



Ministerie van Volksgezondheid,
Welzijn en Sport

Technisch Ontwerp

Generieke Functie Adressering

Versie 1.0.0

Inhoudsopgave

Inhoudsopgave	2
1 Documenthistorie.....	5
2 Inleiding.....	6
2.1 Leeswijzer.....	6
3 Scope en afbakening	6
3.1 Binnen scope.....	6
3.2 Buiten scope.....	7
4 Systeemoverzicht	8
4.1 Systeemlandschap	8
4.1.1 KvK Handelsregister	8
4.1.2 LRZa	9
4.1.3 UZI/DEZI	9
4.1.4 Adresboek Replica	9
4.1.5 Data Source	10
4.1.6 Zorginformatiesysteem (XIS)	10
4.2 Componentenoverzicht generieke functie Adressering.....	11
5 Technische uitgangspunten en standaarden.....	11
6 Architectuurprincipes en -keuzes.....	12
6.1 Architectuurprincipes	12
6.1.1 Registratie & bronnen	12
6.1.2 Consolidatie & distributie	12
6.1.3 Raadplegen & vindbaarheid	12
6.1.4 Interoperabiliteit & standaarden.....	13
6.1.5 Beveiliging & vertrouwen	13
6.2 Architectuurkeuzes	13
6.2.1 Registratie & bronnen	13
6.2.2 6.2.2 Consolidatie & distributie	16
6.2.3 Raadplegen & vindbaarheid	20
6.2.4 Interoperabiliteit & standaarden.....	21
7 Componentenarchitectuur	23
7.1 Data Source Client.....	23
7.2 Local Replica Directory.....	23
7.3 LRZa Directory	24
7.4 LRZa Portaal	24
7.5 Query Client	25

7.6	Update Client	25
8	Interfaces en transacties	26
8.1	Transactieoverzicht	26
8.2	Transacties	26
8.2.1	Care Services Feed (Publiceer wijzigingen)	26
8.2.2	Find Matching Care Services (Zoek zorgdiensten)	26
8.2.3	Request Care Services Updates (Synchroniseer wijzigingen)	27
9	Informatiemodel en databronnen	27
9.1	Informatiemodel	27
9.1.1	Endpoint Resource	27
9.1.2	HealthcareService Resource	28
9.1.3	Location Resource	28
9.1.4	Organization Resource	28
9.1.5	OrganizationAffiliation Resource	29
9.2	Databronnen	29
9.2.1	Kamer van Koophandel (KvK)	29
9.2.2	UZI/DEZI	29
9.2.3	Zorgaanbieder (zelfregistratie)	29
9.3	Data-aggregatie	30
10	Security op hoofdlijnen	30
10.1	Gedelegeerde registratie via leverancier	30
10.2	Optionele ondertekening van mutaties met Provenance	31
10.3	Organisatiegebonden certificaten voor API-toegang	32
11	Non-functional requirements	33
11.1	Registratie & bronnen	33
11.1.1	NFR-01: Leidende bronnen alleen met beheerrelatie	33
11.1.2	NFR-02: Onafhankelijke adresgegevenspublicatie	33
11.1.3	NFR-03: Ondersteuning complexe IT-landschappen	33
11.2	Consolidatie & distributie	34
11.2.1	NFR-04: Consistentie	34
11.2.2	NFR-05: Eenduidige uitkomst per mutatie	34
11.2.3	NFR-06: Gedeeld gezaghebbend beeld	34
11.2.4	NFR-07: Schaalbaarheid	35
11.3	Raadplegen & vindbaarheid	35
11.3.1	NFR-08: Beschikbaarheid	35
11.3.2	NFR-09: Geen centrale afhankelijkheid bij raadplegen	36
11.3.3	NFR-10: Performance	36
11.3.4	NFR-11: Verscheidenheid aan inrichtingen en bevragingsmodellen	36

11.4	Interoperabiliteit & standaarden	37
11.4.1	NFR-12: Interoperabiliteit	37
11.4.2	NFR-13: Uitbreidbaarheid	37
11.5	Beveiliging & vertrouwen.....	37
11.5.1	NFR-14: Authenticeren als zichzelf.....	37
11.5.2	NFR-15: Onafhankelijk verifieerbare herkomst van adresgegevens	38
11.5.3	NFR-16: Wettelijke grondslag voor gegevensverwerking	38
12	Begrippenlijst	39
13	Referenties	41
Bijlage 1: Bronvermeldingen		42
Bijlage 2: Besluitonderbouwingen.....		43
Onderbouwing centraal push-model		43
Onderbouwing zorgverleners niet opnemen		44

1 Documenthistorie

Versie	Status	Datum	Auteur	Wijziging
0.8	Concept	Maart 2026	VWS	Initiële versie
0.9	Concept	Maart 2026	VWS	Aanpassingen verwerkt
0.9.5	Concept	Augustus 2026	VWS	Consultatie verwerkt
0.9.9	Concept	September 2026	VWS	Opmerkingen van DA verwerkt
1.0.0	Release voor pilot	1 oktober 2026	VWS	Aanvullende opmerkingen van DA verwerkt

2 Inleiding

Dit document beschrijft het technisch ontwerp van de generieke functie Adressering. Het biedt een architecturaal overzicht van alle componenten, hun interfaces, het datamodel en de technische eisen waaraan implementaties moeten voldoen.

Het technisch ontwerp beschrijft de generieke functie Adressering aan de hand van de volgende elementen: de centrale LRZa-componenten (Portaal, Directory), de decentrale componenten, de IHE Mobile Care Services Discovery (mCSD)/ HL7 Fast Healthcare Interoperability Resources (FHIR) interfaces en de relatie met de bronregisters (KvK Handelsregister, UZI/DEZI register).

Het doel van de generieke functie Adressering reikt tot en met de vraag met welke dienst of welk endpoint een systeem moet communiceren: het adresboek maakt vindbaar wáár een zorgaanbieder bereikbaar is en via welk protocol. Wat de dienst achter dat endpoint vervolgens precies kan, is een eigenschap van die dienst zelf en valt buiten de generieke functie Adressering.

2.1 Leeswijzer

Binnen de hoofdstukken zijn de architectuurprincipes, architectuurkeuzes en niet-functionele requirements thematisch gegroepeerd. De thema's zijn:

- Registratie & bronnen: welke registers leidend zijn, hoe bronregistergegevens worden overgenomen, en hoe zorgaanbieders zelf gegevens aanleveren.
- Consolidatie & distributie: het centrale push-model, aggregatie en conflictresolutie, en de distributie naar read-only replica's.
- Raadplegen & vindbaarheid: het decentraal zoeken op replica's, de beschikbaarheid en performance van het raadplegen.
- Interoperabiliteit & standaarden: de keuze voor mCSD/eu-core, codelijsten en conformiteit.
- Beveiliging & vertrouwen: authenticatie, certificaten, mandaat en de grondslag voor gegevensverwerking.

3 Scope en afbakening

Dit hoofdstuk beschrijft expliciet welke onderwerpen binnen en buiten de scope van dit document vallen.

3.1 Binnen scope

Componenten van de oplossing

Overzicht centrale en decentrale componenten en hun verantwoordelijkheden

Informatiemodel

Logisch datamodel en bron-mappings

Kwaliteitseisen

Performance, beschikbaarheid, schaalbaarheid

Security architectuur

Beveiligingsmodel op hoofdlijnen

Standaarden en protocollen

Toegepaste standaarden (mCSD, FHIR R4, IHE-profielen, eu-core profielen)

3.2 Buiten scope

Concrete technologiekeuzes

Keuzes voor specifieke technologieën (FHIR-server implementatie, database, deployment platform) worden niet in dit document voorgeschreven. Dit document geeft enkel een overzicht van de algehele technische kaders en concepten van de architectuur.

Conformiteitseisen

Testprocedures en certificeringseisen voor aansluiting op de generieke functie Adressering worden separaat gepubliceerd.

Lidmaatschapsrelaties van samenwerkingsverbanden

De relatie tussen een samenwerkingsverband en de zorgaanbieders die eraan deelnemen valt buiten de scope van de generieke functie Adressering. Het LRZa legt die lidmaatschapsrelatie niet vast. Samenwerkingsverbanden die zelf als zorgaanbieder zijn georganiseerd worden wel ondersteund: zij zijn een gewone Organization en kunnen eigen locaties, diensten en endpoints publiceren. Het zoeken naar dossiergegevens via een samenwerkingsverband hoort bij GF Lokalisatie. Daarbij komt dat veel eerstelijns-samenwerkingsverbanden formeel een relatie met een individuele zorgverlener aangaan; het verwerken van die persoonsgegevens door het LRZa valt eveneens buiten scope (zie Zorgverleners en zorgverlenerrollen).

Migratie en transitie

Migratiestrategieën en uitrolplanning voor de transitie van huidige situatie naar de doelsituatie vallen buiten de scope van dit document.

Operationeel beheer en monitoring

Operationele aspecten zoals incident management, change management, backup/restore procedures en monitoring dashboards zijn buiten scope.

Security architectuur details

Gedetailleerde security architectuur (certificaatbeheer, sessie-management, penetratietesten, WAF-configuratie) wordt in een apart document uitgewerkt. Het technisch ontwerp beschrijft security op hoofdlijnen.

Behandeld in: Apart security-ontwerpdocument

Toegangstijden en capaciteitsinformatie

Het delen van informatie over toegangstijden, wachttijden, beschikbare capaciteit en vergelijkbare beschikbaarheidsgegevens valt buiten de scope van de generieke functie Adressering. De generieke functie Adressering ontsluit waar een zorgaanbieder te bereiken is, niet of en wanneer er plaats is.

Zorgverleners en zorgverlenerrollen

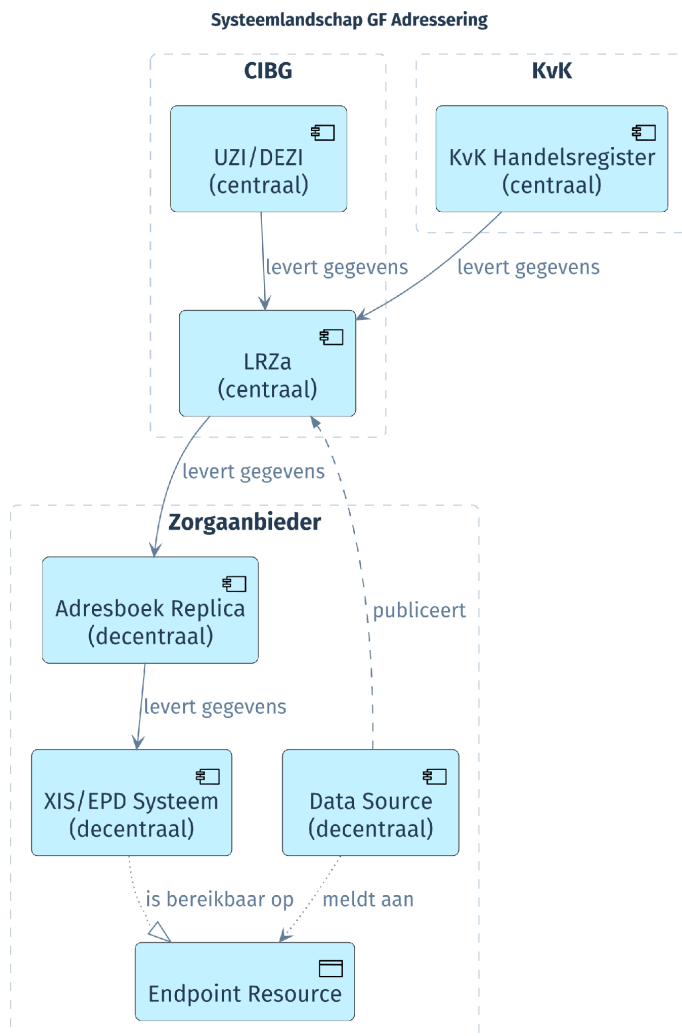
Gegevens over individuele zorgverleners en hun rollen (de mCSD-resources Practitioner en PractitionerRole) vallen buiten de scope van de generieke functie Adressering. Er is geen AVG-grondslag voor het verwerken van deze persoonsgegevens door het LRZa; zie [Onderbouwing zorgverleners niet opnemen](#) voor de afweging en de consequenties.

4 Systeemoverzicht

Dit hoofdstuk beschrijft de generieke functie Adressering op systeemniveau: de betrokken systemen, hun onderlinge samenhang en het deployment model.

4.1 Systeemlandschap

Het onderstaande diagram toont de systemen die binnen de scope van dit document vallen en hun onderlinge relaties.



Figuur: Systeemlandschap generieke functie Adressering

4.1.1 KvK Handelsregister

Verantwoordelijkheid: Handelsregister van de Kamer van Koophandel. Autoritatieve bron voor organisatie-identificatie (KvK-nummer), statutaire naam en vestigingsadressen. Het LRZa bevraagt dit register voor deze gegevens.

Implementatie: Centraal

4.1.2 LRZa

Verantwoordelijkheid: Het LRZa is het centrale systeem binnen de generieke functie Adressering. Het bestaat uit:

- Portaal: voor beheer van autorisaties voor Dienstverleners door Zorgaanbieders
- Directory: voor publicatie van mCSD-conforme FHIR-resources

Implementatie: Centraal

4.1.3 UZI/DEZI

Implementatie: Centraal

Verantwoordelijkheid: UZI-register (en opvolger DEZI), beheerd door CIBG. Autoritatieve bron voor zorgaanbieder-identificatie (URA). Het LRZa bevraagt dit register voor deze gegevens.

4.1.4 Adresboek Replica

Verantwoordelijkheid: De Adresboek Replica is de functionele rol van het lokale, decentrale bevragspunt voor adresboekgegevens. Zorgaanbieders bevragen deze replica (vanuit hun XIS/EPD of andere toepassingen) in plaats van het centrale LRZa rechtstreeks. De replica synchroniseert de geconsolideerde directory vanuit het LRZa en stelt die lokaal beschikbaar.

Implementatie: Decentraal

Onderbouwing voor component: Bevragingen mogen niet afhangen van één landelijke voorziening (zie eis NFR-09: Geen centrale afhankelijkheid bij raadplegen en architectuurkeuze AK-09: Decentrale replica's met periodieke synchronisatie). De decentrale replica borgt leesbeschikbaarheid en lastspreiding: ook bij uitval van het centrale LRZa blijven adresgegevens lokaal bevragebaar. Dit is een bewuste keuze, geen overbodige kopie van het LRZa.

Plaatsing:

De Adresboek Replica valt onder verantwoordelijkheid van de zorgaanbieder, maar waar en hoe deze draait is een implementatiekeuze die de architectuur niet voorschrijft:

- bij de zorgaanbieder zelf, bij diens softwareleverancier, of als gedeelde replica via een integratiedienst die meerdere zorgaanbieders bedient;
- geïntegreerd in het XIS/EPD zelf — de replica is een logische rol, geen verplicht apart systeem.

De generieke functie Adressering schrijft de techniek en de niet-functionele eigenschappen (beschikbaarheid, performance, actualiteit) van de replica niet voor; die bepaalt de zorgaanbieder zelf. Wie liever naar een eigen database (RDBMS, NoSQL) repliceert, kan dat doen mits de bevragsfunctie geleverd wordt.

Voor de conformiteit geldt wél een voorgeschreven set: de synchronisatie met het LRZa is een harde eis, voor de lokale bevraging geldt een advies. Deze eisen en de referentie-invulling staan op pagina "Addressing" van de "Generic Functions & Patterns - Implementation Guide" (vanaf hier: "Implementation Guide"), zie Conformiteit en compliance per rol en Local Replica Directory.

Deze vrijheid in plaatsing is bewust en geldt voor alle decentrale voorzieningen; de eis en de onderbouwing staan in eis NFR-11: Verscheidenheid aan inrichtingen en bevragsmodellen.

Referentie-opdeling:

In de referentie-architectuur bestaat de Adresboek Replica uit twee componenten met gescheiden verantwoordelijkheden:

- de Local Replica Directory (Local Replica Directory) — het lokale FHIR-bevragingspunt;
- de Update Client (Update Client) — de synchronisatie-motor die de replica actueel houdt vanuit het LRZa.

Deze opdeling is een referentie-invulling. Omdat de invulling van de replica vrij is, mag een implementatie deze functies combineren of anders organiseren.

4.1.5 Data Source

Verantwoordelijkheid: De Data Source is de functionele voorziening waarmee een zorgaanbieder zijn adresseringsgegevens beheert en publiceert naar het LRZa. Het is geen nieuw, zelfstandig adresboek: het is het publicatiekanaal richting het centrale register. Beheer (invoeren en actueel houden van endpoints, services, locaties) en publicatie naar het LRZa lopen via deze voorziening.

Implementatie: Decentraal

Plaatsing:

De Data Source valt altijd onder de verantwoordelijkheid van de zorgaanbieder. Waar de voorziening technisch draait — binnen het XIS/EPD, op een integratieplatform, of bij een softwareleverancier — is een implementatiekeuze die de architectuur bewust niet voorschrijft. Het LRZa behandelt elke Data Source gelijk (zie Data Source als enkelvoudig aanspreekpunt). Die vrijheid in plaatsing geldt voor alle decentrale voorzieningen; zie eis NFR-11: Verscheidenheid aan inrichtingen en bevragsmodellen.

Dat meerdere zorgaanbieders dezelfde leverancier of dienst kiezen om hun Data Source te hosten, verandert die verantwoordelijkheid niet: elke zorgaanbieder blijft juridisch verantwoordelijk voor de eigen aangeleverde gegevens. De architectuur kent daarom geen aparte categorie “centrale” of “semi-centrale” Data Source.

Gelijktijdige mutaties:

Meerdere partijen kunnen namens dezelfde zorgaanbieder publiceren, bijvoorbeeld twee leveranciers die elk een deel van de gegevens beheren. Om te voorkomen dat de een de wijziging van de ander ongemerkt overschrijft, verlopen mutaties met optimistic locking: bij een PUT geeft de Data Source de versie mee die zij gelezen heeft, en weigert het LRZa de mutatie als die versie inmiddels is achterhaald. De uitwerking via ETag staat in de Implementation Guide.

Consolidatie van onderliggende systemen:

Een Data Source kan gegevens van één of meerdere onderliggende systemen van de zorgaanbieder consolideren tot één aanlevering. Zij bepaalt de gegevens niet zelfstandig — de inhoud komt uit de bronsystemen van de zorgaanbieder, die verantwoordelijk blijft voor de juistheid ervan.

4.1.6 Zorginformatiesysteem (XIS)

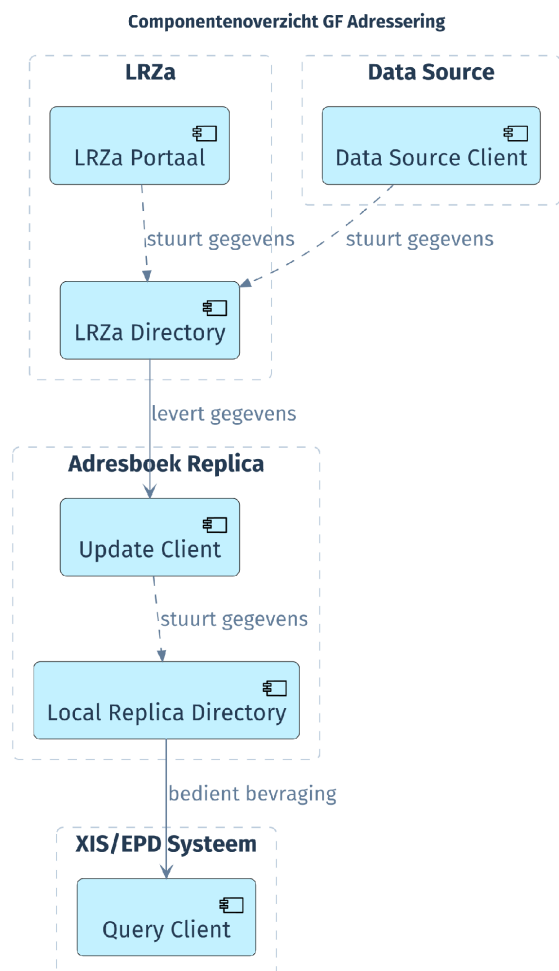
Verantwoordelijkheid: Zorginformatiesysteem of Elektronisch Patiëntendossier van een zorgaanbieder. Dit is het primaire systeem waarmee zorgverleners werken en van waaruit gegevensuitwisseling met andere zorgaanbieders plaatsvindt.

Binnen het XIS/EPD bevindt zich de Query Client, de component waarmee adressen van andere zorgaanbieders worden opgezocht via de decentrale Adresboek Replica.

Implementatie: Decentraal

4.2 Componentenoverzicht generieke functie Adressering

Het onderstaande diagram toont de relaties tussen de componenten binnen de generieke functie Adressering architectuur, gegroepeerd per systeem.



Figuur: Componentenoverzicht generieke functie Adressering

5 Technische uitgangspunten en standaarden

Dit hoofdstuk beschrijft de technische standaarden en kaderstellende documenten waaraan het ontwerp moet voldoen.

Titel	Type	Referentie
Baseline Informatiebeveiliging Overheid (BIO)	standaard	https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/bio-en-ensia/baseline-informatiebeveiliging-overheid/

Titel	Type	Referentie
Functioneel Ontwerp generieke functie Adressering	document	-
HL7 Europe eu-core	standaard	https://hl7.eu/fhir/base/
HL7 FHIR R4	standaard	https://www.hl7.org/fhir/R4/
IHE mCSD	standaard	https://profiles.ihe.net/ITI/mCSD/index.html
Implementation Guide voluit: "Care Service Directory - Implementation Guide"	standaard	https://build.fhir.org/ig/minvws/generiekefuncties-docs/branches/1.0.0/

6 Architectuurprincipes en -keuzes

Dit hoofdstuk beschrijft de leidende architectuurprincipes en architectuurkeuzes die het ontwerp vormgeven.

6.1 Architectuurprincipes

6.1.1 Registratie & bronnen

AP-01: Bronregister is leidend

De generieke functie Adressering hanteert een strikte bronhiërarchie: gegevens uit bronregisters (KvK, UZI/DEZI) zijn altijd leidend boven lokaal beheerde gegevens.

Dit betekent dat alleen aanvullende gegevens die niet in bronregisters voorkomen lokaal beheerd mogen worden. Dit principe waarborgt de integriteit en betrouwbaarheid van de adresboekgegevens.

6.1.2 Consolidatie & distributie

AP-02: Concentreer complexiteit

Complexe logica wordt geconcentreerd op plekken waar deze goed getest, bewaakt en gecorrigeerd kan worden.

Dit geldt met name voor:

- Autorisatielogica (wie mag welke data muteren)
- Databeschermingsregels (voorkomen dat partijen elkaars data overschrijven)
- Aggregatie van meerdere bronnen

Fouten in een centraal bewaakte component worden sneller gevonden dan dezelfde fouten verspreid over vele implementaties.

6.1.3 Raadplegen & vindbaarheid

AP-03: Actoren zijn rollen, geen systemen

Met uitzondering van het LRZa schrijft de generieke functie Adressering geen systemen voor, maar alleen rollen: Data Source, Update Client, Query Client en de Adresboek Replica. Wie die rollen vervult en hoe zij worden ingevuld, bepaalt het veld zelf.

Daaruit volgt dat de architectuur geen eisen stelt aan de verdeling van rollen over partijen. De relatie tussen rol en partij is veel-op-veel: één partij kan meerdere rollen tegelijk vervullen, en dezelfde rol kan door verschillende partijen worden ingevuld. Dit sluit aan bij IHE mCSD, waarin actoren mogen worden gegroepeerd. Een uitspraak over een rol is daarom nooit een uitspraak over een specifiek systeem, en de diagrammen in dit document tonen een voorbeeldinvulling en geen beperking.

Het LRZa is hierop de uitzondering. De LRZa Directory en het LRZa Portaal zijn geen vrij in te vullen rollen maar één concreet, centraal belegd systeem.

6.1.4 Interoperabiliteit & standaarden

AP-04: Internationale standaarden

De generieke functie Adressering maakt bij voorkeur gebruik van breed geadopteerde, internationale open standaarden om interoperabiliteit te bevorderen, leveranciersonafhankelijkheid te waarborgen en aansluiting bij bestaande infrastructuur mogelijk te maken.

6.1.5 Beveiliging & vertrouwen

AP-05: Vinden is niet blind vertrouwen

Een afnemer gebruikt de via de generieke functie Adressering gevonden gegevens om verbinding te leggen met een endpoint. Daarbij stelt de afnemer, conform de GIS-afspraken, zelf vast dat het endpoint bij de beoogde partij hoort. Dat is een aparte, normale stap (mTLS, wederzijdse authenticatie) en staat los van de betrouwbaarheid van de adresgegevens zelf; ook wanneer een adresgegeven cryptografisch verifieerbaar is vastgelegd, ondervangt deze stap fouten op DNS- of netwerkniveau.

6.2 Architectuurkeuzes

6.2.1 Registratie & bronnen

AK-01: Bronregisterdata is read-only in mCSD

Context

De mCSD-resources (Organization, Location, etc.) bevatten gegevens die afkomstig zijn uit bronregisters zoals KvK en UZI/DEZI. Deze gegevens moeten consistent blijven met de bronregisters.

Gegevensvelden in mCSD-resources die afkomstig zijn uit bronregisters (KvK, UZI/DEZI) zijn read-only en kunnen niet worden aangepast op een andere manier dan via de bronregisters zelf. Alleen aanvullende velden die niet uit bronregisters komen zoals afdelingen, Endpoint-configuratie en HealthcareService-details) kunnen door zorgaanbieders/leveranciers worden beheerd.

Rationale

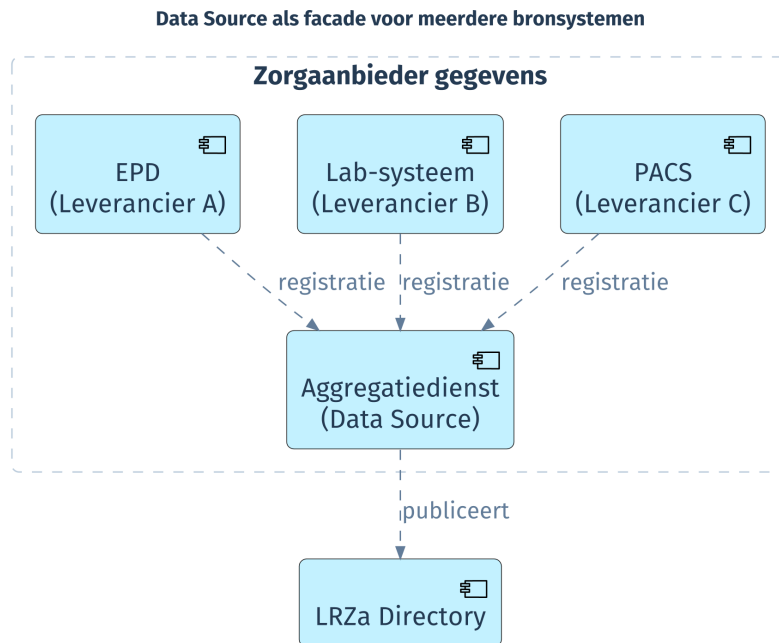
- Voorkomt inconsistenties tussen de generieke functie Adressering en bronregisters
- Vermindert beheerlast: wijzigingen in bronregisters worden automatisch doorgevoerd
- Verhoogt betrouwbaarheid: afnemers kunnen vertrouwen op correctheid van brondata

AK-02: Data Source als enkelvoudig aanspreekpunt

De architectuur staat toe dat een Data Source functioneert als façade voor meerdere achterliggende systemen. De interne organisatie van de Data Source is een implementatiedetail.

Het LRZa behandelt elke Data Source gelijk, ongeacht of deze adresgegevens uit één of meerdere achterliggende systemen bundelt. Er is geen apart registratieproces, API of behandeling voor aggregators.

Voorbeeld



Rationale

- Houdt de LRZa-architectuur eenvoudig: één uniforme interface voor alle Data Sources
- Geeft zorgaanbieders vrijheid om hun aanlevering intern te organiseren
- Voorkomt dat LRZa kennis moet hebben van interne IT-landschappen van zorgaanbieders

Implicaties

- De Data Source is verantwoordelijk voor de kwaliteit van alle aangeleverde gegevens
- LRZa valideert op Data Source-niveau, niet op achterliggende bron-niveau
- Zorgaanbieders autoriseren de Data Source, niet de individuele achterliggende systemen

AK-03: Leidend bronregister versus aanvullende identifieer

Voor registers die niet onder de leidende bronregisters van het LRZa (zie architectuurkeuze AK-04) vallen kent de generieke functie Adressering het concept van een aanvullende identifieer: een nummer uit een register buiten het LRZa om, dat de zorgaanbieder of zijn leverancier zelf op zijn resources registreert. Deze architectuurkeuze beschrijft hoe deze identifiërs op een betrouwbare manier gebruikt kunnen worden.

Zoeken op een aanvullende identifieer

Het LRZa controleert een aanvullende identifieer niet inhoudelijk. Daardoor kan een identifieer door misconfiguratie of fouten bij de verkeerde organisatie geregistreerd worden, bijvoorbeeld wanneer een leverancier meerdere zorgaanbieders ondersteunt. Daarom is direct zoeken op een dergelijke identifieer niet de aanbevolen route. De identifiërs kunnen wel gebruikt worden in het tweestapsproces dat hieronder is beschreven:

- zoek in het externe register op de aanvullende identifieer (in dit voorbeeld de AGB) en neem de leidende identifieer (URA of KvK) over die daar geregistreerd staat;

- zoek in de generieke functie Adressering de organisatie op die leidende identifier.

Op deze wijze is gegarandeerd dat de juiste organisatie gevonden wordt. Een AGB kan ook een onderdeel van een sub-organisatie beschrijven. In dat geval volgt er nog een derde stap: zoek binnen de gevonden organisatie (na stap 2 hierboven) het specifieke onderdeel op de aanvullende identifier.

Doordat de query “gescoped” is op de organisatie die via een leidende identifier is gevonden, werkt dit betrouwbaar.

Overweging

Rechtstreeks zoeken op een aanvullende identifier kost minder stappen, maar levert een ander resultaat op. Het LRZa voert geen inhoudelijke controle uit op een zelf geregistreerde identifier; een onjuiste registratie kan dan naar de verkeerde organisatie leiden. De leidende identifier (KvK/URA) komt uit een bronregister met beheerrelatie en is wel geborgd, waardoor verwijzing naar de verkeerde organisatie uitgesloten is. De route via het externe register kost een stap extra en levert die zekerheid op.

Welke registers het LRZa als leidende bron opneemt, en waarom AGB daar niet toe behoort, legt architectuurkeuze AK-04: Leidende bronregisters van het LRZa vast. Deze keuze gaat alleen over de zoekroute voor een identifier die als aanvullende identifier in het LRZa voorkomt.

Consequenties

Het LRZa kent geen koppeling met de registers achter een aanvullende identifier. De eerste stap naar de leidende identifier ligt bij de afnemer; het LRZa faciliteert die niet.

Deze oplossing geeft deels invulling aan de bredere wens om bestaande AGB-gebaseerde adressering te ondersteunen. Daarmee wordt de migratievraag deels, maar niet volledig, geadresseerd (zie de alinea Migratie en transitie in hoofdstuk 3. Scope en Afbakening).

AK-04: Leidende bronregisters van het LRZa

Het LRZa neemt gegevens over uit KvK voor de juridische entiteit en uit UZI/DEZI voor de zorginhoudelijke toewijzing. Alleen deze registers gelden als leidende bron; het LRZa presenteert hun gegevens als geborgd. Andere registers, zoals het AGB, neemt het LRZa niet als leidende bron op.

Overweging

Leidende bronnen alleen met beheerrelatie vereist dat het LRZa alleen gegevens uit een register als geborgd presenteert wanneer de Beheerder er een beheerrelatie mee heeft. KvK en UZI/DEZI voldoen daaraan en zijn in dit stelsel de aangewezen identificerende nummers.

Het AGB-register is geen leidende bron. De beheerder heeft geen zeggenschap over en geen beheerrelatie met het AGB-register, waardoor afspraken over actualiteit en kwaliteit niet af te dwingen zijn. Bovendien dient AGB een ander primair doel dan identificatie in dit stelsel. Dat AGB in delen van de zorg een belangrijke identifier is, wordt indirect ondersteund: registratie als aanvullende identifier blijft mogelijk onder eis NFR-13: Uitbreidbaarheid, en de zoekroute daarvoor legt architectuurkeuze AK-03: Leidend bronregister versus aanvullende identifier vast.

Consequenties

- AGB wordt niet als leidende bron opgenomen. Een AGB-code kan alleen als aanvullende identifier in het LRZa voorkomen.

- Hetzelfde criterium geldt voor elk (toekomstig) register: opname als leidende bron vraagt een beheerrelatie, aanvullende registratie niet.

Komt voort uit eis:

NFR-01: Leidende bronnen alleen met beheerrelatie

*AK-05: Zorgverleners niet opnemen in het LRZa***Context**

Het mCSD-profiel kent de resources Practitioner en PractitionerRole, waarmee individuele zorgverleners en hun rollen binnen een organisatie worden gemodelleerd. In de consultatie is meermaals gevraagd om adressering op zorgverlenerniveau te ondersteunen.

Deze resources bevatten persoonsgegevens. Een juridische analyse heeft uitgewezen dat er geen AVG-grondslag is voor het verwerken van persoonsgegevens van zorgverleners door het LRZa.

Besluit

Practitioner en PractitionerRole zijn geen onderdeel van de generieke functie Adressering en worden niet in het LRZa opgenomen. Het LRZa accepteert geen registratie van deze resources.

Consequenties

- Het informatiemodel beperkt zich tot Organization, Location, HealthcareService, Endpoint en OrganizationAffiliation.
- Zorgaanbieders kunnen zorgverlenergegevens desgewenst zelf lokaal beschikbaar stellen via een Endpoint dat in het LRZa is geregistreerd. De generieke functie Adressering doet geen uitspraken over de inhoud of werking van een dergelijke voorziening.
- Voor communicatie kunnen contactgegevens van afdelingen, teams of diensten worden gebruikt. Die worden gemodelleerd als Organization, Location en HealthcareService en kunnen wel in het LRZa worden geregistreerd.
- Een internationale mCSD-client ondersteunt Practitioner en PractitionerRole maar deze resources worden niet beschikbaar gesteld door het LRZa.

Rationale

De beperking volgt uit de ontbrekende grondslag, niet uit het datamodel. De functionele behoefte wordt erkend — bijvoorbeeld voor intercollegiale consulten en communicatie naar een huisartspraktijk. Ontstaat er wel een grondslag, dan kan ondersteuning alsnog worden toegevoegd zonder wijziging van de architectuur.

6.2.2 6.2.2 Consolidatie & distributie*AK-06: Centraal push-model met read-only replica's***Context**

Voor de generieke functie Adressering moet worden vastgelegd hoe mutaties van bronnen (zorgaanbieders en hun leveranciers) bij het centrale register terechtkomen en hoe afnemers adresgegevens bevragen. Tijdens de proof-of-concepts is een pull-model met decentrale bronnen beproefd; op grond van de bevindingen daaruit is een centraal push-model uitgewerkt en in de consultatie (v0.9) voorgelegd.

Besluit

De generieke functie Adressering hanteert een centraal push-model:

- Eén gezaghebbend register, het LRZa (CIBG/VWS), waar bronnen mutaties aanleveren (push).
- Aggregatie en conflictresolutie vinden op het moment van schrijven centraal op het LRZa plaats.
- Voor bevestigingen werken afnemers met read-only replica's per afnemer; dit borgt leesbeschikbaarheid en lastspreiding.

Dit besluit is door de DA bekrachtigd.

Rationale

- Directe feedback aan de aanleverende partij: een mutatie wordt geheel geaccepteerd of geweigerd, met reden. In een model waarin elke afnemer zelf aggregaat kan een mutatie stil terzijde worden gelegd zonder dat de aanleverende partij dat merkt; bij aanlevering aan één register is dat uitgesloten.
- Meerdere leveranciers per zorgaanbieder wordt mogelijk: in het pull-model lag de publicatie bij één leverancier, waardoor een tweede leverancier van die eerste afhankelijk werd om gegevens gepubliceerd te krijgen. Doordat elke leverancier zijn mutaties rechtstreeks bij het LRZa aanlevert, vervalt die afhankelijkheid.
- Eén gezaghebbende stand: wijzigingen in aggregatie- en conflictresolutieregels werken meteen voor alle afnemers door, zonder dat elke partij in het veld daarvoor eerst een aanpassing hoeft door te voeren.
- Inhoudelijke divergentie tussen replica's verdwijnt: wat resteert is verschil in actualiteit, niet in inhoud.

Afgewezen alternatieven

Volledig decentraal (geen registerwijzer), centraal zonder replica's, centraal pull met decentrale publicatie, en een hybride model (centrale discovery met decentrale autoritatieve publicatie) zijn afgewogen en afgewezen. De volledige afweging, de PoC-bevindingen en de geaccepteerde prijs staan in Onderbouwing centraal push-model (zie appendix).

Consequenties

- Schrijfbeschikbaarheid is afhankelijk van het centrale LRZa (single point of failure voor mutaties); leesbeschikbaarheid blijft via replica's overeind. Mitigatie via redundantie/SLA en optioneel lokaal cachen-en-pushen.
- Concentratie van inhoudelijk gewicht bij de centrale beheerder; vraagt om expliciete governance.

AK-07: Centrale aggregatie

Context

Aggregatie van meerdere databronnen tot één directory kan op verschillende manieren worden geïmplementeerd: gedistribueerd (elke afnemer aggregaat zelf) of centraal (één component aggregaat).

Aggregatie van bronregisters en zorgaanbiedergegevens vindt centraal plaats in het LRZa. Aggregatielogica op een centrale locatie zorgt voor een gedeeld beeld bij alle gebruikers van de GFA.

Rationale

- Complexiteitsreductie voor de bevrager: zonder centrale aggregatie zou elke afnemer de gegevens zelf moeten samenvoegen. Niet het bevragen van meerdere bronnen is daarbij het probleem, maar de logica om per gegeven alleen de juiste bron over te nemen, en vooral het samenvoegen van de bijdragen van zorgaanbieder/leverancier met de bronregistergegevens (KvK, UZI/DEZI). Tijdens de PoC's bleek precies die samenvoeglogica foutgevoelig wanneer zij gedistribueerd wordt geïmplementeerd.
- Gedistribueerde implementaties van dezelfde logica leiden tot subtiele inconsistenties die moeilijk te traceren zijn. Centraal zijn registratie- en aggregatiefouten eenduidig detecteerbaar en is de bron ervan aanspreekbaar.

Dat mutaties centraal binnenkomen is vastgelegd in architectuurkeuze AK-06: Centraal push-model met read-only replica's; die keuze gaat over het aanlevermodel, deze over de plaats van de aggregatielogica.

Consequenties

- Vertrouwen: alle partijen moeten de LRZa-beheerder vertrouwen voor correcte aggregatie en autorisatie.
- Centrale wijzigingen: aanpassingen aan aggregatielogica hoeven slechts op één plek te gebeuren.

AK-08: LRZa als centraal consolidatie- en distributiepunt

Context

De generieke functie Adressering combineert gegevens uit meerdere bronnen tot één uniforme, mCSD-gemodelleerde gegevensverzameling: authentieke bronregisters (KvK, UZI/DEZI) en gegevens die zorgaanbieders zelf aanleveren (afdelingen of sub-organisaties, endpoints, services, locaties).

Het LRZa is het centrale consolidatie- en distributiepunt voor deze geconsolideerde directory: het register dat de gegevens uit de verschillende bronnen consolideert en als één uniforme view beschikbaar stelt. De term "single source of truth" wordt bewust niet gebruikt: die suggereert dat het LRZa de oorspronkelijke waarheid over alle gegevens bezit, terwijl de authentieke bronregisters leidend blijven voor hun eigen domein. Het LRZa is dus wel een register, maar geen authentieke bron voor de gegevens die het uit KvK en UZI/DEZI overneemt, noch voor de gegevens die zorgaanbieders zelf aanleveren.

Consolidatie en distributie zijn niet hetzelfde als bevraging: het LRZa stelt de geconsolideerde gegevens beschikbaar voor replicatie, maar is zelf geen zoekingang. Zie LRZa als replicatiebron, niet als mCSD Directory-actor.

Het LRZa is als register leidend voor de totale geconsolideerde directory: zowel de geaggregeerde bronregistergegevens als de door zorgaanbieders zelf ingevoerde gegevens. De authentieke bronregisters (KvK, UZI/DEZI) blijven leidend voor hun eigen domein; het LRZa neemt die gegevens over maar vervangt ze niet.

Write/read-splitsing

Het LRZa is leidend voor writes: alle mutaties (van bronregisters én zorgaanbieders) worden centraal in het LRZa verwerkt. Voor reads verzorgen decentrale, read-only replica's de leesbeschikbaarheid (eventual consistency). Afnemers en replica's bevragen voor deze geconsolideerde gegevens altijd het LRZa of hun eigen replica, en niet de bronregisters direct. Voor gegevens die het LRZa niet voert,

zoals zorgverlenergegevens (Zorgverleners niet opnemen in het LRZa), doet dit besluit geen uitspraak over de route die een afnemer kiest.

Zie ook de architectuurkeuze AK-06: Centraal push-model met read-only replica's.

Leidende bron en richting per gegeven

De gesignaleerde schijnbare tegenstrijdigheid ("wie is nu leidend, de zorgaanbieder of het bronregister?") lost op zodra het per gegeven wordt bekeken: geen enkele partij is overal leidend.

Gegeven	Leidende bron/ verantwoordelijke	Richting naar LRZa
Organisatiegegevens (naam, KvK, rechtsvorm)	KvK, authentieke bron	LRZa verzamelt bij KvK
Locatiegegevens van vestigingen	KvK, authentieke bron	LRZa verzamelt bij KvK
Zorgaanbieder-identificer (URA)	UZI/DEZI, authentieke bron	LRZa verzamelt bij UZI/DEZI
Organisatiegegevens van afdelingen en sub-organisaties	Zorgaanbieder, invoer en actueel houden	Push door zorgaanbieder/leverancier
Locatiegegevens die de zorgaanbieder zelf onderscheidt	Zorgaanbieder, invoer en actueel houden	Push door zorgaanbieder/leverancier
Endpoints en services	Zorgaanbieder, invoer en actueel houden	Push door zorgaanbieder/leverancier
Geconsolideerde directory (correcte aggregatie, validatie, beschikbaarstelling)	LRZa	n.v.t. (LRZa is eindpunt)

Voor de gegevens die het LRZa bij KvK en UZI/DEZI verzamelt is het voor afnemers niet van belang of de bronregisters pushen of dat het LRZa pullt.

Het LRZa neemt geen inhoudelijke verantwoordelijkheid voor de juistheid van de door zorgaanbieders zelf ingevoerde adresgegevens (afdelingen, endpoints, services, locaties); de zorgaanbieder is en blijft hiervoor verantwoordelijk.

Rationale

- Eén geconsolideerd, gezaghebbend beeld voorkomt inconsistenties tussen verschillende kopieën.
- Centrale consolidatie maakt autorisatie en databescherming beter bewaakbaar.
- Afnemers hebben één duidelijk punt voor actuele, geconsolideerde data en hoeven niet zelf meerdere bronnen te bevragen en samen te voegen.
- Zorgaanbieders zijn niet afhankelijk van individuele leveranciers voor hun adresgegevens; data blijft beschikbaar ongeacht leveranciersrelaties.

Afbakening

Governance (wie is verantwoordelijk voor welke gegevens, escalatieprocedures, regelbeheer, SLA's) valt buiten dit technisch ontwerp en wordt in een apart governance-traject belegd.

6.2.3 Raadplegen & vindbaarheid*AK-09: Decentrale replica's met periodieke synchronisatie***Context**

De eis NFR-09: Geen centrale afhankelijkheid bij raadplegen vereist dat bevestigingen niet afhankelijk zijn van één centraal systeem. Voor de GFA is gekozen voor decentrale of lokale replica's met periodieke synchronisatie.

Rationale

- Maximale autonomie voor afnemers: zij bepalen zelf hun beschikbaarheidsniveau
- Geen afhankelijkheid van netwerk naar centrale systemen tijdens bevestigingen
- Schaalt onbeperkt: elke nieuwe afnemer voegt eigen capaciteit toe

Voorbeeld

Een integratiedienst kan een Local Replica Directory hosten voor meerdere zorgaanbieders (en leveranciers). Zorgaanbieders hoeven dan geen eigen replica-infrastructuur te beheren, maar bevestigen de gedeelde replica via die dienst. Dit is een implementatiekeuze van de afnemer; het LRZa maakt geen onderscheid.

Synchronisatie-mechanisme

Het synchronisatiemechanisme is normatief gespecificeerd in de Implementation Guide; het technisch ontwerp normeert dit bewust niet. De IG beschrijft onder meer de initial load (met paging), incrementele delta-synchronisatie via FHIR _history, foutafhandeling met retries, en het omgaan met teruggetrokken resources.

Twee architecturale uitgangspunten gelden daarbij:

- Alle resource-types synchroniseren op één gemeenschappelijk interval, zodat onderlinge verwijzingen tussen resources niet langdurig naar een nog-niet-gerepliceerde resource wijzen.
- Het synchronisatie-interval — en daarmee de actualiteit van de replica — is een keuze van de afnemer, binnen de rate-limits die het LRZa via de SLA stelt. De generieke functie Adressering stelt hieraan geen eisen (zie Adresboek Replica).

Consequenties

- Afnemers zijn verantwoordelijk voor eigen replica-infrastructuur
- Gegevens kunnen tijdelijk out-of-sync zijn (eventual consistency)
- Synchronisatie-interval bepaalt maximale vertraging van updates

AK-10: LRZa als replicatiebron, niet als mCSD Directory-actor

Het LRZa is een replicatiebron, geen volwaardige IHE mCSD Directory-actor. De mCSD-Directory-rol waar afnemers tegenaan praten wordt vervuld door de lokale replica, die haar gegevens bij het LRZa ophaalt.

Het LRZa beperkt daartoe de bevestigingsmogelijkheden op de centrale directory: het ondersteunt zoeken op identifier en de replicatie-transacties, maar biedt niet de volledige set zoekparameters die een mCSD Directory kent.

Overweging

De eis NFR-09: Geen centrale afhankelijkheid bij raadplegen legt vast dat het raadplegen niet van één centrale voorziening mag afhangen, en dat het zoeken daarom decentraal gebeurt. Die eis en de mCSD-conformiteit van het centrale register laten zich niet allebei volledig honoreren: een conforme Directory biedt juist wél een volwaardige zoekingang.

IHE mCSD stelt de zoekparameters van ITI-90 als SHALL en staat een Directory toe die set uit te breiden, maar niet in te perken. Het LRZa perkt haar wél in en wijkt daarmee op dit punt echt af van de standaard. Dat is een andere situatie dan bij delete: het al of niet ondersteunen van delete legt mCSD uitdrukkelijk als beleidskeuze bij de directory. Het LRZa staat delete toe, met als aanbevolen route een statuswijziging in plaats van verwijderen omdat die de reden van intrekking bewaart; die keuze blijft binnen de standaard en is geen afwijking.

De alternatieve route is het LRZa de volledige zoekparameters te laten ondersteunen en het gebruik ervan met rate limiting te ontmoedigen. Dat levert formele conformiteit op, maar zet een zoekingang open die architectonisch niet gebruikt moet worden. Wie de parameters aanbiedt en vervolgens onbruikbaar maakt, wekt de schijn van conformiteit in plaats van conform te zijn. De keuze is daarom om de afwijking te benoemen in plaats van te verhullen.

Consequenties

- Conformiteit wordt belegd bij de replica: die is wél een mCSD-conforme Directory (zie Conformiteit en compliance per rol en Local Replica Directory).
- Met IHE NL wordt het gesprek gestart over een nationaal profiel. Het LRZa vervult een rol die mCSD niet kent; het voorstel is daarom geen ingeperkte Directory-actor maar een nieuwe actor die ITI-91 als responder ondersteunt plus een transactie voor het ophalen van de meest recente versie (een uitgekilde ITI-90). Slaagt dat, dan wordt de afwijking alsnog binnen de standaard opgelost.

Komt voort uit eis:

NFR-09: Geen centrale afhankelijkheid bij raadplegen

6.2.4 Interoperabiliteit & standaarden

AK-11: Basisprofielen op eu-core

De profielen van de generieke functie Adressering zijn waar mogelijk gebaseerd op de Europese eu-core basisprofielen.

Overweging

Keuze voor mCSD NL als directory-standaard (gebaseerd op IHE mCSD) legt IHE mCSD vast als basis. Dat profiel schrijft voor welke resources een care services directory kent en hoe ze samenhangen, maar laat de invulling van de afzonderlijke velden grotendeels open. Twee implementaties kunnen daardoor allebei mCSD-conform zijn en toch niet met elkaar overweg, omdat ze dezelfde velden anders invullen. Een basisprofielenset sluit dat gat met datatypes, cardinaliteiten en waardelijsten. Voor de generieke functie Adressering gebeurt dat in mCSD NL: een Nederlandse aanvulling op IHE mCSD die op eu-core is gebaseerd.

De keuze gaat daarmee over de reikwijdte van die basis. eu-core is de Europese basisprofielenset: wie daarop aansluit is niet alleen binnen Nederland interoperabel, maar ook richting grensoverschrijdende uitwisseling. De Nederlandse nl-core-profielen zijn hier de gangbare keuze en sluiten aan op de ZIB's, maar zijn nog niet op die bredere interoperabiliteit gericht.

Een Europese basisprofielenset dekt niet alles wat de generieke functie Adressering nodig heeft. Nederland-specifieke codes en waardelijsten, zoals het URA-nummer, worden in de Implementation Guide via een aanvullend profiel gedefinieerd. Waar een resource geen bruikbaar eu-core-profiel heeft, zoals Endpoint en HealthcareService, wordt direct op FHIR R4 geprofileerd.

Vooruitblik

De nl-core-gbb-profielen worden verwacht in 2026 Q4 en zullen compliant zijn aan eu-core. Daarmee vervalt het bezwaar hierboven: die set sluit dan wél aan op de Europese basis. Bij een volgende versie van de Implementation Guide wordt bekeken of een overstap naar die profielen mogelijk en wenselijk is. Omdat beide sets dan eu-core-conform zijn, is dat een gerichte wijziging en geen herziening van de uitgangspunten.

AK-12: Conformiteit en compliance per rol

De normatieve eisen per rol staan in de Implementation Guide (IG), in de vorm van CapabilityStatements en de bijbehorende SHALL- en SHOULD-bepalingen. Die bepalingen zijn bepalend voor compliance: een implementatie die ze volgt is compliant, een afwijkende implementatie is technisch mogelijk maar geldt dan als niet-compliant.

Het koppelvlak met het LRZa (publicatie en synchronisatie) is verplicht FHIR conform mCSD NL. Voor de lokale bevraging op de replica adviseert de IG hetzelfde mCSD-koppelvlak, maar een systeem kan een eigen interface bieden waar de usecase dat vereist.

De centrale IHE mCSD directory is hierop de uitzondering: het LRZa ondersteunt de mCSD-zoekparameters niet volledig en is daarmee geen conforme Directory-actor. De conformiteit op dat punt ligt bij de replica. Zie LRZa als replicatiebron, niet als mCSD Directory-actor.

Afbakening

Voor de niet-functionele eigenschappen van de lokale replica (beschikbaarheid, performance, actualiteit) stelt de generieke functie Adressering geen aanvullende eisen; die bepaalt de zorgaanbieder of de leverancier namens hem. Test- en certificeringsprocedures voor aansluiting lopen via een apart traject en vallen buiten de scope van dit document (zie Conformiteitseisen).

AK-13: Extensible bindings voor codelijsten

Codelijst-elementen in de profielen staan op extensible. Ten behoeve van interoperabiliteit moet echter minimaal één code uit de codelijst aanwezig zijn. Daarnaast is er ruimte voor aanvullende eigen codering.

Overweging

Een gesloten (required) binding garandeert dat iedereen dezelfde codes gebruikt, maar loopt vast zodra een partij een geval heeft dat de lijst niet kent. Een volledig open binding lost dat op, maar dan kan een afnemer nergens meer op rekenen.

In de profielen is een compromis gemodelleerd door een ondergrens vast te leggen zonder de deuren te sluiten: afnemers kunnen op de benoemde codes blijven vertrouwen, terwijl partijen met een specifieke behoefte niet vastlopen. Dat is de bewuste balans tussen interoperabiliteit en openheid, en de uitwerking in de profielen van eis NFR-13: Uitbreidbaarheid.

De concrete bindings en codelijsten staan in de Implementation Guide.

Komt voort uit eis:

NFR-13: Uitbreidbaarheid

AK-14: Keuze voor mCSD NL als directory-standaard (gebaseerd op IHE mCSD)

Context

De generieke functie Adressering heeft een directory-standaard nodig die interoperabiliteit waarborgt. Het principe GF-PRINC-007 (Internationale standaarden) schrijft voor dat we kiezen voor breed geadopteerde, internationale open standaarden.

Opties

- mCSD NL (gebaseerd op IHE mCSD) - NL-profiel gebaseerd op het internationale IHE mCSD profiel voor care services directories
- Eigen FHIR profiel - Zelf definiëren op basis van FHIR R4, maximale vrijheid maar geen internationale community
- Niet-FHIR oplossing - LDAP, REST API, of andere directory-technologie

Rationale

mCSD NL (optie 1). Het NL-profiel is gebaseerd op IHE mCSD, de FHIR-gebaseerde IHE-standaard voor zorgadressen. Door een NL-variant te gebruiken kunnen we NL-specifieke aanpassingen maken terwijl we profiteren van de internationale basis. Dit sluit aan bij het GF-principe van internationale standaarden.

7 Componentenarchitectuur

Dit hoofdstuk beschrijft per component de verantwoordelijkheid, interfaces en afhankelijkheden.

7.1 Data Source Client

Type: voorziening

Deployment: decentraal

Verantwoordelijkheid:

De Data Source Client is het concrete component dat de publicatie naar het LRZa uitvoert; het realiseert de Data Source-rol (zie systeem Data Source). Waar “Data Source” de functionele voorziening van de zorgaanbieder aanduidt, is de Data Source Client de technische component dat de mutaties (Care Services Feed) naar de centrale LRZa Directory stuurt.

Gebruikers

Dit component kan worden ingezet door:

- Zorgaanbieders: direct publiceren van eigen resources
- Softwareleveranciers: publiceren namens zorgaanbieders (via affiliation), onder verantwoordelijkheid van de zorgaanbieder

7.2 Local Replica Directory

Type: voorziening

Deployment: decentraal

Verantwoordelijkheid:

De Local Replica Directory is de mCSD-conforme referentie-invulling van de Adresboek Replica-rol (zie systeem Adresboek Replica): een lokaal FHIR-bevragingspunt dat de geconsolideerde directory gerepliceerd beschikbaar stelt voor lokale toepassingen. Het ontvangt updates via de Update Client (waarmee het samen wordt gedeployed) en realiseert de zoekfuncties uit het globale FO.

Deze invulling als mCSD-Directory is een referentie, geen verplichting. Een afnemer mag de replica ook op een andere technologie baseren (bijvoorbeeld een RDBMS of NoSQL-database), zolang de bevragsingsfunctie voor lokale toepassingen geleverd wordt. De keuze voor de mCSD-vorm heeft als voordeel dat dezelfde mCSD-query-interface lokaal beschikbaar is als bij het centrale LRZa.

Zoekfunctionaliteit

Welke zoekmogelijkheden de replica aanbiedt is — net als de rest van de invulling — aan de afnemer. De mCSD-query-interface uit de mCSD NL IG vormt de referentie voor veelvoorkomende usecases (zoeken op organisatie, locatie, service en endpoint). Een afnemer mag de zoekfunctionaliteit uitbreiden of anders vormgeven, bijvoorbeeld met een alternatieve interface (zoals OData, GraphQL of een eigen API) bovenop de gerepliceerde data; de gerepliceerde gegevens zelf wijzigen daardoor niet. Een leverancier die nu al een OData-koppeling aanbiedt kan die dus lokaal blijven aanbieden. Alleen het koppelvlak met het LRZa is FHIR/mCSD (zie LRZa Directory).

7.3 LRZa Directory

Type: dienst

Deployment: centraal

Verantwoordelijkheid:

De LRZa Directory is de centrale, publieke FHIR-API conform IHE mCSD die de geconsolideerde directory beschikbaar stelt. Het bewaart zowel de huidige als historische registraties, zodat afnemers via delta-synchronisatie alleen de wijzigingen hoeven op te halen.

Schrijven en lezen

De LRZa Directory biedt twee duidelijk gescheiden interacties aan:

- Schrijven (write): de Data Source Client publiceert mutaties van zorgaanbieders/leveranciers via de Care Services Feed. Bronregistergegevens (KvK, UZI/DEZI) worden centraal aan de directory toegevoegd.
- Lezen (read): de Update Client haalt periodiek delta's op om de decentrale replica's actueel te houden.

Beide interacties met het LRZa verlopen uitsluitend via FHIR conform mCSD NL; lokale bevragsingsinterfaces op de eigen replica zijn vrij (zie Local Replica Directory).

Niet voor directe bevraging

De LRZa Directory is nadrukkelijk niet bedoeld voor directe bevraging door een XIS/EPD. Bevragingen lopen via de decentrale replica's (zie Decentrale replica's met periodieke synchronisatie); directe bevraging zou de leesbeschikbaarheid afhankelijk maken van het centrale systeem. De query-interface van de LRZa Directory wordt daarom beperkt tot wat voor synchronisatie nodig is, om de kans op implementatiefouten te verkleinen.

7.4 LRZa Portaal

Type: voorziening

Deployment: centraal

Verantwoordelijkheid:

Webportaal waar bevoegde medewerkers van zorgaanbieders autorisaties voor het gebruik van de LRZa GFA API voor hun IT-dienstverleners kunnen vastleggen.

7.5 Query Client

Type: voorziening

Deployment: decentraal

Verantwoordelijkheid:

De Query Client is de component binnen het XIS/EPD waarmee een zorgverlener adressen van andere zorgaanbieders opzoekt. Het bevraagt de decentrale Adresboek Replica (zie Adresboek Replica) — niet het centrale LRZa rechtstreeks — en profiteert zo van de lokale leesbeschikbaarheid.

De Query Client is een afnemer van de generieke functie Adressering: het maakt gebruik van de mCSD-query-interface die de replica aanbiedt, maar is geen onderdeel van de generieke functie Adressering zelf.

7.6 Update Client

Type: voorziening

Deployment: decentraal

Verantwoordelijkheid:

De Update Client is de synchronisatie-motor van de Adresboek Replica: het haalt periodiek de wijzigingen (delta's) op bij de centrale LRZa Directory en schrijft deze naar de Local Replica Directory. Het maakt gebruik van het delta-synchronisatiemechanisme conform mCSD NL (gebaseerd op IHE mCSD)¹.

De Update Client en de Local Replica Directory zijn in de referentie-architectuur twee aparte componenten met elk een eigen verantwoordelijkheid — synchroniseren respectievelijk bevragen — maar worden samen gedeployed als onderdeel van de Adresboek Replica (zie Adresboek Replica). Dit onderscheid is een referentie-invulling; een implementatie mag de twee functies combineren.

De Update Client is een rol; aggregatie behoort niet tot de taken daarvan. Aggregatie en conflictresolutie vinden centraal plaats in het LRZa (zie Centrale aggregatie); de Update Client kopieert uitsluitend de reeds geconsolideerde directory.

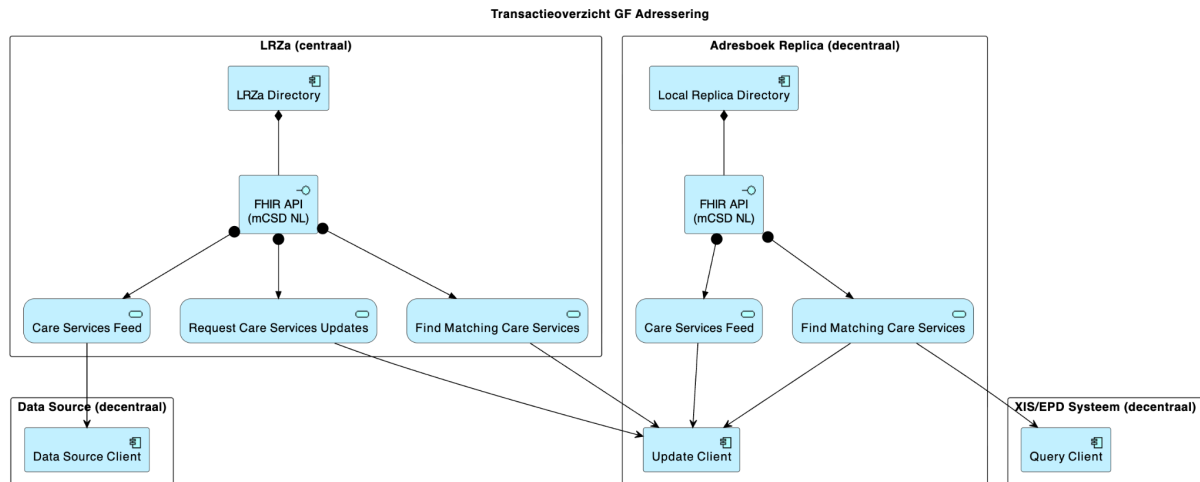
¹ De Update Client initieert beide richtingen zelf: het ophalen bij de centrale LRZa Directory en het wegschrijven in de Local Replica Directory. De volgorde van de stappen staat in de sequentiediagrammen van de Implementation Guide: initial load en incrementele synchronisatie.

8 Interfaces en transacties

Dit hoofdstuk beschrijft de transacties en koppelvlakken binnen de generieke functie Adressering.

8.1 Transactieoverzicht

Het onderstaande diagram toont de transacties tussen de componenten.



Figuur: Transactieoverzicht generieke functie Adressering

8.2 Transacties

Alle transacties zijn gebaseerd op de specificaties in de Implementation Guide.

8.2.1 Care Services Feed (Publiceer wijzigingen)

Aangeboden door

LRZa Directory, Local Replica Directory

Afgenomen door

Data Source Client, Update Client

Omschrijving

Feed transactie waarmee bronnen wijzigingen kunnen doorvoeren in een mCSD directory.

8.2.2 Find Matching Care Services (Zoek zorgdiensten)

Aangeboden door

LRZa Directory, Local Replica Directory

Afgenomen door

Query Client, Update Client

Omschrijving

Query-transactie voor het zoeken naar zorgaanbieders, locaties en diensten in een mCSD directory. Ondersteunt FHIR-search operaties op Organization, Location, HealthcareService en Endpoint resources.

Op de lokale replica is deze transactie volledig beschikbaar; daar vindt het zoeken en matchen plaats. Op de LRZa Directory is zij beperkt tot wat voor replicatie nodig is (zoeken op identifier) en dus niet bedoeld voor bevraging in het primaire proces. Zie LRZa als replicatiebron, niet als mCSD Directory-actor.

8.2.3 Request Care Services Updates (Synchroniseer wijzigingen)

Aangeboden door

LRZa Directory

Afgenomen door

Update Client

Omschrijving

Bulk update transactie voor het ophalen van wijzigingen sinds een vorige synchronisatie. Gebruikt FHIR history interacties om delta's op te halen. Essentieel voor deployments met decentrale replica's die gesynchroniseerd moeten worden.

De normatieve uitwerking — initial load met paging, delta-synchronisatie via `_history`, foutafhandeling en retentie van teruggetrokken resources — is gespecificeerd in de Implementation Guide.

9 Informatiemodel en databronnen

Dit hoofdstuk beschrijft het informatiemodel, de databronnen en data-aggregatie voor de generieke functie Adressering.

9.1 Informatiemodel

Het informatiemodel volgt het canonieke mCSD-datamodel. Als vuistregel voor de modellering geldt: een Organization is een organisatorische eenheid met eigen verantwoordelijkheid (zorgaanbieder, afdeling of sub-organisatie via de partOf-hiërarchie); een Location is een fysieke plek waar zorg wordt geleverd (vestiging, gebouw, praktijkruimte); een HealthcareService is een aangeboden zorgdienst, los van de plek waar die geleverd wordt. Eén entiteit kan meerdere resources opleveren (een afdeling met eigen vestigingsadres is zowel Organization als Location). De onderlinge relaties tussen de resources (bijvoorbeeld de partOf-hiërarchie tussen organisaties en de verwijzing van een HealthcareService naar Organization en Location) volgen uit hetzelfde model.

De normatieve profilering, de cardinaliteiten en de verdere modelleerrichtlijnen op veldniveau staan in de Implementation Guide; het technisch ontwerp herhaalt die bewust niet, om één bron te houden. Zie de entiteiten in de Implementation Guide.

9.1.1 Endpoint Resource

Een Endpoint-resource beschrijft een technisch koppelvlak waarlangs gegevensuitwisseling tussen systemen plaatsvindt. Het legt vast waar een systeem te bereiken is en met welke techniek daar uitgewisseld wordt: het verbindingstype en de soorten gegevens (payloadtypes) die het koppelvlak ondersteunt. Eén Endpoint-resource kan meerdere payloadtypes voeren; waar payloadtypes een verschillend verbindingstype vereisen, worden daarvoor afzonderlijke Endpoint-resources geregistreerd.

Een endpoint hoort bij het achterliggende systeem van een zorgaanbieder en kan door meerdere organisatieonderdelen worden gebruikt; omgekeerd kan één organisatieonderdeel via meerdere

endpoints bereikbaar zijn. Voor organisatieonderdelen geldt dat alleen organisatieonderdelen (Organization-resources) met een URA-identificatie een referentie naar een Endpoint-resource kunnen bevatten. Daarnaast kunnen HealthcareService-resources een referentie naar een Endpoint-resource bevatten. Naast de reguliere levensloopstatus kan een endpoint afgeschermd zijn, zodat het alleen vindbaar en bruikbaar is voor een specifiek uitwisselingssysteem of type uitwisseling.

Of, en wanneer, achter een endpoint plaats is voor een uitwisseling valt buiten de generieke functie Adressering; het endpoint zegt waar en waarvoor een systeem te bereiken is, niet of het beschikbaar is.

De exacte wijze waarop een endpoint moet worden gebruikt valt buiten de generieke functie Adressering; het endpoint zegt welk verbindingstype en welke soorten gegevens het ondersteunt, niet hoe bijvoorbeeld identificatie, authenticatie en autorisatie dienen te worden ingevuld.

9.1.2 HealthcareService Resource

Beschrijft welke zorgdiensten een organisatie aanbiedt.

Een HealthcareService-resource bevat een providedBy-referentie naar een Organization-resource. Er kan alleen worden gerefereerd naar een Organization-resource die een URA heeft, of naar een Organization-resource die via partOf-referenties een Organization met een URA als voorouder heeft.

9.1.3 Location Resource

Representeert fysieke vestigingsadressen en praktijklocaties. Maakt locatie gericht zoeken naar zorgaanbieders en tonen contactgegevens per locatie mogelijk.

De vestigingen die het LRZa uit het KvK Handelsregister overneemt (Vestigingen) komen in het LRZa terug als Location-resources. Wanneer een zorgaanbieder ervoor heeft gekozen om URA-nummers toe te kennen aan een vestiging dan komt deze vestiging in het LRZa terug als Location-resource én als Organization-resource. Partijen zijn daarnaast vrij om extra locaties aan te maken die niet uit het KvK Handelsregister volgen (bijvoorbeeld een praktijkruimte zonder eigen vestigingsadres).

De identificatie van de zorgaanbieder (URA) zit in het mCSD-model op de Organization-resource (Organization), niet op de Location-resource. Een Location-resource beschrijft een fysieke plek. Welke organisatie op die plek zorg levert, volgt uit de koppeling met een Organization Resource. Het URA identificeert een in het UZI-register opgenomen organisatie of organisatieonderdeel, niet een locatie.

9.1.4 Organization Resource

Kernentiteit voor organisatie-identificatie. Bevat kern identifiers voor zorgaanbieders zoals het KvK-nummer en URA (UZI-Register Abonnummer). Ondersteunt uitbouw van organisatiestructuur met afdelingen via partOf-hiërarchie.

Per zorgaanbieder is er één hoofd-Organization, geïdentificeerd door het KvK-nummer en, afhankelijk van de manier waarop de zorgaanbieder zichzelf in het UZI-register heeft geregistreerd, de URA. We onderscheiden twee opties:

- Wanneer de zorgaanbieder een URA-nummer heeft toegekend aan de rechtspersoon van die zorgaanbieder (te herkennen aan een 8-cijferig KvK-nummer) dan wordt de hoofd-Organization geïdentificeerd door KvK-nummer en URA.
- Wanneer de zorgaanbieder een URA-nummer heeft toegekend aan een of meerdere vestigingen van die zorgaanbieder (te herkennen aan een 12-cijferig KvK-vestigingsnummer) dan wordt de hoofd-Organization geïdentificeerd door alleen het KvK-nummer.

Onderliggende organisatieonderdelen zoals afdelingen of sub-organisaties worden als aanvullende Organization-resources gemodelleerd die via partOf naar de hoofd-Organization verwijzen. Meerdere IT-leveranciers kunnen voor dezelfde zorgaanbieder gegevens beheren; zij doen dat namens de hoofd-Organization (zie OrganizationAffiliation en gedelegeerde registratie).

9.1.5 OrganizationAffiliation Resource

Legt de relatie vast tussen een zorgaanbieder en een dienstverlener die namens die zorgaanbieder adresgegevens registreert. Op basis daarvan stelt het LRZa vast of een leverancier bevoegd is om namens een zorgaanbieder te publiceren. Het mandaat is raadpleegbaar zodat het LRZa kan controleren of een leverancier gemandateerd is; dat is nodig om de herkomst van door een leverancier ondertekende mutaties te kunnen verifiëren (Optionele ondertekening van mutaties met Provenance). De keuze voor het gebruik van de OrganizationAffiliation-resource als oplossing voor mandatering wordt heroverwogen wanneer de generieke functie Autorisatie een stelselbrede oplossing voor mandatering definieert.

De gemandateerde leverancier wordt hierin als organisatie vastgelegd via zijn KvK-nummer, langs dezelfde lijn als waarmee hij de API benadert: een organisatiegebonden certificaat op KvK-nummer (Organisatiegebonden certificaten voor API-toegang).

Samenwerkingsverbanden worden hier niet mee gemodelleerd. Een samenwerkingsverband dat zelf als zorgaanbieder is georganiseerd, is een gewone Organization met eigen locaties, zorgdiensten en endpoints; de relatie tussen zo'n samenwerkingsverband en zijn leden valt buiten de generieke functie Adressering.

9.2 Databronnen

De volgende externe bronnen leveren data aan de generieke functie Adressering en zijn leidend voor de betreffende gegevens.

9.2.1 Kamer van Koophandel (KvK)

Handelsregister van de Kamer van Koophandel. Autoritatieve bron voor organisatie-identificatie (KvK-nummer), statutaire naam, vestigingsadressen en SBI-codes van Nederlandse ondernemingen.

9.2.2 UZI/DEZI

UZI-register (en opvolger DEZI), beheerd door CIBG. Autoritatieve bron voor zorgaanbieder-identificatie (URA).

9.2.3 Zorgaanbieder (zelfregistratie)

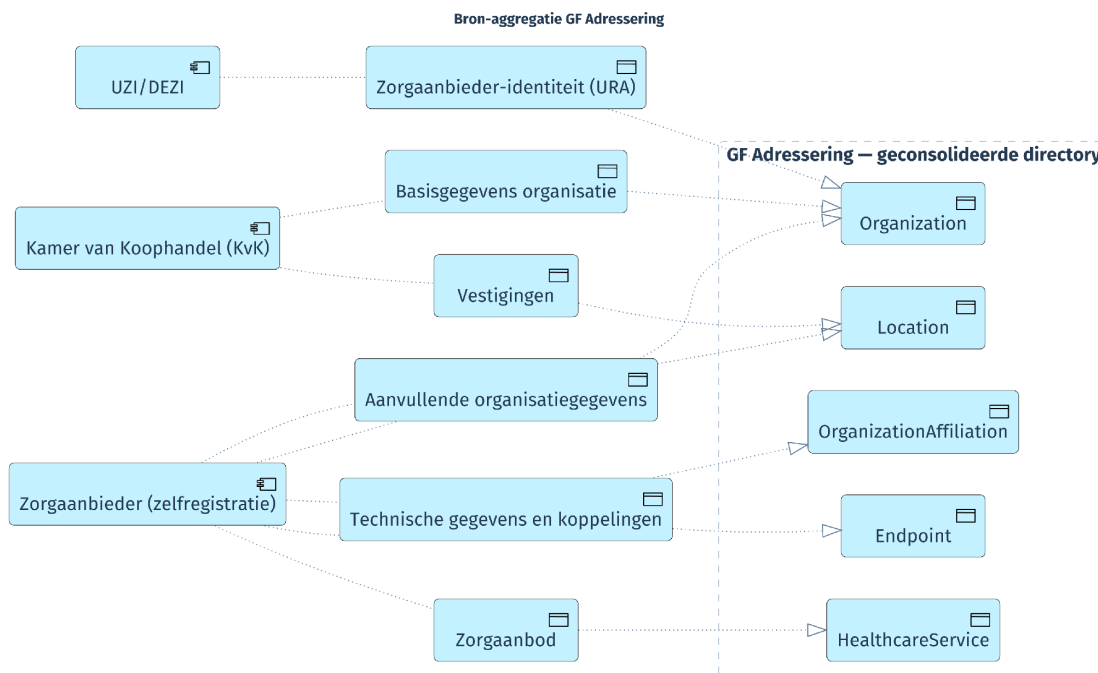
Gegevens die de zorgaanbieder (of de daarvoor aangewezen IT-dienstverlener) zelf beheert via het LRZa. Autoritatieve bron voor organisatie-specifieke gegevens zoals afdelingen, endpoints en healthcareservices.

9.3 Data-aggregatie

De volgende componenten aggregeren data uit bronnen of andere componenten:

Component	Haalt data van
LRZa Directory	Kamer van Koophandel (KvK), Zorgaanbieder (zelfregistratie), UZI/DEZI
Update Client	LRZa Directory

Het onderstaande diagram toont per bron welke gegevens deze aanlevert (in eigen termen) en hoe die mappen op de resources die in de generieke functie Adressering tot één geconsolideerde directory worden samengebracht².



Figuur: Bron-aggregatie generieke functie Adressering

10 Security op hoofdlijnen

Dit hoofdstuk beschrijft de security-architectuur op hoofdlijnen.

10.1 Gedelegeerde registratie via leverancier

Omschrijving

Leveranciers worden als expliciete actor opgenomen in het stelsel. Een leverancier authenticceert als zichzelf bij het LRZa en kan namens zorgaanbieders data registreren.

² Dit is een globaal overzicht van de mapping per bron. Onderlinge verwijzingen tussen de resources (zoals een HealthcareService die bij een Location hoort) vallen buiten dit diagram; de gedetailleerde mapping staat in de Implementation Guide.

Rationale

In de praktijk beheren softwareleveranciers vaak de technische aansluiting namens zorgaanbieders. Door leveranciers expliciet te ondersteunen wordt dit geformaliseerd en controleerbaar.

Implicaties

- Leveranciers hebben eigen identiteit in het stelsel
- Zorgaanbieders behouden controle via expliciete autorisatie
- Audit trail toont welke leverancier namens welke zorgaanbieder heeft gehandeld
- Meerdere leveranciers kunnen onafhankelijk van elkaar namens dezelfde zorgaanbieder opereren
- Geen leverancier heeft exclusieve controle over de adresgegevens van een zorgaanbieder

10.2 Optionele ondertekening van mutaties met Provenance

Context

In het centrale push-model (architectuurkeuze AK-06: Centraal push-model met read-only replica's) levert een bron (zorgaanbieder of leverancier) een mutatie aan bij het LRZa, dat de gezaghebbende stand bijwerkt. Wat ontbreekt is een mechanisme waarmee achteraf, onafhankelijk van de beheerder, te verifiëren is door welke partij een mutatie is aangeleverd en dat de inhoud sindsdien niet is gewijzigd. Die onafhankelijke verifieerbaarheid is de eis uit NFR-15: Onafhankelijk verifieerbare herkomst van adresgegevens.

Besluit

Om verificatie mogelijk te maken kan een mutatie worden voorzien van een ondertekende FHIR Provenance-resource. Die Provenance-resource wordt naast de gemuteerde FHIR-resource gepubliceerd.

- De Provenance wordt na registratie van de mutatie opgesteld en verwijst naar de definitieve resource-versie. Zij wordt ondertekend met een organisatiegebonden certificaat (PKIoverheid of, waar geen PKIoverheid-certificaat beschikbaar is, UZI).
- Ondertekende Provenance-records worden in het LRZa bewaard en meegerepliceerd naar de replica's, zodat de bewijsketen decentraal beschikbaar is.
- Het LRZa verifieert een aangeboden ondertekening tegen de trust-keten (PKIoverheid/UZI); een replica, auditor of toezichthouder kan dat later eveneens doen.
- Wanneer een leverancier namens een zorgaanbieder muteert, is de ondertekening alleen te vertrouwen als vaststaat dat die leverancier gemandateerd was. Het mandaat (de OrganizationAffiliation Resource) wordt daarom publiek vastgelegd, zodat elke verifiërende partij kan controleren dat de ondertekenende partij bevoegd was namens de zorgaanbieder. Zonder dat publieke mandaat is de herkomst van zo'n mutatie niet onafhankelijk vast te stellen.

Voor een volledig sluitende verificatie vereist deze oplossing dat zorgaanbieders hun samenwerking met leveranciers via de Affiliation ondertekenen met een UZI-certificaat. Omdat het beheer van dergelijke certificaten niet voor alle (met name kleinere) zorgaanbieders haalbaar of beschikbaar is, is dit optioneel.

Zodra ondertekenmiddelen breder beschikbaar komen (bijvoorbeeld een EU-wallet) kan deze keuze worden herzien.

Dit betekent wel dat organisaties die niet ondertekenen dus niet op onafhankelijk verifieerbare herkomst van adresgegevens gecontroleerd kunnen worden. Hierbij moet dan van vertrouwen in de beheerder van het LRZa worden uitgegaan.

Afbakening

Het LRZa-portaal blijft bestaan: mandaten en mutaties kunnen ook via het portaal worden beheerd, waarbij authenticatie via eHerkenning op organisatieniveau verloopt (zie Organisatiegebonden certificaten voor API-toegang).

De precieze invulling van de Provenance (velden, canonicalisatie) en het OCSP/CRL-beleid zijn een uitwerking in de Implementation Guide.

Consequenties

- Bronnen die ondertekenen, gebruiken hun bestaande PKI-overheid-certificaten voor ondertekening op recordniveau; dat vraagt implementatiewerk.
- Ondertekening is optioneel, dus niet elke mutatie in het LRZa draagt een bewijs van herkomst. Afnemers kunnen alleen voor ondertekende mutaties de herkomst onafhankelijk vaststellen.
- Het stelsel moet omgaan met certificaatverloop en revocatie; het intrekken van een certificaat werkt door via de reguliere synchronisatie.

Komt voort uit eis:

NFR-15: Onafhankelijk verifieerbare herkomst van adresgegevens

10.3 Organisatiegebonden certificaten voor API-toegang

Omschrijving

Toegang tot de LRZa-API verloopt via organisatiegebonden certificaten: PKI-overheid-certificaten en UZI-servercertificaten.

Overweging

Een certificaat is organisatiegebonden en identificeert daarmee de partij die de API aanroept. Dat is wat Authenticeren als zichzelf nodig heeft: elke partij roept aan met haar eigen certificaat, dus ook een leverancier die namens een zorgaanbieder aanlevert.

De twee soorten sluiten aan op wie er aanroept. Een UZI-servercertificaat bevat het URA-nummer en identificeert daarmee een zorgaanbieder. Een PKI-overheid-certificaat bevat het KvK-nummer en identificeert een organisatie in bredere zin; dat is wat een leverancier nodig heeft, die immers geen URA heeft. Beide leggen de identiteit van de organisatie vast in het certificaat zelf, zodat het LRZa die niet uit de aanroep hoeft af te leiden. Waar over een PKI-overheid-certificaat wordt gesproken, gaat het steeds om een organisatiegebonden certificaat; persoonsgebonden certificaten voor beheerders zijn niet voorzien.

Dat een leverancier namens een zorgaanbieder mag aanleveren is een autorisatievraag, die losstaat van het certificaat waarmee wordt aangeroepen.

Afbakening

Deze keuze gaat over de API. Toegang tot het LRZa-portaal verloopt via eHerkenning op organisatieniveau; dat valt buiten deze keuze.

Komt voort uit eis:

NFR-14: Authenticeren als zichzelf

11 Non-functional requirements

Dit hoofdstuk beschrijft de niet-functionele eisen, waaronder beschikbaarheid, performance en schaalbaarheid.

11.1 Registratie & bronnen

11.1.1 NFR-01: Leidende bronnen alleen met beheerrelatie

Gegevens die het LRZa zelf uit externe registers overneemt en publiceert, komen uitsluitend uit registers waarmee de Beheerder een beheerrelatie heeft. Alleen dan zijn afspraken over actualiteit, kwaliteit en beschikbaarheid te maken en af te dwingen.

Deze eis gaat over de gegevens die het LRZa actief ontsluit. Zij raakt niet aan de gegevens die zorgaanbieders en leveranciers zelf publiceren; daarvoor ligt de verantwoordelijkheid bij de publicerende partij. Het onderscheid zit in wie het gegeven kan vullen: de identifiers uit de leidende bronregisters (KvK-nummer en URA) neemt het LRZa over uit die registers, en een zorgaanbieder of leverancier kan ze niet zelf zetten of wijzigen. Een identifier uit een register zonder beheerrelatie registreert de publicerende partij zelf; het LRZa vult die niet en controleert de inhoud ervan niet.

Rationale

Een leidend bronregister bepaalt mede de kwaliteit van de adressering. Neemt het LRZa gegevens over uit een register waarover de beheerder niets te zeggen heeft, dan belooft het een kwaliteit die het niet kan waarmaken: bij fouten of vertraging is er geen route om correctie af te dwingen. De verantwoordelijkheid ligt dan bij een partij buiten de invloedssfeer van de beheerder, terwijl de afnemer het LRZa aanspreekt.

Door de leidende bronnen te beperken tot registers met een beheerrelatie blijft de keten van verantwoordelijkheid sluitend. Dat sluit aanvullende registraties niet uit; aan het identifier-systeem is te zien of een gegeven uit een leidend bronregister komt of door de publicerende partij zelf is aangeleverd. Zie eis NFR-13: Uitbreidbaarheid voor de ruimte die het model laat voor aanvullende identifiers.

11.1.2 NFR-02: Onafhankelijke adresgegevenspublicatie

Elke leverancier die namens een zorgaanbieder adresgegevens publiceert, moet dit kunnen doen zonder technische of procedurele afhankelijkheid van andere leveranciers die dezelfde zorgaanbieder bedienen.

Rationale

Zorgaanbieders werken vaak met meerdere leveranciers (EPD, lab-systeem, apotheeksysteem). Zonder deze eis kan een situatie ontstaan waarin:

- Leverancier A de publicatie van leverancier B kan blokkeren of vertragen
- Een zorgaanbieder “gevangen” zit bij één leverancier voor adresgegevensbeheer
- Concurrerende leveranciers onderling moeten samenwerken wat tot fricties leidt

Zie ook: Gedelegeerde registratie via leverancier · LRZa als centraal consolidatie- en distributiepunt

11.1.3 NFR-03: Ondersteuning complexe IT-landschappen

De architectuur ondersteunt zorgaanbieders met complexe IT-landschappen door aggregatie van adresgegevens uit meerdere achterliggende systemen toe te staan. Een Data Source kan namens een zorgaanbieder gegevens bundelen en publiceren, ongeacht of deze uit één of meerdere bronnen

afkomstig zijn. Voor het LRZa is dit transparant; de zorgaanbieder blijft verantwoordelijk en behoudt keuzevrijheid in hoe de aanlevering wordt georganiseerd.

Voorbeeld

Een zorgaanbieder met meerdere IT-leveranciers (EPD, labsysteem, PACS) kan via een integratiedienst alle adresgegevens laten bundelen en als één geheel aanleveren bij het LRZa, zonder dat elke leverancier afzonderlijk hoeft aan te sluiten. Die integratiedienst kan een externe leverancier zijn, maar evengoed een eigen interne voorziening; de architectuur schrijft dat niet voor.

Rationale

Complexe zorgorganisaties hebben vaak tientallen systemen van verschillende leveranciers. Door aggregatie toe te staan kunnen zij zelf kiezen hoe ze hun aanlevering organiseren, wat de adoptiedrempel verlaagt.

Zie ook:

Data Source als enkelvoudig aanspreekpunt

11.2 Consolidatie & distributie

11.2.1 NFR-04: Consistentie

De generieke functie Adressering data moet consistent zijn met de authentieke bronregisters (KvK, UZI).

Rationale

Inconsistente gegevens leiden tot fouten in de adressering en kunnen medische fouten veroorzaken wanneer gegevens naar de verkeerde ontvanger worden gestuurd.

11.2.2 NFR-05: Eenduidige uitkomst per mutatie

Elke mutatie binnen de GFA moet een eenduidige, direct bekende uitkomst hebben: zij wordt geheel geaccepteerd of geheel geweigerd. Bij weigering is de reden voor de bron kenbaar. Een mutatie mag niet stil verdwijnen of in een onbepaalde tussentoestand blijven hangen.

Rationale

Wanneer mutaties, bijvoorbeeld een aanpassing aan een endpoint, niet verwerkt worden dan heeft dit tot gevolg dat er een gedeeld beeld ontstaat (Gedeeld gezaghebbend beeld). Er is dan een systeem dat de mutatie gedaan heeft/ wil doen en een of meer andere systemen die deze weigeren over te nemen.

Het moet dus voor een muterend systeem direct duidelijk zijn dat diens mutatie geweigerd dan wel geaccepteerd wordt. Hierbij is ook informatie nodig over de reden van weigering zodat het systeem, of de beheerder/ gebruiker ervan, tot actie kan overgaan en zo nodig gericht opnieuw aanleveren van (een deel van de) gegevens.

Zie ook:

Architectuurkeuze AK-06: Centraal push-model met read-only replica's

11.2.3 NFR-06: Gedeeld gezaghebbend beeld

Alle afnemers moeten, afgezien van replicatievertraging, hetzelfde beeld van de adresgegevens zien. Er mag geen inhoudelijke divergentie tussen replica's bestaan: het enige toegestane verschil tussen twee replica's is verschil in actualiteit, niet in de uitkomst van aggregatie of conflictresolutie.

Rationale

Doordat partijen verschillende implementaties hebben van delen van de GFA kan het mogelijk zijn dat hierdoor een verschillend beeld ontstaat. Voor een zorgverlener kan dit problematisch zijn omdat hierdoor een uitwisseling problemen kan geven. In een dergelijk geval kan het dan lastig zijn te achterhalen waar/ in welk systeem gegevens verkeerd geregistreerd staan.

Een gedeeld beeld voorkomt dat het antwoord op een adresvraag afhangt van welke replica de afnemer toevallig gebruikt.

Zie ook:

Architectuurkeuze AK-06: Centraal push-model met read-only replica's

11.2.4 NFR-07: Schaalbaarheid

De architectuur van de generieke functie Adressering moet schaalbaarheid ondersteunen om groei in aantal zorgaanbieders en query-volume te accommoderen.

Rationale

Het aantal aangesloten zorgaanbieders en het gebruik van de adresseringsfunctie zal naar verwachting groeien naarmate meer zorgtoepassingen aansluiten.

Synchronisatielast en piekspreiding

Doordat de plaatsing van de replica vrij is, kan de synchronisatie met het LRZa in veel decentrale instantiaties plaatsvinden (tot op het niveau van een individuele applicatie-installatie). De synchronisatie is echter laagfrequent en delta-gebaseerd: na de initiële lading haalt een Update Client via `_history` alleen de wijzigingen sinds de vorige ronde op, wat doorgaans een klein of leeg antwoord oplevert. De gemiddelde belasting op het LRZa blijft daardoor beperkt; het werkelijke aandachtspunt is gelijktijdigheid, niet de hoeveelheid werk.

Piekbestendigheid is primair een capaciteitseigenschap van het centrale LRZa (horizontaal schalen, caching, rate-limiting) en wordt als zodanig in de SLA van het LRZa belegd. Aan de client-zijde geldt als aanbeveling dat Update Clients hun synchronisatiemoment over het interval spreiden in plaats van op vaste kloktijden te synchroniseren, zodat een zelf veroorzaakte gelijktijdigheidspiek wordt voorkomen. De normatieve invulling hiervan (spreiding en het omgaan met rate-limiting) staat in de mCSD NL IG.

11.3 Raadplegen & vindbaarheid**11.3.1 NFR-08: Beschikbaarheid**

De architectuur van de generieke functie Adressering moet hoge beschikbaarheid mogelijk maken zodat zorgprocessen niet verstoord worden door uitval van adresseringscomponenten.

Rationale

Zorgprocessen zijn afhankelijk van het kunnen vinden van zorgaanbieders. Wanneer adresseringscomponenten niet beschikbaar zijn, kunnen urgente medische gegevensuitwisselingen niet plaatsvinden.

Zie ook:

Decentrale replica's met periodieke synchronisatie

11.3.2 NFR-09: Geen centrale afhankelijkheid bij raadplegen

Het raadplegen van adresgegevens mag niet afhangen van de beschikbaarheid van één centrale voorziening. Het zoeken en matchen gebeurt daarom op de lokale replica; het centrale LRZa is ingericht op replicatie en niet op operationele bevraging.

Afnemers bevragen hun eigen replica. Het LRZa stelt de gegevens beschikbaar waarmee die replica zich vult en bijwerkt, en is niet bedoeld als zoekingang voor het raadplegen van adresgegevens in het primaire proces. Dit geldt zowel voor zoeken op een identifier als voor zoeken op kenmerken, zoals het tonen van alle zorgaanbieders die een bepaalde dienst leveren binnen een straal.

Rationale

Zou het LRZa de zoekingang voor het primaire proces zijn, dan is het een single point of failure voor de hele zorg: bij uitval kan niemand meer een zorgaanbieder of endpoint vinden. Door het zoeken decentraal te beleggen blijft adressering werken zolang de eigen replica draait, ook als het LRZa onbereikbaar is. De replica loopt dan hooguit achter op de laatste mutaties.

Dat het centrale register hierdoor ook minder leesbelasting krijgt is een gunstig neveneffect, niet de reden voor deze eis. Zie Beschikbaarheid voor de algemene beschikbaarheidseis.

11.3.3 NFR-10: Performance

De architectuur van de generieke functie Adressering moet voldoende performance mogelijk maken voor zorgprocessen, waaronder spoedsituaties.

Deze eis gaat over het bevragen: het opzoeken van een adres gebeurt op de Local Replica Directory en moet daar snel genoeg zijn voor het zorgproces waarin de zorgverlener staat. Muteren en synchroniseren kennen deze eis niet. Een mutatie naar het LRZa en de periodieke synchronisatie van een replica staan los van het moment waarop een zorgverlener een adres nodig heeft; het LRZa hoeft daarvoor geen spoedafhandeling te ondersteunen.

Rationale

Zorgprocessen vereisen (soms) snelle responses. Te lange wachttijden verstoren de werkprocessen van zorgverleners en kunnen de patiëntveiligheid beïnvloeden bij urgente situaties. Doordat het zoeken decentraal is belegd (zie eis NFR-09: Geen centrale afhankelijkheid bij raadplegen), is de responstijd bij een bevraging een eigenschap van de lokale replica en niet van het centrale register.

11.3.4 NFR-11: Verscheidenheid aan inrichtingen en bevragingsmodellen

De generieke functie Adressering moet uiteenlopende inrichtingen en bevragingsmodellen ondersteunen, zodat het passend is voor organisaties van verschillende omvang en voor verschillende usecases. De architectuur schrijft de plaatsing, de techniek en de niet-functionele eigenschappen van de decentrale voorzieningen niet voor; die bepaalt de zorgaanbieder zelf. Dit geldt aan de publicatiekant (Data Source) en aan de bevragingskant (Adresboek Replica).

Rationale

Het zorgveld loopt uiteen van een solistisch werkende zorgverlener tot een academisch centrum met een eigen integratieafdeling. Eén voorgeschreven inrichting zou voor een groot deel van dat veld niet passen en de adoptie belemmeren.

De vrijheid in plaatsing stelt leveranciers bovendien in staat de zorgaanbieder te ontzorgen: aan de publicatiekant door via gedelegeerde registratie namens de zorgaanbieder te publiceren (Gedelegeerde registratie via leverancier), aan de bevragingskant door de replica als functie in een

bestaand systeem te integreren. Een zorgaanbieder hoeft daardoor in de praktijk geen aparte adresboek-infrastructuur te kiezen of te beheren. De generieke functie Adressering verplicht leveranciers niet het zo in te vullen, maar is er expliciet op ingericht dat zij dit kunnen doen. Deze eis gaat over de verscheidenheid tussen zorgaanbieders en usecases. De complexiteit binnen één zorgaanbieder, waarbij gegevens uit meerdere achterliggende systemen worden gebundeld, staat in Ondersteuning complexe IT-landschappen.

11.4 Interoperabiliteit & standaarden

11.4.1 NFR-12: Interoperabiliteit

De architectuur van de generieke functie Adressering moet interoperabiliteit waarborgen zodat zowel nieuwe als bestaande zorgsystemen kunnen koppelen via gestandaardiseerde interfaces.

Rationale

Door gebruik van open standaarden kunnen alle systemen aansluiten, ongeacht hun technische implementatie.

Zie ook:

Keuze voor mCSD NL als directory-standaard (gebaseerd op IHE mCSD)

11.4.2 NFR-13: Uitbreidbaarheid

De architectuur van de generieke functie Adressering moet uitbreidbaar zijn om toekomstige zorgdomeinen en usecases te ondersteunen zonder fundamentele wijzigingen.

Rationale

Het zorglandschap evolueert continu. Nieuwe zorgdomeinen, nieuwe typen endpoints en nieuwe protocollen en gegevenscategorieën moeten zonder impactvolle wijzigingen kunnen worden toegevoegd.

Zie ook:

- architectuurkeuze AK-03: Leidend bronregister versus aanvullende identifier
- architectuurkeuze AK-04: Leidende bronregisters van het LRZa

11.5 Beveiliging & vertrouwen

11.5.1 NFR-14: Authenticeren als zichzelf

Elke partij die met het LRZa communiceert authenticereert zich waar mogelijk als zichzelf, met een eigen (organisatiegebonden) middel.

Het LRZa stelt bij elke aanlevering en beheerhandeling vast welke organisatie de handeling uitvoert, en legt die identiteit vast bij de gegevens. De vastgestelde identiteit is die van de handelende partij zelf: handelt een leverancier namens een zorgaanbieder, dan stelt het LRZa de leverancier vast en niet de zorgaanbieder.

Rationale

Zonder deze eis is achteraf niet vast te stellen wie gegevens heeft aangeleverd of gewijzigd. Dat is nodig om aanleveringen te kunnen herleiden, en om toegang van één partij te kunnen intrekken zonder andere partijen te raken.

11.5.2 NFR-15: Onafhankelijk verifieerbare herkomst van adresgegevens

De herkomst en integriteit van een adresgegevens moeten door een afnemer vast te stellen zijn. Een afnemer moet kunnen bepalen door welke partij een gegeven is aangeleverd en kunnen verifiëren dat dit gegeven sindsdien niet is gewijzigd.

Rationale

Adresgegevens zoals endpoints sturen waar zorggegevens naartoe gaan; een onopgemerkt gewijzigd of vervalst gegeven kan gevolgen hebben voor de overdracht van (medische) gegevens.

De architectuur dient adresgegevens technisch verifieerbaar te maken, zodat een afnemer de herkomst en integriteit kan controleren.

11.5.3 NFR-16: Wettelijke grondslag voor gegevensverwerking

Het juridisch kader van de generieke functie Adressering is beschreven in hoofdstuk 5 van het functioneel ontwerp.

Zie ook:

Zorgverleners niet opnemen in het LRZa

12 Begrippenlijst

Beheerder

De stelselpartij die verantwoordelijk is voor het LRZa en zijn gegevens: CIBG, in opdracht van VWS. De beheerder maakt en handhaaft de afspraken met leidende bronregisters.

Bron: VWS

Centraal

Aanduiding dat één aanwijsbare stelselpartij verantwoordelijk is voor een functie of gegevensverzameling; verwijst naar verantwoordelijkheid en regie, niet naar de fysieke plaats waar software draait.

Bron: VWS

Data Source

mCSD-rol die adresgegevens aan het LRZa aanlevert, bijvoorbeeld namens een zorgaanbieder. De Data Source publiceert mutaties op de organisatie, haar onderdelen, diensten en endpoints; het LRZa neemt die op in de geaggregeerde directory. De concrete invulling van deze rol is de Data Source Client (Data Source Client).

Bron: IHE

Decentraal

Aanduiding dat de verantwoordelijkheid bij de individuele zorgaanbieder ligt, niet bij één stelselpartij; staat los van de fysieke plaatsing, die gedeeld kan zijn.

Bron: VWS

Endpoint

Technisch koppelvlak waarlangs gegevensuitwisseling tussen systemen plaatsvindt. Een endpoint legt vast waar een systeem te bereiken is en met welke techniek daar uitgewisseld wordt. In het informatiemodel wordt het als FHIR-resource gerepresenteerd (Endpoint Resource).

Bron: HL7 FHIR

HealthcareService

FHIR-resource die een specifieke zorgdienst representeert die door een organisatie op één of meerdere locaties wordt aangeboden.

Bron: HL7 FHIR

Local Replica Directory

Lokaal FHIR-bevragingspunt dat de geaggregeerde directory van het LRZa gerepliceerd beschikbaar stelt bij een afnemer. Afnemers raadplegen deze replica in plaats van het centrale LRZa, zodat het raadplegen niet afhangt van één centrale voorziening. De referentie-invulling is de gelijknamige applicatiecomponent (Local Replica Directory).

Bron: IHE

Location

FHIR-resource die een fysieke locatie of vestiging representeert waar zorg wordt verleend, zoals een gebouw, kliniek of praktijkruimte.

Bron: HL7 FHIR

LRZa

Landelijk Register Zorgaanbieders Adressering: het centrale register binnen de generieke functie Adressering dat adresgegevens uit leidende bronregisters aggregeert en aanvult met gegevens die

zorgaanbieders zelf publiceren. Het LRZa vormt hiermee één samenhangende directory van waar zorgaanbieders, hun onderdelen en diensten digitaal bereikbaar zijn. Het stelt die gegevens via replicatie beschikbaar aan afnemers, die ze in een eigen replica raadplegen.

Bron: VWS

mCSD

IHE-profiel Mobile Care Services Discovery, dat beschrijft hoe zorgaanbieders, hun organisatieonderdelen, locaties, diensten en endpoints als FHIR-resources worden gepubliceerd en bevraagd. De generieke functie Adressering gebruikt mCSD als basis voor de directory en onderscheidt daarin de rollen Data Source, Directory en de raadplegende clients.

Bron: IHE

Organization

FHIR-resource die een zorgaanbieder of organisatorische eenheid representeert binnen de generieke functie Adressering, geïdentificeerd door KvK-nummer en optioneel URA-nummer.

Bron: HL7 FHIR

OrganizationAffiliation

FHIR-resource die een relatie tussen twee organisaties vastlegt binnen de generieke functie Adressering. Het wordt onder meer gebruikt om vast te leggen dat een leverancier gemandateerd is om namens een zorgaanbieder adresgegevens te registreren, zodat de herkomst van door die leverancier ondertekende mutaties te verifiëren is (zie OrganizationAffiliation Resource).

Bron: HL7 FHIR

Query Client

mCSD-rol waarmee een afnemer adresgegevens opvraagt. De Query Client bevraagt de lokale replica, niet het centrale LRZa, en zoekt daarin op identifier of op kenmerken. De concrete invulling binnen het XIS of EPD is de applicatiecomponent Query Client.

Bron: IHE

Update Client

mCSD-rol die de lokale replica synchroon houdt met het centrale LRZa. De Update Client haalt periodiek de wijzigingen op bij de centrale directory en werkt daarmee de Local Replica Directory bij. Zij aggregaat zelf niet; aggregatie en conflictresolutie gebeuren centraal. De concrete invulling is de applicatiecomponent Update Client.

Bron: IHE

Zoeken op kenmerken

Het opzoeken van zorgorganisaties, organisatieonderdelen of zorgdiensten op grond van hun eigenschappen, zoals het type dienst of de locatie, in plaats van op een uniek identificerend kenmerk. Een voorbeeld is het tonen van alle zorgaanbieders die fysiotherapie leveren binnen een bepaalde straal. In de doelarchitectuur wordt dit ook “ongericht zoeken” genoemd.

Bron: VWS

13 Referenties

Baseline Informatiebeveiliging Overheid (BIO)

URL: <https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cybersecurity/bio-en-ensia/baseline-informatiebeveiliging-overheid/>

De Baseline Informatiebeveiliging Overheid (BIO) is het basisnormenkader voor informatiebeveiliging binnen alle overheidslagen. De BIO is gebaseerd op de ISO 27001/27002 en is verplicht voor alle overheidsorganisaties, waaronder CIBG als beheerder van het LRZa.

HL7 Europe eu-core

URL: <https://hl7.eu/fhir/base/>

eu-core is de Europese set FHIR-basisprofielen, ontwikkeld binnen HL7 Europe als gemeenschappelijke noemer voor grensoverschrijdende uitwisseling. De profielen van de generieke functie Adressering zijn hierop gebaseerd.

IHE mCSD

URL: <https://profiles.ihe.net/ITI/mCSD/>

IHE Mobile Care Services Discovery (mCSD) profiel. Internationale standaard voor het publiceren van zorgaanbieder directories via FHIR. Definieert hoe Organization, Location, HealthcareService en Endpoint resources gepubliceerd, opgezocht/bevraagd en gerepliceerd moeten worden voor interoperabiliteit.

Implementation Guide

URL: <https://build.fhir.org/ig/minvws/generiekefuncties-docs/branches/1.0.0/>

Waar in dit document de term “Implementation Guide” staat, wordt de “Care Service Directory - Implementation Guide” bedoeld. Deze pagina definieert hoe Organization, Location, HealthcareService en Endpoint resources gepubliceerd, opgezocht en gerepliceerd worden binnen het Nederlandse zorgdomein. Bevat NL-specifieke extensies en profielen.

HL7 FHIR R4

URL: <https://hl7.org/fhir/R4/>

Fast Healthcare Interoperability Resources R4. Internationale standaard voor gegevensuitwisseling in de zorg. Definieert resource types zoals Organization, Location, HealthcareService en Endpoint.

Functioneel Ontwerp generieke functie Adressering

Functioneel ontwerp van de generieke functie Adressering. Beschrijft de overkoepelende kaders waar de generieke functie Adressering invulling aan geeft.

Bijlage 1: Bronvermeldingen

Dit hoofdstuk bevat verwijzingen naar issues en discussies uit architectuurwerkgroepen die relevant zijn voor dit document.

Beschrijving	Link
#127: Als zorgtoepassing wil ik de adresseringsfunctie middels een API kunnen benaderen om te zoeken	https://github.com/minvws/generiekefuncties-adressering/issues/127
#117: Als zorgtoepassing wil ik dat de API getoetst/getest wordt voordat de integratie in productie gaat	https://github.com/minvws/generiekefuncties-adressering/issues/117
#21: Als zorgtoepassing wil ik de benodigde technische endpoints kunnen vinden op basis van het gekozen organisatieonderdeel én type uitwisseling	https://github.com/minvws/generiekefuncties-adressering/issues/21
#110: Als zorgtoepassing wil ik dat de synchronisatie met bronregisters één keer per 24 uur plaatsvindt	https://github.com/minvws/generiekefuncties-adressering/issues/110
#112: Als zorgaanbieder wil ik dat er een lokale subset beschikbaar is wanneer de online-versie niet draait	https://github.com/minvws/generiekefuncties-adressering/issues/112
#19: Als zorgaanbieder wil ik dat de centrale adresseringsfunctie de variatie van mijn fysieke en/of digitale operationele (organisatie)structuren en/of diensten ondersteunt	https://github.com/minvws/generiekefuncties-adressering/issues/19
#111: Als gebruiker wil ik goed geïnformeerd worden wanneer de dienst niet naar verwachting werkt	https://github.com/minvws/generiekefuncties-adressering/issues/111
#106: Als zorgtoepassing wil ik dat de centrale adresseringsfunctie in sync gehouden wordt met relevante bronregisters	https://github.com/minvws/generiekefuncties-adressering/issues/106
#124: Als belanghebbende wil ik inzicht krijgen via een statuspagina	https://github.com/minvws/generiekefuncties-adressering/issues/124

Bijlage 2: Besluitonderbouwingen

Dit hoofdstuk bevat de uitgebreide onderbouwing van zwaarwegende architectuurbesluiten: de afgewogen alternatieven met hun afwijzingsgrond, relevante onderzoeks- en PoC-bevindingen en de geaccepteerde prijs.

Onderbouwing centraal push-model

Onderbouwing bij architectuurkeuze AK-06: Centraal push-model met read-only replica's

Deze onderbouwing hoort bij architectuurkeuze AK-06: Centraal push-model met read-only replica's en bevat de volledige afweging: de afgewezen alternatieven met hun afwijzingsgrond, de PoC-bevindingen die tot de keuze leidden en de geaccepteerde prijs.

PoC-bevindingen

In de proof-of-concepts is een model beproefd met een centrale registerwijzer, decentrale bronnen en een pull-model voor het vullen van de decentrale replica's. Daarbij bleek:

- Verschillende implementaties hanteerden onderling andere aggregatie- en conflictresolutielogica. Tijdens een demo hadden twee leveranciers op hetzelfde moment een verschillend beeld van de geregistreerde endpoints voor dezelfde zorgaanbieder. Code-audits bevestigden dat dit een directe consequentie was van verschillen in de software die de decentrale replica's vulde.
- Het pull-model ondersteunde per zorgaanbieder maar één primaire bron (leverancier), omdat conflictresolutie bij meerdere publicerende leveranciers nog ingewikkelder werd. Zorgaanbieders hebben echter vaak meerdere leveranciers voor verschillende systemen; dit maakte leveranciers onderling afhankelijk.

Afgewezen alternatieven

Volledig decentraal, geen registerwijzer

Vragers bevragen elke leverancier rechtstreeks, zonder centrale verwijzing of register. Reden van afwijzing: vereist dat elke vrager elke leverancier kent en kan aanspreken, schaalt niet bij landelijke uitrol, en conflicten tussen bronnen zijn onoplosbaar zonder coördinatiepunt. Al vóór de PoC's afgewezen.

Centraal zonder replica's (puur direct)

Alle vragers bevragen de centrale dienst rechtstreeks; geen replica's ertussen. Reden van afwijzing: legt de volledige leesbelasting op één punt en laat geen leesbeschikbaarheid over bij uitval van de centrale dienst. Replica's vangen dit op zonder de gezaghebbendheid van het centrale register te ondergraven.

Centraal pull, decentrale publicatie

Bronnen publiceren mutaties in hun eigen systemen; de centrale dienst haalt die periodiek op en aggregereert. Functioneel gelijk aan push; alleen de transportrichting verschilt. Reden van afwijzing: de centrale dienst moet elke bron kennen, monitoren en het risico van trage/onbereikbare bronnen dragen. Belangrijker: de directe terugkoppeling per mutatie gaat verloren. Bij push krijgt een leverancier per mutatie meteen een reactie (geaccepteerd of geweigerd, met reden); bij pull blijft een mutatie 'stil' in de bron staan en ontbreekt bij afwijzing een eenduidig kanaal om dat aan de leverancier te melden (mCSD biedt hier geen oplossing voor). Bij tegenstrijdige data ontstaat een

onoplosbare ambiguïteit (alles overnemen behalve het geweigerde stuk, of niets overnemen) — beide keuzes kunnen verkeerd zijn. Push past hier in het FHIR-protocol met directe terugkoppeling.

Hybride: centrale discovery, decentrale autoritatieve publicatie

Een landelijke, centraal gehoste discovery- of query-voorziening (optioneel te gebruiken) bovenop decentrale bronnen die eigenaar blijven van hun autoritatieve publicatiepad. De bronnen (leveranciers) houden een eigen schrijfbaar directory; de centrale voorziening aggregaat die periodiek en biedt een landelijke zoekingang. Zo blijft schrijven onafhankelijk van de centrale dienst en behouden partijen hun eigen write-path.

Reden van afwijzing: het autoritatieve beeld ontstaat pas in de periodieke aggregatiestap, en die stap draagt precies de aggregatie- en conflictresolutielogica die in de PoC's foutgevoelig bleek. Zolang de autoritatieve stand decentraal wordt gehouden en pas achteraf centraal wordt samengevoegd, keert het divergentieprobleem terug: op enig moment kunnen verschillende afnemers een ander beeld hebben, afhankelijk van welke aggregatie al is gedraaid. De directe terugkoppeling per mutatie ontbreekt om dezelfde reden als bij het pull-model: een bron krijgt geen eenduidig oordeel (geaccepteerd of geweigerd, met reden) op het moment van muteren. Het model verzacht daarmee wel de schrijfbeschikbaarheid, maar tegen de prijs die het centrale push-model juist wil vermijden: geen eenduidige gezaghebbende stand en geen sluitende feedback. Waar het optioneel behouden van een lokale write-buffer wenselijk is, wordt dat in het gekozen model opgevangen door bronnen mutaties lokaal te laten cachen en periodiek te pushen, zonder het autoritatieve beeld te decentraliseren (zie Geaccepteerde prijs).

Geaccepteerde prijs

- Schrijfbeschikbaarheid is afhankelijk van één centrale dienst. De centrale dienst is een single point of failure voor mutaties. Replica's vangen leesuitval op, maar bronnen kunnen tijdens centrale uitval geen mutaties leveren. Mitigatie via redundantie en hersteltijd-SLA; bronnen kunnen mutaties ook lokaal cachen en periodiek naar het LRZa pushen. Blijft een operationeel aandachtspunt.
- Concentratie van inhoudelijk gewicht bij de beheerder van het centrale register. Niet geheel nieuw (deze rol lag al deels centraal), wel groter door toevoeging van aggregatie en conflictresolutie. Vraagt om expliciete governance.

Buiten scope van dit besluit

Bewust nog niet belegd: het securitymodel (trust anchor, autoriteitsverificatie, ondertekening per mutatie, externe verifieerbaarheid); de conflictresolutieregels per gegevenscategorie (uitwerking in de IG); het replicatieprotocol en de verversings-SLA's (IG/NFR); EHDS-/NCPeH-aansluiting; en het migratiepad vanuit bestaande oplossingen.

Onderbouwing zorgverleners niet opnemen

Onderbouwing bij: Zorgverleners niet opnemen in het LRZa

Deze onderbouwing hoort bij het besluit Zorgverleners niet opnemen in het LRZa en bevat de juridische afweging, de afgewezen alternatieven en de geaccepteerde prijs.

Juridische analyse

Practitioner en PractitionerRole bevatten persoonsgegevens. Voor het verwerken daarvan is een AVG-grondslag nodig. Artikel 12 van de Wkkgz biedt een grondslag voor het publiceren van

adresgegevens van zorgaanbieders, maar strekt zich niet uit tot persoonsgegevens van individuele zorgverleners.

De juridische analyse concludeerde dat een dergelijke grondslag ontbreekt. Zolang die er niet is, kunnen deze gegevens niet door het LRZa worden verwerkt — ongeacht de functionele wenselijkheid.

Erkende functionele behoefte

De behoefte aan adressering op zorgverlenerniveau is reëel en is in de consultatie meermaals ingebracht:

- Intercollegiale consulten in de medisch-specialistische zorg worden vaak op zorgverlenerniveau geadresseerd.
- Communicatie naar een huisartspraktijk, bijvoorbeeld een ontslagbrief, is vaak op zorgverlenerniveau.
- Verwijzingen naar medisch-specialistische zorgorganisaties verlopen daarentegen meestal op afdelings- of specialisameniveau, waarvoor Organization, Location en HealthcareService volstaan.

Afgewezen alternatieven

Opt-in door de zorgverlener.

Overwogen is om persoonsgegevens uit het DEZI-register automatisch naar het LRZa te kopiëren en pas na een opt-in zichtbaar te maken. Dit lost het grondslagvraagstuk niet op: ook het kopiëren zelf is een verwerking waarvoor een grondslag nodig is.

Beperken tot PractitionerRole.

Voorgesteld is om alleen PractitionerRole op te nemen en Practitioner weg te laten. PractitionerRole verwijst echter naar een identificeerbare persoon en blijft daarmee een persoonsgegeven.

Geaccepteerde prijs

Het LRZa is op dit punt geen volledige mCSD-directory. Een internationale mCSD-client die Practitioner of PractitionerRole verwacht, wordt niet bediend. Ook los hiervan is het LRZa geen conforme Directory-actor; zie LRZa als replicatiebron, niet als mCSD Directory-actor. Dat is aanvaard: de beperking volgt uit de Nederlandse juridische context en niet uit het datamodel, en kan worden opgeheven zodra er wel een grondslag is.

Zorgaanbieders die zorgverlenergegevens willen ontsluiten kunnen dat lokaal doen via een eigen Endpoint dat in het LRZa is geregistreerd. Interoperabiliteit van zo'n decentrale zoekfunctie is nog niet belegd.