



Ministerie van Volksgezondheid,
Welzijn en Sport

Koppelvlakspecificatie Dezi-Online

Koppelvlak 1: Platformleverancier

Colofon

Projectnaam	Dezi-Online
Organisatie	iRealisatie
Datum:	april 2024
Versie:	1.0

Inhoudsopgave

1. Inleiding
2. Gegevensverwerking
3. Onderdeel 'Identiteitsvaststelling'
3.1 Introductie
3.2 Architectuur
3.3 Het ontkoppelpunt (OIDC-gateway)
3.4 Koppelvlakspecificatie
3.5 Gebruikte standaarden
3.6 Message encryption
3.7 Message signing
3.8 De zorgidentiteit (user data object)
3.9 Geen single sign-on (SSO) en logout
Bijlage 1: Gehanteerde begrippen
Bijlage 2: technische specificaties
Bijlage 3: voorbeeldberichten identiteitsvaststelling

1. Inleiding

Met het nieuwe Dezi-stelsel is het doel om gezondheidsdata gericht toegankelijker te maken voor zorgmedewerkers en -professionals. Dit betekent dat zorgmedewerkers en -professionals alleen medische informatie kunnen zien die relevant is voor hun functie. Deze functie-specifieke informatie wordt vrijgegeven op basis van drie attributen:

Wie ben je? (UZI-nummer)

Waar werk je? (URA-nummer)

Welke bevoegdheden heb je? (rolcode)

Een van de nieuwe functionaliteiten van het nieuwe Dezi-stelsel is de integratie van bestaande zorgplatformen om de drempel van het nieuwe Dezi-stelsel zo laag mogelijk te maken. Deze zorgplatformen kunnen een koppeling maken met het ontkoppelpunt dat als schakel functioneert tussen diverse zorgmiddelen, zorgplatforms en de Dezi-database.

Om aan te sluiten op de technische omgeving, maakt een leverancier een verbinding met het ontkoppelpunt. Dit is een technische voorziening van het CIBG die als OpenID Connect gateway functioneert

Dit koppelvlak-specificatie document beschrijft de methode van aansluiting van een zorgplatform op de technische omgeving middels het ontkoppelpunt.

Naast dit document voor de koppelvlakspecificatie voor zorgplatform leveranciers is er ook een aansluitdocument. In dit aansluitdocument wordt stap voor stap beschreven hoe er een aansluiting gemaakt kan worden met de technische omgeving.

2. Gegevensverwerking

Het ontkoppelpunt (OIDC-gateway) verwerkt op de titel van het CIBG de volgende gegevens van een zorgmedewerker:

- Het (versleuteld) BSN
- Het (versleuteld) UZI-nummer
- Het (versleuteld) URA-nummer
- De (versleutelde) rolcode(s)
- De (versleutelde) voorletter(s) van de voornaam / voornamen
- De (versleutelde) achternaam inclusief tussenvoegsel(s)
- Het IP-adres van het apparaat dat wordt gebruikt (computer, telefoon)

3. Onderdeel 'Identiteitsvaststelling'

3.1 Introductie

Om het nieuwe Dezi-stelsel zo laagdrempelig mogelijk te maken is het mogelijk voor bestaande zorgplatformen om zich aan te sluiten bij het nieuwe Dezi-stelsel. Het aansluiten van een zorgplatform op het nieuwe Dezi-stelsel wordt gedaan middels het aansluiten op het ontkoppelpunt dat is gebouwd op basis van het OpenID connect (OIDC) protocol.

Om een beeld te krijgen van de koppelvlakken die een rol spelen bij het onderdeel 'identiteitsvaststelling', is in onderstaande afbeelding de samenhang abstract weergegeven.



Figuur 1: schematische weergave koppelvlakken en ontkoppelpunt

Het ontkoppelpunt biedt twee verbindingsmogelijkheden afhankelijk van de rol als identity provider of platform leverancier. Platform leveranciers maken verbinding via koppeling 1 waarbij het aangesloten platform als client fungeert en het ontkoppelpunt als OIDC-provider.

Middelenleveranciers maken verbinding via koppeling 2 waarbij het ontkoppelpunt als client fungeert en het aangesloten middel als OIDC-provider.

Dit document betreft alleen informatie die betrekking heeft op koppeling 1 voor platformleveranciers.

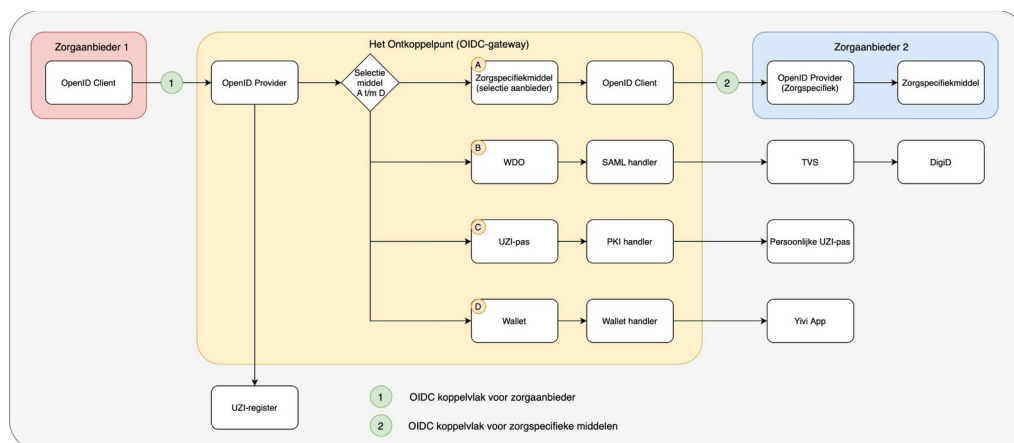
Voor meer informatie betreft koppeling 2 zie het document:

Koppelvlakspecificatie Dezi-Online koppelvlak 2: middelenleverancier

3.2 Architectuur

De architectuur van het nieuwe Dezi-stelsel is zo opgebouwd dat een zorgportaal inlogmiddelen kan aanbieden aan gebruikers van het portaal binnen het nieuwe Dezi-stelsel zonder hiervoor een inlogmiddel specifieke implementatie te bouwen. De communicatie tussen het zorgplatform (rood blok, figuur 3) en het ontkoppelpunt (geel blok, figuur 3) gaat via het OpenID Connect (OIDC) protocol. Het zorgplatform gedraagt zich als OIDC-client en het ontkoppelpunt als OIDC-provider.

Dit betekent dat de gebruiker zich via het ontkoppelpunt authentiseert door middel van de aangesloten inlogmiddelen om vervolgens toegang te krijgen tot zijn of haar zorgidentiteit.



Figuur 2: overzicht koppelvlakken

3.3 Het ontkoppelpunt (OIDC-gateway)

Om aan te sluiten op de technische omgeving maakt een leverancier een verbinding met het ontkoppelpunt. Het ontkoppelpunt laat op basis van het OIDC-protocol de gebruiker inloggen. OIDC is, net als SAML, een federatief authenticatieprotocol: Het systeem waar de identiteit van de gebruiker is opgeslagen, staat dus los van de online dienst waar de gebruiker op inlogt.

Het OIDC protocol vormt een identificerende laag (identity layer) over het OAuth 2.0 protocol heen. Een external identity provider, in dit geval het CIBG, retourneert een (versleuteld) access token met de zorgidentiteit van de zorgprofessional.

Client authenticatie voor token endpoint

Aanvullend aan de parameters die zijn gedefinieerd in de [OAuth2.0](#) specificatie wordt er gebruikgemaakt van [private key jwt](#) voor de client authenticatie in de token endpoint. Hierbij gebruikt de client zijn private key om de JWT te ondertekenen en stuurt deze naar de autorisatie server als bewijs van identiteit. De server kan deze dan verifiëren met behulp van de public key van de client.

De JWT moet de volgende claims bevatten:

```
{
  "iss": [cliend_id],
  "sub": [client_id],
  "aud": "https://max.proeftuin.uzi-online.rdobeheer.nl",
  "exp": a valid expiry date
}
```

3.4 Koppelvlakspecificatie

Het zorgplatform dient aan te sluiten op de technische omgeving op basis van de technische standaard OpenID Connect (OIDC). Dit is een beheerde, open standaard die een technisch koppelvlak biedt dat eenvoudig implementeerbaar is.

Met de OIDC-standaard wordt de PKCE Authorization Code flow gebruikt als extensie op de standaard OIDC specificatie. Daarbij wordt er gebruikgemaakt van de SHA-256 (S256) 'code challenge method' in de authorization code flow. Dit betekent dat er een 'code challenge' en 'code verifier' wordt bijgevoegd in de autorisatie aanvraag. De server is dan in staat te checken of de afzender klopt. Zie RFC 7636.

3.5 Gebruikte standaarden

Tabel 1: gebruikte standaarden

Standaard	RFC	Referentie
OpenID Connect		https://openid.net/specs/openid-connect-core-1_0.html
PKCE Authorization Code Flow (PKCE)	RFC 7636	https://datatracker.ietf.org/doc/html/rfc7636
SHA-256(S256)	RFC 6234	https://datatracker.ietf.org/doc/html/rfc6234
JSON Web Token (JWT)	RFC 7519	https://www.rfc-editor.org/rfc/rfc7519.html
JSON Web Encryption (JWE)	RFC 7516	https://datatracker.ietf.org/doc/html/rfc7516
JSON Web Signature (JWS)	RFC 7515	https://datatracker.ietf.org/doc/html/rfc7515
JSON Web Key (JWK)	RFC 7517	https://datatracker.ietf.org/doc/html/rfc7517
The OAuth 2.0 Authorization Framework	RFC 6749	https://datatracker.ietf.org/doc/html/rfc6749#section-3.2

3.6 Message encryption

De 'userinfo' zoals gespecificeerd in de OpenID Connect specificaties is versleuteld volgens de JSON Web Encryption (JWE, RFC 7516) specificatie. Daarbij wordt er gebruikgemaakt van een nested JWT zoals beschreven in RFC 7519.

Voor de versleuteling door het zorgplatform wordt er gebruikgemaakt van de public key van het ontkoppelpunt die bij de registratie is aangeleverd.

De implementatie van het koppelvlak is volgens de specificatie zoals beschreven in de OpenID specificatie.

Het zorgplatform moet valideren dat de encrypted en signed JWT daadwerkelijk van het ontkoppelpunt komt. Dit betekent dat de signature van de 'inner JWT' gevalideerd moet worden. Het ontkoppelpunt biedt hiertoe een OpenID Connect JWKS Endpoint aan volgens de specificatie van RFC 7515.

De locatie van de JWKS is via de OIDC well-known configuration van de server te vinden. Voor de validatie van de signature is de public key van de authenticatiedienst van het zorgplatform nodig. In de 'inner JWT' is een 'kid'-header (key ID) opgenomen die moet corresponderen met de 'kid' van de

authenticatiedienst van het zorgplatform dat in de jwks-uri staat.

In de payload staat informatie over de geauthenticeerde zorgverlener, gebaseerd op een 'verklaring' die het CIBG heeft afgegeven tijdens de uitgifte van het middel. De uitgifte van de 'verklaring' valt buiten de scope van dit koppelvlak.

3.7 Message signing

De zorgidentiteit die de client opvraagt bij het ontkoppelpunt is ondertekend met de sleutel van het ontkoppelpunt. Hierdoor wordt de client in staat gesteld om te valideren dat de identiteit onaangepast afkomstig is uit het Dezi-stelsel. Deze validatie moet uitgevoerd worden door de client om de betrouwbaarheid van de zorgidentiteit te kunnen garanderen.

Voor de technische omgeving moet een minimale sleutellengte van 4096 bits RSA worden gebruikt om de private key te maken. Voor productieomgevingen is een PKI-O certificaat vereist. Voor niet-productomgevingen kan er gebruikgemaakt worden van publieke CA's of van self-signed certificaten.

3.8 De zorgidentiteit (user data object)

De structuur van het bericht, met daarin de gebruikersdata, moet gevalideerd kunnen worden door een JSON-schema. De locatie van het JSON schema staat in de uitgegeven JWT.

Voor het doen van een identiteitsvaststelling wordt tijdens het proces voor identificatie en authenticatie gewerkt met een aantal persoonsgegevens. Deze zijn afkomstig uit het UZI-register. De zorgidentiteit wordt door middel van de combinatie van gegevens samengesteld. Voorbeelden van deze identiteitsvaststelling zijn te vinden in bijlage 3.

De data bestaan deels uit data over de zorgmedewerker die toegang vraagt tot de applicatie en deels uit technische data.

Hieronder worden de *claims* getoond die de zorg identiteit bepalen:

Data over de zorgmedewerker		
Wat	Data type	Toelichting
initials	<string>	Initialen van zorgmedewerker
surname_prefix	<string>	Tussenvoegsel van achternaam
surname	<string>	Achternaam
uziNumber	<string>	UZI-nummer van de zorgmedewerker
relations	<list of objects>	Dit is een lijst van de onderstaande variabelen
uraname	<string>	Organisatiename
uranumber	<string>	URA-nummer van de zorgaanbieder
roles	<list of string>	Rolcode(s) van de zorgmedewerker bij dit URA-nummer

Tabel 3, data over de zorgmedewerker, data types en toelichting

Technische data		
Wat	Data type	Toelichting
json_schema	<string>	URI van het JSON-schema van het antwoord bericht
request-id	<string>	Technisch nummer, bruikbaar voor auditlog
iss	<string>	Autoritatieve bron (issuing authority)
aud	<string>	Audience van/voor het bericht
exp	<string>	Tijdstempel van maximale geldigheid van de claims (epoch)
nbf	<string>	Tijdstempel van ingangsmoment van de claims (epoch)
loa_authn	<string>	URI van het betrouwbaarheidsniveau van de authenticatie vanuit de authenticatieverklaring
loa_uzi	<string>	URI van het betrouwbaarheidsniveau van de zorg identiteit

Tabel 4, technische data, data types en toelichting

3.9 Geen single sign-on (SSO) en logout

Er wordt door het ontkoppelpunt geen single sign-on functionaliteit geleverd. Deze functionaliteit dient te worden geleverd door de authenticatiemiddelen/-diensten. De kaders waar de erkende middelen en authenticatie diensten aan moeten voldoen zijn bepalend of SSO mag worden ondersteund. Doordat het ontkoppelpunt geen (inlog) sessie bewaart, wordt er ook geen logout functionaliteit aangeboden.

Het ontkoppelpunt levert (enkel) een zorgverleners identiteit op die door het zorgplatform kan worden gebruikt, ook bij het ophalen van gegevens via systeemkoppelingen bij derden.

Het ophalen van gegevens vindt altijd plaats onder de verantwoordelijkheid van het zorgplatform.

Het sessiebeheer voor dit soort uitwisselingen behoort tot de verantwoordelijkheid van de zorgaanbieder, die er zelf SSO-achtige functionaliteit mee kan ontwikkelen.

Authenticatiedienst	De rol van een partij die op basis van een identificatiemiddel een authenticatieverklaring afgeeft. Naast de generieke authenticatiedienst (voor generieke authenticatiemiddelen) kunnen ook zorgspecifieke authenticatiediensten worden opgenomen in het stelsel (voor zorgspecifieke authenticatiemiddelen).
BSN	Burger Service Nummer, waarmee een dienstafnemer zich initieel kan identificeren in het stelsel, die omgewisseld wordt in het Dezi-nummer van de dienstafnemer in het zorgregister.
CIBG	Uitvoeringsorganisatie van VWS verantwoordelijk voor o.a. het zorgregister, en daarmee een partij binnen dit stelsel.
Digitaal ondertekenen	Het proces waarmee een digitaal document wordt voorzien van een elektronische handtekening.
JWE	JSON Web Encryption (JWE) is directe encryptie met een symmetrische AES-sleutel volgens een open standaard (RFC-7516).
JWT	JSON Web Token (JWT) is een open standaard (RFC-7519) die een compacte en op zichzelf staande manier definieert voor het veilig verzenden van informatie tussen partijen als een JSON-object
OIDC-gateway	Technische oplossing die op basis van de OIDC-standaard authenticatiemiddelen ontsluit (via een ander technisch koppelvlak) en met behulp van de identiteitsverklaring een zorgidentiteit samenstelt vanuit het UZI-register. Zie ook Zorgtoegangsdienst.
Ontkoppelpunt	Werktitel voor het systeem dat de functionaliteit implementeert die de OIDC-gateway biedt.
OpenID Connect	OpenID Connect 1.0 is een open standaard voor gedecentraliseerde authenticatie. Het biedt applicaties de mogelijkheid de identiteit van de gebruiker vast te laten stellen door een vertrouwde server, als ook attributen van de gebruiker op te vragen.
technische omgeving	Technische omgeving waarin leveranciers en zorgaanbieders kunnen aansluiten op de technische infrastructuur die in het kader van het project Toekomstbestendig Dezi wordt gerealiseerd. De technische omgeving en bepaalde implementatie-keuzes die daar worden toegepast kunnen nog veranderen. In de technische omgeving wordt niet gewerkt met echte data van echte zorgmedewerkers (gebruikers).

Rolcode	Kenmerk(en) van een zorgmedewerker vastgelegd in het zorgregister of een attribootregister, gerelateerd aan de functie bij de zorgaanbieder (o.b.v. het URA-nummer). Een rolcode drukt de bevoegdheid van een zorgmedewerker uit zoals deze in het UZI-register bekend is. Deze is gebaseerd op erkende beroepen van de wet BIG.
Signeren, signen	Zie digitaal ondertekenen
URA-nummer	Het abonneenummer zoals deze bekend is in het UZI-register. Het is een identificerend nummer die een zorgorganisatie aanduidt.
UZI-nummer/Dezi-nummer	Uniek identificerend nummer voor een zorgmedewerker (natuurlijk persoon) zoals deze bekend is in het UZI-register. Een UZI-nummer is in het UZI-register te relateren aan een BSN.
WetDO / wDO	Wet Digitale Overheid
Zorgaanbieder	Het unieke identificatie-attriboot van een zorgaanbieder binnen het zorgregister (UZI Register Abonneenummer).
Zorgidentiteit	De digitale representatie van de identiteit van een zorgmedewerker in de context van de zorgaanbieder. De zorgidentiteit bestaat uit een aantal kenmerken. Dit zijn ten minste: UZI-nummer + URA-nummer + rolcode(s)
Zorgmedewerker	Een natuurlijke persoon die functiematig zorg verleent in dienst van een zorgaanbieder.
Zorgprofessional	Professionals die taken verrichten in de zorg, dit is (dus) een bredere doelgroep dan de zorgverlener.
Zorgtoegangsdienst	De generieke authenticatie-voorziening voor de zorg, vastgelegd in het stelsel, waarvan het doel is het leveren van een betrouwbare, veilige en interoperabele verstrekking van identiteitsinformatie van de zorgmedewerker aan de zorgaanbieder. Zie ook OIDC-gateway.
Zorgspecifiek middel	Een authenticatiemiddel waarmee zorgprofessionals zich authentifieren, verstrekt door een zorgaanbieder en in overeenstemming met de NEN-7518 norm. De conformiteit kan worden aangetoond met een certificaat van een bevoegde Certificerende Instantie.

Domein/Endpoints	<p>Zoals geconfigureerd in het '.well-known/openid-configuration' endpoint:</p> <p>authorize_endpoint = /authorize jwks_endpoint = /jwks accesstoken_endpoint = /token userinfo_endpoint = /userinfo scopes_supported = openid</p> <p>Het domein moet altijd uitgelezen worden</p>
Koppelvlak- specificatie voor de zorgaanbieder	<p>De beheerde open standaard OpenID Connect (OIDC)</p> <ul style="list-style-type: none"> • de Authorization Code flow met PKCE. Zie: RFC7636 • de SHA-256 (S256) 'code challenge method'. <p>In de vraagberichten dient de URA van de zorgaanbieder als waarde voor het 'client-id'.</p>
OpenID scope(s)	<p>In de oplossing worden door de OIDC-gateway de volgende scopes ondersteund:</p> <p>openid: levert user data object met daarin de vastgestelde zorg identiteit.</p>
lijst van <i>Levels of Assurance</i>	<p>HIGH = ' http://eid.as.europa.eu/LoA/high ';</p>
message signing	<p>Alle (JWT-)berichten in de uitwisseling worden door de afzenders gesigneerd op basis van public/private key pairs.</p> <p>Het certificaat van de OIDC-gateway is (door de applicatie) te downloaden vanuit de JWKS.</p> <p>De Resource maakt gebruik van de public key van het CIBG en kan daarmee het bericht verifiëren.</p>
message encryption	<p>De data is versleuteld op basis van JSON Web Encryption (JWE) volgens de specificatie van RFC7516. Voor versleuteling maakt de Resource gebruik van de public key van de zorgaanbieder, die bij de registratie is aangeleverd.</p> <p>De gegevensbron (OAuth Resource Server) die via het user info endpoint wordt ontsloten, levert een JWT waarin onderdelen zijn versleuteld voor de aanvragende zorgaanbieder.</p>
message decryption	<p>De OpenID-gateway biedt een OpenID Connect JWKS Endpoint aan volgens de specificatie van RFC7517. De locatie van JKWS is via de OIDC-configuration van de Resource te vinden.</p>

	<p>Validatie van de signatuur vereist de public key van het CIBG (de Resource Server).</p> <p>De client van de zorgaanbieder moet de signatuur van de 'inner JWT' valideren, om zeker te weten dat de versleutelde en gesigneerde JWT daadwerkelijk van het CIBG komt. Daarbij moet de 'kid'-header in de 'inner JWT' corresponderen met de 'kid' van het CIBG in de jwks-uri.</p>
bericht-structuur user data object	De structuur van het bericht met daarin de user data, kan worden gevalideerd door een JSON-schema.
single sign-on (SSO)	De OIDC-gateway levert geen Single Sign-On (SSO) functionaliteit. De OIDC-gateway levert (enkel) een zorgmedewerkersidentiteit op, die door de zorgaanbieder kan worden gebruikt. Dit geldt ook voor het ophalen van gegevens via systeemkoppelingen bij derden.
logout functionaliteit	De OIDC-gateway bewaart geen (inlog)sessies en biedt geen log-outfunctionaliteit. Het ophalen van gegevens en het sessiebeheer zijn de verantwoordelijkheid van de zorgaanbieder.

