

ABSTRACT

Het beoogde nieuwe financiële biedt voor medewerkers in de Gemeenschappelijke Regeling (Gemeenten Maasgouw, Echt-Susteren, Roerdalen en het servicecentrum MER) een gebruikersvriendelijke toegang tot financiële processen en de gerelateerde data/gegevens om handmatige werkzaamheden en schaduwboekhouding zo veel mogelijk overbodig te maken. Dit document bevat de eisen waaraan de nieuwe applicatie dient te voldoen

Inhoudsopgave

1 INFORMATISERING (ICT) 4

1.1 ALGEMEEN 4
1.2 ICT-ARCHITECTUUR (COMPONENTEN) 4
1.3 HUIDIG APPLICATIELANDSCHAP 5
1.4 GEWENST APPLICATIELANDSCHAP 5
1.5 INRICHTING 7
1.6 PERFORMANCE 7
1.7 STANDAARDEN, INTEGRATIE, KOPPELINGEN 8
1.8 AUTHENTICATIE EN TOEGANKELIJKHEID 9
1.9 INFORMATIEBEVEILIGING 9
1.10 PRIVACY 10

Wijzigingshistorie

Datum	Omschrijving van uitgevoerde wijziging	Versie
16-08-2022	Inhoud van hoofdstuk 11 (Informatisering – ICT) uit intern Programma van Eisen document versie 2.2 als separaat aanbestedingsdocument gecreëerd.	0.9
18-08-2022	Aanvullingen/correcties inclusief architectuur platen, uit mail Maud Verberne van 17 augustus verwerkt	0.9b

1 Informatisering (ICT)

1.1 Algemeen

1.1.1 GIBIT

De GIBIT (Gemeentelijke voorwaarden bij IT) inkoopvoorwaarden zijn leidend bij de aanschaf van de beoogde oplossing.

1.1.2 Service Level Agreement

Een standaard-SLA maakt onderdeel uit van de offerte en is smart geformuleerd. Het specifiek maken van deze standaard-SLA maakt onderdeel uit van de implementatie. Na implementatie wordt door de leverancier inzage gegeven in het behaalde niveau van dienstverlening (beschikbaarheid, incidentafhandeling, e.d.) in relatie tot de SLA.

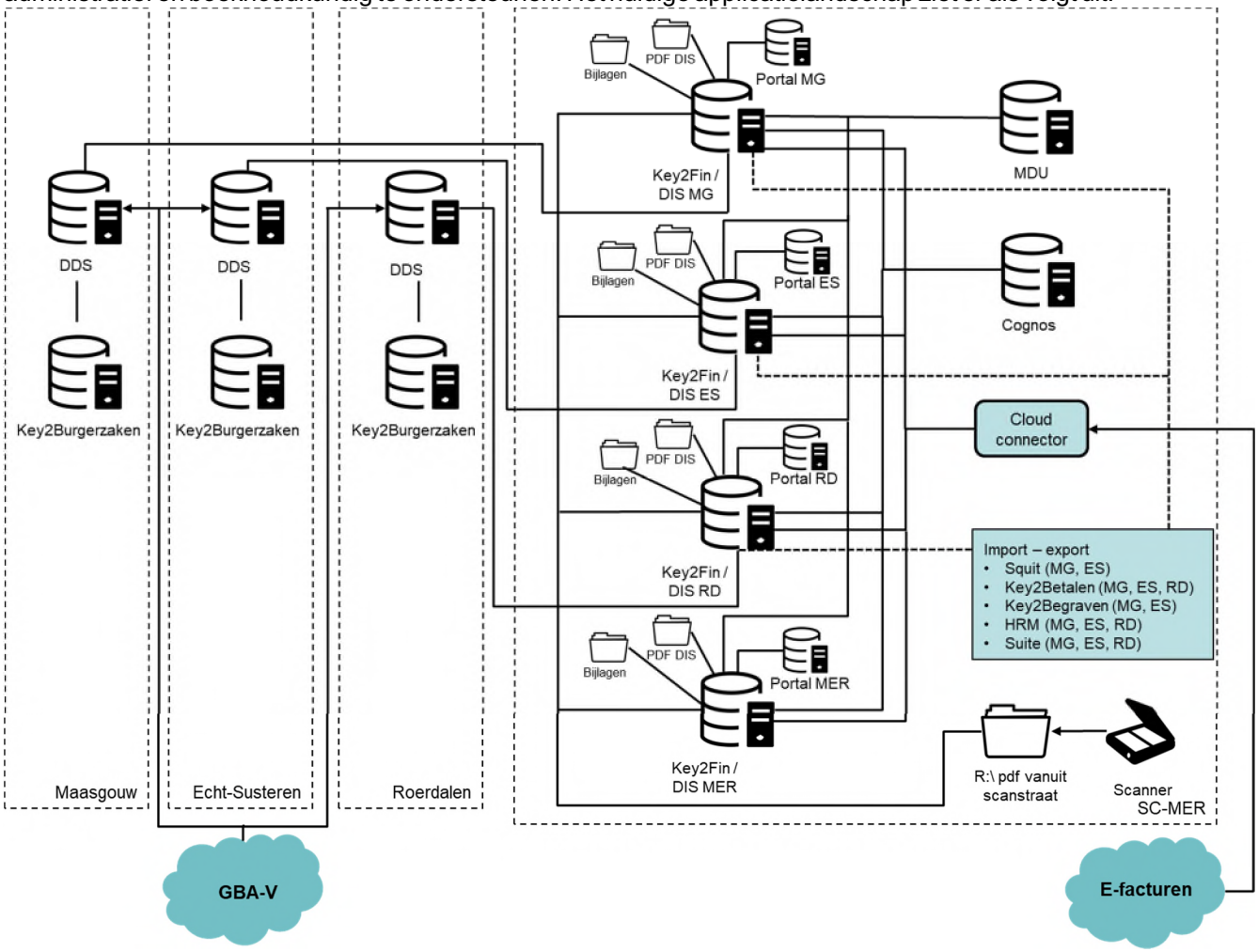
1.2 ICT-architectuur (componenten)

SC-MER (Cluster ICT) onderhoudt en ontwerpt de gezamenlijke technische MER ICT-architectuur. In onderstaande tabel is een compacte beschrijving opgenomen van de componenten (hard- en software) welke worden ingezet binnen de technische architectuur van het SC-MER. Deze zijn bepalend voor de compatibiliteit van nieuwe soft- en/of hardware i.r.t. onze technische ICT-architectuur. De beoogde oplossing dient hierop aan te sluiten.

Hypervisor	VMware vSphere 7.xx
Netwerk virtualisatie	VMware NSX-T
Besturingssysteem server	Windows Server 2019 of hoger
Active Directory Forest / Domain Level	Microsoft AD Forest 2016 / Domain 2016
E-Mail Servers	Microsoft Exchange 2016
Database managementsysteem	▪ Oracle Database Enterprise Edition ▪ Microsoft SQL Server 2019 of hoger
MFA Platform	▪ Microsoft Azure MFA (authenticator)
Mobiel managementsysteem	▪ Mobile Iron
Mobiel besturingssysteem	▪ Android ▪ iOS
Mobiel Applicatie distribute	▪ Google Play Store ▪ Apple App Store
Profielbeheer	▪ Ivanti Workspace Control
Single Sign On (SSO)	▪ VMware Horizon View / ADFS / Azure AD
Virus scanner	▪ TrendMicro Deepsecurity
Thin client	▪ Dell Wyse (Windows IoT)
Besturingssysteem werkplek	▪ Windows 10 Enterprise 21H2
KA omgeving	▪ Microsoft Office 2013
Webbrowser	▪ Microsoft Edge ▪ Firefox
Applicatiedistributie	▪ Ivanti Automation Manager ▪ Portable applicatie (eventueel uitvoerbaar vanuit een fileshare zonder installatie) ▪ Client-server installaties ▪ Webapplicatie (intern of cloud; e.e.a. afhankelijk van informatie, AVG, back-up)
Afhankelijkheden Grafische impact werkplekken	▪ In overleg o.a. bewegende beelden / clips, MS Teams en CAD verwerking

1.3 Huidig applicatielandschap

Op dit moment wordt Key2Financien ingezet om de 4 organisaties en hun administraties, opererend in de gemeenschappelijke regeling van het Servicecentrum MER (de gemeenten Maasgouw, Echt-Susteren en Roerdalen en het servicecentrum zelf), administratief en boekhoudkundig te ondersteunen. Het huidige applicatielandschap ziet er als volgt uit:



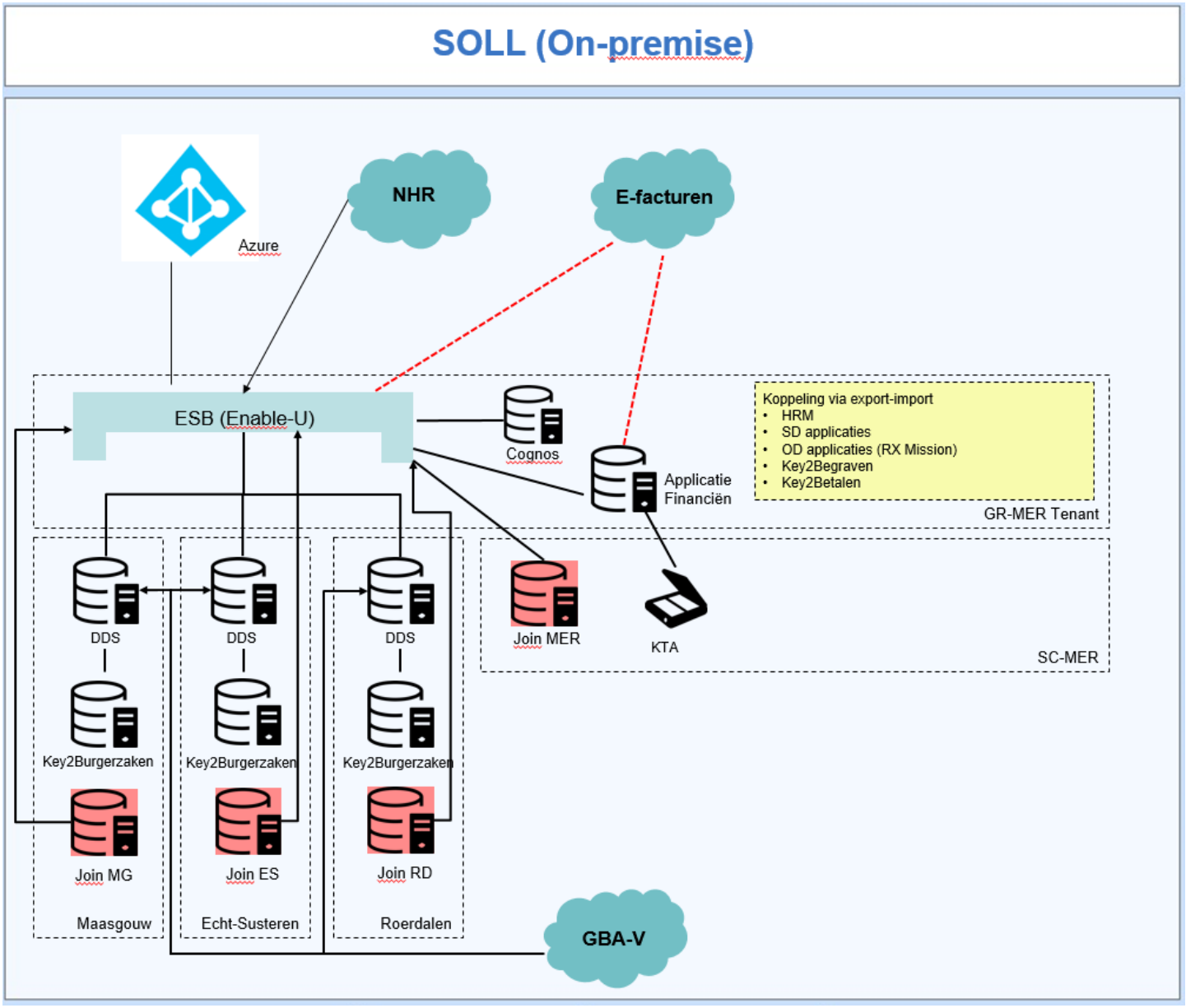
1.4 Gewenst applicatielandschap

Het beoogde nieuw financieel pakket is gericht op het versterken en implementeren van de doelstelling van het Servicecentrum MER, om processen te harmoniseren en te optimaliseren. Een beoogd raamwerk voor vier organisaties met elk een eigen administratie, waarbij er wel wordt gestreefd naar één uniform grootboek rekeningschema, uniforme P&C cyclus), met gestroomlijnde en op elkaar afgestemde processen en werkwijzen.

Servicecentrum MER wil kunnen kiezen voor de meest geschikte oplossing. Deze kan of on-premise worden geïnstalleerd dan wel via de Cloud aangeboden worden. Het streven is in ieder geval om de medewerkers in de Gemeenschappelijke Regeling (Gemeenten Maasgouw, Echt-Susteren, Roerdalen en het Servicecentrum MER) een gebruikersvriendelijke toegang tot financiële processen en de gerelateerde data/gegevens te bieden.

1.4.1 On-premise oplossing

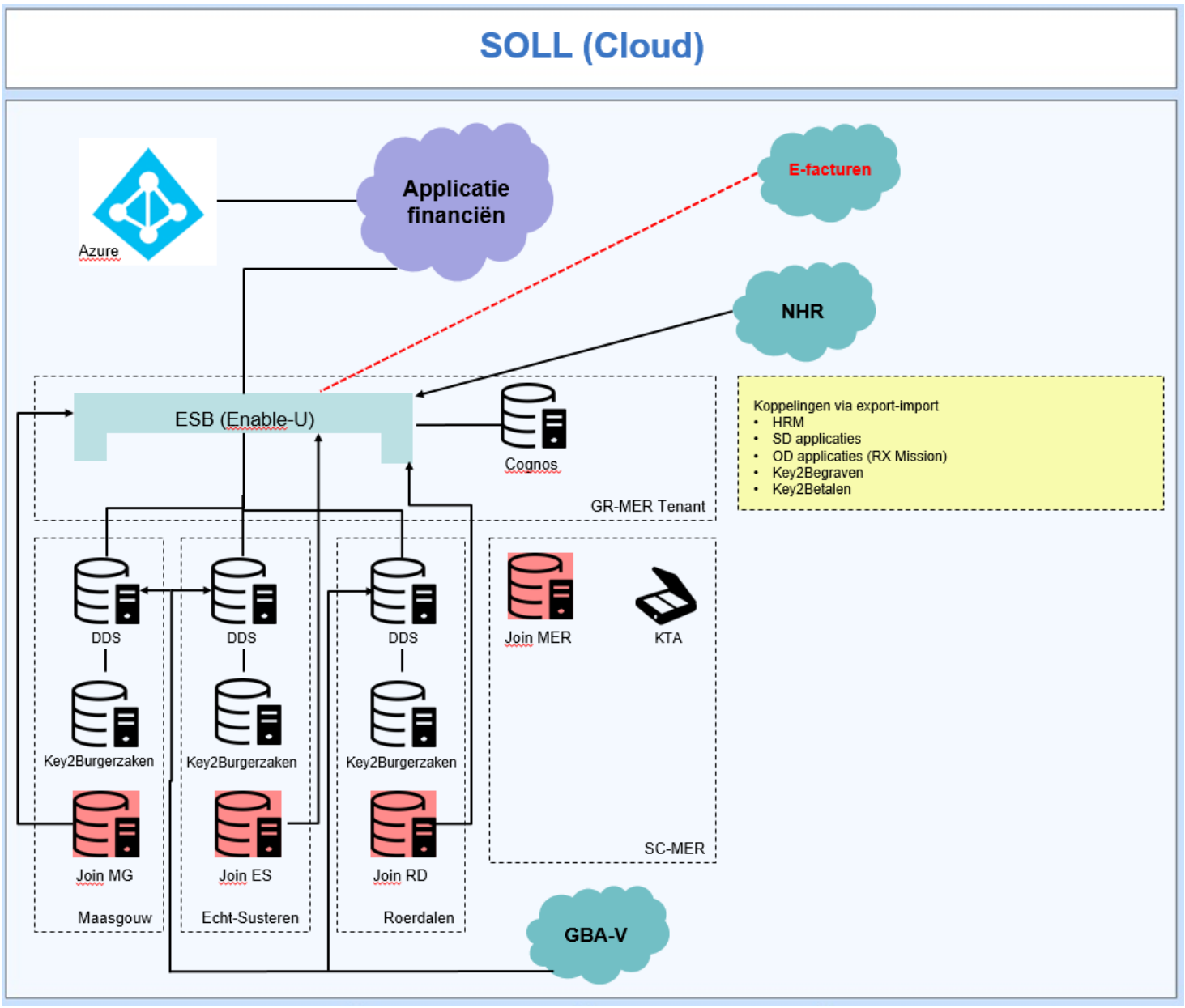
Indien wordt gekozen voor een on-premise oplossing, ziet het beoogde landschap er als volgt uit:



1. Op dit moment is er nog 1 Cognos per organisatie. Er komt op termijn 1 Cognos in de GR-MER tenant
2. Alleen koppeling met zaaksysteem (JOIN) noodzakelijk indien applicatie zelf niet voldoet aan archiveringseisen.
   Er zijn twee mogelijkheden:
   1. Alles archiveren in de Join binnen de MER-omgeving mits er per gemeente een unieke waarde kan worden meegegeven.
   2. Archivering splitsen naar de Join omgevingen van de gemeenten.

1.4.2 Cloud-oplossing

Indien wordt gekozen voor een cloud-oplossing, ziet het beoogde landschap er als volgt uit:



1. Op dit moment is er nog 1 Cognos per organisatie. Er komt op termijn 1 Cognos in de GR-MER tenant
2. Alleen koppeling met zaaksysteem (JOIN) noodzakelijk indien applicatie zelf niet voldoet aan archiveringseisen.
   Er zijn twee mogelijkheden:
   1. Alles archiveren in de Join binnen de MER-omgeving mits er per gemeente een unieke waarde kan worden meegegeven.
   2. Archivering splitsen naar de Join omgevingen van de gemeenten.

1.5 Inrichting

1.5.1 De oplossing is multi-tenant. De oplossing kan verschillende inrichtingen voor verschillende deelnemende organisaties leveren met scheiding van gegevens, autorisaties, workflows.

- Gegevens dienen herleid te kunnen worden naar de verwerkingsverantwoordelijken. Dit is noodzakelijk om te voldoen aan audit verplichtingen, te voldoen aan wetgeving (zoals het beantwoorden van inzageverzoeken), en het kunnen uitvoeren van een exit-plan/ontvlechting. Bij ongestructureerde data neemt dit risico toe. Ook bij een heldere mandatering is herleiding naar verwerkingsverantwoordelijke noodzakelijk.
- Er dient voldoende zicht te zijn op beheeracties zodat beheeracties te herleiden zijn naar de juiste verantwoordelijken.
- Het moet mogelijk zijn om de rechten van medewerkers adequaat te beperken

1.5.2 De oplossing biedt naast een productie-omgeving een test-omgeving.

1.6 Performance

1.6.1 De applicatie dient de wijzigingen realtime te kunnen verwerken.

1.7 Standaarden, integratie, koppelingen

1.7.1 De beoogde oplossing kan door de leverancier on-premise worden geïnstalleerd of via de cloud aangeboden worden. In beide situaties moet worden aangesloten op de aangegeven componentspecificaties in paragraaf 11.2[1]

1.7.2 Indien er wordt gekozen voor een SAAS-oplossing dan moet er probleemloos gekoppeld kunnen worden met andere on-premise en/of SAAS oplossingen die in gebruik zijn bij de drie gemeenten (Maasgouw, Echt-Susteren en Roerdalen) en het Service centrum MER zelf.

1.7.3 De leverancier geeft aan welke koppelingen noodzakelijk zijn voor het juist functioneren van de voorgestelde oplossing. Binnen de Gemeenschappelijke Regeling wordt gebruik gemaakt van microsegmentatie (VMware NSX-T) om te voorzien in een adequate beveiliging van systemen. Dit betekent dat de leverancier een technische beschrijving dient aan te leveren van te realiseren koppelingen. In de technische beschrijving is minimaal beschreven welke netwerk- protocollen, verbindingen en poorten gebruikt worden.

1.7.4 De beoogde oplossing wisselt gegevens uit met andere voorzieningen (zoals taak specifieke applicaties en generieke voorzieningen) via de gemeentelijke service bus (*toelichting*: Open Tunnel van Enable-U wordt ingezet als ESB).

1.7.5 Gegevensuitwisseling gebeurt middels een generiek koppelvlak/ standaard, hiervoor is geen maatwerk nodig

1.7.6 Koppelingen worden gerealiseerd op basis van standaarden zoals geformuleerd door Forum Standaardisatie (https://www.forumstandaardisatie.nl/open-standaarden/stuf). De beoogde oplossing moet gegevens kunnen uitwisselen op basis van deze standaarden.

1.7.7 De beoogde oplossing ondersteunt het gebruik van de standaard API's. Wanneer via Haal Centraal een API beschikbaar wordt gesteld om basisregistratie gegevens uit te wisselen zal de leverancier zo spoedig als mogelijk de beschikbare API's gebruiken.

1.7.8 NAW- en andere gegevens die in een van de landelijke basisregistraties (BRP, BAG, WOZ, NHR, GBA-V) worden bijgehouden, dienen rechtstreeks uit deze registraties te worden gehaald.

1.7.9 De beoogde oplossing dient een mogelijkheid te bieden om te koppelen met de BI-tool van Servicecentrum MER (op dit moment Cognos Analytics) waarbij er rechtstreeks wordt gekoppeld met de database (of via package of API) en niet middels een import of export van csv/Excel bestanden. De gegevens mogen hierbij maximaal 1 dag oud zijn.

1.7.10 De beoogde oplossing heeft koppelingen met de standaard betalingsmethodieken zoals PayPal, IDEAL, credit card.

1.7.11 De beoogde oplossing moet de standaardformaten UBL, XML, csv, xls, pdf/a en XBRL kunnen importeren en exporteren.

1.7.12 De beoogde oplossing kan inkomende e-facturen verwerken conform de geldende wetgeving Nederlandse afgeleide van de Europese norm voor e-facturen, NLCIUS (Nederlandse Core Invoice Usage Specification).

1.7.13 De oplossing kan koppelingen maken met andere systemen met behulp van onderstaande standaarden:

- SimplerInvoicing-UBL + UBL-OHNL
- Betalen en invorderen services (STUF-FIN)
- ISO 20022
- XBRL
- StUF-BG

1.7.14 De leverancier levert en implementeert, inclusief documentatie, de applicatie met de volgende integraties:

- BNG Bank t.b.v. betalingsverkeer;
- Peppol netwerk t.b.v. zowel inkomende als uitgaande e-facturen;
- Kofax Capture/KTM t.b.v. zowel fysieke als digitale facturen

1.7.15 Vereiste koppelingen

De beoogde oplossing dient met de volgende applicaties te kunnen koppelen:

a) Open Tunnel (Enable-U)
b) Suite4Sociaal Domein (Centric)
c) Key2Begraven (Centric)
d) Key2Betalen (Centric)
e) Key2datadistributie (Centric)
f) Decos JOIN (Decos)
g) Profit (AFAS)
h) SquitXo / Rx.Mission (ROXIT)
i) Cognos (IBM)
j) Office 365 (Microsoft)
k) Kofax Capture en KTM

[1] Alle aandachtspunten en eisen met betrekking tot de technische architectuur van het Servicecentrum MER, zijn verwoord in een separaat document (SC-MER Technische Architectuur voor Leveranciers, versie 1.1 van 12 juli 2022).

1.7.16 De leverancier levert op verzoek van Opdrachtgever mondeling en/of schriftelijk inzicht in het fysieke datamodel van de applicatie.

1.8 Authenticatie en toegankelijkheid

1.8.1 De beoogde applicatie moet het mogelijk maken om toegang tot informatie en functionaliteiten (authenticatie en autorisatie) alleen toe te staan aan gebruikers die vanuit hun taken rechten nodig hebben op deze informatie.
1.8.2 Authenticatie moet verlopen via SSO op basis van de door de opdrachtgever gebruikte core identity provider
1.8.3 Indien er wordt gekozen voor een SAAS-oplossing krijgt de medewerker idealiter toegang tot de applicatie via een standaard webbrowser. Uiteraard hoort hier een identificatie-, authenticatie- en autorisatiemechanisme bij dat voldoende beveiliging en betrouwbaarheid biedt.
1.8.4 Indien er wordt gekozen voor een SAAS-oplossing, functioneert deze idealiter op basis van HTML en zijn onafhankelijk van het onderliggende besturingssysteem c.q. plug-ins met als doel dat de applicatie in de virtuele werkplek kan worden gebruikt maar in de toekomst ook daarbuiten.

1.9 Informatiebeveiliging

1.9.1 De leverancier stelt een contactpersoon aan voor de CISO van de opdrachtgever.
1.9.2 In het geval van een inbraak op de beveiliging die van invloed is op, of een risico kan vormen voor de dienstverlening aan opdrachtgever, dan informeert leverancier onverwijld de CISO van de opdrachtgever hierover.
1.9.3 Indien een inbreuk in verband met persoonsgegevens (datalek) of een security incident heeft plaatsgevonden, meldt de leverancier deze zonder onredelijke vertraging en uiterlijk 72 uur nadat hij er kennis van heeft genomen, aan afnemer. Indien de melding aan de afnemer niet binnen 72 uur plaatsvindt, gaat zij vergezeld van een motivering voor de vertraging.
1.9.4 De leverancier is in het bezit van een ISO27001 certificaat op het moment van levering van het beoogde systeem. Tevens dient de leverancier een TPM verklaring te kunnen tonen ten aanzien van de maatregelen die uit de ISO 27002 zijn geselecteerd en die een technisch karakter hebben (ISAE 3000 SOC 2 type 2). De verklaring van toepasselijkheid dient te worden meegestuurd met het certificaat waarmee wordt aangetoond dat de ICT-dienstverlening voldoet aan de kwaliteitsstandaarden van ISO27001 of vergelijkbaar (BIO beveiligingsniveau BBN).
1.9.5 Indien de leverancier tevens in het bezit is van een ISO22301 of ISO 27701 certificaat dan geldt ook hier dat het certificaat getoond dient te worden.
1.9.6 De oplossing mag ten opzichte van onderstaande normeringen geen kritieke of hoog-risico bevindingen bevatten, zowel ten tijde van de aanbesteding als ten tijde van het reguliere gebruik:
1.9.7 Informatiebeveiliging moet aantoonbaar voldoen aan de eisen gesteld door Platform Internetstandaarden (internet.nl, >70%).
1.9.8 De oplossing biedt aantoonbaar minimaal bescherming tegen de OWASP top 10 bedreigingen: https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project
1.9.9 De oplossing voldoet aantoonbaar aan de ICT-Beveiligingsrichtlijnen voor Webapplicaties: https://www.ncsc.nl/actueel/whitepapers/ict-beveiligingsrichtlijnen-voor-webapplicaties.html
1.9.10 Alle verplichte standaarden van het Forum standaardisatie zijn aantoonbaar geïmplementeerd: https://www.forumstandaardisatie.nl/open-standaarden/lijst/verplicht
1.9.11 De leverancier werkt mee aan audits en pentesten op verzoek van de opdrachtgever (right to audit).
1.9.12 De leverancier laat, bij hosting, periodiek (minimaal 1x per jaar) een whitebox penetratietest, waarbij een kwetsbaarheids-scan onderdeel vormt van de pentest, uitvoeren op zijn systemen binnen de scope van de dienstverlening. De resultaten van deze test, de opvolging van de testresultaten en de oplossingsmogelijkheden conform het risicoprofiel worden gerapporteerd aan cluster ICT van SC MER. Daarbij is vereist dat alle high-risk bevindingen opgelost worden binnen de vastgestelde tijd conform de SLA. De penetratietester dient de test uit te voeren onder geheimhouding.
1.9.13 Als de leverancier e-mails dient te verzenden namens de maildomeinen van de gemeenten of het Servicecentrum past de leverancier minimaal de door het NCSC geadviseerde bescherming tegen e-mailspoofing toe en gestelde eisen vanuit de BIO. M.a.w. maakt gebruik van SPF, DKIM en DMARC.
1.9.14 De leverancier beschikt over een expliciete exit-strategie (als bedoeld in artikel 22 GIBIT 2020), waarin minimaal het volgende beschreven is: bij faillissement, overname of ontbinding van het bedrijf van de leverancier of kritische ketenpartners van de leverancier dient te zijn vastgesteld op welke wijze de dienstverlening blijvend kan worden gewaarborgd (ESCROW, verzekeringen, overdracht bij ketenpartners).
1.9.15 De oplossing beschikt over een niet-muteerbare audit-trail van gebruikers en beheerders met daarin minimaal de gebeurtenis; de benodigde informatie die nodig is om de verwerking (conform definitie art. 4 sub 2 AVG) te herleiden tot een gebruiker; de handeling; een datum en tijdstip van de gebeurtenis. Een logregel bevat in geen

geval gegevens die tot het doorbreken van de beveiliging kunnen leiden. Ten behoeve van de loganalyse is op basis van een expliciete risicoafweging de bewaarperiode van de logging bepaald. Binnen deze periode is de beschikbaarheid van de loginformatie gewaarborgd. De logging is read-only en is alleen beschikbaar voor daartoe geautoriseerde medewerkers. Het muteren en verwijderen van logrecords is niet toegestaan.

1.9.16 De autorisatie dient rol gebaseerd te zijn waarbij gebruik gemaakt wordt van de door de opdrachtgever gebruikte core identity provider.

1.9.17 In de SLA van de dienstverlening wordt een beveiligingsparagraaf opgenomen. De leverancier dient hiermee in te stemmen. In de beveiligingsparagraaf worden service levels opgenomen voor:
- maximale oplostijden na penetratietesten of kwetsbaarheids-scans;
- maximaal incident response;
- maximale doorlooptijden voor repareren van kwetsbaarheden;
- wijze van het melden van incidenten zoals beveiligings- of datalekken;
- maximaal toelaatbare uitval van de oplossing en maximaal dataverlies bij uitval (RPO en RTO).

1.9.18 Er wordt, bij hosting door opdrachtnemer, door de opdrachtnemer continu actief gecontroleerd op Intrusion Detection op de applicatie. De resultaten van deze controle, de opvolging van de controle en de oplossing worden gerapporteerd aan Cluster ICT van SR MER.

1.9.19 Indien gebruik wordt gemaakt van cryptografische algoritmen, waarbij sleutelbeheer van toepassing is, dient gebruik gemaakt te worden van PKI overheidscertificaten ten aanzien van het sleutelbeheer (ISO11770).

1.9.20 De juistheid en kwaliteit (integriteit) van persoonsgegevens kunnen via invoermechanismes en importmechanismes afgedwongen worden. Hiervoor is een datamodel beschikbaar.

1.10 Privacy

1.10.1 Leverancier handelt als verwerker in de zin van de Algemene verordening gegevensbescherming.

1.10.2 De leverancier gaat akkoord met het tekenen van een verwerkersovereenkomst, die voldoet aan de meest recente versie van de standaard verwerkersovereenkomst voor gemeenten van de VNG (artikel 28 lid 3 AVG).

1.10.3 De gegevens worden niet verkocht aan derde partijen (Artikel 28 lid 3 onder a AVG).

1.10.4 Er is een goedgekeurde gedragscode voor het omgaan met het verwerken van persoonsgegevens.

1.10.5 Als de leverancier toegang wil tot de gegevens in de applicatie, dan is dit door de beheerorganisatie geïnitieerd en handelt de leverancier vanuit die gedragscode.

1.10.6 Het is mogelijk een overzicht te krijgen van de persoonsgegevens van een persoon die worden opgeslagen, indien dit gevraagd wordt (artikel 28 lid 3 onder e AVG).

1.10.7 Er moet aangegeven kunnen worden op basis van welke grondslag persoonsgegevens bewaard worden. (Artikel 28 lid 3 onder e AVG)

1.10.8 De betrokkene die een rectificatieverzoek (Recht op rectificatie) indient kan een aanvullende verklaring verstrekken. Deze aanvullende verklaring, of zienswijze, moet kunnen worden toegevoegd aan de gewijzigde gegevens.

1.10.9 De gegevens kunnen in een leesbaar bestandsformaat in de vorm van een afschrift overgedragen worden (Recht op dataportabiliteit) (artikel 28 lid 3 onder e AVG).

1.10.10 De rechten van betrokkene worden kosteloos door Leverancier uitgevoerd, tenzij de verzoeken kennelijk ongegrond of buitensporig zijn (artikel 12 lid 5 AVG).

1.10.11 Er is een mogelijkheid voor het anonimiseren en pseudonimiseren van gegevens ten behoeve van de ontsluiting van informatieobjecten met persoonsgegevens (artikel 5 lid 1 onder e AVG).

1.10.12 Gegevens worden binnen de Europese Economische Ruimte opgeslagen en daarmee binnen het werkingsgebied van de AVG (artikel 45 AVG)

1.10.13 Indien sprake is van een subverwerker, dan is daar een verwerkersovereenkomsten mee afgesloten (artikel 28 lid 4 AVG).

1.10.14 De beheerorganisatie wordt op de hoogte gesteld wanneer een nieuwe subverwerker wordt ingeschakeld (artikel 28 lid 3 onder d AVG jo 28 lid 2 AVG)

1.10.15 Er is intern beleid bij de leverancier voor het beveiligen van informatie die tenminste voldoet aan de eisen vanuit de Baseline informatiebeveiliging overheid (BIO). Deze is geïmplementeerd en wordt regulier getest (artikel 28 lid 1 jo artikel 28 lid 3 onder c AVG).

1.10.16 De partij kan bij een fysiek of technisch incident de beschikbaarheid van en de toegang tot de persoonsgegevens tijdig (binnen 48 uur) herstellen. (Artikel 28 lid 3 onder c jo artikel 32 AVG).

1.10.17 Er is een procedure voor het op gezette tijdstippen testen, beoordelen en evalueren van de doeltreffendheid van de technische en organisatorische maatregelen ter beveiliging van de verwerking en deze wordt ook uitgevoerd (artikel 28 lid 3 onder c jo artikel 32 AVG).

1.10.18 Testdata moeten geanonimiseerd zijn volgens de richtlijnen van de AVG.

1.10.19 De leverancier waarborgt dat de tot het verwerken van de persoonsgegevens gemachtigde personen zich ertoe hebben verbonden vertrouwelijkheid in acht te nemen door middel van een geheimhoudingsverklaring (artikel 28 lid 3 onder b AVG).

1.10.20 De leverancier waarborgt in de applicatie dat de rechten van betrokkenen, artikelen 15 tot en met 21 van de AVG, effectief en binnen de wettelijke termijn uitgevoerd kunnen worden (artikel 28 lid 3 onder e AVG).

1.10.21 De leverancier heeft een datalekkenprotocol, datalekkenregister en is in staat om de opdrachtgever binnen 24 uur na het ontstaan van een datalek op de hoogte te stellen van de benodigde informatie over het datalek (artikel 28 lid 3 onder f artikel 33 AVG).

1.10.22 De leverancier heeft een Data Protection Impact Assessment (DPIA) uitgevoerd op de applicatie of is in staat om kosteloos bijstand te verlenen aan het uitvoeren van een DPIA (artikel 28 lid 3 onder f, artikel 35 AVG).

1.10.23 De leverancier waarborgt dat de applicatie het vermogen heeft om op permanente basis de vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht te garanderen (artikel 28 lid 3 onder c, artikel 32 lid 1 onder b AVG).

1.10.24 Waar mogelijk wordt als testdata gebruik gemaakt van kunstmatig gegenereerde persoonsgegevens of fictieve data.

1.10.25 De leverancier die actief is buiten de EER of die subverwerkers heeft die actief zijn buiten de EER heeft een Data Transfer Impact Assessment uitgevoerd op de applicatie of is in staat om kosteloos bijstand te verlenen aan het uitvoeren van een Data Transfer Impact Assessment.

1.10.26 De Leverancier zal, behoudens op haar rustende wettelijke (archief)verplichtingen, alle persoonsgegevens na beëindiging van de overeenkomst, per ommegaande kosteloos retourneren aan de Opdrachtgever en, indien de Opdrachtgever daartoe opdracht heeft gegeven, wissen en uit haar systemen (incl. back-up) verwijderen dan wel vernietigen op de wijze als door de Opdrachtgever bepaald. De vernietiging moet, binnen nader overeen te komen termijn, uitgevoerd worden en hiervan wordt een verslag gemaakt.

1.10.27 De Leverancier zal alle subverwerkers die betrokken zijn bij de verwerking van de persoonsgegevens op de hoogte stellen van de beëindiging van de overeenkomst en zal waarborgen dat alle subverwerkers de persoonsgegevens retourneren, verwijderen dan wel (laten) vernietigen, zoals in het vorige lid bepaald.