



Ministerie van Volksgezondheid,  
Welzijn en Sport

# Koppelvlakspecificatie UZI-Online

Koppelvlak 2: Middelenleverancier

## Colofon

Projectnaam	UZI online
Organisatie	iRealisatie
Datum:	23 februari 2024
Versie:	1.1

# Inhoudsopgave

<b>1. Inleiding</b> .....	<b>4</b>
<b>2. Gegevensverwerking</b> .....	<b>4</b>
<b>3. Onderdeel 'identiteitsvaststelling'</b> .....	<b>5</b>
3.1 Introductie.....	5
3.2 Architectuur.....	6
3.3 Het verkrijgen van een zorg identiteit.....	6
3.4 Het ontkoppelpunt (OIDC-gateway).....	7
3.5 Koppelvlakspecificatie.....	7
3.6 Gebruikte standaarden.....	7
3.7 Message encryption.....	8
3.8 Message signing.....	9
3.9 Geen single sign-on (SSO) en logout.....	9
<b>Bijlage 1: Gehanteerde begrippen</b> .....	<b>9</b>
<b>Bijlage 2: Sequentiediagram Zorgspecifiek middel</b> .....	<b>12</b>

## 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 die worden opgestuurd:

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 zorgspecifieke middelen. Dit betekent dat men in staat is om zich te identificeren en authenticeren door middel van een ziekenhuispas, telefoon, tablet, token, etc. Door meer inlogmiddelen toe te voegen, wordt het toegang krijgen tot een zorgplatform makkelijker en gebruiksvriendelijker via het UZI-stelsel.

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

Op dit moment is de functionaliteit voor het gebruiken van een zorgspecifiek inlogmiddel alleen beschikbaar op de Proeftuin, de testomgeving voor het UZI-stelsel. Op basis van testen met toekomstige gebruikers, platform- en middelenleveranciers is de ambitie om deze functionaliteit te gaan testen in een pilotvorm. De planning hiervoor is afhankelijk van de voortgang van testen op de Proeftuin omgeving.

In deze koppelvlakspecificatie is voor de leveranciers van zorgspecifieke middelen uitgelegd hoe kan worden aangesloten op de technische omgeving ten behoeve van de identificatie en authenticatie in het nieuwe UZI-stelsel.

Naast dit document met de koppelvlakspecificaties, is er ook een aansluitdocument. Hierin 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

Een onderdeel van het nieuwe UZI-stelsel is het vormgeven van een alternatieve oplossing voor de identificatie en authenticatie van zorgprofessionals en -medewerkers. Hiertoe worden bestaande en toekomstige authenticatiemiddelen ingezet. Dit betreft de middelen die onder de Wet Digitale Overheid ([wDO](#)) beschikbaar zullen komen en erkende Europese middelen ([eIDAS-1](#)) van andere Europese lidstaten.

Daarnaast is er behoefte in het zorgveld om ook eigen authenticatiemiddelen te kunnen gebruiken. Deze middelen worden zorgspecifieke middelen genoemd. Kenmerkend voor deze authenticatiemiddelen is dat deze onder de verantwoordelijkheid van een zorgaanbieder worden verstrekt aan zorgmedewerkers. De eisen aan een zorgspecifiek middel worden beschreven in de NEN-7518 (op dit moment in ontwikkeling).

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 OIDC-provider of OIDC-client. Platformleveranciers maken verbinding via koppeling 1 waarbij het aangesloten platform als OIDC-client fungeert en het ontkoppelpunt als OIDC-provider.

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

**Dit document betreft alleen informatie die betrekking heeft op koppeling 2 voor middelenleveranciers.**

Voor meer informatie betreft koppeling 1 zie het document:  
*Koppelvlakspecificatie UZI-online koppelvlak 1: platformleveranciers*

### 3.2 Architectuur

Wanneer men zich identificeert en/of authenticceert met een zorgspecifiek middel, treedt het ontkoppelpunt (gele blok, figuur 2) op als een OIDC-client van de Authenticatiedienst van het Zorgspecifieke middel van de zorgaanbieder (blauwe blok, figuur 2). De Authenticatiedienst gedraagt zich hierbij als een OIDC-provider. De afhandeling van de daadwerkelijke autorisatie met behulp van het zorgspecifieke middel is de verantwoordelijkheid van de desbetreffende OIDC-provider.

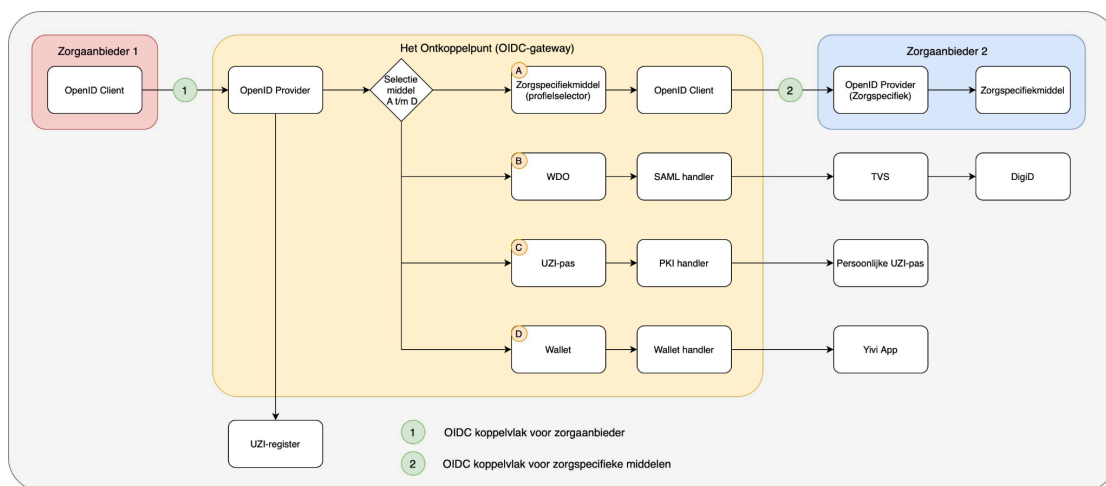
Deze opzet maakt het mogelijk dat ieder soort authenticatiemiddel dat voldoet aan de NEN 7518 kan worden gebruikt waarbij na de authenticatie de OIDC-provider het resultaat van de authenticatie aan het ontkoppelpunt kan meegeven.

### 3.3 Het verkrijgen van een zorg identiteit

In de huidige implementatie is het mogelijk om een tijdelijk JWT-token aan te vragen bij het UZI-register van de Proeftuin. Dit JWT token, dat door het UZI-register is ondertekend, moet worden verstrekt aan het userinfo-endpoint van de OIDC-provider van de ZSM leverancier. Dit token moet als base64 JWT token meegestuurd worden in de 'signed\_userinfo' claim van de /signed-userinfo endpoint van de van de OIDC-provider van de ZSM leverancier.

Het proces vereist dat het token uit het register wordt gehaald en het vervolgens plaatst in de 'signed\_userinfo' claim van de userinfo-endpoint waar de OIDC-client implementatie van het ontkoppelvlak deze informatie vervolgens ophaalt.

Tussen het verkrijgen van de token en het teruggeven om te identificeren moet de ZSM leverancier de identiteit verifiëren. Het is aan de leverancier om ervoor te zorgen dat het token op de juiste manier aan de zorgprofessional wordt verstrekt.



Figuur 2: Overzicht van de koppelvlakken en ontkoppelpunt

### 3.4 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 OpenID Connect protocol de gebruiker inloggen. OpenID Connect 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 OpenID Connect 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 gebruikers identiteit.

### 3.5 Koppelvlakspecificatie

Het zorgspecifieke middel 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. Zie [RFC 7636](#).

### 3.6 Gebruikte standaarden

Tabel 1: gebruikte standaarden

Standaard		Referentie
OpenID Connect		<a href="https://openid.net/specs/openid-connect-core-1_0.html">https://openid.net/specs/openid-connect-core-1_0.html</a>
PKCE Authorization Code Flow (PKCE)	RFC 7636	<a href="https://datatracker.ietf.org/doc/html/rfc7636">https://datatracker.ietf.org/doc/html/rfc7636</a>
SHA-256(S256)	RFC 6234	<a href="https://datatracker.ietf.org/doc/html/rfc6234">https://datatracker.ietf.org/doc/html/rfc6234</a>
JSON Web Token (JWT)	RFC 7519	<a href="https://www.rfc-editor.org/rfc/rfc7519.html">https://www.rfc-editor.org/rfc/rfc7519.html</a>
JSON Web Encryption (JWE)	RFC 7516	<a href="https://datatracker.ietf.org/doc/html/rfc7516">https://datatracker.ietf.org/doc/html/rfc7516</a>
JSON Web Signature (JWS)	RFC 7515	<a href="https://datatracker.ietf.org/doc/html/rfc7515">https://datatracker.ietf.org/doc/html/rfc7515</a>
JSON Web Key (JWK)	RFC 7517	<a href="https://datatracker.ietf.org/doc/html/rfc7517">https://datatracker.ietf.org/doc/html/rfc7517</a>

### 3.7 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.

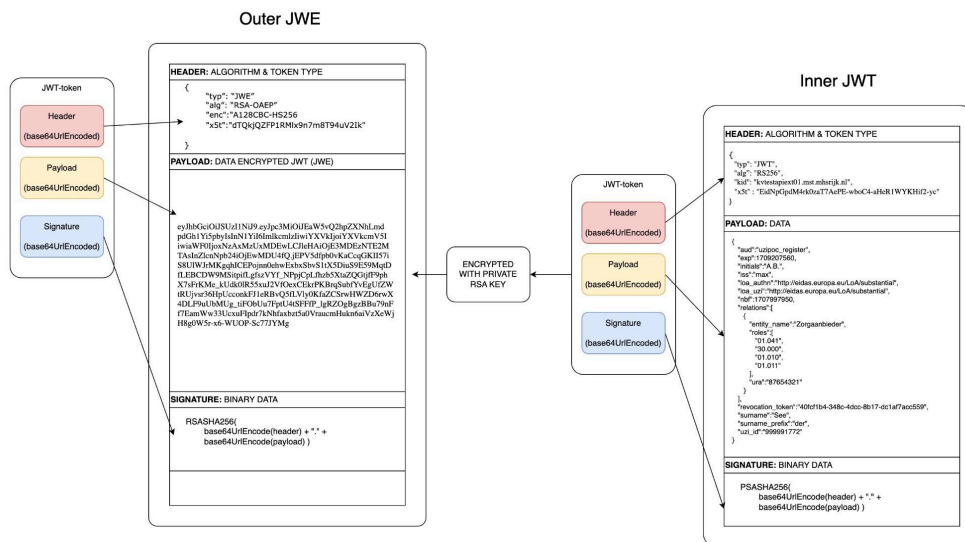
Voor de versleuteling door de zorgmiddelenleverancier wordt de public key van de middelenleverancier gebruikt die bij de registratie is aangeleverd.

De implementatie van het koppelvlak is volgens de specificatie zoals beschreven in de OpenID specificatie waarbij de middelen leverancier de rol van 'Identity Provider' heeft.

Het ontkoppelpunt valideert dat de encrypted en signed JWT daadwerkelijk van de middelenleverancier komt. Dit betekent dat de signature van de 'inner JWT' gevalideerd wordt. De middelenleverancier 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 zorgmiddelenleverancier nodig. In de 'inner JWT' is een 'kid'-header (key ID) opgenomen die moet corresponderen met de 'kid' van de middelenleverancier dat in de jwks-uri staat.

De inhoud van de signed userinfo ziet er als volgt uit:





### 3.8 Message signing

De 'userinfo' die de het ontkoppelpunt opvraagt bij de middelenleverancier is ondertekend met de sleutel van de middelenleverancier. Hierdoor wordt het ontkoppelpunt in staat gesteld om te valideren dat de 'userinfo' onaangepast afkomstig is van de middelenleverancier. Deze validatie moet uitgevoerd worden door het ontkoppelpunt om de betrouwbaarheid van de 'userinfo' 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.

### 3.9 Geen single sign-on (SSO) en logout

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

## 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.



## Bijlage 2: Sequentiediagram Zorgspecifiek middel

Het sequentiediagram van het koppelvlak voor een Zorgspecifieke middel volgens RFC7636.

