Aansluitprincipes, standaarden en uitgangspunten

Architectuurplatform gemeente Midden-Drenthe

Project Sociaal Verbonden

Inhoudsopgave

1. Inleiding

Voor de vervanging van een aantal applicaties voor het sociaal domein van de gemeente Midden-Drenthe (GMD) gelden een aantal standaarden, principes en uitgangspunten. Hierbij is geput uit de referentiearchitecturen zoals de NORA en de GEMMA.
Binnen dit project is een selectie gemaakt van de meest toepasselijke relevante architectuurprincipes en richtlijnen van deze referentiearchitecturen. Aangevuld met de specifieke gemeente Midden-Drenthe principes, standaarden en uitgangspunten.

Binnen de scope van het project wordt ervan uitgegaan dat de standaarden, principes en richtlijnen van toepassing moeten zijn voor de gevraagde oplossing.

1.1 Aansluitprincipes gemeente Midden-Drenthe

De onderstaande aansluitprincipes zijn van toepassing bij het leggen van integraties tussen applicaties. Hierin maken we onderscheid tussen directe point-2-point koppelingen, koppelingen waarbij het gaat om basisregistraties en echte maatwerkkoppelingen.

GEMMA / NORA / GMD	**Principe**	**Implicaties**
GMD_INT001	Point-2-Point / Off-the-shelf integraties zijn de voorkeursmanier om applicaties te koppelen.	Point-2-Point/ Off-the-shelf integraties tussen applicaties houdt in dat applicaties naadloos native met elkaar communiceren en gegevens uitwisselen zonder dat er complexe en op maat gemaakte integraties vereist zijn. Het doel is om de ontwikkeling en implementatie van nieuwe systemen te versnellen en de afhankelijkheid van op maat gemaakte integraties te verminderen.
GMD_INT002	Uitwisseling van gegevens gebeurt, indien beschikbaar, op basis van open standaarden.	Uitwisseling van gegevens geschiedt via gestandaardiseerd berichtenverkeer op basis van open standaarden. Daar waar er geen open standaarden zijn, of waar ze conflicteren, wordt een keuze gemaakt die zoveel mogelijk duurzaam en herbruikbaar is binnen het huidige en toekomstige landschap.
GMD_INT003	Voor gebruik van basis- en kerngegevens moet gebruik worden gemaakt van de beschikbare basis- en kernregistraties.	Gegevens worden bij de bron ontsloten.
GMD_INT004	Applicaties die gebruik maken van gegevens vanuit de Basisregistraties koppelen via de Makelaarsuite (MKS) van de gemeente Midden-Drenthe.	MKS is bedoeld is om de basis- en kernregistraties te ontsluiten. Andere applicaties krijgen via een koppeling met deze Enterprise Service Bus toegang tot de gegevens. Gemeente Midden-Drenthe kan gegevens leveren vanuit de volgende basisregistraties: - BRP, BAG, BRK, GBA-V/BRP, BGT-gegevens Bron: Makelaarsuite | GEMMA Softwarecatalogus

GMD_INT005	Voor maatwerk integraties tussen applicaties wordt gebruikt gemaakt van de ESB.	Bij maatwerk integraties tussen applicaties wordt gebruik gemaakt van een ESB (Enterprise Service Bus). De ESB fungeert als een centraal systeem die de communicatie en integratie tussen verschillende applicaties faciliteert, waardoor gegevensuitwisseling efficiënt en gestandaardiseerd plaatsvindt. Deze ESB is in staat om mappingen en transformaties van berichten uit te voeren. ESB is bij de gemeente Midden-Drenthe de MakelaarSuite in beheer bij een externe partner van de gemeente Midden-Drenthe.

1.2 Richtlijnen gemeente Midden-Drenthe

Onderstaande richtlijnen zijn van toepassing bij de gemeente Midden-Drenthe, deze zijn aanvullend en soms overlappend met de gestelde eisen en wensen vanuit een programma van eisen.

Vanuit deze aansluitvoorwaarden, standaarden en uitgangspunten hechten we in het bijzonder waarde aan de volgende richtlijnen, hier willen we als gemeente ons ook aan houden.

R-NR	Richtlijnen	Toelichting	ARCHITECTUUR LAAG
1	In alle ICT-oplossingen is voor de data een exit-strategie opgenomen, en hierbij wordt specifiek aandacht besteed aan de archiefbescheiden. Alle data moet bij het stopzetten van een contract met een opdrachtnemer of applicatie worden geëxtraheerd op zodanige wijze dat deze bruikbaar is op basis van de geldende archiefnormen. Deze informatieobjecten worden daarna overgebracht naar een andere archiefruimte of nieuw te selecteren partner en applicatie(s).	Voor SaaS geldt dat bij een exit, de informatie kosteloos uit het systeem moet kunnen worden gehaald en inclusief het informatiemodel via een standaard, leesbaar en logisch bestandsformaat wordt opgeleverd aan de GMD.	Informatielaag
2	Bij beëindiging van de overeenkomst verwijdert de opdrachtnemer alle data binnen een overeengekomen termijn (maximaal 30 dagen), en levert hiervan een gewiste-data-verklaring aan	End of Life (EOL) / End of Sale (EOS).	Informatielaag
3	Voor het inloggen in het informatiesysteem en het beheer van gebruikersnaam/ wachtwoord wordt gebruik gemaakt van Entra ID.	Deze securityrichtlijn is aanvullend op de eisen en wensen in het PvE.	Applicatielaag
4	De opdrachtnemer garandeert dat alle data die in het kader van deze opdracht wordt verwerkt of opgeslagen uitsluitend binnen de Europese Economische Ruimte (EER) wordt beheerd en bij voorkeur in Nederland. De opdrachtnemer garandeert data alle data volledig onder EU-jurisdictie valt, en niet toegankelijk is voor derden buiten de EER. Data wordt uitsluitend opgeslagen en verwerkt binnen aangewezen rechtsgebieden die voldoen aan Nederlandse en Europese wet- en regelgeving (o.a. AVG). Export van data buiten deze rechtsgebieden is uitsluitend toegestaan na uitdrukkelijke schriftelijke toestemming van de opdrachtgever.	Deze richtlijn is in het kader van datasoevereiniteit.	Informatielaag
5	Voor de uitwisseling van gegevens is het gebruik van de meest actuele StUF-standaarden, waar deze bestaan en nog niet vervangen zijn door een API-standaard, verplicht.	Voor SaaS geldt dat de API-standaard verplicht is. Zie ook Aanbevolen en verplichte standaarden.	Informatielaag

6	Gegevens die opgeslagen worden op storage en back-up systemen worden versleuteld opgeslagen.	Deze securityrichtlijn is aanvullend op de eisen en wensen in het PvE.	Informatielaag
7	Backup en restore moet ingericht zijn om de status op een bepaald tijdstip in het verleden te kunnen herstellen.	Backup en restore.	Informatielaag
8	Inloggegevens worden alleen over versleutelde verbindingen verstuurd.	Deze securityrichtlijn is aanvullend op de eisen en wensen in het PvE.	Informatielaag
9	Webapplicaties moeten browser-onafhankelijk en W3C-compliant zijn.		Applicatielaag
10	De oplossing dient alle voorkomende diakrieten juist te kunnen tonen, exporteren en af te drukken. Dit geldt ook voor alle interfaces.		Applicatielaag
11	De Leverancier zorgt dat gebruik van gedeelde componenten door andere klanten in de infrastructuur van de Leverancier de performance van de Oplossing niet beïnvloeden en / of bedreigen (bijvoorbeeld tijdens de bulkverwerkingen).		Informatielaag
12	Alle data blijft te allen tijde eigendom van en onverminderd kosteloos toegankelijk conform aansluitvoorwaarden voor opdrachtgever.		Informatielaag
13	De Opdrachtnemer is voorbereid om andere identiteitsmogelijkheden (bv. ID-wallet) te implementeren.		Applicatielaag
14	Het is mogelijk om gemachtigden te laten in loggen met DigiD (aansluiting op de DigiD machtigingsvoorziening).		Applicatielaag

1.3 Standaarden, verplicht en aanbevolen

De onderstaande standaarden zijn tweeledig, we hanteren standaarden die verplicht zijn, hiervan willen we dat een opdrachtnemer aan voldoet of wanneer hier niet aan voldaan kan worden dat er uitgelegd wordt waarom niet en wat het alternatief is.
Naast de verplichte standaard, hanteren we ook een aanbevolen standaard, dit heeft altijd de voorkeur. We volgen voor deze standaarden het pas toe of leg uit beleid.

Bron; pas toe leg uit; 'Pas toe of leg uit'-beleid | Forum Standaardisatie

Applicatiefunctie	**Verplichte standaard (pas toe of leg uit)**	**Aanbevolen standaard**	**Implementatie**
Gegevensintegratie	• OpenAPI Specification 3.0 of nieuwer	• REST • OData 4.0 of nieuwer	• Koppelingen tussen SaaS en SaaS-applicaties dienen Native koppelingen te zijn zonder dat hiervoor

	• REST-API Design Rules 1.0 of nieuwer • NL GOV Assurance Profile for OAuth 2.0 of nieuwer	• SOAP 1.2 of nieuwer	ontwikkeld hoeft te worden. • Koppeling met (on premise) systemen van gemeente uitsluitend via de MKS van de gemeente Midden-Drenthe. • Transformatie en queueing d.m.v (on premise) ESB (MKS) mogelijk. • SFTP bij hoge uitzondering mogelijk voor bestandsuitwisseling. • **Geen** rechtstreekse koppeling (ODBC, JDBC, SQL Net) met databases toegestaan. • **Geen** rechtstreekse koppelingen tussen externe en interne systemen zonder ontkoppeling. • Rechtstreekse koppelingen tussen leveranciers onderling zijn onder voorwaarden toegestaan. • Opdrachtnemer garandeert berichtaflevering bij verstoringen in de koppelingen. • Opdrachtnemer draagt zorg voor logische en leesbare foutmeldingen tussen applicaties.
Gebruiker Authenticatie	• DigiD/eHerkenning		• Inwoners en bedrijven via DigiD en of eHerkenning voor authenticatie /verificatie toegang te geven tot digitale diensten van de gemeente.
Medewerker Authenticatie & SSO	• SAML 2.0 of nieuwer	• OIDC, OAUth 2.0 of nieuwer • RBAC • Least privilige	• Vereist is een koppeling met de gemeentelijke, Entra ID op basis van een van de genoemde standaarden.

			• Door deze koppeling wordt tevens voorzien in twee factor authenticatie via de MS authenticator van de gemeente Midden-Drenthe en single sign-on. • Deze eis impliceert dat een eventuele eigen 2 factor authenticatie implementatie van de leverancier uitgeschakeld moet kunnen worden, zodat de 2fa van gemeente gebruikt kan worden. • De oplossing is snel schaalbaar m.b.t. gebruikers • De oplossing is snel schaalbaar m.b.t. transacties
Identity provisioning	• SCIM 2.0 of nieuwer	• Actuele versie MS Graph API	• SCIM d.m.v. Entra ID heeft de voorkeur.
Data	• Inzicht Informatiemodel.		• Gemeente wil te allen tijde inzicht in het informatie/datamodel van de oplossing.
Front-end	• Voor het gebruik van de applicatie(s) volstaat een HTML5 compliant Web Browser (browser onafhankelijk) • Digitoegankelijk (EN 301 549 met WCAG 2.1 niveau AA status B) • Ontwikkeld en ingericht op basis richtlijnen OWASP Top 10, of aantoonbaar gelijkwaardige richtlijnen.		• Gemeente Midden-Drenthe heeft een HTML5 compliant Web Browser. • De gebruikers interface van de oplossing is responsive t.a.v. verschillende devices (laptop, pc, tablet, Apple- of Androidsmartphones). • De oplossing beschikbaar is voor tenminste de laatste 2 versies van de 5 meest recente en gangbare browsers. • De gebruikersinterface dient bij voorkeur Nederlandstalig te zijn. • Alle interactieve - niet zijnde batchverwerkingen - gebruikersinterfaces van de oplossing voor de

			gebruikers worden in 95% van de gevallen binnen 3 seconden getoond. Dit geldt ook voor het tonen van documenten tot 2 MB. Voor wat betreft de reactie van de gehele oplossing op besturings- en invoermogelijkheden met muis en toetsenbord geldt een directe respons: er is geen vertraging tijdens typen.
Verbinding	• HTTPS • HSTS • TLS 1.2 of nieuwer • DNSSEC	• TLS 1.3 of nieuwer • IPv6	• Voor burgers en bedrijven toegankelijke voorzieningen moeten zowel via IPv4 als IPv6 bereikbaar zijn. • Verbinding over Internet d.m.v. TLS heeft voorkeur, alternatief kan een IPsec verbinding over Internet worden gerealiseerd. • (TLS) encryptie ingericht conform actuele richtlijnen Nationaal Cyber Security Centrum (NCSC).
Cryptografie/ versleuteling		• Gegevens die de SaaS-applicatie opslaat dienen versleuteld te zijn.	• Er dient een gedegen versleuteling van toepassing te zijn op data die door de SaaS-applicatie wordt opgeslagen.
OTAP			• Alle aan te schaffen applicaties hebben naast de productieomgeving tenminste nog 1 andere omgeving te gebruiken voor test en/of acceptatie.
Applicatieontwikkeling	• De gemeente werkt met zoveel mogelijk standaard software, zonder maatwerk.		• De gemeente wil zo veel mogelijk maatwerk voorkomen en werken met standaardsoftware.