Bijlage 6 Programma van Eisen

De Gemeenschappelijke Regeling Belastingsamenwerking gemeenten en hoogheemraadschap Utrecht (BghU)

Belastingsamenwerking
gemeenten & hoogheemraadschap Utrecht

Programma van Eisen voor EA Enterprise Service Bus (ESB) 2021
Openbare Europese Aanbesteding

Versie : 1.0
Datum : 30 september 2021

Inhoudsopgave

Inleiding

Dit Programma van Eisen (PvE) beschrijft de vereiste functionaliteit voor de Enterprise Service Bus (ESB) die Belastingsamenwerking gemeenten en hoogheemraadschap Utrecht (BghU) wenst aan te schaffen. De inschrijver dient aan alle eisen te voldoen op het moment van inschrijven, tenzij een ander moment in de tijd is benoemd. Wanneer aan enige eis niet wordt voldaan, volgt 'knock-out' en wordt de inschrijving niet verder beoordeeld.

A Functioneel

A.1 ESB-functionaliteit

#	Omschrijving
EA-01	De oplossing is flexibel in te zetten voor routering, translaties en protocolwisselingen in de keten van berichten tussen kernapplicaties van Opdrachtgever, deelnemende organisaties in de keten en landelijke voorzieningen.
EA-02	De oplossing is in staat om een inkomend bericht te vertalen in een andere berichten standaard en deze door te sturen. Dit betreft minimaal een binnenkomend XML bericht dat kan worden omgezet in een StUF bericht, en omgekeerd.
EA-03	De oplossing kan worden gebruikt voor het opzetten van beveiligde verbindingen tussen applicaties in verschillende cloudomgevingen, dan wel tussen een cloud en on-premise omgeving.
EA-04	De oplossing voorziet in een Digikoppeling voorziening (oplossing voor koppeling met landelijke basisregistraties).

A.2 Gegevensmagazijn

#	Omschrijving
EA-05	Landelijke voorzieningen en andere initiatieven zijn gericht op het centraal beschikbaar maken van gegevens. Volgens de Common Ground principes betekent dit: eenmalige opslag, direct bevragen bij de bron en gebeurtenisrijk notificeren. De behoefte aan lokale gegevensopslag wordt minder, maar Opdrachtgever voorziet komende jaren nog een overgang situatie. Als onderdeel van de oplossing wordt dan ook een gegevensmagazijn geleverd (niet zijnde een datawarehouse) voor gestructureerde data, gebaseerd op landelijke stelsels van basisregistraties en plusgegevens.
EA-06	De oplossing bevat eveneens een soort van datadistributie mechanisme. Deze bewaakt de distributie van data die in verschillende bronapplicaties wordt beheerd. Zodra de data wijzigt in een bronapplicatie (en het gegevensmagazijn) zorgt het mechanisme ervoor dat alle afnemers (doelapplicaties) de wijzigingen ontvangen.
EA-07	Opdrachtgever wil via andere applicaties (bijvoorbeeld SQL developer en Power BI) de gegevens in het gegevensmagazijn rechtstreeks kunnen benaderen.

B ICT

B.1 Algemeen

#	Omschrijving
EB-01	De gebruikersinterfaces die beschikbaar worden gesteld voor de beheerder dienen webbased te zijn. De oplossing is benaderbaar met de meest actuele versies, inclusief versies van maximaal 1 jaar oud, van de browsers Microsoft Edge, Google Chrome en Mozilla Firefox.
EB-02	Leverancier moet bij elektronische facturen (e-factureren) de Europese richtlijn 2014/55/EU volgen, conform art. 9.7 GIBIT 2020.

B.2 Authenticatie en autorisatie

#	Omschrijving
EB-03	De oplossing ondersteunt SSO (Single Sign On) in combinatie met Windows Active Directory 2012 of hoger (ADFS) en Azure Active Directory.
EB-04	De autorisaties van de oplossing kunnen door de opdrachtgever worden ingesteld.
EB-05	De oplossing wordt ingericht met accounts, die individueel herleidbaar zijn naar medewerkers/personen, voor alle gebruikers en beheerders, zodat in logging duidelijk is wie, wat, wanneer heeft aangepast. Persoonlijke accounts voor applicatiebeheerders en systeembeheerders dienen hiervoor voldoende rechten te hebben, waarbij het niet mogelijk is voor beheerders om via een generiek superuser account te werken.
EB-06	De oplossing ondersteunt autorisaties per rol. Per gebruiker en groepen van gebruikers is te autoriseren of gegevens mogen worden aangemaakt, geraadpleegd, gemuteerd en/of worden verwijderd.
EB-07	Autorisaties van een specifieke gebruiker van de oplossing kunnen worden overgenomen cq. gekopieerd om (nieuwe) gebruikers aan te maken of aan te passen.
EB-08	Voor autorisaties binnen de oplossing geldt dat voor controle en audits een gedetailleerd overzicht van alle gebruikers en bijhorende autorisaties kan worden gegenereerd. De oplossing toont eveneens wijzigingen in autorisaties en een overzichtsscherm van de actuele ingelogde gebruikers.
EB-09	Indien Leverancier toegang tot de oplossing (en/of de database) nodig heeft wordt hiervan te allen tijde melding gemaakt bij de desbetreffende afdeling van Opdrachtgever.
EB-10	De oplossing dient voor alle gebruikers tenminste gebruik te worden gemaakt van 2FA/MFA voor authenticatie.
EB-11	De oplossing ondersteunt ook het bieden van via de IAM-omgeving (op dit moment Azure/ADFS) van Opdrachtgever.
EB-12	De oplossing dient ook via openbare netwerken benaderbaar te zijn en enkel via een door de Opdrachtgever beheerd device, door medewerkers van Opdrachtgever 'in het veld' en vanaf de locatie van organisaties. Hierbij dient tenminste gebruik te worden gemaakt van 2FA/MFA en een VPN verbinding.

B.3 Logging

#	Omschrijving
EB-13	De oplossing beschikt over loggingsfunctionaliteit in het kader van de diverse audits, en om ook de inwoners en ondernemers te kunnen garanderen dat op een veilige manier met hun persoonlijke gegevens wordt omgegaan. Daarnaast maakt het inzichtelijk welke gegevens met wie worden gedeeld en waarom
EB-14	Er is een automatische mutatielogging in werking binnen de oplossing op handeling, gebruiker en tijdstip. De mutatielogging is ingericht volgens normkaders (vaste logregels). Van alle processen wordt een volautomatische mutatielogging aangemaakt. Een nieuwe mutatie mag een oude mutatielogging niet overschrijven. Deze logbestanden zijn beperkt toegankelijk en extra beveiligd.
EB-15	De oplossing voorziet in functionaliteiten voor het borgen en het inzichtelijk maken in de logging van gegevensmutaties, inclusief de oorsprong van de mutatie (gebruiker, tijdstip en/of proces) en behoud van de gegevens voor de mutatie. De invloed hiervan mag geen dusdanig negatieve invloed op de performance tot gevolg hebben dat het werken met de oplossing praktisch onwerkbaar wordt.
EB-16	Er moet een automatisch (technisch) foutmeldingen register worden bijgehouden in de oplossing. Dit geldt voor fouten bij invoer als ook foutmeldingen m.b.t. koppelingen met andere applicaties. Het register is raadpleegbaar, ook voor niet-technisch gebruikers.
EB-17	De oplossing voorziet om geautomatiseerd IT-gerelateerde beveiligingsinformatie te verzamelen, te combineren en te analyseren of kan geautomatiseerd IT-gerelateerde beveiligingsinformatie door zetten naar een Security Information & Event Management oplossing (SIEM).
EB-18	De oplossing ondersteunt minimaal de volgende technische logging opties: • Logging naar meerdere log hosts; • Logging met verschillende methodes (syslog, syslog-ng, SMTP, NFS, SNMP, SOAP); • Logging filters, welke event wel/ niet, IP Address exclusion; • Rate limiting; • Secure logging (signing); Onderscheid tussen accounting, analyse en compliancy.
EB-19	De oplossing biedt een beheerscherm. Hiermee beschikt de beheerder over monitoring-, logging- en signaleringsfuncties op het gebied van gegevensuitwisseling (zowel intern als extern) voor alle koppelingen.
EB-20	Als onderdeel van het functioneel beheer kan beheerder in ieder geval: • Monitoring en beheer van de ESB-oplossing, incl. berichtenstroom van en naar landelijke voorzieningen en applicaties • Analyseren en verhelpen van (toekomstige) problemen • Aanpassen van configuratie instellingen (endpoints, certificaten, routering, e.d.) • Uitval zelfstandig opwerken en waar nodig berichten opnieuw verzenden vanuit de ESB-oplossing • Realiseren van nieuwe ESB-processen met koppelingen naar applicatie, testen en implementeren hiervan • Bijhouden van systeemadministratie, incl. inregelen autorisaties

#	Omschrijving
EB-21	De oplossing beschikt over (visuele) monitoringoverzichten voor, waarbij status van koppelingen, aantal verzonden en ontvangen berichten, uitval en foutieve aflevering, e.d. door beheerders kunnen worden gevolgd. Op basis van deze monitoringfuncties kunnen op flexibele wijze rapportages worden gegenereerd.
EB-22	De oplossing beschikt over signaleringsfunctie die onder andere aangeeft of een webservice is uitgevallen, of de toegang tot een bepaalde service is geweigerd, of berichten niet kunnen worden getransformeerd en/of berichten niet kunnen worden afgeleverd. Deze uitval wordt uitgelijst (in de werkvoorraad), geprioriteerd en is te filteren op datum, reden van uitval, webservice / koppeling. Uitval is voorzien van duidelijke omschrijving van de reden.
EB-23	Logginggegevens dient voor tenminste 1 jaar gearchiveerd te kunnen worden binnen de ESB-oplossing.

B.4 SaaS, Onderhoud en Technisch Beheer

#	Omschrijving
EB-24	De oplossing wordt aangeboden als SaaS-oplossing, inclusief beveiligde verbindingen. Enkel een gateway mag nog in het Demilitarized Zone (DMZ) van Opdrachtgever worden aangeboden, die tussen het interne netwerk en het internet is gepositioneerd. Dit betekent dat: • Opdrachtgever heeft toegang tot de oplossing via internet of een privénetwerk. • de oplossing en alle benodigde overige software en de daarvoor benodigde hardware zijn in eigendom van Leverancier. Opdrachtgever hoeft niets aan te schaffen, maar betaalt slechts voor het gebruik ervan. • de oplossing en overige software en hardware wordt niet bij de Opdrachtgever geïnstalleerd, maar bij Leverancier. Leverancier verzorgt de hosting, het technisch beheer en het applicatiebeheer, zoals het maken van back-ups, het onderhoud en de installatie van nieuwe versies en updates, beveiliging tegen ongeautoriseerde toegang, en dergelijke.
EB-25	Het beheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.
EB-26	Het functioneel beheer wordt door Opdrachtgever uitgevoerd.
EB-27	Het is mogelijk voor Opdrachtgever om de oplossing af te sluiten dan wel toegang tijdelijk te blokkeren voor (groepen van) geautoriseerde gebruikers ten behoeve van beheerwerkzaamheden.
EB-28	Wijzigingenbeheer is procesmatig en wordt procedureel zodanig uitgevoerd dat wijzigingen door Leverancier in de ICT-voorzieningen van de applicaties tijdig (tenminste 5 werkdagen vooraf), geautoriseerd door Opdrachtgever en getest door Leverancier worden doorgevoerd.
EB-29	Leverancier biedt een Service Level Agreement en een Dossier Afspraken en Procedures (DAP) binnen 3 maanden na ondertekening van de Overeenkomst ter acceptatie aan Opdrachtgever. De opgenomen normen in de SLA zijn minimaal gelijk of hoger dan gesteld in de servicenormen in dit Programma van Eisen.

#	Omschrijving
EB-30	Leverancier en de hostingpartij zijn gevestigd onder Nederlands of Europees recht. Hosting van het portaal en de gegevens vindt fysiek plaats in de Europese Economische Ruimte (EER) en in overeenstemming met de eisen van de Europese Unie.
EB-31	Opdrachtgever is en blijft eigenaar van de gegevens/data en heeft daar te allen tijde de zeggenschap over. Gegevens/data zijn ten alle tijden toegankelijk en mogen door de Leverancier niet voor andere doeleinden worden gebruikt.
EB-32	De integriteit van data blijft gewaarborgd door bedrijfskritische data van Opdrachtgever aantoonbaar te scheiden van andere klanten.

B.5 Interoperabiliteit, infrastructuur en koppelingen

#	Omschrijving
EB-33	De architectuur van oplossing voldoet aan de principes van de Nederlandse Overheid Referentie Architectuur (NORA/GEMMA).
EB-34	De oplossing dient volledig aan te kunnen sluiten op de huidige technische infrastructuur voor de hostingomgeving en de architectuur in het aanbestedingsdocument. De oplossing sluit naadloos aan op en werkt correct samen met de aanwezige applicaties binnen het applicatielandschap.
EB-35	De oplossing kent geen beperkingen met betrekking tot aantallen van gebruikers en/of te koppelen applicaties en voorzieningen, hoeveelheden data en berichten.
EB-36	Alle gegevens uit de database van de oplossing kunnen tenminste o.b.v. API, webservices (SOAP/REST), import/export, worden geëxtraheerd via een beschikbaar koppelvlak en in het kader van datagedreven sturing worden gebruikt in een datawarehousing of andere omgeving.
EB-37	Leverancier volgt GDI en GGI ontwikkelingen en werkt mee aan de ondersteuning van deze standaarden.
EB-38	Leverancier neemt toonbaar deel aan de Common Ground ontwikkelingen en kan aannemelijk maken dat het in de oplossing voorsorteert op deze ontwikkelingen door onder andere de ontwikkeling naar een API-based koppelingsvlak in het kader van de ontwikkeling van de Common Ground.
EB-39	De oplossing werkt met geautomatiseerd (binnengemeentelijk) berichtenverkeer op basis van actuele standaarden die door VNG-Realisatie of Forum Standaardisatie zijn vastgesteld en/of voorgeschreven.
EB-40	Leverancier waarborgt dat de aangeboden oplossing niet meer dan één major versie achterloopt op de standaarden van VNG-Realisatie of Forum Standaardisatie die voor de oplossing relevant zijn. Aanpassingen in de hierboven genoemde standaarden worden binnen zes maanden doorgevoerd nadat deze als nieuwe standaard zijn gepubliceerd. Daarnaast wordt de oude versie van de standaard nog minimaal één jaar ondersteund.
EB-41	Voor wat betreft de initiële scope moet de aangeboden oplossing op uiterlijk 31 mei 2022 de vulling en afname van gegevens uit tenminste onderstaande landelijke basisregistraties en voorzieningen via één centrale plek mogelijk maken: 1. Basisregistratie Adressen en Gebouwen (BAG) - afname en levering 2. Basisregistratie Grootschalige Topografie (BGT)

#	Omschrijving
	3. Basisregistratie Handelsregister (HR) 4. Basisregistratie Kadaster (BRK) 5. Basisregistratie Personen (BRP/GBA-V) 6. Basisregistratie Waardering Onroerende Zaken (LV WOZ) - individuele bevraging, indirecte bevraging, levering bronhouder, WOZ digilevering 7. Insolventieregister 8. Rijksbelastingen 9. Rijksdienst Wegverkeer (RDW) 10. Schuldenknooppunt (NVVK/SKP) 11. Stichting Netwerk Gerechtsdeurwaarders (SNG) 12. Terugmeldvoorziening (TMV 2.0) 13. Uitvoeringsinstituut Werknemersverzekeringen (UWV)
EB-42	Voor wat betreft de initiële scope moet de aangeboden oplossing op uiterlijk 31 mei 2022 gegevens kunnen uitwisselen via koppelingen met applicaties binnen het nieuwe applicatielandschap van BghU, zowel als deze on premise of in de cloud staan. Hieronder vallen tenminste: 1. Belastingapplicatie (incl. frontoffice) 2. Waarderingsapplicatie 3. BAG-Geo applicatie *NB. Deze applicaties worden in 2021 opnieuw aanbesteed. Op dit moment is nog niet bekend welke leverancier welke applicatie gaat leveren.*
EB-43	Koppelingen met systemen van opdrachtgevers en derden/deelnemers zijn voorzien in de doorontwikkeling, behoudens een tweetal nu al bestaande koppelingen die ook gelden voor de initiële scope: 1. Gemeente Lopik: VPN Lopik via Centric DDS-Lopik (BAG-gegevens) 2. Gemeente Utrecht: API naar CityControl (foto's naheffingsaanslag parkeren op vorderingsnummer)
EB-44	Komende jaren zal o.a. door verdere modularisatie, het gebruik van API's en de invulling van de Common Ground gedachte een sterk groeiende integratiebehoeften ontstaan. De ESB moet na livegang kunnen voorzien in een groei van gemiddeld ongeveer 2 tot 5 koppelingen per jaar (met deelnemers, interne applicaties onderling, e.d.). Uitgangspunt is dat deze applicaties en voorzieningen op basis van standaarden worden gekoppeld. Zie voor mogelijke koppelingen in deze optionele scope (doorontwikkeling) de opsomming in de aanbestedingsleidraad.
EB-45	De aangeboden oplossing moet het beheren van de toegang tot DigiD, eHerkenning en eIDAS aan verschillende afnemende voorzieningen via één centrale plek mogelijk maken.
EB-46	De oplossing ondersteunt eFacturen op basis van SimplerInvoicing
EB-47	De uitwisseling van gegevens dient plaats te vinden op basis van open standaarden zoals vastgesteld en geadviseerd door het Forum Standaardisatie.

<table>
<tr><th>#</th><th>Omschrijving</th></tr>
<tr><td>EB-48</td><td>De volgende aanbevolen standaarden vanuit het Forum Standaardisatie dient Leverancier toe te passen:
<table>
<tr><th>Standaard</th><th>Typering</th><th>Versie</th></tr>
<tr><td>AES</td><td>Versleutelingstechniek</td><td>FIPS 197</td></tr>
<tr><td>CMIS</td><td>Content-uitwisseling tussen CMS-/DMS-systemen</td><td>1.0</td></tr>
<tr><td>SFTP</td><td>Bestandsuitwisseling</td><td>RDC 959</td></tr>
<tr><td>IP Sec</td><td>Beveiligde IP verbindingen</td><td>RFC 4301 met RFC4309 + RFC 6040 en 7619</td></tr>
<tr><td>JSON</td><td>Uitwisseling van datastructuren</td><td>RFC8259 december 2017</td></tr>
<tr><td>SHA-2</td><td>authenticatie en integriteitscontrole</td><td>ISO/IEC 10118- 3:2016</td></tr>
<tr><td>SSH-2</td><td>Versleuteld inloggen</td><td>RFC 4251:2006</td></tr>
<tr><td>WSDL</td><td>Interface van webservices</td><td>2.0</td></tr>
<tr><td>X509</td><td>Authenticatie (PKI certificaten)</td><td>RFC5280 en update RFC6818</td></tr>
<tr><td>XML</td><td>Opmaaktaal voor gestructureerde gegevens</td><td>1.0</td></tr>
<tr><td>XSL</td><td>Transformeren XML berichten</td><td>XSL family</td></tr>
</table></td></tr>
<tr><td>EB-49</td><td>De Leverancier dient met haar oplossing ook de laatste versie van de Standaard Zaak- en Documentservices/ZKN-DMS, CMIS (https://www.gemmaonline.nl/index.php/Documentatie_Zaak-_en_Documentservices) volledig te kunnen ondersteunen.</td></tr>
<tr><td>EB-50</td><td>De Leverancier dient met haar oplossing ook TMLO/MDTO volledig te kunnen ondersteunen.</td></tr>
</table>

B.6 Backup en herstel

#	Omschrijving
EB-51	Herstelmaatregelen, waaronder back-up en recovery procedures, zijn geïmplementeerd en worden periodiek getest.
EB-52	De aangeboden oplossing biedt mogelijkheden tot error handling

B.7 Documentatie

#	Omschrijving
EB-53	De documentatie bevat minimaal volledige handleidingen en helpfunctie(s) voor beheerders. Hierbij moet ook inzichtelijk gemaakt worden welke parameters binnen de configuratie ingesteld kunnen worden en wat de werking en impact per parameter is.
EB-54	De opdrachtgever heeft het recht de documentatie vrij en kosteloos te verspreiden ten behoeve van de gebruikers.
EB-55	Bij ontbreken van bepaalde documentatie is Leverancier verplicht om op eerste verzoek van Opdrachtgever binnen 5 werkdagen de aanvullende documentatie kosteloos op te stellen en aan te leveren als aanvulling op de reeds beschikbare, officiële documentatie.
EB-56	Bij elke release (update en upgrade) wordt een geactualiseerde versie handleidingen en release notes verstrekt, waarin duidelijk wordt beschreven wat de wijziging zijn en eventuele consequenties voor de werking van de oplossing ten opzichte van de vorige versie.
EB-57	Volledige, actuele en relevante beschrijvingen van de oplossing waarin tenminste de volgende onderwerpen duidelijk worden toegelicht: architectuur, functies en functionele werking en technische specificaties waaronder die voor de koppelvlakken voor technische integratie met de andere applicaties.

#	Omschrijving
EB-58	Volledige en actuele technische infrastructuur van de oplossing waarin tenminste de volgende onderwerpen duidelijk worden toegelicht: ip-adressen, certificaten, locatie, dns naam etc.
EB-59	De Leverancier levert documentatie aan, waarin alle (incl. tweezijdige) koppelingen/koppelvlakken van de oplossing zijn beschreven.

B.8 Privacy en beveiliging

#	Omschrijving
EB-60	Leverancier en de hostingpartij zijn gevestigd onder Nederlands of Europees recht. Hosting van de oplossing en de gegevens vindt fysiek plaats in de Europese Economische Ruimte (EER) en in overeenstemming met de eisen van de Europese Unie.
EB-61	De oplossing voorziet de opdrachtgever in een systeembeschrijving waarin de cloud diensten inzichtelijk en transparant worden gespecificeerd en waarin de jurisdictie, onderzoeksmogelijkheden en certificaten worden geadresseerd.
EB-62	De oplossing heeft voor de cloud diensten een Service Management beleid geformuleerd met daarin richtlijnen voor de beheersingsprocessen, controleactiviteiten en rapportages.
EB-63	De Leverancier heeft ISO 27001 certificering om aan te tonen dat interne procedures op orde zijn.
EB-64	Alle gegevens zijn en blijven te allen tijde eigendom van de Opdrachtgever, zijn ten alle tijden toegankelijk en mogen door de Leverancier niet voor andere doeleinden worden gebruikt.
EB-65	De integriteit van data blijft gewaarborgd door bedrijfskritische data van Opdrachtgever aantoonbaar te scheiden van andere klanten.
EB-66	In de applicatieomgeving zijn signaleringsfuncties (registratie en detectie) actief, effectief en beveiligd ingericht. De loggings- en detectie-informatie (registraties en alarmeringen) en de condities van de beveiliging van ICT-systemen worden regelmatig gemonitord (bewaakt, geanalyseerd) en de bevindingen gerapporteerd.
EB-67	Alle onderdelen van servers met opslagmedia behoren te worden geverifieerd, om te waarborgen dat gevoelige gegevens en in licentie gegeven software voorafgaand aan verwijdering of hergebruik zijn verwijderd of betrouwbaar veilig zijn overschreven.
EB-68	Logbestanden van gebeurtenissen die gebruikersactiviteiten, uitzonderingen en informatiebeveiligingsgebeurtenissen registreren, behoren te worden gemaakt, bewaard en regelmatig te worden beoordeeld.
EB-69	Ter bescherming tegen malware behoren beheersmaatregelen te worden geïmplementeerd voor detectie, preventie en herstel in combinatie met een passend bewustzijn van de gebruikers.
EB-70	De oplossing, de inrichting daarvan en de autorisatie voor gebruik voldoen minimaal aan de richtlijnen van: • het Nationaal Cyber Security Centrum; • de Baseline Informatiebeveiliging Overheden (BIO); • de meest recente ISO normering voor informatiebeveiliging: ISO 27001 (of een vergelijkbare certificering); • alle wettelijke eisen van de AVG en aanpalende wetgeving (zoals o.a. de uitvoeringswet, archiefwet 1995);

#	Omschrijving
	• al het Informatiebeveiligingsbeleid van de opdrachtgever (gebaseerd op de Baseline Informatiebeveiliging Overheid). met inbegrip van de geldende policies t.a.v. autorisatie, logging, wachtwoordbeleid en verwerking van persoonsgegevens.
EB-71	De Leverancier stemt in met een jaarlijkse en kosteloze audit op informatiebeveiliging conform eerder genoemde richtlijnen door een onafhankelijke auditor en levert, als onderdeel van de tot stand te komen overeenkomst, kosteloos een TPM als bewijs van de audit.
EB-72	Functionaliteiten van de oplossing worden jaarlijks en kosteloos door de Leverancier voorzien van een TPM.
EB-73	De oplossing dient zelf standaardcontroles uit te voeren. Dit omvat bestands- en berekencontroles, integriteitcontroles, verbandscontroles, validiteitcontroles, domeincontroles en controles op onlogische data en dergelijke.
EB-74	De Leverancier behoort regelmatig de naleving van de beveiligingsovereenkomsten op compliancy te beoordelen, jaarlijks een assurance verklaring aan de Opdrachtgever uit te brengen en ervoor te zorgen voor onderlinge aansluiting van de resultaten uit deze twee exercities.
EB-75	Informatie over technische kwetsbaarheden van gebruikte informatiesystemen behoort tijdig te worden verkregen; de blootstelling aan dergelijke kwetsbaarheden moet worden geëvalueerd en passende maatregelen moeten worden genomen om het risico dat ermee samenhangt aan te pakken.
EB-76	De performance van de informatiebeveiliging van de cloud omgeving behoort regelmatig te worden gemonitord en hierover behoort tijdig te worden gerapporteerd aan de verschillende stakeholders.
EB-77	De oplossing voldoet aan de Baseline Informatiebeveiliging Overheden (BIO) en meest recente ISO normering voor informatiebeveiliging: ISO 27001.
EB-78	De opdrachtnemer laat jaarlijks zien dat het verschil tussen de ISO 27001 certificering en de in de BIO genoemde overeenkomstige harde maatregelen (passend op de SOA) is opgelost dan wel geïmplementeerd door middel van het afgeven van een Statement of Compliance (zie ook BIO 4.4 laatste paragraaf)
EB-79	De oplossing, de inrichting daarvan en de autorisatie voor gebruik voldoen aan de wettelijke eisen rondom privacy en beveiliging (AVG) en het informatiebeveiligingsbeleid van de Opdrachtgever (gebaseerd op de Baseline Informatiebeveiliging Overheid), met inbegrip van de geldende policies t.a.v. autorisatie, wachtwoordbeleid en verwerking van persoonsgegevens.
EB-80	Beheerders kunnen zonder tussenkomst van Leverancier realtime gebruikers en rollen binnen de oplossing aanmaken, wijzigen en gebruikers(rollen) autoriseren.
EB-81	De oplossing wordt ontsloten op basis van een beveiligde verbinding volgens de geldende (en toekomstige) veiligheidsstandaarden.
EB-82	De koppeling tussen de oplossing en de externe applicaties vindt plaats via een ipsec VPN verbinding of gelijkwaardige verbinding (datalijn) die aan de volgende eisen voldoet: • AES encryptie 128 bit of hoger • SHA2-256 authenticatie of beter

#	Omschrijving
EB-83	Sessie versleuteling. De oplossing past encryptie toe op de communicatie van vertrouwelijke gegevens over niet veilige netwerken, middels: • TLS 1.2 of hoger, HTTPS en HSTS (beveiligde verbinding) • DNSSEC (ondertekende domeinnaam)

B.9 Omgevingen

#	Omschrijving
EB-84	De installatie van de oplossing dient plaats te vinden in een productie- en een testomgeving. Dit dient te geschieden binnen geoffreerde prijsopgave, m.a.w. geen extra kosten per omgeving. De inrichting en het onderhoud van deze omgevingen dienen te worden meegenomen in de prijsopgave met inbegrip van de eventuele consequenties voor licentiekosten.

B.10 Service Levels

De volgende minimale Service Levels voor Onderhoud, Technisch Beheer en ondersteuning zijn van toepassing en dienen door Leverancier na contractering verwerkt te worden in haar standaard SLA en een DAP:

#	Omschrijving

EB-85	<u>Incidenten/problemen, prioriteit en hersteltijd</u>
	• De servicedesk van Leverancier is bereikbaar op Werkdagen van 8:00 tot 17:00.
	• Elk incident/probleem dat bij de servicedesk wordt gemeld, krijgt een bepaalde prioriteitsstelling. Prioriteitstelling vindt plaats op grond van impact en urgentie. De prioriteit van een incident wordt vastgesteld in samenspraak met de contactpersoon van de leverancier. Indien er geen overeenstemming is, stelt Opdrachtgever de prioriteit, en in geval van meerdere incidenten, de volgorde van afwikkeling van de incidenten vast.
	• Een incident/probleem met de hoogste prioriteit, prioriteitsgroep 1, wordt als volgt bepaald: de urgentie van het incident is hoog, want het betreft een kritisch bedrijfsvoeringsproces of de doorgang/voortgang van de bedrijfsvoering is/wordt ernstig verhinderd, en de impact op de organisatie van Opdrachtgever en/of de gebruikers is groot, omdat de gehele organisatie, een of meerdere locaties getroffen zijn dan wel de doorgang/voortgang van de bedrijfsvoering is/wordt ernstig verhinderd.
	• Er geldt geen beperking voor wat betreft het aantal (telefonische) meldingen/calls.
	• Leverancier incidenten/problemen met prioriteit 1 moeten binnen vier (4) uur na het melden van het incident/probleem verholpen zijn.
	  ○ Herstelwerkzaamheden ten behoeve van een prioriteit 1 incident/probleem zullen ononderbroken en ook buiten werkdagen worden uitgevoerd en op kortst mogelijke termijn worden voltooid, mits het incident/probleem tijdens Werkdagen tussen 8:00 en 17:00 is gemeld.
	  ○ Leverancier zal redelijkerwijs voorzien in een werkbare tijdelijke oplossing, indien het systeem - om welke reden ook - langer dan acht (8) uur buiten werking is c.q. niet beschikbaar is c.q. voorzienbaar is of wordt dat het systeem langer dan acht (8) uur buiten werking zal zijn en/of niet beschikbaar zal zijn. Leverancier zal binnen vier (4) uur na aanvang van het onderzoek naar de geëigende herstelmaatregelen een urenschatting afgeven.
	  ○ Een werkbare tijdelijke oplossing voldoet als oplossing, mits de werkbare tijdelijke oplossing ook binnen de gestelde maximale oplostijd beschikbaar is en niet langer dan 48 uur na melding van het incident benodigd is; binnen 48 uur is de oorzaak en het incident volledig opgelost met een structurele oplossing.
	• Alle incidenten/problemen/vragen worden geregistreerd in een servicemanagement tool. Opdrachtgever heeft te allen tijde inzage in (de status van) deze registraties.
	• De servicemanagement tool van de Leverancier moet (automatisch) kunnen koppelen met de meest gangbare servicemanagement tools in de markt. Leverancier koppelt kosteloos met de huidige servicemanagement tool van Opdrachtgever (TOPdesk).

#	Omschrijving
EB-86	Onderhoud Regulier onderhoud zal alleen uitgevoerd mogen worden met de voorafgaande toestemming of op verzoek van BghU op werkdagen tussen 18:00 uur en 7:00 uur of buiten werkdagen. Het uitvoeren van onderhoud zal minimaal vijf (5) werkdagen van tevoren worden aangekondigd.
EB-87	Beschikbaarheidsvenster en beschikbaarheid • Het systeem is in ieder geval gegarandeerd beschikbaar tussen 7:00 en 22:00 uur op werkdagen (beschikbaarheidsvenster). Het systeem is beschikbaar indien er, gedurende het tijdsvenster, geen incidenten uit met prioriteit 1. • Buiten het beschikbaarheidsvenster is het systeem ook te allen tijde beschikbaar, maar op basis van best-effort en behoudens gepland onderhoud. • De norm voor de gemiddelde beschikbaarheid van het systeem is 98,75% gedurende het gegarandeerde beschikbaarheidsvenster over een periode van een maand. • De maximaal aaneengesloten onbeschikbaarheid gedurende het beschikbaarheidsvenster mag niet meer dan 4 uren overschrijden. ○ Minimaal 98,75% beschikbaarheid betekent maximaal 1,25% onbeschikbaarheid per maand. Gemiddeld 261 werkdagen in een jaar, derhalve 21,75 werkdagen per maand. Het gegarandeerde beschikbaarheidsvenster omvat de tijdsperiode 7:00 tot 22:00 = 15 uur. De totale maximale onbeschikbaarheid per maand in het van een 98,0% beschikbaarheid bedraagt daarom: 1,25% x 15 x 21,75 = 4 uur en 5 minuten per maand binnen het beschikbaarheidsvenster.
EB-88	Capaciteit/performance Leverancier garandeert voldoende capaciteit voor het gebruik van de ESB-oplossing en de koppelingen in relatie tot het aantal berichten dat dagelijks en tijdens piekmomenten verzonden moet kunnen worden. Inschatting is dat het grootste piekmoment de LV WOZ en beschikkingen in februari betreft, waarbij de load bestaat uit 400.000 objecten met gemiddeld 3 à 4 berichten (dus ca. 1,5 miljoen berichten) die binnen 24 uur moeten zijn verzonden en waarvoor ontvangstbevestigingen moeten zijn ontvangen. Leverancier biedt voldoende en schaalbare mogelijkheden voor de uitbreiding van de capaciteit van de oplossing in het geval van piekmomenten, toename van het gebruik of anderszins, in relatie tot het regulier gebruik.

EB-89	Backup en herstel
	• Leverancier voert dagelijks back-ups uit voor hersteldoeleinden op twee niveaus:
	  ○ database back-ups
	  ○ server back-ups
	• De Recovery Point Objective (maximale dataverlies) bedraagt maximaal 4 uur.
	• De Recovery Time Objective (maximale hersteltijd) bedraagt maximaal 4 uur.

EB-90	Monitoring Leverancier zal het systeem zodanig inrichten dat het voor de leverancier, die de bewaking uitvoert, mogelijk is om de beschikbaarheid, capaciteit en performance van alle vitale hardware- en softwarecomponenten die noodzakelijk zijn voor (het normale gebruik van) het systeem 24 uur/7 dagen per week te kunnen bewaken. De bewaking van het systeem is zodanig ingericht dat de realisatie van de overeengekomen servicenormen gewaarborgd zijn.

C Implementatie

C.1 Implementatie

#	Omschrijving
D-001	Leverancier is verantwoordelijk voor de volledige ontwikkeling en implementatie van de oplossing conform de Aanbestedingsdocumentatie en dit Programma van Eisen. Hiervoor wordt een plan van aanpak meegestuurd bij de Inschrijving.
D-002	De volgende uiterlijke mijlpalen gelden: • Testomgeving ESB beschikbaar: januari 2022 • Productieomgeving ESB beschikbaar: september 2022
D-003	Leverancier benoemt in het plan van aanpak welke vereisten nodig zijn aan de kant van Opdrachtgever voor de toegang tot de oplossing (de bandbreedte internetsnelheid, poorten, firewalls, systeemeisen aan servers, systeem eisen voor cliënt, etc.).
D-004	De Leverancier levert na definitieve gunning en voor implementatietraject een informatiearchitectuur en technisch ontwerp voor de nieuwe situatie waarin de applicaties, koppelingen en afhankelijkheden met andere zaken binnen de infrastructuur in kaart zijn gebracht en beschreven.
D-005	Voorafgaand aan de implementatie (indien sprake is van standaards) dient de Leverancier een schema op te leveren van het berichtenverkeer. Indien een applicatie niet aan de standaards voldoet is het aan de Leverancier ervoor zorg te dragen dat de betreffende leverancier inzicht krijgt in de afwijkingen van de standaards en Opdrachtgever ondersteunt in het gecorrigeerd krijgen van de afwijking.

C.2 Doorontwikkeling (Upgrades en Updates)

#	Omschrijving
D-006	Naast de realisatie van de bestaande koppelingen met landelijke voorzieningen en kernapplicaties is de verwachting naar de toekomst toe dat de informatiesystemen steeds meer aan elkaar worden gekoppeld, ongeacht of een applicatie in de cloud staat of on-premise. Het dient mogelijk te zijn om nieuwe koppelingen te realiseren. Na oplevering van een nieuwe koppeling wordt deze gedocumenteerd, wordt de architectuur bijgewerkt en toegevoegd aan de totale systeemdocumentatie.
D-007	Bij de doorontwikkeling van de oplossing wordt https://cve.mitre.org/ gebruikt om kwetsbaarheden in software te identificeren.
D-008	Alle gebruikte software wordt, na het ontdekken, binnen onderstaande termijnen voorzien van beschikbare beveiligingsupdates dan wel een workaround voor een adequate mitigering van de kwetsbaarheid: • Voor kwetsbaarheden met een CVSS base score lager dan 4: de eerstvolgende major of minor release van de software; • Voor kwetsbaarheden met een CVSS base score tussen 4.0 en 6.9: binnen 3 maanden na het uitkomen van een patch;

#	Omschrijving
	• Voor kwetsbaarheden met een CVSS base score tussen 7.0 en 8.9: binnen 1 maand na het uitkomen van een patch; • Voor kwetsbaarheden met een CVSS base score tussen 9.0 en 10: binnen 72 uur na het uitkomen van een patch.
D-009	Upgrades en Updates worden vanuit de Leverancier na overleg met en toestemming van Opdrachtgever beschikbaar gesteld. Technische systeemtests worden vooraf door de Leverancier uitgevoerd. De Upgrades en Updates kunnen dan functioneel worden getest door Opdrachtgever.
D-010	Bij Upgrades en Updates geeft de Leverancier tijdig aan wanneer deze plaatsvinden
D-011	Bij Upgrades en Updates van de oplossing zorgt de Leverancier ervoor dat bestaande koppelingen blijven functioneren.
D-012	Bij Upgrades en Updates garandeert de Leverancier dat de bestaande inrichting en werkstromen en instellingen intact blijven en hun werking behouden. Het moet duidelijk zijn welke invloed de wijzigingen hebben op de inrichting en/of werkstromen, zodat deze wijzigingen op zelf ontwikkelde inrichting en werkstromen kunnen worden doorgevoerd.

C.3 Opleidingen

#	Omschrijving
D-013	Inschrijver is verantwoordelijk voor het geven van de opleidingen aan de beheerders voor het gebruik van de oplossing conform de Aanbestedingsleidraad en het PvE. Toelichting op deze opleiding dient te worden opgenomen in het plan van aanpak.

C.4 Testen en acceptatie

#	Omschrijving
D-014	Inschrijver zorgt voor het beschikbaar stellen en onderhouden van een representatieve test- en productieomgeving conform beschreven eisen en overeengekomen KPI's.
D-015	Leverancier levert testscenario's die als basis dienen voor het technisch testen en accepteren van de oplossing.
D-016	Leverancier ondersteund actief bij de functionele testen die vanuit de vakinhoudelijke applicaties plaatsvinden (o.a. waarderen, belastingen en BAG-Geo).
D-017	In het plan van aanpak bij de Inschrijving dient de procedure voor het testen en accepteren te worden beschreven. Opdrachtgever wil hier duidelijk verwoord zien wat de criteria zijn voor acceptatie waarbij dus duidelijk is in welk geval er geen tijdige acceptatie is.

---oOo---