

Bijlage 7B: PvE-CMS: “Eisen CMS” Rolcontainers AI2022-0068

In deze bijlage beschrijft de Gemeente het Programma van Eisen CMS (PvE-CMS) waar het CMS aan moet voldoen. Dus de minimale randvoorwaarden waaraan het CMS, de Opdrachtnemer en zijn dienstverlening voor het CMS aan moet voldoen.

Definities

API	Application Programming Interface
BI	Business Intelligence van de Gemeente
CMS	ContainerManagementSysteem, het systeem of applicatie gebouwd, geleverd dan wel beschikbaar gesteld door de Opdrachtnemer aan de Gemeente voor het doel waarvoor de Gemeente het wenst te gebruiken en welke voldoet aan de eisen van de Gemeente.
FB	Functioneel Beheer(der)
Gemeente	Gemeente Amsterdam tevens Opdrachtgever en Verwerkingsverantwoordelijke.
Opdrachtnemer	Onderneming aan wie de Gemeente de opdracht heeft gegeven om een CMS beschikbaar te stellen of te bouwen, tevens Verwerker.
RFC	Verzoek tot Wijziging (Request for Change)
Servicedesk	Fysieke helpdesk van Opdrachtnemer (al dan niet ondersteund door een callcenter) waar gebruikers hun problemen en vragen kwijt kunnen.

Eisen ICT Algemeen	
Nr.	Omschrijving
ICT-1	Opdrachtnemer levert een ContainerManagementSysteem (CMS) in de vorm van een SaaS-oplossing. De software dient middels configuratie ingericht te kunnen worden ten behoeve van de Gemeente. Zie ook voor globale schema Bijlage 7B-1.
ICT-2	De SaaS-oplossing is geschikt om volgens de STOSAG-data uit te wisselen.
ICT-3	Met het CMS als SaaS-oplossing moet ten minste dagelijks een actueel beeld van iedere rolcontainer van de Gemeente kunnen worden opgevraagd.
ICT-4	Het dient mogelijk te zijn om vanuit het CMS op ieder gewenst moment data/gegevens op te halen door de Gemeente.
ICT-5	Het dient mogelijk te zijn om via een Application Programming Interface (API) gegevens op te halen. Hiermee kan een automatische onttrekking van decentrale data plaatsvinden.
ICT-6	Opdrachtnemer is verantwoordelijk voor het mogelijk maken van communicatie tussen het CMS enerzijds en de (data)omgeving van de Gemeente anderzijds.
ICT-7	Het uploaden van batches en het doorvoeren van mutaties met betrekking tot de beheerdiensten (uitrolgegevens en onderhoud/defecten oplossen) wordt binnen drie (3) werkdagen door Opdrachtnemer uitgevoerd.
ICT-8	Onderdeel van de opdracht voor het CMS is het verzorgen van upgrades en updates van het CMS gedurende de eerste twee jaar van de looptijd van de Raamovereenkomst, welke daarna kan worden verlengd. Het CMS zal als een nadere opdracht worden uitgevraagd direct na opdrachtverstrekking en moet nadat de nadere opdracht is opgedragen binnen 2 weken functioneel en beschikbaar voor de Gemeente zijn.
ICT-9	Opdrachtnemer conformeert zich aan de Open Standaarden van Forum Standaardisatie voor: • authenticatie, autorisatie en identificatie; • beveiligde, betrouwbare verbindingen; • beveiligde, betrouwbare berichten- en/ of bestandsuitwisseling; • metadatering; • digitale bestandsformaten. Zie: https://www.forumstandaardisatie.nl/
ICT-10	Het CMS biedt de mogelijkheid om minimaal wekelijks gegevens te exporteren in (CSV of XML) richting een kantoorautomatiseringsoplossing van Assetmanagement van de Gemeente.

Eisen Informatiebeveiliging & Privacy	
Nr.	Omschrijving
SEC-1	Opdrachtnemer moet zorgen dat zijn producten en organisatie voldoen aan NCSC-beveiligingsrichtlijnen voor webapplicaties (https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-webapplicaties (of equivalent).
SEC-2	Het CMS moet voldoen aan de meest actuele OWASP-richtlijnen: https://owasp.org/www-project-top-ten/ . Webapplicaties en mobiele apps worden ieder jaar op de laatst bekende versie van de OWASP (top 10) norm getoetst door middel van een veiligheidstest die door een onafhankelijke derde wordt uitgevoerd. Opdrachtnemer levert hiervoor jaarlijks een rapportage of een TPM-verklaring aan van een onafhankelijke derde partij.
SEC-3	Bij koppelingen (in- en uitgaand) biedt het CMS een mechanisme om het datatransport te versleutelen (bijvoorbeeld SSL/TLS).
SEC-4	Toegang tot het CMS via een Internet Browser vindt versleuteld plaats ("https") met TLS1.2 of hoger.
SEC-5	In het kader van de Algemene Verordening Gegevensverwerking (AVG) tekent Opdrachtnemer de Verwerkersovereenkomst van de gemeente Amsterdam.
SEC-6	De data van het CMS wordt gehost in een EER land.

SEC-7	Het is mogelijk dat alle rollen (medewerker, leidinggevende, professional en functioneel beheerder) via een Internetbrowser, zonder additionele plugins of andere software, gebruik kunnen maken van de SaaS-applicatie. De SaaS-applicatie is voor deze rollen een "Zero Footprint" webapplicatie.
SEC-8	Voor authenticatie en autorisatie van het CMS dient gebruik te worden gemaakt van de identity en access voorziening van de Gemeente.
SEC-9	Wachtwoorden moeten zijn samengesteld op basis van de geldende beveiligingseisen (bijv. NIST 800-63) en mogen niet leesbaar worden opgeslagen, maar voorzien zijn van een salt van 32 bits of meer, een gecodeerde HMAC-hash met SHA-1, SHA-2 of SHA-3 en het "stretching" -algoritme PBKDF2 met ten minste 10.000 iteraties.
SEC-10	Een "admin" of "superuser account" is voor exclusief gebruik door Functioneel Beheer van de Gemeente.
SEC-11	Functioneel Beheer van de Gemeente dient, indien nodig, extra rechten (raadplegen, mutatie- en beheerrechten, etc.) aan rollen en profielen te kunnen toewijzen, zodat er verschillende rollen ondersteund kunnen worden.
SEC-12	De gebruiker van het CMS dient zelf het wachtwoord te kunnen wijzigen middels een vastgestelde procedure.
SEC-13	De logging dient alleen toegankelijk te zijn voor daartoe door de Gemeente aangewezen users.
SEC-14	Log bestanden dienen toegankelijk te zijn of moeten aansluiten op de SIEM oplossing van de Gemeente Data logging.
SEC-15	Inlogpogingen moeten beperkt zijn tot slechts 4 foutieve pogingen per keer, met daarna een lockperiode van 5 minuten voordat weer kan worden ingelogd. Dit om bruteforcing te voorkomen.
SEC-16	Uitzonderingen en informatiebeveiligingsgebeurtenissen worden gelogd en minimaal voor drie (3) maanden te worden bewaard. Op aanvraag van de Gemeente worden deze ter beschikking gesteld.
SEC-17	Pen- en Hacktesten. a. Het CMS is in acceptatie fase aan een veiligheidstest onderworpen en bevindingen zijn aantoonbaar verholpen voordat deze in productie gaat; b. Alvorens de toepassing door de Gemeente in gebruik genomen wordt, wordt/is een zogenaamde Pen- en Hacktest uitgevoerd. De uitvoering van de Pen- en Hacktest vindt plaats, of heeft aantoonbaar plaatsgevonden, door een onafhankelijke partij. c. Opdrachtnemer draagt de kosten voor de Pen- en Hacktest; Penetratietests worden procesmatig en procedureel, ondersteund door richtlijnen, uitgevoerd op de infrastructuur van de Opdrachtnemer.
SEC-18	Voor het CMS wordt (logische) netwerksegmentatie toegepast waarbij productie, acceptatie en test omgevingen van elkaar gescheiden worden.
SEC-19	Verkeer tussen de verschillende segmenten in de infrastructuur wordt gefilterd (minimaal op IP) en verkeer wordt alleen toegestaan in overeenstemming met applicatie benodigdheden.
SEC-20	Data van de Gemeente mag niet voor andere dan de beoogde gebruikers beschikbaar komen. In geval van "multi-tenancy" oplossingen mogen API-services en netwerk-services shared zijn, maar dataopslag niet. De data is alleen per tenant toegankelijk en opgeslagen.
SEC-21	In het geval van multi-tenancy; moeten virtuele servers of applicaties geïsoleerd zijn van andere virtuele servers en applicaties van de andere tenants.
SEC-22	Verbindingen tussen cliënt (webbrowser/app) en de (SaaS) server dienen versleuteld (minimaal SSL) plaats te vinden op basis van een Extended Validation SSL certificaat (zowel intern als extern).
SEC-23	Bij systeemkoppelingen (in- en uitgaand) van data met een hogere van integriteit en vertrouwelijkheid vindt er wederzijds systeemauthenticatie plaats door middel van certificaten ("Two Way SSL").
SEC-24	Er is een back-up policy overeengekomen die gebaseerd is op de eisen en wensen van de Gemeente. Back-up media worden conform deze policy opgeslagen en periodiek gecontroleerd op herstelbaarheid.
SEC-25	Opdrachtnemer heeft een actief patchbeleid, procesmatig en procedureel, ondersteund door richtlijnen, zodanig uitgevoerd dat laatste (beveiligings)patches conform de aanwijzingen van de fabrikant van de software zijn geïnstalleerd in de ICT-voorzieningen van de Opdrachtnemer.
SEC-26	Opdrachtnemer moet proactief en onmiddellijk beveiligingsincidenten/datalekken melden aan de Gemeente.
SEC-27	Opdrachtnemer heeft een protocol om cyberaanvallen te weren of de eventueel geleden schade op een gestructureerde en adequate manier op te lossen.
SEC-28	Malafide code detectie (anti-virus) is actief op de infrastructuur van de Opdrachtnemer.

Eisen Rapportages	
Nr.	Omschrijving
RAP-1	Opdrachtnemer stelt online rapportages ter beschikking waarop beschikbaarheid, storingen, gebruik, en, indien van toepassing, vullingsgraad te zien zijn.
RAP-2	De rapportages hebben een exportfunctie in ieder geval csv formaat, opdat de Gemeente zelf deze gegevens kan beschikken en in kan lezen in een eigen rapportagetool.

Eisen Functioneel Beheer Gemeente		
Nr.	Categorie	Omschrijving
RR1	Rollen en rechten	Het CMS logt welke gebruiker op welk tijdstip welke handeling uitvoert zodat een audit trail gemaakt kan worden. Functioneel Beheerder kan dit logbestand binnen het CMS lezen. Van de logbestanden kunnen rapportages worden gemaakt. De eisen die de Gemeente stelt aan de logbestanden zijn: • Ze moeten leesbaar zijn; • Ze zijn voorzien van een timestamp; • Ze zijn herleidbaar tot een natuurlijke persoon of indien van toepassing tot een proces en/of handeling; • Ze mogen niet muteerbaar zijn; • Ze mogen de performance van het CMS niet belemmeren.
RR2	Rollen en rechten	Het CMS is functioneel schaalbaar voor wat betreft: • Rol/minicontainers (binnen alle bestaande kenmerken zoals formaat, kleur, uitvoering, type, toebehoren, adresgegevens, maar ook het toevoegen en uitbreiden van nieuwe kenmerken); • gebruikers van de Gemeente; • gebruikersgroepen van de Gemeente; • rollen van gebruikers van de Gemeente.
RR3	Rollen en rechten	Het (web)applicatie- en Functioneel Beheer is procesmatig en procedureel ingericht, waarbij geautoriseerde beheerders op basis van functieprofielen taken verrichten.
RR4	Rollen en rechten	De Functioneel Beheerder dient binnen het CMS rollen kunnen definiëren op basis van functieprofielen.
RR5	Rollen en rechten	De te distribueren toegangsrechten moeten per rol, groep of per (individuele) gebruiker configureerbaar zijn.
RR6	Rollen en rechten	De Functioneel Beheerder kan binnen het CMS één (1) of meerdere rollen (maximaal alle beschikbare rollen) aan een account koppelen.
RR7	Rollen en rechten	De Functioneel Beheerder kan binnen het CMS gebruikersaccounts aanmaken, wijzigen, deactiveren, activeren en verwijderen.
RR8	Rollen en rechten	Het is mogelijk geldigheidsdatum in te stellen per account bij het aanmaken van een account.
FB1	FB	De inrichting van het CMS (processen, menu's, autorisaties e.d.) wordt in overleg met de Functioneel Beheerder bij de Gemeente bepaald en uitgevoerd.
FB2	FB	Van uitgegeven autorisaties aan gebruikers kunnen op eenvoudige wijze door Functioneel Beheerder rapportages/selecties gemaakt en geëxporteerd worden.
FB3	FB	Het CMS beschikt over functionaliteit om beheer activiteiten uit te voeren door Functioneel Beheerder, zonder tussenkomst van de Opdrachtnemer, zoals het kunnen opstarten en monitoren van batches.
FB4	FB	Opdrachtnemer stelt bij bekende 'bugs' bijbehorende workarounds beschikbaar.
FB5	FB	Het CMS is flexibel van opzet, wordt gedurende de looptijd van de Overeenkomst verder door ontwikkeld en verbeterd en houdt gelijke tred met wijzigingen in standaarden en wijzigingen in wet- en regelgeving om de functionaliteit van het CMS te waarborgen.
FB6	FB	Minimaal een kwartaal vooruit wordt inzicht gegeven in geplande releases (met releasenotes), Life Cycle Management (LCM)-trajecten, upgrades en vergelijkbare changes.
FB7	FB	Opdrachtnemer is verantwoordelijk voor het gecontroleerd doorvoeren van wijzigingen (Changes), de Opdrachtnemer richt een changemanagementproces in.
FB8	FB	Binnen het changeproces worden RFC's onderkend die geïnitieerd kunnen worden door de Opdrachtnemer en/of de Gemeente, waarbij de wijzigingen niet worden uitgeleverd als maatwerk, maar als standaard functionaliteit.
FB9	FB	Opdrachtnemer voert alleen gepland onderhoud uit in het Maintenance Window en stelt de Gemeente daarop op de hoogte. Opdrachtnemer stuurt een risico analyse van gepland onderhoud aan de Gemeente en na akkoord door de Gemeente kan het onderhoud worden uitgevoerd.
FB10	FB	Opdrachtnemer zal regelmatig software updates uitvoeren. Met deze updates worden bekende fouten in de software hersteld of kleine verbeteringen in de functionaliteiten doorgevoerd. Opdrachtnemer zal de Gemeente hierover voortijdig informeren. Opdrachtnemer zal updates en upgrades doorvoeren op de server. Opdrachtnemer zal de Gemeente op de hoogte brengen als een update of upgrade is uitgevoerd en meldt daarbij welke verbeteringen of veranderingen zijn doorgevoerd in de software.
DM1	DM	Functioneel beheerder kan stamgegevens invoeren, wijzigen en verwijderen zonder tussenkomst van de Opdrachtnemer.
DM2	DM	Functioneel beheerder kan keuzelijsten aanmaken, wijzigen en verwijderen.
DM3	DM	Functioneel beheerder kan, d.m.v. importfunctie in het CMS, stamgegevens importeren in stamtabellen. Voorwaarde is dat data-integriteit gewaarborgd wordt d.m.v. unique-key te hanteren bij import-script.
DM4	DM	Functioneel beheerder kan alle stamdata en keuzelijsten exporteren.
DM5	DM	Het CMS heeft een gegevensservice of API voor de import en export van data. Data worden ontsloten via een gegevensservice of API die voor eenieder die door de Gemeente geautoriseerd is, beschikbaar zijn
DM6	DM	Opdrachtnemer stelt acceptatieomgeving beschikbaar en het is bedoeld onder andere voor het testen van nieuwe functionaliteiten. De Gemeente is de eigenaar van deze omgeving. Opdrachtnemer heeft eigen ontwikkel- en testomgeving.

DM7	DM	Functioneel beheer heeft toegang tot de database in de acceptatieomgeving.
DM8	DM	Functioneel beheerder kan data in de acceptatieomgeving verversen vanuit de productieomgeving d.m.v. een opdracht-button binnen de applicatie.
DOC1	Docu-mentatie	Zie voor bepalingen omtrent documentatie ten aanzien van het Onderhoud en het gebruik van het CMS artikel 11 van de "Gemeentelijke Inkoopvoorwaarden bij IT" (GIBIT) van de Gemeente.
DOC2	Docu-mentatie	Het CMS en alle documentatie - voor zowel gebruikers als beheerders - zijn volledig Nederlandstalig en bevatten ten minste: • juiste en volledige beschrijving van het geleverde en de functies daarvan; • de datastructuur: entiteiten, entiteit relaties en attributen op een dusdanige wijze beschreven dat de FB en BI van de Gemeente zelf middels opvraagmogelijkheden rapportages kan samenstellen.
DOC3	Docu-mentatie	Gedurende de looptijd van deze Overeenkomst zal Opdrachtnemer ervoor zorg dragen dat de door haar geleverde gebruikers- en beheerders handleidingen, documentatie in de aanpassingen van de applicatie- en data-architectuur zo spoedig mogelijk op haar kosten zal worden vervangen, gewijzigd of aangepast.
SLA1	SLA	Opdrachtnemer zorgt ervoor dat de gewenste dienstverlening, op het vlak van Hosting en technisch beheer van het CMS in een SLA wordt vastgelegd. De SLA wordt met de inschrijving aangeleverd.
SLA2	SLA	Voor het verhelpen van storingen en het beantwoorden van vragen met betrekking tot het CMS heeft de Opdrachtnemer een Servicedesk ingericht, beschikbaar van 7.30 tot 18.30 uur.
SLA3	SLA	Opdrachtnemer draagt zorg voor het beantwoorden van gebruikersvragen via de Servicedesk. De gebruikersvragen aan de Servicedesk worden gesteld door de functionele en applicatiebeheerders van de Gemeente.
SLA4	SLA	Opdrachtnemer ondersteunt de volgende service support processen: • Incident management; • Problem management; • Change management; • Configuratie management.
SLA5	SLA	Opdrachtnemer maakt gebruik van een web-based applicatie voor het proces van incidenten/meldingen. Het CMS is toegankelijk voor de applicatie- en functioneel beheerders bij de Gemeente. Met het CMS zijn zowel door de Opdrachtnemer als de Gemeente rapportages te maken.
SLA6	SLA	Opdrachtnemer levert aan de Functioneel beheerder van de Gemeente een beschrijving van de eigen testprocedure van updates, upgrades en patches en geeft input voor de daaropvolgende gebruikerstests (maakt deel uit van de SLA) in een testomgeving.
SLA7	SLA	In de SLA worden nadere afspraken gemaakt over de afhandeling van supportaanvragen. De SLA dient voor ondertekening van de overeenkomst klaar te zijn.
SLA8	SLA	Opdrachtnemer monitort voortdurend de beschikbaarheid en neemt proactief maatregelen op het moment dat de beschikbaarheid onder de dreigt te komen.
SLA9	SLA	Opdrachtnemer verricht EDP audits en technische penetratietest en overhandigt de resultaten aan de Gemeente.
SLA10	SLA	Bij update door de Opdrachtnemer van (delen van) het CMS de continuïteit van gerealiseerde koppelingen en koppelvlakken gewaarborgd.

Eisen Beheer	
Nr.	Omschrijving
BEH-1	Opdrachtnemer stelt bij bekende 'bugs' bijbehorende workarounds beschikbaar aan Gemeente.
BEH-2	In geval van contact met technisch applicatiebeheer en de Gemeente is de voertaal Nederlands.
BEH-3	De Gemeente krijgt bij een fout in het CMS een duidelijke instructie in gebruikerstaal hoe deze fout op te lossen.
BEH-4	De Gemeente wordt actief geïnformeerd bij systeemfouten middels e-mailnotificatie of andere actieve foutenlog.
BEH-5	Het servicewindow is op maandag t/m vrijdag van 07.30 - 18.30 uur. Uitzondering hierop vormen de officiële nationale feestdagen zoals bepaald door de Rijksoverheid. Tijdens dit servicewindow dienen medewerkers van Opdrachtnemer telefonisch bereikbaar te zijn. Gedurende 24 x 7 dient het mogelijk te zijn om de servicedesk te e-mailen.
BEH-6	De Service Desk voert uitsluitend de Nederlandse taal.
BEH-7	Incidenten worden voorzien van een prioriteit: 1. Incidenten die leiden tot volledige uitval van één of meer bedrijfskritische procesonderdelen. Deze Incidenten komen in de Service Management rapportage tot uiting in een verlaagd beschikbaarheid percentage. 2. Incidenten die ernstig impact hebben op de dienstverlening en die leiden tot een uitval of verminderde dienstverlening voor een groot deel van de gebruikers. 3. Incidenten die een beperkte impact hebben, die slechts voor enkele gebruikers merkbaar zijn, uitval van niet-bedrijf kritische applicatie.
BEH-8	Als incidenten/meldingen niet adequaat worden opgevolgd wordt geëscaleerd conform door de Gemeente en de Opdrachtnemer ingerichte escalatieprocedure op 3 niveaus (Strategisch/Tactisch/ Operationeel).
BEH-9	Opdrachtnemer stelt een contactpersoon aan die aangesproken kan worden over de voortgang c.q. afhandeling van een incident of melding.
BEH-10	Bij iedere change levert de Opdrachtnemer releasedocumentatie en is verantwoordelijk voor het uitvoeren van de technische test. De Gemeente is verantwoordelijk voor de acceptatietest.

BEH-11	Opdrachtnemer voert alleen gepland onderhoud uit in het onderhoudswindow (vastgelegd in de SLA) en stelt de Gemeente daarvan op de hoogte. Opdrachtnemer stuurt een risicoanalyse van gepland onderhoud aan Gemeente en na akkoord de Gemeente kan het onderhoud worden uitgevoerd.
BEH-12	Opdrachtnemer is verantwoordelijk voor het opstellen van een Exit Plan na het beëindigen van de overeenkomst.
BEH-13	Opdrachtnemer dient een Service Level Agreement (SLA) aan te leveren en dient afspraken met prestatie-indicatoren ten aanzien van de volgende onderwerpen ter accordering voor te leggen aan de Gemeente: • Bereikbaarheid; • Beschikbaarheid; • Incidentmanagement; • Securitymanagement; • Change management; • Releasemanagement; • Servicereportages; • Servicegesprekken. Opdrachtnemer is verantwoordelijk voor het actueel houden van de SLA en dient wijzigingen ter accordering voor te leggen aan de Gemeente.
BEH-14	Opdrachtnemer is verantwoordelijk voor het nader uitwerken en bijhouden van afspraken in: 1. DAP (Dossier Afspraken en Procedures): procedures met de Opdrachtnemer; 2. DFA (Dossier Financiële Afspraken): financiële afspraken. Deze documenten dienen vervolgens ter accordering te worden voorgelegd aan de Gemeente.

Eisen Informatiebeheer	
Nr.	Omschrijving
IB-1	Het CMS moet functionaliteit bevatten die de Gemeente in staat stelt om de gewenste dan wel wettelijke bewaartermijnen te handhaven: 1. Er moet een bewaartermijn kunnen worden ingericht op basis van een geïdentificeerd werkproces en er moeten metadata over de bewaartermijn en einddatum van het proces kunnen worden toegevoegd. 2. Van informatieobjecten die voor vernietiging in aanmerking komen, moeten op basis van het jaar van vernietiging overzichten kunnen worden gecreëerd. 3. Informatieobjecten en bijbehorende metadata moeten onherstelbaar kunnen worden vernietigd op basis van de als zoekcriteria (metadata) opgegeven waardering/vernietigingstermijn. 4. Van de vernietiging moet een verklaring worden opgeleverd waarin minimaal wordt aangegeven om welke informatie het gaat, dat de vernietiging volledig is uitgevoerd en om hoeveel data het gaat (TB, MB, etc.) 5. Opdrachtnemer garandeert dat bij een back-up-recovery geen gegevens terug in productie worden gezet die formeel al vernietigd zijn.
IB-2	Het moet mogelijk zijn om een export te maken van bestanden en bijbehorende metadata op basis van opgegeven zoekcriteria, ten behoeve van bijvoorbeeld overdracht naar een andere omgeving, zoals bij het einde van de overeenkomst. De onderlinge samenhang tussen gegevens, indien van toepassing, kan worden blijven gelegd (bijv.: metadata en bestanden, relationele database) om informatieverlies te voorkomen.

Eisen Privacy	
Nr.	Omschrijving
Priv-1	Opdrachtnemer is ISO 27001 gecertificeerd of gelijkwaardig en toont dit, door middel van een TPM verklaring aan ten aanzien van: a. Verwerker is ISO 27001 (of gelijkwaardig) gecertificeerd; b. Verwerker toont zelf aan dat hij aan de eisen uit de Baseline Informatiebeveiliging Overheid (BIO) voldoet (door een GAP analyse inclusief overzicht van genomen maatregelen); c. Verwerker levert eenmalig bij gunningen jaarlijks een audit of TPM: een ISAE 3402 type 2 rapport, waarmee een onafhankelijke externe auditor rapporteert over de opzet, bestaan en werking van beheersmaatregelen; d. Verwerkingsverantwoordelijke ontvangt jaarlijks dit rapport en heeft een right-to audit om eventueel aanvullend te toetsen; De Verwerker hanteert een integriteitscode dan wel een interne gedragscode voor zijn medewerkers waaruit blijkt dat de medewerkers en door de Verwerker ingeschakelde derden de vertrouwelijkheid in acht nemen. (artikel 28 lid 3 AVG: Verwerker moet bewijsbaar integere medewerkers in dienst hebben), afgedekt met getekende geheimhoudingsovereenkomst. Verwerker levert persoonlijke VOG aan voor betrokken medewerkers die activiteiten uitvoeren.

Eisen Data	
Nr.	Omschrijving
Dat-1	Data Eisen De Gemeente is bronhouder van alle data die door of in opdracht van de Gemeente worden verzameld. De Gemeente heeft daarmee de verantwoordelijkheid om zich ervan te vergewissen dat zulke data op een juiste manier worden verwerkt. Van de Opdrachtnemer wordt gevraagd om niet alleen bij aanbesteding, maar ook daarna periodiek of op aanvraag: • Aan te tonen op welke wijze wordt voldaan aan de eisen die door wet- en regelgeving aan de dataverwerking worden gesteld (o.a. AVG en informatiebeveiliging). • Inzicht te geven in: ○ gebruikte bronnen, transformatiemodel, datamodel en semantiek; ○ toegepaste internationale en landelijke standaarden; ○ de wijze van ontsluiting conform de data architectuur van de Gemeente (zie Dat-2. Data Architectuur); ○ de wijze van kwaliteitsborging (zie Dat-4. Datakwaliteit); ○ de wijze waarop historie is vastgelegd (zie Dat-3. Technische Historie); ○ de inrichting van het beheer conform het vastgestelde incident -en changemanagement proces. • Daar waar relevant actuele documentatie op te leveren op bovengenoemde onderwerpen, in ieder geval voor de gebruikte bronnen, transformatiemodel, datamodel en semantiek en de benodigde handleidingen voor dataverwerking.
Dat-2	Data Architectuur De datastrategie van de Gemeente richt zich op de ontwikkeling van een datafundament, dat bestaat uit datasets die zich in onderlinge samenhang verhouden als herbruikbare bouwstenen. Deze data laag is onafhankelijk van specifieke applicaties en toepassingen. Met dit doel voor ogen worden applicatie-applicatiekoppelingen zoveel mogelijk vermeden. In plaats daarvan worden data uit applicaties onttrokken en voor het beoogd hergebruik beschikbaar gesteld in het gemeentelijk dataplatform. Tegen deze achtergrond: • Opdrachtnemer die in opdracht van de Gemeente data verzamelt of produceert, is verplicht om alle data in 'ruwe' vorm beschikbaar te stellen aan de Gemeente. Dit gebeurt in een geautomatiseerd proces en standaardformaat, bij voorkeur Rest API of gangbare uitwisselingsformaat. • Opdrachtnemer voorziet de datalevering van actuele informatie over het toegepaste datamodel, het transformatiemodel en semantiek. • Wanneer Opdrachtnemer data nodig heeft die op het gemeentelijk dataplatform beschikbaar is, moet gebruik gemaakt van die voorziening - en niet van een andere. Er worden geen directe koppelingen tussen applicaties gemaakt. Als data pas later beschikbaar komt in het gemeentelijk dataplatform, gaat Opdrachtnemer binnen maximaal één half jaar over naar de nieuwe situatie.
Dat-3	Technische Historie De technische historie van wijzigingen wordt standaard bijgehouden dat als een dataset in het dataplatform wordt ontsloten. Als door de bronhouder is aangegeven dat de inhoudelijke historie moet worden vastgelegd, dan gebeurt dat in de brondataset. <i>Ter illustratie: een straatnaamwijziging wordt doorgevoerd in de BAG. De technische wijzigingen zijn 'beëindiging oude straatnaam' en 'aanmaak nieuwe straatnaam'. De logische historie legt de relatie tussen 'het oude' en 'het nieuwe adres'.</i> Als de inhoudelijke historie dient te worden vastgelegd in de bron, dan dient dit te zijn opgenomen in de functionele data requirements.
Dat-4	Datakwaliteit Het datamodel, de inrichting van de database en validatie van nieuwe of gewijzigde data dienen maximaal de kwaliteit van de opgeslagen data te waarborgen. Om dit te realiseren gelden de volgende uitgangspunten: • Geen of zo weinig mogelijk vrije invoervelden gebruiken; daar waar mogelijk dient bij het wijzigen/-invoeren van data gebruikt gemaakt te worden van gecontroleerde referentie-/domeinwaarden; het inhoudelijk beheer van de domeintabellen ligt bij de bronhouder. • Bij invoer dient validatie op constraints uitgevoerd te worden, waarbij foutenafhandeling helder en begrijpelijk wordt uitgevoerd ten behoeve van de gegevensbeheerder. • Als additionele datakwaliteitsregels (business rules) door de bronhouder worden bepaald dan dient hier ook op gevalideerd te worden bij het wijzigen/invoeren van data. • Als gegevens uit een basis- of een kernregistratie worden gebruikt, dan dient ten alle tijde verplicht gebruik gemaakt te worden van de betreffende basis- of kernregistratie (al dan niet via het Dataplatform) en de relatie met de gebruikte entiteiten vastgelegd te worden. Let op: bij het definiëren van de functionele data requirements dienen ook de business rules vastgesteld te worden.

Eisen Productstandaarden per domein & Technische aansluitstandaarden

1. Inleiding en Achtergrond

Dit document behartigt de volgende belangen:

- **Vroegtijdige informatievoorziening aan de eigen en de klant organisatie.**
Door vroegtijdig informatie te geven omtrent landingsplatformen en koppel mogelijkheden kan beter worden geborgd dat projecten al tijdens de verkenning de belangen van de rve ICT meenemen.
- **Vermindering noodzaak voor overleggen omtrent technische 'FIT' van applicaties en services.**
Het aantal mensen dat kan aansluiten bij overleggen in de verkenningsfase is beperkt. Door standaarden te definiëren en aan te leveren kan de inzet van deze beperkte groep beter worden gekanaliseerd richting werkelijk complexe inrichtingsvraagstukken
- **Vergroten toegankelijkheid en inzicht in technische standaarden en de vernieuwing hiervan.**
Om de informatie omtrent standaarden laagdrempelig te kunnen leveren is een a4 document opgesteld. Dit document beslaat de domeinen Technisch Applicatiebeheer, Hosting, Werkruimten en User Access Services. Dit document wordt onder regie van architectuur centraal beschikbaar gesteld en aan eenieder aangeboden die hier behoefte aan heeft.
- **Standaardisatie van en regie op het vernieuwingsproces.**
Vernieuwing en verandering van dit document wordt uitgevoerd onder regie van de lead architect door solution architecten binnen de rve-ICT. Het document wordt goedgekeurd door het Architectuur Overleg Operations. Updates en lifecycles worden goedgekeurd door de LCM-Stuurgroep. Uitbreiding van het landschap wordt vastgesteld door het Managementteam.
- **Standaardisatie van het technologie landschap in het kader van operational excellence.**
De rve-ICT biedt een beperkte variatie in haar dienstverlening. Dit document helpt om deze beperking zichtbaar en inzichtelijk te maken en te houden.

De standaarden zijn technisch van aard en daardoor niet voor iedereen goed te lezen c.q. interpreteren. Bij vragen kan altijd contact worden gezocht met de rve-ICT in het algemeen en de lead architect in het bijzonder.

1.1 Leeswijzer

De productstandaarden zijn verdeeld in Productstandaarden en aansluitvoorwaarden.

De productstandaarden betreffen technische platform standaarden voor front-end en backend landingsplatformen. Hierbij wordt het volgende onderscheid gemaakt:

- **N-Variant:** Het huidige standaard platform. Hierop wordt iedere applicatie geacht te landen wil het vanuit de datacenters van de rve-ICT worden aangeboden.
- **N-1-Variant:** De standaard van gisteren. Hierop kan in uitzonderingssituatie nog nieuwe dienstverlening worden geïmplementeerd. Deze dienstverlening binnen afzienbare tijd te worden vernieuwd zodanig dat deze kan landen op de N standaard.

De aansluitstandaarden hebben betrekking op dienstverlening die vanuit een Cloud of SaaS propositie wordt aangeboden en beschrijven bonding hoe kan worden aangesloten op dienstverlening geleverd door de rve-ICT.

2. Productstandaarden per domein

2.1. Vigerende klantplatformen: Back-End

Platform	N	N-1
Windows applicatieserver	MS Windows Server 2019 Standard IIS 10.0 Java VM 8 .NET Framework 3.5 t/m 4.6	MS Windows server 2016 Standard IIS 8.5 Java VM 8 .NET framework 3.5 t/m 4.5
Windows database server	MS Windows Server 2019 Standard MS SQL Server 2019 RDBMS	MS Windows server 2016 Standard MS SQL server 2017 RDBMS
JEP applicatieserver	RHEL 7.X ¹ Weblogic 12.2 Ansible OSB 12.2	RHEL 6.5 Puppet 3.8 Weblogic 10.3.6 (11g) XL Deploy OSB 10.3.6 (11g)
JEP database server	RHEL 7.X ¹ Oracle RDBMS 19c Ansible	RHEL 6.5 Oracle RDBMS 12.2
Linux applicatieserver	RHEL 7.X ¹ Weblogic 12.2 Ansible	RHEL 6.5 Weblogic 10.3.6 (11g) Ansible
Linux webserver	RHEL 7.X ¹ NginX 1.13.0 Ansible	RHEL 6.5 Apache 2.4
Oracle database server	RHEL 7.X ¹ Oracle RDBMS 19.2 Ansible	RHEL 6.5 Oracle RDBMS 11.2
PostgreSQL database platform	RHEL 7.X ¹ PostgreSQL 10.6	RHEL 7.X ¹ PostgreSQL 9.6

2.2. Vigerende klantplatformen: Front-End

Platform	N	N-1
Windows Workspace ADW	XenDesktop 1912 LTSR Shared Windows 2016 Citrix Workspace App 1904.1 Ivanti WS Control 10.3 App-V 5.1	Niet van toepassing
ADW Desktop	Windows 10 Build 1909 Citrix Workspace App 1904.1 Ivanti WS Control 10.3 App-V 5.1	Niet van toepassing
ADW Taakgerichte werkplek	Windows 10 Build 1909 Citrix Workspace App 1904.1 Ivanti WS Control 10.3 App-V 5.1	Niet van toepassing

2.3. Vigerende protocollen

Platform	LAN protocollen	WAN protocollen
File uitwisseling	Sftp Ftps https ftp (I&V <2) http (I&V <2) SMB2 (Client Server) SMB2+ (Server Server) SMB3 (Encrypted) (Server Server)	Sftp Ftps https
Data uitwisseling	REST (over https) SOAP(over https) ODBC (SSL bij IV>1) SQLNet (Encrypted bij IV>1)	REST (over https) SOAP(over https)
Authenticatie protocollen	SAML 2.0 (over https) Kerberos LDAPs OAUTH 2.0	SAML 2.0 (over https) OAUTH 2.0

• ¹ Minor versie wordt maandelijks verhoogd in lijn met RHEL updatebeleid
Programma van Eisen ContainerManagementSysteem AI2022-0068

3. Aansluitvoorwaarden

3.1. Web toepassingen

- Verkeer encrypted middels TLS 1.2 over http (https);
- Compatible met Internet Explorer 11. of Google Chrome;
- Geen applicatiespecifieke plugins;
- Compatible met office 2013 / 2016;
- Geen interactie met overige applicaties binnen de gemeentelijke infrastructuur behalve wanneer deze internet enabled API's hanteren. (geen backchannel communicatie);
- Authenticatie op basis van WAN-authenticatie protocollen (op basis van Post/Post);
- User provisioning op basis van SOAP/ REST via Amsterdams Dataknooppunt / Access Manager;
- Burger authenticatie via DigiD;
- Ketenauthenticatie via eHerkenning.

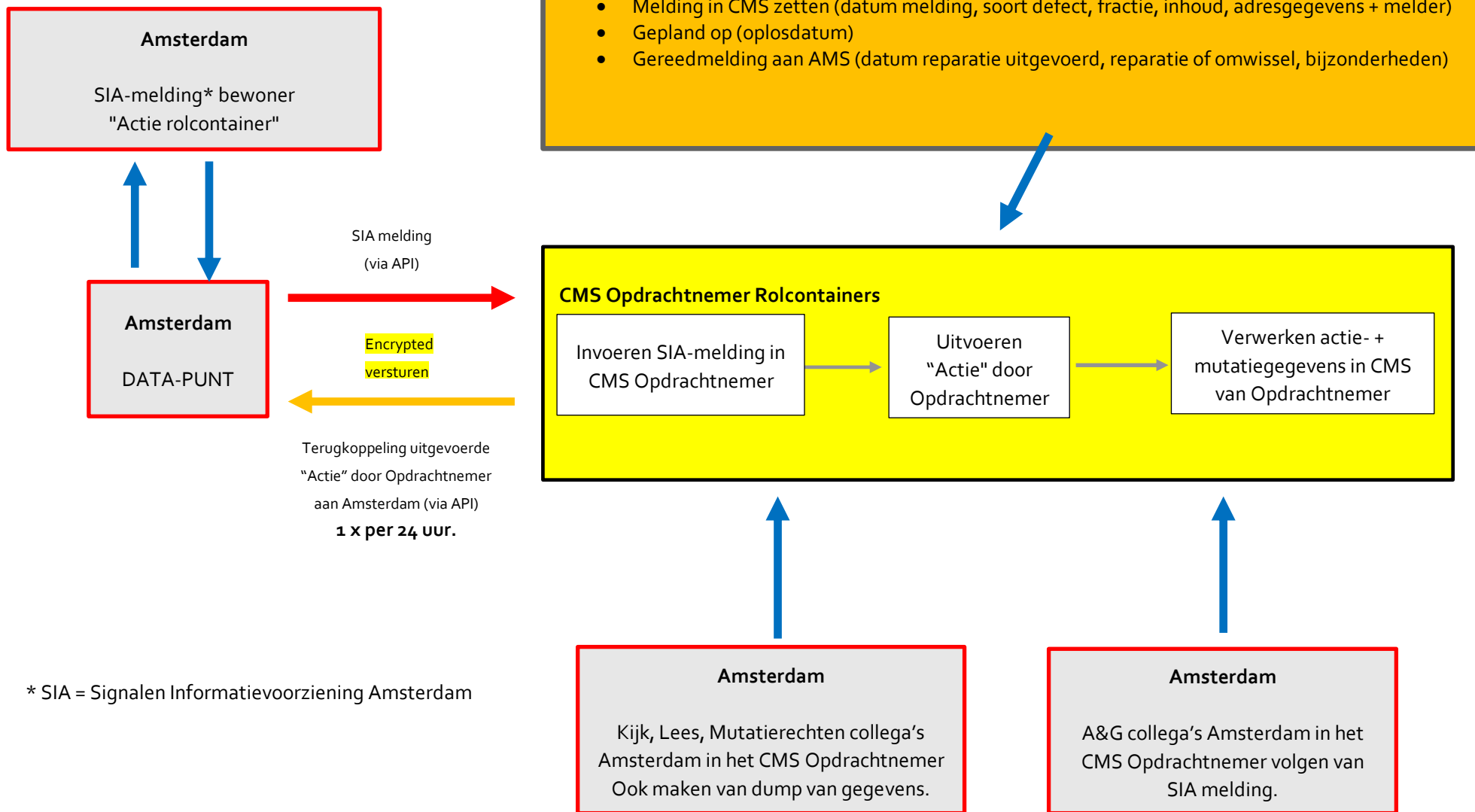
3.2. API gebaseerde client applicaties

- Verkeer encrypted middels TLS1.2 over http via poort 443 (https);
- Connectie op basis van internet routable DNS;
- API's zijn gebaseerd op POX, REST of SOAP;
- Geen applicatiespecifieke plugins;
- Geen interactie met overige applicaties binnen de gemeentelijke infrastructuur behalve wanneer deze internet enabled API's hanteren (geen backchannel communicatie);
- Alle output, exports, of gecreëerde bestanden via de frontend benaderbaar. Geen shares of bestandsservices die rechtstreeks moeten worden benaderd (behalve via daarvoor geschikte API's);
- Printing via de Amsterdamse workspace en/of via IPPS;
- Compatible met office 2013 / 2016;
- Authenticatie op basis van WAN-authenticatie protocollen;
- Geen generieke user authenticatie;
- User provisioning op basis van SOAP/ REST via Amsterdams Dataknooppunt / Access Manager;
- Geen interactie met overige applicaties binnen de gemeentelijke infrastructuur behalve wanneer deze API's hanteren die hiervoor geschikt zijn (geen backchannel communicatie);
- Burger authenticatie via DigiD;
- Ketenauthenticatie via eHerkenning.

3.3. SBC-oplossingen (worden slechts in uitzonderingssituaties geaccepteerd – ter beoordeling aan een projectarchitect)

- Uitsluitend ondersteuning voor ICA en RDP-verkeer via HTTPs;
- Ontsluiting middels een portaal (geen losse RDP/ ICA files of lokale client configuraties);
- Federatieve authenticatie op basis van WAN-authenticatie protocollen;
- Compatible met de laatste client (RDP of ICA) release en loopt nooit meer dan 1 client (RDP of ICA) release achter;
- Uitsluitend via de Amsterdamse Digitale Werkrumte aangeboden;
- Geen forwarding van lokale printers;
- Geen forwarding van lokale disks of netwerk disks;
- Data-uitwisseling richting gebruikers via de Amsterdamse Clouddrive (o.b.v Citrix ShareFile) of een vergelijkbare service van de Opdrachtnemer;
- Data uitwisseling richting backend systemen via de Amsterdamse brievenbus (o.b.v. Serv-U MFT server) via FTPs, HTTPs of een vergelijkbare service van de Opdrachtnemer.

Bijlage 7B-1 Schema CMS SIA-melding



* SIA = Signalen Informatievoorziening Amsterdam