Reacties van aanbesteders op melding over beoordeling

Inleiding: melden van beoordeling aan aanbesteders

Elk jaar beoordelen wij voor de Monitor Open standaarden ongeveer 70 aanbestedingen. Op basis van de aanbestedingsdocumenten wordt bepaald welke open standaarden van de lijst relevant zijn en wordt vervolgens nagegaan of om die standaarden is gevraagd. Na de second opinion-sessie zijn de beoordelingen in principe definitief, deze vormen de basis voor de tabellen en grafieken in de monitor.

Sinds 2019 sturen wij de contactpersoon voor de betreffende aanbesteding (volgens Tenderned) een email met een korte toelichting op het onderzoek en met de uitkomsten van de beoordeling. Op deze manier brengen wij het onderzoek en – vooral – het open standaardenbeleid nogmaals gericht onder de aandacht bij de mensen die dit in de praktijk uitvoeren. Wij vragen daarbij ook om feedback op het oordeel, vooral om in gesprek te komen met de aanbestedende diensten en meer inzicht te krijgen in wat hen drijft bij het opstellen van een bestektekst en bij het al dan niet expliciet vragen om relevante open standaarden bij de aanbesteding.

Van de reacties op deze meldingen naar aanleiding van de Monitor 2020 is dit jaar een beknopte inventarisatie gemaakt. De resultaten daarvan beschrijven wij in deze notitie.

Aantal en aard van de reacties

Voor de Monitor 2019 zijn 72 aanbestedingen beoordeeld, waarvan 37 van de Rijksoverheid (en onder andere uitvoeringsorganisaties, agentschappen en ZBO's) en 35 van mede-overheden (bijvoorbeeld gemeenten, provincies en waterschappen). Op de meldingen over deze 72 beoordelingen hebben wij 31 reacties ontvangen:

- 9 reacties die leidden tot enige technisch-inhoudelijke discussie (welke standaarden zijn relevant voor de aanbesteding, en/of de vraag of er om een standaard is gevraagd of niet);
- 10 andere inhoudelijke reacties (zoals een toelichting op de aanbesteding en/of de gemaakte keuzes door de aanbesteder, soms de vraag welke standaarden dan niet uitgevraagd zouden zijn);
- en 12 reacties van meer administratieve aard (ontvangstbevestiging, out of office reply et cetera).

In deze notitie delen wij de eerste twee soorten reacties, zij leveren zeer leerzame praktijkvoorbeelden.

1. Reacties die leidden tot enige technisch-inhoudelijke discussie

(Of een standaard al dan niet relevant is, danwel of er al dan niet om gevraagd is.)

In het navolgende zijn woordelijk onderdelen van de reacties, vragen en opmerkingen weergegeven[1]. Omdat niet met de betrokkenen was afgesproken dat wij hen zouden citeren, vragen wij de lezer om hier zorgvuldig mee om te gaan. Om die reden hebben wij ook de namen en organisaties weggelaten. Van twee van de negen inhoudelijke reacties hebben we geen woordelijke reactie vastgelegd.

[A] De relevantie van de ISO's wordt door de aanbestedende partij in twijfel getrokken. De reactie van TNO luidt: Wij achten de ISO 27001/27002 standaarden (gericht op informatiebeveiliging) relevant voor de aanbesteding vanwege de grote collectie jaarrekeningen die de opdrachtnemer in het bezit krijgt

[1] We hebben daarbij eventuele typefoutjes niet gecorrigeerd.

(om deze vervolgens te converteren). Het is van belang dat hier netjes en veilig mee omgesprongen wordt en vandaar dat de informatiebeveiligingsstandaarden ISO27001/27002 van toepassing zijn.

[B] Het verbaasd ons dat u onze aanbesteding als slecht beoordeeld. Wij hebben voor de ontwikkeling van een app […] een functionele specificatie opgesteld, waarbij wel geen enkele beperking hebben aangegeven met betrekking tot standaarden. Er kan natuurlijk gesteld worden dat wij niet specifiek gevraagd hebben om open standaarden, maar op deze manier hebben wij de markt in de gelegenheid gesteld om aan te bieden wat zij willen en kunnen. Er is voor hun dus alle vrijheid.

[C] Intern is nog wel de vraag gesteld of [wij] als organisatie wel binnen de doelgroep vallen van organisaties waar Forum Standaardisatie naar kijkt. [Wij zijn] immers geen overheidsorganisatie, maar een overheidsbedrijf dat valt onder de speciale sector. Naar onze mening vallen wij dan ook niet onder de door u beschreven scope en zijn wij niet gehouden aan de Instructie rijksdienst inzake aanschaf ICT-diensten. Wat de inhoud betreft; bij het opstellen van de tender documenten hebben wij uitvoerig gekeken naar de Eisen en Wensen en de daarbij behorende uitvraag richting de markt. Zowel vanuit de verwachting handelend dat de markt weet wat zij aanbiedt en waaraan aan succesvolle […] Tooling aan zou moeten voldoen dan wij dit als aanbestedende dienst zouden over specificeren. Uiteindelijk draait het om de juiste invulling van de behoefte van [organisatie]. Inhoudelijk hebben wij gekeken naar de lijst die wordt voorgeschreven, waarvan is gesteld dat deze relevant zijn. We hebben gekeken in hoeverre dit overeenkomt en hoewel we een aantal standaarden zagen die we inderdaad uitgevraagd hebben, is een groot aantal gericht op cyber security welke we niet allemaal expliciet hebben gemaakt op voorhand. Hetgeen we wel hebben uitgevraagd stond in de concept security annex opgenomen (annex bij de overeenkomst), maar de definitieve security annex wordt altijd achteraf bepaald aan de hand van een solution BIA (business impact analyse). Verder is de oplossing die is uitgevraagd een SaaS-oplossing voor intern gebruik en mogelijk een inzage voor bepaalde instanties. Er vindt verder geen communicatie plaats tussen […] en [klanten] of andere geïnteresseerden. Waardoor een tal van de voorgestelde standaarden niet strikt noodzakelijk geacht worden voor de […] tooling.

[D] Ons inziens hebben we de standaard ISO 27001 wel uitgevraagd. Bij beide aanbestedingen hebben we namelijk de volgende KO-eis (eis 1.2.5) geformuleerd: “De Inschrijver dient over een ISO 27001 certificaat of conform de Aanbestedingswet 2012 "gelijkwaardige maatregelen" te beschikken. ISO 27001 is de internationale standaard voor informatiebeveiliging. Het ISO 27001 certificaat, dan wel gelijkwaardig, is het bewijs dat uw organisatie de nodige voorzorgsmaatregelen heeft genomen om gevoelige informatie te beschermen tegen ongeautoriseerde toegang en bewerking. Inschrijver zal mbt "gelijkwaardige maatregelen" zelf dienen aan te tonen dat de door haar genomen maatregelen vergelijkbaar zijn met ISO27001. De Aanbestedende dienst wijst erop dat het gevraagde certificaat, dan wel de toelichting op "gelijkwaardige maatregelen" direct bij het indienen van de Inschrijving moeten worden verstrekt. Inschrijver dient het document toe te voegen middels een upload en toont hiermee aan dat zij aan de eis voldoet”. Bij de aanbesteding voor [organisatie] hebben we de Gemeentelijke Inkoopvoorwaarden bij IT (GIBIT) versie 2016 van toepassing verklaard en meegestuurd. Door gebruik van de GIBIT worden ook de Gemeentelijke ICT-kwaliteitsnormen van toepassing verklaard. Hierin worden de aangegeven open standaarden benoemd. Vanuit gangbaarheid / pas-toe waren wij van mening dat dit toereikend was. Klaarblijkelijk bekijkt ICTU dit anders.

(Naar aanleiding van deze mailwisseling is de beoordeling aangepast, en is besloten om voortaan ‘GIBIT uitvragen’ voldoende te laten zijn voor een oordeel ‘uitgevraagd’ m.b.t. de ISO standaarden.)

[E] De relevantie van de ISO-standaarden wordt door de aanbestedende partij in twijfel getrokken. De reactie van TNO luidt: Vooropgesteld hebben we het hier over een aanbesteding waarbij geen nieuw product wordt aanbesteed en doorontwikkeling niet aan de orde is, maar waar gevraagd wordt om een leverancier voor onderhoud en support. Bij dergelijke aanbestedingen die gaan over beheer wordt zijn de meeste open standaarden die op de pas-toe-of-leg-uit lijst staan dus niet relevant, maar wordt er nog wel geoordeeld of de ISO27001 en ISO27002 standaarden relevant zijn i.v.m. informatiebeveiliging. Die achten wij in dit geval zeker relevant aangezien op pagina 14 in Bijlage A duidelijk wordt aangegeven dat de leverancier toegang verkrijgt tot vertrouwelijke gegevens van [organisatie]. Beveiliging van deze informatie is van belang en vandaar dat de ISO-standaarden relevant worden geacht.

[F] De contactpersoon gaat vooral in op de open standaarden die zij niet (volledig) hebben uitgevraagd:

- ISO 27001, ISO 27002: Ja we hadden nadrukkelijk ook 002 moeten noemen als invulling, instrument voor 001 (mogelijk is dit wel uitgevraagd in de Nota van Inlichtingen);
- Digikoppeling, we hebben Digikoppeling niet nadrukkelijk benoemd omdat het een oplossing is maar we vragen wel om qua koppelvlakken aan te sluiten op de geldende rijksoverheid standaarden (zijn in gesprek over de opvolger PAPPEL);
- DNSSEC, HTTPS & HSTS, TLS, SPF zijn de facto standaarden zonder welke er geen betrouwbare verbindingen opgebouwd kunnen worden (we hebben het gebruik van PKI Overheid certificaten nadrukkelijk wel benoemd). Op dit moment is het zo dat oplossingen die deze standaarden NIET gebruiken ook niet operationeel te krijgen zijn. Zonder deze standaarden is BBN2 in mijn optiek niet te halen. Dat was de aanleiding om ze niet expliciet te vragen;
- DKIM, DMARC en STARTTLS & DANE, onze achilleshiel van beveiligd e-mailen. Onze uitvraag zal geen eigen email relay krijgen maar gebruik maken de SSC-ICT external email relay. We vragen niet in deze EUA maar aan SSC-ICT om applicatie emailverbindingen die op orde zijn, vandaar dat ze ontbreken in deze aanbesteding. Of omgekeerd SSC-ICT biedt deze standaarden expliciet aan in hun product External Email Relay

[G] De aanbestedende partij betwijfelt de relevantie van twee standaarden: XBRL en Digikoppeling. Na uitwisseling van argumenten krijgt de aanbestedende partij gelijk. De uiteindelijke reactie van TNO luidt: In overleg met mijn collega waarmee ik de beoordelingen heb gedaan hebben we ervoor gekozen beide standaarden bij nader inzien toch niet relevant te achten. Digikoppeling blijkt eigenlijk meer als vergelijkingsmateriaal te worden gebruikt i.p.v. dat een koppeling met de basisregistraties wordt gevraagd. Daarnaast zijn wij te streng geweest door XBRL relevant te achten. XBRL is van toepassing bij "financieel verantwoordingsverkeer" en om een FMIS-systeem daaronder te scharen gaat bij nader inzien te ver. In het algemeen betekent dit dat het oordeel van de aanbesteding wijzigt van 'op de goede weg' naar 'perfect' omdat alle 15 relevante standaarden worden uitgevraagd en er aandacht is voor de pas-toe-of-leg-uit lijst. Chapeau!

2. Andere inhoudelijke reacties

(Een toelichting op de aanbesteding en/of de gemaakte keuzes door de aanbesteder.)

[H] Vanzelfsprekend zullen wij zoveel mogelijk open standaarden uitvragen indien hier mogelijkheden voor zijn. Voornamelijk met SaaS applicaties (en daar gaat het hier om) moeten we toch voor een groot deel schikken naar hetgeen de leverancier maakt en verkoopt. Dit zijn over het algemeen geen openstandaard software pakketten. Het eisen van een totale open standaard, SaaS applicatie zal

ervoor zorgdragen dat de meest belangrijke partijen met de gewenste functionaliteiten niet gaan inschrijven.

[I] Voor wat betreft ISO 27002 geldt dat deze niet is opgenomen omdat je hiervoor geen certificaat kan ontvangen. In de templates voor aanbestedingsdocumenten gaan we ervan uit dat, indien wij inschrijvers vragen aan een bepaalde certificering te voldoen, dat ze dit ook moeten kunnen aantonen (en dat wij dit vervolgens moeten kunnen controleren). Omdat er geen certificaat kan worden overlegd, wordt dit niet standaard uitgevraagd in de templates. Voor de overige standaarden geldt dat deze in de eisen wel zijn uitgevraagd, maar de namen van de standaarden niet specifiek zijn benoemd. Naar aanleiding van uw bericht hebben we besproken dat in de templates van de aanbestedingsdocumenten een opmerking wordt geplaatst in de kantlijn, waardoor inkopers zich bewust worden van het bestaan van standaarden bij ICT-aanbestedingen. Daarnaast maakt [organisatie] gebruik van een standaard programma van eisen omtrent informatiebeveiliging. Mijn collega van IV gaat intern navragen of het mogelijk is dat in dit programma van eisen ook de specifieke benamingen van de standaarden worden opgenomen, zodat dit in volgende aanbestedingen kan worden meegenomen.

[J] Volgens jullie experts zijn 4 standaarden uitgevraagd, terwijl er 12 van toepassing lijken te zijn. Wij volgen het open standaarden beleid van de overheid en maken dat ook expliciet in onze interne beleidsdocumenten. Wij vragen dit ook van onze leveranciers. Dit mag ook blijken uit het feit dat in het aanbestedingsdocument wel degelijk wordt verwezen naar deze standaarden. Eis 21, onder het kopje inhoudelijke eisen: De oplossing voldoet aan de toepasselijke standaarden zoals gepubliceerd door het forum voor standaardisatie https://www.forumstandaardisatie.nl/open-standaarden. Dat we niet elk van de mogelijk relevante individuele eisen expliciet hebben genoemd is geen bewuste keuze vooraf en ook geen indicatie dat we overwogen willen afwijken van bepaalde standaarden. Tegelijkertijd ondervinden we dat voor leveranciers de algemene verwijzing niet altijd voldoende is, en dat sommige standaarden van de overheid kennelijk niet tot de standaarden in de markt behoren. Bijvoorbeeld de standaarden voor het tegengaan van phishing. Wij zullen daarom bespreken en overwegen - n.a.v. deze vraagstelling van ICTU - om standaarden explicieter uit te vragen, en daar vanuit ons CIO Office ook toezicht op te houden. Hopelijk zijn wij daarmee iets meer dan ‘op de goede weg’.

[K] De reden dat open standaarden niet of niet volledig worden uitgevraagd is gelegen in het feit dat de huidige configuratie van het applicatielandschap dit niet (altijd) toelaat. Er liggen diverse afhankelijkheden. [Organisatie] streeft er uiteraard naar, ondanks het niet zijn van een Rijksoverheid, nu en in de toekomst het gebruik van open standaarden daar waar mogelijk optimaal te stimuleren bij de daarvoor relevante c.q. geschikte inkooptrajecten.

[L] De projectleider die deze aanbesteding heeft gecoördineerd en ook de stukken heeft geschreven is inmiddels niet meer bij ons werkzaam. Zelf ben ik maar zijdelings betrokken geweest. Wij kunnen u dan ook helaas niet de verzochte informatie aanleveren.

[M] Uiteraard zijn we ons er bewust van dat niet alle open standaarden van toepassing zijn op deze aanbesteding. Vandaar dat we verwijzen naar het werkingsgebied van deze aanbesteding. Hieruit kan de conclusie getrokken worden dat we in deze aanbesteding 100% aansluiting zoeken bij de pas-toe-of-leg-uit standaarden. Met andere woorden, we vragen binnen deze aanbesteding, dat waar de open standaarden kunnen worden toegepast, ook daadwerkelijk de aansluiting wordt gevonden. Bovenop de beschrijving dat ten minste aan alle van toepassing zijnde open standaarden wordt voldaan, worden enkele open standaarden ook expliciet belicht. Dit gebeurt om extra aandacht te vestigen op deze standaarden. Deze uitvraag kan gezien worden als een verdieping van de

Gemeentelijke ICT-kwaliteitsnormen. Hiermee kan niet gesteld worden dat alle open standaarden welke niet expliciet zijn benoemd, dan ook niet van toepassing zijn. Onze opvatting is dan ook dat [organisatie] volledig voldoet aan alle pas-toe-of-leg-uit standaarden welke op deze aanbesteding van toepassing zijn. Een score van 72% geeft dan ook onvoldoende weer wat ons inziens kan worden opgemaakt. We hopen dan ook dat u genegen bent om de (voorlopige) score in positieve zin bij te stellen. De kritische blik van de experts leert echter wel dat we scherper kunnen zijn op dat wat we wel beschrijven en de interpretatie van dat wat we niet beschrijven. We begrijpen dat door het expliciet benoemen van specifieke open standaarden, de indruk zou kunnen ontstaan, dat hierdoor de overige open standaarden niet van toepassing zouden zijn. En ook al is dat geenszins het geval, in een transparant proces van aanbesteden mag er volgens ons geen enkele onduidelijkheid bestaan. Om die reden zullen we naar aanleiding van dit schrijven en de voorlopige score uit de monitor, de lopende en toekomstige aanbestedingen kritisch beoordelen. Van een professionele overheidsorganisatie mag immers verwacht worden dat het niet enkel de intentie is om de open standaarden te omarmen, maar dat dit ook duidelijk blijkt uit hetgeen beschreven.

[N] Interessant dat u ongevraagd en onaangekondigd onze aanbestedingsdocumenten beoordeeld. Het siert dat u ons om een reactie vraagt. Wij kunnen u melden dat wij wel degelijk met een (schuin) oog hebben gekeken naar de standaarden. Ons antwoord inzake de aandacht voor de standaarden is:

- ISO 27001 hebben we uitgevraagd bij de kerncompetentie;
- ISO 27002 is geen management standaard. Certificering is niet mogelijk dus een goede en onafhankelijke beoordeling is er niet. 27002 is een verdieping van 27001 en bestaat uit een lijst met maatregelen inzake risico's. Dat is mooi, maar wij hebben liever dat ze zelf er over nadenken en het regelen;
- PDF standaard is zo standaard dat het er naar vragen complete onzin is. Tevens kunnen alle mogelijke aanbieders van de gevraagde SaaS hieraan voldoen. Deze standaard eisen is dus ook hierdoor niet nodig. Zit wel in een van de eisen verwerkt;
- DNSSEC. wij vragen een SaaS dienst. De oproepbaarheid van hun dienst en programma is de levensader van het programma/dienst. Ons was bekent dat bij alle mogelijke aanbieders de standaard is geïmplementeerd;
- Digitoegankelijk, was beschreven;
- IPv4 en IPv6: wij vragen een SaaS dienst. De IP adressering is de levensader van het programma/dienst die wij uitvragen. Ons was bekent dat bij alle mogelijke aanbieders beide standaarden aangesproken kunnen worden;
- E-portfolio, Niet expliciet naar gekeken;
- HTTPS is reeds een standaard die wordt gedragen door alle mogelijke aanbieders;
- HSTS is een standaard die intern van belang is voor het nog veiliger aangaan van een verbinding. Is niet ter zake voor deze aanbesteding. TLS is zo standaard voor de potentiele aanbieders dat wij die niet hebben uitgevraagd omdat iedereen daar toch aan voldoet;
- SAML, Niet naar gekeken, maar achteraf denken wij dat dit niet ter zake doende is voor de toepassing die wij hebben uitgevraagd;
- SETU is standaard voor de toepassing die wij uitvragen. Alle mogelijke aanbieders van de gevraagde SaaS voldoen hieraan. Deze standaard eisen was dus niet nodig;
- ODF: wij hebben Microsoft Office als standaard. Deze is in staat eventuele ODF documenten te lezen. Het programma /dienst die wij vragen zal niets doen met de documenten. Wij zullen nooit ODF documenten gebruiken. Wij hebben derhalve deze dan ook niet gevraagd;
- SPF is standaard voor de toepassing die wij uitvragen. Alle mogelijke aanbieders van de gevraagde SaaS voldoen hieraan. Deze standaard eisen was dus niet nodig;
- DKIM; Niet expliciet naar gekeken;
- DMARC; Niet expliciet naar gekeken;

– STARTTLS & DANE is een standaard zodat je mail niet wordt aangemerkt als spam. Het programma/dienst die is uitgevraagd gaat niet over het verzenden van mails. Uitvraag van deze standaard is dus niet van toepassing.

[O] [Organisatie] heeft besloten om op basis van diverse motiverende redenen de aanbesteding […] in te trekken. De afhandeling is nog niet voltooid (daarom nog niet zichtbaar op Negometrix/TenderNed), maar dit is mogelijk wel relevante informatie voor uw onderzoek.

[P] De adviseurs van [organisatie] begeleiden een groot aantal aanbestedingen voor zaak- en documentmanagementsystemen voor overheidsorganisaties. Onlangs hebben wij van een deel van onze opdrachtgevers vernomen dat zij vanuit ICTU een bericht hebben ontvangen over missende open standaarden. Het betreft missende open standaarden in het Programma van Eisen en Wensen (PvE) dat gebruikt is tijdens de aanbestedingen. Wij willen onze opdrachtgevers graag zo goed mogelijk ondersteunen en ons basis-PvE zo compleet mogelijk houden. Echter viel het ons op dat een wisselend aantal open standaarden gevraagd werd per gemeente. Zo verwachtte ICTU bij de gemeente [X] 18 standaarden in totaal, bij de gemeente [Y] 16 standaarden en bij de gemeente [Z] 15 standaarden. Kunnen jullie hier een toelichting over geven? Waar zijn deze aantallen per gemeenten op gebaseerd?

(ICTU heeft hierop gereageerd, en daarbij aangegeven dat er – hoewel het in alle drie de gevallen om een zaaksysteem gaat – waarschijnlijk op onderdelen wel verschillen in de gevraagde systemen zitten. Voor 2 van de 3 gemeente zijn de Geo-standaarden relevant beoordeeld, voor 1 van de 3 gemeenten zijn CMIS en ODF relevant geacht. Verder hebben wij erop gewezen dat 15 standaarden voor alle drie de aanbestedingen relevant waren, en daarvan zijn Digikoppeling en IPv6 voor geen van de drie gemeenten gevraagd en PDF is voor één gemeente niet gevraagd.)

[Q] Reden van afwijking is dat het hier om het opnieuw aanbesteden van beheer gaat voor een (speciaal)product dat al bij [organisatie] in gebruik en beheer is. Het gaat hier dus niet om aanschaf maar om het continueren van dienstverlening omdat de bestaande overeenkomst afliep. Vanwege de geraamde budgetten was een EU aanbesteding noodzakelijk. Het gebruikte product veranderd dus niet, daarom zijn de standaarden ook niet specifiek uitgevraagd, functioneel veranderd er immers niets.

De meeste van deze contacten zijn beperkt gebleven tot één mailwisseling. Een paar toelichtingen door aanbesteders bevatten informatie die ook voor TNO relevante inzichten boden; deze zijn aan TNO doorgestuurd. Soms heeft TNO daar nog op gereageerd richting aanbestedende partij.

Joost Vreuls, 15 februari 2021