Reacties van aanbesteders op melding over beoordeling (Monitor 2021)

Inleiding: melden van beoordeling aan aanbesteders

Elk jaar beoordelen wij voor de Monitor Open standaarden een aantal aanbestedingen, voor de Monitor 2021 waren dat er 40. 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 iedere beoordeelde aanbesteding een email met een korte toelichting op het onderzoek en met de uitkomsten van de beoordeling. Op die 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 2021 is een beknopte inventarisatie gemaakt. De resultaten daarvan beschrijven wij in deze notitie.

Aantal en aard van de reacties

Voor de Monitor 2021 zijn 40 aanbestedingen beoordeeld, waarvan 20 van de Rijksoverheid (en onder andere uitvoeringsorganisaties, agentschappen en ZBO's) en 20 van mede-overheden (bijvoorbeeld gemeenten, provincies en waterschappen). Op de meldingen over deze 40 beoordelingen hebben wij 17 reacties ontvangen:

- 8 reacties die leidden tot enige technisch-inhoudelijke discussie (welke standaarden zijn relevant, en/of de vraag of er om een standaard is gevraagd of niet); in enkele gevallen heeft dit geleid tot het aanpassen van de beoordeling;
- 2 andere inhoudelijke reacties (zoals een toelichting op de aanbesteding en/of de gemaakte keuzes door de aanbesteder);
- en 7 reacties van administratieve aard (mail onbestelbaar, out of office reply et cetera).

De eerste twee soorten reacties vatten wij samen, zij leveren leerzame praktijkvoorbeelden.

1. Reacties die leidden tot enige technisch-inhoudelijke discussie

(Of een standaard al dan niet relevant is, dan wel 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.

[1] We hebben daarbij eventuele typefoutjes niet gecorrigeerd.

[A] De aanbestedende partij zegt over de 11 niet-gevraagde standaarden: dit "(…) zijn tegenwoordig standaarden die wij altijd al hanteren en die internationaal als standaarden worden gehanteerd. Vanuit de BIO en de ISO27001 en 27002 nemen we deze al mee. Verder heeft (…) de Handreiking Verwerving Omgevingswet software gevolgd met daarin de opgenomen requirements. Wat betreft de koppelingen, deze zijn niet gedicteerd, maar moeten wel gerealiseerd worden middels standaarden, zoals ook opgenomen in de GIBIT2016."
De reactie van de beoordelaars luidt: er wordt alleen verwezen naar standaarddocumenten (GIBIT en requirementdocumenten van VNG). Er wordt wel geëist dat gebruik moet worden gemaakt van open standaarden, maar de voor deze aanbesteding relevante open standaarden worden nauwelijks met name genoemd, met Digikoppeling en HTTPS/HSTS/TLS als uitzondering. Ook wordt er geen aandacht besteed aan de 'pas toe of leg uit'-lijst van het Forum Standaardisatie. Wanneer jullie de aangegeven standaarden "altijd al hanteren", dan is het zaak om dit ook in de aanbestedingsteksten op te nemen zodat de inschrijvers dit weten en hieraan kunnen voldoen met het geleverde ICT-product. In de uitgangspunten die wij hanteren is het vragen van GIBIT onvoldoende voor het uitvragen van ISO 27001/27002. Verder staat nergens dat ISO 27001/27002 moet worden toegepast, en ook wordt niet gevraagd om de BIO/BIG. Wij beschouwen dan ook ISO 27001/27002 als niet gevraagd.

[B] De aanbestedende partij gaat in haar reactie op elk van de genoemde niet-gevraagde standaarden in:

- "HTTPS en HSTS. We hebben duidelijk aangegeven dat we op een veilige en correcte wijze onze verbindingen tussen systemen willen leggen. Als we over certificaten praten dan hebben we het al snel over de ontbrekende begrippen HTTPS en HSTS (wordt nog niet veel gebruikt volgens ons).
- TLS en StartTLS and Dane. TLS heeft puur met de security tussen servers en systemen te maken. Dit zijn breed bekende internationale standaarden waar je al niet aan ontkomt als je over beveiliging tussen systemen vanuit Cloud en Interne systemen praat of systemen die direct naar buiten praten. StartTLS and Dane standaard was ons nog niet bekend dat deze verplicht is binnen de Overheid.
- SPF en DKIM. Zelfde geldt voor SPF (…) en DKIM (…) die wij ook standaard moeten toepassen en constant onderhouden omdat anders onze emails niet verzonden en of ontvangen kunnen worden vanuit verschillende systemen en websites en vooral vanuit onze inwoners. Dat is een constante uitdaging, maar ligt vooral bij (…). Dit zou wat anders zijn als we ons emaildomein gaan aanbesteden en bij een externe partij in beheer laten nemen. Dan moet je afspraken over SPF en DKIM maken, dat zij dit allemaal op de meest verantwoordde wijze toepassen en kunnen laten toetsen.
- DMARC en DNSSEC en IPv4 en IPv6. Deze hebben te maken met internationale standaarden die op een veilige wijze systemen, websites en dergelijke op een veilige wijze onderscheiden en man in the middle attacks voorkomen. Dit is gewoon normaal dat een relevante markt partij aan deze standaarden voldoet. Dit betreft het vertalen van bijvoorbeeld (webdomein) naar een publiek ip-adres en een opname in de publieke DNS records van Internet Service Providers zoals Ziggo, KPN etc maar ook Google.
- ODF. Dit betreft de Openoffice Document Format (.odt) en die zit standaard in onze Office 365. Was ons niet bekend dat we hier specifiek om moesten vragen in het PvE.
- OpenApi spec en Rest API Design. Volgens ons vallen dit soort API's ook onder de Common Ground API's die specifiek voor Gemeentes ontwikkeld zijn en daar hebben we wel omgevraagd.

- Digitoegankelijk. DigiToegankelijk is de Nederlandse naam voor de standaard waarmee overheidsorganisaties hun websites en apps toegankelijk moeten maken voor alle burgers. Toegankelijk betekent hier bruikbaar voor iedereen: jong, oud, met of zonder beperking. Dit hebben we niet uitgevraagd maar dat zou een logische uitvraag zijn bij de aanbesteding voor een nieuwe (…) website. De aanbesteding (…) raakt dit slechts deels. Dus conclusie om dit begrip zeker mee te nemen in de Website aanbesteding.
- NI GOV Ass. Dit is ons niet bekend en bij het nakijken op internet konden we niets vinden. Ben wel benieuwd wat het omvat zodat we hier een volgende keer wellicht wel rekening mee kunnen houden.
- TLS, STARTTLS en DANE maken onderdeel uit van de open standaarden lijst van het forum standaardisatie, welke weer onderdeel uitmaken van de GIBIT voorwaarden. Hier heeft de leverancier standaard mee te maken. Kleine kanttekening voor wat betreft DANE overigens. Deze wordt (nog) niet ondersteunt binnen Microsoft 365. Eind 2021 zal Microsoft de ondersteuning voor DANE uitrollen."

De reactie van de beoordelaars luidt: Het impliciet benoemen van relevante standaarden, zoals hier bijvoorbeeld bij HTTPS/HSTS, DNSSEC en IPv4/6 het geval is, is niet voldoende. Het is belangrijk dat deze open standaarden expliciet benoemd worden richting inschrijvers om er zeker van te zijn dat het ICT-product hieraan voldoet. Wanneer inschrijvers moeten voldoen aan de GIBIT is dit zeker nog niet voldoende om open standaarden op de 'pas toe of leg uit'-lijst als gevraagd te beschouwen. Voor de mailstandaarden (SPF, DKIM, DMARC, STARTTLS en DANE) geven jullie aan dat deze inderdaad moeten worden toegepast, maar wel met de vraag of dit ook zo is wanneer dit vooral bij (…) zelf ligt. Wij achten deze standaarden wel relevant voor de aanbesteding omdat bij de mailcommunicatie vanuit de SaaS of on-premise oplossing deze onderliggende standaarden moeten worden toegepast voor veilig e-mail-verkeer. Vandaar dat we deze - uitgevraagd willen zien in de aanbestedingsdocumenten. NL Gov Ass staat voor NL GOV Assurance profile for OAuth 2.0. Zie ook https://www.forumstandaardisatie.nl/open-standaarden/nl-gov-assurance-profile-oauth-20. In Eis 3-5 (Programma van Eisen) wordt, naast SAML, ook gevraagd om Openauth authenticatie. Zoals het kopje 'nut' aangeeft op de webpagina bij Forum Standaardisatie zijn in de NL GOV standaard "bindende afspraken vastgelegd over het gebruik van de standaard OAuth 2.0 bij de Nederlandse overheid." Deze open standaard staat nog niet zo lang op de 'pas toe of leg uit'-lijst, dus wellicht dat deze daardoor nog niet bij jullie bekend is.

[C] De aanbesteder heeft om 14 van de 18 relevante standaarden wèl gevraagd. Over de vier niet-gevraagde standaarden zegt hij:

- "ODF wordt voor eHRM helemaal niet gebruikt en dus ook niet relevant voor de opdracht.
- OpenAPI spec, REST-API Design en NL GOV Assurance Profile for OAuth 2.0 zijn alle 3 aan elkaar gerelateerd en zijn de nieuwste technologieën voor gegevensuitwisseling. De markt van eHRM is nog niet zo ver. Dit was ook gebleken uit een marktonderzoek. Dit had dus geen enkele toegevoegde waarde om uit te vragen."

De reactie van de beoordelaars luidt: ODF wordt relevant geacht voor deze aanbesteding aangezien er een export plaatsvindt van gegevens naar Excel en rapportages naar Word. ODF is het open formaat voor spreadsheets (.ods) en teksten (.odt) en zou in dit geval gevraagd moeten worden aangezien de applicaties van het Microsoft Office pakket proprietary formaten zijn. Bij eis ICTe14-1 wordt bijvoorbeeld wel .txt genoemd, net als ODF ook een meer lightweight tekstbestand. In dat rijtje hadden we graag ODF geëist zien worden. Dan wat betreft de relevantie van de standaarden OpenAPI Specification, REST-API Design Rules en NL GOV Assurance profile for OAuth 2.0. Deze eerste twee standaarden

m.b.t. (REST) API's zijn duidelijk relevant aangezien in eis ICTe13-3.1 er gevraagd wordt om "het veilig beschikbaar stellen van bestaande services (web services, REST)" en "gegevensuitwisseling op basis van API's" waarbij REST services relevant worden geacht. In ICTe13-1.1 komt duidelijk OAuth naar voren als authenticatieprotocol, waardoor het NL GOV Assurance profiel hierover moet worden toegepast. Wanneer deze standaarden relevant zijn voor een aanbesteding, moeten overheden deze uitvragen, ook als het nieuwe technologieën betreft en u de indruk heeft gekregen dat de markt nog niet zo ver is. Forum Standaardisatie houdt hiermee ook rekening bij het plaatsen van standaarden op de 'pas toe of leg uit'-lijst. Deze drie standaarden zijn relatief recent geplaatst maar hadden inmiddels echt moeten worden geëist. Ik begrijp uw reactie goed, maar juist met de eisen vanuit aanbesteders weten softwareleveranciers wat er aan nieuwe requirements worden gesteld. Als u het niet te stellig er in had willen zetten, kan u bijvoorbeeld de standaarden wel in de aanbestedingsteksten eisen, maar dan met de kanttekening die u vanuit het marktonderzoek heeft opgehaald om zo om een inhoudelijke uitleg te vragen mochten inschrijvers inderdaad niet aan de standaarden kunnen voldoen.

[D] De aanbestedende partij zegt over de niet-gevraagde standaarden:

- Gezien het zeer beperkte aantal aanbieders (4) in de markt voor belastingsystemen zal een te restrictieve uitvraag leiden tot te weinig of geen inschrijvingen. Hetgeen ook daadwerkelijk plaatsvond bij de eerste aanbesteding voor het belastingsysteem. Toen werd slechts één inschrijving ontvangen die achteraf ongeldig bleek te zijn. Ook bij de tweede aanbesteding dreigden marktpartijen af te zien van inschrijving door een te restrictieve uitvraag. Pas de derde aanbesteding bevatte een voldoende realistische uitvraag die tot meerdere inschrijvingen leidde. Dat was mede de motivatie voor de keuze voor een "milde" set aan verplichte standaarden.
- HTTPS & HSTS, TLS. Encryptie is reeds één van de "controls" uit de ISO27001 en op die manier uitgevraagd. Daarnaast vermeldt het bestek letterlijk: "Dataverbindingen voldoen aan gangbare standaarden voor authenticatie en encryptie. De verantwoordelijkheid van het functioneren van de koppeling ligt bij de Inschrijver."
- SPF, DKIM, DMARC, STARTTLS & DANE. De oplossing verstuurt geen email, maar gebruikt een PIP of de Berichtenbox. De aan email gerelateerde standaarden zijn dus niet van toepassing.
- Digitoegankelijk. Door de webrichtlijnen van toepassing te verklaren is naar onze mening voldoende invulling gegeven aan deze standaard.
- ODF. Aangezien Microsoft Office algemeen als een defacto standaard wordt beschouwd zien wij geen reden om ODF te eisen.
- DNSSEC, IPv4 en IPv6. Aangezien de uitvraag een SaaS oplossing betreft ligt de verantwoordelijkheid hiervoor mede aan de kant van het datacenter van de externe hosting partij. Voor de gemeente volstaat daarom de uitvraag van algemene standaarden ohgv (de beveiliging van) datacommunicatie.

De reactie van de beoordelaars luidt: allereerst over de algemene, begrijpelijke opmerking. Het komt vaker voor dat het aantal inschrijvers beperkt is en dat hierbij de aanbesteding nogmaals met minder restricties gepubliceerd wordt. Het is dan zaak om hierbij inderdaad de balans te vinden tussen strikt- en mildheid. Wat opvalt bij jullie aanbesteding is dat juist de meer specifieke standaarden, zoals Digikoppeling, SAML en StUF, wel worden uitgevraagd, maar dat de meer algemene ICT-standaarden die relevant zijn voor de SaaS/on-premise-oplossing niet worden gevraagd. Deze standaarden zijn wel essentieel voor de veiligheid, betrouwbaarheid en toegankelijkheid van de oplossing. Daarnaast is het uitvragen van deze

relevante open standaarden die op de 'pas toe of leg uit'-lijst staan verplicht. Dit zou het in theorie niet hoogdrempeliger moeten maken voor aanbieders om in te schrijven, omdat dit basale ICT-standaarden zijn waaraan iedere SaaS/on-premise-oplossing zou moeten voldoen. In de praktijk is nu gebleken dat er minder inschrijvers waren, maar aangezien ik geen inzicht heb in de eerdere aanbestedingsdocumenten, kan ik ook niet oordelen of de relevante standaarden eerder wel werden uitgevraagd. Dan wat betreft de specifieke standaarden. Richtinggevende en implicerende teksten zijn onvoldoende om aan de 'pas toe of leg uit'-verplichting te voldoen. Bijvoorbeeld, de tekst "Dataverbindingen voldoen aan gangbare standaarden voor authenticatie en encryptie" is onvoldoende om HTTPS/HSTS/TLS als gevraagd te beschouwen, omdat de inschrijver hierbij mogelijk aan andere standaarden denkt. Het is van belang deze standaarden expliciet te noemen en als ze niet relevant zijn, dan te vermelden waarom dit niet zo is. Hetzelfde geldt in zekere zin voor DNSSEC en IPv4/6. Die worden onvoldoende gedekt door de uitvraag van algemene standaarden, terwijl de inschrijver wel degelijk verantwoordelijk is voor de hosting van de oplossing. ODF relateert aan het bovenstaande. Microsoft Office is een proprietary formaat waarmee inderdaad bestanden ook als ODF kunnen worden opgeslagen. Het is volgens het 'pas toe of leg uit'-beleid echter wel verplicht om de ODF-standaard expliciet te eisen. Het aanbestede ICT-product betreft een SaaS/On Premise-oplossing inclusief hosting. Dit is voor ons als beoordelaars een trigger om de mailstandaarden SPF, DKIM, DMARC, STARTTLS en DANE relevant te achten. De mailstandaarden zijn eigenlijk altijd relevant vanwege e-mail-notificaties dan wel wachtwoord-vergeten-functionaliteit van de oplossing. Of is dat niet van toepassing voor deze ICT-oplossing omdat de PIP dan wel Berichtenbox deze communicatie afvangt? Webrichtlijnen is door User-interface Eis 2 (Bijlage 04 Programma van Eisen en Wensen) bij nader inzien voldoende om Digitoegankelijk als uitgevraagd te beschouwen. Wij zullen dit aanpassen in de beoordeling.

[E] De aanbesteder heeft om 10 van de 14 relevante standaarden wèl gevraagd. Over de vier niet-gevraagde standaarden zegt hij: "Waarschijnlijk wordt alles gedekt door: Opdrachtnemer draagt er zorg voor dat Opdrachtgever te allen tijde kan voldoen aan de volgende wetgeving en standaarden voor Informatiebeveiliging: - Algemene Verordening Gegevensbescherming; - Wet Digitale Overheid/Wet Structuur Uitvoeringsorganisatie Werk en Inkomen; - Baseline Informatiebeveiliging Overheid /ISO 27001:2017/relevante controls ISO 27002:2017; - Grip op Secure Software Development/Open Web Application Security Project. Ten aanzien van IPv4 en IPv6: ik zie dat in een reviewronde deze opmerking ook is gemaakt (…) en dat toen is verwezen naar de BVO, waar dit in afgedekt zou moeten zijn. Ik kan me voorstellen dat dat ook voor de andere punten geldt. Ten aanzien van XBRL: ons programma van eisen bevat ten aanzien van reporting vereisten alleen dashboard tooling, geen interfacing om data naar (…) te halen. Dergelijke interfacing zou mogelijk op basis van XBRL moeten zijn. Wij zien geen noodzaak XBRL als standaard toe te voegen aan ons Programma van Eisen."
De reactie van de beoordelaars luidt: Overheden moeten bij het aanbesteden van ICT-producten of diensten om de relevante open standaarden op de 'pas toe of leg uit'-lijst van Forum Standaardisatie vragen indien deze relevant zijn. In de documenten van deze aanbesteding is geen aandacht besteed aan open standaarden en de 'pas toe of leg uit'-lijst van Forum Standaardisatie. Dat "waarschijnlijk alles gedekt wordt door" de beveiligings-richtlijnen en toetsen die worden geciteerd, is zeker niet het geval. De wetgeving en standaarden die u in het citaat benoemt kennen wij, maar vragen geen van deze standaarden expliciet uit (alleen de BIO eist ISO 27001/27002). Het is onvoldoende om hier

enkel naar te verwijzen en verder geen concrete open standaarden te vragen. Ook de BVO, de Beveiligings- en Verwerkersovereenkomst (Bijlage 4.11), is beoordeeld, maar ook hier worden de standaarden niet geëist (dus o.a. geen IPv4/IPv6) of komt het open standaarden beleid naar voren. Ter illustratie: er zijn ook toetsen, certificaten en specificatiedocumenten waarbij wel een aantal van de open standaarden worden geëist als de aanbesteder vraagt om te voldoen aan die toets of certificaat. Voorbeelden hiervan zijn de internet.nl test, Qualys SSL-labs test of NCSC Beveiligingsrichtlijnen voor webapplicaties. Wanneer geëist wordt dat inschrijvers door deze tests heen komen en dat lukt ze, dan beschouwen wij de standaarden die hierin getest worden als geëist. Tot slot de relevantie van XBRL: bij nader inzien zijn we wellicht te streng geweest in het relevant achten van XBRL voor deze aanbesteding. De reden dat XBRL door ons relevant werd geacht was vanwege de digitale uitwisseling van documenten/berichten (facturen) waarin financiële informatie een belangrijk component is, maar in het functioneel toepassingsgebied staat ook dat het verkeer te kenmerken is als verantwoordingsverkeer. Bovendien geldt de verplichting alleen bij het investeren in ICT-systemen voor bedrijfsadministratie en boekhouding. De aanbesteding relateert hieraan, maar gaat meer over de uitwisseling richting deze systemen. XBRL zullen we daarom als relevante standaard laten vallen.

[F] De aanbesteder heeft om veel van de relevante standaarden wèl gevraagd. Over de niet-gevraagde standaarden zegt hij: "Het is mij niet geheel duidelijk hoe 'de experts' tot hun mening zijn gekomen, maar als zij de aanbestedingsstukken goed gelezen zouden hebben dan hadden zij kunnen zien dat: (1) email geen onderdeel van de opdracht uitmaakt en derhalve het gebruik/voorschrijven van SPF, DMARC, DKIM, STARTTLS en DANE niet aan de orde is; (2) voorzover de aangeboden oplossing tòch email zou bevatten de leverancier in Bijlage K onder B4 gevraagd wordt toe te lichten welke standaarden hij daarvoor gebruikt danwel te onderbouwen waarom hij ze niet gebruikt; (3) berichtenuitwisseling via DigiPoort verloopt, dus op basis van FTP(s), WUS(WSDL/UDDI/SOAP) en ebMS (dus niet op basis van email); (4) in het geval van het Catalogusplatform er weliswaar sprake is van de mogelijkheid om te connecteren op API's maar dat dit dan API's betreft van leveranciers die middels een API hun catalogus/catalogi beschikbaar stellen aan de Rijksoverheid. Als de Rijksoverheid van mening is dat deze (>3000) leveranciers dienen te voldoen aan standaarden had zij deze ten tijde van de aanbestedingen dwingend moeten voorschrijven. Het Catalogusplatform zelf kent geen API en OpenAPI/REST-API standaarden zijn derhalve niet aan de orde."
De reactie van de beoordelaars luidt: De mailstandaarden worden door ons relevant geacht wanneer het een SaaS-oplossing betreft. Dit komt omdat SaaS-oplossingen altijd enige vorm van e-mailverkeer initiëren, danwel door het uitsturen van e-mailnotificaties, danwel middels een wachtwoord-vergeten-functionaliteit. Dit wordt ook bevestigd door Eis A11, waar staat: "Als leverancier ontvang ik een notificatie als er een document klaarstaat, minimaal via een e-mail en notificatie in het leverancierssportaal." Ook bij Eis B5, B6 en E15 vindt er e-mail-verkeer plaats. Hierom worden de standaarden SPF, DMARC, DKIM, STARTTLS en DANE relevant geacht. In Bijlage K worden inderdaad de mailstandaarden als wens beschreven. De mailstandaarden zijn hier door ons onterecht aangemerkt als niet gevraagd, dus we zullen hier onze beoordeling op aanpassen. Beide API-standaarden worden relevant geacht door twee specifieke eisen. Eis B3 stelt dat leveranciers hun catalogus kunnen aanmaken op basis van een API-koppeling. Die API-koppeling zou dan wel vanuit het portaal moeten worden aangeboden en dus (als OpenAPI Specification) moeten worden gedefinieerd. Eis G6 stelt ook dat de functioneel beheerder een koppeling moet kunnen opzetten en

beheren, waarbij een API als voorbeeld wordt genoemd. Dit is de reden waarom beide API-standaarden door ons relevant zijn geacht. Beide standaarden zijn niet gevraagd.

[G] Over de niet-gevraagde standaarden zegt de aanbesteder: "Bij een drietal standaarden begrijp ik niet waarom deze als 'rood' gemarkeerd zijn, aangezien we hier juist veel aandacht aan besteed hebben: Open API spec. De data moeten toegankelijk zijn via een API-toegang d.m.v. OGC-standaarden (WMS, WMTS, WFS, WCS), zie o.a. p. 12 REST-API. De data moeten toegankelijk zijn via een RESTFul API, zie o.a. pagina 12. Digitoegankelijk. Dit is als eis opgenomen in 3.2.4. 'De viewer moet toegankelijk zijn voor mensen met een functiebeperking volgens de norm EN 301549'. Er zijn geen eisen gesteld op de veiligheid (Https, TLS, DNSSEC), maar er is beoordeeld op veiligheid (5.2.3, p. 23). Het gaat hierbij om de veiligheid van de verbinding en het accountbeheer, waarbij er gerefereerd wordt naar PKI en ISO27001. En volgens mij gaan we hierin vrij ver, door zelfs te wensen dat het portaal ook anoniem bezocht kan worden door bepaalde gebruikers in het veiligheidsdomein. We hebben gekozen om dit via wensen op te nemen i.p.v. eisen, omdat we hier ook op wilden beoordelen en graag wilden horen wat de ideeën vanuit de markt op dit gebied zijn. Het klopt dat er geen referentie gemaakt is op Internetprotocol (IPv4, IPv6). Ik heb nog niet gemerkt dat hier problemen bij ontstaan zijn sinds het portaal in 2012 operationeel is. Maar dit kunnen we zeker een volgende keer wel doen."
De reactie van de beoordelaars luidt: De twee API-standaarden worden relevant geacht omdat inderdaad op pagina 11 staat de REST API's worden gehost als data interface. Bij het aanbieden van deze REST API's wordt de OGC-standaard ingezet, maar worden, als ik het goed interpreteer, ook andere REST API's aangeboden die niet perse aan die standaard hoeven te voldoen. Uit de documentatie van de OGC API blijkt dat deze inderdaad gedefinieerd zijn als OpenAPI specificatie, maar het is ook van belang om de OpenAPI Specification standaard te eisen voor die andere API's die worden aangeboden. De andere standaard is de REST-API Design Rules standaard die moeten worden toegepast bij het aanbieden van REST API's. Dat staat dus niet gelijk aan het gebruik van REST API's alleen. Het is een set aan regels die moet worden toegepast wanneer een REST API wordt gedefinieerd. Op basis van deze uitleg ben ik voor beide API-standaarden dan nog steeds van mening dat ze gevraagd hadden moeten worden, maar dat niet is gedaan. Met betrekking tot Digitoegankelijk moet ik het oordeel herzien. De passage die u aanhaalt is inderdaad door ons gezien. Op de EN301549 is de Nederlandse Digitoegankelijk standaard gebaseerd. Echter hanteerden wij tijdens de beoordeling dat EN301549 in combinatie moet worden gevraagd met WCAG 2.0/2.1 om voldoende te zijn voor Digitoegankelijk gevraagd, maar hier moet ik op terugkomen. Bij het doornemen van de EN301549 documentatie constateer ik dat daar duidelijk staat dat de technische standaard WCAG 2.1 hierin verwerkt zit. Digitoegankelijk veranderen wij dus van niet gevraagd naar gevraagd. Dan nog de veiligheidsstandaarden HTTPS, TLS en DNSSEC. Dit zijn drie belangrijke standaarden die als verplicht zijn opgenomen op de pas-toe-of-leg-uit lijst. Voor een portaal, waar deze aanbesteding over gaat, is het echt van belang dat deze standaarden geëist worden i.p.v. dat de inschrijver gevraagd wordt om te overwegen of hij deze standaarden gaat gebruiken of niet. De pas-toe-of-leg-uit lijst verplicht dan ook dat deze drie standaarden geëist worden in de aanbesteding. Bij het beoordelen vinden wij over het algemeen het eisen van SSL ook voldoende. SSL komt in 5.2.3 ook naar voren, maar enkel als wens en voorbeeld, dit niet onvoldoende.

[H] De aanbesteder heeft om veel van de relevante standaarden wèl gevraagd. Over de niet-gevraagde standaarden zegt hij: Deze aanbesteding (…) betreft een dienst die aan het

bedrijfsvoeringssysteem van (…) wordt gekoppeld. Vanuit de (applicatie) wordt weer gekoppeld met de relevante banken. Deze banken zijn verspreid over de gehele wereld.

- IPv4 & IPv6 – Deze wordt wel standaard uitgevraagd als het gaat om webapplicaties. Daar is hier geen sprake van, het gaat om M2M communicatie. Hier geldt dus niet de verplichting dat (…) toegankelijk is via IPv6. Het gebruik van TCP/IP voor communicatie met de (applicatie) was misschien waarschijnlijk, maar niet de enige mogelijkheid. Voor de uitvraag was het onderliggende IP protocol niet een essentieel eis voor de selectie van de leverancier. Wat wel zeer essentieel is, is dat de verbinding maximaal veilig is. Met andere woorden (…) past zich aan de (applicatie) aan voor wat betreft IP protocol.
- SPF, DKIM, DMARC, STARTTLS & DANE – Mailverkeer is geen onderdeel van de gevraagde oplossing en financiële zaken zullen en mogen nooit via mail verlopen. Omdat partijen soms mailcontact met elkaar kunnen hebben, ook al is het niet formeel, is het goed om voor authenticatie waar mogelijk standaard veiligheidseisen te stellen. Er is actie genomen om deze open standaards in onze standaard lijst van eisen toe te voegen voor toekomstige uitvragingen.
- XBRL – Voor het overmaken van geld, zijn andere protocollen in gebruik. Betalingen kennen meerdere formats en in Europa is SEPA/ISO20022 de standaard. Dat geldt niet voor de andere landen. Rapportages over betalingen worden via het MT940 standaard en niet via XBRL gedaan. Wij kunnen er echter niet op vertrouwen dat alle banken overal ter wereld deze ISO20022 en MT940 standaard ondersteunen. Dat doen ze niet allemaal en er zijn zelfs kleine verschillen in implementaties tussen banken die deze ISO20022 standaard wel hanteren.

De <u>reactie van de beoordelaars</u> luidt: Het aanbestede ICT-product betreft een SaaS-oplossing inclusief hosting. Dit is voor ons als beoordelaars een trigger om IPv4/6 zeker relevant te achten, maar ook de mailstandaarden SPF, DKIM, DMARC, STARTTLS en DANE. Uit uw uitleg begrijp ik dat de software machine-to-machine gekoppeld is en dus geen enkele gebruikersinteractie mogelijk maakt. Dat is anders dan wat wij typisch bij SaaS producten zien, aangezien daarbij de mailstandaarden eigenlijk altijd relevant zijn vanwege e-mailnotificaties danwel wachtwoord-vergeten-functionaliteit. Dus wij kunnen meegaan met de stelling dat de emailstandaarden hier niet relevant zijn. Alhoewel "voor de uitvraag het onderliggende IP protocol niet een essentiële eis voor de selectie van de leverancier was", is het uitvragen van IPv4/6 wel essentieel vanuit de optiek van de wetgeving rondom open standaarden en de 'pas toe of leg uit'-lijst. Wanneer dit "niet de enige mogelijkheid" was, vraagt de Instructie Rijksdienst om uit te leggen waarom er moeten worden voldaan aan een andere standaard en waarom IPv4/6 als niet relevant wordt beschouwd. Deze uitleg is niet opgenomen waardoor de inschrijver hier niet over wordt geïnformeerd. Overigens wordt gesuggereerd dat bij M2M-communicatie de verplichting voor IPv6 niet geldt. Waaruit blijkt dit? Het is niet zo dat wij vinden dat voor alle M2M verbindingen er geen IPv6 verbindingen nodig zijn. Bij deze specifieke situatie gaat het om bewezen en bestaande systemen waarbij beide connectiepunten vast liggen. Er is dus geen sprake van multicasting, een groot voordeel van IPv6. Het gaat dus ook niet om een webapplicatie met veel verschillende gebruikers waarvoor snellere routering belangrijk is, het andere grote voordeel van IPv6. De noodzaak om vanwege schaarste aan adressen over te gaan naar IPv6 onderschrijven wij natuurlijk wel. Voor deze specifieke vraag is IPv6 toch niet als eis opgenomen. Naast dat IPv6 voor onze behoefte niet nodig was zou de eis een risico vormen omdat de markt voor deze applicatie klein is. Een IPv6 eis zou een knock-out betekenen voor alternatieven die alleen met IPv4 beschikbaar zijn. In retrospectief zou deze aanbesteding door een IPv6 eis zelfs

mislukt zijn, maar vooraf wisten wij dat niet. We hadden het internet protocol achteraf gelukkig opengelaten. Wel hadden we IPv6 als wens kunnen meenemen, maar dat niet overwogen vanwege eerder genoemde gebrek aan directe voordelen. Dan m.b.t. XBRL. Er zit inderdaad een verschil tussen het uitwisselen van bank/geldtransacties en het digitaal uitwisselen van financiële rapportages zoals een balans en/of winst- en verliesrekening d.m.v. XBRL. Dat eerste is de kern van deze aanbesteding. Wel heeft u het over "rapportages over betalingen". Dat wekt de indruk dat het iets anders dan de geldtransacties zelf betreft. Betreft dit wel of geen "digitale uitwisseling van documenten en berichten dat te kenmerken is als verantwoordingsverkeer en waarin financiële informatie een belangrijke component is" (functioneel toepassingsgebied XBRL)? De rapportages over betalingen betreffen toegang tot een dashboard van de (applicatie), het gaat niet om het verzenden van rapportages. Het enige dat wordt verzonden zijn de bank statements (MT940). Deze worden 1 op 1 doorgezet door de (applicatie). Op basis van het bovenstaande zullen wij de relevantie van de mailstandaarden en van XBRL laten vallen.

2. Andere inhoudelijke reacties

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

[I] "Wij hebben de open standaarden nu toegevoegd in de uitvraag middels de Nota van inlichtingen (NVI). Tevens zullen wij deze nu standaard opnemen in de (concept/ standaard) uitvraagbrief voor ICT uitvragen. Zodat bij elke ICT uitvraag de Standaardisatie word meegenomen."

[J] "Ik heb de taken van vorige architect overgenomen en hij is niet meer in dienst. Ik heb de ontbrekende standaarden (DNSSEC, HTTPS & HSTS, TLS, SPF, DKIM, DMARC, STARTTLS & DANE, Digikoppeling, E-portfolio, ODF en SAML) gecontroleerd m.b.t. de aanbesteding (…). Voor mij is niet helder waarom deze standaarden zijn niet opgenomen in de aanbesteding. Ik kan u informeren dat het aangeschafte pakket (…) de rood gemarkeerde standaarden in uw e-mail bevat behalve E-portfolio."

Joost Vreuls & Jaap Korpel, 22 maart 2022