OPEN STANDAARDEN BIJ AANBESTEDINGEN 2025 ('pas toe' en 'leg uit')

Onderdeel van de Monitor Open Standaarden 2026

Auteurs: Hanne Bosma, Siwert de Groot, Michel Gunsing
Versie: 0.95
Datum: 21 mei 2026

Inhoudsopgave

i. Samenvatting

Ingeburgerde standaarden
Dit onderzoek naar aanbestedingen uit 2025 laat zien dat de adoptie van verplichte open standaarden bij aanbestedingen sterk verschilt per standaard. Sommige standaarden zijn duidelijk ingeburgerd. AdES, NLCIUS, StUF en vooral ISO 27001 en ISO 27002 worden relatief vaak uitgevraagd wanneer zij relevant zijn. Ook PDF, Digitoegankelijk, TLS en HTTPS en HSTS scoren redelijk, al is het opvallend dat wettelijk verplichte standaarden als Digitoegankelijk en HTTPS en HSTS niet altijd worden uitgevraagd wanneer zij relevant zijn. Overall wordt net iets minder dan de helft van de relevante standaarden uitgevraagd.

Achterblijvende standaarden
Tegelijkertijd blijft een groep standaarden structureel achter. Dat geldt met name voor REST-API Design Rules, NL GOV Assurance, WPA2 Enterprise, ODF, RPKI en security.txt. Ook internet- en e-mailveiligheidsstandaarden zoals DNSSEC, SPF, DKIM, DMARC en STARTTLS en DANE worden relatief weinig uitgevraagd, terwijl zij vaak relevant zijn bij webapplicaties en cloudoplossingen. Beleidsmatig is dat een belangrijk signaal: juist standaarden die bijdragen aan digitale veiligheid, gegevensuitwisseling en leveranciersonafhankelijkheid blijven te vaak buiten beeld.

Kwaliteit van aanbestedingen
De kwaliteit van aanbestedingen laat een gemengd beeld zien. Een deel van de aanbestedingen toont dat volledige of bijna volledige naleving van het open standaardenbeleid mogelijk is, ook bij complexe opdrachten. Twee vermeldenswaardige voorbeelden zijn een aanbesteding van het ministerie van Defensie en van de gemeente Tilburg. Van de 70 onderzochte aanbestedingen zijn 15 als perfect beoordeeld. Daarbij moet wel worden opgemerkt dat dit oordeel mede een gevolg is van de (nieuwe) bonus als er in de aanbesteding wordt verwezen naar het open standaardenbeleid of de ‘Pas toe of leg uit’-lijst.

Verantwoording over aanbestedingen is nodig
In 66 van de 70 onderzochte aanbestedingen werd ten minste één relevante verplichte standaard niet uitgevraagd; formeel zou daarover verantwoording moeten worden afgelegd in het jaarverslag. Uit de departementale jaarverslagen over 2025 blijkt dat deze verantwoording in de praktijk maar beperkt wordt aangetroffen. De hoor-en-wederhoorfase van het onderzoek is een informele correctie- en leerfunctie: aanbestedende diensten kunnen toelichten waarom zij standaarden wel of niet relevant vinden, waardoor beoordelaars hun oordeel soms kunnen bijstellen.

De FDS-standaarden
De aanvullende analyse op de FDS-standaarden laat zien dat standaarden voor federatief datadelen nog beperkt landen in aanbestedingen. Vooral REST-API Design Rules en Digikoppeling/FSC zijn relevant, maar worden nog weinig uitgevraagd; standaarden als MIM, SKOS en CloudEvents kwamen wel als relevant naar voren, maar werden niet gevraagd. Beleidsmatig is dit relevant omdat goede toepassing van deze standaarden randvoorwaardelijk is voor gegevensdeling, hergebruik en het functioneren van het Federatief Datastelsel.

ii. Voorwoord

In het kader van de Monitor Open Standaarden 2026 is voor het vijftiende jaar op rij onderzoek gedaan naar de toepassing van open standaarden bij aanbestedingen door overheden. Het gaat om 70 aanbestedingen die in 2025 gepubliceerd werden: 35 van de rijksoverheid en 35 van medeoverheden. Per aanbesteding is vastgesteld welke open standaarden van de 'Pas toe of leg uit'-lijst van relevant waren en in hoeverre daar in de aanbestedingsstukken daadwerkelijk om is gevraagd.

Indeling
De opzet van deze rapportage is als volgt. In paragraaf 1 wordt in het kort het open standaardenbeleid beschreven en de rol van Forum Standaardisatie daarin. Lezers die daarmee bekend zijn, kunnen direct naar paragraaf 2 gaan. Daarin staat het 'Pas Toe'-deel in aanbestedingen centraal. Er wordt in de tweede paragraaf vooral naar individuele standaarden gekeken. In paragraaf 3 verschuift de focus naar de kwaliteit van de aanbesteding als geheel. De methodologie van de beoordeling van aanbesteding is dit jaar enigszins aangepast. In paragraaf 4 staat 'Leg uit' centraal. In deze paragraaf gaat het over de formele verantwoording via jaarverslagen van departementen en over het informele deel van 'Leg uit': de hoor-en-wederhoorfase van het onderzoek. In de laatste paragraaf van deze rapportage richten we de aandacht op een andere selectie van open standaarden, te weten open standaarden die voor het Federatief Datastelsel van belang zijn.

Onderdelen van de Monitor Open Standaarden 2026
Deze rapportage over de aanbestedingen in 2025 is onderdeel van de Monitor Open Standaarden 2026. Andere onderdelen zijn de rapportage over de implementatie van open standaarden in een selectie van overheidsvoorzieningen. Die selectie komt grotendeels overeen met de voorzieningen van de Gemeenschappelijke Digitale Infrastructuur. In de loop van 2026 komt ook het onderzoek naar de gebruiksgegevens van open standaarden beschikbaar, inclusief gesprekken met leveranciers en/of aanbestedende diensten. En een onderzoek dat op verzoek van het OBDO wordt gedaan naar de rol van een vijftal ICT-kaders bij aanbestedingen.

1. Het open standaardenbeleid in het kort

Open standaarden zijn specificaties van een bepaald type IT-product of -dienst die door alle partijen die dat willen vrijelijk gebruikt kunnen worden, zonder hindernissen van intellectueel eigendomsrecht. Een voorbeeld van een open standaard is HTML: de standaard opmaaktaal voor webpagina's. Forum Standaardisatie verbindt aan het **open** zijn van standaarden voorwaarden ten aanzien van het gebruik (gratis), intellectueel eigendom (iedereen mag de standaard gebruiken), inspraakmogelijkheden bij de ontwikkeling, onafhankelijkheid en duurzaamheid.

De overheid wil met het beleid voor open standaarden een aantal doelen bereiken. Overheidsorganisaties moeten over de juiste gegevens beschikken en moeten deze op het juiste moment kunnen delen met elkaar en met burgers en ondernemers. Dit vereist afspraken over hoe gegevens worden vastgelegd en uitgewisseld, dat wordt interoperabiliteit genoemd. Standaardisatie verbetert ook de kwaliteit van data.

Het open standaardenbeleid bevordert ook onafhankelijkheid van leveranciers: door open standaarden toe te passen, kan men eenvoudiger van ICT-aanbieder wisselen. Bovendien verhogen open standaarden de veiligheid, bijvoorbeeld door websites en applicaties te beschermen tegen misbruik. Verder zorgen standaarden voor openheid en toegankelijkheid, zodat ook mensen met een beperking met de overheid kunnen communiceren.

Kortom, open standaarden zijn essentieel voor een veilige, inclusieve en digitale samenleving en helpen de publieke dienstverlening te verbeteren. De open standaarden maken deel uit van de *Generieke Digitale Infrastructuur* die naast standaarden bestaat uit afspraken en voorzieningen die alle publieke dienstverleners gebruiken voor hun digitale diensten aan burgers en ondernemers.

Het centrale beleidsinstrument voor open standaarden is het principe van *'Pas toe of leg uit'*. Dit houdt in dat overheidsorganisaties verplicht zijn relevante open standaarden toe te passen bij de inkoop en eigen ontwikkeling van ICT-producten en diensten.[1] Als een standaard wel relevant is maar tijdens de aanbesteding niet wordt uitgevraagd, dan moet de organisatie hierover uitleg geven in het jaarverslag. Een overzicht van alle voor Nederlandse overheidsorganisaties *verplichte open standaarden* is te vinden op de website van Forum Standaardisatie. In 2025 bestond de lijst uit 42 verplichte open standaarden, per 1 januari 2026 zijn daar 3 standaarden aan toegevoegd.

De rol van het Forum Standaardisatie is om standaarden te beoordelen en te adviseren of ze aanbevolen worden voor overheidsorganisaties of zelfs opgenomen worden op de *'Pas toe of leg uit'*-lijst: de verplichte open standaarden. Open standaarden op deze lijst kunnen een extra verplichting krijgen: een *streefbeeldafspraak*. Daarbij moet de standaard voor een bepaalde datum ingevoerd zijn. In dat geval is er geen mogelijkheid meer om van die

1 Sinds 2008 is het voor onderdelen van de rijksoverheid verplicht om bij de aanschaf van ICT te vragen om de relevante open standaarden van de Pas toe of leg uit-lijst. Deze verplichting is later uitgebreid naar medeoverheden en uitvoeringsorganisaties en is in april 2022 door het Overheidsbreed Beleidsoverleg Digitale overheid voor onbepaalde tijd opnieuw bevestigd.

verplichting af te wijken (via ‘Leg uit’). Die afspraak geldt dan niet alleen bij aanbestedingen maar ook voor bestaande systemen. Er zijn op dit moment streefbeeldafspraken voor de volgende open standaarden: DKIM, DMARC, DNSSEC, IPv6 en IPv4, RPKI, STARTTLS en DANE, SPF en TLS. Er geldt bovendien een *wettelijke verplichting* voor een drietal standaarden: Digitale toegankelijkheid en HTTPS en HSTS.

Forum Standaardisatie houdt zich ook bezig met de ontwikkeling van nieuwe standaarden. Daarnaast worden activiteiten ondernomen om de adoptie te bevorderen doormiddel van bijeenkomsten, webinars, congressen en presentaties in allerlei netwerken. De Monitor Open Standaarden is zelf ook een middel om het gebruik van open standaarden te stimuleren. De publicatie en actieve verspreiding dragen bij aan het uitdragen van het beleid. De gesprekken tussen onderzoekers en beheerders van voorzieningen over de adoptie van open standaarden zijn voor sommige beheerders een prikkel om opnieuw na te denken over de adoptie. Op eenzelfde manier zijn de gesprekken over aanbestedingen een gelegenheid voor organisaties om nog eens naar hun eigen open standaarden praktijk te kijken.

2. “Pas toe” van open standaarden

In de 70 aanbestedingen uit 2025 die in deze monitor beoordeeld zijn, werden 1.080 open standaarden als relevant beoordeeld. In de praktijk werden er echter slechts 534 standaarden uitgevraagd, wat resulteert in een uitvraagpercentage van 49 procent. Een structurele verbetering ten opzichte van voorgaande jaren blijft daarmee uit. Een overzicht van de open standaarden die in het onderzoeksjaar 2025 verplicht waren is te vinden in Bijlage 1.

Uitgevraagde versus relevante open standaarden: per domein

Wanneer wij verder inzoomen kunnen wij de ontwikkelingen per domein en bestuurslaag vergelijken. Tabel 1 geeft een overzicht van het uitvraagpercentage per domein. Vanwege de betrouwbaarheid van deze cijfers zijn ook de vijfjaargemiddelden opgenomen, waarmee inzicht wordt gegeven in een langere periode.

Tabel 1. Relevant en aandeel uitgevraagd, per domein (procentueel).

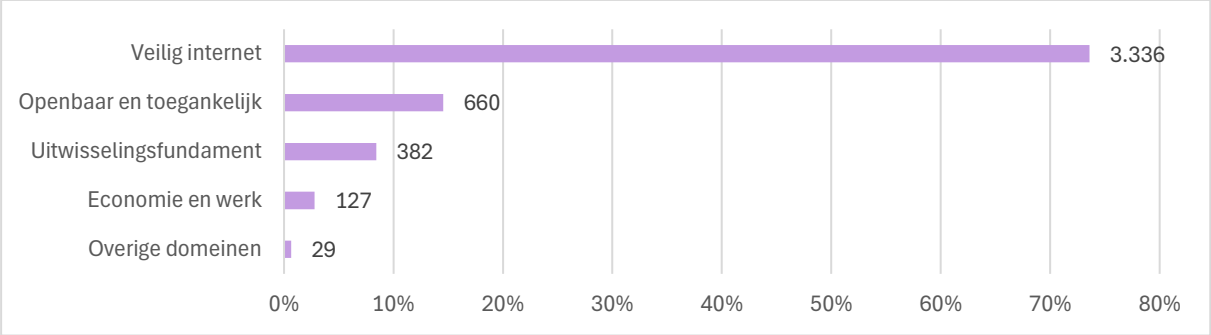
	2025	2025	2021-2025	2021-2025	2021-2025
Domein	**Relevant (absoluut)**	**Percentage uitgevraagd**	**Relevant (absoluut)**	**Percentage Uitgevraagd**	**Aandeel relevant in totaal relevant**
Veilig internet	725	44%	3.336	47%	74%
Openbaar en toegankelijk	183	63%	660	61%	15%
Uitwisselingsfundament	107	39%	382	50%	8%
Economie en werk	55	95%	127	83%	3%
Overige domeinen	10	50%	29	45%	1%
Eindtotaal	1.080	49%	4.534	50%	100%

(Bron: onderzoek aanbestedingen 2025, uitgevoerd in 2026)

Voor de open standaarden die zijn uitgevraagd binnen de betreffende inhoudelijke domeinen is het beeld behoorlijk stabiel: het uitvraagpercentage in 2025 zit relatief dicht in de buurt van het vijfjaargemiddelde. Uitzondering hierop vormen de standaarden die behoren tot het domein van het uitwisselingsfundament: het uitvraagpercentage in 2025 was met 39 procent beduidend lager dan gemiddeld in de afgelopen vijf jaar (50 procent). Dit zijn standaarden - waaronder Digikoppeling, OpenAPI Specification en REST-API Design Rules – die bijdragen aan het veilig uitwisselen van gegevens met burgers en tussen overheidsorganisaties. Een daling in dit domein is teleurstellend als bedacht wordt dat gegevensuitwisseling en datadeling één van de kernprioriteiten is in de Nederlandse Digitaliseringsstrategie (NDS).

Het totale uitvraagpercentage in 2025, eerdergenoemde 49 procent, bevindt zich behoorlijk dicht in de buurt van het gemiddelde in de afgelopen vijf jaar. In eerdere Monitors zagen we dat dit percentage telkens rond de vijftig procent schommelt.

Figuur 1. Aandeel en aantal relevante standaarden per domein (2021 - 2025)



(Bron: onderzoek aanbestedingen 2025, uitgevoerd in 2026)

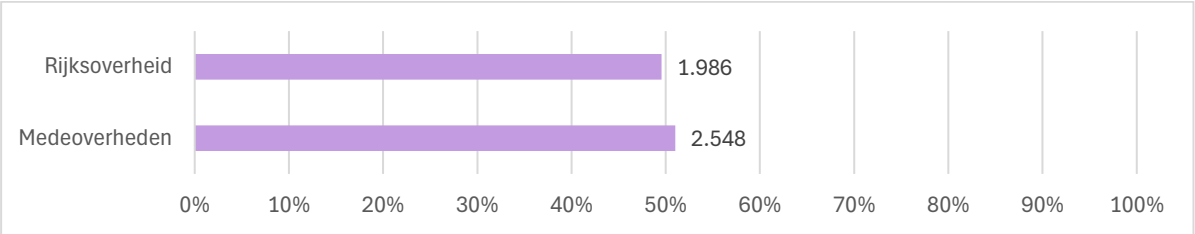
Uit Figuur 1 blijkt dat de open standaarden binnen het domein *Veilig internet* veruit het vaakst relevant zijn bij de aanbestedingen. Bijna driekwart van alle als relevant aangemerkte standaarden valt binnen dit domein, wat een duidelijke invloed heeft op zowel het totaal als het gemiddelde. Dat beeld is verklaarbaar: het merendeel van de standaarden op de "'Pas toe of leg uit'"-lijst valt onder dit domein. Daarnaast zien wij door de tijd een toenemende focus op complexe webapplicaties en clouddiensten. Zo bevatte het merendeel van de beoordeelde aanbestedingen uit 2025 een cloudcomponent (60 procent). Met deze ontwikkeling wordt internetveiligheid steeds relevanter.

De open standaarden in de domeinen Openbaar en toegankelijk, Uitwisselingsfundament en Economie en werk zijn in aflopende mate relevant. We zien een klein aandeel van standaarden binnen de 'Overige domeinen' (Schoon water en beschermde bodem, Bouwen en wonen, Bestuur en recht en Onderwijs en cultuur). Deze overige domeinen bevatten standaarden die in hun werkingsgebied specifieker zijn, wat hun kleinere aandeel verklaart

Uitgevraagde versus relevante open standaarden: bestuurslaag

In Figuur 2 is te zien dat de rijksoverheid in de afgelopen vijf onderzoeksjaren met 50 procent gemiddeld genomen een iets lager uitvraagpercentage kent dan de medeoverheden (51 procent). In de figuur is tevens zichtbaar dat in de aanbestedingen van de rijksoverheid verhoudingsgewijs een iets kleiner aantal relevante open standaarden voorkwam (bijna 2.000) dan bij de medeoverheden (ruim 2.500 relevante standaarden).

Figuur 2. Aandeel relevant en uitgevraagd, per bestuurslaag (2021 - 2025, procentueel)



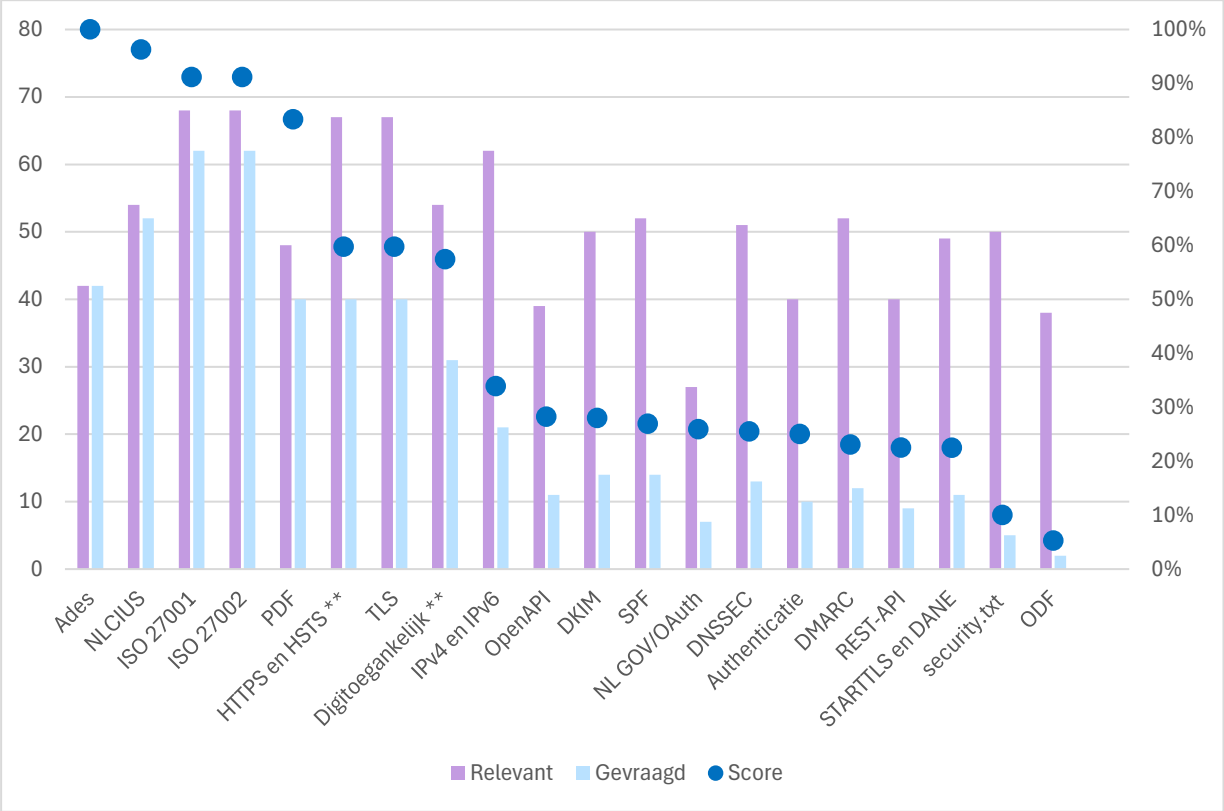
(Bron: onderzoek aanbestedingen 2025, uitgevoerd in 2026)

Uitgevraagde versus relevante open standaarden: individuele standaarden

Ook binnen de domeinen zijn er verschillen te zien in het uitvraagpercentage. Daarom worden in deze sectie de standaarden individueel van elkaar geanalyseerd. Figuur 3 geeft een

overzicht van de uitgevraagde versus de relevante open standaarden. In bijlage 1 zijn de onderliggende cijfers in tabelvorm te vinden. De paarse balken geven aan hoe vaak een standaard relevant was en de blauwe balk hoe vaak deze daadwerkelijk uitgevraagd is. De blauwe stippen in de figuur laten bovendien per standaard het uitvraagpercentage zien, dat wil zeggen: het aandeel relevante standaarden dat daadwerkelijk uitgevraagd is (de 'Score'). De standaarden zijn geordend aan de hand van dit uitvraagpercentage: links de standaarden die relatief het vaakst uitgevraagd worden, rechts de standaarden waarbij dit in mindere mate gebeurt.

Figuur 3. Relevant (>15x), uitgevraagd en aandeel uitgevraagd (score) per standaard (2025).



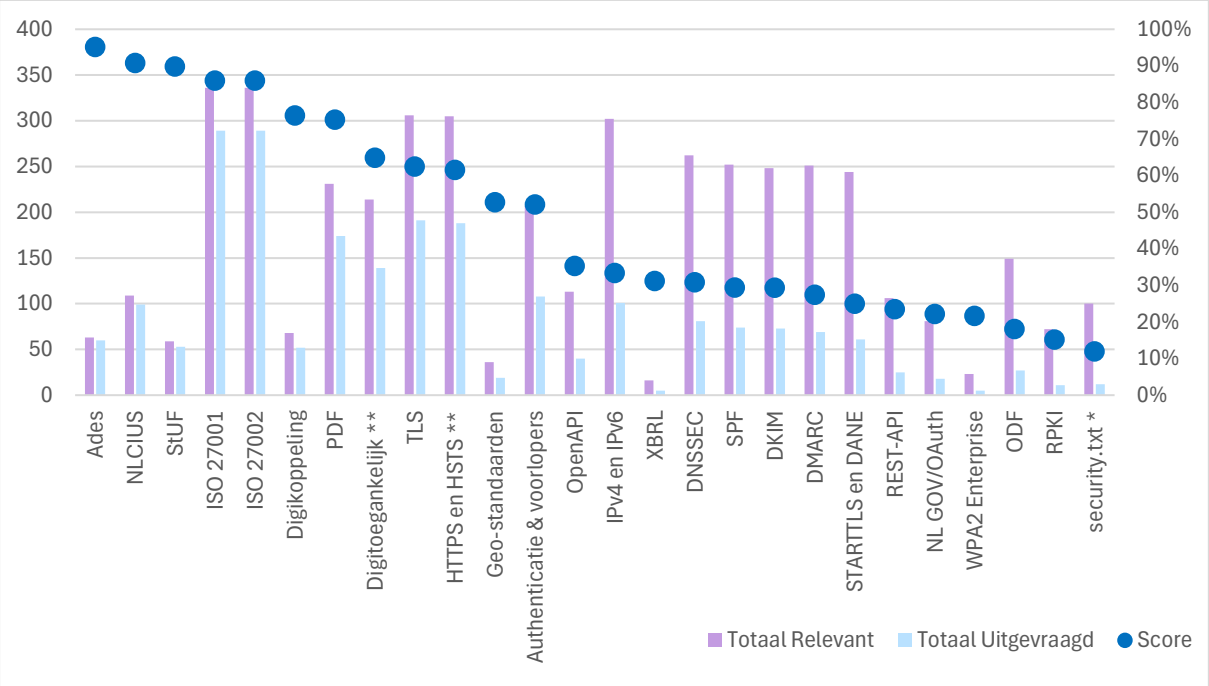
(Bron: onderzoek aanbestedingen 2025, uitgevoerd in 2026)
** Open standaarden met twee sterretjes achter hun naam, zijn wettelijk verplicht.

In de figuur zijn niet alle open standaarden opgenomen; de ondergrens voor opname was dat de standaarden minimaal 15 keer relevant werden geacht. In het totaal was er een achttal standaarden dat door de experts in geen enkele van de onderzochte aanbestedingen, als relevant werd aangemerkt. Dat betrof de volgende standaarden: BWB, ECLI, EML_NL, IFC, JCDR, SIKB0101, SIKB0102 en WDO Datamodel. Dit betekent niet dat deze standaarden in 2025 in geen enkele overheidsaanbesteding relevant waren, in dit onderzoek wordt immers een steekproef van aanbestedingen onderzocht, maar het is wel een aanwijzing dat deze open standaarden verhoudingsgewijs minder vaak relevant zijn.

ISO 27001 en 27002 zijn in absolute aantallen in 2025 zowel het vaakst relevant waren als het meest uitgevraagd. AdES en NLCIUS waren minder vaak relevant, maar zijn met een score van 100 procent en 96 procent relatief het vaakst uitgevraagd. Ook PDF scoort goed.

Kijken we omwille van de betrouwbaarheid van de gegevens, naar een wat langere periode, dan is het beeld van de meest relevante en uitgevraagde standaarden over de afgelopen vijf jaar als volgt (Figuur 4).

Figuur 4. Relevant (>15x), uitgevraagd en aandeel uitgevraagd per standaard (gemiddeld 2021-2025)



(Bron: onderzoek aanbestedingen 2025, uitgevoerd in 2026)
* Open standaarden met een sterretje achter hun naam zijn standaarden die niet gedurende de gehele periode van 5 jaar verplicht waren.

AdES, NLCIUS en StUF kennen het hoogste uitvraagpercentage: respectievelijk 95, 91 en 90 procent in de afgelopen vijf jaar. In absolute zin worden deze standaarden echter veel minder vaak relevant geacht (50 tot 100 keer in de afgelopen 5 jaar) dan een aantal andere standaarden. ISO 27001/27002, TLS, HTTPS en HSTS, IPv4 en IPv6 zijn in absolute aantallen het vaakst relevant (300 tot 350 keer per standaard in de afgelopen 5 jaar).

We zien in deze grafiek een drietal groepen bij de standaarden die vaak relevant zijn (vaker dan 200 keer):

1. Standaarden die vaak relevant zijn én veel (vaker dan 80 procent) uitgevraagd worden: ISO 27001 en 27002;
2. Standaarden die vaak relevant zijn en gemiddeld (50 tot 80 procent) worden uitgevraagd: PDF, Digitoegankelijk, TLS, HTTPS en HSTS en Authenticatie-standaarden (OpenID.NLGov en SAML);
3. En tot slot standaarden die vaak relevant zijn en relatief weinig (minder dan 50 procent) worden uitgevraagd: IPv4 en IPv6, DNSSEC, SPF, DKIM, DMARC, STARTTLS en DANE.

Beide ISO-standaarden worden zeer frequent uitgevraagd: elk bijna 300 keer in de afgelopen vijf jaar (zie ook figuur 4). Een belangrijke verklaring hiervoor is dat zij zijn opgenomen in de Baseline Informatiebeveiliging Overheid (BIO), waarin het basisniveau voor

informatiebeveiliging binnen de overheid is vastgelegd. De BIO is breed bekend en wanneer in een aanbesteding wordt geëist dat aan de BIO wordt voldaan, worden deze standaarden automatisch als uitgevraagd beschouwd. Daarnaast zijn de ISO-standaarden relevant om aan te tonen dat wordt voldaan aan wet- en regelgeving, zoals de AVG. Er loopt op dit moment een discussie over de vraag of de twee ISO-standaarden wel op de "'Pas toe of leg uit'"-lijst moeten blijven staan, juist omdat ze bijna altijd uitgevraagd worden wanneer ze relevant zijn.

De standaarden in de tweede categorie krijgen al langere tijd relatief veel aandacht. Zo geldt voor PDF dat deze term inmiddels zo bekend is dat zij vaak wordt gebruikt als synoniem voor een niet-bewerkbaar einddocument en op deze manier terugkomt inde aanbestedingen. Ook Digitoegankelijk, TLS, HTTPS en HSTS zijn goed bekend. Deze laatste drie zijn sterk aan elkaar gerelateerd en worden gezamenlijk als uitgevraagd beschouwd wanneer ten minste één ervan wordt opgenomen. Daarnaast zijn Digitoegankelijk, HTTPS en HSTS wettelijk verplicht. Dat deze standaarden in sommige aanbestedingen toch ontbreken, kan samenhangen met het feit dat zij met name relevant zijn wanneer webfunctionaliteit wordt gevraagd. In een deel van de aanbestedingen betreft dit echter slechts een beheer- of ondersteuningsportaal, dat een ondergeschikte rol speelt binnen de totale scope van de aanbesteding. Het lijkt erop dat de relevante standaarden voor een dergelijk portaal over het hoofd worden gezien (zie ook het onderdeel hoor en wederhoor in de paragraaf op pagina 21). Verder valt op dat de authenticatie-standaarden in 2025 significant minder zijn uitgevraagd: in 2025 was het uitvraagpercentage 25 procent, ten opzichte van 52 procent in de periode 2021-2025.

Ook voor de standaarden in de derde categorie geldt dat een deel van de verklaring voor het lage uitvraagpercentage, gelegen kan zijn in het over het hoofd zien van de relevante open standaarden voor een beheer- of ondersteuningsportaal. Een dergelijk portaal gaat vaak gepaard met een eigen maildomein, waardoor de mailstandaarden DMARC, DKIM, SPF, STARTTLS en DANE van toepassing zijn. Zelfs wanneer er geen sprake is van een mailserver waarmee daadwerkelijk e-mail wordt verzonden, dient het maildomein minimaal te voldoen aan DMARC en SPF om het risico op phishing en misbruik te beperken.

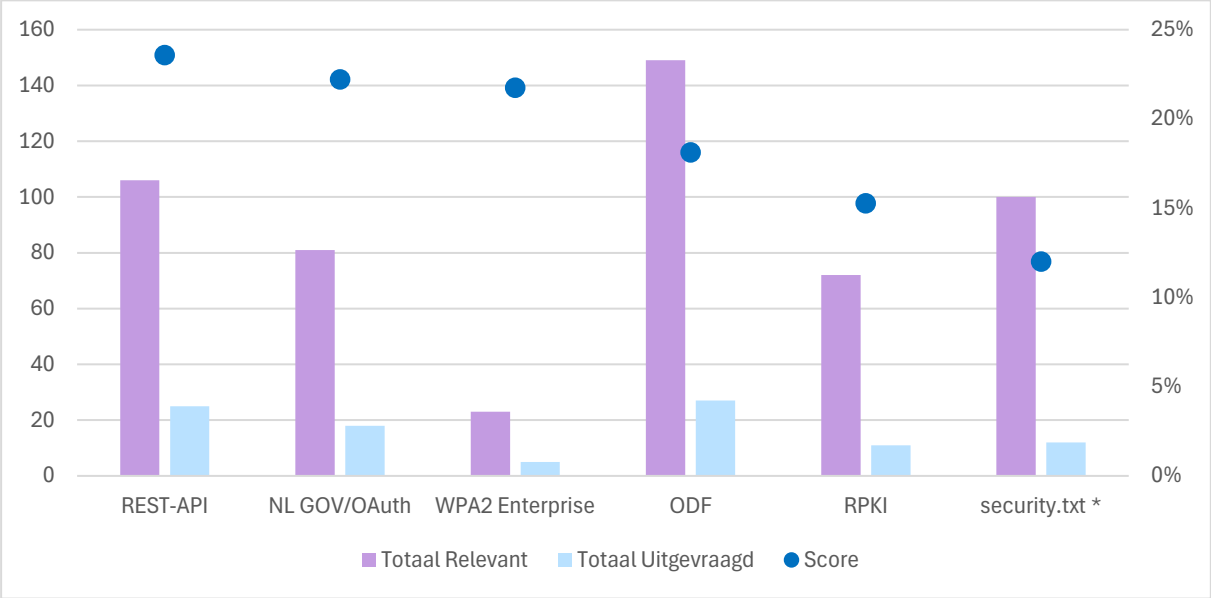
Categorie die aandacht verdient: relevante en weinig uitgevraagde standaarden

We zagen aan de rechterkant van Figuur 4 dat er een aantal standaarden is met lage uitvraagpercentages. In Figuur 5 wordt het zestal standaarden met de laagste uitvraagpercentages in de periode 2021-2025 nogmaals getoond.

Hoewel security.txt in veel gevallen relevant is, werd deze standaard in slechts twaalf procent van deze gevallen meegenomen, kijkend naar periode 2021-2025. Daarbij hoort de kanttekening dat deze standaard pas sinds mei 2023 verplicht is. Daarnaast scoren ook de standaarden RKPI, ODF, NL GOV Assurance en REST-API Design Rules slecht, met een uitvraagpercentage van minder dan 25 procent. Met uitzondering van ODF, bevinden al deze standaarden zich in het domein Veilig internet.

Ondanks de lage score over de periode 2021-2025, kan gemeld worden dat de standaard RPKI in recente jaren steeds vaker wordt uitgevraagd. Zo was het uitvraagpercentage 50 en 56 procent in 2024 en 2025 respectievelijk.

Figuur 5. Relevant (>15x), uitgevraagd en aandeel uitgevraagd (score); laagste percentage uitgevraagd (2021-2025).



(Bron: onderzoek aanbestedingen 2025, uitgevoerd in 2026)

De ODF standaard (Open Document Format), is van belang omdat het een format is voor het bewaren en/of uitwisselen van bewerkbare tekstbestanden, rekenbladen en presentaties. Door deze standaard toe te passen, worden gebruikers niet gedwongen om een applicatie van een specifieke leverancier te gebruiken. En een dergelijk laag uitvraagpercentage is, in het licht van de maatschappelijke en politieke aandacht voor onafhankelijkheid van IT-leveranciers, onwenselijk.

Aangrijpingspunten voor aanvullende maatregelen

Het behalen van een uitvraagpercentage van 100 procent, dat wil zeggen dat altijd alle relevante open standaarden daadwerkelijk uitgevraagd worden, is niet realistisch. Maar het is ook duidelijk dat een gemiddeld uitvraagpercentage van 50 procent als onvoldoende moet worden beschouwd. Als men de adoptie van open standaarden wil verhogen, dan zijn maatregelen nodig. Die mogelijke maatregelen zullen voor een groot deel gericht zijn op het geheel van de lijst van verplichte (en eventueel aanbevolen) standaarden, op het stimuleren van adoptie en op toezicht en handhaving.

In aanvulling op dat algemene beleid valt, zoals in de Monitor van 2025 gesuggereerd, te overwegen om bij de inzet van de schaarse middelen (geld, menskracht), de aandacht te richten op die standaarden waar de meeste winst te behalen valt. En daartoe kan de bovenbeschreven categorisering helpen. Er kan bijvoorbeeld ingezet worden op standaarden die frequent relevant zijn en die tegelijkertijd slechts gemiddeld scoren, denk aan: PDF, Digitoegankelijk, TLS, HTTPS en HSTS en Authenticatie-standaarden. Of op de standaarden die benedengemiddeld uitgevraagd worden, zoals IPv4 en IPv6, DNSSEC, SPF, DKIM, DMARC, STARTTLS en DANE. En er zou ook nog gekozen kunnen worden voor specifieke domeinen zoals veiligheid of het uitwisselingsfundament en zelfs voor bijzondere aandacht voor een specifieke standaard zoals ODF.

Samenvattende conclusie: geen groei in uitvraag relevante standaarden
De mate van adoptie tussen de verschillende open standaarden varieert sterk. Enkele standaarden vallen op door hun hoge uitvraagpercentage, zoals AdES, NLCIUS, StUF, ISO 27001 en 27002. Hun sterke positie hangt waarschijnlijk samen met opname in bredere kaders, zoals de BIO en standaard aanbestedingsteksten. Daartegenover staan standaarden die weliswaar vaak relevant zijn, maar beperkt worden uitgevraagd. De minst vaak uitgevraagde zijn REST-API Design Rules, NL GOV Assurance, WPA2 Enterprise, ODF, RPKI en Security.txt. Hoewel enkele standaarden breed ingeburgerd zijn geraakt, blijft de adoptie van andere standaarden dus duidelijk achter. Dit benadrukt het belang van voortdurende monitoring, gerichte ondersteuning én handhaving van het open standaardenbeleid.

Kijkend naar de wat langere termijn is er in de adoptie van open standaarden in aanbestedingen geen duidelijke groei zichtbaar. Het aandeel uitgevraagde ten opzichte van relevante standaarden schommelt al geruime tijd rond de vijftig procent. Er lijkt een verzadigingspunt bereikt. Ook tussen de onderzochte bestuurslagen zijn nauwelijks verschillen zichtbaar. Een vergelijkbaar beeld zien we bij de verschillende domeinen, met uitzondering van het uitwisselingsfundament, waar in 2025 een daling van het uitvraagpercentage lijkt op te treden. Het grootste deel van de relevante standaarden bevindt zich in het domein Veilig internet (circa driekwart).

In paragraaf 5 van de rapportage op hoofdlijnen van de Monitor Open Standaarden 2025, hebben we de verschillende verklaringen voor de relatief trage adoptie van standaarden op een rij gezet. Let wel, in dit hoofdstuk hebben we ook gezien dat er grote verschillen zijn in de mate van adoptie van de verschillende standaarden.

3. Kwaliteit van aanbestedingen

De aanbestedingen zijn door een tweetal experts beoordeeld waarbij per open standaard werd bekeken in hoeverre die standaard relevante was voor de betreffende aanbesteding en of de standaard (op de juiste wijze) in de aanbesteding werd uitgevraagd. Over het beeld per individuele standaard is in de vorige paragraaf gerapporteerd, in deze paragraaf richten we de aandacht meer op de kwaliteit van de aanbestedingen als geheel. Het oordeel over individuele relevante standaarden is of ze al dan niet uitgevraagd zijn, het oordeel over de aanbesteding als geheel is gebaseerd op het aandeel van het totale aantal relevante standaarden dat daadwerkelijk uitgevraagd is. Bij wijze van voorbeeld: als 12 open standaarden als relevant worden beoordeel en 6 daarvan daadwerkelijk uitgevraagd worden, dan scoort de aanbesteding als geheel 50 procent. Als ze alle 12 uitgevraagd worden, dan is de score 100 procent. Enzovoort.

De beoordelaars hebben de volgende categorieën bij hun oordeel toegepast:

- 'perfect' (alle relevante standaarden zijn gevraagd, 100 procent)
- 'op weg naar perfect' (aanbestedingen waarbij om 67 tot en met 99 procent van de relevante standaarden gevraagd is);
- 'op de goede weg; middenmoot' (met uitvraagscores van 34 tot en met 66 procent);
- 'nog een heel eind te gaan' (met uitvraagscores van 1 tot en met 33 procent);
- 'slecht' (geen van de relevante standaarden is gevraagd).

Nieuw: bonus voor verwijzing naar de lijst of het beleid
In overleg met de opdrachtgever is de bovenstaande wijze van beoordelen enigszins aangepast. Aanbestedingen krijgen dit jaar een bonus wanneer zij naar het open standaardenbeleid of de 'Pas toe of leg uit'-lijst van het Forum Standaardisatie verwijzen. Het is onbevredigend dat twee aanbestedingen met een zelfde of vergelijkbare score, waarbij in de ene aanbesteding wel en in de andere niet naar het beleid en/of de 'Pas toe of leg uit'-lijst werd verwezen, een zelfde oordeel kregen. Een verwijzing dient bovendien als vangnet voor het geval men het vergeet om relevante standaarden expliciet uit te vragen. Met deze verwijzing worden deze vergeten standaarden impliciet alsnog meegenomen, waardoor de aanbesteding als volledi ger kan worden beschouwd. Om deze reden worden aanbestedingen met een verwijzing één categorie hoger beoordeeld.

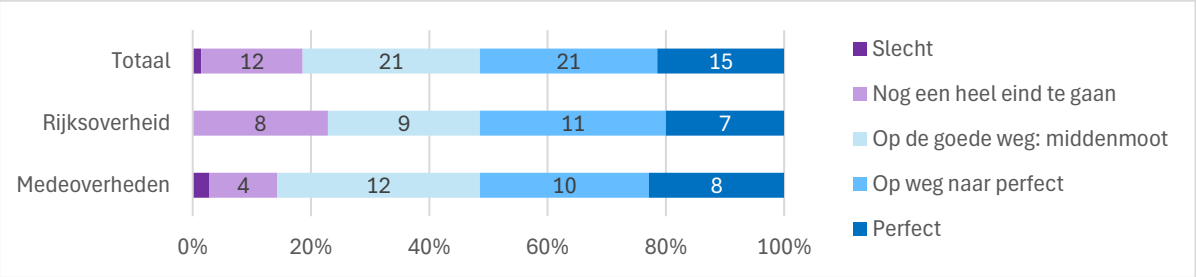
Een voorbeeld: in een aanbesteding wordt 56 procent van de relevante standaarden uitgevraagd, daarbij verwijst men ook naar het open standaardenbeleid. Op basis van de het percentage zou de aanbesteding als 'op de goede weg' worden beoordeeld, maar vanwege de verwijzing wordt de aanbesteding als 'op weg naar perfect' beoordeeld.

Aanbestedingen die 100 procent scoren krijgen op basis daarvan al het label perfect en kunnen dus niet hoger worden beoordeeld als er ook wordt verwezen naar het open standaardenbeleid of de 'Pas toe of leg uit'-lijst. 'Perfect' blijft dus de hoogst haalbare categorie, maar deze aanbestedingen – 100 procent & een verwijzing - krijgen een aparte vermelding in het vervolg van deze paragraaf.

Aanbestedingen 2025

De beoordeling van de aanbestedingen uit 2025 leiden tot het onderstaande beeld (Figuur 6). In deze figuur is per bestuurslaag uiteengezet hoe volledig het open standaardenbeleid is toegepast in de onderzochte aanbestedingen uit 2025.

Figuur 6. beoordelingen van de aanbestedingen uit 2025, uitgesplitst naar bestuurslaag (absoluut)



(Bron: onderzoek aanbestedingen 2025, uitgevoerd in 2026)

In de figuur is te zien dat de experts in totaal 15 aanbestedingen (21 procent) als 'perfect' hebben beoordeeld. Deze aanbestedingen voldoen volledig aan het 'pas toe'-principe; ofwel alle relevante standaarden worden uitgevraagd, ofwel meer dan 66 procent van de relevante standaarden wordt uitgevraagd, inclusief verwijzing naar het open standaardenbeleid of de 'Pas toe of leg uit'-lijst. Door de nieuwe beoordelingssystematiek, de bonus voor verwijzing naar de lijst of het beleid, is vergelijking met eerdere jaren niet mogelijk.

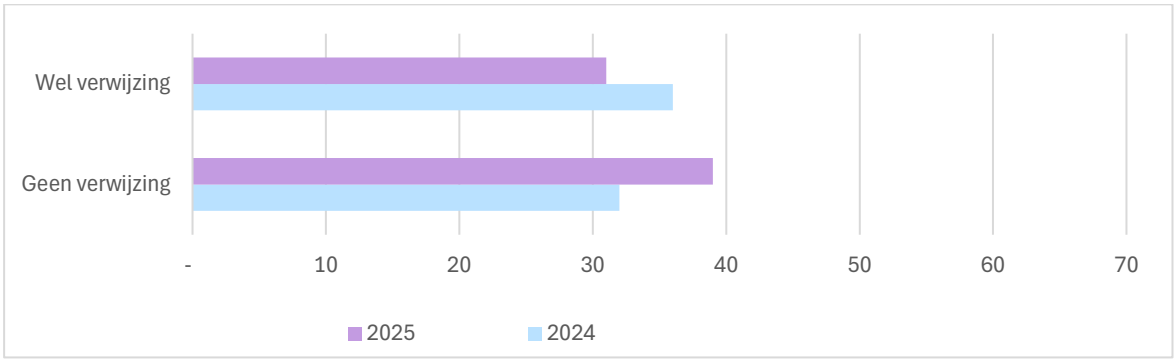
Zeven van de perfecte aanbestedingen kwamen van de rijksoverheid: Dienst Justitiële Inrichtingen, Ministerie van Defensie (tweemaal), Ministerie van Infrastructuur en Waterstaat, Ministerie van Landbouw, Visserij, Voedselzekerheid en Natuur, Ministerie van Volksgezondheid, Welzijn en Sport en Rijkswaterstaat. Acht van de perfecte aanbestedingen kwamen van medeoverheden: Gemeente 's Hertogenbosch, Gemeente Apeldoorn, Gemeente Beverwijk, Gemeente Breda, Gemeente Emmen, Gemeente Sittard-Geleen, Gemeente Tilburg en Gemeente Zutphen.

Verder werd bij 42 aanbestedingen (60 procent) gevraagd om een deel van de voor die aanbesteding relevante standaarden ('op de goede weg' en 'op weg naar perfect'). Slechts één aanbesteding werd als 'slecht' beoordeeld; geen van de relevante standaarden werd uitgevraagd en er werd ook niet verwezen naar het open standaardenbeleid of de 'Pas toe of leg uit'-lijst.

Afname in verwijzingen

Dit jaar werd er in 31 van de 70 beoordeelde aanbestedingen verwezen naar het open standaardenbeleid of de 'Pas toe of leg uit'-lijst (zie Figuur 7). 31 aanbestedingen met een verwijzing staat gelijk aan 44 procent van het totaal. Dat is een daling ten opzichte van 2024, toen 53 procent van de aanbestedingen een verwijzing bevatte. Iets meer van de helft van de beoordeelde aanbestedingen bevat dus geen vangnet voor het geval men vergeten heeft om relevante standaarden expliciet uit te vragen.

Figuur 7. Verwijzing naar open standaardenbeleid of de 'Pas toe of leg uit'-lijst of in aanbestedingen (2025)



(Bron: onderzoek aanbestedingen 2025, uitgevoerd in 2026)

Casuïstiek: (bijna) perfecte aanbestedingen

Ook dit jaar lichten wij weer enkele goede voorbeelden van aanbestedingen uit. Bij de selectie van deze voorbeelden was een 'perfecte' score niet doorslaggevend. Sommige aanbestedingen behalen een perfecte score omdat slechts enkele standaarden relevant waren, terwijl complexere aanbestedingen soms net onder een perfecte score blijven. Daarnaast zijn er aanbestedingen die niet alle standaarden expliciet uitvragen, maar toch hoog scoren dankzij een verwijzing naar de PTOLU-lijst.

<u>Rijksoverheid</u>

Ministerie van Defensie

- De scope van de opdracht omvat de levering van servers, storage en losse componenten, inclusief onderhoud en support, evenals het onderhoud van de bestaande apparatuur.
- De volgende acht standaarden zijn relevant en allemaal uitgevraagd: AdES, HTTPS en HSTS, IPv6, NEN-ISO/IEC 27001, NEN-ISO/IEC 27002, NLCIUS, PDF (NEN-ISO) en TLS.
- Daarnaast wordt er in deze aanbesteding verwezen naar de 'Pas toe of leg uit'-lijst.
- Een 100 procent volledige uitvraag van de relevante standaarden levert deze aanbesteding de score 'perfect' op.

Ministerie van Landbouw, Visserij, Voedselzekerheid en Natuur

- De opdracht betreft een project om vooruitlopend op Europese regelgeving ervaring op te doen met het continu meten van motorvermogen bij (kust)visserijvaartuigen, met als doel mogelijke brede implementatie en kennisdeling binnen de EU.
- De volgende vijf standaarden zijn relevant en allemaal uitgevraagd: NLCIUS, HTTPS en HSTS, TLS, NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002.
- Een 100 procent volledige uitvraag van de relevante standaarden levert deze aanbesteding de score 'perfect' op.

Ministerie van Infrastructuur en Waterstaat

- De opdracht omvat de inkoop van geavanceerde bliksemdetectiediensten voor Nederland, de Benelux, West-Europa en de Caribische Nederlandse gemeenten Bonaire, Sint-Eustatius en Saba.
- Van de negen relevante standaarden zijn er acht uitgevraagd: AdES, Geo-Standaarden, HTTPS en HSTS, NEN-ISO/IEC 27001, NEN-ISO/IEC 27002, NLCIUS, PDF (NEN-ISO) en TLS.
- Alleen ODF is niet uitgevraagd, maar wel relevant
- Een voor 89% volledige uitvraag van de relevante standaarden levert deze aanbesteding de score 'op weg naar perfect' op.

Rijkswaterstaat

- De opdracht betreft een Europese aanbesteding voor het uitvoeren van geodetische en topografische dienstverlening.
- Van de acht relevante standaarden zijn er zeven uitgevraagd: AdES, Geo-Standaarden, HTTPS en HSTS, NEN-ISO/IEC 27001, NEN-ISO/IEC 27002, PDF (NEN-ISO) en TLS.
- Alleen ODF is niet uitgevraagd, maar wel relevant.
- Een voor 88% volledige uitvraag van de relevante standaarden levert deze aanbesteding de score 'op weg naar perfect' op.

Rijksdienst voor Ondernemend Nederland (RVO)

- De opdracht betreft de inkoop, verwerking en levering optische satellietdata en afgeleide producten voor het Satellietdataportaal van de Nederlandse overheid.
- Van de zeven relevante standaarden zijn er zes uitgevraagd: Geo-Standaarden, HTTPS en HSTS, NEN-ISO/IEC 27001, NEN-ISO/IEC 27002, NLCIUS en TLS
- Alleen PDF (NEN-ISO) is niet uitgevraagd, maar wel relevant.
- Een voor 86% volledige uitvraag van de relevante standaarden levert deze aanbesteding de score 'op weg naar perfect' op.

<u>Medeoverheden</u>

Gemeente Tilburg

- De opdracht betreft de levering en implementatie van een nieuw klantgeleidingssysteem met bijbehorende koppelingen, inclusief inrichting, testen, training, datamigratie en ondersteuning tijdens beheer en gebruik.
- De volgende vijftien standaarden zijn relevant en allemaal uitgevraagd: Digitoegankelijk (EN 301 549 met WCAG 2.1), security.txt, OpenAPI Specification, DKIM, STARTTLS en DANE, DMARC, NLCIUS, HTTPS en HSTS, REST-API Design Rules, IPv6, SPF, NEN-ISO/IEC 27001, NEN-ISO/IEC 27002, TLS en NL GOV Assurance.
- Daarnaast wordt er in deze aanbesteding verwezen naar de 'Pas toe of leg uit'-lijst.
- Een 100 procent volledige uitvraag van de relevante standaarden levert deze aanbesteding de score 'perfect' op.

Gemeente Emmen

- De opdracht betreft het leveren en (mede)beheren van de ICT-netwerkvoorziening voor zowel de huidige als de nieuwe omgeving van de gemeente Emmen en haar partners.
- De volgende dertien standaarden zijn relevant en allemaal uitgevraagd: NEN-ISO/IEC 27001, NEN-ISO/IEC 27002, TLS, SPF, DKIM, AdES, DMARC, NLCIUS, DNSSEC, STARTTLS en DANE, HTTPS en HSTS, WPA2 Enterprise en IPv6.
- Een 100 procent volledige uitvraag van de relevante standaarden levert deze aanbesteding de score 'perfect' op.

Gemeente 's Hertogenbosch

- De opdracht betreft het selecteren en contracteren van toekomstbestendige bedrijfssoftware die naadloos aansluit op de primaire processen van de Afvalstoffendienst van de gemeente 's-Hertogenbosch.
- Van de 21 standaarden zijn er negentien uitgevraagd: RPKI, NLCIUS, StUF, Authenticatie-standaarden (OpenID.NLGov en SAML), PDF (NEN-ISO), Digitoegankelijk (EN 301 549 met WCAG 2.1), SPF, DKIM, AdES, DMARC, OpenAPI Specification, DNSSEC, HTTPS en HSTS, security.txt, IPv6, STARTTLS en DANE, TLS, NEN-ISO/IEC 27001 en NEN-ISO/IEC 27002.
- NL GOV Assurance en REST-API Design Rules zijn wel relevant, maar niet uitgevraagd.
- Daarnaast wordt er in deze aanbesteding verwezen naar de 'Pas toe of leg uit'-lijst.
- Een voor 90% volledige uitvraag van de relevante standaarden inclusief een verwijzing naar de 'Pas toe of leg uit'-lijst levert deze aanbesteding de score 'perfect' op.

Gemeente Breda

- De opdracht betreft de digitalisering van de BredaPas, inclusief bijbehorende dienstverlening, die inwoners met een laag inkomen toegang geeft tot voorzieningen en regelingen.
- Van de twintig relevante standaarden zijn er zeventien uitgevraagd: AdES, Digitoegankelijk (EN 301 549 met WCAG 2.1), DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv6, NEN-ISO/IEC 27001, NEN-ISO/IEC 27002, NLCIUS, OpenAPI Specification, RPKI, security.txt, SPF, STARTTLS en DANE, StUF en TLS.
- Authenticatie-standaarden (OpenID.NLGov en SAML), PDF (NEN-ISO) en REST-API Design Rules zijn wel relevant, maar niet uitgevraagd.
- Daarnaast wordt er in deze aanbesteding verwezen naar de 'Pas toe of leg uit'-lijst.
- Een voor 85% volledige uitvraag van de relevante standaarden inclusief een verwijzing naar de 'Pas toe of leg uit'-lijst levert deze aanbesteding de score 'perfect' op.

Gemeente Apeldoorn

- De opdracht betreft de levering en het onderhoud van *multifunctionals* en printers voor de gemeenten Apeldoorn en Epe.
- Van de achttien relevante standaarden zijn er vijftien uitgevraagd: AdES, Authenticatie-standaarden (OpenID.NLGov en SAML), Digitoegankelijk (EN 301 549 met WCAG 2.1), DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv6, NEN-ISO/IEC 27001, NEN-ISO/IEC 27002, NLCIUS, security.txt, SPF, STARTTLS en DANE en TLS.
- ODF, OpenAPI Specification en REST-API Design Rules zijn wel relevant, maar niet uitgevraagd.

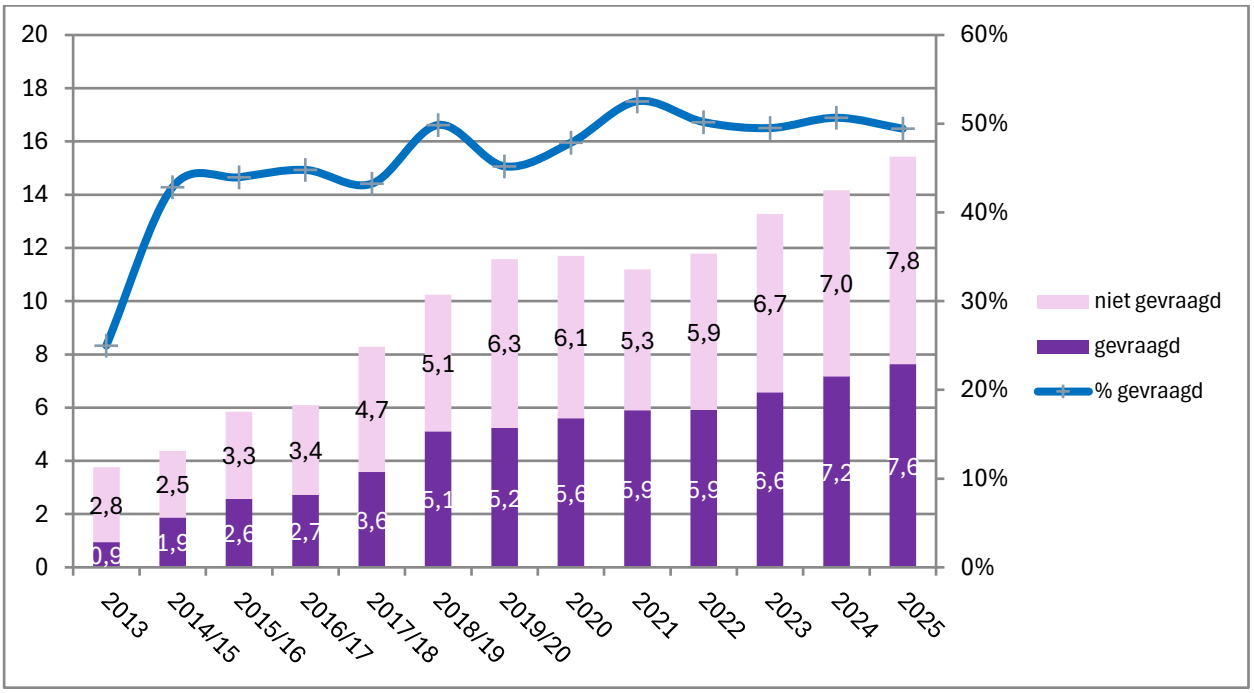
- Een voor 83% volledige uitvraag van de relevante standaarden levert deze aanbesteding de score ‘op weg naar perfect’ op.

Bevindingen door de jaren heen

De onderstaande figuur vergelijkt het aantal relevante standaarden per aanbesteding over een langere periode. Hier is te zien dat het aantal relevante en uitgevraagde standaarden over de jaren heen gestegen is (tot gemiddeld 15,4 per aanbesteding in 2025). In eerdere Monitors is als mogelijke verklaring hiervoor, gewezen op het toegenomen aantal verplichte open standaarden. Die toename deed zich met name voor aan het begin van het ‘Pas toe of leg uit’ beleid (zie ook
Figuur 9, in Bijlage 1). Een andere verklaring is te vinden in het feit dat aanbestedingen steeds complexer worden. Hoewel er geen harde cijfers over bestaan, lijken de gevraagde systemen minder vaak losse applicaties te zijn en vaker onderdelen van een digitaal ecosysteem: werkend in ketens en gekoppeld aan basisregistraties, identity/access-management, berichtenvoorzieningen, cloudplatforms, API’s, data-analyse en cybersecurity.

Figuur 8 bevestigt het beeld dat er in de afgelopen jaren geen significante stijging is in het percentage relevante standaarden dat daadwerkelijk wordt uitgevraagd. Zoals eerder vermeld, werden in 2025 per aanbesteding gemiddeld 49 procent van de relevante standaarden uitgevraagd. Kortom, hoewel er meer standaarden worden uitgevraagd neemt de volledigheid van de aanbestedingen m.b.t. het open standaardenbeleid niet toe.

Figuur 8. Aantal relevante en gevraagde standaarden per aanbesteding (2013-2025)



Samenvattende conclusie
Het grootste gedeelte van de beoordeelde aanbestedingen uit 2025 is goed op weg met het toepassen van het open standaardenbeleid (81 procent scoort 'op de goede weg' of hoger). Slechts één aanbesteding vroeg geen enkele relevante standaard uit. De medeoverheden scoorden in 2025 wat beter dan de rijksoverheid. 86 procent van de beoordeelde aanbestedingen van medeoverheden scoorde 'op de goede weg' of hoger, ten opzichte van 77 procent van de rijksoverheid.

21 procent van de aanbestedingen uit de steekproef kan ook daadwerkelijk als perfect worden beschouwd, al betekent dit door de toekenning van de bonus niet direct dat alle relevante standaarden zijn uitgevraagd. Deze score werd in sommige gevallen ook behaald door het verwijzen naar het open standaardenbeleid of de 'Pas toe of leg uit'-lijst. Bij 44 procent van de aanbestedingen werd hiernaar verwezen.

Ten slotte zien we een toenemende relevantie van open standaarden, met een groeiend aantal relevante standaarden per aanbesteding. De volledigheid waarmee deze standaarden expliciet worden uitgevraagd, blijft echter al jaren nagenoeg gelijk. Desondanks laten aanbestedingen van het ministerie van defensie, het ministerie van Landbouw, Visserij, Voedselzekerheid en Natuur, de gemeente Tilburg en de gemeente Emmen zien dat het ook bij complexe aanbestedingen mogelijk is om alle relevante standaarden van het open standaardenbeleid expliciet uit te vragen.

4. “Leg uit”

Het Leg uit-deel van het open standaardenbeleid kent twee componenten. De voornaamste en formele kant van Leg uit betreft de verantwoording in jaarverslagen. Voor de rijksoverheid geldt dat artikel 3 van de Instructie Rijksdienst bij aanschaf ICT-diensten of ICT-producten stelt dat een rijksorganisatie bij aanschaf moet kiezen voor een ICT-dienst of een ICT-product dat gebruik maakt van de van toepassing zijnde open standaarden van de website van Forum Standaardisatie. Daarvan kan afgeweken worden “indien een dergelijke dienst of product naar verwachting in onvoldoende mate wordt aangeboden, onvoldoende veilig of zeker functioneert, of om andere redenen van bijzonder gewicht.” Daarbij geldt de verplichting om die afwijking gemotiveerd vast te leggen in de departementale administratie. In het jaarverslag verklaart men in algemene zin over de naleving van het open standaarden beleid. Deze verplichting is later uitgebreid naar medeoverheden en uitvoeringsorganisaties en is in april 2022 door het Overheidsbreed Beleidsoverleg Digitale Overheid voor onbepaalde tijd opnieuw bevestigd.

Naast de formele route van de jaarverslagen is er ook een informele route. Er worden ten behoeve van de Monitor 70 aanbestedingen beoordeeld. De conceptoordelen van de experts zijn, onder de noemer van hoor en wederhoor, voorgelegd aan de aanbestedende diensten. Een flink aantal daarvan heeft gereageerd op het conceptoordeel. In een beperkt aantal gevallen werd het initiële oordeel over standaarden aangepast. Verderop in deze paragraaf gaan we in op dit soort discussies. Deze uitwisseling van overwegingen beschouwen wij als de informele manier om afwijkingen van het beleid uit te leggen.

De formele route: leg uit in jaarverslagen

Van de 70 aanbestedingen die onderzocht werden, waren er 4 waarbij alle relevante standaarden uitgevraagd werden, 2 daarvan bij de rijksoverheid en 2 bij de medeoverheden (zie Tabel 2). Dat betekent dat in 66 aanbestedingen op zijn minst 1 of meer verplichte open standaarden die wel relevant werden geacht, niet uitgevraagd werden. Daarover zouden aanbestedende diensten zich in hun jaarverslagen moeten verantwoorden.

Tabel 2. Leg uit, per bestuurslaag (2025)

	Rijk	Medeoverheden	Totaal
Perfect: geen leg uit nodig	2	2	4
Leg uit verplicht	33	33	66

Uit eerdere Monitors bleek dat bij de overheid eigenlijk nooit een dergelijke verantwoording werd aangetroffen. In de jaarverslagen van departementen is veelal een paragraaf opgenomen over open source en de naleving van het open standaardenbeleid. Die departementale jaarverslagen zijn 21 mei 2026 (de derde woensdag in mei, ook wel bekend als verantwoordingsdag) gepubliceerd. De jaarverslagen hebben betrekking op de ministeries en hun agentschappen en diensten. Die laatste twee zijn formeel onderdeel het ministerie, hun verslaglegging is geïntegreerd in het overkoepelende departementale jaarverslag dat de betreffende minister aanbiedt aan het parlement.

In de steekproef van aanbestedingen die beoordeeld zijn, komen de volgende departementen en agentschappen en diensten van departement voor: Defensie, Financiën Belastingdienst), Infrastructuur en Waterstaat (Rijkswaterstaat), Justitie en Veiligheid (Dienst Justitiële Inrichtingen), ministerie van Landbouw, Visserij, Voedselzekerheid en Natuur, ministerie van Onderwijs, Cultuur en Wetenschap, Volksgezondheid, Welzijn en Sport en Economische Zaken (Rijksdienst voor Ondernemend Nederland). In de Tabel 3, hebben informatie over naleving van het beleid voor alle departementen opgenomen.

Tabel 3. Jaarverslagen ministeries 2025.

#	Organisatie	Kernpassage / toelichting	Verwijzing
I	De Koning, Staten Generaal, Overige Hoge Colleges van Staat, Kabinetten en de Kiesraad	Geen passage aangetroffen in scan op open standaarden/open source/aanbestedingen.	Bron
III	Algemene Zaken	Geen passage aangetroffen in scan op open standaarden/open source/aanbestedingen.	Bron
V	Buitenlandse Zaken	De instructie rijksdienst inzake open standaarden en open source is opgenomen in de BZ IT-sourcing strategie. Met de implementatie van de sourcing strategie is naleving van de instructie naar verwachting geborgd.	Bron
VI	Justitie en Veiligheid	JenV stelt eisen aan de inzet van open source bij ICT-projecten en in aanbestedingen vanuit kaders en architectuur. JenV conformeert zich aan het overheidsbeleid om bij ICT-ontwikkeling zoveel mogelijk gebruik te maken van open standaarden en open source software. Het belang hiervan neemt volgens JenV toe door geopolitieke ontwikkelingen.	Bron
VII	Binnenlandse Zaken en Koninkrijksrelaties	BZK handelt volgens artikel 3 van de Instructie Rijksdienst bij aanschaf van ICT-diensten of ICT-producten. BZK wil voldoen aan de open standaarden op de Pas Toe of Leg Uit-lijst van Forum Standaardisatie en volgt publieke websites en diensten in de Monitor Open Standaarden op beveiliging van domeinen en e-mail.	Bron
VIII	Onderwijs, Cultuur en Wetenschap	OCW beschrijft dat bij aanschaf en ontwikkeling van ICT-diensten of ICT-producten in beginsel open standaarden van Forum Standaardisatie moeten worden gebruikt. In 2025 was er geen afwijking van de instructie.	Bron
IX	Financiën en Nationale Schuld	Financiën beschrijft dat de Instructie Rijksdienst voorschrijft dat bij aanschaf en ontwikkeling van ICT-diensten of ICT-producten open standaarden van Forum Standaardisatie moeten worden gebruikt. Bij de Belastingdienst is het proces ingericht, maar centrale registratie ontbreekt. In 2026 wordt monitoring verbeterd.	Bron
X	Defensie	Het beleid inzake open standaarden en open source software is opgenomen in het inkoopproces van software. Geen nadere toelichting of afwijking	Bron
XII	Infrastructuur en Waterstaat	IenW meldt dat voortgang op internetbeveiligingsstandaarden gestaag doorgaat. Bij CIO-oordelen en verwante toetsen wordt toepassing van standaarden conform Forum Standaardisatie expliciet beoordeeld. Uit	Bron

		de jaarlijkse Monitor Open Standaarden (MOS) komt naar voren dat Rijkswaterstaat afgelopen jaar een als perfect beoordeelde aanbesteding heeft gedaan.	
XIII	Economische Zaken	Geen passage aangetroffen in scan op open standaarden/open source/aanbestedingen.	Bron
XIV	Landbouw, Visserij, Voedselzekerheid en Natuur / Diergezondheidsfonds	Geen passage aangetroffen in scan op open standaarden/open source/aanbestedingen.	Bron
XV	Sociale Zaken en Werkgelegenheid	Geen passage gevonden over open standaarden/open source of aanbestedingen in relatie daarmee.	Bron
XVI	Volksgezondheid, Welzijn en Sport	VWS herkent de knelpunten uit de Monitor Open Standaarden, waaronder stagnerende voortgang. Volgens VWS zijn naast aanjagen ook fundamentelere veranderingen nodig in het inkoopproces, contractmanagement en leveranciersmanagement. Aanvullende verdiepende onderzoeken binnen VWS laten zien dat naast het actief blijven adresseren en aanjagen er ook fundamentelere veranderingen nodig zijn in o.a. het inkoopproces en het contract- en leveranciersmanagement dat daarop volgt.	Bron
XXII	Volkshuisvesting en Ruimtelijke Ordening	VRO handelt volgens artikel 3 van de Instructie Rijksdienst bij aanschaf van ICT-diensten of ICT-producten. VRO wil voldoen aan de Pas Toe Of Leg Uit-lijst van Forum Standaardisatie en volgt publieke websites en diensten in de Monitor Open Standaarden op domein- en e-mailbeveiliging.	Bron
XXIII	Klimaat en Groene Groei	Geen passage gevonden over open standaarden/open source of aanbestedingen in relatie daarmee.	Bron

Samenvattend is de meest expliciete verantwoording over het open standaardenbeleid te vinden bij de ministeries van **BZK, OCW, Financiën, IenW, VWS, JenV en VRO**. Het ministerie van OCW meldt expliciet dat er geen afwijkingen zijn van de Instructie Rijksdienst in 2025, het Ministerie van **Financiën meld dat de monitoring bij de Belastingdienst** in 2026 wordt verbeterd, het ministerie van **VWS** benoemt structurele knelpunten in inkoop, contractmanagement en leveranciersmanagement en het ministerie van **JenV zegt** expliciet dat er eisen worden gesteld aan open source en standaarden bij ICT-projecten en aanbestedingen.

Hoor en wederhoor: de informele route

→ Een *grote nationale uitvoeringsorganisatie* (een zbo) stelde in een uitgebreide mail dat verschillende constateringen van de beoordelaars onjuist zouden zijn. Aan de ene kant was de redenering dat dat een aantal standaarden wel degelijk voldoende geborgd waren in de *Non Functional Requirements* (een van de documenten behorend bij de aanbesteding). Andere standaarden zouden volgens de uitvoerder niet relevant zijn door de specifieke aard van het gevraagde systeem.

De herbeoordeling leidt tot een aantal wijzigingen in het initiële oordeel. Het oordeel van security.txt wordt aangepast naar niet relevant omdat er geen publiek benaderbare ondersteunende website of HTTPS-systeem is. Daarnaast worden DKIM, STARTTLS en DANE aangepast naar het oordeel niet relevant, na de bevestiging van de aanbestedende dienst dat er helemaal geen e-mailfunctionaliteit gebruikt wordt.

Het grootste deel van het oorspronkelijke oordeel blijft staan, dat geldt voor standaarden als OpenID.NLGov, SAML, NL GOV Assurance profile OAuth 2.0, OpenAPI Specification en REST-API Design Rules. Er wordt benadrukt dat het noodzakelijk is om de specifieke standaarden te noemen en daar waar het Forum specifieke profielen of ontwerpregels voorschrijft, die ook expliciet moeten worden uitgevraagd.

Voor de mailstandaarden DKIM, DMARC, SPF, STARTTLS en DANE wordt uitgelegd dat deze bij cloudapplicaties vaak relevant zijn, omdat dergelijke diensten doorgaans e-mail gebruiken voor bijvoorbeeld wachtwoordherstel, helpdesk of ondersteuning. Bij DMARC wordt opgemerkt dat deze standaard ook moet worden toegepast op overheidsdomeinen waarmee niet wordt gemaild. Digitoegankelijk is relevant, ook voor interne systemen, omdat ook rolbeheerders beperkingen kunnen hebben

→ Een *agentschap van een ministerie* laat weten blij te zijn dat het initiële oordeel positief is ("op weg naar perfect") maar vraagt zich af waarom de verplichte open standaard **PDF** relevant is voor deze uitvraag. De specifieke data waar het in deze aanbesteding om gaat, wordt nooit als PDF geleverd. De reactie van de beoordelaar is dat er in de aanbestedingsdocumenten een eis staat over het leveren van geschreven rapportage. Op basis daarvan hebben de beoordelaars geconcludeerd dat PDF expliciet had moeten worden uitgevraagd.

→ Een gemeenschappelijke regeling is het niet eens met het oordeel omdat in de aanbestedingsdocumenten de Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT) expliciet van toepassing is verklaard en dat daarin wordt verwezen naar de standaarden van Forum Standaardisatie. ICTU antwoordde dat verwijzing naar de GIBIT volgens Forum Standaardisatie onvoldoende is: standaarden moeten expliciet worden uitgevraagd. De aanbestedende dienst reageerde daarop met de mededeling dat expliciete vermelding van standaarden wordt opgenomen in hun aanbestedingsprocedure voor IT-systemen/applicaties.

→ Een *agentschap van een ministerie* laat weten dat hun aanbesteding een niet-openbare concurrentiegerichte dialoog betrof. In de beoordeelde fase ging het alleen om selectie van partijen; het programma van eisen en wensen was nog niet opgesteld of gepubliceerd. Volgens het agentschap worden de open standaarden pas in de dialoogfase meegenomen en verwerkt in het definitieve programma van eisen en wensen, dat alleen met de geselecteerde partijen wordt gedeeld.

In reactie daarop liet de beoordelaar weten dat het inderdaad om een vroege fase gaat en dat het oordeel daarom een ander gewicht heeft dan bij volledig uitgewerkte aanbestedingen. Positief is dat al wordt verwezen naar de lijst van Forum Standaardisatie. Wel blijft de aanbeveling om standaarden die waarschijnlijk relevant zijn zo vroeg mogelijk expliciet mee te nemen. Het agentschap bedankte voor de terugkoppeling en de bevestiging dat men goed op weg is.

→ Een *medeoverheid* schrijft in een reactie op het initiële oordeel dat men de beoordelingssystematiek herkent, maar plaatst kanttekeningen bij de context. De aanbesteding betreft een raamovereenkomst voor fysieke producten, te bestellen via een digitaal keuzeplatform.

De medeoverheid stelt dat de IT-dienst c.q. het digitaal platform niet de primaire opdracht betreft. Daardoor acht de men standaarden als DNSSEC en security.txt slechts beperkt relevant. Digitoegankelijk is niet expliciet uitgevraagd in het Programma van Eisen, maar wel toegelicht in de inschrijvingsleidraad. Volgens de aanbestedende dienst blijkt uit de inschrijvingen dat digitale keuzeplatformen hieraan invulling geven. De onderzoekers constateren dat het een vaker voorkomend misverstand is dat in dit soort gevallen specifieke standaarden niet relevant zouden zijn.

→ Een andere *medeoverheid* reageerde op het conceptoordeel door te melden dat men bij het opstellen van de aanbesteding gebruik heeft gemaakt van de ICO Wizard van BIO-overheid. Relevante inkoopeisen voor onder meer ketenpartners en clouddiensten zouden zijn opgenomen, evenals verwijzingen naar de BIO. De standaarden uit de 'Pas toe of leg uit'-lijst zijn niet expliciet genoemd, maar volgens de aanbestedende dienst is wel geëist dat relevante nationale en internationale standaarden worden toegepast. Ook werd betwist dat e-mailstandaarden relevant zijn, omdat de uitvraag volgens de aanbestedende dienst geen communicatiedienst betreft. ODF werd evenmin relevant geacht. In de reactie hierop is toegelicht dat de beoordelaar de oplossing als SaaS/hybride dienst ziet, met mogelijk mail vanaf printers. Daarom zijn diverse standaarden relevant bevonden. Ook werd benadrukte dat het in het algemeen verwijzen naar verplichte open standaarden onvoldoende is; zij moeten expliciet genoemd worden.

→ Verschillende organisaties stellen de vraag wat zij zelf hebben aan een oordeel over hun aanbesteding in een fase dat de aanbesteding is afgerond en gunning heeft plaatsgevonden. Vanuit de organisatie bezien is dat een begrijpelijke reactie, tegelijkertijd zien we ook dat het oordeel aanleiding kan zijn om het eigen aanbestedingsbeleid aan te scherpen.

→ In reactie op vragen of bezwaren op het initiële oordeel, als men aangeeft dat men meer in het algemeen heeft verwezen naar de noodzaak om relevante standaarden te implementeren, wordt vaak verwezen naar de veelgestelde vragen op de site van Forum Standaardisatie, zie ook Tekstvak 1.

Tekstvak 1. Veelgestelde vragen website Forum Standaardisatie: verwijzen naar de lijst of de standaard?

Samenvattende conclusie

De verantwoording over het beleid voor open standaarden is in de jaarverslagen over 2025 van de ministeries ongelijkmatig en vaak beperkt uitgewerkt. Waar departementen wel rapporteren, blijft de toelichting meestal procesmatig. Slechts enkele ministeries leggen een concrete relatie met aanbestedingen, monitoring of verbetermaatregelen. Daarmee functioneert de jaarverslagverantwoording nog onvoldoende als volwaardig 'leg uit'-instrument voor naleving van het openstandaardenbeleid.

De hoor-en-wederhoorfase laat zien dat deze een bijdrage levert aan de zorgvuldigheid, correctheid en transparantie van het beoordelingsproces. In een aantal gevallen leidde de inhoudelijke terugkoppeling van aanbestedende diensten tot herbeoordeling of bijstelling van het oordeel.

Tegelijkertijd dat er bij aanbestedende diensten onduidelijkheid bestaat over het moment en de wijze waarop open standaarden moeten worden uitgevraagd, met name in complexe of gefaseerde aanbestedingen. Dit bevestigt het belang van expliciete formuleringen in het Programma van Eisen (PvE) en van meer voorlichting en ondersteuning tijdens het aanbestedingsproces.

Een belangrijk signaal kwam ook van een uitvoeringsorganisatie, die pleitte voor een actiever ondersteuningsaanbod tijdens lopende aanbestedingen. Deze suggestie biedt aanknopingspunten voor doorontwikkeling van het beleid en het ondersteuningsinstrumentarium.

De hoor-en-wederhoorfase vervult draagt bij aan het lerend vermogen van zowel beoordelaars als aanbestedende diensten en levert daarmee inzichten op voor verbetering van het beleid rond open standaarden.

5. Standaarden voor het federatieve datastelsel

Op verzoek van het Federatief Datastelsel (FDS) is er dit jaar in de aanbestedingen ook gekeken naar een aantal standaarden die van belang zijn voor de Generieke Digitale Infrastructuur (GDI) en het FDS. Voor het federatief datadelen is het belangrijk dat organisaties gebruikmaken van gemeenschappelijke standaarden die er voor zorgen dat data uit verschillende bronnen eenduidig beschreven, gevonden en uitgewisseld kan worden, terwijl gegevens bij de bron blijven. Er zijn 8 open standaarden onderzocht: SKOS, REST-API Design Rules, NL GOV profile for CloudEvents, DCAT, Digikoppeling (FSC), MIM, NL-SBB en SHACL. De twee eerste standaarden stonden in 2025 op de Forum Standaardisatie lijst met 'Pas toe of leg uit'-standaarden. NL GOV profile for CloudEvents en NL-SBB staan daar sinds begin 2026 op. Voor Digikoppeling[2] – eveneens een verplichte standaard - is specifiek naar de onderliggende Federated Service Connectivity (FSC) standaard gekeken. De overige onderzochte standaarden staan niet op de Forum Standaardisatie lijst met verplichte open standaarden, maar behoren tot de aanbevolen open standaarden. Om verwarring te voorkomen, verwijzen we in het kader van deze rapportage naar deze 8 open standaarden als de *FDS-standaarden*.

In vergelijking met de rest van het aanbestedingenonderzoek, zijn de FDS-standaarden niet beoordeeld vanuit het perspectief van 'Pas toe of leg uit' (verplichte standaarden), maar betreft het vooral een inventarisatie of ze al dan niet in de onderzochte aanbestedingen relevant waren en gevraagd werden.

Uitgevraagde versus relevante FDS-standaarden

In de 70 aanbestedingen uit 2025 die zijn beoordeeld was het in het totaal 51 maal relevant geweest om de FDS-standaarden uit te vragen(Tabel 4). In de praktijk is er maar 11 keer om. Dat levert een uitvraag-percentage op van 22 procent. Voor standaarden die nodig zijn voor *datadelen* gaat het om 49 FDS-standaarden die uitgevraagd hadden moeten worden en een uitvraagpercentage van 23 procent. De standaarden die dienen om *inzicht in de data* te krijgen hadden 2 keer uitgevraagd moeten worden, maar dat is in geen van beide gevallen gedaan. De uitvraagpercentages bij het Rijk zijn met 25 procent iets hoger dan bij de medeoverheden die 19 procent scoren.

Als we inzoomen op de 8 FDS-standaarden dan zijn er 3 standaarden (DCAT, NL-SBB, SHACL) die in de steekproef ook niet relevant waren voor de betreffende aanbesteding. Dit zijn standaarden die bijdragen aan het meer inzicht krijgen in het data-aanbod.

Drie standaarden die bijdragen aan data inzicht (MIM, SKOS) en aan data delen (CloudEvents) hadden wel uitgevraagd moeten worden maar zijn niet uitgevraagd. (uitvraagpercentage 0 procent) Alleen voor Digikoppeling onderdeel FSC en REST-API Design Rules is een uitvraagpercentage van 33 respectievelijk 23 procent aangetroffen.

[2] Digikoppeling is een familie met een viertal onderliggende standaarden (koppelvlakspecificaties voor gestructureerd gegevensuitwisseling met en tussen overheidsorganisaties). Voor het FDS is alleen de REST API (Digikoppeling API) van belang, en die maakt gebruik van de Federated Service Connectivity (FSC) standaard voor het verlenen van toegang tot API's. Bij deze aanvullende beoordeling specifiek kijken naar FSC.

Tabel 4. FDS-standaarden, relevant en uitgevraagd, naar doel en bestuurslaag (2025).

Doel	Standaard	Relevant	Gevraagd	Uitvraag %
Data delen	Digikoppeling FSC	6	2	33%
	REST-API Design Rules	40	9	23%
	CloudEvents	3	0	0%
	Subtotaal	49	11	22%
Data inzicht	MIM	1	0	0%
	SKOS	1	0	0%
	DCAT	n.v.t.		n.v.t.
	NL-SBB	n.v.t.		n.v.t.
	SHACL	n.v.t.		n.v.t.
	Subtotaal	2	0	0%
Eindtotaal		**51**	**11**	**22%**
Bestuurs-lagen	Rijk	20	5	25%
	Medeoverheden	31	6	19%

(Bron: onderzoek aanbestedingen 2025, uitgevoerd in 2026)

Verloop van de adoptie

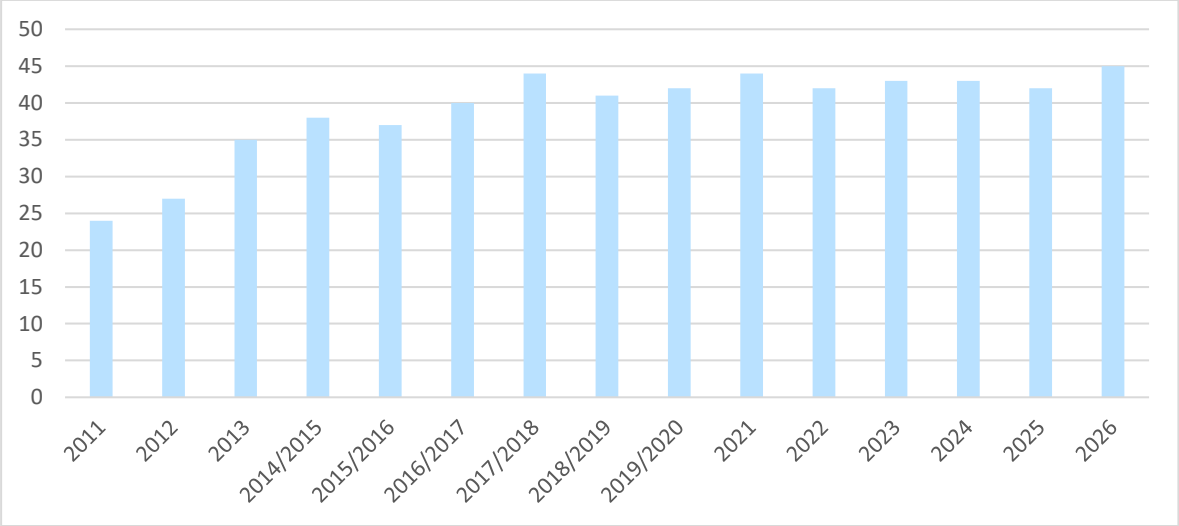
Er zijn zoals eerder aangegeven 2 FDS-standaarden die ook op de 'Pas toe of leg uit'-lijst staan en die dus in voorgaande versies van de Monitor Open Standaarden zijn meegenomen. Die twee standaarden zijn SKOS en REST-API Design Rules. Voor SKOS geldt dat die standaard in de eerder onderzochte aanbestedingen zo zelden relevant waren, dat er geen betrouwbare uitspraken kunnen worden gedaan over de ontwikkeling in de tijd. Dat soort uitspraken kan wel gedaan worden voor de REST-API Design Rules standaard. Het uitvraagpercentage van deze standaard was in 2024 33 procent (tabel 3 in de Monitor Open Standaarden 2025) en 23 procent in 2025 (Tabel 4). Met die daling bevindt de REST-API Design Rules standaard zich weer in de buurt van het 5-jaarsgemiddelde van 22 procent.

Bijlage 1: Overzicht van open standaarden

Tabel 5. Verplichte openstandaarden in 2025

Standaard:	Met als doel:
DKIM, DMARC, SPF	*Bescherming tegen e-mailspoofing en phishing.*
DNSSEC	*Beveiliging van domeinnamen tegen manipulatie.*
HTTPS & HSTS	*Versleuteling van webverkeer; wettelijk verplicht.*
TLS, STARTTLS & DANE	*Beveiligde communicatie over internet en e-mail.*
IPv6 & IPv4	*Internetadressering voor netwerken.*
ISO 27001 & 27002	*Managementsysteem en richtlijnen voor informatiebeveiliging.*
RPKI	*Beveiliging van internetroutering.*
Authenticatie-standaarden (OpenID.NLGov en SAML)	*Authenticatie- en autorisatiestandaarden.*
STIX & TAXII	*Uitwisseling van cyberdreigingsinformatie.*
WPA2 Enterprise	*Beveiligde toegang tot WiFi-netwerken.*
security.txt	*Publicatie van contactinformatie voor beveiligingsmeldingen.*
AdES Baseline Profiles	*Digitaal ondertekenen van documenten.*
Digitoegankelijk (EN 301 549)	*Toegankelijkheid van websites en documenten; wettelijk verplicht.*
ODF, PDF (NEN-ISO)	*Open formaten voor documenten en archivering.*
SKOS	*Structureren van thesauri en begrippenlijsten.*
OpenAPI Specification	*Beschrijven van RESTful API's.*
REST-API Design Rules, NL GOV Assurance profile for OAuth 2.0	*Richtlijnen voor het ontwerpen van REST API's en voor het autoriseren van toegang tot REST-API's.*
NLCIUS, SETU,	*Elektronisch factureren, Inhuur van flexibele arbeidskrachten*
WDO, XBRL	*Douane-informatie en bedrijfsrapportages.*
Digikoppeling, StUF,	*Veilige gegevensuitwisseling.*
Aquo-standaarden, GWSW, SIKB0101/0102, Geo-standaarden	*Standaarden voor waterbeheer, bodeminformatie en geografische informatie*
IFC, NLCS, VISI	*Bouwwerkinformatiemodellen en bouwprocesinformatie.*
BWB, ECLI, EML_NL, JCDR	*Identificatie van wet- en regelgeving en verkiezingsgegevens.*
E-Portfolio NL	*Uitwisseling van werkervaring.*

Figuur 9. Aantallen verplichte open standaarden per onderzoeksjaar (2011 - 2026)



Bron: https://www.forumstandaardisatie.nl

Bijlage 2. Getallen per standaard

	2025	2025	2021-2025	2021-2025
	Relevant	*% uitge-vraagd*	*Relevant*	*% uitge-vraagd*
1. Veilig internet	**725**	**44%**	**3336**	**47%**
NEN-ISO/IEC 27001	68	91%	336	86%
NEN-ISO/IEC 27002	68	91%	336	86%
TLS	67	60%	306	62%
HTTPS en HSTS	67	60%	305	62%
RPKI	9	56%	72	15%
IPv6	62	34%	302	33%
STIX en TAXII	3	33%	11	45%
WPA2 Enterprise	10	30%	23	22%
DKIM	50	28%	248	29%
SPF	52	27%	252	29%
NL GOV Assurance	27	26%	81	22%
DNSSEC	51	25%	262	31%
Authenticatie-standaarden	40	25%	207	52%
DMARC	52	23%	251	27%
STARTTLS en DANE	50	22%	245	25%
security.txt *	50	10%	100	12%
2. Openbaar en toegankelijk	**183**	**63%**	**660**	**61%**
AdES	42	100%	63	95%
PDF (NEN-ISO)	48	83%	231	75%
Digitoegankelijk	54	57%	214	65%
ODF	38	5%	149	18%
SKOS	1	0%	3	67%
3.Economie en werk	**55**	**95%**	**127**	**83%**
NLCIUS	54	96%	109	91%
XBRL	1	0%	16	31%
SETU	0	-	2	50%
4.Uitwisselingsfundament	**107**	**39%**	**382**	**49%**
Digikoppeling	8	88%	68	76%
StUF	8	88%	59	90%
Geo-Standaarden	12	67%	36	53%

OpenAPI Specification	39	28%	113	35%
REST-API Design Rules	40	23%	106	24%
5.Schoon water en beschermde bodem	**0**	**-**	**5**	**60%**
Aquo-standaard	0	-	4	75%
GWSW	0	-	1	0%
6.Bouwen en wonen	**5**	**80%**	**9**	**67%**
VISI	1	100%	2	50%
IFC	1	100%	1	100%
NLCS	3	67%	5	80%
WDO Datamodel	0	-	1	0%
7.Bestuur en recht	**3**	**33%**	**7**	**29%**
ECLI	2	50%	3	33%
BWB	1	0%	4	25%
8.Onderwijs en cultuur	**2**	**0%**	**8**	**25%**
E-Portfolio NL	2	0%	6	17%
Eindtotaal	**1080**	**49%**	**4534**	**50%**

Bijlage 3: Onderzoeksverantwoording

Op Tenderned selecteerden we alle overheidsaanbestedingen die in 2025 aangekondigd werden en die betrekking hadden op de aanschaf van computeruitrusting- en benodigdheden, IT-diensten (adviezen, softwareontwikkeling en internetondersteuning), Telcommunicatiediensten en Software en Informatiesystemen. Uit die selectie van aanbestedingen trokken wij een aselecte steekproef van aanbestedingen bij de rijksoverheid (departementen, agentschappen, diensten en zelfstandige bestuursorganen) en aanbestedingen bij de medeoverheden (gemeenten, provincies, waterschappen en gemeenschappelijke regelingen). Het doel was om voor beide bestuurslagen 35 aanbestedingen te beoordelen. Daarvoor is het nodig om ook een aantal reserve aanbestedingen achter de hand te hebben omdat tijdens het beoordelen soms blijkt dat de aanbesteding niet te beoordelen is omdat die bij nader inzien geen IT-aanbesteding blijkt te zijn, de aanbestedende dienst niet tot het rijk of de medeoverheden behoort of omdat het om een aanbesteding van een raamovereenkomst waarvan de functionaliteit nog niet of slechts zeer ten dele beschreven is.

In de Monitor Open Standaarden 2025 zijn we specifiek ingegaan op de vraag hoe representatief de resultaten van de monitor zijn. We concludeerde toen dat het beperkte aantal beoordeelde aanbestedingen is niet robuust genoeg is voor een wetenschappelijk overallbeeld, maar wel genoeg is om een inzichtelijke doorsnede van de praktijk te geven. Omwille van de betrouwbaarheid hebben we toen de 5-jaarsgemiddelden geïntroduceerd om daarmee een stabieler en betrouwbaarder beeld te krijgen. In deze rapportage hebben we voor diezelfde aanpak gekozen.

Bonus voor verwijzing naar de 'Pas toe of leg uit'-lijst of het open standaardenbeleid
In overleg met de opdrachtgever is de wijze van beoordelen dit jaar enigszins aangepast. Aanbestedingen krijgen voortaan een bonus wanneer zij naar het open standaardenbeleid of de 'Pas toe of leg uit'-lijst van het Forum Standaardisatie verwijzen. Een dergelijke verwijzing dient als vangnet voor het geval men het vergeet om relevante standaarden expliciet uit te vragen. Met deze verwijzing worden deze vergeten standaarden impliciet alsnog meegenomen, waardoor de aanbesteding als vollediger kan worden beschouwd. Om deze reden worden aanbestedingen met een verwijzing één categorie hoger beoordeeld.

Bijvoorbeeld: Een aanbesteding vraag 56% van de relevante standaarden uit, maar verwijst wel naar het open standaardenbeleid. Op basis van de het percentage zou de aanbesteding als 'op de goede weg' worden beoordeeld, maar vanwege de verwijzing wordt de aanbesteding uiteindelijk als 'op weg naar perfect' beoordeeld.

Perfecte aanbesteding zijn al volledig en zullen niet hoger worden beoordeeld wanneer er ook wordt verwezen naar het open standaardenbeleid of de 'Pas toe of leg uit'-lijst. 'Perfect' blijft dus de hoogst haalbare categorie, maar deze aanbestedingen krijgen wel een vermelding in het vervolg van deze paragraaf.

Bijlage 4: Overzicht van aanbestedingen Rijk

Organisatie	Aanbesteding	Relevant & Gevraagd	Relevant & Niet gevraagd	Score (%)	Score inclusief bonus.
ministerie van Defensie	EA Hosting en Infrastructuur Componenten met Onderhoud en Support (HIC) 2026	AdES, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, NLCIUS, PDF, TLS		100%	Perfect +
ministerie van Landbouw, Visserij, Voedselzekerheid en Natuur	Het betrouwbaar vaststellen van het motorvermogen tijdens visactiviteiten via sensoren en blackboxsystemen	HTTPS en HSTS, ISO 27001, ISO 27002, NLCIUS, TLS		100%	Perfect
ministerie van Infrastructuur en Waterstaat	Lightning Detection Data	AdES, Geostandaarden, HTTPS en HSTS, ISO 27001, ISO 27002, NLCIUS, PDF, TLS	ODF	89%	Op weg naar perfect
Rijkswaterstaat (RWS)	Geo-informatie	AdES, Geostandaarden, HTTPS en HSTS, ISO 27001, ISO 27002, PDF, TLS	ODF	88%	Op weg naar perfect
Rijksdienst voor Ondernemend Nederland (RVO)	The procurement and processing of satellite data for the Netherlands Satellite Data Portal	Geo-standaarden, HTTPS en HSTS, ISO 27001, ISO 27002, NLCIUS, TLS	PDF	86%	Op weg naar perfect
ministerie van Defensie	Groot formaat 3D printer	AdES, ISO 27001, ISO 27002, NLCIUS, PDF	ODF	83%	Op weg naar perfect
Rijkswaterstaat (RWS)	31196123 Upgrade IA/IT-systemen voor de Bediening & Bewaking van en vervangen camera's op diverse objecten areaal Zee en Delta	AdES, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, NLCS, PDF, TLS, VISI	ODF, WPA2 Enterprise	82%	Op weg naar perfect
ministerie van Defensie	EA Hosting en Infrastructuur Componenten met Onderhoud en Support (HIC) 2025	AdES, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, PDF, TLS	Digitoegankelijk, ODF	78%	Perfect

ministerie van Infrastructuur en Waterstaat	Beheer en onderhoud, ontwikkeling en toepassing van Verkeers- en vervoersmodellen	AdES, Digitoegankelijk, ISO 27001, ISO 27002, NLCIUS, PDF	Geo-standaarden, ODF	75%	Op weg naar perfect
ministerie van Infrastructuur en Waterstaat	Verwerving SaaS inkoopapplicatie	AdES, Authenticatiestandaarden, Digitoegankelijk, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, NL GOV Assurance, NLCIUS, OpenAPI Specification, PDF, REST-API Design Rules, RPKI, security.txt, TLS	DKIM, DMARC, DNSSEC, SPF, STARTTLS en DANE	75%	Perfect
Rijkswaterstaat (RWS)	Levering en implementatie van een SaaS-oplossing ter ondersteuning van de VTH-processen.	AdES, Digitoegankelijk, DKIM, DMARC, DNSSEC, Geo-standaarden, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, NL GOV Assurance, NLCIUS, SPF, STARTTLS en DANE, StUF, TLS	Authenticatiestandaarden, ECLI, ODF, OpenAPI Specification, REST-API Design Rules, security.txt	73%	Perfect
DJI (Dienst Justitiële Inrichtingen)	Boodschappensysteem ten behoeve van DJI 2.0	AdES, Digitoegankelijk, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, NL GOV Assurance, NLCIUS, OpenAPI Specification, PDF, REST-API Design Rules, SPF, TLS, WPA2 Enterprise	Authenticatiestandaarden, DKIM, DMARC, DNSSEC, ODF, STARTTLS en DANE	70%	Perfect
ministerie van Volksgezondheid, Welzijn en Sport	Europees Openbare Aanbesteding LCMS	AdES, Authenticatiestandaarden, Digitoegankelijk, DKIM, DMARC, HTTPS en HSTS, ISO 27001, ISO 27002, NL GOV Assurance, NLCIUS, PDF, SPF, TLS	DNSSEC, IPv4 en IPv6, ODF, OpenAPI Specification, REST-API Design Rules, security.txt	68%	Perfect
DJI (Dienst Justitiële Inrichtingen)	Vernieuwing Offender Management Systeem (OMS)	Digikoppeling, ECLI, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, NL GOV Assurance, OpenAPI Specification, REST-API Design Rules, TLS	Digitoegankelijk, DKIM, DMARC, security.txt, SPF, STARTTLS en DANE	63%	Op weg naar perfect
ministerie van Defensie	EA Netwerk- en Multifunctional printers A4/A3 formaat	Authenticatiestandaarden, Digitoegankelijk, HTTPS en HSTS, IPv4 en IPv6,	DKIM, DMARC, NL GOV Assurance, SPF, STARTTLS en DANE, WPA2 Enterprise	63%	Op weg naar perfect

		NLCIUS, ODF, OpenAPI Specification, PDF, REST-API Design Rules, TLS			
ministerie van Financiën (belastingdienst)	API Management	AdES, Digitoegankelijk, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, NLCIUS, OpenAPI Specification, RPKI, TLS	Authenticatiestandaarden, DKIM, DMARC, NL GOV Assurance, ODF, REST-API Design Rules, security.txt, SPF, STARTTLS en DANE	55%	Op weg naar perfect
Rijkswaterstaat (RWS)	31204340 RWS Ondersteuning QBLOK	Digitoegankelijk, NLCIUS, PDF	ISO 27001, ISO 27002, ODF	50%	Op de goede weg: middenmoot
DJI (Dienst Justitiële Inrichtingen)	Portofonie inclusief toebehoren en bijkomende Diensten 2026 t.b.v. de rijksoverheid	HTTPS en HSTS, ISO 27001, ISO 27002, NLCIUS, ODF, PDF	Digitoegankelijk, DNSSEC, IPv4 en IPv6, REST-API Design Rules, security.txt, TLS, WPA2 Enterprise	46%	Op de goede weg: middenmoot
Politie	Europees Openbare Aanbesteding LCMS	AdES, Digitoegankelijk, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, NLCIUS, PDF, TLS	Authenticatiestandaarden, DKIM, DMARC, DNSSEC, E-portfolio, NL GOV Assurance, ODF, OpenAPI Specification, REST-API Design Rules, security.txt, SPF, STARTTLS en DANE	43%	Op weg naar perfect
Rijksdienst voor Ondernemend Nederland (RVO)	IWR2025 | Werkplekhardware | Beeldschermen incl. accessoires en optionele Diensten	AdES, HTTPS en HSTS, ISO 27001, ISO 27002, NLCIUS, TLS	Authenticatiestandaarden, Digitoegankelijk, DKIM, DMARC, DNSSEC, IPv4 en IPv6, PDF, security.txt, SPF, STARTTLS en DANE	38%	Op de goede weg: middenmoot
DJI (Dienst Justitiële Inrichtingen)	Een opslagsysteem voor verpakt celmateriaal t.b.v. het NFI	AdES, HTTPS en HSTS, ISO 27001, ISO 27002, NLCIUS, TLS	Digitoegankelijk, DKIM, DMARC, DNSSEC, IPv4 en IPv6, OpenAPI Specification, REST-API Design Rules, security.txt, SPF, STARTTLS en DANE	38%	Op de goede weg: middenmoot
Reclassering Nederland	Beveiligingstechniek	ISO 27001, ISO 27002, PDF	Digitoegankelijk, HTTPS en HSTS, IPv4 en IPv6, TLS, WPA2 Enterprise	38%	Op de goede weg: middenmoot

RDW	EA - Het leveren van een Network Fabric	Digitoegankelijk, HTTPS en HSTS, ISO 27001, ISO 27002, NLCIUS, PDF, TLS	Authenticatie-standaarden, DKIM, DMARC, DNSSEC, IPv4 en IPv6, NL GOV Assurance, OpenAPI Specification, REST-API Design Rules, RPKI, security.txt, SPF, STARTTLS en DANE	37%	Op de goede weg: middenmoot
RDW	Outputmanagement RDW	AdES, Digitoegankelijk, ISO 27001, ISO 27002, NLCIUS, PDF	Authenticatie-standaarden, DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, OpenAPI Specification, REST-API Design Rules, security.txt, SPF, START-TLS en DANE, TLS	33%	Op de goede weg: middenmoot
RDW	Europese Openbare aanbesteding Identity & Access Management (IAM) oplossing voor RDW relaties	HTTPS en HSTS, ISO 27001, ISO 27002, NLCIUS, TLS	Authenticatie-standaarden, Digitoegankelijk, DMARC, DNSSEC, IPv4 en IPv6, NL GOV Assurance, ODF, OpenAPI Specification, PDF, REST-API Design Rules, SPF	31%	Nog een heel eind te gaan
RDW	CyberArk Support	Digitoegankelijk, ISO 27001, ISO 27002, NLCIUS	DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, security.txt, SPF, STARTTLS en DANE, STIX en TAXII, TLS	29%	Nog een heel eind te gaan
ministerie van Defensie	3D metaalprinters	NLCS, PDF	HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, TLS	29%	Nog een heel eind te gaan
ministerie van Onderwijs, Cultuur en Wetenschap	Parametrisch model onderwijshuisvesting	Geo-standaarden, IFC, ISO 27001, ISO 27002, NLCIUS	BWB, Digitoegankelijk, DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, NL GOV Assurance, ODF, OpenAPI Specification, REST-API Design Rules, security.txt, SPF, STARTTLS en DANE, TLS	25%	Nog een heel eind te gaan
DJI (Dienst Justitiële Inrichtingen)	Huren van Digitale Kiosken	NLCIUS	HTTPS en HSTS, IPv4 en IPv6, ODF, TLS	20%	Nog een heel eind te gaan
ministerie van Justitie en Veiligheid	Kantoorautomatisering diensten ten behoeve van het Openbaar Ministerie	AdES, ISO 27001, ISO 27002	Authenticatie-standaarden, Digitoegankelijk, DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, ODF, PDF, security.txt,	19%	Nog een heel eind te gaan

			SPF, STARTTLS en DANE, TLS		
ministerie van Financiën (belastingdienst)	Contact Center as a Service (CCaaS)	ISO 27001, ISO 27002, PDF	Authenticatiestandaarden, Digitoegankelijk, DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, NL GOV Assurance, NLCIUS, ODF, OpenAPI Specification, REST-API Design Rules, security.txt, SPF, STARTTLS en DANE, TLS	16%	Nog een heel eind te gaan
DJI (Dienst Justitiële Inrichtingen)	EPD HIS - Huisartsinformatiesysteem	AdES, ISO 27001, ISO 27002	Authenticatiestandaarden, Digitoegankelijk, DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, NL GOV Assurance, NLCIUS, ODF, OpenAPI Specification, PDF, REST-API Design Rules, security.txt, SPF, STARTTLS en DANE, TLS	15%	Op de goede weg: middenmoot
ministerie van Defensie	Automatische Identificatie Technologie (AIT)	NLCIUS, PDF	DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, ODF, security.txt, SPF, STARTTLS en DANE, TLS	14%	Op de goede weg: middenmoot
ministerie van Volksgezondheid, Welzijn en Sport	Monitoren en samenvatten van mediafragmenten	NLCIUS, PDF	Digitoegankelijk, DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, ODF, security.txt, SPF, STARTTLS en DANE, TLS	13%	Nog een heel eind te gaan
ministerie van Volksgezondheid, Welzijn en Sport	VWS-EA PoC's en Pilots Generieke functies	NLCIUS	Authenticatiestandaarden, Digitoegankelijk, DKIM, DMARC, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, security.txt, SPF, STARTTLS en DANE, TLS	8%	Op de goede weg: middenmoot

Bijlage 5: Overzicht van aanbestedingen Medeoverheden

Organisatie	Aanbesteding	Relevant & Gevraagd	Relevant & Niet gevraagd	Score (%)	Score inclusief bonus.
Gemeente Tilburg	Klantgeleidings-systeem	Digitoegankelijk, DKIM, DMARC, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, NL GOV As-surance, NLCIUS, OpenAPI Specification, REST-API Design Rules, security.txt, SPF, START-TLS en DANE, TLS		100%	Perfect +
Gemeente Emmen	Het leveren en (mede)beheren van de ICT-netwerkvoor-ziening	AdES, DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, NLCIUS, SPF, STARTTLS en DANE, TLS, WPA2 Enterprise		100%	Perfect
Gemeente ‘s Hertogen-bosch	Bedrijfssoftware AFV	AdES, Authenticatie-standaarden, Digi-toegankelijk, DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, NLCIUS, OpenAPI Specification, PDF, RPKI, security.txt, SPF, STARTTLS en DANE, StUF, TLS	NL GOV Assurance, REST-API Design Rules	90%	Perfect
Gemeente Breda	Digitalisering BredaPas	AdES, Digitoegankelijk, DKIM, DMARC, DNS-SEC, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, NLCIUS, OpenAPI Specification, RPKI, security.txt, SPF, STARTTLS en DANE, StUF, TLS	Authenticatie-standaarden, PDF, REST-API Design Rules	85%	Perfect
Gemeente Apeldoorn	Multifunctionals en Printers	AdES, Authenticatie-standaarden, Digi-toegankelijk, DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, NLCIUS, security.txt, SPF, STARTTLS en DANE, TLS	ODF, OpenAPI Specifi-cation, REST-API Design Rules	83%	Perfect

Gemeente Sittard-Geleen	Plan- en regelsoftware Omgevingswet	AdES, DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, NLCIUS, PDF, SPF, STARTTLS en DANE, TLS	Authenticatie-standaarden, Digitoegankelijk, security.txt	81%	Perfect
Gemeente Beverwijk	E-HRM en Salarisverwerkingsdienst	AdES, Authenticatie-standaarden, Digitoegankelijk, DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, NLCIUS, PDF, SPF, STARTTLS en DANE, STIX en TAXII, TLS, WPA2 Enterprise	NL GOV Assurance, OpenAPI Specification, REST-API Design Rules, RPKI, security.txt, XBRL	74%	Perfect
Provincie Noord-Holland	Europese openbare aanbesteding – Raamovereenkomst Eindejaarsgeschenken PNH	AdES, HTTPS en HSTS, ISO 27001, ISO 27002, PDF, TLS	Digitoegankelijk, DNSSEC, security.txt	67%	Op de goede weg: middenmoot
Gemeente Zutphen	Learning Experience Platform (LXP) of Learning Management System (LMS)	AdES, Authenticatie-standaarden, Digitoegankelijk, DKIM, DNSSEC, HTTPS en HSTS, ISO 27001, ISO 27002, NLCIUS, SPF, STARTTLS en DANE, TLS	DMARC, IPv4 en IPv6, NL GOV Assurance, OpenAPI Specification, REST-API Design Rules, security.txt	67%	Op weg naar perfect
Hoogheemraadschap van Rijnland	Technisch beheer en hosting websites HHR en HHSK	AdES, Authenticatie-standaarden, Digitoegankelijk, DKIM, DMARC, DNSSEC, HTTPS en HSTS, ISO 27001, ISO 27002, SPF, TLS	IPv4 en IPv6, OpenAPI Specification, REST-API Design Rules, RPKI, security.txt, STARTTLS en DANE	65%	Op de goede weg: middenmoot
WIJ Groningen	Europees openbare aanbesteding Omgevingsgerichte Oplossing	AdES, DKIM, DMARC, DNSSEC, HTTPS en HSTS, ISO 27001, ISO 27002, NLCIUS, RPKI, SPF, STARTTLS en DANE, TLS	Authenticatie-standaarden, Digitoegankelijk, IPv4 en IPv6, NL GOV Assurance, OpenAPI Specification, REST-API Design Rules, security.txt	63%	Op de goede weg: middenmoot
Gemeente Rotterdam	Aanbesteding Hoog Volume Printers	AdES, Authenticatie-standaarden, Digikoppeling, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, NL GOV Assurance, PDF, REST-API Design Rules, TLS	DKIM, DMARC, DNSSEC, ODF, OpenAPI Specification, SPF, STARTTLS en DANE	61%	Op weg naar perfect
Gemeente Utrecht	Dynamisch Verkeersmanagement	AdES, Digikoppeling, DNSSEC, HTTPS en HSTS,	Digitoegankelijk, DKIM, DMARC, IPv4 en IPv6,	56%	Op de goede

	systeem Zuidwest (DVM Zuidwest)	ISO 27001, ISO 27002, PDF, StUF, TLS	security.txt, SPF, START-TLS en DANE		weg: mid-denmoot
Provincie Noord-Brabant	Klantportaal ten behoeve van E-dienstverlening	AdES, Authenticatie-standaarden, Digi-toegankelijk, Geo-standaarden, ISO 27001, ISO 27002, NLCIUS, OpenAPI Specification, PDF	DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, REST-API Design Rules, security.txt, SPF, TLS	53%	Op weg naar per-fect
Werkorgani-satie HLT Samen	Handhavingsap-plicatie	Digikoppeling, Digi-toegankelijk, DKIM, DMARC, DNSSEC, ISO 27001, ISO 27002, PDF, SPF, STARTTLS en DANE	Authenticatie-standaarden, Geo-standaarden, HTTPS en HSTS, IPv4 en IPv6, ODF, OpenAPI Specification, REST-API Design Rules, security.txt, TLS	53%	Op weg naar per-fect
Gemeente Gooise Me-ren	SaaS-oplossing schuldhulpverlening	AdES, Digikoppeling, Digitoegankelijk, HTTPS en HSTS, ISO 27001, ISO 27002, NLCIUS, PDF, StUF, TLS	Authenticatie-standaarden, DKIM, DMARC, DNSSEC, IPv4 en IPv6, NL GOV Assur-ance, ODF, security.txt, SPF, STARTTLS en DANE	50%	Op weg naar per-fect
Gemeente Hengelo	Telefonie gemeente Hengelo	AdES, HTTPS en HSTS, ISO 27001, ISO 27002, NLCIUS, OpenAPI Specification, REST-API Design Rules, TLS	Authenticatie-standaarden, Digi-toegankelijk, DKIM, DMARC, DNSSEC, IPv4 en IPv6, security.txt, SPF, STARTTLS en DANE	47%	Op weg naar per-fect
Gemeente Zoetermeer	Leermanagement-systeem + functie van opleidingsinter-mediair	AdES, Digitoegankelijk, DKIM, ISO 27001, ISO 27002, NLCIUS, Open-API Specification, PDF, REST-API Design Rules	Authenticatie-standaarden, DMARC, DNSSEC, E-portfolio, HTTPS en HSTS, IPv4 en IPv6, ODF, security.txt, SPF, STARTTLS en DANE, TLS	45%	Op de goede weg: mid-denmoot
Gemeente Hoeksche Waard	Multifunctionals en plotters voor ge-meente Hoeksche Waard	AdES, HTTPS en HSTS, ISO 27001, ISO 27002, NLCIUS, PDF, TLS	Authenticatie-stan-daarden, DKIM, DMARC, DNSSEC, IPv4 en IPv6, security.txt, SPF, STARTTLS en DANE, WPA2 Enterprise	44%	Op de goede weg: mid-denmoot
Gemeente Purmerend	Het leveren van 5G toegangssystemen en een container-management-systeem	AdES, Digikoppeling, Digitoegankelijk, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, TLS	Authenticatie-standaarden, DKIM, DMARC, DNSSEC, NL GOV Assurance, ODF, OpenAPI Specification, REST-API Design Rules, security.txt, SPF, START-TLS en DANE	42%	Op weg naar per-fect

Gemeente Leusden	Gemeente Leusden - Raadsinformatiesysteem	Digitoegankelijk, HTTPS en HSTS, ISO 27001, ISO 27002, NLCIUS, PDF, StUF, TLS	Authenticatie-standaarden, DKIM, DMARC, DNSSEC, IPv4 en IPv6, ODF, OpenAPI Specification, REST-API Design Rules, security.txt, SPF, STARTTLS en DANE	42%	Op de goede weg: middenmoot
Gemeente Amersfoort	Colocatie Datacenter(s)	AdES, ISO 27001, ISO 27002, NLCIUS	Digitoegankelijk, HTTPS en HSTS, IPv4 en IPv6, RPKI, STIX en TAXII, TLS	40%	Op de goede weg: middenmoot
Gemeente Midden-Drenthe	VTH-applicatie	AdES, Digitoegankelijk, Geo-standaarden, ISO 27001, ISO 27002, NLCIUS, PDF, REST-API Design Rules	Authenticatie-standaarden, DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, NL GOV Assurance, ODF, OpenAPI Specification, security.txt, SPF, STARTTLS en DANE, TLS	38%	Op weg naar perfect
Gemeente Almere	Stadspas Almere	Digitoegankelijk, HTTPS en HSTS, ISO 27001, ISO 27002, NLCIUS, PDF, TLS	Authenticatie-standaarden, DKIM, DMARC, DNSSEC, IPv4 en IPv6, NL GOV Assurance, ODF, OpenAPI Specification, REST-API Design Rules, security.txt, SPF, STARTTLS en DANE	37%	Op de goede weg: middenmoot
Noord-Hollands Archief	Collectiebeheersysteem	Digitoegankelijk, HTTPS en HSTS, ISO 27001, ISO 27002, NLCIUS, PDF, TLS	Authenticatie-standaarden, DKIM, DMARC, DNSSEC, IPv4 en IPv6, ODF, OpenAPI Specification, REST-API Design Rules, security.txt, SKOS, SPF, STARTTLS en DANE	37%	Op de goede weg: middenmoot
Gemeente Midden-Groningen	Vervanging applicatie GEO-viewer	AdES, Digikoppeling, Digitoegankelijk, Geo-standaarden, ISO 27001, ISO 27002, PDF, StUF	DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, NL GOV Assurance, NLCS, ODF, OpenAPI Specification, REST-API Design Rules, security.txt, SPF, START-TLS en DANE, TLS	36%	Op weg naar perfect
Gemeente Harderwijk	Dynamische bollard installatie gemeente Harderwijk- herziene uitvraag	ISO 27001, ISO 27002, NLCIUS, PDF	HTTPS en HSTS, IPv4 en IPv6, NL GOV Assurance, ODF, OpenAPI Specification, REST-API Design Rules, TLS	36%	Op de goede weg: middenmoot

Gemeente Haarlemmermeer	Laptopregeling kindpakket	Digitoegankelijk, ISO 27001, ISO 27002, NLCIUS, PDF	DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, security.txt, SPF, STARTTLS en DANE, TLS, WPA2 Enterprise	33%	Op de goede weg: middenmoot
Waterschap Vallei en Veluwe	Cliënt ICT-hardware, smartphones en servers	ISO 27001, ISO 27002, NLCIUS	Digitoegankelijk, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, security.txt, TLS, WPA2 Enterprise	30%	Nog een heel eind te gaan
Gemeente Land van Cuijk	Vaste telefoniediensten; gemeente Land van Cuijk	AdES, IPv4 en IPv6, ISO 27001, ISO 27002, NLCIUS	Authenticatie-standaarden, Digitoegankelijk, DKIM, DMARC, DNSSEC, HTTPS en HSTS, ODF, OpenAPI Specification, REST-API Design Rules, security.txt, SPF, STARTTLS en DANE, TLS	28%	Op de goede weg: middenmoot
ICT Noord- en Midden-Limburg (ICT NML)	ICT Hardware werkplekken	ISO 27001, ISO 27002, NLCIUS	Authenticatie-standaarden, Digitoegankelijk, DKIM, DMARC, DNSSEC, HTTPS en HSTS, IPv4 en IPv6, security.txt, SPF, STARTTLS en DANE, TLS	21%	Nog een heel eind te gaan
Gemeente Midden-Drenthe	Softwarebroker	AdES, ISO 27001, ISO 27002, NLCIUS	Authenticatie-standaarden, Digikoppeling, DKIM, DMARC, DNSSEC, Geo-standaarden, HTTPS en HSTS, IPv4 en IPv6, NL GOV Assurance, ODF, OpenAPI Specification, PDF, REST-API Design Rules, security.txt, SPF, STARTTLS en DANE, StUF, TLS	18%	Nog een heel eind te gaan
Provincie Utrecht	Dataplatform, provincie Utrecht (Best Value)		Authenticatie-standaarden, Digitoegankelijk, DKIM, DMARC, DNSSEC, Geo-standaarden, HTTPS en HSTS, IPv4 en IPv6, ISO 27001, ISO 27002, NL GOV Assurance, OpenAPI Specification, PDF, REST-API Design Rules, security.txt, SPF, STARTTLS en DANE, TLS	0%	Slecht