

Handreiking
'pas toe of leg uit'- standaarden bij aanschaf van ICT

Voor opdrachtgevers en inkopers in het publieke domein

Datum	28 september 2020
Status	Concept versie 1.13

Colofon

Projectnaam	Handreiking 'pas toe of leg uit'-standaarden bij aanschaf van ICT
Auteurs v1	drs. R.M.A. (Wob) Rombouts mr. drs. B. (Bart) Knubben (Bureau Forum Standaardisatie)
Auteurs v2	mr. Dr. M.H. (Mathieu) Paapst mr. I.(Iris) de Groot mr. D. B. (Desiree) Castillo Gosker (Bureau Forum Standaardisatie)
Organisatie	Forum Standaardisatie Postbus 96810 2509 JE Den Haag forumstandaardisatie@logius.nl www.forumstandaardisatie.nl

Inhoudsopgave

COLOFON	2
INHOUDSOPGAVE	3
1 INLEIDING	6
OPDRACHTGEVERS EN INKOPERS IN HET PUBLIEKE DOMEIN	6
AANSCHAF VAN ICT	6
DEZE HANDREIKING, WAAROM?	6
WAT STAAT ER IN DEZE HANDREIKING?	7
2 DE STANDAARDEN VAN DE 'PAS TOE OF LEG UIT'- LIJST EN HUN DOEL	8
EEN OVERZICHT VAN ALLE 'PAS TOE OF LEG UIT'-STANDAARDEN	8
EERSTE HELFT: STANDAARDEN OP DE LIJST DIE VAAK VAN TOEPASSING ZIJN	8
TWEDE HELFT: STANDAARDEN OP DE LIJST DIE MINDER VAAK VAN TOEPASSING ZIJN (MAAR NIET MINDER BELANGRIJK)	9
IETS MEER OVER HET WAAROM	10
<i>Interoperabiliteit</i>	10
<i>Leveranciersonafhankelijkheid</i>	10
<i>Veiligheid</i>	10
<i>Toegankelijkheid</i>	10
<i>Openbaarheid</i>	10
3 DE JUISTE OPEN STANDAARDEN KIEZEN	11
DE BESLISBOOM OPEN STANDAARDEN	11
MEER SPECIFIEK VOOR BIO BEVEILIGSEISEN: GEBRUIK DE ICO-WIZARD	11
4 PRAKTIJKVOORBEEDEN PER ICT CATEGORIE	12
4.1 WEBSITES OF WEBAPPLICATIES	12
<i>CPV codes gerelateerd aan websites en webapplicaties</i>	12
<i>Praktijkvoorbeeld: Webapplicaties voor publieke radiozender</i>	12
<i>Nog een paar algemene opmerkingen over standaarden en websites en webapplicaties</i>	13
<i>Handreiking rijksoverheid verplichte richtlijnen websites en andere online middelen</i>	13
4.2 WERKPLEK EN KANTOORSOFTWARE	13
<i>CPV codes gerelateerd aan werkplek en kantoorsoftware</i>	13
<i>Praktijkvoorbeeld: Digitale werkomgeving</i>	14
4.3 E-MAIL	14
<i>CPV codes gerelateerd aan e-mail</i>	14
<i>Praktijkvoorbeeld: E-mailmanagementvoorziening</i>	15
<i>Nog een paar algemene opmerkingen over standaarden en e-mail</i>	15
4.4 SPRAAK EN/ OF DATACOMMUNICATIEDIENSTEN	16
<i>CPV codes gerelateerd aan spraak en/of communicatiediensten</i>	16
<i>Praktijkvoorbeeld: Vaste spraakdiensten</i>	16
<i>Nog een paar algemene opmerkingen over standaarden en spraak en/of datacommunicatie</i>	17
4.5 MULTIFUNCTIONALS	17

CPV codes gerelateerd aan multifunctionals	17
Praktijkvoorbeeld fullcolor hoogvolume rolprintoplossing.....	17
Nog een paar algemene opmerkingen over standaarden en multifunctionals	18
4.6 FINANCIËEL/ ADMINISTRATIEVE SYSTEMEN	18
CPV codes gerelateerd aan financieel/ administratieve systemen	18
Praktijkvoorbeeld: portaal voor subsidieaanvraag	18
Nog een paar algemene opmerkingen over standaarden en financieel/ administratieve systemen	18
4.7 E-HRM-SYSTEMEN	19
CPV codes gerelateerd aan e-HRM systemen	19
Praktijkvoorbeeld: SaaS oplossing voor HRM en Finance & Control processen	19
Nog een paar algemene opmerkingen over standaarden en e-HRM-systemen	19
4.8 NETWERKEN.....	20
CPV codes gerelateerd aan netwerken	20
Praktijkvoorbeeld: Wifi op alle locaties	20
Nog een paar algemene opmerkingen over standaarden en netwerken.....	21
4.9 BASISREGISTRATIES/ OVERHEIDSGEGEVENS	21
CPV codes gerelateerd aan basisregistraties/ overheidsgegevens.....	21
Praktijkvoorbeeld: zaaksysteem.....	21
Nog een paar algemene opmerkingen over standaarden en basisregistraties/ overheidsgegevens	22
4.10 INHUUR.....	22
CPV codes gerelateerd aan inhuur.....	22
Praktijkvoorbeeld:	22
Nog een paar opmerkingen over standaarden en inhuur.....	23
5 VOORBEELD BESTEKTEKSTEN ALGEMEEN	24
INLEIDING.....	24
TOELICHTENDE BESTEKTEKST	24
GESCHIKTHEIDSEISEN.....	25
SELECTIEMETHODE	25
6 VOORBEELD BESTEKTEKSTEN, SPECIFIEK PER STANDAARD.....	26
BEGRIPPEN	26
ONDERDELEN BESTEKTEKSTEN	26
6.1 INTERNET EN BEVEILIGING	27
IPv4 & IPv6 (Internetnummers) voor servers.....	27
IPv4 & IPv6 (Internetnummers) voor clients.....	28
DNSSEC (Domeinnaambeveiliging)	29
TLS (Beveiligde verbinding).....	31
DKIM (Anti-phishing).....	32
SPF (Anti-phishing).....	33
SAML (Inloggegevens).....	34
ISO 27001 (Managementsysteem informatiebeveiliging).....	35
ISO 27002 (Richtlijnen en principes informatiebeveiliging).....	36
HTTPS en HSTS	37
DMARC	38
Starttls/Dane	39
6.2 DOCUMENTEN EN (WEB)CONTENT	40
PDF/A (Formaat documentpublicatie / archivering).....	40
PDF 1.7 (Formaat documentpublicatie)	41

<i>ODF (Formaat documentbewerking)</i>	42
<i>Digitoegankelijk</i>	43
<i>SKOS (Thesauri en begrippenwoordenboeken)</i>	44
<i>Open API specification (beschrijven van REST APIs)</i>	45
7 TOT SLOT, LEG UIT	46
GELDIGE REDENEN	46
<i>onvoldoende aanbod van de standaard onvoldoende veiligheid van de</i> <i>standaard onvoldoende zekerheid bij het functioneren van de standaard of</i> <i>een andere andere redenen van bijzonder gewicht</i>	46
IN HET JAARVERSLAG OF ANDERS?	46
UITLEGGEN NAAR AANLEIDING VAN DE MONITOR OPEN STANDAARDEN	46

CONCEPT

1 Inleiding

Opdrachtgevers en inkopers in het publieke domein

Ondanks dat overheden en andere organisaties in de publieke sector in verwervingstrajecten moeten kiezen voor de open standaarden van de 'pas toe of leg uit'-lijst, blijkt uit de Monitor Open Standaarden, het jaarlijkse onderzoek naar het gebruik van open standaarden in aanbestedingen, dat dit nog te weinig gebeurt en dat dit onvoldoende wordt uitgelegd. Dit constateert ook de Tweede Kamer, die aandringt op meer gebruik van de juiste open standaarden.

De uiteindelijke verantwoordelijkheid om aan het 'pas toe of leg uit'-beleid te voldoen ligt bij de opdrachtgever of budgethouder onder wienst mandaat een ICT-aanschaf plaats vindt. Aan de andere kant is het de taak van inkoopadviseur om de opdrachtgever zo nodig te wijzen op het 'pas toe of leg uit'-beleid. 'Pas toe of leg uit' geldt voor overheidsorganisaties als een verplichting en andere organisaties in het publieke domein als een dringende aanbeveling. Meer informatie over het 'pas toe of leg uit'-beleid en de Monitor Open Standaarden is te vinden op de website van het Forum Standaardisatie.

Aanschaf van ICT

Aanschaf van ICT is een ruim begrip. Het kan gaan om een product of een dienst, aanbesteding of inbesteding, een heel nieuw project, maar ook beheer en verbouw van reeds bestaande systemen vallen onder het begrip aanschaf. Zie hiervoor ook de bijlage en de toelichting op de instructie rijksdienst bij aanschaf van ICT-diensten en ICT-producten, waarin de verplichting tot toepassen of uitleggen voor rijksorganisaties nader geregeld is en bestuurlijk van toepassing verklaard voor de meeste overheidsorganisaties. Maar of het nu gaat om een verplichting of om een dringend advies, neem als vuistregel aan: besteedt een organisatie met belastinggeld een bedrag van € 50.000 euro of meer aan een ICT-dienst of ICT-product, dan moeten de relevante 'pas toe of leg uit'-standaarden gebruikt worden. Welke dat zijn, dat hangt af van de soort aanschaf en moet per situatie worden bepaald. Zijn de juiste standaarden uiteindelijk in beeld, dan kan een organisatie bewust een keus maken ze wel of niet toe te passen. Voor niet toepassen kunnen goede redenen zijn. Hoe in dat geval correct uitgelegd kan worden, meer in hoofdstuk 7.

Deze handreiking, waarom?

Welke standaarden relevant zijn voor een specifieke aanschaf, dat blijkt in de praktijk niet altijd even eenvoudig te bepalen. Ook leven er veel misverstanden over wat 'leg uit' betekent. Wat geldige redenen zijn om de standaarden van de 'pas toe of leg uit'-lijst achterwege te laten en hoe deze publiek kenbaar gemaakt moeten worden. Het doel van deze handreiking is om methoden aan te reiken om redelijk vlot te kunnen bepalen welke open standaarden relevant zijn voor in een specifieke situatie en door in te gaan op de vraag hoe correct uitgelegd kan worden als een organisatie vervolgens toch bewust de keuze maakt de relevante standaarden achterwege te laten.

Wat staat er in deze handreiking?

Hoofdstuk 2 geeft een overzicht van de standaarden op basis van de officiële 'pas toe of leg uit'-lijst en gaat kort in op de vraag waarom het nodig is om deze standaarden toe te passen.

In hoofdstuk 3 volgt een verwijzing en een korte toelichting op de Beslisboom Open Standaarden om de juiste standaarden te selecteren. Ook staat hier een link naar de ICO-Wizard voor het selecteren van veiligheidseisen op basis van de BIO.

Hoofdstuk 4 geeft voor tien inkoopcategorieën, cpv-codes en een praktijkvoorbeeld van een aanbesteding.

Hoofdstuk 5 gaat over algemeen vragen om open standaarden in een aanbesteding en biedt hiervoor voorbeeld-bestekteksten.

Hoofdstuk 6 gaat over het specifiek vragen van open standaarden in een aanbesteding en biedt voorbeeld-bestekteksten voor een aantal vaak relevante standaarden.

Hoofdstuk 7 gaat in op geldige redenen om relevante open standaarden toch niet toe te passen en hoe dit goed uitgelegd kan worden in het jaarverslag.

2 De standaarden van de 'pas toe of leg uit'- lijst en hun doel

Een overzicht van alle 'pas toe of leg uit'-standaarden

Op de website van het Forum Standaardisatie vind u de formele en meest actuele, versie van de 'pas toe of leg uit'-lijst: <https://forumstandaardisatie.nl/open-standaarden/verplicht>.

Deze officiële 'pas toe of leg uit'-lijst doornemen vergt echter veel aandacht en tijd en ook het nut per standaard blijkt vaak pas bij nadere bestudering van de meeste standaarden. Daarom hier om te beginnen *quick and dirty* een overzicht als om in een oogopslag meer overzicht te krijgen.

In dit overzicht is een tweedeling aangebracht op basis van gebruiksonderzoek naar de vraag om open standaarden in aanbestedingen, tussen standaarden die in de aanbestedingspraktijk vaak, of minder vaak van toepassing lijken te zijn

Let op: dit overzicht dient als eerste scan, bedoeld om snel inzicht te krijgen, maar is zeker niet volledig en zal waarschijnlijk ook snel gedateerd raken na het uitkomen van deze handreiking. Gebruik het daarom vooral als hulpmiddel *naast* en *niet in plaats van* de officiële lijst op de website van het Forum Standaardisatie.

Eerste helft: standaarden op de lijst die vaak van toepassing zijn

Domein	Open standaard	Over	Doel
Internet en beveiliging	IPv4 & IPv6	Internetnummers	Interoperabiliteit
	DNSSEC	Domeinnaambeveiliging	Veiligheid
	TLS	Beveiligde verbinding	Veiligheid
	DKIM	Anti-phishing	Veiligheid
	SPF	Anti-phishing	Veiligheid
	DMARC	Anti-phishing	Veiligheid
	HTTPS & HSTS	Beveiligde websiteverbinding	Veiligheid
	SAML	Inloggegevens	Veiligheid
	RPKI	Beveiliging routing infrastructuur	Veiligheid
	STARTTLS en DANE	Beveiligde verbinding tussen mailservers	Veiligheid
	WPA2 Enterprise	Beveiligde WiFi netwerken	Veiligheid
	STIX en TAXII	Uitwisseling van cyberdreigingsinformatie	Veiligheid
	ISO 27001	Managementsysteem informatiebeveiliging	Veiligheid
	ISO 27002	Richtlijnen en principes informatiebeveiliging	Veiligheid
Documenten en (web)content	PDF/A-1 en -2	Documentpublicatie / archivering	Openbaarheid
	PDF 1.7	Documentpublicatie	Openbaarheid
	ODF	Formaat voor bewerkbare documenten	Openbaarheid
	Ades Baseline Profiles	Digitale handtekeningen	Veiligheid
	Digitotoegankelijk	Toegankelijkheid websites	Toegankelijkheid

	OWMS	Metadata overheidsinformatie	Openbaarheid
	SKOS	Thesauri en begrippenwoordenboeken	Openbaarheid
	OpenAPI Specification	Beschrijven van REST APIs	Interoperabiliteit
E-facturatie en administratie	SETU	Informatie flexibele arbeidskrachten	Interoperabiliteit
	XBRL	Bedrijfsrapportages	Interoperabiliteit
	NLCIUS	Elektronisch factureren	Interoperabiliteit
	WDO	Douane-informatie	Interoperabiliteit

Tweede helft: standaarden op de lijst die minder vaak van toepassing zijn (maar niet minder belangrijk)

Domein	Open standaard	Over	Doel
Stelsels	Digikoppeling	Veilige berichtuitwisseling	Interoperabiliteit
	StUF	Uitwisseling administratieve overheidsgegevens	Interoperabiliteit
	Geo-standaarden	Geografische informatie	Interoperabiliteit
Water en bodem	Aquo-standaarden	Waterbeheer	Interoperabiliteit
	SIKB0101	Bodeminformatie	Interoperabiliteit
Bouw	VISI	Bouwprocesinformatie	Interoperabiliteit
	NLCS	Tekenstandaard	Interoperabiliteit
	COINS	Uitwisseling bouwinformatie	Interoperabiliteit
	IFC	Bouwwerkinformatiemodellen	Interoperabiliteit
Wetgeving Regelgeving Jurisprudentie	BWB	Verwijzingsmechanisme voor wet- en regelgeving	Openbaarheid
	JCDR	Verwijzingsmechanisme decentrale regelgeving	Openbaarheid
	ECLI	Verwijzingsmechanisme rechterlijke uitspraken	Openbaarheid
Onderwijs en loopbaan	e-Portfolio	Uitwisseling werkervaring en competenties	Interoperabiliteit
Verkiezingen	EML_NL	Verkiezingsgegevens	Openbaarheid

Iets meer over het waarom.

Dat reden dat de open standaarden op de 'pas toe of leg uit'-lijst staan, is omdat deze standaarden meer en beter gebruikt moeten worden in het publieke domein. In het overzicht hierboven staat in de laatste kolom per open standaard met een doel genoemd. Vaak dient het gebruik van de standaard meer doelen, maar het genoemde doel is hier het meest in het oog lopend. Hier kort iets meer over.

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 voor interoperabiliteit en leveranciersafhankelijkheid. Bij sommige standaarden wordt interoperabiliteit tentatief aangemerkt als het meest prominente doel omdat zij vooral zorgen voor een goede doorstroom van digitale gegevens in ketens.

Leveranciersafhankelijkheid

Interoperabiliteit en leveranciersafhankelijkheid worden vaak in een adem genoemd als het gaat om het gebruik van open standaarden. Want het is de openheid van de standaarden die kan zorgen voor marktwerking. Meer marktwerking betekent meer keuze in leveranciers minder hoge kosten voor ICT voor de publieke sector.

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 deze veiligheidsstandaarden kan tot grote schade leiden tast de betrouwbaarheid van 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, ook in de digitale wereld.

Meer over toegankelijkheid: <https://www.digitoeankelijk.nl/>

Openbaarheid

Openbaarheid van bestuur en rechtspraak, openbare informatie, linked open data, zonder het gebruik van de juiste open open standaarden niet waar te maken. Maak publieke informatie vindbaar, herbruikbaar en openbaar en gebruik hiertoe de standaarden van de 'pas toe of leg uit'-lijst als ze relevant zijn voor de ICT waar u aan werkt.

Deze korte schets van de doelen licht maar tipje van de sluiter op van de wereld die achter het gebruik van open standaarden schuil gaat, want meer gaat het bestek van deze handreiking te buiten. Maar hopelijk is het genoeg om u ervan te overtuigen dat het gebruik van de juiste open standaarden belangrijk is voor de kwaliteit van de digitale infrastructuur als geheel die gefinancierd wordt met belastinggeld en dat letten op het gebruik van de juiste standaarden hoort bij verantwoord ICT-opdrachtgeverschap in het publieke domein.

3 De juiste open standaarden kiezen

De Beslisboom Open Standaarden

Op de website van het Forum Standaardisatie staat het meest aangewezen instrument om de weg te vinden in de toepassingsgebieden bij de standaarden op de 'pas toe of leg uit'- lijst.

Het is bedoeld om tot een eerste inschatting te komen van de juiste standaarden voor een ICT-aanschaf.

Beantwoord hiertoe de vragen bij voorkeur samen met de deelnemers van het project van ICT-aanschaf.

Neem voor meer advies op maat contact op met het Bureau Forum Standaardisatie.
info@forumstandaardisatie.nl



Meer specifiek voor BIO beveiligingseisen: gebruik de ICO-Wizard

Heel vaak is de BIO (Baseline Informatiebeveiliging Overheid) van toepassing, danwel de ISO 27001 en ISO 27002 standaarden. Ten tijde van het schrijven van deze handreiking ontwikkelt het Centrum voor Informatie en Privacybescherming een instrument om te zorgen dat bij inkoop op basis van de BIO tijdig de juiste veiligheidsnormen in beeld komen zodat de organisatie ze ook kan opnemen in het programma van eisen van een aanbesteding.

De ICO-Wizard is een prima instrument om deze beveiligingsnormen meer en beter in praktijk te brengen. Veel standaarden van de 'pas toe of leg uit'- lijst zijn hierin ook opgenomen. <https://www.bio-overheid.nl/ico-wizard/>

Let op: Het gaat hier echter alleen om de standaarden voor internet en beveiliging en niet om alle standaarden van de 'pas toe of leg uit'-lijst. Daarvoor is de Beslisboom Open Standaarden meer geschikt.

4 Praktijkvoorbeelden per ICT categorie

Om een brug te slaan tussen de praktijk en de toepassingsgebieden van de standaarden 'pas toe of leg uit'-lijst, geven we hier voorbeelden van ICT aanbestedingen voor tien ICT-categorieën:

1. Websites of webapplicaties
2. Werkplek en kantoorsoftware
3. E-mail
4. Spraak- of datacommunicatiediensten
5. Multi-functionals
6. Financieel/administratieve systemen
7. e-HRM-systemen
8. Netwerken
9. Basisregistraties/overheidsgegevens
10. Inhuur

Met een rijtje CPV-codes wordt een poging gedaan nader te verduidelijken wat voor ICT-diensten en ICT-producten deze categorie kan inhouden. Deze "Common Procurement Vocabulary"-codes zijn het Europese classificatiesysteem voor werken, leveringen en diensten.

Valt uw aanschaf in een of meer van deze categorieën, let dan vooral op de toepassing van de standaarden die bij de voorbeelden worden genoemd en hierbij nader worden toegelicht.

4.1 Websites of webapplicaties

CPV codes gerelateerd aan websites en webapplicaties

48000000-8 Software en informatiesystemen
48222000-0 Software voor webserver
48224000-4 Software voor webpage-editen
72000000-5 IT-diensten: adviezen, softwareontwikkeling, internet en ondersteuning
72330000-2 Diensten voor inhouds- of datastandaardisatie en -classificatie
72413000-8 Diensten voor het ontwerpen van websites
72415000-2 Verlenen van hostingdiensten voor websites
72417000-6 Internet-domeinnamen

Praktijkvoorbeeld: Webapplicaties voor publieke radiozender

De Nederlandse Publieke Omroep doet 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.

<https://www.tenderned.nl/tenderned-tap/aankondigingen/132192>

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, HSTS en TLS, want het betreft een webapplicatie en voor beveiliging van netwerkverbindingen.
- Open API, vanwege de wens om gebruik te maken van gestandaardiseerde en gedocumenteerde koppelvlakken.

Nog een paar algemene opmerkingen over standaarden en websites en webapplicaties

DNSSEC voorkomt dat cybercriminelen het internetverkeer van uw organisatie kunnen omleiden naar valse websites of e-mailpostbussen.

TLS, HTTPS en HSTS zorgen ervoor dat gebruikers de authenticiteit van de website kunnen controleren en dat hackers de internetverbinding met een website of e-mail server niet kunnen afluisteren en zo gevoelige informatie kunnen onderscheppen.

Biedt uw website of webapplicatie e-mailfunctionaliteit, let dan ook op deze standaarden:

De combinatie van SPF, DKIM en DMARC bestrijdt e-mailfraude waaronder phishing en de verspreiding van gijzelsoftware.

STARTTLS en DANE zorgen ervoor dat mailverkeer middels encryptie onderweg niet kan worden afgeluisterd.

Ieder half jaar meet het Forum Standaardisatie het gebruik van belangrijke informatieveiligheidsstandaarden en publiceert de resultaten.

Handreiking rijksoverheid verplichte richtlijnen websites en andere online middelen

Op de website van het Forum Standaardisatie staat de Handreiking verplichte richtlijnen websites en online middelen waarin ook de standaarden van de 'pas toe of leg uit'- lijst zijn opgenomen. Deze handreiking is in eerste instantie geschreven voor rijksoverheidsorganisaties, maar ook organisaties buiten het rijk kunnen hier hun voordeel mee doen.

4.2 Werkplek en kantoorsoftware

CPV codes gerelateerd aan werkplek en kantoorsoftware

30200000-1 Computeruitrusting en -benodigdheden
 30213000-5 Personal computers
 32250000-0 Mobiele telefoons
 48000000-8 Software en informatiesystemen
 48200000-0 Software voor netwerken, internet en intranet
 48510000-6 Communicatiesoftware
 48620000-0 Besturingssystemen
 48300000-1 Software voor het maken van documenten, tekeningen, afbeeldingen, dienstregelingen en productiviteit
 72212300-2 Diensten voor ontwikkeling van software voor het maken van documenten, tekeningen, afbeeldingen, dienstregelingen en productiviteit

72512000-7 Documentbeheerdiensten
72330000-2 Diensten voor inhouds- of datastandaardisatie en -classificatie

Praktijkvoorbeeld: Digitale werkomgeving

Het Huis voor Klokkenluiders zoekt 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.

<https://www.tenderned.nl/tenderned-tap/aankondigingen/125308>

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.
- IPv4 en IPv6, voor internetverbinding van de digitale werkomgeving.
- DNSSEC, voor domeinnaam van de digitale werkomgeving.
- STARTTLS, DANE, SPF en DKIM, 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.

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.

4.3 E-mail

CPV codes gerelateerd aan e-mail

48000000-8 Software en informatiesystemen
48200000-0 Software voor netwerken, internet en intranet
48811000-6 E-mail-systeem
64200000-8 Telecommunicatiediensten
64216000-3 Elektronische berichten- en informatiediensten
64216120-0 E-maildiensten
72000000-5 IT-diensten: adviezen, softwareontwikkeling, internet en ondersteuning
72400000-4 Internetdiensten
72412000-1 Provider voor e-maildiensten
72417000-6 Internet-domeinnamen

Praktijkvoorbeeld: E-mailmanagementvoorziening

Het ministerie van Algemene Zaken vraagt in een aanbesteding om het leveren en beheren van een e-mailmanagementvoorziening voor het Platform Rijksoverheid Online (PRO), inclusief facultatieve dienstverlening rondom optimalisatie van het e-mailkanaal.

<https://www.tenderned.nl/tenderned-tap/aankondigingen/146062>

In deze aanbesteding zijn waarschijnlijk de volgende standaarden relevant:

- IPv4 en IPv6, 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 / 27002, voor informatiebeveiliging.
- PDF en ODF vanwege het werken met reviseerbare en niet-reviseerbare documenten (zoals kunnen uitdraaien van managementrapportages).
- Open API specificatie, vanwege de mogelijkheid dat gebruik zal worden gemaakt van een API.

Zoals hiervoor al aangegeven is de BIO, danwel 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 emailadressen) gemigreerd moest gaan worden van het oude naar het nieuwe systeem.

Ook het gebruik van ODF is in deze aanbesteding terecht van de toekomstige leverancier geeist:

“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 geeist:

“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”.

Nog een paar algemene opmerkingen over standaarden en e-mail

DNSSEC voorkomt dat cybercriminelen het internetverkeer van uw organisatie kunnen omleiden naar valse websites of e-mailpostbussen.

TLS, HTTPS en HSTS zorgen ervoor dat gebruikers de authenticiteit van de website kunnen controleren en dat hackers de internetverbinding met een website of e-mail server niet kunnen afluisteren en zo gevoelige informatie kunnen onderscheppen.

De combinatie van SPF, DKIM en DMARC bestrijdt e-mailfraude waaronder phishing en de verspreiding van gijzelsoftware.

STARTTLS en DANE zorgen ervoor dat mailverkeer middels encryptie onderweg niet kan worden afgeluisterd.

Ieder half jaar meet het Forum Standaardisatie het gebruik van belangrijke informatieveiligheidsstandaarden en publiceert het de resultaten in een magazine.

In de Baseline Informatiebeveiliging Overheid (BIO) is opgenomen dat persoonsgegevens niet onversleuteld over onbeveiligde/onvertrouwde netwerken verzonden mogen worden. Informatie die is opgenomen in een elektronisch bericht behoort passend te worden beschermd. Deze baseline verplicht zodoende afgedwongen versleuteling van verbindingen zoals STARTTLS die in combinatie met DANE ondersteunt.

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

Het gaat 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-mail-protocol 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.

4.4 Spraak en/ of datacommunicatiediensten

CPV codes gerelateerd aan spraak en/of communicatiediensten

64200000-8 Telecommunicatiediensten
64215000-6 IP-telefoondiensten
32400000-7 Netwerken
32250000-0 Mobiele telefoons
32550000-3 Telefoonuitrusting
72417000-6 Internet-domeinnamen

Praktijkvoorbeeld: Vaste spraakdiensten

Luchtverkeersleiding Nederland wil 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.

<https://www.tenderned.nl/tenderned-tap/aankondigingen/162632>

Voor deze aanbesteding zijn waarschijnlijk de volgende standaarden relevant:

- IPv4 / IPv6, 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.
- ISO27001 / 27002. De leverancier is immers de spil in het communicatienetwerk van LVNL.

Nog een paar algemene opmerkingen over standaarden en spraak en/of datacommunicatie

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 enveilig 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 een absolute must.

4.5 Multifunctionals

CPV codes gerelateerd aan multifunctionals

30200000-1 Computeruitrusting en -benodigdheden
30232100-5 Printers en plotters
48773000-7 Printersoftware-faciliteiten
48824000-0 Printerservers
30216110-0 Scanners voor computergebruik
48318000-0 Scannersoftware
79999100-4 Scanningsdiensten

Praktijkvoorbeeld fullcolor hoogvolume rolprintoplossing

IUC-Noord vraagt in een aanbesteding om het leveren, installeren en onderhouden van een fullcolour hoogvolume rolprintoplossing en bijbehorende randapparatuur. Niet limitatief zijn de volgende standaarden relevant:

<https://www.tenderned.nl/tenderned-tap/aankondigingen/168900>

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

Nog een paar algemene opmerkingen over standaarden en multifunctionals

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 emailen, dan dienen ook de beveiligingstandaarden uit de inkoopcategorie "email" hier geëist te worden.

4.6 Financieel/ administratieve systemen

CPV codes gerelateerd aan financieel/ administratieve systemen

48400000-2 Software voor zakelijke transacties en persoonlijke zaken
48440000-4 Software voor financiële analyse en boekhouding
48444100-3 Factureringsstelsel
79999200-5 Factureringsdiensten

Praktijkvoorbeeld: portaal voor subsidieaanvraag

ZonMw financiert gezondheidsonderzoek. Het doel van de nieuwe applicatie 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.

<https://www.tenderned.nl/tenderned-tap/aankondigingen/119454>

Standaarden die waarschijnlijk relevant zijn:

- XBRL, want het betreft rapportages met een financiële component en gegevensuitwisseling met een financieel stelsel.
- HTTPS en HSTS & TLS, want het betreft een webportaal.
- ISO 27001 / 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.

Nog een paar algemene opmerkingen over standaarden en financieel/

administratieve systemen

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.

4.7 E-HRM-systemen

CPV codes gerelateerd aan e-HRM systemen

Algemene personeelsdiensten voor de overheid
79211110-0 Loonadministratiediensten
79600000-0 Recruiteringsdiensten
79631000-6 Personeels- en loonlijstdiensten
79634000-7 Diensten voor loopbaanbegeleiding
48440000-4 Software voor financiële analyse en boekhouding
48450000-7 Software voor tijdregistratie of human resources

Praktijkvoorbeeld: SaaS oplossing voor HRM en Finance & Control processen

De Nederlandse Zorgautoriteit zoekt een partij voor het leveren van een integrale SaaS oplossing voor de HRM en F&C processen en 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.

<https://www.tenderned.nl/tenderned-tap/aankondigingen/129833>

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 / 27002, voor informatie-veiligheid van o.a. persoonsgegevens.
- SAML, want single sign on functionaliteit gevraagd.
- HTTPS, 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.

Nog een paar algemene opmerkingen over standaarden en e-HRM-systemen

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.

4.8 Netwerken

CPV codes gerelateerd aan netwerken

32400000-7 Netwerken
48200000-0 Software voor netwerken, internet en intranet
Toevoegen
48210000-3 Netwerksoftware
72000000-5 IT-diensten: adviezen, softwareontwikkeling, internet en ondersteuning
72513000-4 Kantoorautomatiseringsdiensten
72700000-7 Computernetwerkdiensten
72710000-0 LAN-diensten
72720000-3 WAN-diensten
72400000-4 Internetdiensten
72411000-4 Internetproviders (ISP)
64212000-5 Mobiele telefoondiensten

Praktijkvoorbeeld: Wifi op alle locaties

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. 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 en support van apparatuur en dienst, en internetconnectiviteit incl. DNS en DHCP.

<https://www.tenderned.nl/tenderned-tap/aankondigingen/145911>

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

- ISO 27001 / 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.
- IPv4 en IPv6, vanwege het gebruik van IP-reeksen.
- HTTPS, HSTS en TLS, voor een beveiligde verbinding met internet.

Nog een paar algemene opmerkingen over standaarden en netwerken

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) een absolute must. 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, risicogebaseerd 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.

4.9 Basisregistraties/ overheidsgegevens

CPV codes gerelateerd aan basisregistraties/ overheidsgegevens

48000000-8 Software en informatiesystemen

38221000-0 Geografische informatiesystemen (GIS of dergelijke)

Praktijkvoorbeeld: zaaksysteem

Het Ministerie van Sociale Zaken en Werkgelegenheid doet een aanbesteding voor 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.

<https://www.tenderned.nl/tenderned-tap/aankondigingen/128880>

Waarschijnlijk zijn de volgende standaarden relevant:

- StUF, voor uitwisseling gegevens uit de basisregistraties.
- ISO 27001 / 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/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.

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

Nog een paar algemene opmerkingen over standaarden en basisregistraties/overheidsgegevens

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.

4.10 Inhuur

CPV codes gerelateerd aan inhuur

79610000-3 Plaatsing van personeel
79620000-6 Diensten voor de terbeschikkingstelling van personeel, met inbegrip van tijdelijk personeel
79630000-9 Personeelsdiensten, met uitzondering van plaatsing en 'outplacement'
72000000-5 IT-diensten: adviezen, softwareontwikkeling, internet en ondersteuning
72330000-2 Diensten voor inhouds- of datastandaardisatie en -classificatie
72413000-8 Diensten voor het ontwerpen van websites
72415000-2 Verlenen van hostingdiensten voor websites

Praktijkvoorbeeld:

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.

<https://www.tenderned.nl/tenderned-tap/aankondigingen/113868>

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.

Nog een paar opmerkingen over standaarden en inhuur

Waar het gaat om software of diensten ten behoeve van de inhuur van personeel, zijn meerdere standaarden relevant uit de clusters "Internet en beveiliging" en "E-Facturatie en administratie". Zo kan aan de dienstverlener gevraagd worden te voldoen aan ISO 27002 aangezien de uitvraag en het aanbod vrijwel altijd persoonsgegevens bevatten, waaronder uurtarieven.

De SETU-standaarden zijn ontwikkeld door de grote uitzendorganisaties en is de Nederlandse implementatie van de internationale HR-XML standaard. Door toepassing van de SETU standaarden ontstaat uniformering van het elektronisch berichtenverkeer tussen aanbieders en afnemers (inleners) van tijdelijk personeel (flexibele arbeid). Het eisen van deze standaarden kan ook relevant zijn bij de inkoop van e-HRM systemen, of bij financieel/administratieve systemen.

NB: Als het gaat om eisen die *inhoudelijk* gesteld mogen worden aan de mensen die ingehuurd worden (en niet aan de ICT systemen) dan mag kennis en kunde gevraagd worden van de 'pas toe of leg uit'- lijst in het algemeen of van een aantal specifieke standaarden, afhankelijk van wat de dienst inhoudt. Denk bijvoorbeeld aan Digitoegankelijkheid voor het ontwerpen van websites en SKOS voor de inhuur van diensten voor inhouds- of datastandaardisatie en -classificatie.

5 Voorbeeld bestekteksten algemeen

Inleiding

In dit en het volgende hoofdstuk staan voorbeeld-bestekteksten. 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 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.

Toelichtende bestektekst

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

Toelichtende bestektekst
Open Standaarden
[Aanbestedende dienst] wil graag dat de dienst of product, conform het openstandaardenbeleid 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 (www.forumstandaardisatie.nl).
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 [aanbestedende dienst] zijn gewaarborgd.
Garanties naar de toekomst
In het kader van Preventief en/of Innovatief Onderhoud garandeert inschrijver/gegadigde ten minste: i) dat de dienst of het product steeds tijdig zal blijven voldoen aan de relevante Wet- en regelgeving; ii) 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; iii) 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;

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.

Bestektekst geschiktheidseisen	Doel en toelichting
Kerncompetentie Ervaring	
De [gegadigde/inschrijver] dient aan te tonen dat hij in de afgelopen [x] 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.	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	
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. 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.	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.

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.

6 Voorbeeld bestekteksten, specifiek per standaard

Dit hoofdstuk bevat voor de 'pas toe of leg uit'-standaarden voorbeelden voor gunningseisen (Eis) en gunningscriteria (Wens), vooralsnog alleen voor de functionele clusters "Internet en beveiliging" en "Documenten en (web)content".

Hieronder worden de begrippen en onderdelen van het gebruikte sjabloon nader toegelicht.

Begrippen

Toepassing

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.

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 specificatie-document 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.

Inkoopcategorie

De categorie uit hoofdstuk 4 waarbij de standaard vaak relevant is.

Onderdelen bestekteksten

Besteksonderdeel	Voorbeeld-bestektekst
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.

6.1 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-document

<https://tools.ietf.org/html/rfc2460>

<https://tools.ietf.org/html/rfc791>

Relevante inkoopcategorieën uit hoofdstuk 4:

- Website of webapplicatie
- E-mail
- Spraak- en/of datacommunicatiediensten
- Netwerken
- En alle overige aan internet te koppelen ICT-systemen, zoals multifunctionals

Besteksonderdeel	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: 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. 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 op https://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
Relevante inkoopcategorie	• Werkplek en kantoorsoftware • Netwerken
Besteksonderdeel	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 internetverbinding-test op https://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)

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.
Relevante inkoopcategorie	Website of webapplicatie E-mail Sprak- en/of datacommunicatiediensten Netwerken Alle overige aan internet te koppelen ICT-systemen
Besteksonderdeel	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.

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.
Relevante inkoopcategorie	Werkplek en kantoorsoftware Netwerken
Besteksonderdeel	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 op https://www.internet.nl .
Wens	Beschrijf uw procedure voor het omgaan met validatie-fouten 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/
Relevante inkoopcategorie	Website of webapplicatie E-mail Sprak- en/of datacommunicatiediensten
Besteksonderdeel	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: 1. er een geldig (PKIoverheid-)certificaat is geïnstalleerd op het ICT-systeem; 2. op basis waarvan andere systemen een TLS-verbinding kunnen opzetten met dit ICT-systeem; 3. waarvan de veiligheid van de TLS-configuratie voldoet aan de "ICT-beveiligingsrichtlijnen voor TLS" van NCSC; 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 op https://www.internet.nl .
Wens	Beschrijf uw beheerprocedure om 1. het PKI overheid-certificaat veilig te beheren tijdig te vernieuwen; 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
Relevante inkoopcategorie	E-mail
Besteksonderdeel	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: 1. op het systeem een publiek/privaat sleutelpaar is gegenereerd of kan worden gegenereerd; 2. de publieke DKIM-sleutel is gepubliceerd in de DNS van de e-maildomeinnaam; 3. alle uitgaand e-mailberichten worden ondertekend met de private DKIM-sleutel; 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 op https://www.internet.nl , https://www.mail-tester.com of via de tools op https://dmarc.org/resources/deployment-tools/ .
Wens	Beschrijf uw beheerprocedure om: 1. de DKIM-sleutels veilig te genereren, te beheren en te vernieuwen; en 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	IETF
Specificatie-document	https://tools.ietf.org/html/rfc7208
Relevante inkoopcategorie	E-mail
Besteksonderdeel	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: - de IP-adressen van de verzendende systemen als SPF-record worden geregistreerd in de DNS van de verzendende domeinnaam; - 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 op https://www.internet.nl , https://www.mail-tester.com of via de tools op https://dmarc.org/resources/deployment-tools/ .
Wens	Beschrijf uw beheerprocedure om: - de SPF-records te genereren en indien nodig aan te passen, en - 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/
Relevante inkoopcategorie	Website of webapplicatie
Besteksonderdeel	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. - Succesvol doorlopen van Interoperability Certification Program van Kantara of vergelijkbaar (http://kantarainitiative.org/confluence/display/certification/Interoperability+Program). - 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-Shop/Norm/NENISOIEC-270012013C112014-nl.htm
Relevante inkoopcategorie	Alle ICT-systemen/-diensten, met name die met privacy- en/of bedrijfs-gevoelige informatie.
Besteksonderdeel	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.
Verificatie eis	• Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem/-dienst aan deze standaard voldoet. • 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-Shop/Norm/NENISOIEC-270022013C22015-nl.htm
Relevante inkoopcategorie	Alle ICT-systemen/-diensten, met name die met privacy- en/of bedrijfs-gevoelige informatie.
Besteksonderdeel	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.
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 Baseline informatiebeveiliging Overheid (BIO) 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 Baseline Informatiebeveiliging Overheid.

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
Relevante inkoopcategorie	• Website of webapplicatie • E-HRM systemen • Netwerken
Besteksonderdeel	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. • 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/
Relevante inkoopcategorie	E-mail
Besteksonderdeel	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. - Testresultaten van validatietooling 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, af luisteren 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
Relevante inkoopcategorie	• E-mail
Besteksonderdeel	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. • 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.

6.2 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-Shop/Norm/NENISO-1900512005-en.htm https://www.nen.nl/NEN-Shop/Norm/NENISO-1900522011-en.htm
Relevante inkoopcategorie	• Website of webapplicatie • Werkplek en kantoorsoftware • Multi-functionals
Besteksonderdeel	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. 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. 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. • Testresultaten van validatietooling voor PDF/A zoals VeraPDF (https://verapdf.org), Adobe Preflight en tooling op https://forumstandaardisatie.nl/pdfa.
Wens	Geen
Beoordeling wens	Geen
Opmerkingen	Voor meer achtergrond zie de informatie over open documentformaten op de website van Forum Standaardisatie (https://www.forumstandaardisatie.nl/opendoc).

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
Relevante inkoopcategorie	• Website of webapplicatie • Werkplek en kantoorsoftware • Multi-functionals
Besteksonderdeel	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. 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. 4. Met de te leveren multi-functional kan de gebruiker scans maken en vastleggen 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.
Verificatie eis	• Akkoordverklaring eventueel met toelichting hoe hij borgt dat zijn ICT-systeem aan deze standaard voldoet. • Testresultaten van validatietooling voor PDF1.7 zoals Adobe Preflight.
Wens	Geen
Beoordeling wens	Geen
Opmerkingen	Voor meer achtergrond zie de informatie over open documentformaten op de website van Forum Standaardisatie (https://www.forumstandaardisatie.nl/opendoc).

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/
Relevante inkoopcategorie	• Website of webapplicatie • Werkplek en kantoorsoftware • Multi-functionals
Besteksonderdeel	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. 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. 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. • Testresultaten van validatietooling voor ODF zoals ODF Validator (http://odf-validator.rhcloud.com/), ODFAutoTests (http://autotests.opendocumentformat.org/). 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 (https://www.forumstandaardisatie.nl/opendoc). 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	
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
Relevante inkoopcategorie	Website of webapplicatie
Besteksonderdeel	
Eis	Voorbeeld-bestektekst 1. De op te leveren website voldoet aantoonbaar aan de toegankelijkheidsrichtlijnen van Digitoegankelijk -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig. 2. Het op te leveren document voldoet aantoonbaar aan de toegankelijkheidsrichtlijnen van Digitoegankelijk -zoals opgenomen op de 'pas toe of leg uit'-lijst van Forum Standaardisatie- of daaraan gelijkwaardig
Verificatie eis	- Akkoordverklaring eventueel met toelichtende beschrijving van specifieke situaties en uitzonderingen op basis van digitoegankelijk.nl/beleid/specifieke-situaties. - Handmatig onderzoek en advies door een toegankelijkheidsexpert. - 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. - 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).

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/
Relevante inkoopcategorie	• Website of webapplicatie • Werkplek en kantoorsoftware
Besteksonderdeel	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. • Testresultaten van validatietooling 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
Relevante inkoopcategorie	Alle ICT-systemen/-diensten indien er gebruik wordt gemaakt van een REST API.
Besteksonderdeel	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.

Tot slot, leg uit

Geldige redenen

Wat zijn goede redenen om open standaarden niet toe te passen?

De reden om niet te kiezen voor een open standaard zal enige substantie moeten hebben. Het is niet de bedoeling dat voor gesloten standaarden gekozen wordt enkel en alleen omdat het tijdsbeslag dan wat korter is, de kosten wat lager zijn, of de tijdslijn van een aanbesteding wat korter.

Maar wat is nu wel een geldige reden?

onvoldoende aanbod van de standaard
onvoldoende veiligheid van de standaard
onvoldoende zekerheid bij het functioneren van de standaard
of een andere andere redenen van bijzonder gewicht

Van onvoldoende aanbod zal bijvoorbeeld sprake zijn indien tevoren is te verwachten dat een product of dienst gebaseerd op een standaard uit de lijst naar verwachting niet of door een zeer gering aantal aanbieders wordt aangeboden. Bij het laatste punt zal het praktisch gezien gaan om aspecten van geld, tijd of capaciteit.

In het jaarverslag of anders?

Welke reden ook speelt: leg uit. Zorg dat de motivering minimaal vastligt in het aanbestedingsdossier- bijvoorbeeld in een apart hoofdstuk van de inkoopstrategie of het verwervingsplan- én dat de reden gemeld wordt in het jaarverslag.

Voor overheidsorganisaties geldt de melding in het jaarverslag als een verplichting die is geregeld in de bijlage van de instructie rijksdienst bij aanschaf van ICT-diensten en ICT-producten artikel 3 en 4. Hier haakt ook de bedrijfsvoeringsparagraaf van de Rijksbegrotingsvoorschriften, op aan in model 3.24.

Voor gemeentes en provincies is de verplichting tot uitleggen over het nalaten van de juiste open standaarden vastgelegd in het Besluit begroting en verantwoording provincies en gemeenten.

Voor andere organisaties in de publieke sector geldt 'leg uit' als een dringend advies. Volg het voorbeeld van overheidsorganisaties of zorg voor een andere (bij voorkeur publiek toegankelijke) plaats waar de reden terug te vinden is, en waar gemakkelijk naar verwezen kan worden mocht hierover later discussie ontstaan.

Nu is het geen geheim dat van het uitleggen in het jaarverslag over het nalaten van het gebruik van open standaarden in de praktijk vooralsnog weinig terecht komt. Daarom onderzoekt het Forum Standaardisatie mogelijkheden die mogelijk laagdrempeliger zijn. Een ervan is deze:

Uitleggen naar aanleiding van 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 aanbestedingen onderzocht. Sinds kort publiceert het Forum Standaardisatie deze

onderzochte aanbestedingen met de standaarden die gevraagd zijn en de standaarden die achterwege zijn gebleven en waar dus een uitleg bij zou horen.

De onderzoekers van de Monitor Open Standaarden sturen een e-mail naar de contactpersonen van alle aanbestedingen die zij onderzoeken. Als de aanbesteding wordt beoordeeld, ontvangt de contactpersoon bericht met de vraag om uit te leggen waarom sommige standaarden achterwege zijn gelaten, mocht dit het geval zijn.

De redenen kunnen in overleg met de aanbestedende dienst in aanmerking komen voor publicatie in de Monitor Open Standaarden en bij de beoordeling gepubliceerd worden.

Op deze manier uitleggen zou in de praktijk wellicht beter kunnen werken dan hierover verantwoording afleggen in het jaarverslag, maar vooralsnog is dit niet de officiële weg en blijft afhankelijk van de verantwoordelijkheid die ICT opdrachtgevers en inkopers nemen voor hun aandeel in het meer en beter gebruik van open standaarden in de publieke sector.

Maar intussen heeft u deze handreiking nu misschien wel helemaal gelezen, en dat biedt goede hoop.

CONCEPT