Ministerie van Volksgezondheid,
Welzijn en Sport

Koppelvlakspecificatie UZI-Online

Koppelvlak 1: Platformleverancier

Colofon

Projectnaam	Toekomstbestendig UZI
Organisatie	iRealisatie
Datum:	12 december 2023
Versie:	0.2

Inhoudsopgave

1. Inleiding

Het ministerie van Volksgezondheid, Welzijn en Sport is bezig met de herziening van het UZI-stelsel. Onder het UZI stelsel vallen het UZI-register, de UZI-passen en de UZI-servercertificaten.
Daarbij wordt het mogelijk om naast de UZI pas ook in te kunnen loggen met digitale middelen zoals DigiD, een digitale wallet of zorgspecifieke middelen die zijn ontwikkeld vanuit het zorgveld.

Met het nieuwe UZI-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 UZI-stelsel is de integratie van bestaande zorgplatformen om de drempel van het nieuwe UZI-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 UZI-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 ontkoppelingspunt.

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:

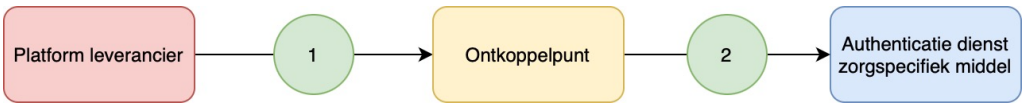
- Het (versleuteld) BSN
- Het (versleuteld) UZI-nummer
- Het (versleuteld) URA-nummer
- De (versleutelde) rolcode(s)
- De (versleutelde) voorletter(s) van de voornaam / voornamen
- De (versleutelde) achternaam inclusief tussenvoegsel(s)
- Het IP-adres van het apparaat dat wordt gebruikt (computer, telefoon)

3. Onderdeel ‘Identiteitsvaststelling’

3.1 Introductie

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



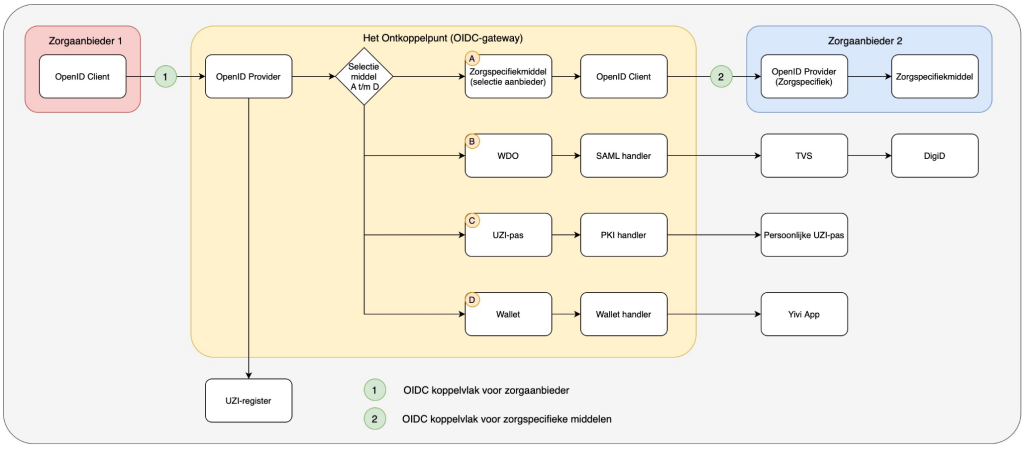
Figuur 1: schematische weergave koppelvlakken en ontkoppelpunt

Het ontkoppelpunt biedt twee verbindingsmogelijkheden afhankelijk van de rol als ID-provider of ID-client. Platformleveranciers maken verbinding via koppeling 1 waarbij het aangesloten platform als ID-client fungeert en het ontkoppelpunt als ID-provider.
Middelenleveranciers maken verbinding via koppeling 2 waarbij het ontkoppelpunt als ID-client fungeert en het aangesloten middel als ID-provider.

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

3.2 Architectuur

De architectuur van het nieuwe UZI-stelsel is zo opgebouwd dat een zorgportaal inlogmiddelen kan aanbieden binnen het nieuwe UZI-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 protocol. Het zorgplatform gedraagt zich als OpenID client en het ontkoppelpunt als OpenID 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 een 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.

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

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.

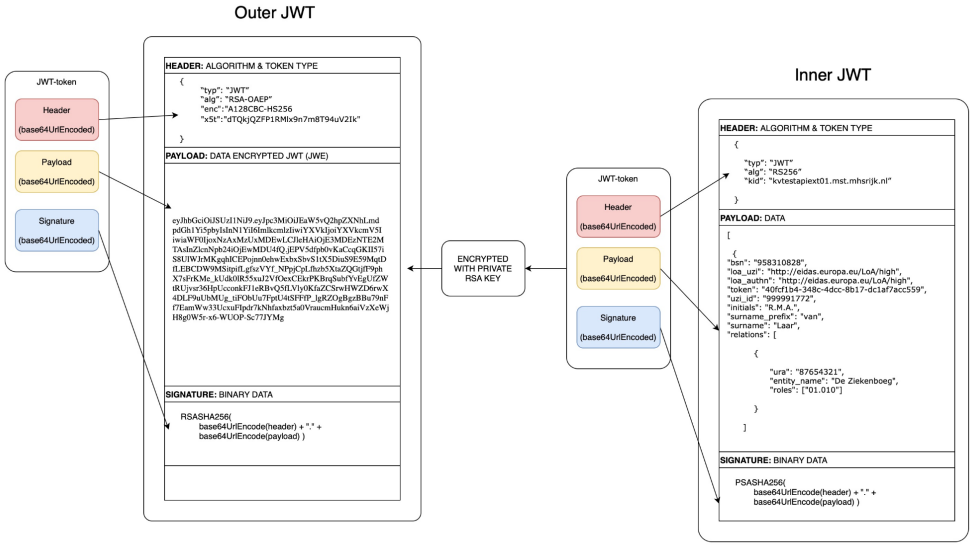
De implementatie van het koppelvlak is volgens de specificatie zoals beschreven in de OpenID specificatie.

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 JKWS is via de OIDC-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.

Onderstaand figuur is de schematische weergave van de JWT die het userinfo endpoint oplevert:

Voor een uitvergrote weergave zie bijlage 4



Figuur 3: Contents outer-JWT en inner-JWT

Links in het figuur staat de 'outer JWT' met in de header informatie over de encryptie van de payload en de daarvoor gebruikte public key.
In de header van de inner JWT bevinden zich: het algoritme voor het maken van de digitale handtekening, het encryptie algoritme waarmee de payload is versleuteld en de 'kid' (key ID). In de payload bevindt zich de JWT die op basis van JWE is versleuteld.

Aan de rechterkant van het figuur staat de JWT die is ontsleuteld met de private key van de zorgaanbieder. Deze ontsleutelde JWT bevat in de header de 'kid' van de authenticatiedienst van het zorgspecifieke middel.

In de payload staat informatie over de geauthenticeerde zorgverlening, 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 UZI 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 productie omgevingen is een PKI-O certificaat vereist. Voor niet productie omgevingen kan er gebruik gemaakt 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 user data, 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:

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

Data over de zorgmedewerker		
Wat	Data type	Toelichting
Initials	<string>	Inititalen 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>	Organisatienaam
uranumber	<string>	URA-nummer van de zorgaanbieder
Roles	<list of string>	Rolcode(s) van de zorgmedewerker bij dit URA-nummer

Tabel 4, technische data, 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 autenticatieverklaring
Loa_uzi	<string>	URI van het betrouwbaarheidsniveau van de zorg identiteit

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.

Bijlage 1: Gehanteerde begrippen

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 UZI-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 UZI 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 attribuutregister, 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	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-attribuut 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 authentiseren, 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.

Bijlage 2: technische specificaties

Domein/Endpoints	Zoals geconfigureerd in het '.well-known/openid-configuration' endpoint: authorize_endpoint = /authorize jwks_endpoint = /jwks accesstoken_endpoint = /token userinfo_endpoint = /userinfo scopes_supported = openid Het domein moet altijd uitgelezen worden
Koppelvlak- specificatie voor de zorgaanbieder	De beheerde open standaard OpenID Connect (OIDC) • de Authorization Code flow met PKCE. Zie: RFC7636 • de SHA-256 (S256) 'code challenge method'. In de vraagberichten dient de URA van de zorgaanbieder als waarde voor het 'client-id'.
OpenID scope(s)	In de oplossing worden door de OIDC-gateway de volgende scopes ondersteund: openid: levert user data object met daarin de vastgestelde zorg identiteit.
lijst van *Levels of Assurance*	HIGH = ' http://eidas.europa.eu/LoA/high ';
message signing	Alle (JWT-)berichten in de uitwisseling worden door de afzenders gesigneerd op basis van public/private key pairs. Het certificaat van de OIDC-gateway is (door de applicatie) te downloaden vanuit de JWKS. De Resource maakt gebruik van de public key van het CIBG en kan daarmee het bericht verifiëren.
message encryption	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. De gegevensbron (OAuth Resource Server) die via het user info endpoint wordt ontsloten, levert een JWT waarin onderdelen zijn versleuteld voor de aanvragende zorgaanbieder.
message decryption	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. Validatie van de signatuur vereist de public key van het CIBG (de Resource Server). 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.
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.

Bijlage 3: voorbeeldberichten identiteitsvaststelling

Ter illustratie van het sequentiediagram (zie 2.4 Sequentiediagram) zijn de drie vraagberichten (A,B,C) vanuit de zorgaanbieder aan de OpenID-gateway en Resource opgenomen en één antwoord (D).
Merk op dat er als gevolg van de lengte van de vraagberichten koppelstreepjes (-) in de voorbeeldberichten staan waar de 'zin' (in dit document) is afgebroken.

Voorbeeld van JSON schema:
https://max.proeftuin.uzi-online.rdobeheer.nl/json-schema.json

A: Authorization request

```
GET /authorize?response_type=code&redirect_uri=http%3A%2F%2Flocalhost%3A9000%2
Foidc%2Flogin&client_id=006fbf34-a80b-4c81-b6e9-593600675fb2&nonce=226b78cf4ddfe
8f98f6385774b078e69&state=e5bafe7f6ea6973045f2bae163d454d5&scope=+openid&code
_challenge=9cQ5rg8PsWtxFuLCbhTnxqdGJxJRLeqzKwMMBez81j0&code_challenge_method
=S256 HTTP/1.1
Host: max.proeftuin.uzi-online.rdobeheer.nl
```

B: Request access token

```
POST /token HTTP/1.1
Host: max.proeftuin.uzi-online.rdobeheer.nl
Content-Type: application/x-www-form-urlencoded
Content-Length: 315
grant_type=authorization_code&code=678713c9bfd94391a3e33c59e653dab2&redirect_uri
=http%3A%2F%2Flocalhost%3A9000%2Foidc%2Flogin&client_id=006fbf34-a80b-4c81-b6
e9-593600675fb2&code_verifier=a8d5c772d3e4ca73cd81bc9e58457aafbd2c9f47a0932f65
478c5488b81c78475c05a29b38cd7f8824aa45925f9fdf6b6e77536d44afea954c9a1bb35256
5070
```

C: Request authorized resource (user info request)

```
GET /userinfo HTTP/1.1
Host: max.proeftuin.uzi-online.rdobeheer.nl
Authorization: Bearer 7aef577745ad442788cc454cc5a6ca14
```

D: User data object (voor zorgaanbieder versleutelde, door CIBG gesignde payload)


```
eyJhbGciOiJSU0EtT0FFUCIsImN0eSI6IkpXVCIsImVuYyI6IkExMjhDQkMtSFMyNTYiLCJ0eXAiOiJKV1QiLCJ4NXQiOiJuTjFNV0F4VFlNSDE4TjlwUFYyVUhiVVlUNU5ZMHJPX1NodDItZlVYX2c4In
0.HpnnLnzfbFInMp5eiH7n20mYWJaXFrvD1JDc483QS5jcbtCdags03pbM3_2ta4WnqYytFE7ETliB5FLge7C6NJEGbIwFIatKdBsEumIFvMmKbFSEMpzLj858vyn61NL1BcHK5TezXMPNya-ifRBXL
1xDgHfQ0_gMY--DeG1_li03Nih2dwPO8JOnGGazcv9racWG1W3wqM3DB9Ip5c2UvB_GOl6js-XiN0JCGgXUxwnjmr_6ZYu93k7IGS0pfBtR14Em03YuKHG0h86BJlLBePlVX6aeapjjgXRkE244_R
UQvvs7XqGufwwFs1ojw18m17aPzAaV67Oda6VCuOdt7w.Oyp49Wab5gh619FUDA1a2w.SdZ9MB1_fa_dZtR3qISF4awO-C59aboLyIrcO8hTUx_IL_N7LJ1iG1iUVNikjXj2_XdB2XyvQ24TUVZX
hvMjajcdzcfh28FxKfa0Mzwo8IwkdtY5-ZtchCD965SgufLsaASGFos9173f_XaF3-KncoyWcAQ8WnUkRcVYVg5wcnANDVlY7Ltp6xwNlfic5yAz-v2HC9_bFVehYUPNafnPEQYmUPpQLyo5gr56jXy
r5SZRByWzCcPvqJ-xXjKoydNnvII54-zc71rBY2JEzPvGdZCVoPViuK1n0O6xwYIPf7KNG2eZ4k6DPWKWUS72rL-vDfrGZ7ezlM3d1pSxyOcoojLy29DoLSmKKYk78xfKS4gzOC4E1RgYP7ieFmvJE
1BiO_uumazr5lp2w7Zwz9TJ6UyoKbrRmD6G5kXx0prHiUB-oDE6FKcxQfGbA7qLV8WiX8FbVS3sHnqG8VcLKEJBCdCQJyNXj5ORP_FFcXqqaBv5HcDBURyPCgboZO0jR-MPN_luy6QgaKDtAnkI
cVoBUUCS7OanxeVgKWtJR6j962sghDO3x0V-V1md4Xnifxet9Zy9xGaGz98fIAaN4BMU_LldQzuQp-bupIAGQvVZIf0vRu-0QVljbb7MG-y-Myo0KcsyoyGemY6pi22wx9NSsu1y_FZHwrKulWeD
ycYz02OxQkoSVKDrd770BRxjyjArvPMiGGGsamqlGuWQ4nAqKuxGdorVsHwBKtkSGPLQiRFI7-iAI4o8gII-a6fFNwxNgxS6mW19434CbmS6EQkx3LA2M8tAuzGs7MUvbjRLVJNwQi9TMwFtglry
kItY40eNSDuzwBorvBliB22FfmUrs6gCPGp5xFZQhEgriqQyAHuEG0H_5yfJlEkAUfU3S5B4ZgAVIEuFOdZObYQkDxYtJU69vBJHAQtdqnrs9rxI0UOQYgzRxb84guypyXkOe0ie5Piq2G35i3bnP40
urzs7pq4tp75LQURYOauW8R3S6WriopFTxR_y-JkgwyFo2eVzjKw4aIw8-SOnN4X4Pd1gfK2eladQ52T1Ug1fctJ23VOSvSH3fvXmhgwZj3nBMpJiwPupWP-APO1e2DJGvtACb9OWekV9XrWQKm
TNBGf5ir9kSpGQaEAfhaab5H5OXFDkpvncU5paeBrxoCuXhAw_onYm5iDnswzSnUp3Kz80IASIX4qiZ-wNdZYzUOVeLafvcRdSSEpKkaLd6KRF1IP-SEq6aNto2ttnpBM69ZixN2jfR9PXsm8ep6xF
yfKz_Zvdo7weNmMYYMXrm25JprWV2s1GFnBV77SCA10WEFhh4Y36T85Vc8Hrc9WjyWWPSRjsF6esh5DD6bhbEoTgUrteLqKDPfA1DCvht-DjhI57sEvc7z1n3rY1S__O9vfb0bcSBdrqOLB7Oto
BL1chSbJp_1CBIBv9JpZVuXV5x9hxyzgi2td-PnYkOUOZP8ibcAbyIkyoKYvIyWNM1yeDN6LVsPpGQSrAn5l4frYO8ml6Bj16Y1FqvDEwgwTTJBEhjU0y8NIlVLBvK6NHYGlfiFXGz1nrRzfCgB81xbTc
xqV9ZHkLboLw4IAWrwG8D3dBofFuSLATaY0XjMAMYBT4eZkku0gSSPsdjtqHbkHEAL4dmw6NeTHCQ3BG2-Ap8OP952bOdUrBN-n0qKrD5AelCh5FlUHzevJ6IctKU3GuL0pFQbHKXl5MrZ22lYa
dk1zW2uXtKph2cGluGHdr04nTTb884EpEJi1IGAmbcozPgk2JL1hUwgHI2Q_fB1FvWS1I1yBXipIMYngIcZPPoBFy-jPi2Fs3Z9jKywiwzox77VXhLmXH8sJaAhKNVOEF_B8DLvR8m_XSbKj7rnv8-
bXpBSr4HBkrXYwIZTPazdK7VzZtehRV0AQhpD7jh0pDS_2-q_8MvSWYwHuc3qdMmbwzj4nsFOYmm84XWzckcxThdxpNR7hKGY0IBEmj5Oak8iQ-G2E0svzTQM1eJOAQg-MyBasyNiTRa9061
N0FwZAQSieOvEg6R1eEEMxyZDcmi8MO0t4Kkaq4Q2-Qq8ITLozAchoF6G3IkKlmT2IJ7ujxzjSQ2erniZU3gj0MrQqnOMhBpPCUff74wvWtgyRQIlXaXi_Jk23w8Ir5DjDY5TgyDrH4nXZh32-qZhd
AoggiCJ6Feq5zdb65VgEVez9hZ8Xqm_R6G7BZFC9XZvB-RilqmIIxJyk0AxCaTlVD1oi4EPiBknCNMLwSDXRH36AB3dA0KqeRAhmoR7bT5zQWhTSwYGRTOGIQxRUoADSFEqHNf_Mkw9imEnh
ajQK-emONxLKNnAFlG7Ser9nZMaTFWABBpIGCKUQZTUGmd12A0mDDIJnCRhxdB2YH1vYknXshb0H2nUmFz75fvsFOcurU2_SapWBHNAd8IKBdD2wX2HdCd81vyMtyRkCeljqRlXyJXrtXM9e
h6HiSCrOoKeRRw1SdAbUp3Ygc6c6jHVyhxblTQnVCurHM00rgSouFH2MNl8FIO2gsOYeevSoZwU9Y6PEuS72hEmzziKV7KBrpw2fztnSALpveB5NMGhGGU3I63EUQzbaRChrXRBQuahOlPesNg0
CNC-MKI1G8ws670vsIe8LSRGJzH1BZX33bRr_Lq2IMh3lYy4N41z6k8m_4Ps9Qic3IL6PpsveuP4-AeFJZ7wmIS3tj-D4KnO51mRrVp1Tvdeq69BpQNxesOccEmnBKqxczULyUluU6oPVIiEmA8qQ
eNcryTMJfc2EK7S21HUueOty_PZhmnk5fOWY0sQOlfeYa3BiII-lRzDgCpeCxzC6U33ASfYvZFQd6d2CUaewyGOkMUc7_3jPrZNJ-c_y1k8ESkmcOygAe72eNLVDh2PbJlpKV-u-c8yYFH9fAcOlI0s
Hx6HCYiL5Sz5XWCjLRTCW0850seGS_lx4u2btYReHTepPlRvII_QZWA5o7qYReq8ysPjqGuzCBXn2jtWJcP3X5hO1vo36qdMQON7Jnq6UfS41062NdFuV2MJOd9eVJzEIJodps2R_ErkCDs8LTkSx
Xj1U5LtZ38p1CEZHvgqs72UhLTtN8DhtZszf_9xav5gEkx6Qwz2cBwORvoWfk-r3hC2hN5vtWWOo0lx7TxG5t2iuAE19jkrDqNZWBHz4z6nVYyooA5zZW07J05zRe_guwDbnDTHzP9zcJD_PNZ-_
4WvLXvqv_eWzz4LHkXOPs2B4dSudtPwJmskpOjDxUCvfgJ-PyAQMYo5eGS33GUK5W_5_4Amn82HS5pXLkQOB5QTNHY0_sbl_maeE0Lr35uGO_Lt5ZPqVNTafbQKouwa-cdoM8o0IBvNODHX
am07OD0TXTrkQ4mQlc9lBryPrriQGvL3HiOCudTtNQWB5pTbZAhqKFKZzGtzaFhT6FoRp94mfwG5fWZQQB3E2ysqrNqZ1ADt14bL9V9G5lsPaoqPt61-SUf_PX4_461vTvnnJz-ulKWaCEVGbCor4
_l-8dyhFgf3hLy1hOgwQyg5V4eDN-PXzHpXXnRJKinFrU1yQ02TN2biNJ0AkaOEMlyvV1uBGuSItXHe9aDYEW5Q8m-mVhuupLYjQSLKbwcIvONDoVpzYa8AFSQfiTyehg8cYzBv5geWk86UYYUH
B0_dolVoguL88cI5vy6--CgK0WqOm6iOQ7jXpA_tLKUqKNA06cYoB2TH6eLhWN9Ms6nf7yUBwgWKmzkFunKLRMc_Vlj-loQT91HHE4yaaOxd0zQJjy7D-MZQqzWBEND7VUNPIN-J7SN7t4U9se
f3Z7Z9kOQ7VjOiWiQ33JFtEqQNGLntOxbPSj2bEHsWr8D9piQ99ls_evjZlJf1eCDaLOViDX2rhtNv29SYKjoBeOOe0xGRNPnYYbMsJOeHXKNDG8ANSOfqBm.jd5FjZMPca0uz9w6SMHsAA
```

D: User data object ontsleutelt door zorgaanbieder


```
eyJhbGciOiJSUzI1NiIsImtpZCI6IjFNY2p3cjgxMGpOVUZHVHR6T21MeTRTNnN5cVJ1aVZ1YVM0UmZyWmZwOEk9IiwieDV0Ijoibk4xTVdBeFRZTUgxOE45cFBWMlVIYlVZVDVOWTByT19TaHQyLWZVWF9nOCJ9.eyJhdWQiOiIwMDZmYmYzNC1hODBiLTRjODEtYjZlOS01OTM2MDA2NzVmYjIiLCJleHAiOjE3MDE5MzM2OTcsImluaXRpYWxzIjoiQi5CLiIsImlzcyI6Imh0dHBzOi8vbG9jYWxo
b3N0OjgwMDYiLCJqc29uX3NjaGVtYSI6Imh0dHBzOi8vbG9jYWxob3N0OjgwMDYvanNvbl9zY2hlbWEuanNvbiIsImxvY V9hdXRobiI6Imh0dHA6Ly9laWRhcy5ldXJvcGEuZXUvTG9BL2hpZ2giLC
Jsb2FfdXppIjoiaHR0cDovL2VpZGFzLmV1cm9wYS5ldS9Mb0EvaGlnaCIsIm5iZiI6MTcwMTkzMzYyNywicmVsYXRpb25zIjpbeyJlbnRpdHlfbmFtZSI6IlpvcmdhYW5iaWVkZXIiLCJyb2xlcyI6WyIw
MS4wNDEiLCIzMC4wMDAiLCIwMS4wMTAiLCIwMS4wMTEiXSwidXJhIjoiODc2NTQzMjEifV0sInN1cm5hbWUiOiJKYW5zZW4iLCJzdXJuYW1lX3ByZWZpeCI6InZhbiBkZXIiLCJ1emlfaWQiOiI5M
DAwMDAwMDkiLCJ4NWMiOiJNSUlEMWpDQ0FiNENDUUQwRmx2SnNiY3J2VEFOQmdrcWhraUc5dzBCQVFzRkFEQW9NUXN3Q1FZRFZRUUREQUpWXG5VekVaTUJjR0ExVUVBd3dRYVc1bpTM
DJMWFY2YVhCdlI5MWpZVEFlRncweU16RXlNREV4TWpNek16QmFGdzB5XG5OVEEwTVRReE1qTXpNekJhTURJeEN6QUpCZ05WQkFZVEFsVlRNU013SVFZRFZRUUREQnB1YkMxMWVtbHdiM
k10XG5jR2h3TFd4aGNtRjJaV3d0WkdWdGJ6Q0NBU0I3RFFZSktvWklodmNOQVFFQkJRQURDQ0FRb0NnZ0VCQXB5QjJDQ0dZYTcwL0VlS2dwc0N0QnRHUmlWVJyb2RWQWN0b
HJPTUhFZDI2aGpSdmN0TGZOaXl0MFF5QkZseKN2XG4wVkRYUjc3OWVvU1E2bWdPYURjNzFrYi9zR1dxbjhMZFE3NEp0WTVnSTVxRzduM1JYM0VRWkxFdGIxNmp6WWROXG5LMU5mMm9G
K0tNV2t2eWMwVjlSNWUyNjdyTjJpUklHQlNKUTFmZmN4RHFUZnJNVmxjaFYyZmdWVDdZTzQ3U25qXG5MMXdDK0Z4cXhTRzc1N056OHlleVBncjJaazFvaWF6dHhQY1hXRlpTklGWm9KUzlp
VzdITTZyQ2O4WjcvbVJjXG40Qm5kbC9wbkZIMjVrZmhPZzlKSVVNbzFvcjltbDZDSXN6Um9aL2hTOHZCOUduNldUS05CYUgxMTB6Sno4eXNkXG42cXM4WkpCYURia0pnSTZMNlZtL3d0OENB
d0VBQVRBTkJna3Foa2lHOXcwQkFRc0ZBQU9DQWdFQWI6eEJmYUFhXG5ETlFOOWhYS0ZKZVB6N2RUUEx3SFkvWmpDNDlkUXJ0eVd6ZmdyMUxLaTRvMWI4amtkZzJGWFU5dCt4TXVXZ3hY
XG5GZGJqT0pMZGNRWVdFWWIrVzdLbWtnbEljUDhiT2tSRFdmcGxnc2twYVRvZ1JLMDk1UzFDdU1NOXYwYktDL3RzXG5kSGIzVWZxVzRVNFprbzM4L1VlOWZSRjhyYTJwNzFRRnM4K250L0J
Bd0NrenJOTHpheE1ZOC8vVGlGVStaRVlMXG56UElRQmpLYVlCOHlWaDBXaDNxYWllQjJCektVYW4rRXlzaDJiVWM5VHBsUXlrSWRrNHo2VCtGTzVLVGo1ZVZrXG42enBIZmxXV0NUNjF5MTVtd
TN4QUViODNyT2YrekZwb05HaURzc2lrbzBPZUxLN0ZscWg3SHVDUDI2Tk5ud3NiXG5WR3drZzYwcER1K0FTRzJhbTNUUGlmM0pwSTdza3pBQkZ3NHZidlBVcElrNktM3IjQzk4R3lYb3dRdWpJ
MFpUXG4xNmRYZmgxRTM4cHNSVWVPNW8rdXhZNk1VUFhOU2lvWVowbWYzQkFSTGFoTjQxcnF4S1h6NU1MMURTWm5JT1pLXG5GM3BlU2dnYVpvUmkxaDByNlcxNFdFY1l2eGRIRGtWUjZ
NMXFXMGk3WWVJQms2a2FYRWt3Q21GejNoazV3OWFuXG5XSkRqbk1xU1JnUnNGVmNJTC9FemkvRWx1YmsyMWY0TEhURVFtc2p6emQxRytkMDlmamRJNkpyaFlNZnRHdVlaXG40ak9aWl
dwem9NSDFUaVpaK0prQmR5UndFZGJxelcrdisvMEJaUXk2SFJhWmxvbWJjT21TOU1TakZSRFk5VUdXXG5EOUYxZVVJcUtjdDB5eUpQUFhIM2xEa3pxcXRYNERMY29wbzBifQ.VvzIXZ8FCIwxv
P3Wc4kLvIgQChJZAhS-DcKKvkiZg677w-ZRciIFCWUH5oXLqG-emyV4f87tIoWnp4TY3gGFNljNrtITVCv3zXaTCxHwzL6q2QCs1liBus2uPv0kjBtzeve2G5_Owst3ndeUcwLJPnTIoYRLvbjjaPkFTg
49K5ZTpN8E9dI7Gimwgv_rZ1fOH7XrAwITY-jF34wsR_K17wHI5Zp237_HcAPqnMI8P3U7u74Vu-3mqCePubVBDnT4bGcd4flZCFH-LTDhew9BO4cBkBxafAev7OB5A9qGOKEtRynTDAOkazyb8
_qwJAGnyCAVxBQ4VFRB1-cE576TLQ
```


Header:
```
{
  "alg": "RS256",
  "kid": "1Mcjwr810jNUFGTtzOmLy4S6syqRuiVuaS4RfrZfp8I=",
  "x5t": "nN1MWAxTYMH18N9pPV2UHbUYT5NY0rO_Sht2-fUX_g8"
}
```
Payload:
```
{
  "aud": "006fbf34-a80b-4c81-b6e9-593600675fb2",
  "exp": 1701933697,
  "initials": "B.B.",
  "iss": "https://max.proeftuin.uzi-online.rdobeheer.nl",
  "json_schema": "https://max.proeftuin.uzi-online.rdobeheer.nl/json_schema.json",
  "loa_authn": "http://eidas.europa.eu/LoA/high",
  "loa_uzi": "http://eidas.europa.eu/LoA/high",
  "nbf": 1701933627,
  "relations": [
    {
      "entity_name": "Zorgaanbieder",
      "roles": [
        "01.041",
        "30.000",
        "01.010",
        "01.011"
      ],
      "ura": "87654321"
    }
  ],
  "surname": "Jansen",
  "surname_prefix": "van der",
  "uzi_id": "900000009",
  "x5c":
"MIID1jCCAb4CCQD0FlvJsbcrvTANBgkqhkiG9w0BAQsFADAoMQswCQYDVQQDDAJV\nUzEZMBcGA1UEAwwQaW5nZS02LXV6aXBvYy1jYTAeFw0yMzEyMDExMjMzMzBaFw0y\nNTA0MTQx
MjMzMzBaMDIxCzAJBgNVBAYTAlVTMSMwIQYDVQQDDBpubC11emlwb2Mt\ncGhwLWxhcmF2ZWwtZGVtbzCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB\nAKbCCGYa70/EeKgps
CtBtGRiHYRrodVActlrOMHEd26hjRvctLfNiyt0QyBFlzCv\n0VDXR779eoSQ6mgOaDc71kb/sGWqn8LdQ74JtY5gI5qG7n3RX3EQZLEtb16jzYdN\nK1Nf2oF+KMWkvyc/V9RSe267rN2iRIGBSJQ1
ffcxDqTfrMVlchV2fgVT7YQ47Snj\nL1wC+FxqxSG757Nz8yeyPgr2Zk1oiaztxPcXWFUINIFZoJS9iW7HM6rCm8Z7/mRc\n4Bndl/pnFe25kfhOg9IUMo1or9mI6ClszRoZ/hS8vB9Gn6WTKNBaH1
10zJz8ysd\n6qs8ZJBaDbkJgI6L6Vm/wt8CAwEAAaNBgkqhkiG9w0BAQsFAAOCAgEAizxBfaAa\nDNQN9hXKFJePz7dTPLwHY/ZjC49dQrtyWzfgr1LKi4o1ixjkdg2FXU9t+xMuWgxX\nFdbjOJLd
cQYWEYb+W7KmkgIcP8bOkRDWfplgskpaTogRK095S1CuMM9v0bKC/ts\ndHb3UfqW4U4Zko38/Ue9fRF8ra2p71QFs8+nt/BAwCkzrNLzaxMY8//TiFU+ZEYL\nzPIQBjKaYB8yVh0Wh3qaieB2
BzKUan+Eysh2bUc9TplQykIdk4z6T+FO5KTj5eVk\n6zpHfIlWWCT61y15mu3xAEb83rOf+zFpoNGiDssiko0OeLK7Flqh7HuCP26NNnwsb\nVGwkg60pDu+ASG2am3TPif3JpI7skzABFw4vbvPU
pIk6Im3ycC98GyXowQujI0ZT\n16dXfh1E38psRUeO5o+uxY6MUPXNSioYZ0mf3BARLahN41rqxKXz5ML1DSZnIOZK\nF3peSggaZoRi1h0r6W14WEcYvxdHDkVR6M1qW0i7YeIBk6kaXEkwC
mFz3hk5w9an\nWJDjnMqSRgRsFVcIL/Ezi/Elubk21f4LHTEQmsjzzd1G+d09fjdI6JrhYMftGuYZ\n4jOZZWpzoMH1TiZZ+JkBdyRwEdbqzW+v+/0BZQy6HRaZlombcOmS9MSjFRDTyUGW\nD9
F1eUIqKct0yyJPPXH3lDkzqqtX4DLcopo="
}
```

Bijlage 4: Inner JWT en outer JWT