PvE Zorgverlener Namens Patiënt (ZNP)

Datum:	28 juni 2021
Status:	Definitief
Versie:	3.8.0
Classificatie:	Vertrouwelijk
Eigenaar:	VZVZ
Revisie:	

Documenthistorie

Documentnaam	Locatie
VZVZ_Mitz_PvE_ZNP_Zorgverlener_Namens_Patient_v3.8.0.docx	Confluence

Documentversies

Datum	Status	Versie	Omschrijving	Auteur
15-03-2020	Concept	3.6.0.0	Initiële versie	Pieter van Gemeren
03-04-2020	Ter goedkeuring	3.6.0.0	Ter goedkeuring versie 3.6.0.0 release na interne review	F. Schipper
01-05-2020	Ter goedkeuring	3.6.0.1	Bewaartermijn toegevoegd	D. Donker
05-06-2020	Ter goedkeuring	3.6.0.2	Logging toegevoegd	D. Donker
24-06-2020	Ter goedkeuring	3.6.1	Eisen OTV-ZNP-AS-0920 en OTV-ZNP-AS-0930 toegevoegd	D. Donker
16-07-2020	Ter verbetering	3.6.2.TV	Interne review versie 3.6.2 release	F. Schipper
28-07-2020	Ter goedkeuring	3.6.2.TG	Externe review versie 3.6.2 release	F. Schipper
06-08-2020	Concept	3.7.0.01	Uitwerking migratie	F. Schipper
16-09-2020	Ter verbetering	3.7.0.TV	Uitwerking migratie interne review v3.7.0	F. Schipper
30-09-2020	Ter goedkeuring	3.7.0.TG	Uitwerking migratie externe review v3.7.0	F. Schipper
27-01-2021	Concept	3.8.0.C	Uitwerking toestemmingsknop	N. Anbeek
24-03-2021	Ter verbetering	3.8.0.TV	Versnelde toestemmingsknop aangepast, zodat ook Spoedtoestemmingen goed verwerkt worden.	N. Anbeek
04-05-2021	Ter goedkeuring	3.8.0.TG	Externe review versie 3.8.0 release	N. Anbeek
28-06-2021	Definitief	3.8.0.D	Transactietoken ondertekend met UZI-pas	D. Donker

Accordering

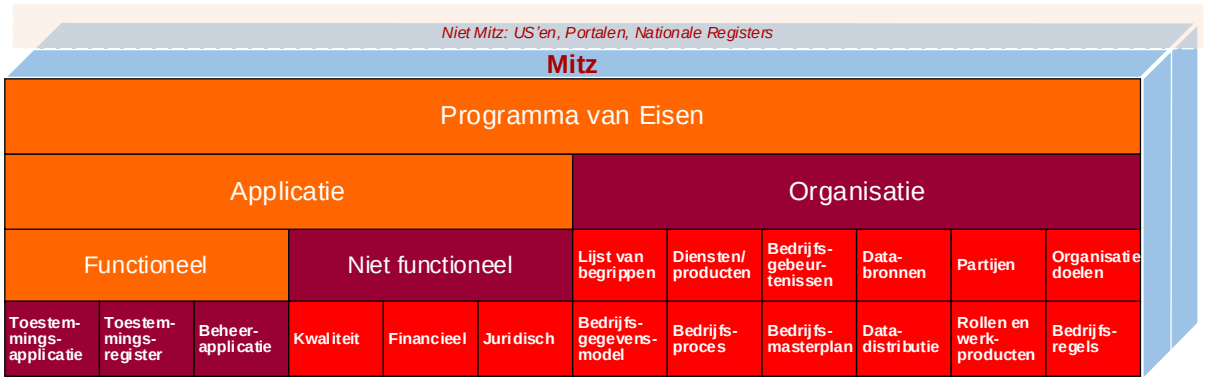
Datum	Status	Versie	Wie
17-04-2020	Definitief	3.6.0.0	A. Vlug
06-07-2020	Definitief	3.6.1	A. Vlug
06-08-2020	Definitief	3.6.2	A. Vlug
30-11-2020	Definitief	3.7.0	A. Vlug
28-06-2021	Definitief	3.8.0	A. Vlug

Inhoudsopgave

1 Inleiding

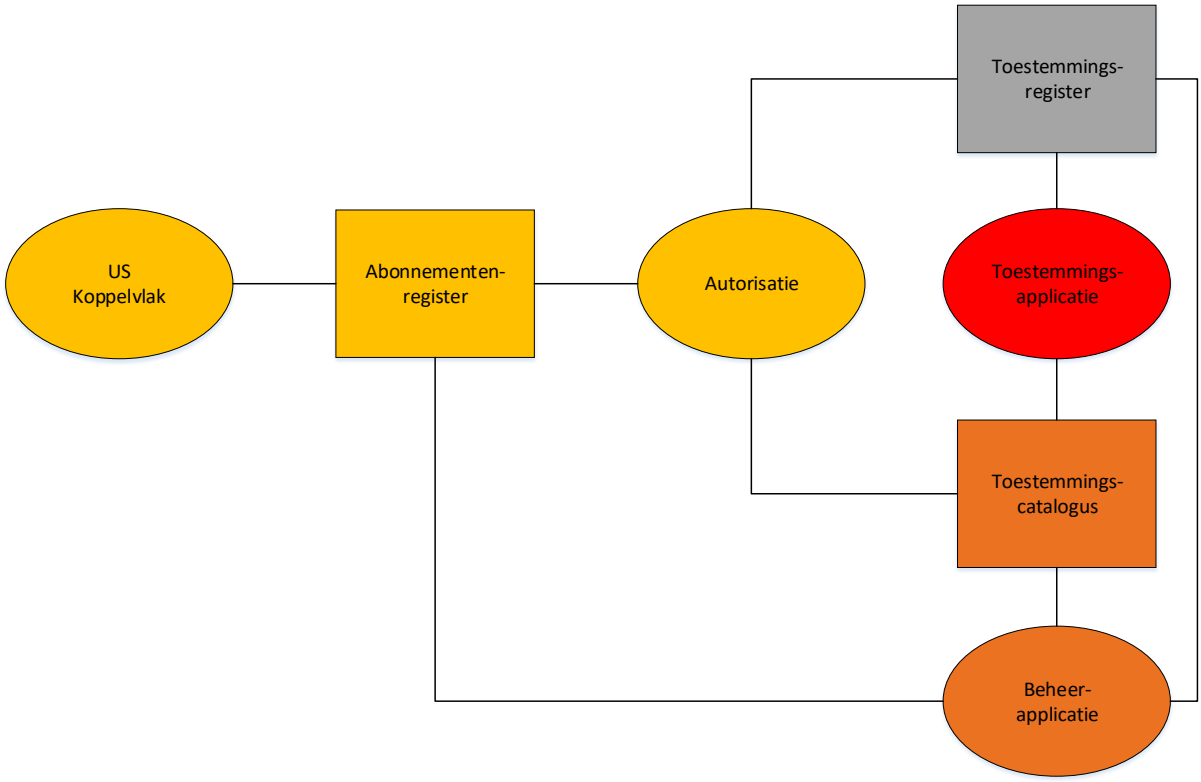
Het voorliggende document maakt deel uit van een programma van eisen (PVE) voor de online toestemmingsvoorziening Mitz. Een oplegger voor dit programma bevat een algemene inleiding over de verschillende soorten vereisten, de samenhang van de documenten en informatie over afkortingen versienummering, et cetera. Deze oplegger linked naar het voorliggende document volgens onderstaande structuur.

- Mitz
  - Applicatief
    - Functioneel
      - [PVE TAP] Toestemmingsapplicatie
      - [PVE REG] Eisen aan toestemmings-/abonnementenregister
      - [PVE BAP] Beheerapplicatie en toestemmingscatalogus
    - Niet functioneel
      - [PVE NF] Non functionals
- Niet Mitz (aansluitende systemen)
  - [PVE AUS] Aansluiteisen uitwisselingssystemen
  - **[PVE ZNP] Zorgaanbieder legt toestemmingskeuzes vast namens patiënt'**



1.1 Toelichting eisen koppeling ten behoeve van ZNP

Het voorliggende document bevat de functionele eisen van de koppeling met Mitz om als zorgaanbieder toestemmingskeuzes namens de patiënt vast te leggen of te wijzigen. Deze maken deel uit van de set van functionele eisen. Daar waar relevant verwijzen codes in de vereisten naar een model in een logische architectuur document zoals bijvoorbeeld "Contextdiagram – registreren/inloggen/persoonsgegevens". De technische specificaties zijn opgenomen in de 'Implementatiehandleiding ZNP'.



1.2 Uitleg presentatie van eisen

De eisen die in dit document zijn opgenomen, worden uniform gepresenteerd waardoor ze makkelijker leesbaar zijn geworden. De gebruikte tabel per eis bevat de tekst van de eis en uitleg ten aanzien van de functie en de applicatie waar de eis mede op van toepassing is.

Sommige vereisten bevatten een tekst tussen dubbele aanhalingstekens, “ … “. Deze tekst is dan bedoeld ter illustratie en is ook wijzigbaar.

2 Uitgangspunten betrouwbaarheid registratie

2.1 Auteur van toestemmingskeuze

Voor het delen van gegevens waar uitdrukkelijke toestemming voor vereist is, kunnen zorgaanbieders via Mitz vaststellen of deze toestemming is vastgelegd. De auteur van deze toestemming moet onweerlegbaar en eenduidig zijn.

Als de patiënt zelf inlogt met DigiD in MijnMitz en toestemmingskeuzes vastlegt, is de patiënt zowel ‘auteur’ als ‘betrokkene’ (over wie de gegevens gaat).

Als de patiënt zich (te zijner tijd) laat vertegenwoordigen, kan er via DigiD-Machtigen een auteur gemachtigd worden om voor de betrokken patiënt gegevens vast te leggen. Een gemachtigde kan met een eigen DigiD inlogmiddel zelf de toestemmingskeuzes vastleggen voor de patiënt en de patiënt krijgt daarvan een melding in zijn of haar meldingenbox en kan daar desgewenst een e-mail notificatie van krijgen.

Een patiënt kan ook aan een zorgverlener vragen om het vastleggen van toestemmingskeuzes namens hem uit te voeren in Mitz. De zorgverlener is dan de 'auteur' en de patiënt is de 'betrokkene'.

Als de zorgverlener de auteur is van toestemmingskeuzes van de patiënt, dient hij minimaal in te loggen op hetzelfde betrouwbaarheidsniveau als de patiënt (en als een gemachtigde). Dat is substantieel zodra dit breed beschikbaar is, en tot die tijd: minimaal met een 2e-factor. Een UZI-pas-op-naam is hiervoor te gebruiken en heeft al niveau ‘substantieel’.

Mitz voert de authenticatie zelf uit, zodat er altijd zekerheid is over de auteur. Alle betrokken partijen mogen er op vertrouwen dat Mitz rechtmatige toestemmingskeuzes bevat, waarvan de auteur onweerlegbaar is vastgelegd.

Vanwege de traceerbaarheid en aansprakelijkheid is de auteur een persoon en geen organisatie of systeem. Een medewerker kan zich (eenmalig) laten mandateren door een zorgverlener (met een UZI-pas).

De eisen om toegang te krijgen tot Mitz worden in dit document beschreven.

2.2 Gebruik van geverifieerd BSN

Mitz vereist dat er op alle koppelvlakken gebruik wordt gemaakt van een geverifieerd BSN. Zorgaanbieders kunnen na het vaststellen van de identiteit van een persoon (vergewissen of WID-controle) het BSN verifiëren door bijvoorbeeld een check bij SBV-Z. Pas daarna worden medische gegevens in een elektronisch dossier gezet.

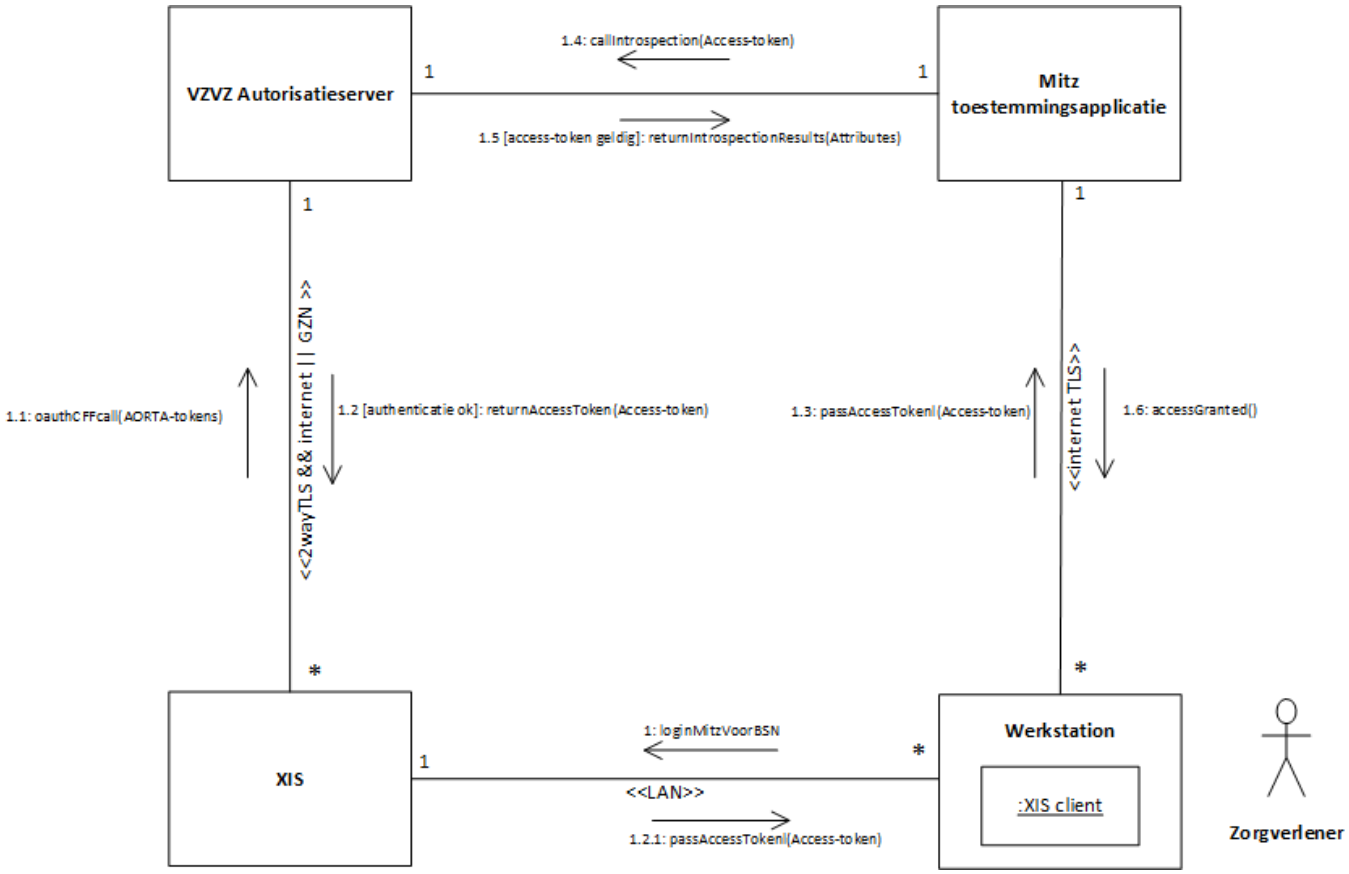
De link naar Mitz vanuit een zorgaanbiedersysteem zal plaatsvinden nadat de zorgverlener of medewerker is ingelogd en een ingeschreven patiënt geselecteerd heeft. In het proces van een zorgaanbieder kan het wenselijk of noodzakelijk zijn om eerst een inschrijftoken aan te maken en daarna pas de check bij SBV-Z uit te voeren. Dat wordt in Mitz ondersteund: in het inschrijftoken kan de (geplande) datum van de SBV-Z check worden opgenomen en het token kan ondertekend worden door de zorgmedewerker zelf. Een dergelijk token mag pas worden vrijgegeven voor gebruik in een Mitz koppelvlak (bijvoorbeeld ZNP), nadat de check succesvol is afgerond.

Vanwege de informatiebeveiliging wordt dit BSN veilig vanuit het zorgaanbiedersysteem in de aanroep van Mitz opgenomen.

3 Secure Link

3.1 Flow

OTV-ZNP-SL-0100 – Clients Credentials Flow	
Voor het inloggen van een zorgverlener en het veilig doorgeven van een BSN, wordt de open standaard OAuth 2.0 gebruikt en daarvan de 'client credentials flow' (CCF).	
Functie	Op een standaard manier een client authenticeren en attributen met relevante gegevens veilig meegeven vanuit het XIS aan Mitz.



De in de UML-tekening genoemde stappen worden in de navolgende eisen beschreven. De zorgverlener is de gebruiker van het werkstation (XIS client).

3.2 Gebruik van tokens

OTV-ZNP-SL-0200 – Mandaattoken	
Een zorgverlener die een medewerker mandateert voor de 'zorgaanbieder namens patiënt'-functie in Mitz, ondertekent het mandaattoken, dat zijn systeem genereert, eenmalig met zijn persoonlijke UZI-pas.	
Functie	De verantwoordelijke zorgverlener moet onweerlegbaar te identificeren zijn.
Toelichting	Het mandaattoken is gedefinieerd in de Implementatiehandleiding ZNP. Het ondertekenen kan desgewenst met Zorg-ID worden uitgevoerd.

OTV-ZNP-SL-0300 – Inschrijftoken	
Een zorgaanbieder die voor een patiënt toestemmingskeuzes wil vastleggen, kan dat alleen doen voor patiënten die zijn ingeschreven in zijn systeem. De zorgverlener of (balie)medewerker die een patiënt inschrijft, ondertekent het inschrijftoken dat het zorgsysteem genereert, eenmalig (bijvoorbeeld bij de inschrijving) met zijn persoonlijke UZI-pas.	
Functie	De patiënt en diens BSN dienen geverifieerd te zijn en dit geverifieerde BSN gaat naar Mitz om onweerlegbaar de identiteit van de patiënt (als betrokkene) vast te leggen in de toestemmingskeuzes.
Toelichting	Het inschrijftoken is gedefinieerd in de Implementatie Handleiding ZNP. Het ondertekenen kan desgewenst met Zorg-ID worden uitgevoerd.

OTV-ZNP-SL-0400 – Transactietoken	
Op het moment dat een medewerker van een zorgaanbieder naar Mitz wil gaan om toestemmingskeuzes voor een patiënt te bepalen, zal het systeem waar de zorgaanbieder ingelogd is, een transactietoken aanmaken en ondertekenen met het UZI-servercertificaat van die zorgaanbieder of met de UZI-pas van de zorgverlener.	
Functie	De zorgaanbieder (als organisatie) wordt onweerlegbaar vastgelegd bij elke aanroep naar Mitz, zodat een patiënt kan zien (in MijnMitz) vanuit welke zorgaanbieder namens hem toestemmingskeuzes zijn vastgelegd.
Toelichting	Het transactietoken is gedefinieerd in de Implementatie Handleiding ZNP. Het ondertekenen kan desgewenst met Zorg-ID worden uitgevoerd. Indien het transactietoken ondertekend is met de UZI-pas van een zorgverlener, dan biedt dit token voldoende waarborg en zijn mandaattoken en inschrijftoken niet meer nodig.

3.3 Aanroep naar Mitz website

OTV-ZNP-BTN-0500 – Activeren link naar Mitz	
Een medewerker van een zorgaanbieder kan de link naar Mitz pas activeren nadat hij is ingelogd op het systeem van de zorgaanbieder en een ingeschreven patiënt heeft geselecteerd. Om toegang te krijgen tot Mitz, dient er via de autorisatieserver een access token gegenereerd te worden.	
Functie	De attributen met gevoelige informatie (onder andere BSN) van de aanroep worden niet via een webbrowser over het netwerk verstuurd, maar via een 'beveiligde back channel' die door Mitz kan worden geraadpleegd.
Toelichting	De URL van de autorisatieserver is gedefinieerd in de Implementatie Handleiding ZNP.

OTV-ZNP-BTN-0560 – Up-to-Date Browser	
Om toegang te krijgen tot Mitz, dient de XIS-client gebruik te maken van een up-to-date browser.	
Functie	Vermijden beveiligingslekken door een verouderde browser.
Toelichting	De XIS-beheerder is verantwoordelijk voor het up-to-date houden van browserfaciliteiten.

OTV-ZNP-BTN-0580 – TLS (XIS)

Om toegang te krijgen tot Mitz dient de XIS-client de volgende kenmerken te accepteren: • tweezijdige authenticatie met behulp van het UZI-servercertificaat van het XIS en het servercertificaat van de autorisatieserver; • tijdelijke sleutels die periodiek ververst worden; • gebruikmakend van versies en algoritmes die door het NCSC minimaal worden gekenmerkt als goed en tevens worden ondersteund door de autorisatieserver; • een maximale sessieduur.	
Functie	Een voldoende hoog beveiligingsniveau waarborgen bij het opzetten van een tweezijdige TLS-sessie tussen XIS en autorisatieserver.
Toelichting	De NCSC-richtlijnen zijn gepubliceerd in het document: ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS).

3.4 Communicatie met autorisatieserver

OTV-ZNP-AS-0600 – Aanroep autorisatieserver

In de aanroep vanuit het systeem van de zorgaanbieder (‘XIS-server’ zie plaatje stap 1.1) worden mandaattoken, inschrijftoken en transactietoken samen met de geboortedatum van de patiënt als payload van de HTTP call opgestuurd naar de autorisatieserver.	
Functie	De tokens vormen het authenticatie mechanisme.
Toelichting	Het meesturen van de tokens is gedefinieerd in de Implementatie Handleiding ZNP.

OTV-ZNP-AS-0700 – Sessie met autorisatieserver

De sessie tussen het systeem van de zorgaanbieder (‘XIS’) en de autorisatieserver valt binnen de scope van de NEN:7510, 7512 en 7513 normering van de zorgaanbieder. Ook is de AVG hier van toepassing, aangezien er persoonsgegevens worden uitgewisseld.	
Functie	Beveiligde lijn opzetten om een access token te verkrijgen.

OTV-ZNP-AS-0800 – Relatie tussen sessies

De sessie tussen het systeem van de zorgaanbieder (‘XIS’) en de autorisatieserver moet eenduidig verbonden zijn met de sessie tussen XIS en werkstation waarop een patiënt is geselecteerd en tussen het werkstation en de Mitz-website waarop de inlogactie plaats heeft.	
Functie	Patiëntverwisseling tijdens de OAuth flow mag niet voorkomen.

OTV-ZNP-AS-0801 – Binding tussen gebruiker, patiënt en de sessies

De gebruiker, de door de gebruiker geselecteerde patiënt en de in dit kader opgezette sessies horen bij elkaar.	
Functie	Patiëntverwisseling tijdens de OAuth flow mag niet voorkomen.
Toelichting	Voorbeelden waarmee de binding tussen XIS en werkstation gerealiseerd kan worden zijn: • openID connect intern • OAuth intern • terminal services • Windows authenticatie (NTLM / Kerberos)

OTV-ZNP-AS-0900 – Access token verkrijgen

Het systeem van de zorgaanbieder ('XIS') moet in staat zijn het access token dat door de autorisatieserver wordt gegenereerd te ontvangen (stap 1.2). De autorisatieserver stuurt pas een access token terug indien het XIS geauthenticeerd is en de 3 tokens gevalideerd konden worden. Het access token wordt door de autorisatieserver ondertekend teruggestuurd.	
Functie	Op een veilige manier controleren of de zorgaanbieder, de medewerker en de patiënt geauthenticeerd kunnen worden.
Toelichting	Het access token is een JWT-assertion en kan een 'random block' aan data bevatten. Op basis van die data kan Mitz bepalen welke attributen horen bij een sessie met een werkstation, zonder dat de data in de sessie tussen werkstation en Mitz mee hoeven te gaan (minder veilig).

OTV-ZNP-AS-0910 – Geldigheidsduur access token

Het access token heeft een geldigheidsduur van maximaal 15 minuten.	
Functie	Limitatie van de geldigheidsduur van het access token
Toelichting	De geldigheid van het token verloopt 15 minuten na de aanmaaktijd.

OTV-ZNP-AS-0920 – Random nummer generator

Bij de creatie van het token ID van het access token dient gebruik gemaakt te worden van een cryptografische random nummer generator.	
Functie	Creatie van een willekeurige versie 4 UUID met voldoende entropie ten behoeve van het token ID.
Toelichting	De random number generator dient te voldoen aan de eisen zoals gespecificeerd in [NIST SP 800-90A Recommendation for Random Number Generation Using Deterministic Random Bit Generators].

OTV-ZNP-AS-0925 – Beveiliging Secret

Het secret waarmee het access token ondertekend wordt, dient eenmalig gegenereerd te worden en minimaal 256 bit groot te zijn. Het secret dient dusdanig bewaard te worden zodat alleen geautoriseerde systeembeheerders er toegang toe hebben.	
Functie	Voorkomen van misbruik.
Toelichting	Het secret kan bijvoorbeeld in de password store binnen de applicatie opgeslagen worden.

OTV-ZNP-AS-0930 – Systeemgebonden vertrouwensmiddel

De autorisatieserver is voorzien van een geldig systeemgebonden vertrouwensmiddel (PKIo-certificaat met bijbehorende private sleutel) dat op naam staat van de Mitz-opdrachtgever en dat is uitgegeven door een CA onder de root van de Staat der Nederlanden. De autorisatieserver dient dit vertrouwensmiddel zodanig te beschermen dat dit niet kan worden gestolen of zonder toestemming van de Mitz-opdrachtgever kan worden gekopieerd, gewijzigd of verwijderd en moet daarbij voldoen aan de eisen van de CA.	
Functie	Het veiligstellen van het systeemcertificaat van de autorisatieserver.
Toelichting	Zie ook de "Certification Practice Statement" (CPS) van PKIoverheid.

OTV-ZNP-AS-0950 – TLS

De autorisatieserver dient TLS-sessies, opgezet vanuit een XIS, met de volgende kenmerken te accepteren: • tweezijdige authenticatie met behulp van het UZI-servercertificaat van het XIS en het servercertificaat van de autorisatieserver; • tijdelijke sleutels die periodiek ververst worden; • gebruikmakend van versies en algoritmes die door het NCSC minimaal worden gekenmerkt als goed en tevens worden ondersteund door de autorisatieserver; • een maximale sessieduur.	
Functie	Een voldoende hoog beveiligingsniveau waarborgen bij het opzetten van een tweezijdige TLS-sessie tussen XIS en de autorisatieserver.
Toelichting	De NCSC richtlijnen zijn gepubliceerd in het document: ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS).

OTV-ZNP-AS-0960 – Token-validaties

De autorisatieserver dient de ontvangen tokens te valideren en te controleren of de voor de ondertekening gebruikte certificaten geldig zijn en zijn ondertekend met UZI-middelen.	
Functie	Een voldoende hoog beveiligingsniveau waarborgen zonder de zorgaanbieder te belasten met extra administratieve taken.
Toelichting	De token-validaties zijn gedefinieerd in de Implementatie Handleiding ZNP.

3.5 Communicatie met Mitz

OTV-ZNP-TV-1000 – Inloggen bij Mitz

Het access token wordt in de sessie tussen het werkstation en Mitz verzonden naar Mitz (stap 1.3). Nadat Mitz het access token heeft gevalideerd (bij de autorisatieserver) en de bijbehorende attributen (van de autorisatieserver) heeft ontvangen, is de medewerker van de zorgaanbieder ingelogd (stap 1.6) en kan het profiel aanpassen in opdracht van en namens de patiënt.	
Functie	Identiteit van auteur en betrokkene zijn onweerlegbaar bekend in Mitz, zonder deze gegevens over de lijn (tussen werkstation en Mitz) te versturen, zodat het bijbehorende profiel van de patiënt kan worden getoond aan de medewerker.
Toelichting	Het valideren van het access token door de autorisatieserver wordt geïnitieerd door webserver van Mitz en is de introspectie stap 1.4 en 1.5 in de OAuth flow.

OTV-ZNP-TV-1100 – TLS (werkstation)

Mitz dient TLS-sessies, opgezet vanuit een werkstation, met de volgende kenmerken te accepteren: • eenzijdige authenticatie met behulp van het servercertificaat van Mitz; • tijdelijke sleutels die periodiek ververst worden; • gebruikmakend van versies en algoritmes die door het NCSC minimaal worden gekenmerkt als goed en tevens worden ondersteund door de Mitz; • een maximale sessieduur.	
Functie	Een voldoende hoog beveiligingsniveau waarborgen bij het opzetten van een TLS-sessie tussen werkstation en Mitz.
Toelichting	De NCSC-richtlijnen zijn gepubliceerd in het document: ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS).

3.6 Bewaartermijn

OTV-ZNP-AS-0980 – Bewaartermijn access token en geassocieerde data

De autorisatieserver dient het uitgegeven access token en de daarmee geassocieerde data te bewaren gedurende de levensduur van het token of totdat een intrekking (revocation) is ontvangen. De revocation kan verstuurd zijn door de Mitz-toestemmingsapplicatie (resource server) of door het systeem van de zorgaanbieder (XIS-client).	
Functie	Het opruimen van gevoelige data.
Toelichting	Indien het access token verloopt of als een revocation wordt ontvangen, dient het token en de daarmee geassocieerde data verwijderd te worden van de autorisatieserver.

3.7 Logging

OTV-ZNP-LOG-0100 – Logging koppelvlak XIS – AS “Access token request”

De autorisatieserver logt bij het ‘verkrijgen access token’ (stap 1.2) de volgende gegevens:

- Transactietype [“token.oauth2”]
- Transactiedatum/tijd [DatumTijd]
- Zorgaanbieder [URA]
- UZI-nr_verantwoordelijke [UZI]
- PatientID [BSN]
- Uitvoerende_organisatie [IssuerSerial]
- Succes-status [OK/Foutcode]
- TokenID [jti]

Functie	Correcte logging
Toelichting	Bij de uitvoerende organisatie dient de IssuerSerial uit het certificaat, waarmee de TLS-verbinding is opgezet, overgenomen te worden. De Succes-status wordt gevuld met “OK” indien de aangeleverde tokens correct gevalideerd zijn, het access token is aangemaakt en geretourneerd aan het aanvragende XIS. Indien dit niet het geval is, dan wordt de Succes-status gevuld met de foutcode zoals gegenereerd volgens de respectievelijke implementatiehandleiding. Indien succesvol een access token is aangemaakt, dient tokenID gevuld te worden met het element “jti” (Jason Token Identifier), zie Implementatie Handleiding ZNP.

OTV-ZNP-LOG-0150 – Logging koppelvlak XIS – AS “Access token revocatie”

De autorisatieserver logt bij het ‘intrekken access token’ (zie eis OTV-ZNP-AS-0980) de volgende gegevens:

- Transactietype [“revoke”]
- Transactiedatum/tijd [DatumTijd]
- Uitvoerende_organisatie [IssuerSerial]
- Succes-status [OK/Foutcode]
- TokenID [jti]

Functie	Correcte logging
Toelichting	Bij de uitvoerende organisatie dient de IssuerSerial uit het certificaat, waarmee de TLS-verbinding is opgezet, overgenomen te worden. De Succes-status wordt gevuld met “OK” indien de aangeleverde tokens correct gevalideerd zijn, het access token is aangemaakt en geretourneerd aan het aanvragende XIS. Indien dit niet het geval is, dan wordt de Succes-status gevuld met de foutcode zoals gegenereerd volgens de respectievelijke implementatiehandleiding. TokenID wordt gevuld met het element “jti” (Jason Token Identifier), zie Implementatie Handleiding ZNP.

OTV-ZNP-LOG-0200 – Logging koppelvlak TAP – AS “Introspectie”

De autorisatieserver logt bij de ‘Introspectie’ (stap 1.4) de volgende gegevens:

- Transactietype [“introspect”]
- Transactiedatum/tijd [DatumTijd]
- Succes-status [OK/Foutcode]
- TokenID [jti]

Functie	Correcte logging

Toelichting	De Succes-status wordt gevuld met “OK” indien de aangeleverde tokens correct gevalideerd zijn, het access token is aangemaakt en geretourneerd aan het aanvragende XIS. Indien dit niet het geval is, dan wordt de Succes-status gevuld met de foutcode zoals gegenereerd volgens de respectievelijke implementatiehandleiding. TokenID wordt gevuld met het element “jti” (Jason Token Identifier), zie Implementatie Handleiding ZNP.

OTV-ZNP-LOG-0250 – Logging koppelvlak TAP – AS “Access token revocatie”

De autorisatieserver logt bij het ‘intrekken access token’ (zie eis OTV-ZNP-AS-0980) de volgende gegevens:

- Transactietype [“revoke”]
- Transactiedatum/tijd [DatumTijd]
- Uitvoerende_organisatie [IssuerSerial]
- Succes-status [OK/Foutcode]
- TokenID [jti]

Functie	Correcte logging
Toelichting	Bij de uitvoerende organisatie dient de IssuerSerial uit het certificaat waarmee de TLS-verbinding is opgezet overgenomen te worden. De Succes-status wordt gevuld met “OK” indien de aangeleverde tokens correct gevalideerd zijn, het access token is aangemaakt en geretourneerd aan het aanvragende XIS. Indien dit niet het geval is, dan wordt de Succes-status gevuld met de foutcode zoals gegenereerd volgens de respectievelijke implementatiehandleiding. TokenID wordt gevuld met het element “jti” (Jason Token Identifier), zie Implementatie Handleiding ZNP.

OTV-TAP-LOG-0300 – Logging koppelvlak TAP – AS “Introspectie”

De Toestemmingsapplicatie (TAP) logt bij de ‘Introspectie’ (stap 1.4) de volgende gegevens:

- Transactietype [“introspect”]
- Transactiedatum/tijd [DatumTijd]
- Zorgaanbieder [URA]
- UZI-nr_verantwoordelijke [UZI]
- PatientID [Pseudoniem]
- Geboortedatum [Datum]
- Succes-status [OK/Foutcode]
- TokenID [jti]

Functie	Correcte logging
Toelichting	Het pseudoniem van de PatientID wordt verkregen door het BSN direct naar de REG te sturen. De Succes-status wordt gevuld met “OK” indien de aangeleverde tokens correct gevalideerd zijn, het access token is aangemaakt en geretourneerd aan het aanvragende XIS. Indien dit niet het geval is, dan wordt de Succes-status gevuld met de foutcode zoals gegenereerd volgens de respectievelijke implementatiehandleiding. TokenID wordt gevuld met het element “jti” (Jason Token Identifier), zie Implementatie Handleiding ZNP.

4 Smart Link (nader te bepalen)

(niet in scope)

5 Toestemmingsknop

Het is mogelijk om, bijvoorbeeld in een XIS of een zorgaanbieder specifiek portaal, een toestemmingsknop in te bouwen. Deze toestemmingsknop geeft de mogelijkheid om de voor de zorgaanbieder relevante toestemmingsmogelijkheden te combineren en in één keer te beantwoorden. Hieronder zal steeds uitgegaan worden van een XIS.

Wanneer de toestemmingsknop wordt gebruikt, worden alle toestemmingsmogelijkheden die binnen deze toestemmingsknop zijn gedefinieerd, beantwoord met een Ja of een Nee.

Het XIS stuurt de betreffende toestemmingskeuzes naar het US. Het US stuurt op basis hiervan een toestemmingsbericht naar Mitz.

Het systeem dat de toestemmingskeuzes uit deze toestemmingsknop naar het US stuurt, dient een authenticatieniveau te hebben, die afhankelijk is van het type toestemmingsknop. Dit wordt beschreven in de overeenkomstige eisen.

Wanneer de toestemmingsknop wordt gebruikt door (een medewerker van) de zorgaanbieder, valt dit, vanuit juridisch en organisatorisch oogpunt, onder de ZNP-functie. Dat betekent dat de zorgmedewerker de auteur is van de toestemming en verantwoordelijk is voor authenticatie van en machtiging door de patiënt.

OTV-TK-0100 – Toestemmingsbericht

Voor alle vormen van de toestemmingsknop geldt dat het toestemmingsbericht de onderstaande gegevens bevat:

- Situatiecode behorende bij de toestemmingsknop;
- Identificatie van de patient (geverifieerd BSN);
- Geboortedatum van de patient;
- E-mailadres patiënt (optioneel);
- Telefoonnummer patiënt (optioneel);
- Authenticatieniveau toestemming;
- Unieke identificatie van de verantwoordelijke zorgverlener;
- Unieke identificatie van de uitvoerende zorgmedewerker (optioneel);
- Unieke identificatie van zorgaanbieder waar de verantwoordelijke zorgverlener en uitvoerende zorgmedewerker werkzaam zijn – doel: identificatie van de zendende zorgaanbieder;
- Unieke identificatie van de dossierhoudende zorgaanbieder, inclusief categorie – alleen in geval van toestemmingen aan individuele dossierhouders – doel: bepaling op welke zorgaanbieder de toestemming van toepassing is;
- Unieke identificatie van de raadplegende zorgaanbieder, inclusief categorie – alleen in geval van toestemmingen aan individuele raadplegers (voorbehouden aan raadplegende onderzoeksinstellingen, niet in scope)
- Toestemmingsantwoord (Ja/Nee);
- Datum en tijdstip van de vastlegging van de toestemming (vastleggingsmoment);
- Tekstuele weergave van de toestemming (optioneel).

De Situatiecode geeft aan voor welke zorgsituatie deze toestemmingen van toepassing zijn. In de toestemmingscatalogus zijn de Situatiecodes gedefinieerd die geïmplementeerd kunnen worden met de toestemmingsknop. Hierbij wordt ook vastgelegd welke set toestemmingsmogelijkheden hieraan gekoppeld is (zie eis OTV-TR-0105).
Bij de Situatiecode in de toestemmingscatalogus wordt een geldigheidsduur vermeld. De toestemmingskeuzes (uit de toestemmingsbundel) worden samen met de geldigheidsduur in de Situatiecode in het toestemmingsprofiel van de desbetreffende patiënt vastgelegd conform Eis OTV-TR-0100.

De geboortedatum van de patiënt wordt meegegeven om het voor het Toestemmingsregister mogelijk te maken om door middel van introspectie bij de Autorisatieserver de authenticiteit van het bericht te controleren.

Unieke identificatie van de dossierhoudende zorgaanbieder is alleen verplicht wanneer in de toestemmingscatalogus bij deze specifieke situatie is aangegeven dat deze voor dossierhoudend “Individueel” is.
Analoog geldt dat de unieke identificatie van de raadplegende zorgaanbieder verplicht en alleen verplicht is, wanneer bij deze specifieke situatie is aangegeven dat deze voor raadplegend “Individueel” is.

Bij de Situatiecode wordt een informatietekst voor de patiënt opgenomen, die in detail beschrijft welke toestemmingen hierop van toepassing zijn.
De zorgaanbieder is verplicht om de patiënt te informeren conform de informatietekst, die behoort bij de Situatiecode en ingebouwd is in het XIS.

De Situaties en Sets van toestemmingsmogelijkheden ten behoeve van de toestemmingsknoppen worden gedefinieerd in de toestemmingscatalogus.

Functie	Gebruikersgemak voor de zorgverlener
Toelichting	Alle varianten van de toestemmingsknop werken volgens deze eis.

OTV-TK-0110 – Standaard toestemmingsknop

Het is mogelijk voor een leverancier om een standaard toestemmingsknop in te bouwen. Deze standaard toestemmingsknop is een functionaliteit waarmee voor de desbetreffende patiënt een individuele toestemming aan de dossierhoudende zorgaanbieder wordt vastgelegd voor het delen van gegevens met alle raadpleegcategorieën.

De standaard toestemming is een specifieke invulling van de toestemminsknop die overeenkomt met de situatiecode voor de standaardsituatie. Deze is terug te vinden in de toestemmingscatalogus.

De toestemmingskeuze voor een individuele zorgaanbieder (dossierhoudend) en categorale zorgaanbieders (raadplegend) is weergegeven in de toestemmingscatalogus, doordat bij de situatiecode is aangegeven dat dit dossierhoudend “individueel” is en raadplegend “categoraal”.

Functie	Gebruikersgemak voor de zorgverlener

OTV-TK-0120 – Configureerbare toestemmingsknop

Het is mogelijk voor een leverancier om maximaal één configureerbare toestemmingsknop in te bouwen per werkstation (naast een optionele configureerbare toestemmingsknop voor een Spoedsituatie (niet in scope)). Deze configureerbare toestemmingsknop maakt het mogelijk om een set van toestemmingsmogelijkheden tegelijkertijd vast te leggen, die ook kunnen gelden voor andere dossierhouders.

Functie	Gebruikersgemak voor de zorgverlener

OTV-TK-0121 – Authenticatie configureerbare toestemmingsknop

Indien gebruik wordt gemaakt van de configureerbare toestemmingsknop, niet zijnde de standaard toestemmingsknop, dan dienen voor de authenticatie de tokens gebruikt te worden op de manier zoals beschreven bij de situatiecode.

De tokens die gebruikt dienen te worden in een specifieke situatie zijn gekoppeld aan de situatiecode en worden weergegeven en de definitie hiervan wordt beheerd in de Toestemmingscatalogus.

Functie	Op een standaard manier een client authenticeren en attributen met relevante gegevens veilig meegeven vanuit het XIS aan Mitz.

OTV-VTK-0122 – Configureerbare toestemmingsknop: Spoed (niet in scope)

Het is mogelijk voor een leverancier om de optionele configureerbare toestemmingsknop Spoed in te bouwen. Deze configureerbare toestemmingsknop Spoed bestaat uit dezelfde toestemmingsmogelijkheden in de Spoed-toestemmingsmogelijkheid bundel staan die in de TAP wordt gebruikt.

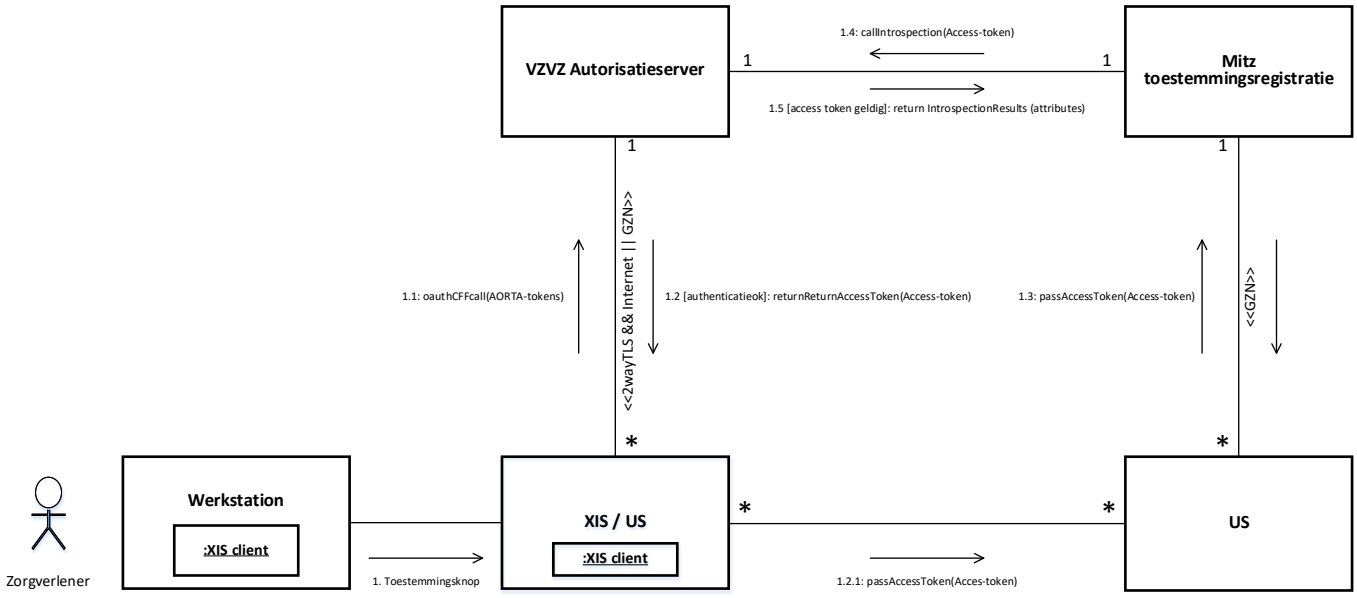
Deze toestemmingsknop functioneert conform de betreffende eisen voor de toestemmingsknop met een situatiecode voor een Spoedsituatie. De geldigheidsduur van de toestemmingen kan beperkt of onbeperkt zijn. Voor beide mogelijkheden is een aparte Situatiecode van toepassing.

Het is ook mogelijk om door middel van de configureerbare toestemmingsknop toestemmingen voor de raadpleegsituatie “Spoed” vast te leggen. In dit geval zal in de Set die bij de betreffende situatiecode hoort ook de keuzemogelijkheid “Spoed” worden opgenomen. Dit betekent dat deze toestemming geldig is voor alle toestemmingskeuzes waarvan in de toestemminscatalogus is aangegeven dat ze van toepassing zijn op “Spoed” en betrekking hebben op de raadpleegsituatie “Spoed”. Hiernaast zijn in de Set opgenomen “normale” toestemmingskeuzes ook nog geldig.
Functie | Gebruikersgemak voor de zorgverlener

5.1 Flow

OTV-TK-0130 – Clients Credentials Flow

Voor het gebruik van de toestemmingsknop door een zorgverlener en het veilig doorgeven van een BSN, wordt de open standaard OAuth 2.0 gebruikt en daarvan de ‘client credentials flow’ (CCF).
Functie | Op een standaard manier een client authenticeren en attributen met relevante gegevens veilig meegeven vanuit het XIS aan Mitz.



De in de UML-tekening genoemde stappen worden in de navolgende eisen beschreven. De zorgverlener is de gebruiker van het werkstation (XIS-client).

5.2 Gebruik van tokens

OTV-TK-0150 – Tokens

Voor het gebruik van de toestemmingsknop zijn de volgende eisen uit de Secure Link valide (indien het betreffende token vereist is voor de situatie): Eis OTV-ZNP-SL-0200 – Mandaattoken Eis OTV-ZNP-SL-0300 – Inschrijftoken Eis OTV-ZNP-SL-0400 – Transactietoken
Functie | Gedeelde eis(en)

5.3 Aanvragen access token

OTV-TK-0200 – Activeren link naar Mitz	
Een medewerker van een zorgaanbieder kan de toestemmingsknop pas gebruiken nadat hij is ingelogd op het systeem van de zorgaanbieder en een ingeschreven patiënt heeft geselecteerd. Om een toestemmingsbericht te kunnen samenstellen, dient er via de autorisatieserver een access token gegenereerd te worden.	
Functie	Het verkrijgen van gewaarborgde informatie met betrekking van auteur, verantwoordelijke en BSN.
Toelichting	De URL van de autorisatieserver is gedefinieerd in de Implementatie Handleiding ZNP.

OTV-TK-0210 – TLS (XIS)	
Zie Eis OTV-ZNP-BTN-0580 – TLS (XIS)	
Functie	Gedeelde eis

5.4 Communicatie met autorisatieserver

OTV-TK-0250 – Aanroep autorisatieserver	
In de aanroep vanuit het systeem van de zorgaanbieder ('XIS-server' zie plaatje stap 1.1) worden mandaattoken, inschrijftoken en transactietoken samen met de situatiecode en geboortedatum als payload van de HTTP call opgestuurd naar de autorisatieserver.	
Functie	De tokens vormen het authenticatie mechanisme.
Toelichting	Het meesturen van de tokens is gedefinieerd in de Implementatie Handleiding ZNP. In plaats van de XIS-server mag ook het US het access-token opvragen bij de Autorisatieserver.

OTV-AS-0800 – Relatie tussen sessies	
De sessie tussen het systeem van de zorgaanbieder ('XIS' of US) en de autorisatieserver moet eenduidig verbonden zijn met de sessie tussen XIS en werkstation waarop een patiënt is geselecteerd en tussen het werkstation en de toestemmingsknop.	
Functie	Patiëntverwisseling tijdens de OAuth flow mag niet voorkomen.

OTV-TK-0260 – Overige	
Voor het gebruik van de toestemmingsknop zijn de volgende eisen uit de Secure Link valide. Eis OTV-ZNP-AS-0700 – Sessie met autorisatieserver Eis OTV-ZNP-AS-0801 – Binding tussen gebruiker, patiënt en de sessies Eis OTV-ZNP-AS-0900 – Access token verkrijgen Eis OTV-ZNP-AS-0910 – Geldigheidsduur access token Eis OTV-ZNP-AS-0920 – Random nummer generator Eis OTV-ZNP-AS-0925 – Beveiliging Secret Eis OTV-ZNP-AS-0930 – Systeemgebonden vertrouwensmiddel Eis OTV-ZNP-AS-0950 – TLS Eis OTV-ZNP-AS-0960 – Token-validaties	
Functie	Gedeelde eis (en)
Toelichting	Aangezien het US ook het access token op mag vragen, dient in de bovengenoemde eisen in plaats van ('XIS') ('XIS of US') gelezen te worden.

5.5 Communicatie met Mitz

OTV-TK-0300 – Gebruik access token	
Het access token wordt toegevoegd aan het toestemmingsbericht en verzonden naar Mitz (stap 1.3). Nadat Mitz het access token heeft gevalideerd (bij de autorisatieserver) en de bijbehorende attributen (van de autorisatieserver) heeft ontvangen kan het toestemmingsregister het toestemmingsbericht verwerken.	
Functie	Identiteit van auteur en betrokkene zijn onweerlegbaar bekend in Mitz.
Toelichting	Het valideren van het access token door de autorisatieserver wordt geïnitieerd door het toestemmingregister van Mitz en is de introspectie stap 1.4 en 1.5 in de OAuth flow.

5.6 Bewaartermijn

OTV-TK-0350 – Bewaartermijn access token en geassocieerde data	
De autorisatieserver dient het uitgegeven access token en de daarmee geassocieerde data te bewaren gedurende de levensduur van het token of totdat een intrekking (revocation) is ontvangen. De revocation kan verstuurd zijn door het Mitz-toestemmingsregister (resource server) of door het systeem van de zorgaanbieder (XIS-client).	
Functie	Het opruimen van gevoelige data.
Toelichting	Indien het access token verloopt of als een revocation wordt ontvangen, dient het token en de daarmee geassocieerde data verwijderd te worden van de autorisatieserver. Bijvoorbeeld wanneer de REG of een XIS een onregelmatigheid constateert, dan moet het token ingetrokken worden.

5.7 Logging

OTV-LOG-0300 – Logging gebruik toestemmingsknop	
Conform NEN:7513 moet het gebruik van de toestemmingsknop worden gelogd.	
Functie	Correcte logging
Toelichting	In de onderstaande eisen is dit verder uitgewerkt.

OTV-LOG-0310 – Logging koppelvlak XIS – AS “Access token request”	
De autorisatieserver logt bij het ‘verkrijgen access token’ (stap 1.2) de volgende gegevens indien de AS daarover beschikt: • Transactietype [“token.oauth2”] • Transactiedatum/tijd [DatumTijd] • Zorgaanbieder [URA] uit transactietoken • UZI-nr_verantwoordelijke [UZI] uit mandaat token • PatientID [BSN] uit inschrijftoken • Uitvoerende_organisatie [IssuerSerial] • Succes-status [OK/Foutcode] • TokenID [jti]	
Functie	Correcte logging
Toelichting	Aangezien de AS, afhankelijk van de situatie(code), 1, 2 of 3 tokens aangereikt heeft gekregen is niet altijd alle informatie aanwezig. Indien ontbrekend wordt het veld leeggelaten. Bij de uitvoerende organisatie dient de IssuerSerial uit het certificaat, waarmee de TLS-verbinding is opgezet, overgenomen te worden. De Succes-status wordt gevuld met “OK” indien de aangeleverde tokens correct gevalideerd zijn, het access token is aangemaakt en geretourneerd aan het aanvragende XIS. Indien dit niet het geval is, dan wordt de Succes-status gevuld met de foutcode zoals gegenereerd volgens de respectievelijke implementatiehandleiding. Indien succesvol een access token is aangemaakt, dient tokenID gevuld te worden met het element “jti” (Jason web Token Identifier), zie Implementatie Handleiding ZNP.

OTV-LOG-0320 – Logging koppelvlak REG – AS "Introspectie"

De autorisatieserver logt bij de 'Introspectie' (stap 1.4) de volgende gegevens: • Transactietype ["introspect"] • Transactiedatum/tijd [DatumTijd] • Succes-status [OK/Foutcode] • TokenID [jti]	
Functie	Correcte logging
Toelichting	De Succes-status wordt gevuld met "OK" indien de aangeleverde tokens correct gevalideerd zijn, het access token is aangemaakt en geretourneerd aan het aanvragende XIS. Indien dit niet het geval is, dan wordt de Succes-status gevuld met de foutcode zoals gegenereerd volgens de respectievelijke implementatiehandleiding. TokenID wordt gevuld met het element "jti" (Jason web Token Identifier), zie Implementatie Handleiding ZNP. Het staat de REG vrij om te loggen wat nodig wordt geacht.

OTV-LOG-0330 – Logging koppelvlak REG – AS "Access token revocatie"

De autorisatieserver logt bij het 'intrekken access token' (zie eis OTV-ZNP-AS-0980) de volgende gegevens: • Transactietype ["revoke"] • Transactiedatum/tijd [DatumTijd] • Uitvoerende_organisatie [IssuerSerial] • Succes-status [OK/Foutcode] • TokenID [jti]	
Functie	Correcte logging
Toelichting	Bij de uitvoerende organisatie dient de IssuerSerial uit het certificaat waarmee de TLS-verbinding is opgezet overgenomen te worden. De Succes-status wordt gevuld met "OK" indien de aangeleverde tokens correct gevalideerd zijn, het access token is aangemaakt en geretourneerd aan het aanvragende XIS. Indien dit niet het geval is, dan wordt de Succes-status gevuld met de foutcode zoals gegenereerd volgens de respectievelijke implementatiehandleiding. TokenID wordt gevuld met het element "jti" (Jason Token Identifier), zie Implementatie Handleiding ZNP.

OTV-LOG-0340 – Logging koppelvlak REG – AS "Introspectie"

Het Toestemmingsregister (REG) logt bij de 'Introspectie' (stap 1.4) de volgende gegevens indien de REG daarover beschikt: • Transactietype ["introspect"] • Transactiedatum/tijd [DatumTijd] • Zorgaanbieder [URA] • UZI-nr_verantwoordelijke [UZI] • PatientID [Pseudoniem] • Geboortedatum [Datum] • Succes-status [OK/Foutcode] • TokenID [jti]	
Functie	Correcte logging
Toelichting	Aangezien de AS, afhankelijk van de situatie(code), 1, 2 of 3 tokens aangereikt heeft gekregen is niet altijd alle informatie aanwezig na introspectie van het access token. Indien ontbrekend is het veld leeggelaten. De Succes-status wordt gevuld met "OK" indien de aangeleverde tokens correct gevalideerd zijn, het access token is aangemaakt en geretourneerd aan het aanvragende XIS. Indien dit niet het geval is, dan wordt de Succes-status gevuld met de foutcode zoals gegenereerd volgens de respectievelijke implementatiehandleiding. TokenID wordt gevuld met het element "jti" (Jason Token Identifier), zie Implementatie Handleiding ZNP.

OTV-LOG-0990 – Token revocatie	
Voor het gebruik van de toestemmingsknop zijn de volgende eisen uit de Secure Link valide.: Eis OTV-ZNP-LOG-0150 – Logging koppelvlak XIS – AS “Access token revocatie”	
Functie	Gedeelde eis(sen)