|---|---|
| Toepassing | OAS moet worden toegepast op het beschrijven en specificeren van een REST API. |
| Volledige naam | OpenAPI Specification |
| Standaardisatie-organisatie | OpenAPI Initiative |
| Specificatie-document | https://github.com/OAI/OpenAPI-Specification/blob/master/versions/3.0.1.md |
| ICT-diensten of producten | Alle ICT-systemen/-diensten indien er gebruik wordt gemaakt van een REST API. |
| Bestekonderdeel | Voorbeeld-bestektekst |

| | |
|---|---|
| Eis | De eigenschappen van benodigde API's dienen in mee te leveren documentatie beschreven te zijn conform de OpenAPI Specification |
| Verificatie van de eis | • Akkoordverklaring eventueel met toelichting hoe hij borgt dat de documentatie aan deze standaard voldoet |
| Wens | Geen |
| Beoordeling wens | Geen |
| Opmerkingen | 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. OAS 3.0 is zowel compatibel met de voorgaande versie OAS 2.0 als met de alternatieve standaard RAML (RESTful API Modeling Language) die ook veel gebruikt werd. Het Deelprogramma Digitaal Stelsel Omgevingswet gebruikt OAS 2.0 en OAS 3.0. |

## 5. Leg uit in het jaarverslag

Overheidsorganisaties mogen alleen afwijken van de toepassing van de 'pas toe of leg uit'-standaarden op twee voorwaarden:

- Het moet ten eerste gaan om reden van bijzonder gewicht;
- en ten tweede moet die reden terug te vinden zijn in het jaarverslag.

Om hieraan te kunnen voldoen is het belangrijk dat reden wordt vastgelegd in het aanbestedingsdossier en de tweede om deze aan te bieden voor opname in het jaarverslag. Geldige redenen om een 'pas toe of leg uit'- standaard niet te gebruiken kunnen zijn:

- onvoldoende aanbod van de standaard door de markt;
- onvoldoende veiligheid van de standaard;
- onvoldoende zekerheid bij het functioneren van de standaard;
- of een andere andere redenen van bijzonder gewicht.

De vermelding in het jaarverslag is voor rijksoverheidsorganisaties geregeld in de bijlage van de instructie rijksdienst bij aanschaf van ICT-diensten en ICT-producten artikel 3 en 4, die in samenhang moet worden gelezen met de bedrijfsvoeringsparagraaf van de Rijksbegrotingsvoorschriften, model 3.24.

Elementen die in het jaarverslag terug moeten komen zijn:

1. om welke aanschaf het nalaten van de relevante standaarden betrekking heeft,
2. welke standaarden hiervoor relevant waren maar achterwege zijn gelaten,
3. met welke reden deze standaarden achterwege zijn gelaten.

In algemene zin verklaren over het 'pas toe of leg uit'- beleid voor open standaarden in het jaarverslag is geen geldige uitleg.

Dus niet: "Er zijn in de regel geen nieuwe ICT-diensten of -producten aangeschaft waarbij is afgeweken van de open standaarden op de «pas toe of leg uit»- lijst van het Forum Standaardisatie."

Maar:

In jaar X deed organisatie Y een aanschaf naar Z.

(Indien het geval: deze aanschaf is ook onderzocht in de Monitor Open Standaarden van jaar X+1).

Toepassing van de standaard(en) a (b, en c) is daarbij achterwege gelaten omdat...

### 5.1 Uitleggen en de Monitor Open Standaarden

Via de Monitor Open Standaarden voert het Forum Standaardisatie jaarlijks onderzoek uit naar het gebruik van de standaarden op de 'pas toe of leg uit'-lijst. Hiertoe worden ook openbare aanbestedingsdocumenten en jaarverslagen onderzocht.

Sinds 2018 publiceert het Forum Standaardisatie de onderzoeksresultaten van het onderzoek naar de aanbestedingsdocumenten in een bijlage bij de Monitor Open Standaarden. Hierin staan alle onderzochte aanbestedingen met de standaarden die gevraagd zijn en de standaarden die niet gevraagd zijn en waar dus een uitleg verwacht mag worden.

## Documentatie-type

documentatie