Ministerie van Volksgezondheid,
Welzijn en Sport

Aansluitdocumentatie zorgaanbieders proof-of-concept ‘Toekomstbestendig UZI’

Versie 0.6

Datum	januari 2023
Status	Definitief

Colofon

Secretaris Generaal / plv. Secretaris Generaal
Directie Informatiebeleid / CIO

Bezoekadres:
Parnassusplein 5 2511 VX Den Haag

Contactpersoon

L. Kielman
Projectleider
l.kielman@minvws.nl

B. Kerver
Adviseur
b.kerver@minvws.nl

Versie 0.6

Inhoudsopgave

Inleiding

Het ministerie van Volksgezondheid, Welzijn en Sport (minVWS) is bezig met de herziening van het UZI-stelsel. Onder het UZI-stelsel vallen het UZI-register, de UZI-passen en de UZI-Servercertificaten.

In het project 'Toekomstbestendig UZI' wordt de beoogde oplossingsrichting uitgewerkt voor de vervanging voor het huidige UZI-stelsel. Deze oplossingsrichting wordt voortdurend afgestemd met het zorgveld. Dit verloopt via expertsessies, een klankbord, de kerngroep Informatieberaad (IB) en het IB zelf.

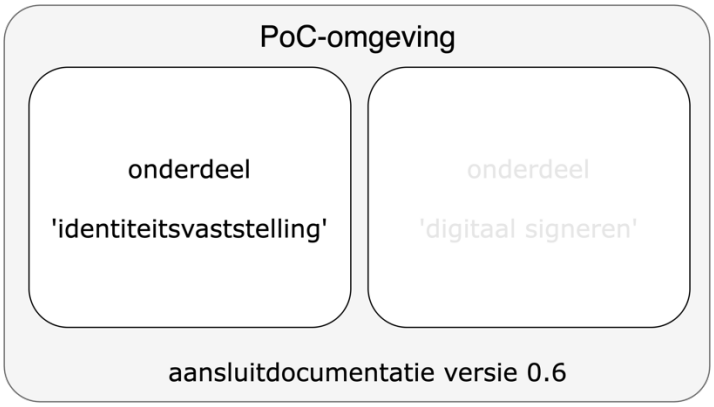
Vervolgens wordt de beoogde oplossingsrichting aan de hand van verschillende proof-of-concepts (PoC) op onderdelen technisch beproefd. Doel is de werking van keten van de oplossingsrichting aan te tonen.

Dit document beschrijft de algemene werking van de PoC-omgeving en is gericht op het ondersteunen van de leveranciers in het aansluiten op de technische omgeving van de proof-of-concept 'Toekomstbestendig UZI' (PoC). Het gaat in de PoC-omgeving om enerzijds de identificatie en authenticatie van de zorgprofessional en anderzijds om de functionaliteit voor digitale ondertekening en verzegeling (e.d.).

De PoC-omgeving en bepaalde implementatie-keuzes kunnen gedurende de PoC-fase nog veranderen. Deze wijzigingen zullen in een volgende versie van dit document worden beschreven.

In deze versie van het aansluitdocument (versie 0.6) is voor de leveranciers en zorgaanbieders beschreven hoe kan worden aangesloten op de PoC-omgeving voor:

- Identificatie en authenticatie van een zorgprofessional (onderdeel "Identiteitsvaststelling")



1. Algemeen

1.1 Gehanteerde begrippen

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 Zorgtoegangsdient.
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.
Rolcode	Kenmerk(en) van een zorgprofessional 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 zorgverlener 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 zorgprofessional (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 zorgprofessional in de context van de zorgaanbieder. De zorgidentiteit bestaat uit een aantal kenmerken. Dit zijn ten minste: UZI-nummer + URA-nummer + rolcode(s)
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 zorgprofessional aan de zorgaanbieder. Zie ook OIDC-gateway.

1.2 Gegevensverwerking (AVG)

De OIDC-gateway verwerkt op de titel van het CIBG de volgende gegevens van een zorgverlener:

- 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 (bv computer, telefoon)

Omdat in de PoC met test-data (test inlogmiddelen, test zorgidentiteiten) wordt gewerkt, is er geen DPIA uitgevoerd.

De verwerking van daadwerkelijke persoonsgegevens in de PoC is beperkt tot het IP-adres van het apparaat van de gebruiker die test met de PoC-omgeving (bv computer, telefoon).

Zodra er wordt besloten de ervaringen uit de PoC-omgeving te gaan beproeven met echte gebruikers wordt er een pilot-omgeving opgebouwd. Een dergelijke technische pilot-omgeving staat los van de PoC-omgeving. Per pilot een (afzonderlijke) DPIA worden uitgevoerd. Pilot-omgevingen vallen buiten de scope van dit document.

2. Onderdeel 'Identiteitsvaststelling'

2.1 Introductie

Met de huidige 'UZI-passen' kunnen zorgprofessionals zich digitaal identificeren. In de huidige situatie zijn er persoonlijke UZI-passen ('Zorgverlenerspas' en 'Medewerkerspas op naam') en UZI-passen die door een aantal zorgprofessionals gedeeld gebruikt kan worden ('Medewerkerspas niet op naam').

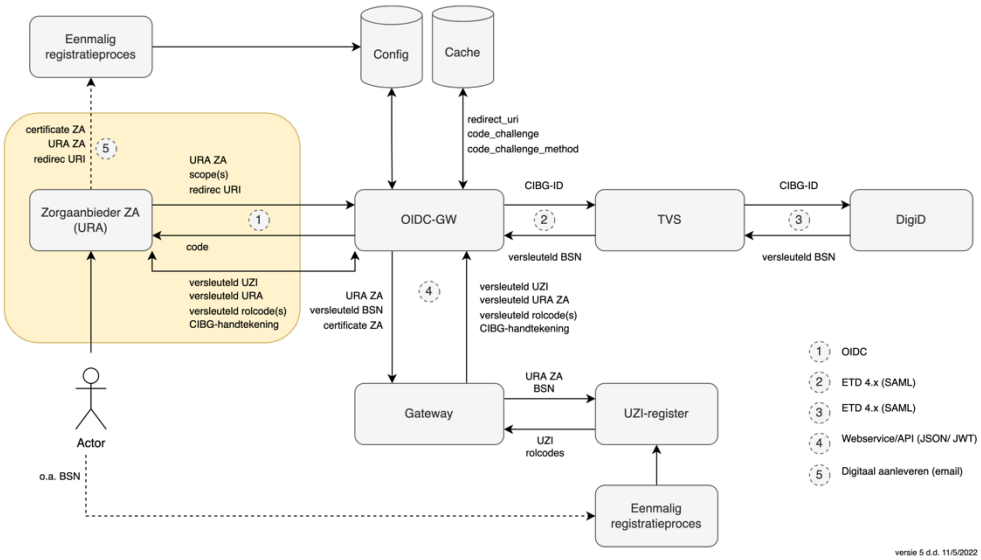
Een van de doelen van het project is iedere zorgprofessional uniek te kunnen identificeren. Dat betekent dat in de toekomstige situatie alleen nog persoonsgebonden identificatiemiddelen onderdeel zullen zijn van het stelsel. Onderdeel van het project is het vormgeven van een alternatieve oplossing voor de (unieke) identificatie en authenticatie van zorgprofessionals. Waar mogelijk worden hiertoe bestaande en toekomstige authenticatiemiddelen ingezet, bijvoorbeeld de middelen die onder de wDO beschikbaar zullen komen.

Binnen de PoC-omgeving is het mogelijk de werkende keten van de authenticatie van een zorgprofessional te beproeven. In de PoC van de werkende keten worden momenteel DigiD, de UZI-pas en een wallet als authenticatiemiddel beschikbaar gesteld.

2.2 Architectuur

Om een beeld te krijgen van de componenten die een rol spelen bij het onderdeel 'identiteitsvaststelling', is in onderstaande afbeelding de samenhang abstract weergegeven (zie bijlage 1 voor grotere afbeelding). Het relevante koppelvlak voor de zorgaanbieder, waarmee een aansluiting is te realiseren de PoC-omgeving, staat in het gele kader.

<u>Het gaat om het koppelvlak met de OIDC-GW (weergegeven als 1).</u>



De volgende stappen worden bij de 'identiteitsvaststelling' doorlopen:

- De zorgprofessional benadert de online-dienst van de zorgaanbieder.
- Deze applicatie verwijst voor authenticatie naar de OIDC-gateway (1).
- De OIDC-gateway toont een selectiescherm met authenticatiemiddelen.
- De zorgprofessional kiest het authenticatiemiddel en wordt via de TVS (2) doorgeleid naar het authenticatiemiddel (3), in deze DigiD.
- Na succesvolle authenticatie bij DigiD wordt de zorgprofessional met een versleutelde identiteitsverklaring teruggestuurd via de OIDC-gateway (3,2).
- De OIDC-gateway levert de versleutelde identiteitsverklaring af (4) bij het CIBG die daar een versleutelde zorgidentiteit mee samenstelt en verwijst de zorgprofessional door gaan de applicatie van de zorgaanbieder (1).
- De versleutelde zorgidentiteit kan door de zorgaanbieder worden opgehaald en ontsleuteld tot leesbare zorgidentiteit (1).

2.3 Koppelvlakspecificatie voor de zorgaanbieder

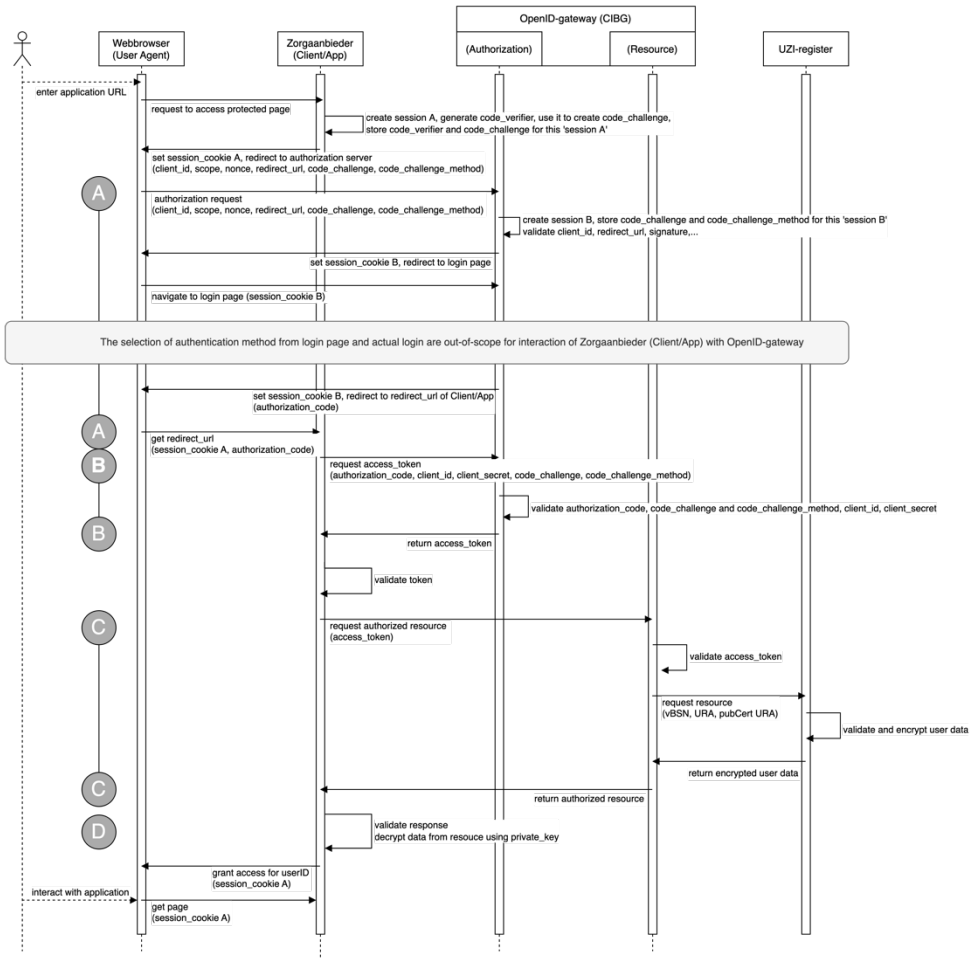
De zorgaanbieder dient aan te sluiten op de PoC-omgeving op basis van de technische standaard OpenID Connect (OIDC)[1]. Dit is een beheerde, open standaard die een technisch koppelvlak biedt dat eenvoudig implementeerbaar is.

Van de OIDC-standaard wordt de Authorization Code flow gebruikt met PKCE. Deze is beschreven in RFC7636[2]. Er wordt gebruik gemaakt van de SHA-256 (S256) 'code challenge method'. In de vraagberichten wordt de URA van de zorgaanbieder gebruikt als waarde voor het 'client-id'.

[1] https://openid.net/connect/
[2] https://tools.ietf.org/html/rfc7636

2.4 Sequentiediagram

Het sequentiediagram van het koppelvlak vanuit Zorgaanbieder (volgens RFC7636):



In hoofdstuk 5 zijn voorbeeldberichten opgenomen van stappen A t/m D. In bijlage 2 is een grotere versie van dit diagram opgenomen.

2.5 Message signing

Alle (JWT-) berichten in de uitwisseling worden door de afzenders gesigned op basis van public/private keypairs.

- De zorgaanbieder gebruikt voor het signeren het bij de registratie aangeleverde certificaat. Voor de PoC moet een minimale sleutellengte van 2048 bits RSA worden gebruikt om de private key te maken. Er kan bij de PoC een self-signed, een PKI-O of UZI-

  Voorbeeld aanmaken van self-signed sleutels met behulp van openSSL:

  openssl req -x509 -nodes -days 365 -newkey rsa:2048 -keyout private_zorgaanbieder.key -out public_zorgaanbieder.crt

  server certificaat worden gebruikt.

- De OIDC-gateway maakt gebruik van een certificaat.

  Gebruikelijk is dat OIDC software-bibliotheken certificaatbeheer zelf regelen. Het certificaat is (door de applicatie) te downloaden vanuit de JWKS die te vinden is via de "jwks_uri" uit de openid-configuration:

  https://poc-1.uzi.bavod.nl/.well-known/openid-configuration

- De Resource maakt gebruik van een certificaat om de berichten te signen. Er wordt in de PoC gebruik gemaakt van de public key van het UZI-register (CIBG).

  Gebruikelijk is dat OIDC software-bibliotheken certificaatbeheer zelf regelen. Het certificaat is (door de applicatie) te downloaden vanuit de JWKS die te vinden is via de "jwks_uri" uit de openid-configuration:

  https://poc-1.uzi.bavod.nl/.well-known/openid-configuration

2.6 Message encryption

De bron met gegevens (OAuth Resource Server) die via het userinfo endpoint wordt ontsloten, levert een JWT waarin onderdelen zijn versleuteld voor de aanvragende zorgaanbieder. Dit zodat het bemoeilijkt wordt voor (eventuele) tussenliggende schakels in de keten/infrastructuur de inhoud van het bericht te lezen.

De data is versleuteld op basis van JSON Web Encryption (JWE) volgens de specificatie van RFC7516[3].

Voor de versleuteling wordt door de Resource gebruik gemaakt van de public key van de zorgaanbieder die bij de registratie is aangeleverd.

De implementatie is volgens de specificatie zoals beschreven in: https://openid.net/specs/openid-connect-core1_0.html#UserInfoResponse:

> If the UserInfo Response is signed and/or encrypted, then the Claims are returned in a JWT and the content-type MUST be application/jwt. The response MAY be encrypted without also being signed. If both signing and encryption are requested, the response MUST be signed then encrypted, with the result being a Nested JWT, as defined in https://openid.net/specs/openid-connect-core-1_0.html#JWT.

De client van de zorgaanbieder ***moet*** valideren dat de encrypted en signed JWT daadwerkelijk van het CIBG komt. Dit betekent dat de signature van de 'inner JWT' gevalideerd moet worden. De OpenID-gateway biedt hiertoe een OpenID Connect JWKS Endpoint aan volgens de specificatie van RFC7517[4].

De locatie van JKWS is via de OIDC-configuration van de Resource te vinden.

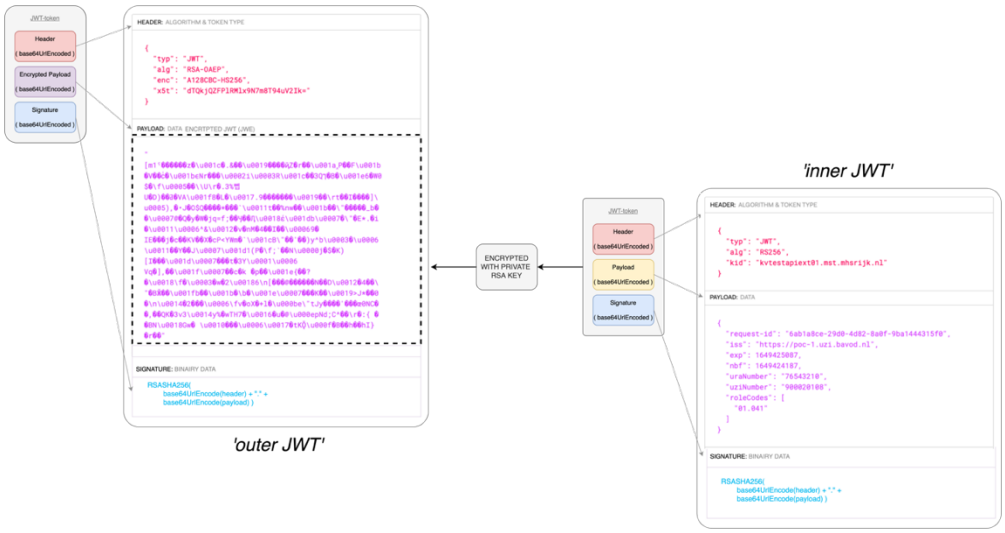
Gebruikelijk is dat OIDC software-bibliotheken certificaatbeheer zelf regelen. Het certificaat is (door de applicatie) te downloaden vanuit de JWKS die te vinden is via de "jwks_uri" uit de openid-configuration:

https://poc-1.uzi.bavod.nl/.well-known/openid-configuration

[3] https://tools.ietf.org/html/rfc7516
[4] https://www.ietf.org/rfc/rfc7517.txt

Voor de validatie van de signature is de public key van het CIBG (de Resource Server) nodig. In de 'inner JWT' is de 'kid'-header opgenomen die *moet* corresponderen met de 'kid' van het CIBG die in de jwks-uri staat.

Onderstaand figuur is de schematische weergave van de JWT die het userinfo endpoint oplevert (stap D sequentiediagram). Links in het figuur de 'outer JWT' met in de header informatie over de encryptie van de payload en de daarvoor gebruikte public key. In de payload de op basis van JWE versleutelde JWT met het user data object. Rechts in de figuur de via de private key van de zorgaanbieder ontsleutelde JWT met in de header de 'kid' van het CIBG, in de payload de informatie over de geauthenticeerde zorgverlener. De signature is van het CIBG volgens de specificatie in de header gemaakt en te valideren via de 'kid'.



2.7 Transportbeveiliging (TLS)

Er dient adequate transportbeveiliging te worden ingeregeld. In de PoC kan gebruik gemaakt worden van een self-signed of een PKI-O certificaat.

2.8 Berichtstructuur user data object

De structuur van het bericht met daarin de user data, kan worden gevalideerd door een JSON-schema. De huidige versie van het JSON-schema is te downloaden van:

https://www.inge6.nl/json_schema_v1.json

NB: bij een nieuwe versie van het koppelvlak 'identiteitsvaststelling' zal een nieuw JSON-schema worden gebruik. Een verwijzing naar het gebruikte schema is onderdeel van het antwoordbericht.

2.9 De zorgidentiteit (user data object)

Het user data object kent na decryptie de volgende velden (claims) die de zorgidentiteit bepalen:

Data over de zorgverlener:

initials	<string>	Initialen van de zorgverlener (comfortinformatie)
surname_prefix	<string>	Tussenvoegels bij achternaam (comfortinformatie)
surname	<string>	Achternaam (comfortinformatie)
uziNumber	<string >	UZI-nummer van de zorgverlener
relations	<list of object>	
uraname	<string>	Organisatienaam (comfortinformatie)
uranumber	<string >	URA-nummer van de zorgaanbieder
roles	<list of string>	Rolcode(s) van de zorgverlener bij deze URA

Technische data bij de zorgidentiteit:

json_schema	<string>	URI van het JSON-schema van het antwoordbericht
request-id	<string>	Technisch nummer bruikbaar voor auditlog
iss	<string>	Autoritieve bron (Issuing authority).
aud	<string>	Audience van/voor het bericht
exp	<string>	Tijdstempel maximale geldigheid van de claims (EPOCH)
nbf	<string>	Tijdstempel van ingangsmoment geldigheid van de claims (EPOCH)
loa_authn	<string>	URI van de betrouwbaarheidsniveau van de authenticatie vanuit de authenticatieverklaring
loa_uzi	<string>	URI van Betrouwbaarheidsniveau van de zorgidentiteit

Als in het UZI-register geen relatie is gevonden voor de combinatie BSN + URA van de zorgaanbieder waarop de gebruiker probeert in te loggen, zullen er geen 'relations' worden opgenomen in het antwoordbericht. Dit treedt op wanneer een zorgverlener probeert in te loggen bij een zorgaanbieder waar geen (arbeids-) relatie (meer) mee bestaat in het UZI-register.

2.10 OpenID scope(s)

In de PoC worden door de OIDC-gateway de volgende scopes ondersteund:

openid : levert user data object met daarin de vastgestelde zorgidentiteit

NB: in een volgende versie kunnen mogelijk aanvullende scopes worden toegevoegd.

2.11 Geen single sign-on (SSO) en logout

Er wordt door de OIDC-gateway 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 de OIDC-gateway geen (inlog) sessie bewaard, wordt er ook geen logout functionaliteit aangeboden.

De OIDC-gateway levert (enkel) een zorgverlenersidentiteit op die door de zorgaanbieder kan worden gebruikt, ook bij in het ophalen van gegevens

via systeemkoppelingen bij derden. Het ophalen van gegevens vindt altijd plaats onder de verantwoordelijkheid van de zorgaanbieder. Het sessiebeheer voor dit soort uitwisselingen behoort tot de verantwoordelijkheid van de zorgaanbieder, die er zelf SSO-achtige functionaliteit mee kan ontwikkelen.

4. Aanvraag aansluiting op PoC infrastructuur

Een leverancier of zorgaanbieder die ervaring wil opdoen met de oplossing die binnen het project wordt ontwikkeld, zowel voor het onderdeel 'identiteitsvaststelling' als 'digitaal signeren', kan een aanvraag indienen om een aansluiting te krijgen.

- De aanvraag wordt per e-mail gedaan bij de beheerder van de technische infrastructuur: helpdesk@rdobeheer.nl

- Het onderwerp van de mail moet duidelijk beschrijven dat het gaat om het aanvragen van een koppeling op de PoC-omgeving:

  "Verzoek tot aansluiting op PoC-omgeving UZI voor <naam-organisatie>"

- Via de mail moeten de volgende gegevens aangeleverd:
  1. De URA van de zorgaanbieder;
  2. Redirect URI (s) van de aan te sluiten applicatie(s);
  3. Het publieke deel van een (self-signed/UZI/PKI-O) certificate (zie hoofdstuk Message Signing).

- De helpdesk van RDO-beheer is alleen op werkdagen tijdens kantooruren bereikbaar en levert de ondersteuning op de PoC-omgeving op basis van best-effort.

Wanneer uw organisatie niet beschikt over een URA, dan zal er voor deze PoC-omgeving door RDO-beheer een (fictieve) URA worden aangewezen.

5. 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.

A: Authorization request

```
https://poc-
1.uzi.bavod.nl/authorize?response_type=code&redirect_uri=https%3A%2F%2Fuzi-
test.nl%2Fprotected%2F&client_id=76543210&nonce=2ac278bbf8a9f9d701ac801488321
b61&state=b01d1af9128421ee7b079d18b21d865f&scope=openid&code_challenge=jS7z-
5-H3Pi0IWp3nTTGokJ0KvURQO6_v_wl2ApLvzk&code_challenge_method=S256
```

B: Request access token

```
https://poc-
1.uzi.bavod.nl/accesstoken?grant_type=authorization_code&code=9b896d0579
984ee6853762fe77644dd3&redirect_uri=https%3A%2F%2Fuzi-
test.nl%2Fprotected%2F&client_id=76543210&code_verifier=9896b3a21cddb9d
e8063503cffec3652537a9bc4e6d0718d4e16dc
c1dde059c7e2f593a6739aa5b18976b18c5e78c8c2e94d77140b0fbc0d0ce8ef448
ecdc558
```

C: Request authorized resource (user info request)

```
https://poc-1.uzi.bavod.nl/userinfo?schema=openid

HTTP-header: Authorization: Bearer 8217de98ccc84c878a67c7bc4adb5b99
```

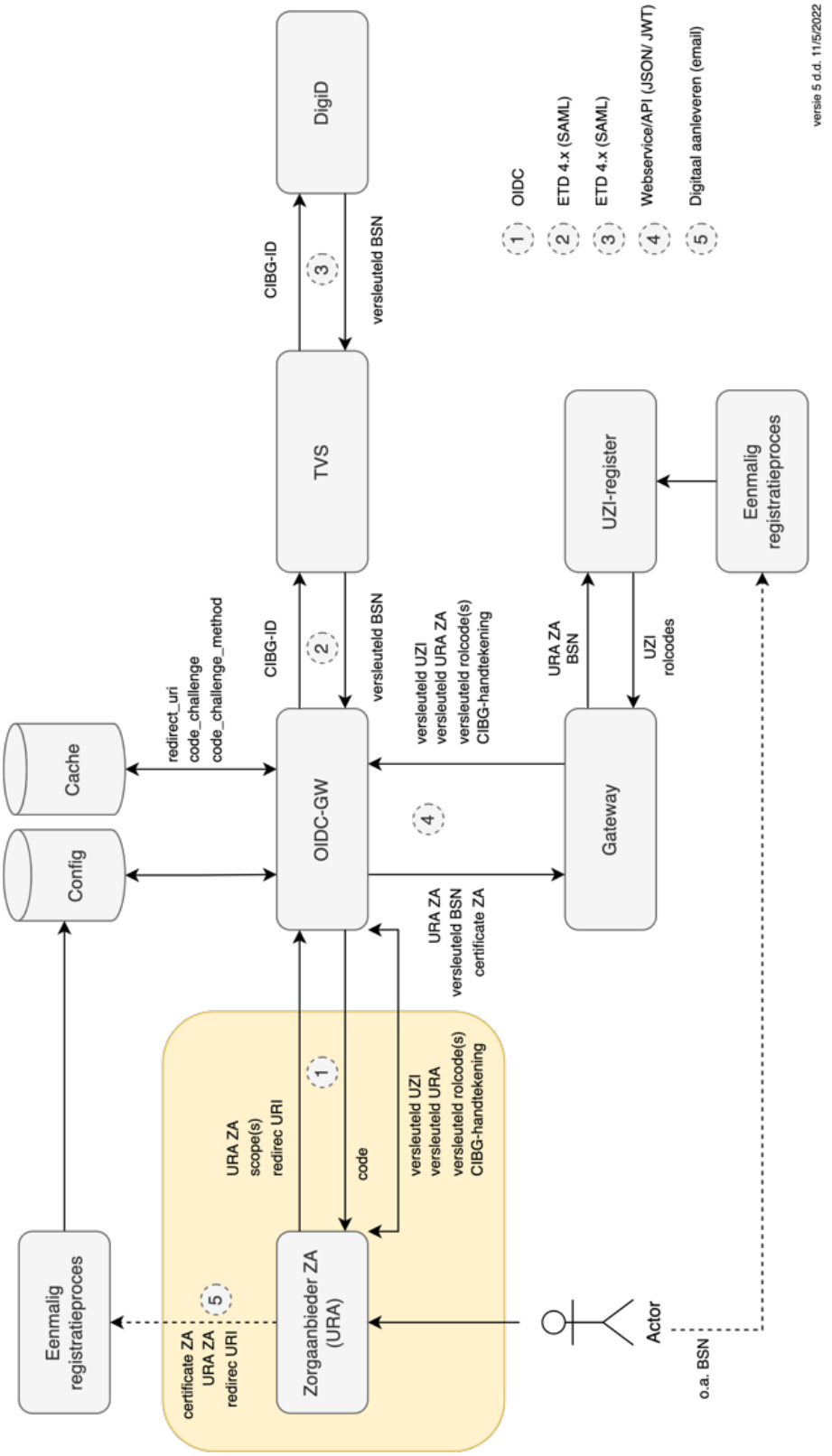
D: User data object (voor zorgaanbieder versleutelde, door CIBG gesignde payload)

eyJ0eXAiOiJKV1QiLCJhbGciOiJSU0EtT0FFUCIsImVuYyI6IkExMjhDQkMtSFMyNTYiLCJ4NXQiOiJkVFFralFaRlBsUk1seDlON204VDk0dVYySWs9In0.bwcAY9wzL8zHbvKfX-3qCDGUlGWoA5QhDhm8b5CPdrJFZJ91A-tbBScDI9dIrqItzpm6kxj07K2G1owbzCWaOXCCNq-W8DF_QUV5TybCFe1HEn2vS141DGimpKgolH01kuJZi_DW3OlgK279iqKipQeA8wGBPABzpxv8G3H5yy
IJZ-3aImmCBywOEXaQoAIcL07PmQ5zTFCzRZltIIX5qKEpuyFdY26xMDfRul-I2be7h-OhHTBPcn1yYye4igkXDt1_ZsxhDnEDtdpD3T0DlINDjlimuAv76UeEkR89vp7jyg0RaLwgIG3p5P2QxN7FM2
tJVcnC5SUcCfPGmp6qtfZkdMaG3fjxWK48oARVG6jdS_f7fCRVFXLMg3wta_Ee6gwHE8dZGXQgECJG8QAZPKk_fRa_ZKZ8br7zs3e1U_hoWNJZ0SR_rvr3E3I4GevKHcCF10lljGzk4xStW93lFkhV4C
yTXYlFingB8KlBSWxZfvMlo1ps1FD0mWWHWzF7g2OhkVqNmnIluYpb9fVJBQQRdJc9WzNhdDia_Tk-RXxWYctRfzv1mjsgB8q7oBHSqlLRNBMOZyN6FXTDm3b2aPQs1XRWEzxyIFT_SeMYe10vnAWFL2
7-sJDIiVhWcx8_t6f9s0XCNO7TXuKV5SMnTQI-kya5Pr9R957vAAp5msQ.HmxFp-zLBzOS-dq_JsYBJg.1WlYiqiBfNtb4HiSw8YhpHPWZ_TqEZnGZTSxCM6Ri821rTUtsz4RrWt8t-2KPvMjyjj76Tz
VTiTJD6XHmYDen_hdYMgf6bGLfkN3OYpD9fjXC8POwLyw7zOkFl23UuaVJ2S5p_U0rTW94c7Ov7xx4LPahp7uvrsBKKG5B-yeBvBtJDk8XDwMpEYAzBU3t1A09FzLXMe-enc_ImMb4w2etN_MmAymtS-JJnnoxglBO39AQW9Khj7OPUrU1lRAAqvlNcARkkqxsSXq9L2NI36QkfOs6WE9SHSq_wTacJnilvuXan5dtxwEcvYQfznH7BeKsoPsC_LXSP9FN49pEyhgMSgUTUVsSXcV-juu8ncl8-ei6l2io4akvRI
pwL6nDXp3or1UfyU8scBCdZmtP9JSE6a_G0IKheH4kidvbAhswnbVD1w7Eanu0B_GRmL1jcVk8v9Bm5PWCxGkroW4-2Cs-5u1nAnMNFQH-EUpNYlleV3tgHdlMO5idhZ5hXjRWX0i98KNZyl01OQZcaX
LlMSvtY3__ZhxLfrG0cK6q_zA4ddLv9fa8kYP2rsjJBGrsnGUJEWmNwlc6QFnlkbf4Cvln3mkztviUZVwtByeQIVSF9bAuvg2ZnGtdzk9_e26uL_7iWdqyRbSpH_PqfNB0PljkLjtzXWpZaGwBpv2Vbz
1mTRHdsF89EV_stwQnNIlD84fsrb5yUtJWv1tS3XPkeNh2NpV89ixik8tJ3rOunQU85HbcZC1ZTdQF2scZ63rGgctRLklJ-TP2eJqng6WLEH26v5P46mRplLVFOZsseOjDseTL4vHt_MJgYbZV_9LH23
aZ84i3ci46x3UmcrpBktk_a2uyXGsFiex6CENvbT5HaVmV5ICGlcuhzH38ePwgF7Tj5UxyvGlCh3J4grQRGYJSQ.yN6cQwX4t81r-XdbubiP8g

D: User data object ontsleutelt door zorgaanbieder


```
{
    "json_schema": https://www.inge6.nl/json_schema_v1.json,
    "request-id": "dbcc3cb0-1ddf-412b-9f1e-66b448773b24",
    "iss": "test_issuer",
    "aud": "test_audience",
    "exp": 1658229240,
    "nbf": 1658228340,
    "loa_authn": http://eidas.europa.eu/LoA/substantial,
    "loa_uzi": http://www.uziregister.nl/loa/1.0/eidas-high,
    "initials": "J.J.",
    "surname_prefix": "van der",
    "surname": "Waarden",
    "uziNumber": "900020108",
    "relations": [
        {
            "uraname": "Ziekenboeg B.V.",
            "roles": [
                "01.041"
            ],
            "uranumber": "87654321"
        }
    ]
}
```

Bijlage 1 Componenten onderdeel 'identiteitsvaststelling'



Bijlage 2 Sequentiediagram onderdeel 'identeitsvaststelling'